ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ

ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ

ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

ΔΙΕΡΕΥΝΗΣΗ ΧΡΗΣΗΣ ΤΟΥ BLOCKCHAIN ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΜΕΤΑΝΑΣΤΕΥΤΙΚΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μάλλιου Ι. Ηλιάνας

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2020

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

ΔΙΕΡΕΥΝΗΣΗ ΧΡΗΣΗΣ ΤΟΥ BLOCKCHAIN ΣΤΗ ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ ΜΕΤΑΝΑΣΤΕΥΤΙΚΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Μάλλιου Ι. Ηλιάνας

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 18η Νοεμβρίου 2020

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Χάρης Δούκας
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2020

.....

Ηλιάνα Μάλλιου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Ηλεκτρονικών Υπολογιστών Ε.Μ.Π.

Περίληψη

Σκοπός της παρούσας διπλωματικής είναι η διερεύνηση της χρήσης της τεχνολογίας Blockchain στη διαχείριση των μεταναστευτικών και προσφυγικών ροών στην Ευρωπαϊκή Ένωση. Στο πρώτο κεφάλαιο πραγματοποιείται μία εκτενής μελέτη της τεχνολογίας Blockchain. Αναλύονται τα βασικά χαρακτηριστικά, η δομή και ο τρόπος λειτουργίας του Blockchain, καθώς και η διαδικασία δημιουργίας και επικύρωσης έξυπνων συμβάσεων (smart contracts). Επιπλέον, εξηγούνται οι τρόποι με τους οποίους επιτυγχάνεται η ασφάλεια σε ένα δίκτυο blockchain, οι οποίοι περιλαμβάνουν μεθόδους σύνθετης κρυπτογραφίας, το μηχανισμό ψηφιακής υπογραφής και τους μηχανισμούς συναίνεσης. Παρατίθενται παραδείγματα μηχανισμών συναίνεσης, καθώς και τύπων blockchain, τα οποία αναλύονται λεπτομερώς. Στο δεύτερο κεφάλαιο, μελετώνται στοιχεία σχετικά με τη μετακίνηση πληθυσμών μεταναστών και προσφύγων προς την Ευρωπαϊκή Ένωση. Πραγματοποιείται, επίσης, έρευνα σχετικά με το σχέδιο της Ευρωπαϊκής Ένωσης για τη διαχείριση των ροών αυτών των πληθυσμών, και παρουσιάζεται μία κριτική ανάλυση του σχεδίου αυτού. Στο τρίτο κεφάλαιο μελετάται, η Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain (EBSI). Αναλύονται οι στόχοι και τα οφέλη της υποδομής EBSI, καθώς και η αρχιτεκτονική και οι παρεχόμενες υπηρεσίες της. Μελετώνται όλα τα βασικά σενάρια χρήσης της υποδομής EBSI, με ιδιαίτερη έμφαση στην «Ευρωπαϊκή Αυτοδύναμη Ταυτότητα (ESSIF)», και στην υπηρεσία «Notarisation». Η υπηρεσία «ESSIF» δίνει τη δυνατότητα στους χρήστες να δημιουργούν και να διαχειρίζονται την ταυτότητά τους χωρίς να βασίζονται σε κάποια κεντρική αρχή, ενώ η υπηρεσία «Notarisation» παρέχει στους χρήστες τη δυνατότητα συμβολαιογραφικής θεώρησης εγγράφων. Στο τέταρτο κεφάλαιο, παρουσιάζεται ο σχεδιασμός της διαδικασίας ένταξης υπηκόων τρίτων χωρών στην Ευρωπαϊκή Ένωση με τη χρήση των υπηρεσιών του EBSI. Παρουσιάζεται ένα σενάριο χρήσης, το οποίο περιλαμβάνει τη διαδικασία εισόδου και ένταξης ενός υπηκόου τρίτης χώρας στην κοινωνία της Ευρωπαϊκής Ένωσης, και στη συνέχεια περιγράφεται η υλοποίηση αυτής της διαδικασίας με τη χρήση της υποδομής EBSI. Στο τελευταίο κεφάλαιο, αναλύονται τα συμπεράσματα της παρούσας διπλωματικής και επισημαίνονται οι προκλήσεις σχετικά με την εποικοδομητική χρήση της τεχνολογίας Blockchain για τη διαχείριση των μεταναστευτικών και προσφυγικών ροών στην Ευρωπαϊκή Ένωση.

Λέξεις Κλειδιά: Blockchain, peer-to-peer network, Merkle trees, ψηφιακή υπογραφή, μηχανισμός συναίνεσης, μετανάστευση, πρόσφυγας, αιτών άσυλο, μετεγκατάσταση, European Union, EBSI, ESSIF, Notarisation, DID, eIDAS

Abstract

This thesis is aiming to investigate the use of Blockchain technology regarding the management of migration and refugee flows in European Union. First chapter provides an extensive study on Blockchain technology and how this kind of technology works. Following that, the key concepts and the structure of this technology are being analyzed as well as the process of creating and validating smart contracts. In addition, ways in which security is achieved in Blockchain networks are explained, including complex cryptographic methods, digital signature and consensus mechanisms. In order to demonstrate the use of these methods and the capabilities of blockchain technology, examples and use cases are provided and explained in detail. The second chapter, examines the data and the information related to movement of migrant and refugee populations to EU. Furthermore, follows the description of a study that was carried out, about the action plan of EU so as to manage this flow. Third chapter includes the strategic goals, benefits, key concepts, architecture and provided services of European Blockchain Services Infrastructure. All the currently available use cases of EBSI are being examined by focusing on European Self Sovereign Identity framework (ESSIF) and Notarisation Service. According to the Self-Sovereign Identity approach, users are able to create and control their own identity across borders, with no need to depend on any centralized authority while Notarisation service enables users to notarise their documents and create trusted digital audit trails. The fourth chapter presents the process of integration of third-country nationals in the EU, based on EBSI services, providing also a corresponding use case. This use case describes the entry process and the integration of a third-country national into EU and therefore, provides the proposed corresponding implementation based on EBSI. The last chapter presents the conclusions of this thesis and describes the challenges related to the use of Blockchain technology for the management of migration and refugee flows in the European Union.

Keywords: Blockchain, peer-to-peer network, Merkle trees, digital signature, consensus mechanism, migration, refugee, asylum seeker, relocation, European Union, EBSI, ESSIF, Notarisation, DID, eIDAS

Η σελίδα αυτή είναι σκόπιμα λευκή.

Ευχαριστίες

Με την παρούσα διπλωματική ολοκληρώνονται οι σπουδές μου στη Σχολή των Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π.. Πριν από την παρουσίασή της, θα ήθελα να ευχαριστήσω όλους όσους συνεργάστηκα και συνέβαλαν σημαντικά στην ολοκλήρωσή της. Αρχικά, ευχαριστώ θερμά τον επιβλέποντα της διπλωματικής μου εργασίας, Καθηγητή κύριο Δημήτριο Ασκούνη για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία καθώς και για τη συνεχή παροχή υποστήριξης. Επιπλέον, θα ήθελα να ευχαριστήσω θερμά τον Υπ. Διδάκτορα Χρήστο Κοντζίνο για την ουσιαστική καθοδήγηση που μου παρείχε και για την υποστήριξη σε κάθε στάδιο κατά την εκπόνηση της διπλωματικής εργασίας, όπως επίσης και την κυρία Ουρανία Μαρκάκη για την πολύτιμη βοήθειά της.

Περιεχόμενα

1 Εισαγωγή στην τεχνολογία Blockchain

1.1 Ορισμός και ιστορική αναδρομή

1.1.1 Ορισμός

Το Blockchain είναι ένα ανοιχτό κατανεμημένο ημερολόγιο στο οποίο καταγράφονται με αποτελεσματικό και έγκυρο τρόπο συναλλαγές μεταξύ των μερών που συμμετέχουν. Οι συναλλαγές αυτές οργανώνονται σε μία αλυσίδα από μπλοκ (blocks).[1] Η αλυσίδα αναπτύσσεται συνεχώς καθώς πραγματοποιούνται νέες συναλλαγές και προστίθενται νέα μπλοκ σε αυτή. Ουσιαστικά, το blockchain μπορεί να θεωρηθεί ως μία κατανεμημένη βάση δεδομένων στην οποία καταγράφονται συναλλαγές. Κάθε συναλλαγή επικυρώνεται με τη συναίνεση της πλειοψηφίας των συμμετεχόντων μερών και από τη στιγμή που καταγράφεται, έκτοτε δεν είναι δυνατό να διαγραφεί. Η χρήση τεχνολογιών όπως η κρυπτογραφία, η ψηφιακή υπογραφή και ο κατανεμημένος μηχανισμός συναίνεσης καθιστά το περιβάλλον στο οποίο λειτουργεί το Blockchain ένα αποκεντρωμένο περιβάλλον. Με αυτόν τον τρόπο, περιορίζεται σε μεγάλο βαθμό το κόστος και βελτιώνεται η αποδοτικότητα του συστήματος συναλλαγών.[1]

1.1.2 Ιστορική Αναδρομή

Μια δομή παρόμοια με αυτή του blockchain είχε περιγραφεί το 1991 σε ερευνητική εργασία (“How to Time-Stamp a Digital Document”), που παρουσίασε μια διαδικασία με την οποία ένα αρχείο στέλνεται σε έναν server και αυτός του προσδίδει το τρέχον χρονικό αποτύπωμα και, επίσης, το συνδέει με το προηγούμενό του έγγραφο. Το σύστημα που περιγράφηκε δεν επέτρεπε την παραβίαση των δεδομένων από τη στιγμή που πέρασαν και επισημάνθηκαν χρονικά από τον server. Σκοπός αυτής της ερευνητικής εργασίας ήταν η εύρεση μιας μεθόδου με την οποία τα ψηφιακά έγγραφα αποκτούν αυτόματα ψηφιακή σφραγίδα, έτσι ώστε κάθε αλλαγή, έστω και ενός μόνο στοιχείου του αρχείου, να είναι πάντα εμφανής και να γίνεται αντιληπτή. Επίσης, σύμφωνα με την ερευνητική εργασία θα έπρεπε να είναι αδύνατο ένα έγγραφο να αποκτήσει χρονικό αποτύπωμα με ημερομηνία και ώρα διαφορετικές από αυτές της δημιουργίας του.[1]

Αδιαμφισβήτητα, η πιο σημαντική ανακάλυψη που οδήγησε στο Blockchain ήταν το Bitcoin. Η ανακάλυψη του Blockchain οφείλεται στον Satoshi Nakamoto, ο οποίος το 2008 δημοσίευσε μια ερευνητική εργασία στην οποία παρουσίασε το Bitcoin ως ένα σύστημα ομότιμων συναλλαγών χρημάτων. Ο κύριος σκοπός αυτής της εργασίας ήταν να δημιουργήσει ένα ψηφιακό νόμισμα που θα έδινε τη δυνατότητα στους ανθρώπους να το ξοδέψουν απευθείας χωρίς να απαιτείται η συνδρομή κάποιου χρηματοπιστωτικού οργανισμού. Ήταν μια τεράστια ανακάλυψη που επέτρεψε στο χρήστη να πραγματοποιεί συναλλαγές χωρίς να βασίζεται σε τρίτους. Η ανακάλυψη του Blockchain κατέστησε το Bitcoin το πρώτο ψηφιακό νόμισμα που έλυσε το πρόβλημα των διπλών δαπανών (double-spending) χωρίς την ύπαρξη κάποιας κεντρικής αξιόπιστης αρχής [3]. Στο πεδίο των ψηφιακών νομισμάτων το πρόβλημα των διπλών δαπανών έγκειται στο γεγονός ότι τα ψηφιακά νομίσματα δεν είναι παρά ψηφιακά έγγραφα, τα οποία μπορούν να αντιγραφούν ή να πλαστογραφηθούν και επομένως το ίδιο ψηφιακό νόμισμα να ξοδεύεται παραπάνω από μία φορές [4][5]. Ο Satoshi αποσύρθηκε από το έργο αυτό στα τέλη του 2010 και δεν

[1] https://en.wikipedia.org/wiki/Blockchain

αποκαλύφθηκαν πολλά για την ταυτότητα του. Από τότε, η κοινότητα του Bitcoin μεγάλωσε εκθετικά με έναν μεγάλο αριθμό προγραμματιστών να ασχολούνται με το Bitcoin.[2]

1.1.3 Bitcoin

Το Bitcoin είναι ένα δίκτυο συναίνεσης που, στην πραγματικότητα, αποτελεί ένα νέο σύστημα πληρωμών. Παρέχει μια εντελώς ψηφιακή μορφή χρημάτων. Είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμής μεταξύ ομότιμων χρηστών (peer-to-peer) που λειτουργεί χωρίς την ύπαρξη κάποιας κεντρικής αρχής ή κάποιου μεσάζοντα. Η σημασία του δικτύου ομότιμων κόμβων εξηγείται στο *κεφάλαιο 1.2.1*.

Από την πλευρά του χρήστη, το Bitcoin είναι σαν τα μετρητά χρήματα του Διαδικτύου. Κάποιες από τις βασικές αρχές του δικτύου Bitcoin είναι οι εξής[2]:

- Δεν υπάρχει ιδιοκτήτης του δικτύου Bitcoin. Ο έλεγχος του Bitcoin ανήκει στους χρήστες Bitcoin σε όλο τον κόσμο.
- Ενώ βελτιώνεται το λογισμικό, δεν μπορεί να πραγματοποιηθεί καμία αλλαγή στο πρωτόκολλο του Bitcoin. Οι χρήστες είναι ελεύθεροι να επιλέξουν την έκδοση του λογισμικού που χρησιμοποιούν. Όλοι οι χρήστες θα πρέπει να χρησιμοποιούν το λογισμικό που υπακούει στους ίδιους κανόνες, προκειμένου να διατηρείται η συμβατότητα.
- Το Bitcoin λειτουργεί σωστά μόνο όταν υπάρχει πλήρης συναίνεση μεταξύ όλων των χρηστών.
- Από την πλευρά των χρηστών, το Bitcoin είναι μια εφαρμογή κινητού τηλεφώνου ή υπολογιστή, που παρέχει ένα προσωπικό πορτοφόλι και τους δίνει τη δυνατότητα να στέλνουν και να λαμβάνουν bitcoins μέσω αυτού.

Στο παρασκήνιο, οι χρήστες του δικτύου Bitcoin μοιράζονται ένα δημόσιο ημερολόγιο, blockchain. Το blockchain περιλαμβάνει κάθε μία συναλλαγή που έχει ποτέ επεξεργαστεί από το δίκτυο. Με αυτόν τον τρόπο, ο χρήστης έχει τη δυνατότητα να εξακριβώνει την εγκυρότητα κάθε συναλλαγής. Για την προστασία της αυθεντικότητας των συναλλαγών χρησιμοποιούνται οι ψηφιακές υπογραφές *(κεφάλαιο 1.4.3)* που αντιστοιχούν στις διευθύνσεις αποστολής. Έτσι οι χρήστες του δικτύου Bitcoin μπορούν να έχουν τον πλήρη έλεγχο κατά την αποστολή bitcoins από τις δικές τους διευθύνσεις Bitcoin. Τέλος, δίνεται η δυνατότητα στον καθένα να επεξεργαστεί συναλλαγές με τη χρήση της υπολογιστικής ισχύος υλικού (hardware) και να κερδίσει μια ανταμοιβή σε bitcoins για την υπηρεσία αυτή. Η διαδικασία αυτή ονομάζεται εξόρυξη (mining). Περισσότερα για τη διαδικασία της εξόρυξης και το μηχανισμό συναίνεσης (Proof-of-Work), που χρησιμοποιούνται στο Bitcoin αναλύονται στο *κεφάλαιο 1.4.4.1*.[1]

1.1.4 Ethereum

Εκτός από το Bitcoin, μια ακόμη δημοφιλής πλατφόρμα που στηρίζεται στο blockchain είναι το Ethereum. Δημιουργήθηκε το 2015 και αποτελεί το blockchain που δίνει τη δυνατότητα προγραμματισμού στους χρήστες του. Πρόκειται για μία πλατφόρμα ανοιχτού κώδικα που έχει το δικό της κρυπτονόμισμα, το ether.[2] Στο Ethereum αντί για εξόρυξη bitcoin, οι κόμβοι εργάζονται για εξόρυξη ether. Πέρα από κρυπτονόμισμα για εμπορική χρήση, το ether χρησιμοποιείται από τους προγραμματιστές εφαρμογών για την πληρωμή των χρεώσεων και

[1] https://bitcoin.org/el/faq#what-is-bitcoin
[2] https://en.wikipedia.org/wiki/Ethereum

των υπηρεσιών στο δίκτυο Ethereum.[1] Ουσιαστικά, αποτελεί ένα ανοιχτού κώδικα λειτουργικό σύστημα που προσφέρει τη δυνατότητα εκτέλεσης έξυπνων συμβάσεων (smart contracts).[2] Μια έξυπνη σύμβαση στο blockchain είναι ένα αυτοματοποιημένο πρόγραμμα που εκτελείται αυτόματα και μπορεί να διευκολύνει την ανταλλαγή χρημάτων, μετοχών ή κάποιας άλλης αξίας.[7] Η βασική καινοτομία του Ethereum είναι η εικονική μηχανή Ethereum Virtual Machine (EVM). Πρόκειται για ένα Turing Complete λογισμικό που τρέχει στο δίκτυο του Ethereum και επιτρέπει σε οποιονδήποτε να εκτελεί οποιοδήποτε πρόγραμμα, ανεξάρτητα από τη γλώσσα προγραμματισμού του, παρέχοντας αρκετό χρόνο και μνήμη. Αυτή η εικονική μηχανή διευκολύνει τη διαδικασία δημιουργίας εφαρμογών blockchain. Το Ethereum επιτρέπει δυνητικά την ανάπτυξη χιλιάδων διαφορετικών εφαρμογών σε μία πλατφόρμα, χωρίς να χρειάζεται να αναπτύσσεται ένα εξ ολοκλήρου νέο blockchain για κάθε εφαρμογή. Χιλιάδες προγραμματιστές σε όλον τον κόσμο αναπτύσσουν εφαρμογές στο Ethereum. Τέτοιες εφαρμογές είναι τα ψηφιακά πορτοφόλια κρυπτονομισμάτων που επιτρέπουν τις φθηνές και άμεσες πληρωμές, οι χρηματοοικονομικές εφαρμογές που επιτρέπουν στους χρήστες να δανείσουν και να δανειστούν ή να επενδύουν τα ψηφιακά τους στοιχεία, αποκεντρωμένες αγορές που επιτρέπουν την ανταλλαγή ψηφιακών περιουσιακών στοιχείων καθώς και παιχνίδια στα οποία διατίθενται τα περιουσιακά στοιχεία και υπάρχει και η δυνατότητα αποκόμισης κέρδους πραγματικών χρημάτων. Δεν υπάρχει κεντρικός οργανισμός που να ελέγχει το Ethereum.[3] Το Ethereum διαφέρει από το Bitcoin ως προς το σκοπό, καθώς εκτός από την πραγματοποίηση συναλλαγών μέσω του ether, επιτρέπει σε προγραμματιστές να αναπτύσσουν νέα είδη αποκεντρωμένων εφαρμογών, οι οποίες επωφελούνται από την τεχνολογία του blockchain και των κρυπτονομισμάτων.[4]

1.1.5 Χαρακτηριστικά του Blockchain

Στη συνέχεια αναλύονται τα βασικά χαρακτηριστικά της τεχνολογίας Blockchain:

- **Αποκέντρωση**

Όλες οι συναλλαγές που πραγματοποιούνται στο σύγχρονο ψηφιακό κόσμο εξαρτώνται από την εμπιστοσύνη μας σε κάποια συγκεκριμένη κεντρική αξιόπιστη αρχή. Μπορεί να πρόκειται, για παράδειγμα, είτε για κάποια τράπεζα που μας εγγυάται την αξιόπιστη μεταφορά των χρημάτων μας σε κάποιον άλλο λογαριασμό είτε για κάποια υπηρεσία που επικυρώνει την αξιοπιστία εγγράφων. Κάθε σύστημα συναλλαγών βασίζεται σε κάποια εξωτερική οντότητα τρίτων, η οποία αν παραβιαστεί τότε τα δεδομένα των συναλλαγών δεν είναι πλέον ασφαλή[1]. Η θεμελιώδης ιδέα του blockchain είναι ότι δεν υπάρχει κάποια κεντρική αρχή που ελέγχει το σύστημα. Η αποκέντρωση αποτελεί ένα από τα σημαντικότερα προτερήματα της τεχνολογίας blockchain. Εξαιτίας του σχεδιασμού του, το blockchain αποτελεί μία πλατφόρμα που λειτουργεί κάθε φορά με διαφορετικούς ηγέτες. Αυτοί επιλέγονται μέσω των μηχανισμών συναίνεσης του blockchain. Οποιοσδήποτε από τους συμμετέχοντες μπορεί να ανταγωνιστεί τους υπόλοιπους προκειμένου να γίνει αυτός το κέντρο λήψης αποφάσεων. Για παράδειγμα, μια δημοφιλής μέθοδος συναίνεσης που χρησιμοποιείται γι' αυτό το σκοπό, και θα αναλυθεί στη συνέχεια (κεφάλαιο 1.4.4.1), είναι η γνωστή ως «απόδειξη εργασίας» (Proof-of-Work)[6].

[1] https://blockgeeks.com/guides/ethereum/
[2] https://en.wikipedia.org/wiki/Ethereum
[3] https://ethereum.org/what-is-ethereum/

- **Διαφάνεια**

Στο Blockchain η ταυτότητα κάθε συμμετέχοντα αποκρύπτεται με τη χρήση μεθόδων σύνθετης κρυπτογραφίας. Έτσι, ενώ η πραγματική ταυτότητα του είναι ασφαλής, οι υπόλοιποι συμμετέχοντες γνωρίζουν όλες τις συναλλαγές που έχει πραγματοποιήσει μέσω της δημοσίας διεύθυνσής του. Από τη στιγμή που πρόκειται για ένα κοινό και αμετάβλητο ημερολόγιο, οι πληροφορίες είναι ανοικτές και μπορεί οποιοσδήποτε να τις δει. Ως εκ τούτου, οτιδήποτε υπάρχει στο blockchain είναι από τη φύση του διαφανές και όλοι οι συμμετέχοντες είναι υπόλογοι για τις ενέργειες τους. [1]

- **Σταθερότητα**

Το Blockchain χαρακτηρίζεται από σταθερότητα, διότι από τη στιγμή που καταγράφεται σε αυτό μια συναλλαγή, δεν μπορεί έπειτα να τροποποιηθεί. Αυτό επιτυγχάνεται με τη χρήση των κρυπτογραφικών συναρτήσεων κατακερματισμού.[1] Επιπλέον, κάθε μπλοκ που περιέχει συναλλαγές μεταδίδεται σε όλο το δίκτυο και επικυρώνεται από πολλούς χρήστες, με αποτέλεσμα οποιαδήποτε παραποίηση να μπορεί να εντοπιστεί εύκολα [7].

- **Ελεγξιμότητα**

Δεδομένου ότι κάθε μία από τις συναλλαγές στο blockchain επικυρώνεται και αποκτά χρονική επισήμανση, οι χρήστες μπορούν εύκολα να επαληθεύσουν και να εντοπίσουν τις προηγούμενες καταγραφές συναλλαγών μέσω της πρόσβασης σε οποιονδήποτε κόμβο του κατανεμημένου δικτύου. Στο blockchain του Bitcoin, κάθε συναλλαγή μπορεί να εντοπιστεί με την επαναληπτική ιχνηλάτηση των προηγούμενων συναλλαγών. Έτσι βελτιώνεται η ελεγξιμότητα και η διαφάνεια των δεδομένων που είναι αποθηκευμένα στο blockchain. [7]

1.1.6 Δυνητικό πεδίο εφαρμογής

Ορισμένοι από τους τομείς εφαρμογής της τεχνολογίας Blockchain παρουσιάζονται παρακάτω:

- **Έξυπνα Συμβόλαια (Smart Contracts)**

Ένα κατανεμημένο ημερολόγιο, όπως το blockchain, δίνει τη δυνατότητα κωδικοποίησης απλών συμβάσεων. Οι έξυπνες συμβάσεις είναι, στην πραγματικότητα, προγράμματα τα οποία εκτελούνται τη χρονική στιγμή στην οποία πληρούνται όλες οι προϋποθέσεις τους.[1] Όταν μια προκαθορισμένη συνθήκη σε ένα έξυπνο συμβόλαιο πληρείται τότε μπορούν να πραγματοποιηθούν αυτόματα πληρωμές, μεταξύ των συμμετεχόντων, που υποδεικνύονται από τη συνθήκη αυτή του συμβολαίου, με πλήρη διαφάνεια [1]. Όπως αναφέρθηκε και παραπάνω, το Ethereum, ένα blockchain ανοιχτού κώδικα, δημιουργήθηκε με σκοπό να υλοποιήσει ακριβώς αυτή τη δυνατότητα. Η σημερινή τεχνολογία επιτρέπει μέχρι στιγμής τον προγραμματισμό έξυπνων συμβάσεων που πραγματοποιούν απλές λειτουργίες.[1]

- **Οικονομία Διαμοιρασμού (Sharing Economy)**

Η οικονομία διαμοιρασμού αναπτύσσεται με γρήγορους ρυθμούς, γεγονός που αποδεικνύεται από την επιτυχία των εταιριών όπως η Uber και η Airbnb. Παρόλα αυτά, μέχρι στιγμής όταν κάποιος επιθυμεί να χρησιμοποιήσει για παράδειγμα μια υπηρεσία

[1] https://blockgeeks.com/guides/what-is-blockchain-technology/

διαμοιρασμού οχημάτων πρέπει να βασιστεί σε κάποιον τρίτο διαμεσολαβητή, όπως στην προκειμένη περίπτωση στην εφαρμογή Uber. Το blockchain ενεργοποιεί τις συναλλαγές μεταξύ ομότιμων χρηστών και έτσι ανοίγει την πόρτα για μια πραγματικά αποκεντρωμένη οικονομία διαμοιρασμού.[1]

- **Χρηματοδότηση από το πλήθος (Crowdfunding)**

Η δημοτικότητα των εφαρμογών όπως το Kickstarter και το GoFundMe υποδεικνύει την ανάγκη για άμεση ανταπόκριση σε καινοτόμες ιδέες που διατίθενται για χρηματοδότηση. Το blockchain μπορεί να βοηθήσει σε αυτή την κατεύθυνση ακόμη περισσότερο συγκεντρώνοντας χρηματοδοτικά κεφάλαια από το πλήθος.[1]

- **Κυβέρνηση**

Η τεχνολογία του blockchain, μια τεχνολογία κατανεμημένης βάσης δεδομένων, μπορεί να επιτύχει την πλήρη διαφάνεια και προσβασιμότητα στο πεδίο των αποτελεσμάτων μιας ψηφοφορίας και επομένως να εξασφαλίσει πλήρη διαφάνεια στις εκλογές ή σε οποιοδήποτε άλλο είδος δημοσκόπησης. Οι έξυπνες συμβάσεις συμβάλλουν στην αυτοματοποίηση της διαδικασίας. Η εφαρμογή Boardroom (Αίθουσα Συσκέψεων) επιτρέπει τη λήψη αποφάσεων σε οργανωμένο επίπεδο στο Blockchain. Στην πράξη, αυτό σημαίνει ότι η εταιρική διακυβέρνηση γίνεται πλήρως διαφανής και επαληθεύσιμη όταν διαχειρίζεται ψηφιακά στοιχεία ενεργητικού, μετοχές ή πληροφορίες.[1]

- **Έλεγχος Εφοδιαστικής Αλυσίδας**

Οι καταναλωτές ενδιαφέρονται σε σημαντικό βαθμό για την προέλευση των προϊόντων που αγοράζουν. Ένα κατανεμημένο ημερολόγιο παρέχει έναν εύκολο τρόπο ώστε να ελέγχονται τα ιστορικά στοιχεία των καταναλωτικών αγαθών και επομένως η γνησιότητά τους. Η διαφάνεια εξασφαλίζεται με τη χρονική σήμανση βάσει ημερομηνίας και τοποθεσίας που αντιστοιχούν σε κάποιον αριθμό προϊόντος.[1] Για παράδειγμα, η ψηφιακή πλατφόρμα Provenance δίνει τη δυνατότητα σε εταιρίες να κάνουν σημαντικά βήματα για την εξασφάλιση της διαφάνειας σε σχέση με την προέλευση και την πορεία των προϊόντων τους στην εφοδιαστική αλυσίδα. Το λογισμικό αυτό τους βοηθά να συγκεντρώνουν και να παρουσιάζουν ιστορικά δεδομένα σχετικά με τα προϊόντα τους.[2]

- **Αποθήκευση Αρχείων**

Η αποκεντρωμένη αποθήκευση αρχείων συμβάλει στη διατήρηση της ασφάλειας των δεδομένων και τα προστατεύει από ενδεχόμενη παραβίασή τους.[1]

- **Αγορές Προβλέψεων**

Οι εταιρίες προβλέψεων εμπορεύονται τις προβλέψεις τους σχετικά με την έκβαση ορισμένων γεγονότων. Το πλήθος των δειγμάτων στα οποία στηρίζεται το αποτέλεσμα της πρόβλεψης παίζει πολύ σημαντικό ρόλο. Επίσης, πολύ σημαντικό είναι να λαμβάνονται υπόψη και οι μεροληπτικές αντιλήψεις ή οι προκαταλήψεις ακόμα κι αν είναι μέρος της μειοψηφίας και να μη στρογγυλοποιείται το αποτέλεσμα με βάση το μέσο όρο, με αποτέλεσμα να διαστρεβλώνεται. Το Blockchain που είναι μια τεχνολογία με τη δυνατότητα,

[1] https://blockgeeks.com/guides/what-is-blockchain-technology/
[2] https://www.provenance.org/about

λόγω του χαρακτηριστικού της αποκέντρωσης, να συγκεντρώνει πληροφορίες από το πλήθος, μπορεί να βρει εφαρμογή σε αυτόν τον τομέα.[1]

- **Πνευματική Ιδιοκτησία**

Τα ψηφιακά δεδομένα διανέμονται ευρέως στο διαδίκτυο. Το γεγονός αυτό έχει οδηγήσει τους κατόχους δικαιωμάτων πνευματικής ιδιοκτησίας να χάνουν τον έλεγχο αυτής της ιδιοκτησίας τους. Οι έξυπνες συμβάσεις (smart contracts) μπορούν να συμβάλουν στην προστασία των πνευματικών δικαιωμάτων και να αυτοματοποιήσουν την πώληση έργων στο διαδίκτυο, εξαλείφοντας τον κίνδυνο αντιγραφής ή αναδιανομής τους.[1]

- **Διαδίκτυο των Πραγμάτων (Internet of Things)**

Οι έξυπνες συμβάσεις (smart contracts) καθιστούν δυνατή την αυτοματοποίηση των συστημάτων IoT, δηλαδή των συστημάτων απομακρυσμένης διαχείρισης ηλεκτρονικών συσκευών. Συμβάλουν στην αύξηση της απόδοσης του συστήματος και βελτιώνουν το κόστος παρακολούθησης των συσκευών.[1]

- **Μικροσυστήματα**

Σε συνδυασμό με την ανάπτυξη της τεχνολογίας του IoT, τα έξυπνα συμβόλαια (smart contracts) μπορούν να βελτιώσουν τη λειτουργία κάποιων μικροσυστημάτων. Για παράδειγμα, όταν τα ηλιακά πάνελ μιας γειτονιάς παράγουν υπερβολική ενέργεια, τα smart contracts (που βασίζονται στο Ethereum) έχουν τη δυνατότητα να την αναδιανέμουν αυτόματα.[1]

- **Διαχείριση Ταυτότητας**

Η δυνατότητα επαλήθευσης της προσωπικής ταυτότητας είναι πολύ σημαντική για τις οικονομικές συναλλαγές που συμβαίνουν στο διαδίκτυο. Η καταχώρηση μιας ασφαλούς ταυτότητας είναι, επίσης, πολύ χρήσιμη σε διαδικτυακές αλληλεπιδράσεις όπως σε εφαρμογές οικονομίας διαμοιρασμού (sharing economy). Το blockchain προσφέρει βελτιωμένες μεθόδους ανάπτυξης προτύπων ψηφιακής ταυτότητας και ψηφιοποίησης προσωπικών εγγράφων.[1]

- **Καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML) και Έλεγχος των δραστηριοτήτων των πελατών (KYC)**

Επί του παρόντος, τα χρηματοπιστωτικά ιδρύματα προκειμένου να καταπολεμήσουν τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες (AML) μέσω του ελέγχου των δραστηριοτήτων των πελατών τους (KYC) ακολουθούν μια σύνθετη διαδικασία που απαιτεί αρκετό χρόνο για κάθε πελάτη. Με τη χρήση του blockchain τα κόστη του KYC θα μπορούσαν να μειωθούν μέσω σταυροειδούς επαλήθευσης των πληροφοριών από διαφορετικές υπηρεσίες και να βελτιωθεί η αποτελεσματικότητα της παρακολούθησης.[2]

- **Διαχείριση Προσωπικών Δεδομένων**

Στις μέρες μας, οι χρήστες του διαδικτύου χρησιμοποιούν πλατφόρμες μέσων κοινωνικής δικτύωσης, σε αντάλλαγμα των προσωπικών τους δεδομένων. Μελλοντικά, θα έχουν τη

[1] https://blockgeeks.com/guides/what-is-blockchain-technology/

[2] https://blockgeeks.com/guides/what-is-blockchain-technology/

δυνατότητα να διαχειρίζονται και να πωλούν τα δεδομένα που παράγει η ηλεκτρονική τους δραστηριότητα. Πιθανότατα το Bitcoin να είναι το νόμισμα που χρησιμοποιείται γι' αυτές τις συναλλαγές.[1]

- **Καταγραφή Τίτλων Ιδιοκτησίας**

Το Blockchain, επειδή είναι ένα δημόσιο ημερολόγιο, μπορεί να συμβάλει στην αρχειοθέτηση κάθε είδους με αποτελεσματικό τρόπο. Για παράδειγμα, θα μπορούσε να αποδειχτεί πολύ χρήσιμο στη διαχείριση τίτλων ιδιοκτησίας, που είναι αρκετά ευάλωτοι σε απάτη και επίσης απαιτούν αρκετό χρόνο και εργασία για την αρχειοθέτηση τους.[1]

- **Συναλλαγές Μετοχών**

Μια ακόμη περίπτωση χρήσης του Blockchain είναι οι συναλλαγές μετοχών. Σε ένα δίκτυο ομότιμων χρηστών, όπως είναι το Blockchain, οι συναλλαγές των μετοχών είναι δυνατό να πραγματοποιούνται στιγμιαία. Επομένως, οι ενδιάμεσες διαδικασίες όπως η εκκαθάριση που μπορεί να διαρκέσει έως τρεις μέρες, καθώς και οι διαμεσολαβητές όπως οι ελεγκτές και οι θεματοφύλακες απομακρύνονται από τη διαδικασία.[1]

1.2 Τρόπος λειτουργίας Blockchain

Το blockchain είναι μια σειρά αμετάβλητων αρχείων δεδομένων με χρονική σφραγίδα (blocks), τα οποία συνδέονται μεταξύ τους με τη χρήση κρυπτογραφικών συναρτήσεων. Αυτά τα block τα διαχειρίζεται ένα σύμπλεγμα (δίκτυο) υπολογιστών που δεν ανήκουν σε κάποια κεντρική οντότητα. Το δίκτυο αυτό των υπολογιστών είναι στην πραγματικότητα ένα δίκτυο peer-to-peer (P2P), που αποτελείται από ένα σύνολο υπολογιστών (nodes).[1]

1.2.1 Δίκτυο Peer-to-Peer

Το δίκτυο peer-to-peer αποτελεί μια κατανεμημένη αρχιτεκτονική που διαμοιράζει το φόρτο εργασίας μεταξύ των κόμβων – υπολογιστών, οι οποίοι μοιράζονται τους πόρους τους ισοδύναμα. Οι κόμβοι έχουν ίσα δικαιώματα. Επομένως, πρόκειται για ένα δίκτυο ομότιμων κόμβων. Οι κόμβοι κάνουν μέρος των πόρων τους, όπως η επεξεργαστική ισχύς, ο αποθηκευτικός χώρος και το εύρος ζώνης του δικτύου (bandwidth), άμεσα διαθέσιμο σε άλλους κόμβους χωρίς την ύπαρξη κεντρικού συντονισμού. Οι ομότιμοι κόμβοι είναι ταυτόχρονα και προμηθευτές και καταναλωτές πόρων, σε αντίθεση με το παραδοσιακό μοντέλο πελάτη-εξυπηρετητή (client-server), στο οποίο η κατανάλωση και ο εφοδιασμός διαιρείται σε πελάτες (clients) και εξυπηρετητές (servers) αντίστοιχα.[1] Το πλεονέκτημα αυτών των συστημάτων είναι το γεγονός ότι επιτρέπουν στους χρήστες να αλληλοεπιδρούν απευθείας μεταξύ τους αντί να αλληλοεπιδρούν με έμμεσο τρόπο μέσω κάποιου μεσάζοντα. Με την αντικατάσταση αυτού του μεσάζοντα από το σύστημα peer-to-peer, μειώνεται το κόστος και αυξάνεται η ταχύτητα επεξεργασίας του συστήματος. Το σημαντικό πλεονέκτημα του Blockchain είναι ότι χρησιμεύει ως εργαλείο για την επίτευξη και διατήρηση της ακεραιότητας σε κατανεμημένα δίκτυα peer-to-peer, τα οποία δύνανται να φέρουν μεγάλη αλλαγή στο τομέα των βιομηχανιών, λόγω αυτής της αποδέσμευσης από την ύπαρξη διαμεσολαβητή.[8]

[1] https://en.wikipedia.org/wiki/Peer-to-peer

1.2.2 Διαδικασία Δημιουργίας και Επικύρωσης μιας Συναλλαγής

Οι κόμβοι είναι είτε κόμβοι που συμμετέχουν στη λήψη αποφάσεων και στη δημιουργία νέων μπλοκ είτε κόμβοι υπογράφοντες (signers) που επικυρώνουν και υπογράφουν ψηφιακά τις συναλλαγές. Μια κρίσιμη απόφαση που πρέπει να ληφθεί από κάθε blockchain είναι σε ποιον κόμβο θα προσαρτήσει το επόμενο μπλοκ. Αυτό αποφασίζεται με τη χρήση του μηχανισμού συναίνεσης, ο οποίος θα αναλυθεί στη συνέχεια *(κεφάλαιο 1.4.4)*. [6]

Τώρα θα εξηγηθεί πως το blockchain επικυρώνει τις συναλλαγές και δημιουργεί και προσθέτει μπλοκ για να αναπτυχθεί η αλυσίδα και θα δοθεί μια γενική ιδέα για το ποια είναι η σχέση μεταξύ συναλλαγών και μπλοκ. Σε γενικές γραμμές ακολουθούνται τα παρακάτω βήματα:

1. Ένας κόμβος, που αποτελεί τον ένα συμμετέχοντα στη συναλλαγή, ξεκινά μια συναλλαγή (πρώτα δημιουργώντας τη και στη συνέχεια υπογράφοντας τη ψηφιακά με το προσωπικό του ιδιωτικό κλειδί - private key). Μια συναλλαγή μπορεί να αντιπροσωπεύει διάφορες ενέργειες μέσα σε ένα blockchain. Πιο συχνά, μια συναλλαγή είναι μια δομή δεδομένων που αντιπροσωπεύει τη μεταφορά αξίας μεταξύ των χρηστών στο blockchain. Αυτή η δομή δεδομένων συνήθως αποτελείται από σχετικούς κανόνες της μεταφοράς αξίας, καθώς και άλλων πληροφοριών επικύρωσης.[6]
2. Η συναλλαγή που ζητήθηκε αναμεταδίδεται στο δίκτυο peer-to-peer.[1] Το δίκτυο κόμβων επικυρώνει τη συναλλαγή αυτή, με βάση παρόντα κριτήρια. Η συναλλαγή επαληθεύεται τις περισσότερες φορές από χιλιάδες ή εκατομμύρια υπολογιστές στο δίκτυο. Μια επικυρωμένη συναλλαγή μπορεί να περιλαμβάνει κρυπτονομίσματα (όπως στο Bitcoin), συμβόλαια, αρχεία ή άλλες πληροφορίες.[6]
3. Από τη στιγμή που η συναλλαγή έχει επικυρωθεί, συνδυάζεται με άλλες συναλλαγές και επομένως ενσωματώνεται σε ένα μπλοκ δεδομένων του ημερολογίου (blockchain). Σε αυτό το σημείο η συναλλαγή θεωρείται ότι έχει επιβεβαιωθεί.[1]
4. Το μπλοκ προστίθεται στο ήδη υπάρχον blockchain με τέτοιο τρόπο που να είναι μόνιμο και μη τροποποιήσιμο.[1] Το επόμενο μπλοκ που θα γίνει μέρος του blockchain συνδέεται κρυπτογραφικά με αυτό το μπλοκ. [6]
5. Η συναλλαγή έχει ολοκληρωθεί.

Το blockchain προσφέρει έναν απλό, πλήρως αυτοματοποιημένο και ασφαλή τρόπο για να μεταφέρονται πληροφορίες από τον ένα συμμετέχοντα στον άλλον. Η παραποίηση μιας συναλλαγής θα σήμαινε την παραποίηση ολόκληρης της αλυσίδας σε εκατομμύρια σημεία. Επομένως, είναι πρακτικά αδύνατη και οι συναλλαγές είναι πλήρως ασφαλείς.[6]

1.2.3 Έξυπνες Συμβάσεις (Smart Contracts)

Μια έξυπνη σύμβαση είναι ένα πρόγραμμα υπολογιστή που ελέγχει με άμεσο και αυτόματο τρόπο τη μεταφορά ψηφιακών στοιχείων μεταξύ των εμπλεκόμενων μερών υπό συγκεκριμένες προϋποθέσεις. Λειτουργεί με τον ίδιο τρόπο που λειτουργεί και μια παραδοσιακή σύμβαση και ταυτόχρονα διεκπεραιώνει τη σύμβαση με αυτόματο τρόπο. Οι έξυπνες συμβάσεις είναι προγράμματα που εκτελούνται ακριβώς όπως έχουν προγραμματιστεί από τους δημιουργούς τους.

Το 1994, ο Nick Szabo, υπότροφος Νομικής Σχολής, αναγνώρισε την ευκαιρία εφαρμογής των έξυπνων συμβάσεων στο αποκεντρωμένο ημερολόγιο. Σκέφτηκε ότι αυτές οι συμβάσεις θα

[1] https://blockgeeks.com/guides/what-is-blockchain-technology/

μπορούσαν να είναι γραμμένες σε κώδικα που μπορεί να αποθηκευτεί και να εκτελεστεί στο σύστημα καθώς και να εποπτεύεται από το δίκτυο υπολογιστών που συνιστούν το blockchain.

Μια έξυπνη σύμβαση έχει λεπτομέρειες, σχετικά με άδειες και δικαιώματα, γραμμένες σε κώδικα, οι οποίες απαιτούν την πραγματοποίηση μιας ακριβούς ακολουθίας γεγονότων έτσι ώστε να δοθεί το έναυσμα για να πραγματοποιηθεί η συμφωνία των όρων που αναφέρονται στην έξυπνη σύμβαση. Επίσης, μπορεί να περιλαμβάνει τους χρονικούς περιορισμούς της σύμβασης, οι οποίοι εισάγουν προθεσμίες στο έξυπνο συμβόλαιο.

Πρώτη φορά έξυπνα συμβόλαια χρησιμοποιήθηκαν στο Bitcoin για να πραγματοποιηθεί μεταφορά αξίας από το ένα άτομο στο άλλο. Στο Bitcoin, η εμπλεκόμενη σύμβαση βασίζεται σε βασικούς όρους όπως ο έλεγχος εάν το ποσό της αξίας για τη μεταφορά είναι πράγματι διαθέσιμο στο λογαριασμό του αποστολέα. Αργότερα, αναπτύχθηκε η πλατφόρμα Ethereum, η οποία θεωρήθηκε πιο ισχυρή, επειδή οι προγραμματιστές μπορούσαν να δημιουργούν προσαρμοσμένες συμβάσεις σε μια Turing-complete γλώσσα. Οι έξυπνες συμβάσεις που δημιουργήθηκαν στην περίπτωση του δικτύου Bitcoin γράφτηκαν σε μια Turing-incomplete γλώσσα, περιορίζοντας έτσι τις δυνατότητες εφαρμογής των έξυπνων συμβάσεων στο Bitcoin. Η ιδέα των έξυπνων συμβάσεων είναι ότι με τη δημιουργία συμβάσεων μεταξύ των εμπλεκόμενων μερών σε μορφή κώδικα υπολογιστή και την αποθήκευση τους στο blockchain, οι συμβάσεις αυτές μπορούν να είναι αμετάβλητες, δηλαδή να μη μπορεί κανείς να τις παραβιάσει, και να εκτελούνται από μόνες τους και με αυτόματο τρόπο μόλις τηρούνται οι απαιτούμενες προϋποθέσεις. Μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση, η διαδικασία μπορεί να γίνει λιγότερο επικίνδυνη και πιο αποδοτική [9]. Το γεγονός ότι η σύμβαση είναι ενσωματωμένη στο blockchain την καθιστά διαφανή, αμετάβλητη, φθηνή και αποκεντρωμένη.[1] Σφάλματα σε έξυπνες συμβάσεις μπορούν να προκαλέσουν καταστροφικές ζημίες. Επομένως, έχει μεγάλη σημασία η ανάλυση επιθέσεων σε έξυπνα συμβόλαια. Με την τεχνολογία του blockchain να αναπτύσσεται τόσο γρήγορα, όλο και περισσότερες εφαρμογές που βασίζονται στα έξυπνα συμβόλαια μπορούν να αναπτύσσονται.[7]

Προκειμένου να μετατραπεί ένα συμβατικό συμβόλαιο σε μια έξυπνη σύμβαση θα πρέπει η συμφωνία να είναι δυνατόν να αναπαρασταθεί ως ένα λογικό διάγραμμα ροής που περιλαμβάνει εξαρτήσεις του τύπου : “if X, then Y, else Z”. Είναι πολλές οι περιπτώσεις στις οποίες οι συμβάσεις και οι συμφωνίες περιέχουν ασάφειες ως προς το εάν κάποια από τις συνθήκες τους έχει στην πραγματικότητα ικανοποιηθεί. Παρόλο που έχουν προταθεί διάφορες λύσεις ώστε να επιλυθεί αυτό το πρόβλημα (όπως η χρήση κατανεμημένων αγορών πρόβλεψης- prediction markets ή κλειδιά κρυπτογράφησης πολλαπλών σημείων υπογραφής), το πραγματικά ενδιαφέρον ερώτημα είναι αν θα δημιουργηθούν νέες τεχνικές ανάπτυξης αυτοματοποιημένων συμβάσεων, οι οποίες, τουλάχιστον σε ορισμένες περιπτώσεις, θα έχουν τη δυνατότητα να διαχειρίζονται αυτές τις ασάφειες. [9]

Οι τυπικές συναλλαγές στο blockchain αποτελούν ένα μέσο για τη μεταφορά ιδιοκτησίας από τον ένα εμπλεκόμενο στον άλλο και επίσης χρησιμεύουν ως τρόπος περιγραφής και επαλήθευσης της ιδιοκτησίας. Οι συναλλαγές είναι στην πραγματικότητα μικρές αυτοτελείς συμβάσεις. Περιέχουν όλες τις απαραίτητες πληροφορίες για να πραγματοποιηθεί μια μεταβίβαση ιδιοκτησίας. Η ιδέα αυτή οδήγησε στην ανάπτυξη των έξυπνων συμβολαίων στο blockchain. Όπως και τα δεδομένα συναλλαγών, έτσι και τα έξυπνα συμβόλαια είναι

[1] https://blockgeeks.com/guides/what-is-blockchain-technology/

μηχανικά αναγνώσιμες περιγραφές της συμφωνίας μεταξύ των εμπλεκομένων μερών. Βέβαια, σε αντίθεση με τα απλά δεδομένα συναλλαγών, τα έξυπνα συμβόλαια είναι πολύ πιο ευέλικτα όσον αφορά στις συνθήκες που μπορούν να χρησιμοποιηθούν. Από τεχνική άποψη, τα έξυπνα συμβόλαια είναι αυτοδύναμα προγράμματα ηλεκτρονικών υπολογιστών γραμμένα σε μια ειδική γλώσσα προγραμματισμού στο blockchain. Προκειμένου να συμπεριλάβει και τα έξυπνα συμβόλαια, η τεχνολογία του blockchain έχει επεκταθεί ενσωματώνοντας επιπλέον την ικανότητα εκτέλεσης κώδικα. Αυτή η επέκταση έχει μεταμορφώσει το blockchain από ένα κατανεμημένο σύστημα που εστιάζει κυρίως στην αποθήκευση δεδομένων συναλλαγής σε ένα κατανεμημένο σύστημα εικονικών μηχανών που εκτελεί έξυπνες συμβάσεις. Η δυνατότητα εκτέλεσης κώδικα προγράμματος έχει επεκτείνει τις δυνατότητες ανάπτυξης εφαρμογών στο blockchain. Ο όρος «έξυπνες συμβάσεις» αρχικά αναφερόταν σε κάποια συμφωνία μεταξύ των εμπλεκόμενων μερών. Πλέον, χρησιμοποιείται για να αναφερθεί σε κάποιο κομμάτι κώδικα που και εκτελείται στο blockchain.[8]

Λόγω της ευελιξίας τους, οι έξυπνες συμβάσεις μπορούν να χρησιμοποιηθούν για να περιγράψουν ένα ευρύ φάσμα συμβάσεων του πραγματικού κόσμου, όπως για παράδειγμα την πληρωμή του ενοικίου σε τακτική βάση, τη λήψη ενός δανείου, την εξόφληση ενός δανείου, την τοποθέτηση και τη διευθέτηση πολύπλοκων στοιχημάτων. Οι έξυπνες συμβάσεις αποτελούν την πιο σημαντική και πολλά υποσχόμενη δυνατότητα του blockchain τα τελευταία χρόνια.[8]

Ο Emin Gün Sirer, αναπληρωτής καθηγητής της επιστήμης υπολογιστών στο πανεπιστήμιο Cornell, που έχει συμμετάσχει σε έναν μεγάλο αριθμό έργων σχετικών με το Blockchain, υποστηρίζει πως το Blockchain θα μπορούσε να εκδημοκρατίσει τον ασφαλιστικό κλάδο. Σύμφωνα με τον ίδιο, αυτό θα μπορούσε να επιτευχθεί με τη χρήση έξυπνων συμβάσεων που θα ενεργοποιούν την πληρωμή των ασφαλιστήριων συμβολαίων χωρίς να χρειάζεται να επέμβουν οι ασφαλισμένοι.[10]

Η έξυπνη περιουσία (Smart Property) είναι μια άλλη σχετική έννοια που αφορά τον έλεγχο της ιδιοκτησίας ενός ακινήτου ή ενός περιουσιακού στοιχείου μέσω του Blockchain με τη χρήση έξυπνων συμβολαίων. Η ιδιοκτησία μπορεί να έχει φυσική υπόσταση όπως είναι ένα αυτοκίνητο, ένα σπίτι ή ένα smartphone, ή μπορεί να μην έχει φυσική υπόσταση όπως είναι οι μετοχές μιας εταιρίας. Σ' αυτό το σημείο αξίζει να σημειωθεί ότι το Bitcoin, στην πραγματικότητα, σχετίζεται ακριβώς με τον έλεγχο της ιδιοκτησίας του χρήματος.[1]

Ωστόσο, τα έξυπνα συμβόλαια δεν βρήκαν εφαρμογή μέχρι και την ανακάλυψη των ψηφιακών νομισμάτων (κρυπτονομισμάτων). Τώρα, με την ενσωμάτωση τους στο Blockchain μπορούν να ενεργοποιούν πληρωμές όταν ισχύσουν η προϋποθέσεις μιας συμφωνίας με τη μορφή συμβολαίου.[1]

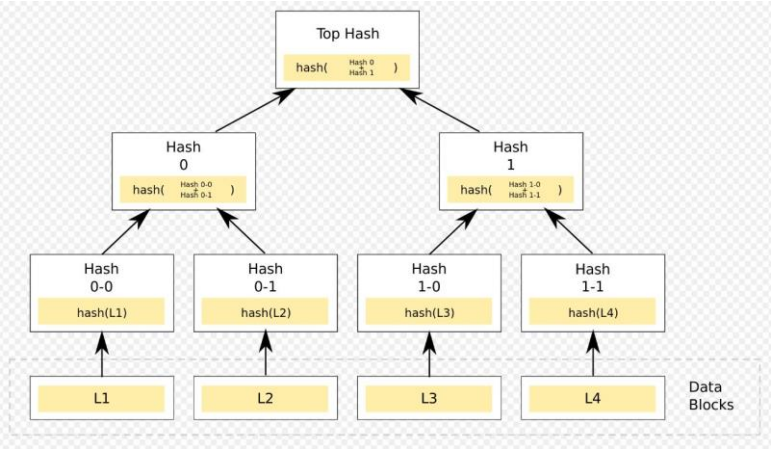
1.3 Δομή Blockchain

1.3.1 Δέντρα Merkle

Τα δέντρα κατακερματισμού (hash trees) ή δέντρα Merkle ανακαλύφθηκαν και πήραν το όνομά τους, το 1979, από τον ιδρυτή τους Ralph Merkle.[1] Ένα δέντρο Merkle είναι ένα δυαδικό δέντρο στο οποίο αρχικά οι είσοδοι τοποθετούνται στα φύλλα, δηλαδή στους κόμβους που δεν έχουν παιδιά.[6] Η κάθε τιμή ενός φύλλου είναι, στην πραγματικότητα, το κρυπτογραφικό αποτύπωμα (hash) ενός block δεδομένων.[1] Η τιμή του κάθε γονικού κόμβου

[1] https://en.wikipedia.org/wiki/Merkle_tree

είναι ο συνδυασμός των hashes των κόμβων παιδιών του. Δηλαδή, στο επόμενο στάδιο, οι τιμές των ζευγαριών των κόμβων παιδιών ενώνονται και παράγουν την τιμή του γονικού κόμβου, έως ότου παραχθεί τελικά η τιμή κατακερματισμού (hash) της ρίζας του δέντρου, η οποία είναι γνωστή και ως ρίζα Merkle (ή root hash)[1] [6]. Στην παρακάτω εικόνα παρουσιάζεται ένα δυαδικό δέντρο Merkle. Οι τιμές 0-0 και 0-1 είναι τα κρυπτογραφικά αποτυπώματα (hashes) των μπλοκ δεδομένων L1 και L2 αντίστοιχα. Το hash 0 του γονικού κόμβου προκύπτει από τη συνένωση των hashes των δύο παιδικών του κόμβων (hash0=hash(hash 0-0 + hash(0-1)).



Εικόνα 1:Παράδειγμα δέντρου Merkle[1]

Τα δέντρα Merkle αποτελούν μία γενίκευση των καταλόγων κατακερματισμού (hash lists) και των αλυσίδων κατακερματισμού (hash chains)[1] . Μια λίστα κατακερματισμού είναι ένας κατάλογος των hashes των block δεδομένων και αποτελεί ουσιαστικά μια δευτερεύουσα διάταξη του δέντρου Merkle.[1] Μια αλυσίδα κατακερματισμού (hash chain) προκύπτει από τη διαδοχική εφαρμογή μιας κρυπτογραφικής συνάρτησης κατακερματισμού (hash function) σε πρόσθετα κομμάτια δεδομένων, προκειμένου να καταγραφεί η χρονολογία ύπαρξής τους.[2]

Επειδή το δέντρο κατακερματισμού είναι ένα δυαδικό δέντρο, για τον υπολογισμό της ρίζας Merkle απαιτείται υπολογισμός ενός αριθμού hashes ανάλογου με τον λογάριθμο του αριθμού των κόμβων-φύλλων του δέντρου, σε αντίθεση με τις λίστες κατακερματισμού, όπου ο αριθμός αυτός είναι ανάλογος του αριθμού των κόμβων-φύλλων.[11]

Τα δένδρα Merkle χρησιμοποιούνται ευρέως για την ασφαλή και αποτελεσματική επαλήθευση οποιουδήποτε μεγάλου συνόλου δεδομένων που έχει αποθηκευτεί σε υπολογιστές ή μεταφερθεί μεταξύ υπολογιστών [3][6]. Μπορούν να εξασφαλίσουν ότι τα μπλοκ δεδομένων που λαμβάνονται από άλλους ομότιμους κόμβους σε ένα δίκτυο peer-to-peer είναι άθικτα και αμετάβλητα, καθώς επίσης και να ελέγχουν ότι οι υπόλοιποι ομότιμοι κόμβοι δεν αποστέλλουν παραποιημένα, κατεστραμμένα ή ψεύτικα μπλοκ δεδομένων.[1]

Στον Blockchain, τα δένδρα Merkle χρησιμοποιούνται κυρίως για την αποτελεσματική επαλήθευση των συναλλαγών. Η ρίζα Merkle σε ένα blockchain βρίσκεται στο τμήμα κεφαλίδας ενός μπλοκ (block header), το οποίο αποτελεί το hash όλων των συναλλαγών ενός

[1] https://en.wikipedia.org/wiki/Hash_list
[2] https://en.wikipedia.org/wiki/Hash_chain
[3] https://en.wikipedia.org/wiki/Merkle_tree

μπλοκ. Συνεπώς, αυτό σημαίνει ότι η επαλήθευση μόνο της ρίζας Merkle είναι αρκετή και για την επαλήθευση όλων των συναλλαγών που υπάρχουν στο δέντρο Merkle, και επομένως όλων των συναλλαγών ενός μπλοκ, αντί για την εξακρίβωση όλων των συναλλαγών μία προς μία.[6] Τα δέντρα Merkle χρησιμοποιούνται στο δίκτυο ομότιμων κόμβων του Bitcoin και του Ethereum.[12]

Οι περισσότερες υλοποιήσεις των δέντρων κατακερματισμού είναι δυαδικές, δηλαδή κάτω από κάθε γονικό κόμβο υπάρχουν δύο παιδικοί κόμβοι. Ωστόσο, είναι δυνατό να υπάρχουν και υλοποιήσεις δέντρων Merkle που χρησιμοποιούν πολύ περισσότερους παιδικούς κόμβους κάτω από κάθε γονικό κόμβο.[1]

Για τον κατακερματισμό (hashing) χρησιμοποιείται μία κρυπτογραφική συνάρτηση κατακερματισμού. Ένα παράδειγμα μιας τέτοιας συνάρτησης είναι η SHA-2. Εάν το δέντρο κατακερματισμού χρησιμοποιείται αποκλειστικά για προστασία από πιθανή ακούσια ζημιά, τότε μπορεί να χρησιμοποιηθεί η συνάρτηση κατακερματισμού CRC. Αυτές και άλλες συναρτήσεις κατακερματισμού αναλύονται στο κεφάλαιο 1.4.1.[1]

Στην κορυφή κάθε δυαδικού δένδρου κατακερματισμού, όπως εξηγήθηκε παραπάνω, υπάρχει το κορυφαίο hash (top hash ή root hash) ή αλλιώς η ρίζα Merkle. Σε ένα δίκτυο peer-to-peer το root hash αποκτάται από μία αξιόπιστη πηγή, πριν ακόμα από τη λήψη ενός αρχείου από οποιονδήποτε ομότιμο κόμβο του δικτύου. Από τη στιγμή που είναι διαθέσιμο το root hash, το δέντρο κατακερματισμού μπορεί να ληφθεί από οποιαδήποτε μη αξιόπιστη πηγή, όπως από οποιονδήποτε ομότιμο χρήστη στο δίκτυο peer-to-peer. Στη συνέχεια, το root hash του δέντρου που έχει προέλθει από τον ομότιμο κόμβο συγκρίνεται με το αρχικό root hash του έμπιστου δέντρου. Εάν το δέντρο κατακερματισμού είναι κατεστραμμένο ή ψεύτικο, τότε θα δοκιμαστεί ένα άλλο δέντρο κατακερματισμού από άλλον ομότιμο κόμβο μέχρι να εντοπιστεί ένα που αντιστοιχεί στον στο root hash του έμπιστου δέντρου.[13]

Η βασική διαφορά ενός δέντρου κατακερματισμού από μία λίστα κατακερματισμού είναι ότι είναι δυνατόν ένα κλαδί (branch) του δέντρου κατακερματισμού να μεταφορτώνεται κάθε φορά και έτσι είναι δυνατόν να ελέγχεται αμέσως η ακεραιότητα κάθε κλαδιού, χωρίς να χρειάζεται να είναι το όλο το δέντρο διαθέσιμο. Στην *Εικόνα 1* για παράδειγμα, η ακεραιότητα του μπλοκ δεδομένων L2 είναι δυνατόν να επαληθευτεί άμεσα, εάν το δέντρο κατακερματισμού περιέχει ήδη το hash 0-0 και το hash 1. Η επαλήθευση πραγματοποιείται εφαρμόζοντας τη συνάρτηση κατακερματισμού (hashing) στο μπλοκ L2 και στη συνέχεια, συνδυάζοντας το hash που προκύπτει με το hash 0-0, και ύστερα πάλι συνδυάζοντας το hash που προκύπτει με το hash 1 για να καταλήξουμε στο hash της ρίζας. Το hash της ρίζας που βρέθηκε συγκρίνεται με το αρχικό, αυθεντικό top hash του έμπιστου δέντρου. Εάν είναι ίδια, τότε επαληθεύεται το μπλοκ δεδομένων L2. Σε αντίθετη περίπτωση, γίνεται αντιληπτό ότι πρόκειται για ένα τροποποιημένο μπλοκ δεδομένων. Με όμοια λογική, η ακεραιότητα του μπλοκ L3 μπορεί να επαληθευτεί, εάν το δέντρο κατακερματισμού περιέχει ήδη το hash 1-1 και το hash 0. Αυτό μπορεί να είναι ένα πολύ σημαντικό πλεονέκτημα, δεδομένου ότι είναι εφικτό να χωριστούνε τα δεδομένα σε μικρά μπλοκ δεδομένων, έτσι ώστε να χρειάζεται να μεταφορτωθούν ξανά μικρά μπλοκ δεδομένων σε περίπτωση που καταστραφούν. Εάν το αρχείο των κρυπτογραφικών αποτυπωμάτων (hashes) των δεδομένων είναι πολύ μεγάλο τότε είναι αναπόφευκτο και το μεγάλο μέγεθος της λίστας κατακερματισμού ή του δέντρου κατακερματισμού που δημιουργούνται με βάση αυτό. Όμως, αν δημιουργηθεί ένα δέντρο

αντί για λίστα, τότε η ακεραιότητα ενός κλαδιού μπορεί γρήγορα να ελεγχθεί και ύστερα να μεταφορτωθούνε τα δεδομένα που χρειάζονται. [1]

Η ρίζα Merkle (root hash) του δέντρου κατακερματισμού δεν υποδεικνύει ποιο είναι το βάθος του δέντρου. Ένα είδος επίθεσης, λοιπόν, περιλαμβάνει τη δημιουργία ενός αρχείου διαφορετικού από το αυθεντικό, το οποίο όμως έχει πανομοιότυπη ρίζα Merkle, αλλά διαφορετικό βάθος. Για παράδειγμα, αν κοιτάξουμε την *Εικόνα 1*, είναι δυνατό να δημιουργηθεί ένα αρχείο, το οποίο περιέχει δύο μπλοκ δεδομένων, αντί για τέσσερα που περιέχει το αυθεντικό, με κρυπτογραφικά αποτυπώματα hash 0-0 + hash 0-1 για το πρώτο μπλοκ, και hash 1-0 + 1-1 για το δεύτερο. Το δέντρο αυτό έχει την ίδια ρίζα Merkle με το αυθεντικό της εικόνας, είναι όμως ένα διαφορετικό δέντρο κατακερματισμού[14][15]. Μια απλή διόρθωση είναι η εξής: στην περίπτωση που υπολογίζεται το hash ενός φύλλου τότε προστίθεται ένα byte 0x00 μπροστά από το hash, ενώ στην περίπτωση που υπολογίζεται το hash ενός εσωτερικού κόμβου προστίθεται ένα byte 0x01 μπροστά από το hash.

1.3.2 Hash chain

Όπως έχει αναφερθεί πολλές φορές, το Blockchain είναι μια σειρά μπλοκ δεδομένων με χρονική σφραγίδα, τα οποία διαχειρίζονται από ένα δίκτυο υπολογιστών, ένα δίκτυο ομότιμων κόμβων peer-to-peer. Τα μπλοκ αυτά σχηματίζουν μια αλυσίδα, συνδέονται δηλαδή μεταξύ τους μέσω της κρυπτογραφίας, και συγκεκριμένα με τη χρήση αλυσίδων κατακερματισμού (hash chains).[2]

Μια αλυσίδα κατακερματισμού είναι η διαδοχική εφαρμογή μιας κρυπτογραφικής συνάρτησης κατακερματισμού σε ορισμένα δεδομένα. Στον τομέα της ασφάλειας υπολογιστών, η αλυσίδα κατακερματισμού είναι μια μέθοδος για την παραγωγή ενός μεγάλου αριθμού κωδικών μιας χρήσης (one-time passwords), δηλαδή κωδικών που είναι ενεργοί μόνο για μία σύνδεση [3], από μόνο έναν κωδικό (κλειδί ή password). Η συνάρτηση κατακερματισμού μπορεί να εφαρμοστεί διαδοχικά σε κομμάτια δεδομένων έτσι ώστε να καταγράφει τη χρονολογία δημιουργίας τους.[4]

Στην περίπτωση ενός string έστω x , η αλυσίδα κατακερματισμού είναι η διαδοχική εφαρμογή μιας συνάρτησης κατακερματισμού h σε αυτό. Για παράδειγμα, η παράσταση $h(h(h(h(x))))=h^4(x)$ δηλώνει την εφαρμογή της συνάρτησης κατακερματισμού τέσσερις φορές στο string x και δημιουργεί μια αλυσίδα κατακερματισμού με μήκος 4.[1]

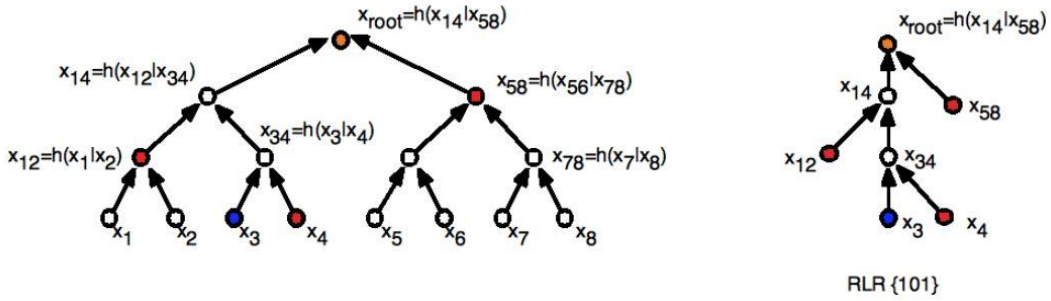
Οι αλυσίδες κατακερματισμού προτάθηκαν πρώτη φορά από τον Lamport το 1981 ως ένας τρόπος προστασίας των password σε ανασφαλές περιβάλλον. Ένας server που παρέχει επαλήθευση ταυτότητας (authentication) είναι προτιμότερο να αποθηκεύει μια αλυσίδα κατακερματισμού από ένα κείμενο χαρακτήρων προκειμένου να αποτρέψει την κλοπή του password κατά τη μετάδοση από τον server. Για παράδειγμα, ένας server εφαρμόζει τη συνάρτηση κατακερματισμού 1000 φορές σε ένα password που του δίνεται από το χρήστη και αποθηκεύει το h^{1000}(password) στην αλυσίδα κατακερματισμού. Όταν ένας χρήστης ζητά πιστοποίηση τότε δίνει στο server το h^{999}(password). Ο server υπολογίζει το h(h^{999}(password))= h^{1000}(password) και επαληθεύει ότι αυτό ταιριάζει με αυτό που είχε αποθηκευτεί στην αλυσίδα κατακερματισμού. Στη συνέχεια, αποθηκεύει το h^{999}(password)

[1] https://en.wikipedia.org/wiki/Merkle_tree
[2] https://blockgeeks.com/guides/what-is-blockchain-technology/#How_Does_a_Blockchain_Work?
[3] https://en.wikipedia.org/wiki/One-time_password
[4] https://en.wikipedia.org/wiki/Hash_chain

για να το χρησιμοποιήσει την επόμενη φορά που θα ζητήσει πιστοποίηση ο χρήστης, ο οποίος θα του δώσει το h^{998}(password). Ένας κακόβουλος χρήστης βλέποντας το h^{999}(password) να παρέχεται στον server δεν έχει τη δυνατότητα να δώσει στο server την ίδια αλυσίδα κατακερματισμού καθώς τώρα ο server περιμένει το h^{998}(password). Εξαιτίας της ιδιότητας των συναρτήσεων κατακερματισμού να μην είναι αντιστρέψιμες είναι ανέφικτο για τον εισβολέα να αντιστρέψει τη συνάρτηση κατακερματισμού και να αποκτήσει ένα παλιότερο κομμάτι της αλυσίδας. Σε αυτό το παράδειγμα, ο χρήστης μπορούσε να ζητήσει πιστοποίηση 1000 φορές, πριν εξαντληθεί η αλυσίδα. Κάθε φορά η τιμή κατακερματισμού (hash) είναι διαφορετική και, συνεπώς, δεν μπορεί να αντιγραφεί από κανέναν εισβολέα.[1]

Δυαδικές αλυσίδες κατακερματισμού (Binary Hash Chains)

Οι δυαδικές αλυσίδες κατακερματισμού συνήθως χρησιμοποιούνται σε συνδυασμό με τα δέντρα κατακερματισμού. Μία δυαδική αλυσίδα κατακερματισμού παίρνει ως είσοδο δύο τιμές κατακερματισμού (hashes), τις ενώνει και εφαρμόζει μια συνάρτηση κατακερματισμού στην ένωση τους, παράγοντας ένα τρίτο hash. Το παρακάτω σχήμα (*Εικόνα 2*) απεικονίζει ένα δέντρο κατακερματισμού με 8 κόμβους – φύλλα και δεξιά την αλυσίδα κατακερματισμού για το τρίτο φύλλο. Επιπλέον, είναι απαραίτητο να καθορίζεται και η σειρά με την οποία γίνεται η ένωση των τιμών κατακερματισμού (πχ πρώτα το αριστερά φύλλο και μετά το δεξί), προκειμένου να ολοκληρωθεί η αλυσίδα κατακερματισμού.[1]



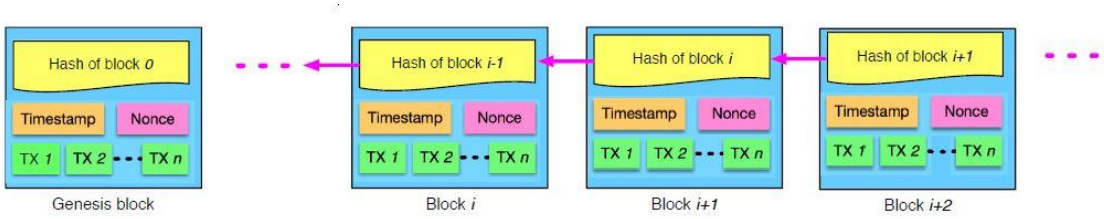
Εικόνα 2: Binary Hash Chain [2]

Στη δομή της αλυσίδας κατακερματισμού στηρίζεται και η δομή της αλυσίδας του blockchain, καθώς και οι δύο χρησιμοποιούν κάποια συνάρτηση κατακερματισμού προκειμένου να δημιουργήσουν σύνδεσμο μεταξύ των δεδομένων, όπως μεταξύ των μπλοκ στο blockchain.[1] Το blockchain, δηλαδή, ως κατανεμημένο σύστημα ενσωματώνει στη δομή του τις αλυσίδες κατακερματισμού. Κάθε νέο μπλοκ προσαρτάται στο τέλος της αλυσίδας και κάθε ένα μπλοκ συνδέεται με το προηγούμενο του μέσω κρυπτογραφικής συνάρτησης κατακερματισμού. Οντότητες που λαμβάνουν δεδομένα από κάποιο μπλοκ του blockchain έχουν τη δυνατότητα να ελέγχουν την εγκυρότητα της αλυσίδας, μέσω του ελέγχου των κρυπτογραφικών δεσμών. Από τη στιγμή που έχουν καταγραφεί τα δεδομένα σε ένα μπλοκ του blockchain, δεν είναι δυνατό έκτοτε να τροποποιηθούν χωρίς την τροποποίηση και των επόμενων μπλοκ καθώς και τη συμμετοχή και έγκριση όλου του δικτύου.[16]

Στην *Εικόνα 3* φαίνεται ένα παράδειγμα blockchain, που αποτελείται από μία συνεχή ακολουθία μπλοκ. Τα δεδομένα από τα οποία αποτελείται ένα block (timestamp, nonce κ.τ.λ.), καθώς και η σημασία του genesis block, εξηγούνται στη συνέχεια (κεφάλαιο 1.3.3).[7]

[1] https://en.wikipedia.org/wiki/Hash_chain

[2] https://en.wikipedia.org/wiki/Hash_chain#Binary_hash_chains



Εικόνα 3: Αλυσίδα Blockchain [7]

1.3.3 Δομή block

Κάθε μπλοκ στο blockchain μπορεί να αναγνωριστεί από την τιμή κατακερματισμού του, το hash του. Το hash κάθε μπλοκ δημιουργείται με τη χρήση ενός κρυπτογραφικού αλγόριθμου κατακερματισμού (π.χ SHA256) και βρίσκεται στο τμήμα που ονομάζεται κεφαλίδα (header) του μπλοκ. Κάθε μπλοκ περιέχει μια αναφορά στο προηγούμενο του μπλοκ, το οποίο ονομάζεται και γονικό μπλοκ, στο ειδικό πεδίο του header που ονομάζεται «hash του προηγούμενου μπλοκ» (previous hash).[1] Η συναλλαγή (transaction) είναι η καταγραφή ενός γεγονότος, όπως για παράδειγμα μια μεταφορά χρημάτων από κάποιον αποστολέα σε κάποιον δικαιούχο.[6] Το block είναι γενικά μία συλλογή από συναλλαγές που οργανώνονται με λογικό τρόπο. Είναι, δηλαδή, μία δομή δεδομένων, η οποία συγκεντρώνει έναν αριθμό συναλλαγών προς ενσωμάτωση στο ημερολόγιο του blockchain. Το μέγεθος του block ποικίλει ανάλογα με τον τύπο και τον σχεδιασμό του blockchain που χρησιμοποιείται. Η τοποθεσία του κάθε block στο blockchain καθορίζεται από ένα index. Το πρώτο block έχει index “0”, το επόμενο έχει index “1” κ.ο.κ. Το ύψος του block είναι ο αριθμός των προηγούμενων του block στην αλυσίδα του blockchain. Υπάρχουν δύο τρόποι αναγνώρισης ενός block. Αυτοί είναι πρώτον το hash του και δεύτερον το ύψος του[1].

Στον παρακάτω πίνακα (*Πίνακας 1*) αναλύεται με λεπτομέρεια η δομή ενός block (ενδεικτικό παράδειγμα προερχόμενο από το Bitcoin).

Πεδίο	**Μέγεθος**	**Περιγραφή**
Block size	4 bytes	Το μέγεθος του block
Block header	80 bytes	Περιλαμβάνει τα πεδία του block header (της κεφαλίδας του block), που αναλύεται στον επόμενο πίνακα.
Transaction Counter	Μεταβλητό (1-9 bytes)	Ο αριθμός των συναλλαγών που περιέχει το block.
Transactions	Μεταβλητό	Οι συναλλαγές που καταγράφονται σε αυτό το block.

Πίνακας 1: Δομή Block [6]

Το block αποτελείται από μία κεφαλίδα (block header), η οποία συνοδεύεται από ένα εκτενές αρχείο συναλλαγών που αυξάνουν το μέγεθός του block. Στο ενδεικτικό αυτό παράδειγμα που προέρχεται από το Bitcoin, η κεφαλίδα του block έχει μέγεθος 80 bytes. Ένα κοινό block περιλαμβάνει περισσότερες από 1900 συναλλαγές. Ένα πλήρες block, με τον μέγιστο αριθμό συναλλαγών που μπορεί να περιέχει, είναι σχεδόν 10.000 φορές μεγαλύτερο από την κεφαλίδα του block. [2]

[1] https://cryptoticker.io/en/blockchain-data-structure/
[2] https://cryptoticker.io/en/blockchain-data-structure/

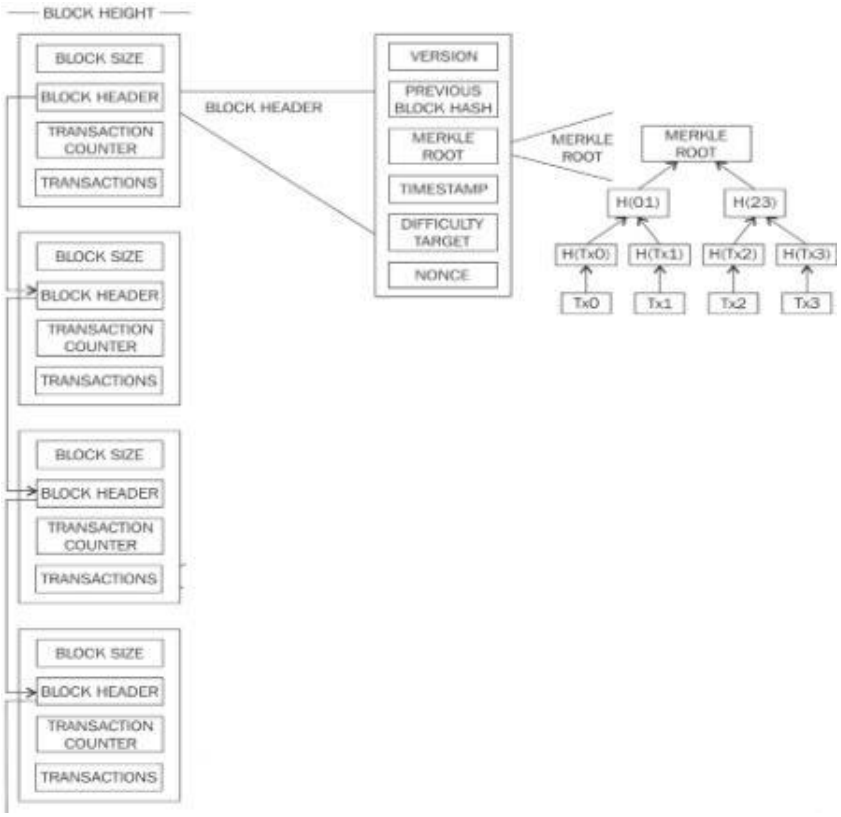
1.3.3.1 Δομή Block Header

Το block header περιλαμβάνει μεταδεδομένα (metadata), δηλαδή δεδομένα που περιγράφουν ένα άλλο σύνολο δεδομένων, όπως είναι η ρίζα του δέντρου Merkle, καθώς και το χρονικό αποτύπωμα (timestamp) και τον τυχαίο αριθμό (nonce) που σχετίζονται με το μηχανισμό συναίνεσης (consensus protocol). Στον πίνακα που ακολουθεί αναλύεται με λεπτομέρεια η δομή του block header (ενδεικτικό παράδειγμα).[1] [6]

Πεδίο	**Μέγεθος**	**Περιγραφή**
Version	4 bytes	Ο αριθμός έκδοσης του block για την παρακολούθηση αναβαθμίσεων λογισμικού Υπαγορεύει τους κανόνες επικύρωσης του block που πρέπει να ακολουθούνται.
Previous block's header hash	32 bytes	Η αναφορά στο hash του προηγούμενου (γονικού) block της αλυσίδας
Merkle root hash	32 bytes	Το hash της ρίζας του δέντρου Merkle αυτού του block, δηλαδή το hash της ρίζας του δέντρου Merkle όλων των συναλλαγών που περιλαμβάνονται σε αυτό το block
Timestamp	4 bytes	Ο χρόνος δημιουργίας του block προσεγγιστικά (Unix epoch time format)
Difficulty target	4 bytes	Το difficulty target του αλγορίθμου συναίνεσης (π.χ proof-of-work) για το block
Nonce	4 bytes	Τυχαίος αριθμός (counter) που χρησιμοποιείται από τον αλγόριθμο συναίνεσης. Η λειτουργία των αλγορίθμων συναίνεσης αναλύεται στο κεφάλαιο 1.4.4.

Πίνακας 2: Δομή Block Header [1][6]

Η παρακάτω εικόνα (*Εικόνα 4*) δείχνει μια high-level απεικόνιση του Bitcoin blockchain. Στην αριστερή πλευρά φαίνονται τα block της αλυσίδας. Η κεφαλίδα (block header) του πρώτου block επεκτείνεται στο δεξί μέρος της εικόνας και φαίνονται τα επιμέρους δεδομένα που περιλαμβάνει. Επίσης, απεικονίζεται και το δέντρο Merkle που αντιστοιχεί στο πρώτο block καθώς και πως υπολογίζεται η ρίζα Merkle, που αποτελεί το hash του block. Όπως φαίνεται ξεκάθαρα και στην *Εικόνα 4*, το blockchain είναι μια αλυσίδα από blocks, στην οποία κάθε block συνδέεται με το προηγούμενό του, μέσω μιας αναφοράς στο hash του προηγούμενου block, που βρίσκεται στο block header. Αυτή η δομή του blockchain, με τη σύνδεση των block μέσω των hashes εξασφαλίζει τη διαφάνεια και αμεταβλητότητα της αλυσίδας, αφού δεν είναι δυνατό να τροποποιηθεί καμία συναλλαγή εκτός αν το block που την περιέχει, καθώς και όλα τα block που την ακολουθούν επίσης τροποποιηθούν. [6]



Εικόνα 4: Απεικόνιση Blockchain, block, block header

1.3.3.2 Genesis Block

Το πρώτο block της αλυσίδας δεν έχει γονικό block, δηλαδή δε συνδέεται με κανένα προηγούμενο block και ονομάζεται “genesis block”. Με άλλα λόγια, αν κάποιος διαλέξει τυχαία ένα μπλοκ στην αλυσίδα και κινηθεί σε αυτή με αριστερόστροφη φορά, τότε θα καταλήξει στο genesis block. Το genesis block είναι σχεδόν πάντα ενσωματωμένο στο λογισμικό των εφαρμογών που χρησιμοποιούν το blockchain. Κάθε κόμβος στο δίκτυο έχει τουλάχιστον ένα block της αλυσίδας, το genesis block, το οποίο δεν μπορεί να τροποποιηθεί. Κάθε κόμβος πάντα αναγνωρίζει το genesis block, το hash, τη δομή του και το πότε δημιουργήθηκε. Έτσι, κάθε κόμβος γνωρίζει το σημείο εκκίνησης της αλυσίδας, μια ασφαλή ρίζα από την οποία θα χτίσει ένα αξιόπιστο blockchain. [1]

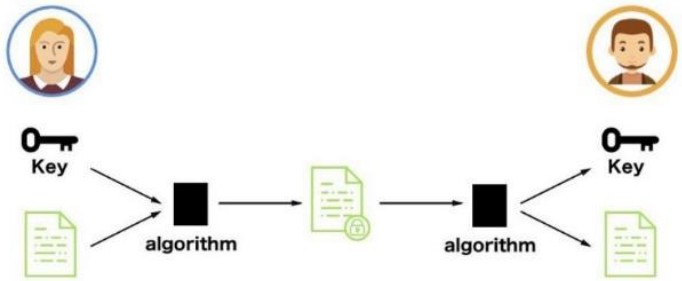
1.4 Ασφάλεια στο Blockchain

Η βασική ιδέα της κρυπτογραφίας είναι η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση. Το Blockchain είναι ένα δίκτυο peer-to-peer. Καθένας μπορεί να συνδεθεί και να συνεισφέρει υπολογιστικούς πόρους ή να υποβάλει κάποια νέα συναλλαγή δεδομένων στο σύστημα. Παρόλα αυτά, δεν είναι επιθυμητό να έχουν πρόσβαση όλοι οι χρήστες στην ιδιοκτησία που έχει ανατεθεί στους λογαριασμούς, τους οποίους διαχειρίζεται το Blockchain. Το βασικό χαρακτηριστικό της ιδιωτικής ιδιοκτησίας είναι η αποκλειστικότητα. Το δικαίωμα μεταφοράς κάποιας ιδιοκτησίας σε άλλο λογαριασμό περιορίζεται στον κάτοχο του λογαριασμού, ο οποίος κατέχει και την κυριότητα του. Ένας πολύ σημαντικός στόχος που πετυχαίνει το Blockchain είναι η προστασία της ιδιοκτησίας που

[1] https://cryptoticker.io/en/blockchain-data-structure/

ανήκει στους λογαριασμούς, χωρίς όμως να περιορίζεται η ανοικτή αρχιτεκτονική του κατανεμημένου συστήματος.[8]

Τα βασικά στοιχεία της κρυπτογραφίας είναι οι κρυπτογραφικοί αλγόριθμοι (συναρτήσεις κατακερματισμού) και τα κλειδιά.[1] Τα δεδομένα τα οποία έχουν κρυπτογραφηθεί αναφέρονται ως cypher text (κρυπτογράφημα). Το cypher text είναι χρήσιμο μόνο σε όσους διαθέτουν το απαραίτητο κλειδί και γνωρίζουν τον αλγόριθμο για την αποκρυπτογράφηση του. Τα δεδομένα που έχουν αποκρυπτογραφηθεί είναι ταυτόσημα με τα αρχικά δεδομένα πριν κρυπτογραφηθούν[8]. Συνεπώς, η βασική ιδέα της κρυπτογραφίας μπορεί να συνοψιστεί στα εξής βήματα: κάποιος χρήστης πραγματοποιεί κρυπτογράφηση κάποιων δεδομένων με ένα κλειδί και έναν αλγόριθμο (παράγεται το cypher text), τα δεδομένα αυτά είτε διατηρούνται από τον αρχικό χρήστη είτε αποστέλλονται σε κάποιον άλλο χρήστη, τα αρχικά δεδομένα ανακτώνται με την αποκρυπτογράφηση του cypher text με τη χρήση του ίδιου αλγορίθμου καθώς και πάλι ενός κλειδιού. Σε περίπτωση που κάποιος προσπαθήσει να αποκρυπτογραφήσει τα δεδομένα χρησιμοποιώντας εσφαλμένο κλειδί, το αποτέλεσμα θα είναι μια σειρά άχρηστων αριθμών, γραμμάτων και συμβόλων που δεν αποκαλύπτουν τίποτα για τα αρχικά δεδομένα που κρυπτογραφήθηκαν. Τα βασικά αυτά βήματα της κρυπτογραφίας φαίνονται στην *Εικόνα 5*.[1]



Εικόνα 5: Βασική λογική κρυπτογραφίας [1]

1.4.1 Συναρτήσεις Κατακερματισμού

Οι συναρτήσεις κατακερματισμού είναι κάποιες μαθηματικές συναρτήσεις που έχουν δημιουργηθεί με στόχο τη χρήση τους στην κρυπτογραφία. Οι συναρτήσεις αυτές παίρνοντας ως είσοδο κάποια δεδομένα δίνουν ως έξοδο (hash) μια σειρά δεδομένων καθορισμένου μεγέθους. Οι συναρτήσεις κατακερματισμού είναι μη αντιστρέψιμες, δηλαδή δεν είναι δυνατό να παραχθεί η αρχική είσοδος με κανέναν τρόπο από την έξοδο. Μια αποτελεσματική συνάρτηση κατακερματισμού υπολογίζει εύκολα την τιμή κατακερματισμού (hash) οποιασδήποτε εισόδου και επίσης τηρεί απόλυτα τον παραπάνω κανόνα της μη αντιστρεψιμότητας. Επιπλέον, σε περίπτωση που τροποποιηθεί η είσοδος τότε μεταβάλλεται και το hash, δηλαδή η έξοδος, και ακόμη δεν είναι δυνατό να υπάρχουν δύο διαφορετικές είσοδοι που να οδηγούν στην ίδια έξοδο (hash), όταν πρόκειται για μια αποτελεσματική και ασφαλή συνάρτηση κατακερματισμού.[2]

1.4.1.1 Αλγόριθμος MD5

Ο αλγόριθμος MD5 (message-digest) αποτελεί μια συνάρτηση κατακερματισμού, που χρησιμοποιείται ευρέως. Λαμβάνει μια συμβολοσειρά οποιουδήποτε μήκους (έως 256 χαρακτήρες) και κωδικοποιώντας τη, παράγει μια τιμή κατακερματισμού 128-bit. Η

[1] https://taisukemino.com/ds/
[2] https://el.wikipedia.org/wiki/Κρυπτογραφική_Συνάρτηση_Κατατεμαχισμού

κωδικοποίηση της ίδιας συμβολοσειράς με τον αλγόριθμο MD5 έχει πάντα ως αποτέλεσμα την ίδια τιμή κατακερματισμού 128-bit. [17] Επειδή ο αλγόριθμος MD5 παράγει πάντα την ίδια έξοδο για την ίδια δεδομένη είσοδο, οι χρήστες μπορούν να συγκρίνουν το hash του αρχείου προέλευσης με το πρόσφατα δημιουργημένο hash του αρχείου προορισμού, για να ελέγξουν ότι το αρχείο είναι άθικτο και δεν έχει τροποποιηθεί.[1] Ο αλγόριθμος σχεδιάστηκε το 1991 από τον Ronald Rivest, προκειμένου να αντικαταστήσει τον προηγούμενο από αυτόν αλγόριθμο κατακερματισμού MD4. [18]

Παρόλο που ο αλγόριθμος MD5 έχει βρεθεί ότι είναι ευάλωτος σε αρκετές επιθέσεις και έχει αποδυναμωθεί από εμπειρογνώμονες ασφαλείας, χρησιμοποιείται ακόμα για την επαλήθευση της ακεραιότητας των δεδομένων, αλλά μόνο ενάντια στην ακούσια αλλοίωση τους [17][19]. Μία από τις βασικές απαιτήσεις οποιασδήποτε κρυπτογραφικής συνάρτησης κατακερματισμού είναι ότι θα πρέπει να είναι υπολογιστικά ανέφικτο να βρεθούν δύο διαφορετικά μηνύματα με την ίδια τιμή κατακερματισμού. Ο αλγόριθμος MD5 αποτυγχάνει σε αυτή την απαίτηση, καθώς τέτοιες αντικρουόμενες τιμές κατακερματισμού είναι δυνατόν να υπολογιστούν σε δευτερόλεπτα από έναν συνηθισμένο οικιακό υπολογιστή.[2] Ωστόσο, αποτελεί μια μη αντιστρέψιμη συνάρτηση (μονής κατεύθυνσης) και ως εκ τούτου είναι σχεδόν αδύνατο να αντιστραφεί για την ανάκτηση της αρχικής συμβολοσειράς. Συνεπώς, παρέχει έναν εύκολο και γρήγορο τρόπο για τον κατακερματισμό μιας απλής συμβολοσειράς. Οι τιμές κατακερματισμού MDA χρησιμοποιούνται συνήθως για μικρές συμβολοσειρές για την αποθήκευση κωδικών πρόσβασης, αριθμών πιστωτικών καρτών ή άλλων ευαίσθητων δεδομένων σε βάσεις δεδομένων όπως η MySQL. [1]

Όπως υπογραμμίστηκε και παραπάνω, ο αλγόριθμος MD5 επεξεργάζεται ένα μήνυμα μεταβλητού μήκους και παράγει μια έξοδο σταθερού μήκους 128-bit. Ο αλγόριθμος έχει ως εξής:

Η συμβολοσειρά εισόδου χωρίζεται σε επιμέρους κομμάτια των 512 bits (16 λέξεις των 32 bit). Ακολουθείται μια διαδικασία padding έτσι ώστε το μήνυμα εισόδου να έχει μήκος που να διαιρείται ακριβώς από το 512. Το padding λειτουργεί ως εξής: πρώτα ένα bit 1 προστίθεται στο τέλος της συμβολοσειράς και αυτό ακολουθείται από τόσα μηδενικά όσα απαιτούνται ώστε το μήκος της συμβολοσειράς να είναι μικρότερο κατά 64 bit από ένα πολλαπλάσιο του 512. Αυτό γίνεται επειδή τα υπόλοιπα δυαδικά ψηφία γεμίζουν με 64 bits που αντιπροσωπεύουν το μήκος του αρχικού μηνύματος modulo 2^{64}. [1]

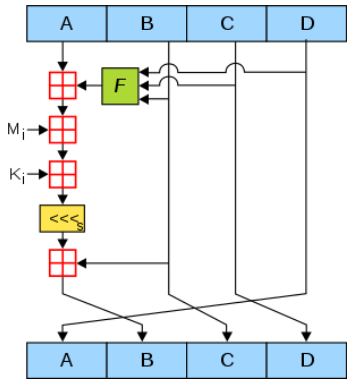
Ο βασικός MD5 αλγόριθμος λειτουργεί σε κατάσταση (state) 128 δυαδικών ψηφίων, τα οποία χωρίζονται σε τέσσερις λέξεις των 32 bit, οι οποίες σημειώνονται ως A,B,C και D. Αυτές αρχικοποιούνται σε συγκεκριμένες σταθερές. Ο αλγόριθμος, στη συνέχεια, αλλάζει την κατάσταση των τεσσάρων αυτών λέξεων χρησιμοποιώντας γι' αυτό το σκοπό με τη σειρά κάθε κομμάτι των 512 bits. Η επεξεργασία κάθε ενός από αυτά τα κομμάτια αποτελείται από τέσσερεις παρόμοιους γύρους. Κάθε γύρος αποτελείται από 16 παρόμοιες λειτουργίες που βασίζονται σε μία μη γραμμική συνάρτηση F, στην αριθμητική υπολοίπων και στην αριστερή ολίσθηση. Υπάρχουν τέσσερις πιθανές συναρτήσεις, από τις οποίες χρησιμοποιείται μία διαφορετική σε κάθε γύρο. Αυτές φαίνονται στην *Εικόνα 6* που ακολουθεί, όπου τα σύμβολα ⊕, Λ, V, ¬ δηλώνουν τις πύλες XOR, AND, OR και NOT αντίστοιχα. [1]

[1] https://www.md5hashgenerator.com/
[2] https://en.wikipedia.org/wiki/MD5

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

Εικόνα 6: Συναρτήσεις μετασχηματισμού (1/4 ανά γύρο) [1]

Η *Εικόνα 7* δείχνει μία λειτουργία του αλγορίθμου MD5. Ο MD5 περιλαμβάνει 64 τέτοιες λειτουργίες, οι οποίες ομαδοποιούνται σε τέσσερις γύρους των 16 λειτουργιών. Η F στην εικόνα είναι η μη γραμμική συνάρτηση. Μία συνάρτηση χρησιμοποιείται σε κάθε γύρο. Το M_i δηλώνει ένα μπλοκ 32-bit της συμβολοσειράς εισόδου. Όπως τονίστηκε και παραπάνω κάθε κομμάτι 512-bit της συμβολοσειράς εισόδου αποτελείται από 16 λέξεις των 32 bit. Το K_i δηλώνει μία σταθερά 32-bit, διαφορετική για κάθε λειτουργία. Το $<<<_s$ δηλώνει αριστερή ολίσθηση κατά s θέσεις. Το s ποικίλει ανάλογα με τη λειτουργία. Το σύμβολο με κόκκινο χρώμα δηλώνει πρόσθεση modulo 2^{32}. [1]



Εικόνα 7: Λειτουργία-Διεργασία MD5[1]

1.4.1.2 Αλγόριθμος SHA-1

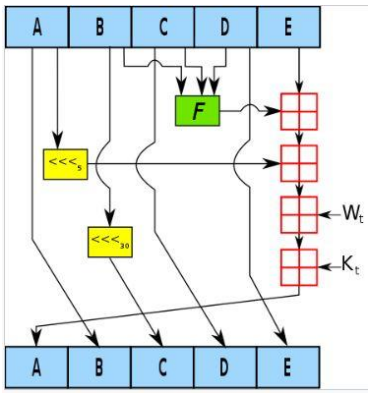
Το σύνολο των αλγορίθμων «Secure-Hash-Algorithms» είναι μια οικογένεια κρυπτογραφικών συναρτήσεων κατακερματισμού που δημοσιεύτηκαν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ως Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών των Η.Π.Α. [2]

Ο SHA-1 (Secure Hash Algorithm 1) είναι ο κρυπτογραφικός αλγόριθμος κατακερματισμού, ο οποίος παίρνει μια είσοδο και παράγει μια τιμή κατακερματισμού (message digest) 160 bit (20 byte). Η τιμή κατακερματισμού(hash) τυπικά αποδίδεται ως ένας δεκαεξαδικός αριθμός 40 χαρακτήρων. Ο αλγόριθμος σχεδιάστηκε από τον Οργανισμό Εθνικής Ασφάλειας των Η.Π.Α. Το 2020 αποδείχθηκε ότι οι επιθέσεις κατά του SHA-1 είναι το ίδιο αποτελεσματικές όσο και κατά του MD5. Ως εκ τούτου, έχει συσταθεί η αφαίρεση του SHA-1 από τα προϊόντα, ειδικότερα από αυτά που τον χρησιμοποιούν για υπογραφές, και η αντικατάστασή του από τους αλγορίθμους SHA-256 ή SHA-3. Το Φεβρουάριο του 2017 η CWI Amsterdam και η Google ανακοίνωσαν ότι πραγματοποίησαν επίθεση κατά του SHA1 και δημοσίευσαν δύο διαφορετικά αρχεία PDF που παρήγαγαν ακριβώς το ίδιο hash του SHA-1. [3]

Ο αλγόριθμος SHA-1 μοιάζει με τον αλγόριθμο MD5. Όπως και στον αλγόριθμο MD5 ακολουθείται μια διαδικασία padding έτσι ώστε το μήνυμα εισόδου να έχει μήκος που να διαιρείται ακριβώς από το 512. Η *Εικόνα 8* δείχνει τη λειτουργία συμπίεσης του αλγορίθμου SHA-1. Τα A,B,C,D και E είναι οι πέντε λέξεις των 32-bit της κατάστασης της συγκεκριμένης

[1] https://en.wikipedia.org/wiki/MD5
[2] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
[3] https://en.wikipedia.org/wiki/SHA-1

λειτουργίας. Όπως υπογραμμίστηκε και παραπάνω, ο αλγόριθμος SHA-1, σε αντίθεση με τον αλγόριθμο MD5 που λειτουργεί σε κατάσταση 128-bit, λειτουργεί σε κατάσταση 160-bit (πέντε λέξεις 32-bit). Η F στην εικόνα είναι μη γραμμική συνάρτηση. Το K_t δηλώνει μία σταθερά διαφορετική για κάθε γύρο t. Το W_t είναι το διευρυμένο μήνυμα (λέξη) του γύρου t. Το $<<<_n$ δηλώνει αριστερή ολίσθηση κατά n θέσεις. Το n ποικίλει ανάλογα με τη λειτουργία. Το σύμβολο με κόκκινο χρώμα δηλώνει πρόσθεση modulo 2^{32} .[1]



Εικόνα 8: Μια επανάληψη της λειτουργίας συμπίεσης του SHA-1 [1]

1.4.1.3 Αλγόριθμος SHA-2

Ο αλγόριθμος SHA-2 αποτελεί στην πραγματικότητα μια οικογένεια δύο παρόμοιων συναρτήσεων κατακερματισμού, με διαφορετικά μεγέθη μπλοκ, οι οποίες είναι γνωστές ως SHA-256 και SHA-512. Σχεδιάστηκαν από τον Οργανισμό Εθνικής Ασφάλειας των Η.Π.Α (NSA) και δημοσιεύτηκαν για πρώτη φορά το 2001. Διαφέρουν ως προς το μέγεθος της λέξης καθώς ο αλγόριθμος SHA-256 χρησιμοποιεί λέξεις 32-bit και ο αλγόριθμος SHA-512 χρησιμοποιεί λέξεις 64-bit. Επίσης, υπάρχουν συντομευμένες εκδόσεις του κάθε προτύπου γνωστές ως SHA-224, SHA-384, SHA-512/224 και SHA-512/256. Ο αλγόριθμος SHA-256 είναι αυτός που χρησιμοποιεί το Bitcoin. [2]

Ο αλγόριθμος SHA-2 είναι σημαντικά διαφορετικός από τον προκάτοχό του, τον SHA-1. Η οικογένεια SHA-2 αποτελείται από έξι συναρτήσεις κατακερματισμού με τιμές κατακερματισμού (hash values) μεγέθους 224, 256, 384 ή 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. Οι συναρτήσεις κατακερματισμού SHA-256 και SHA-512 χρησιμοποιούν για τους υπολογισμούς τους λέξεις των 32-bit και 64-bit αντίστοιχα. Δηλαδή, ο αλγόριθμος SHA-256 λειτουργεί σε κατάσταση 256-bit (8 λέξεις 32-bit) και ο αλγόριθμος SHA-512 λειτουργεί σε κατάσταση 512-bit (8 λέξεις των 64-bit). Όσον αφορά στον αλγόριθμο SHA-512, το μέγεθος του μπλοκ του, που προκύπτει από τη διαδικασία του padding, είναι 1024 bits, σε αντίθεση με τους αλγορίθμους MD5, SHA-1 και SHA-256 που έχουν μέγεθος block 512 bits. Χρησιμοποιούν διαφορετικές ολισθήσεις και διαφορετικές σταθερές που προστίθενται. Οι δομές τους είναι κατά τα άλλα σχεδόν ταυτόσημες, διαφέρουν μόνο στον αριθμό των γύρων. Οι πιο ισχυρές δημόσιες επιθέσεις κάμπτουν την αντίσταση πριν την εικόνα (pre-image resistance) του αλγορίθμου SHA-256 για 52 από τους 64 γύρους και του αλγορίθμου SHA-512 για 57 από τους 80 γύρους. Επίσης, κάμπτουν την

[1] https://en.wikipedia.org/wiki/SHA-1
[2] https://en.wikipedia.org/wiki/Secure_Hash_Algorithms

αντίσταση σύγκρουσης (collision resistance) για 46 από τους 64 γύρους του αλγορίθμου SHA-256.[1]

Η ιδιότητα της αντίστασης πριν την εικόνα (pre-image resistance) είναι η ιδιότητα μιας συνάρτησης κατακερματισμού και σημαίνει ότι πρέπει να είναι υπολογιστικά δύσκολο να αντιστραφεί η συνάρτηση κατακερματισμού. Δηλαδή προσφέρει προστασία απέναντι σε έναν εισβολέα που έχει στη διάθεσή του μόνο την τιμή κατακερματισμού και προσπαθεί να βρει την είσοδο. Η ιδιότητα της αντίστασης σύγκρουσης (collision resistance) σημαίνει ότι πρέπει να είναι υπολογιστικά δύσκολο να βρεθούν δύο διαφορετικές είσοδοι οποιουδήποτε μήκους που να έχουν ως αποτέλεσμα της συνάρτησης κατακερματισμού την ίδια τιμή κατακερματισμού (hash). Δεδομένου ότι μια συνάρτηση κατακερματισμού βασίζεται σε λειτουργία συμπίεσης με σταθερό μήκος τιμής κατακερματισμού (hash), είναι αδύνατο να μην υπάρχουν τέτοιου είδους συγκρούσεις. Αυτή η ιδιότητα της αντίστασης σύγκρουσης επιβεβαιώνει μόνο ότι τέτοιες συγκρούσεις θα πρέπει να βρίσκονται σπάνια. Αυτή η ιδιότητα καθιστά πολύ δύσκολο για έναν εισβολέα να βρει δύο τιμές εισόδου με την ίδια τιμή κατακερματισμού (hash).[2]

Στον παρακάτω πίνακα φαίνεται η σύγκριση των αλγορίθμων MD5, SHA-1 και SHA-2.

Αλγόριθμος		Μέγεθος Εξόδου (bits)	Μέγεθος εσωτερικής κατάστασης λειτουργίας (bits)	Μέγεθος block (bits)	Γύροι	Λειτουργίες	Επίπεδο ασφάλειας (σε bits) ενάντια στις επιθέσεις σύγκρουσης
MD5		128	128 (4x32)	512	64	And, Xor, Rot, Add(mod 2^{32}), Or	≤18
SHA-1		160	160 (5x32)	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	≤63
SHA-2	SHA-256	256	256 (8x32)	512	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	128
	SHA-512	512	512 (8x64)	1024	8	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	256

Πίνακας 3: Σύγκριση των αλγορίθμων MD5,SHA-1,SHA-2

Στην κρυπτογραφία, το επίπεδο ασφάλειας είναι ένα μέτρο της ισχύος μιας συνάρτησης κατακερματισμού. Συνήθως, εκφράζεται σε bits, όπου η n-bit ασφάλεια σημαίνει ότι ο κακόβουλος χρήστης θα πρέπει να εκτελέσει 2n λειτουργίες για να «σπάσει» τη συνάρτηση κατακερματισμού.[20] Με βάση αυτό, όπως βλέπουμε από τον πίνακα ο αλγόριθμος SHA-2 φαίνεται να είναι πιο ασφαλής από τους MD5 και SHA-1.

1.4.2 Διαχείριση κλειδιών

Η κρυπτογραφία αποτελεί το ψηφιακό ισοδύναμο των κλειδαριών ή των χρηματοκιβωτίων τραπεζών, τα οποία προστατεύουν επίσης το περιεχόμενό τους από μη εξουσιοδοτημένη πρόσβαση. Παρόμοια με τις κλειδαριές στον φυσικό κόσμο, η κρυπτογραφία χρησιμοποιεί επίσης κλειδιά για την προστασία των δεδομένων. Η βασική ιδέα είναι η αντιμετώπιση των λογαριασμών των χρηστών όπως γραμματοκιβώτια. Ο καθένας μπορεί να μεταφέρει ένα είδος ιδιοκτησίας μέσα σε ένα γραμματοκιβώτιο, αλλά μόνο ο ιδιοκτήτης του μπορεί να έχει

[1] https://en.wikipedia.org/wiki/SHA-2

[2] https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

πρόσβαση σε ό,τι συλλέγεται εκεί. Όλοι γνωρίζουν την τοποθεσία του γραμματοκιβωτίου και επομένως, ο καθένας μπορεί να τοποθετήσει κάτι μέσα σε αυτό. Μονό ο ιδιοκτήτης του όμως μπορεί να το ανοίξει με το κλειδί. Η δυνατότητα διπλής πρόσβασης στο γραμματοκιβώτιο, τόσο από το κοινό όσο και από τον ιδιοκτήτη του, καθώς και η ύπαρξη του ιδιωτικού κλειδιού, αποτελούν ένα ισοδύναμο της ψηφιακής κρυπτογραφίας δημόσιου-ιδιωτικού κλειδιού (public-private-key encryption). Κάποιος χρησιμοποιεί δημόσια κλειδιά (public keys) για τον εντοπισμό λογαριασμών, στους οποίους ο καθένας μπορεί να μεταβιβάσει κάποια ιδιοκτησία, ενώ η πρόσβαση περιορίζεται σε αυτούς που κατέχουν τα αντίστοιχα ιδιωτικά κλειδιά (private keys). Αυτό το είδος της κρυπτογραφίας χρησιμοποιείται και στο Blockchain για να εξυπηρετήσει και μία από τις βασικές απαιτήσεις του που είναι η ταυτοποίηση των λογαριασμών των χρηστών, στη διαδικασία μιας συναλλαγής.[8]

1.4.2.1 Συμμετρική κρυπτογραφία

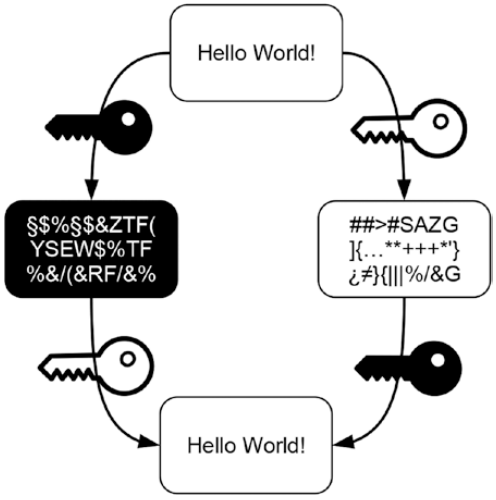
Το είδος της κρυπτογραφίας στο οποίο χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων ονομάζεται συμμετρική κρυπτογραφία[8]. Η βασική ιδέα φαίνεται στην *Εικόνα 1.* Στην περίπτωση που γίνεται μεταβίβαση πληροφορίας από έναν χρήστη σε έναν άλλον, και τα δύο μέρη θα πρέπει να έχουν το ίδιο κλειδί έτσι ώστε να μοιραστούν την πληροφορία. Ως εκ τούτου, το πρόβλημα με τη συμμετρική κρυπτογραφία είναι ότι το κλειδί είναι δυνατό να κλαπεί κατά τη μεταφορά.[1]

Εικόνα 9: Απεικόνιση συμμετρικής κρυπτογραφίας[8]

1.4.2.2 Ασύμμετρη κρυπτογραφία

Το είδος της κρυπτογραφίας το οποίο χρησιμοποιεί δύο συμπληρωματικά κλειδιά ονομάζεται ασύμμετρη κρυπτογραφία, και είναι αυτή που χρησιμοποιεί και η τεχνολογία του Blockchain. Στην ασύμμετρη κρυπτογραφία, το κρυπτογράφημα (cypher text) που δημιουργείται με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο συμπληρωματικό κλειδί και αντίστροφα. Αυτή η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης στην ασύγχρονη κρυπτογραφία φαίνεται στην *Εικόνα 10.* Το πάνω μέρος απεικονίζει την κρυπτογράφηση ενώ το κάτω μέρος την αποκρυπτογράφηση.[8]

[1] https://taisukemino.com/ds/



Εικόνα 10: Σχηματική αναπαράσταση ασύμμετρης κρυπτογραφίας [8]

Το μαύρο και το άσπρο κλειδί αποτελούν το ζευγάρι των συμπληρωματικών κλειδιών. Τα αρχικά δεδομένα είναι δυνατό να κρυπτογραφηθούν είτε με το μαύρο κλειδί παράγοντας το cypher text στο μαύρο κουτί με τα άσπρα γράμματα, είτε με το άσπρο κλειδί παράγοντας το cypher text στο άσπρο κουτί με τα μαύρα γράμματα. Στο κάτω μέρος της εικόνας φαίνεται το πως λειτουργεί η αποκρυπτογράφηση στην ασύμμετρη κρυπτογραφία. Το κείμενο στο μαύρο κουτί μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το άσπρο κλειδί, και αντίστροφα το κείμενο στο άσπρο κουτί μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το μαύρο κλειδί.[8] Το σημαντικό στην ασύμμετρη κρυπτογραφία είναι ότι δεν είναι δυνατό να αποκρυπτογραφηθούν δεδομένα με το ίδιο κλειδί με το οποίο κρυπτογραφήθηκαν. Με αυτόν τον τρόπο, λόγω της ασύμμετρης κατανομής της κρυπτογραφικής ισχύος στα δύο κλειδιά, γίνεται δυνατός ο διαχωρισμός της ομάδας των ατόμων που μπορούν να κρυπτογραφούν δεδομένα από τα άτομα που αποκρυπτογραφούν δεδομένα.

Στη συνέχεια αναλύονται τα δύο βασικά είδη της ασύμμετρης κρυπτογραφίας και εξηγείται η χρήση τους στην τεχνολογία Blockchain.

Public-to-Private

Στην περίπτωση αυτήν τα κλειδιά αυτά ονομάζονται δημόσιο και ιδιωτικό κλειδί. Γι’ αυτό και το είδος της κρυπτογραφίας που χρησιμοποιεί το Blockchain όσον αφορά στο κομμάτι της ταυτοποίησης των χρηστών ονομάζεται ασύμμετρη κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού. Το δημόσιο κλειδί είναι διαθέσιμο σε όλους. Δηλαδή, ο καθένας μπορεί να έχει ένα αντίγραφο του δημόσιου κλειδιού ανεξάρτητα ανεξαρτήτως της αξιοπιστίας του. Αντίθετα, το private key διατηρείται ασφαλές και ιδιωτικό. Ο στόχος της ασύμμετρης είναι η αποστολή των κρυπτογραφημένων δεδομένων στον ιδιοκτήτη του ιδιωτικού κλειδιού. Ο καθένας έχει τη δυνατότητα να κρυπτογραφεί δεδομένα με το δημόσιο κλειδί, αλλά μόνο ο ιδιοκτήτης του ιδιωτικού κλειδιού μπορεί να τα αποκρυπτογραφεί και να έχει πρόσβαση σε αυτά. Το σημαντικό με την ασύμμετρο σύστημα είναι ότι δεν υπάρχει το ρίσκο μεταφοράς του ιδιωτικού κλειδιού, όπως στο συμμετρικό σύστημα, στο οποίο εάν παραβιαζόταν ένα μέρος της συναλλαγής ουσιαστικά παραβιαζόταν όλο το σύστημα.[1] Για να εφαρμόσει κάποιος την ασύμμετρη κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού πραγματοποιούνται τα εξής:

[1] https://taisukemino.com/ds/

1. Δημιουργεί ένα ζευγάρι συμπληρωματικών κλειδιών.
2. Το ένα το ονομάζει public key.
3. Το άλλο το ονομάζει private key.
4. Κρατάει το private key για τον ίδιο.
5. Διαθέτει το public key στους υπόλοιπους.

Η τεχνολογία του Blockchain χρησιμοποιεί την ασύμμετρη κρυπτογραφία για να πετύχει δύο βασικούς στόχους: την ταυτοποίηση των λογαριασμών και τον έλεγχο εξουσιοδότησης για την πραγματοποίηση συναλλαγής. Το Blockchain είναι απαραίτητο να ταυτοποιεί τους λογαριασμούς χρηστών, έτσι ώστε να διατηρεί τη σύνδεση μεταξύ του ιδιοκτήτη και της ιδιοκτησίας του, καθώς και να ελέγχει τη μεταφορά ιδιοκτησίας μεταξύ των χρηστών. Οι αριθμοί των λογαριασμών των χρηστών είναι στη ουσία δημόσια κλειδιά. Επομένως, τα δεδομένα συναλλαγής χρησιμοποιούν τα δημόσια κλειδιά προκειμένου να ταυτοποιούν τους λογαριασμούς που εμπλέκονται σε μεταφορά ιδιοκτησίας. Για τον παραπάνω σκοπό, όπως υπογραμμίστηκε και παραπάνω, χρησιμοποιείται η ασύμμετρη κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού (public-to-private key encryption).

Private-to-Public

Για το κομμάτι του ελέγχου εξουσιοδότησης για την πραγματοποίηση συναλλαγής χρησιμοποιείται το αντίστροφο είδος ασύμμετρης κρυπτογραφίας που ονομάζεται ασύμμετρη κρυπτογραφία ιδιωτικού-δημόσιου-κλειδιού (private-public-key encryption). Χρησιμοποιώντας τα κλειδιά με αυτόν τον τρόπο, η πληροφορία ρέει από το ιδιωτικό κλειδί, με το οποίο κρυπτογραφείται, προς το δημόσιο κλειδί με το οποίο αποκρυπτογραφείται. Ο καθένας, ο οποίος έχει ένα αντίγραφο του δημόσιου κλειδιού μπορεί να έχει πρόσβαση στην πληροφορία, μόνο όμως ο ιδιοκτήτης του ιδιωτικού κλειδιού έχει τη δυνατότητα να δημιουργεί την πληροφορία. Τα δεδομένα συναλλαγής πάντα θα πρέπει να περιλαμβάνουν και δεδομένα που χρησιμεύουν ως απόδειξη ότι ο κάτοχος του λογαριασμού που εκχωρεί την ιδιοκτησία πράγματι συμφωνεί με την μεταφορά της. Το γεγονός ότι το cypher text που δημιουργείται με το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το συμπληρωματικό δημόσιο κλειδί είναι χρήσιμο ως απόδειξη ότι ο κάτοχος του ιδιωτικού κλειδιού είναι αυτός που έχει κρυπτογραφήσει το μήνυμα.[8] Λεπτομέρειες για αυτή τη διαδικασία, που ονομάζεται ψηφιακή υπογραφή, καθώς και για τη συνολική λογική της διαδικασίας μιας συναλλαγής, που περιλαμβάνει την υπογραφή και την ταυτοποίηση της, δίνονται στη συνέχεια.

1.4.3 Ψηφιακή υπογραφή (Digital Signature)

Σύμφωνα με τα παραπάνω, η ασύμμετρη κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού(public-private-key encryption) δεν αποδεικνύει δύο πολύ βασικά στοιχεία, των οποίων η επικύρωση είναι απαραίτητη στο Blockchain. Τα στοιχεία αυτά είναι τα εξής: πρώτον η απόδειξη ότι ο χρήστης που κρυπτογραφεί το μήνυμα είναι όντως αυτός που υποστηρίζει και δεύτερον η απόδειξη ότι τα δεδομένα που μεταφέρονται δεν έχουν τροποποιηθεί, δηλαδή ότι διατηρείται η ακεραιότητα της συναλλαγής. Όπως είδαμε πιο πάνω, το πρώτο μπορεί να αποδειχθεί με τη χρήση τα ασύμμετρης κρυπτογραφίας ιδιωτικού-δημόσιου κλειδιού(private-public-key encryption). Το δεύτερο αποδεικνύεται με τη χρήση των κρυπτογραφικών συναρτήσεων κατακερματισμού που αναλύθηκαν στο *κεφάλαιο 1.4.1.* Ο συνδυασμός αυτών των δύο αποτελεί την ψηφιακή υπογραφή (digital signature), την οποία ενσωματώνει η τεχνολογία του Blockchain.[8]

Ας υποθέσουμε ότι ο χρήστης Α του δικτύου ομότιμων κόμβων του Blockchain, επιθυμεί να πραγματοποιήσει μια συναλλαγή και να μεταφέρει κάποια ιδιοκτησία στον χρήστη Β. Θα πρέπει να εξασφαλιστούν οι εξής τρεις προϋποθέσεις: πρώτον τα δεδομένα της συναλλαγής θα πρέπει να κρυπτογραφηθούν έτσι ώστε ο παραλήπτης της ιδιοκτησίας να είναι ο χρήστης Β, δεύτερον θα πρέπει να αποδεικνύεται ότι αυτός που πραγματοποιεί τη συναλλαγή είναι ο χρήστης Α και τρίτον θα πρέπει να αποδεικνύεται ότι τα δεδομένα δεν τροποποιήθηκαν κατά τη μεταφορά. Για να ικανοποιηθούν τα παραπάνω θα χρησιμοποιηθούν αντίστοιχα : η public-to-private ασύμμετρη κρυπτογραφία για την κρυπτογράφηση, η private-to-public ασύμμετρη κρυπτογραφία για την πιστοποίηση αυθεντικότητας του χρήστη, μία συνάρτηση κατακερματισμού για την πιστοποίηση μη τροποποίησης ακεραιότητας των δεδομένων. [1]

Και οι δύο χρήστες δημιουργούν από ένα ζεύγος κλειδιών ο καθένας, ένα δημόσιο(public) και ένα ιδιωτικό(private) κλειδί ο καθένας. Ο χρήστης Β δημοσιοποιεί το δημόσιο κλειδί του (το γνωρίζει και ο χρήστης Α) και το ίδιο και ο χρήστης Α. Ο χρήστης Α που είναι ο δημιουργός της συναλλαγής αρχικά συμπεριλαμβάνει όλα τα απαραίτητα δεδομένα της συναλλαγής όπως για παράδειγμα κάποιο ποσό που μεταφέρεται, τις απαραίτητες διευθύνσεις (σε αυτό το πεδίο δημοσιοποιείται το δημόσιο κλειδί του) κτλ. Χρησιμοποιώντας τη συνάρτηση κατακερματισμού, δημιουργεί ένα hash για τα δεδομένα συναλλαγής. Έπειτα, κρυπτογραφεί αυτή την τιμή κατακερματισμού (hash) με το ιδιωτικό του κλειδί. Προσθέτει αυτό το κρυπτογραφημένο hash στη συναλλαγή, δηλαδή ουσιαστικά προσθέτει την ψηφιακή του υπογραφή στη συναλλαγή. Κρυπτογραφεί τη συναλλαγή με το δημόσιο κλειδί του χρήστη Β ώστε η ιδιοκτησία να μεταφερθεί σε αυτόν. Τέλος, μεταδίδει τη συναλλαγή ευρέως στο δίκτυο.[1]

Προκειμένου ο χρήστης Β να επαληθεύσει τη συναλλαγή, την αποκρυπτογραφεί αρχικά με το ιδιωτικό του κλειδί και εφαρμόζει την ίδια συνάρτηση κατακερματισμού προκειμένου να παράγει την τιμή κατακερματισμού. Αποκρυπτογραφεί την ψηφιακή υπογραφή της συναλλαγής, που έχει δημιουργήσει ο χρήστης Α, χρησιμοποιώντας το δημόσιο κλειδί του χρήστη Α (το οποίο περιλαμβάνεται στο πεδίο της διεύθυνσης που έχει συμπεριλάβει ο χρήστης Α στα δεδομένα συναλλαγής). Συγκρίνει το hash από τον αλγόριθμο κατακερματισμού που εφάρμοσε με το hash που αποκρυπτογράφησε από την ψηφιακή υπογραφή. Εάν αυτές οι τιμές είναι ίδιες τότε έχει επικυρώσει τη συναλλαγή. Πιστοποιεί της αυθεντικότητα του δημιουργού και την ακεραιότητα των δεδομένων συναλλαγής, ενώ περνάει η ιδιοκτησία στα χέρια του. Η συναλλαγή όπως υπογραμμίστηκε παραπάνω μεταδίδεται ευρέως στο δίκτυο του Blockchain, προκειμένου να καταγραφεί στο ημερολόγιο. Επειδή όλοι οι υπόλοιποι χρήστες-κόμβοι του δικτύου έχουν πρόσβαση στο δημόσιο κλειδί του χρήστη Α, μπορούν επίσης να επικυρώσουν τη συναλλαγή αυτού του χρήστη.[2]

1.4.4 Μηχανισμοί Συναίνεσης

Παρόλο που στο Blockchain δεν υπάρχει κάποια κεντρική οντότητα για την επικύρωση και την επαλήθευση των συναλλαγών, κάθε συναλλαγή θεωρείται ότι έχει επαληθευτεί πλήρως. Ο λόγος για τον οποίο αυτό είναι δυνατό είναι η ύπαρξη του πρωτοκόλλου συναίνεσης (Consensus Protocol), που αποτελεί και βασικό στοιχείο για κάθε δίκτυο Blockchain.

Ένας αλγόριθμος συναίνεσης (consensus algorithm) αποτελεί ουσιαστικά μια διαδικασία μέσω της οποίας όλοι οι κόμβοι του δικτύου του Blockchain καταλήγουν σε μια κοινή

[1] https://taisukemino.com/ds/
[2] https://taisukemino.com/ds/

συμφωνία για την παρούσα κατάσταση του κατανεμημένου ημερολογίου. Με αυτόν τον τρόπο, οι αλγόριθμοι συναίνεσης επιτυγχάνουν αξιοπιστία στο δίκτυο του Blockchain και δημιουργούν εμπιστοσύνη μεταξύ άγνωστων χρηστών-κόμβων στο κατανεμημένο υπολογιστικό περιβάλλον. Στην πραγματικότητα, το πρωτόκολλο συναίνεσης διασφαλίζει ότι κάθε νέο μπλοκ που προστίθεται στο Blockchain αποτελεί τη μόνη έκδοση της αλήθειας στην οποία συμφωνούνε όλοι οι κόμβοι του Blockchain.[1]

Το πρωτόκολλο συναίνεσης, που χρησιμοποιεί κάθε δίκτυο Blockchain, περιλαμβάνει ορισμένους στόχους, όπως η επίτευξη συμφωνίας, η συνεργασία, η εξασφάλιση ίσων δικαιωμάτων για κάθε κόμβο-χρήστη καθώς και η υποχρεωτική συμμετοχή κάθε κόμβου στη διαδικασία συναίνεσης. Έτσι λοιπόν, ένας αλγόριθμος συναίνεσης αποσκοπεί στην εύρεση μιας κοινής συμφωνίας, που αποτελεί μια νίκη για ολόκληρο το δίκτυο του blockchain.

Στη συνέχεια, παρουσιάζονται κάποιοι αλγόριθμοι συναίνεσης και αναλύεται ο τρόπος λειτουργίας τους.

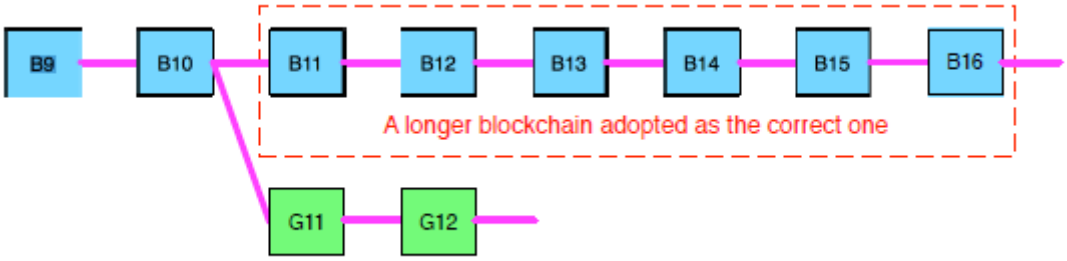
1.4.4.1 Proof of Work (PoW) – Απόδειξη εργασίας

Η απόδειξη εργασίας (PoW) είναι ένας αλγόριθμος συναίνεσης που χρησιμοποιείται στο Bitcoin. Απαιτεί μία περίπλοκη υπολογιστική διαδικασία. Στην απόδειξη εργασίας, ο κάθε κόμβος του δικτύου του Blockchain υπολογίζει την τιμή κατακερματισμού (hash) του συνεχώς μεταβαλλόμενου block header του μπλοκ. Υπολογίζει δηλαδή το συνεχώς μεταβαλλόμενο Merkle root hash του δέντρου Merkle του μπλοκ. Ο μηχανισμός συναίνεσης απαιτεί η υπολογιζόμενη τιμή κατακερματισμού να είναι ίση ή μικρότερη από μία ορισμένη δεδομένη τιμή. Στο αποκεντρωμένο δίκτυο, όλοι οι συμμετέχοντες θα πρέπει να προσπαθούν να υπολογίσουν συνεχώς την τιμή κατακερματισμού χρησιμοποιώντας διαφορετικές τιμές του nonce, μέχρι να επιτευχθεί ο στόχος. Υπενθυμίζεται εδώ ότι το nonce είναι στοιχείο της δομής του block, βρίσκεται συγκεκριμένα στο block header, και είναι ένας τυχαίος αριθμός (counter), όπως εξηγήθηκε στο *κεφάλαιο 1.3.3*. Μόλις ένας κόμβος υπολογίσει την τιμή, όλοι οι υπόλοιποι κόμβοι πρέπει να επιβεβαιώσουν αμοιβαία την ορθότητά της. Έπειτα, οποιεσδήποτε συναλλαγές στο νέο block θα επικυρώνονται μόνο σε περίπτωση απάτης. Η συλλογή των συναλλαγών που χρησιμοποιούνται για τον υπολογισμό της τιμής κατακερματισμού, είναι ουσιαστικά το αποτέλεσμα της επικύρωσης, το οποίο δηλώνεται με την προσθήκη του νέου block στην αλυσίδα. Οι κόμβοι αυτοί του δικτύου που υπολογίζουν τις τιμές κατακερματισμού ονομάζονται κόμβοι εξόρυξης ή miners και η διαδικασία απόδειξης εργασίας (PoW) ονομάζεται εξόρυξη (mining). Από τη στιγμή που αυτή η διαδικασία επαλήθευσης είναι χρονοβόρα, υπάρχει ένας μηχανισμός παροχής κινήτρων (όπως για παράδειγμα η χορήγηση ενός ποσού Bitcoins στον κόμβο που πραγματοποιεί την εξόρυξη - miner).[7]

Στο αποκεντρωμένο δίκτυο, είναι πιθανό να δημιουργηθούν ταυτόχρονα έγκυρα blocks όταν πολλαπλοί κόμβοι βρίσκουν την κατάλληλη τιμή του nonce ταυτόχρονα. Αυτό έχει ως αποτέλεσμα να δημιουργούνται διαφορετικοί κλάδοι της αλυσίδας, δηλαδή σχήματα σαν «πιρούνια» (forks), όπως φαίνεται στην *Εικόνα 11*. Ωστόσο, είναι σχεδόν αδύνατο δύο ανταγωνιστικά κλαδιά της αλυσίδας να παράγουν το επόμενο block ταυτόχρονα. Στο πρωτόκολλο συναίνεσης απόδειξης εργασίας, η αλυσίδα η οποία γίνεται μετέπειτα του διαχωρισμού μεγαλύτερη σε μήκος θεωρείται ως η αυθεντική. Στην *Εικόνα 11*, εξετάζουμε τους δύο κλάδους που δημιουργήθηκαν από την ταυτόχρονη επικύρωση των μπλοκ B11 και

[1] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/

G11. Οι κόμβοι εξόρυξης (miners) δουλεύουν και στους δύο κλάδους και προσθέτουν με τη διαδικασία της επικύρωσης το νεοσυσταθέν block σε έναν από αυτούς τους κλάδους. Όταν ένα νέο block (για παράδειγμα το B12) προστίθεται στο block B11, οι κόμβοι εξόρυξης που εργάζονται στον κλάδο G11-G12 θα μεταβούν στο B12. Το block G12 στον κλάδο G11-G12 γίνεται «ορφανό» block, αφού πλέον δεν επεκτείνεται. Γενικά, μετά από έναν συγκεκριμένο αριθμό νέων block που προσαρτώνται στο blockchain, είναι σχεδόν αδύνατο να αντιστραφούν οι κλάδοι με σκοπό την παραβίαση των συναλλαγών. Στο Bitcoin, όταν έχουν δημιουργηθεί περίπου έξι block στον κλάδο, αυτή η αλυσίδα θεωρείται ως αυθεντική (για παράδειγμα η αλυσίδα B11-B12-B13-B14-B15-B16 στην *Εικόνα 11.* Αυτός ο αριθμός, που καθορίζει πότε αποκλείεται ο ένας εκ των δύο κλάδων, εξαρτάται από τη ρύθμιση των κατάλληλων παραμέτρων του blockchain. Στο Bitcoin δημιουργείται ένα block περίπου κάθε δέκα λεπτά, ενώ στο Ethereum περίπου κάθε 17 δευτερόλεπτα.[7]



Εικόνα 11: Σενάριο δημιουργίας διαφορετικών κλάδων στην αλυσίδα του Blockchain

Οι κόμβοι- χρήστες εξόρυξης θα πρέπει, συνεπώς, να πραγματοποιήσουν πολλαπλούς υπολογισμούς και επομένως πρέπει να ξοδέψουν πολλούς υπολογιστικούς πόρους. Προκειμένου να μετριαστεί αυτή η σπατάλη των πόρων, έχουν αναπτυχθεί κάποια πρωτόκολλα απόδειξης εργασίας (PoW protocols) με τα οποία το έργο αυτό της εξόρυξης υποστηρίζεται παράλληλα από κάποιες πλευρικές εφαρμογές. Για παράδειγμα, το Primecoin αναζητά έναν ειδικό περιττό αριθμό αλυσίδων, οι οποίες είναι χρήσιμες για μαθηματική έρευνα. Αντί να καταναλώνεται ενέργεια με τη χρήση του μηχανισμού απόδειξης εργασίας, χρησιμοποιείται το πρωτόκολλο «Proof of Burn» (PoB). Αυτός ο μηχανισμός συναίνεσης ζητά από τους miners να στείλουν τα κρυπτονομίσματά τους σε ειδικές διευθύνσεις, από τις οποίες αυτά δεν μπορούν να εξαργυρωθούν. Με αυτή την «καταστροφή» νομισμάτων, οι miners αποκτούν πιθανότητες για εξόρυξη των blocks χωρίς την κατανάλωση ενέργειας και πόρων που απαιτεί η απόδειξη εργασίας.[7]

1.4.4.2 Proof of Stake (PoS) – Απόδειξη Πονταρίσματος

Ο αλγόριθμος συναίνεσης «proof of stake» αποτελεί το πιο συνηθισμένο εναλλακτικό πρωτόκολλο της απόδειξης εργασίας (PoW), που αποσκοπεί στην εξοικονόμηση ενέργειας. Αυτό που ζητείται από τους χρήστες είναι η απόδειξη της ιδιοκτησίας των ψηφιακών τους νομισμάτων, διότι θεωρείται ότι οι χρήστες που έχουν στην κατοχή τους τα μεγαλύτερα ποσά ψηφιακών νομισμάτων έχουν και τη μικρότερη πιθανότητα να πραγματοποιήσουν κάποια κακόβουλη επίθεση ενάντια στο σύστημα.[7] Το Ethereum έχει αλλάξει το πρωτόκολλο συναίνεσής του από PoW σε PoS. Σε αυτόν τον τύπο αλγορίθμου συναίνεσης, αντί οι χρήστες του δικτύου, που πραγματοποιούν την επικύρωση των μπλοκ, να επενδύουν σε ακριβό υλικό προκειμένου να επιλύσουν ένα σύνθετο πρόβλημα, επενδύουν στα ψηφιακά νομίσματα του συστήματος, κλειδώνοντας κάποια από τα δικά τους νομίσματα ως συμμετοχή (stake) σε ένα στοίχημα (ποντάρισμα) μεταξύ όλων των δυνητικών χρηστών που επικυρώνουν νέα μπλοκ. Έπειτα, όλοι οι χρήστες-επικυρωτές θα ξεκινήσουν να επικυρώνουν νέα μπλοκ. Η επικύρωση

πραγματοποιείται στην ουσία βάζοντας στοίχημα για το αν θα ανακαλύψουν ένα μπλοκ το οποίο πιστεύουν ότι μπορεί να προστεθεί στην αλυσίδα. Ύστερα, με βάση τα πραγματικά μπλοκ που προστίθενται στην αλυσίδα του Blockchain, όλοι οι χρήστες-επικυρωτές λαμβάνουν μία ανταμοιβή ανάλογη με τα στοιχήματά τους και η συμμετοχή τους (stake) αυξάνεται αναλόγως. Στο τέλος, με βάση την οικονομική του συμμετοχή (stake) στο δίκτυο επιλέγεται ένας χρήστης-επικυρωτής να δημιουργήσει ένα καινούριο μπλοκ. Αυτό προκύπτει από το βασικό κριτήριο του συγκεκριμένου πρωτοκόλλου, που υπογραμμίστηκε και παραπάνω, ότι οι «πλουσιότεροι» χρήστες είναι και οι περισσότερο ακίνδυνοι για το σύστημα. Έτσι, το πρωτόκολλο συναίνεσης PoS ενθαρρύνει τους χρήστες να επικυρώνουν μπλοκ μέσω ενός μηχανισμού παροχής κινήτρων με στόχο την επίτευξη συμφωνίας στο δίκτυο. [1]

1.4.4.3 Delegated Proof of Stake (DPoS) – Κατ' εξουσιοδότηση απόδειξη πονταρίσματος

Στον αλγόριθμο DPoS, παρόμοια με τον αλγόριθμο PoS, οι κόμβοι εξόρυξης έχουν την προτεραιότητα να δημιουργούν τα μπλοκ ανάλογα με το ποντάρισμά τους. Η πιο σημαντική διαφορά μεταξύ των δύο αλγορίθμων είναι ότι ο αλγόριθμος PoS είναι άμεσα δημοκρατικός ενώ ο αλγόριθμος DPoS είναι αντιπροσωπευτικά δημοκρατικός. Δηλαδή, οι ενδιαφερόμενοι (stakeholders) εκλέγουν τους αντιπροσώπους τους για τη δημιουργία και την επικύρωση ενός μπλοκ. Με σημαντικά μικρότερο αριθμό κόμβων να συμμετέχουν στην επικύρωση του μπλοκ, αυτό μπορεί να επικυρωθεί πιο γρήγορα, με αποτέλεσμα η διαδικασία επικύρωσης των συναλλαγών να γίνεται ταχύτερη. Επιπλέον, δεν υπάρχει ανησυχία στους χρήστες για την ύπαρξη ανέντιμων αντιπροσώπων γιατί αυτοί μπορούν εύκολα να προκύψουν από ψηφοφορία.[7]

1.4.4.4 Practical Byzantine Fault Tolerance (pBFT)

Byzantine Fault Tolerance (ανοχή στο σφάλμα) είναι ένα χαρακτηριστικό ενός κατανεμημένου δικτύου με βάση το οποίο πραγματοποιείται η επίτευξη συναίνεσης στο δίκτυο, ακόμα και αν ορισμένοι από τους κόμβους του δικτύου αποτυγχάνουν να απαντήσουν ή απαντούν με εσφαλμένες πληροφορίες. Ο στόχος δηλαδή του μηχανισμού pBFT είναι η διασφάλιση του δικτύου του blockchain ενάντια στις αποτυχίες (βλάβες) του συστήματος μέσω της χρήσης της συλλογικής λήψης αποφάσεων. Δηλαδή, βασίζεται στη συλλογική λήψη αποφάσεων, λαμβάνοντας υπόψη αμφότερους τους έγκυρους και τους ελαττωματικούς κόμβους, στοχεύοντας στην μείωση της επιρροής των ελαττωματικών κόμβων. Ο μηχανισμός συναίνεσης BFT απορρέει από το Byzantine General's Problem (πρόβλημα των Βυζαντινών Στρατηγών).[2]

Το παραπάνω πρόβλημα είχε περιγραφεί σε επιστημονικό κείμενο της Microsoft από τους Leslie Lamport, Robert Shostak και Marshall Pease το 1982. Στο πρόβλημα αυτό περιγράφονται κάποια τμήματα του βυζαντινού στρατού, τα οποία κατασκηνώνουν έξω από μία εχθρική πόλη. Κάθε τμήμα διοικείται από το δικό του στρατηγό. Οι στρατηγοί μπορούν να επικοινωνούν μεταξύ τους μόνο μέσω αγγελιαφόρου. Εφόσον εντοπίσουν δυνάμεις του εχθρού, θα πρέπει να αποφασίσουν ένα κοινό σχέδιο δράσης. Ωστόσο, υπάρχει πιθανότητα κάποιοι από τους στρατηγούς των τμημάτων να είναι προδότες και να προσπαθούν να εμποδίσουν τους έντιμους στρατηγούς να καταλήξουν σε συμφωνία. Οι στρατηγοί πρέπει να αποφασίζουν πότε θα επιτεθούν στην εχθρική πόλη, αλλά χρειάζονται την ισχυρή πλειοψηφία του στρατού τους έτσι ώστε να επιτεθούν όλα τα τμήματα ταυτόχρονα. Για αυτό

[1] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/
[2] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/

το σκοπό, οι στρατηγοί θα πρέπει να χρησιμοποιούν έναν αλγόριθμο που εγγυάται πρώτον ότι όλοι οι έντιμοι στρατηγοί αποφασίζουν για το ίδιο σχέδιο δράσης, και δεύτερον ότι ένας μικρός αριθμός από προδότες στρατηγούς δεν μπορεί να οδηγήσει τους έντιμους στρατηγούς να υιοθετήσουν ένα μη αποτελεσματικό σχέδιο. Οι έντιμοι στρατηγοί θα ακολουθήσουν ό,τι υποδεικνύει ο αλγόριθμος, αλλά και οι προδότες στρατηγοί έχουν τη δυνατότητα να κάνουν κι αυτοί οτιδήποτε θέλουν. Για αυτό το λόγο, ο αλγόριθμος θα πρέπει να εγγυάται την πρώτη προϋπόθεση που υπογραμμίστηκε παραπάνω, ανεξάρτητα από τις ενέργειες των προδοτών. Οι έμπιστοι στρατηγοί πρέπει όχι μόνο να καταλήξουν σε συμφωνία, αλλά και να συμφωνήσουν σε ένα λογικό σχέδιο.[1]

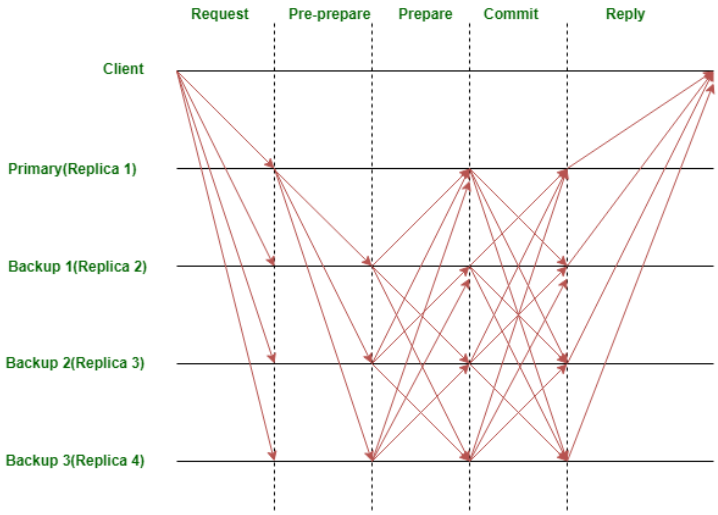
Με βάση λοιπόν την αναλογία με το παραπάνω πρόβλημα, η ανοχή του συστήματος στο σφάλμα (Byzantine fault tolerance) μπορεί να επιτευχθεί εάν οι έγκυροι κόμβοι του δικτύου καταλήξουν σε συμφωνία. Η Leslie Lamport απέδειξε ότι αν υπάρχουν 3m+1 έγκυροι κόμβοι-επεξεργαστές του δικτύου, μπορεί να επιτευχθεί συναίνεση με την προϋπόθεση ότι οι μη έγκυροι επεξεργαστές είναι το πολύ m. Αυτό σημαίνει ότι μεγαλύτερο μέρος από τα δύο τρίτα του συνολικού αριθμού των κόμβων-επεξεργαστών πρέπει να είναι ειλικρινείς προκειμένου να επιτευχθεί η συμφωνία.[1]

Ο μηχανισμός συναίνεσης pBFT παρέχει στην ουσία ένα πρακτικό αντίγραφο του μηχανισμού συναίνεσης που περιγράφτηκε στο πρόβλημα των στρατηγών, το οποίο λειτουργεί ακόμα και όταν μη έγκυροι κόμβοι ενεργούν στο σύστημα. Σε ένα κατανεμημένο σύστημα με πρωτόκολλο pBFT κάποιος κόμβος είναι ο κύριος (leader node) και οι υπόλοιποι είναι δευτερεύοντες κόμβοι (secondary – backup nodes). Εδώ σημειώνεται ότι οποιοσδήποτε κόμβος του συστήματος, που τηρεί τις προϋποθέσεις, μπορεί να γίνει κύριος (πρωτεύον) κόμβος μεταβαίνοντας από την κατάσταση δευτερεύοντος κόμβου στην κατάσταση πρωτεύοντος κόμβου. Ο στόχος είναι όλοι οι τίμιοι κόμβοι να συμβάλουν στην επίτευξη συναίνεσης όσον αφορά στην κατάσταση του συστήματος, χρησιμοποιώντας τον κανόνα της πλειοψηφίας. Ένα σύστημα pBFT μπορεί να λειτουργήσει επιτυχώς με την προϋπόθεση ότι ο μέγιστος αριθμός κακόβουλων κόμβων δεν είναι μεγαλύτερος ή ίσος από το ένα τρίτο (1/3) όλων των κόμβων στο σύστημα. Καθώς ο αριθμός των κόμβων αυξάνεται, το σύστημα γίνεται πιο ασφαλές[1]. Στο πρωτόκολλο pBFT σε κάθε κύκλο προστίθεται και ένα block στην αλυσίδα [7].

Οι κύκλοι συναίνεσης του μηχανισμού pBFT χωρίζονται σε τέσσερις φάσεις, όπως φαίνεται και στην *Εικόνα 12* [1]:

- 1η φάση: Ο πελάτης (client) στέλνει ένα αίτημα στον πρωτεύοντα κόμβο (leader node).
- 2η φάση: Ο πρωτεύον κόμβος μεταδίδει το αίτημα ευρέως σε όλους του δευτερεύοντες κόμβους.
- 3η φάση: Οι κόμβοι (πρωτογενείς και δευτερογενείς) εκτελούν την αιτούμενη υπηρεσία και ύστερα στέλνουν πίσω μία απάντηση στον πελάτη.
- 4η φάση: Το αίτημα έχει ικανοποιηθεί επιτυχώς μόνο όταν ο πελάτης λάβει m+1 απαντήσεις από διαφορετικούς κόμβους του δικτύου με το ίδιο αποτέλεσμα, όπου m είναι ο μέγιστος αριθμός μη έγκυρων κόμβων που επιτρέπονται.

[1] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/



Εικόνα 12: Οι τέσσερις φάσεις του μηχανισμού pBFT

Ο πρωτεύον κόμβος αλλάζει κατά τη διάρκεια κάθε προβολής (δηλαδή κύκλου συναίνεσης pBFT) και μπορεί να αντικατασταθεί μέσω ενός πρωτοκόλλου αλλαγής προβολής, εάν ένα προκαθορισμένο χρονικό διάστημα έχει λήξει χωρίς ο πρωτεύον κόμβος να έχει μεταδώσει κάποιο αίτημα στους δευτερεύοντες κόμβους. Εάν χρειαστεί, η πλειοψηφία των τίμιων κόμβων μπορεί να ψηφίσει για τη νομιμότητα του πρωτεύοντος κόμβου και να τον αντικαταστήσει με τον επόμενο στη σειρά κορυφαίο κόμβο.[1]

Μειονεκτήματα του μηχανισμού συναίνεσης pBFT

Το μοντέλο συναίνεσης pBFT λειτουργεί αποτελεσματικά μόνο όταν ο αριθμός των κόμβων στο κατανεμημένο δίκτυο είναι μικρός εξαιτίας της μεγάλης επιβάρυνσης λόγω επικοινωνίας, η οποία αυξάνεται εκθετικά με κάθε επιπλέον κόμβο στο δίκτυο.[47]

- **Επιθέσεις Sybil:** Οι μηχανισμοί συναίνεσης pBFT είναι ευαίσθητοι σε επιθέσεις Sybil [47]. Σε μία επίθεση Sybil, ο κακόβουλος χρήστης δημιουργεί ένα μεγάλο αριθμό ψεύτικων ταυτοτήτων και τις χρησιμοποιεί για να αποκτήσει δυσανάλογα μεγάλη επιρροή στο δίκτυο. Όσο ο αριθμός των κόμβων του δικτύου αυξάνεται, γίνεται ακόμη πιο δύσκολη η αντιμετώπιση των επιθέσεων αυτών.[2] Επειδή, λοιπόν, ο μηχανισμός συναίνεσης pBFT αντιμετωπίζει τέτοια προβλήματα κλιμάκωσης, χρησιμοποιείται σε συνδυασμό με κάποιον άλλον ή κάποιους άλλους μηχανισμούς συναίνεσης.[47]
- **Κλιμάκωση:** Ο μηχανισμός pBFT δεν κλιμακώνεται ικανοποιητικά εξαιτίας του μεγάλου φόρτου επικοινωνίας (επικοινωνία με όλους τους κόμβους σε κάθε βήμα). Όσο αυξάνεται ο αριθμός των κόμβων στο δίκτυο, τόσο αυξάνεται και ο χρόνος που απαιτείται για την απάντηση στο αίτημα του πελάτη.[47]

Πλεονεκτήματα του μηχανισμού συναίνεσης pBFT

- **Ενεργειακή απόδοση:** Ο μηχανισμός pBFT μπορεί να επιτύχει κατανεμημένη συναίνεση χωρίς να εκτελεί πολύπλοκους μαθηματικούς υπολογισμούς (όπως ο μηχανισμός PoW). Για παράδειγμα, η πλατφόρμα Zilliqa χρησιμοποιεί το μηχανισμό pBFT σε συνδυασμό με κάποιους περίπλοκους υπολογισμούς, που μοιάζουν με αυτούς του μηχανισμού PoW, για κάθε εκατοστό block του blockchain.[47] Η Zilliqa είναι μια πλατφόρμα blockchain

[1] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
[2] https://en.wikipedia.org/wiki/Sybil_attack

σχεδιασμένη γύρω από τη λογική της διαίρεσης του δικτύου (sharding) σε πολλά μικρότερα δίκτυα, τα οποία είναι σε θέση να επεξεργάζονται παράλληλα συναλλαγές.[1]

- **Οριστικοποίηση συναλλαγής:** Οι συναλλαγές δεν απαιτούν πολλαπλές επιβεβαιώσεις, αφού οριστικοποιηθούν και συμφωνηθούν. Στην περίπτωση του μηχανισμού PoW στο Bitcoin, όπου κάθε κόμβος μεμονωμένα επαληθεύει όλες τις συναλλαγές προτού προστεθεί το νέο μπλοκ στο blockchain, οι επαληθεύσεις των μπλοκ μπορεί να διαρκέσουν από δέκα έως εξήντα λεπτά.**Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**
- **Χαμηλή διακύμανση ανταμοιβής:** Κάθε κόμβος στο δίκτυο παίρνει μέρος στην απάντηση στο αίτημα του πελάτη και επομένως, κάθε κόμβος αποκτά κίνητρο να αναλάβει ηγετικό ρόλο, να γίνει δηλαδή ο πρωτεύον κόμβος. Το γεγονός αυτό οδηγεί στην μικρή διακύμανση της ανταμοιβής των κόμβων που συμβάλουν στη λήψη αποφάσεων.**Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.**

Όπως ο μηχανισμός συναίνεσης pBFT, ένα ακόμα πρωτόκολλο συναίνεσης που βασίζεται στη «βυζαντινή συμφωνία» είναι και το Αστρικό πρωτόκολλο συναίνεσης (Stellar consensus protocol -SCP). Στο μηχανισμό pBFT δεν ακολουθείται κάποια διαδικασία κατακερματισμού, αλλά οι κόμβοι υποβάλλουν ερωτήματα σε άλλους κόμβους, ενώ το πρωτόκολλο SCP δίνει στους συμμετέχοντες κόμβους το δικαίωμα να επιλέξουν το σύνολο των υπόλοιπων συμμετεχόντων που εμπιστεύονται.[7]

Πλατφόρμες που χρησιμοποιούν το πρωτόκολλο συναίνεσης pBFT ή παραλλαγές του

- Η πλατφόρμα Zilliqa, η λειτουργία της οποίας επισημάνθηκε και παραπάνω, χρησιμοποιεί το πρωτόκολλο pBFT σε συνδυασμό με το μηχανισμό συναίνεσης proof-of-work (PoW).[2]
- Η πλατφόρμα Fabric, που αποτελεί ένα Hyperledger, χρησιμοποιεί μία έκδοση του μηχανισμού pBFT.[50] Το Hyperledger είναι μια συνεργατική προσπάθεια που ξεκίνησε τον Δεκέμβριο του 2015 από τον οργανισμό Linux Foundation και έχει λάβει συνεισφορές από την IBM, την Intel και τη SAP Ariba, για να υποστηρίξει τη συνεργατική προώθηση των blockchain τεχνολογιών μεταξύ βιομηχανιών.[21] Το Hyperledger Fabric είναι μια υποδομή blockchain, την οποία συνεισέφεραν αρχικά η IBM και η Digital Asset. Παρέχει μια αρθρωτή αρχιτεκτονική με μια οριοθέτηση ρόλων μεταξύ των κόμβων, εκτέλεση έξυπνων συμβολαίων (που ονομάζονται "chaincode" στο Fabric) και υπηρεσίες συναίνεσης και συμμετοχής.[3,4]
- Η πλατφόρμα Tendermint χρησιμοποιεί το μηχανισμό pBFT σε συνδυασμό με το πρωτόκολλο delegated proof-of-stake (dPoS). Το Tendermint ανήκει σε μία κατηγορία πρωτοκόλλων που εφαρμόζουν την συναίνεση υπό μερικώς συγχρονισμένη επικοινωνία. Βασίζεται σε υποθέσεις χρονισμού για να σημειώσει πρόοδο το δίκτυο. Η ταχύτητα της προόδου δεν εξαρτάται από τις παραμέτρους του συστήματος, αλλά από την πραγματική ταχύτητα του δικτύου.[50]

1.4.4.5 Σύγκριση Αλγορίθμων Συναίνεσης

Οι αλγόριθμοι συναίνεσης έχουν διαφορετικά πλεονεκτήματα και μειονεκτήματα. Ο παρακάτω *Πίνακας 4* δείχνει τη σύγκριση μεταξύ των διαφορετικών αλγορίθμων συναίνεσης.

[1] https://en.bitcoinwiki.org/wiki/Zilliqa
[2] https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/
[3] https://en.wikipedia.org/wiki/Hyperledger
[4] https://www.hyperledger.org/

- **Διαχείριση ταυτότητας κόμβου**: Ο μηχανισμός PBFT πρέπει να γνωρίζει την ταυτότητα κάθε κόμβου που πραγματοποιεί «εξόρυξη», προκειμένου να επιλέξει ποιος θα είναι ο πρωτεύον κόμβος σε κάθε γύρο. Στους μηχανισμούς PoW και PoS, οι κόμβοι μπορούν ελεύθερα να συμμετέχουν στο δίκτυο.[7]
- **Εξοικονόμηση ενέργειας**: Στο πρωτόκολλο PoW οι κόμβοι εξόρυξης (miners) υπολογίζουν την τιμή κατακερματισμού (hash) του συνεχώς μεταβαλλόμενου block header του μπλοκ. Επομένως, η ποσότητα της ηλεκτρικής ενέργειας που απαιτείται για αυτή τη διαδικασία φτάνει σε μεγάλη κλίμακα. Όσον αφορά τον μηχανισμό PoS, οι κόμβοι εξόρυξης και πάλι υπολογίζουν την τιμή κατακερματισμού, αλλά η εργασία που πραγματοποιείται μειώνεται σε μεγάλο βαθμό, καθώς ο χώρος αναζήτησης είναι σχεδιασμένος ώστε να είναι περιορισμένος. Ο μηχανισμός συναίνεσης pBFT δεν περιλαμβάνει διαδικασία εξόρυξης. Έτσι, εξοικονομεί ενέργεια σε μεγάλο βαθμό.[7]
- **Ανοχή στη δύναμη του αντιπάλου**: Σε γενικό πλαίσιο, το 51% της ισχύος κατακερματισμού θεωρείται το κατώτερο όριο για να αποκτήσει κανείς τον έλεγχο του δικτύου. Ωστόσο, η στρατηγική της «εγωιστικής εξόρυξης» στα συστήματα που ακολουθούν το πρωτόκολλο PoW μπορεί να βοηθήσει τους κόμβους εξόρυξης να αποκομίσουν περισσότερα έσοδα κατέχοντας μόνο το 25% της ισχύος κατακερματισμού. Ο μηχανισμός pBFT είναι σχεδιασμένος έτσι ώστε να μπορεί να «ανεχτεί» έως και ένα τρίτο (1/3) μη έντιμους κόμβους από το συνολικό αριθμό κόμβων στο δίκτυο.[7]
- **Παραδείγματα**: Το **Bitcoin** βασίζεται στο μηχανισμό PoW, ενώ το **Peercoin** είναι ένα νέο δίκτυο (peer-to-peer) που βασίζεται στο πρωτόκολλο συναίνεσης PoS. Το **Bitshares**, μια πλατφόρμα ανάπτυξης για smart contracts, χρησιμοποιεί το πρωτόκολλο συναίνεσης DPoS. Τα πρωτόκολλα pBFT και **Tendermint** είναι πρωτόκολλα που απαιτούν άδεια. Δηλαδή, οι ταυτότητες των κόμβων αναμένεται να είναι γνωστές σε ολόκληρο το δίκτυο, ώστε να μπορούν να χρησιμοποιηθούν σε εμπορική λειτουργία και όχι σε δημόσια.[7]

Πρωτόκολλο Συναίνεσης	PoW	PoS	pBFT
Διαχείριση ταυτότητας κόμβου	Ανοιχτό	Ανοιχτό	Με άδεια (Permissioned)
Εξοικονόμηση ενέργειας	Όχι	Μερική	Ναι
Ανοχή στη δύναμη του αντιπάλου	<25% Υπολογιστική ισχύς	<51% Ποντάρισμα (stake)	<33% Μη έγκυροι κόμβοι
Παράδειγμα	Bitcoin	Peercoin	Hyperledger Fabric

Πίνακας 4: Σύγκριση πρωτοκόλλων συναίνεσης [7]

1.5 Τύποι Blockchain

Ένα σύστημα που βασίζεται στην τεχνολογία του blockchain μπορεί να χωριστεί σε δύο κατηγορίες, ανάλογα με επίπεδο ανοικτότητας (openness): blockchain με άδεια (permissioned) και blockchain χωρίς άδεια (permissionless) ή αλλιώς δημόσιο (public) blockchain. Το blockchain με άδεια (permissioned) μπορεί να διαιρεθεί περαιτέρω στο ιδιωτικό (private) blockchain και στο blockchain κοινοπραξίας (consortium).[22]

1.5.1 Δημόσιο Blockchain (Public Blockchain)

Όπως ακριβώς υποδηλώνει και το όνομα τους, τα δημόσια blockchains δεν ανήκουν σε κανέναν. Είναι ανοιχτά στο κοινό και μπορεί να συμμετέχει οποιοσδήποτε ως κόμβος σε αυτά χωρίς κάποια άδεια (permissionless). Επομένως, οποιοσδήποτε μπορεί να συμμετέχει στη διαδικασία λήψης αποφάσεων, στη διαδικασία της συναίνεσης, ή στην πραγματοποίηση συναλλαγών. Όλοι οι χρήστες διατηρούν ένα αντίγραφο του ημερολογίου στους τοπικούς τους κόμβους και χρησιμοποιούν έναν κατανεμημένο μηχανισμό συναίνεσης έτσι ώστε να αποφασίζουν και να διαμορφώνουν την τελική κατάσταση του ημερολογίου[6]. Το δημόσιο blockchain ενσωματώνει απόλυτα την έννοια της αποκέντρωσης. Στο δημόσιο blockchain ως μηχανισμοί συναίνεσης χρησιμοποιούνται συνήθως οι PoW και PoS.[1] Το Bitcoin και το Ethereum είναι και τα δύο δημόσια (public) blockchains.[6]

Πλεονεκτήματα του Δημόσιου Blockchain

- Ανοιχτή άδεια ανάγνωσης και εγγραφής: Οποιοσδήποτε μπορεί να συμμετάσχει υποβάλλοντας συναλλαγές στο blockchain.[54]
- Ασφάλεια και διαφάνεια: Ο μηχανισμός συναίνεσης διασφαλίζει ότι όλοι οι κόμβοι στο δίκτυο συμφωνούν ότι ένα συγκεκριμένο block περιλαμβάνει τις έγκυρες συναλλαγές. Επίσης, ο καθένας μπορεί να δει τις συναλλαγές σε ένα δημόσιο δίκτυο blockchain.[2]

1.5.2 Ιδιωτικό Blockchain (Private Blockchain)

Το ιδιωτικό blockchain είναι ένα blockchain, του οποίου η άδεια εγγραφής ελέγχεται από κάποιον οργανισμό ή κάποιο ανεξάρτητο άτομο και, η άδεια ανάγνωσης μπορεί να είναι ανοιχτή στο κοινό. Το ιδιωτικό blockchain αποτελεί το πιο κλειστό σύστημα blockchain και η χρήση του περιορίζεται στις επιχειρήσεις, τους κρατικούς φορείς ή σε ανεξάρτητα άτομα. Δεν επιλύει πλήρως το πρόβλημα εμπιστευτικότητας, αλλά βελτιώνει σημαντικά τη δυνατότητα ελέγχου.[22] Ο ιδιοκτήτης του ιδιωτικού blockchain, που μπορεί να είναι κάποιος οργανισμός, επιθυμεί να ελέγξει ποιος μπορεί να διαβάσει ή να γράψει στο ιδιωτικό blockchain. Προκειμένου να το πετύχει, θα πρέπει να γνωρίζει την ταυτότητα των χρηστών, επειδή καθίσταται αδύνατο να καθοριστούν οι κανόνες άδειας σχετικά με το ποια δεδομένα μπορούν να καταχωρηθούν με εμπιστοσύνη στο blockchain και ποια μπορούν να ανακτηθούν από αυτό.[54] Το Hyperledger Fabric και το R3 Corda είναι δύο ιδιωτικά blockchains.

Πλεονεκτήματα του Ιδιωτικού Blockchain

- Απαραίτητη άδεια: Η πρόσβαση στο blockchain ελέγχεται.[54]
- Ταχύτερες συναλλαγές: Το ιδιωτικό blockchain έχει λιγότερους κόμβους, γεγονός που καθιστά τις συναλλαγές πολύ πιο γρήγορες για επιβεβαίωση.[54]
- Καλύτερη κλιμάκωση: Οι οργανισμοί ελέγχουν τον αριθμό των κόμβων. Ο αριθμός των κόμβων που προστίθενται στο δίκτυο καθορίζεται με βάση τη ζήτηση.[54]

1.5.3 Blockchain Κοινοπραξίας (Consortium Blockchain)

Το blockchain κοινοπραξίας αποτελεί ένα blockchain το οποίο περιορίζει τη συμμετοχή των μελών του σε αυτούς που συμμετέχουν στην κοινοπραξία. Τα δικαιώματα ανάγνωσης και

[1] https://medium.com/7sevencoin/types-of-blockchain-public-private-and-consortium-blockchain-e190604df820
[2] https://medium.com/swlh/everything-you-need-to-know-about-public-private-and-consortium-blockchain-54821c159c7a

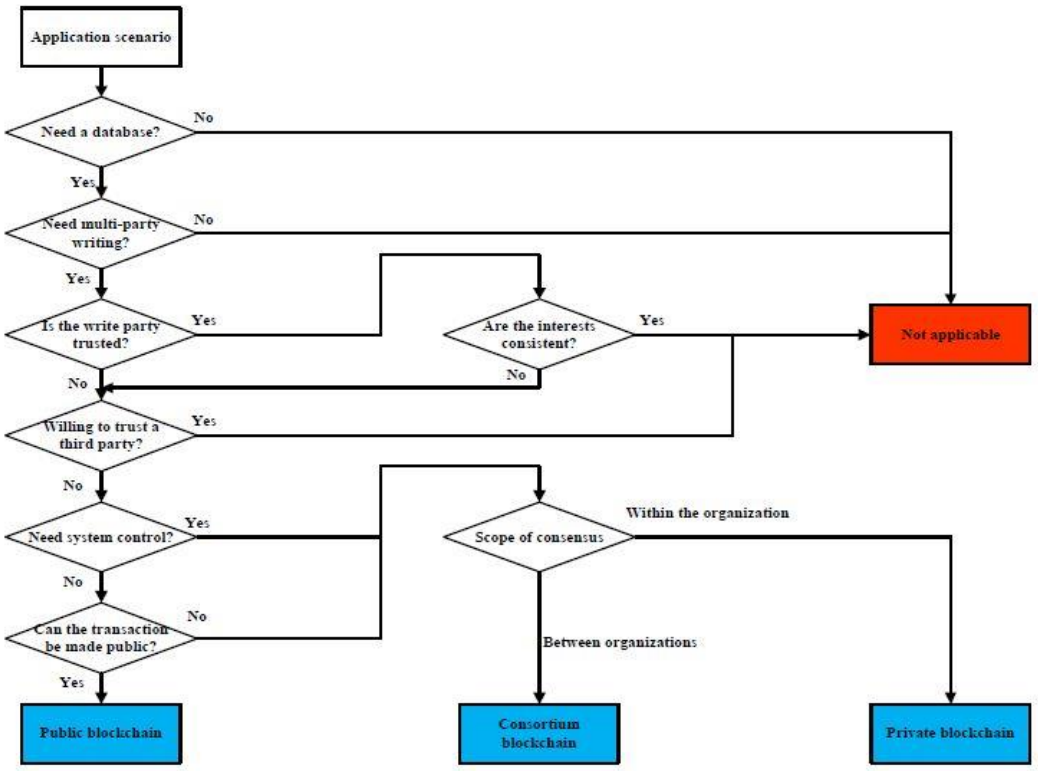
εγγραφής στο blockchain καθώς και τα σχετικά με τις συναλλαγές δικαιώματα καθορίζονται από τους κανόνες της κοινοπραξίας. Τα δεδομένα που δημιουργούν οι συμμετέχοντες είναι δυνατό να προβληθούν από τους ίδιους ή από εξουσιοδοτημένα άτομα. Με αυτόν τον τρόπο επιλύονται ζητήματα απορρήτου και ασφάλειας δεδομένων και επιτυγχάνεται η αποκέντρωση. Το blockchain κοινοπραξίας είναι ένας συνδυασμός του δημόσιου και του ιδιωτικού blockchain.[22]

Ο παρακάτω *Πίνακας 1* συνοψίζει τα χαρακτηριστικά των τριών ειδών blockchain, που αναλύθηκαν παραπάνω. Κατά την επιλογή του είδους του blockchain που θα χρησιμοποιηθεί σε ένα σύστημα, παράγοντες όπως οι απαιτήσεις βάσης δεδομένων και η πολυμερής εγγραφή στο blockchain πρέπει να λαμβάνονται υπόψη.[22]

Τύπος Blockchain	**Δημόσιο**	**Ιδιωτικό**	**Κοινοπραξίας (Consortium)**
Πρόσβαση	Δημόσια	Δημόσιο ή Περιορισμένο	Δημόσιο ή Περιορισμένο
Ενέργεια	Υψηλή	Χαμηλή	Χαμηλή
Ταχύτητα	Χαμηλή	Υψηλή	Υψηλή
Αποδοτικότητα	Χαμηλή	Υψηλή	Υψηλή
Ασφάλεια	Proof-of-work, proof-of-stake και άλλους μηχανισμούς συναίνεσης	Προ-εγκεκριμένοι συμμετέχοντες και πολυμερής συναίνεση	Προ-εγκεκριμένοι συμμετέχοντες και πολυμερής συναίνεση
Αμεταβλητότητα	Σχεδόν αδύνατο να παραβιαστεί	Μπορεί να παραβιαστεί	Μπορεί να παραβιαστεί
Διαδικασία Συναίνεσης	Χωρίς άδεια και ανώνυμη	Με άδεια και με γνωστές ταυτότητες χρηστών	Με άδεια και με γνωστές ταυτότητες χρηστών
Καθορισμός συναίνεσης	Κόμβοι εξόρυξης	Κεντρικός οργανισμός	Ομάδα πρωτευόντων κόμβων
Δίκτυο	Αποκεντρωμένο	Κεντρικό	Ημικεντρικό
Περιουσιακό στοιχείο συναλλαγών	Εγγενές ψηφιακό περιουσιακό στοιχείο	Οποιοδήποτε	Οποιοδήποτε
Έγκριση Συναλλαγής	Της τάξης κάποιων λεπτών	Της τάξης των milliseconds	Της τάξης των milliseconds

Πίνακας 5: Χαρακτηριστικά των τριών τύπων Blockchain (Public, Private, Consortium)[22]

Ερευνητική εργασία, που δημοσιεύτηκε το 2018 από την Ακαδημία Τεχνολογίας Πληροφοριών και Επικοινωνιών και Αξιόπιστων Τεχνολογιών Blockchain της Κίνας, πρότεινε ένα διάγραμμα ροής για την επιλογή του κατάλληλου είδους blockchain *(Εικόνα 13)*.[22]



Εικόνα 13: Διάγραμμα ροής για την επιλογή του κατάλληλου τύπου Blockchain

1.5.4 Υβριδικό Blockchain (Hybrid Blockchain)

Το υβριδικό blockchain είναι το blockchain που επιχειρεί να συνδυάσει τα καλύτερα χαρακτηριστικά τόσο των ιδιωτικών, όσο και των δημόσιων blockchain. Δεν είναι ανοιχτό σε όλους αλλά συνεχίζει να προσφέρει κάποια χαρακτηριστικά του blockchain όπως είναι η ακεραιότητα κα η διαφάνεια. Το υβριδικό blockchain είναι προσαρμοζόμενο. Τα μέλη του μπορούν να αποφασίσουν για το ποιος θα συμμετάσχει στο blockchain ή για το ποιες συναλλαγές δημοσιοποιούνται. Παρόλο που οι συναλλαγές δε δημοσιοποιούνται πάντα, εξακολουθούν να μπορούν να επαληθεύονται όταν αυτό χρειάζεται. Κάθε συναλλαγή που πραγματοποιείται στο υβριδικό blockchain είναι δυνατό να διατηρείται ιδιωτική και ταυτόχρονα πάντα ανοιχτή για επαλήθευση όταν αυτό απαιτείται. Επίσης, διασφαλίζεται το πιο σημαντικό χαρακτηριστικό του blockchain που είναι η αμεταβλητότητα.

Στο υβριδικό blockchain, κάθε συναλλαγή καταγράφεται μία φορά και δεν είναι δυνατό να τροποποιηθεί σε εύθετο χρόνο. Οι χρήστες έχουν τα ίδια δικαιώματα ως προς την πραγματοποίηση των συναλλαγών, αλλά η ταυτότητά τους διατηρείται μυστική από τους υπόλοιπους συμμετέχοντες. Αυτό γίνεται για την προστασία του απορρήτου του χρήστη. Όταν κάποιος χρήστης συναλλάσσεται με έναν άλλον χρήστη, τότε η ταυτότητά του αποκαλύπτεται μόνο στο μέρος (άτομο ή ομάδα ατόμων) που ασχολείται με αυτή τη συναλλαγή. Προκειμένου να διασφαλιστεί ότι η παραπάνω διαδικασία αναγνώρισης γίνεται σωστά, οι εταιρίες και οι οργανισμοί ακολουθούν τη διαδικασία KYC (Know Your Customer). Ειδικότερα, τα χρηματοπιστωτικά ιδρύματα πρέπει να χειρίζονται απόλυτα σωστά αυτή τη διαδικασία αναγνώρισης, καθώς δεν μπορούν να επιτρέψουν την πραγματοποίηση μιας συναλλαγής από κάποιον χρήστη που δεν είναι απολύτως γνωστός στο blockchain. Παρόλο που στο υβριδικό blockchain υπάρχει περιορισμένη ανωνυμία για τους χρήστες που

συμμετέχουν στο δίκτυο, η δημόσια ανωνυμία συνεχίζει να διατηρείται. Με αυτόν τον τρόπο, κανείς εκτός του δικτύου δεν γνωρίζει πληροφορίες για τους χρήστες. Το γεγονός αυτό δείχνει ότι πρόκειται για έναν αποτελεσματικό συνδυασμό του δημόσιου και του ιδιωτικού συστήματος blockchain.[1]

Μπορεί να φαίνεται ότι το υβριδικό blockchain έχει παρόμοια χαρακτηριστικά με το blockchain κοινοπραξίας (consortium), αλλά τεχνικά λειτουργούν με εντελώς διαφορετικό τρόπο. Το blockchain κοινοπραξίας λειτουργεί χρησιμοποιώντας διαφορετικό μηχανισμό συναίνεσης και ελέγχεται από κόμβους οι οποίοι είναι προεπιλεγμένοι. Το κοινό μπορεί να έχει πρόσβαση στο blockchain μέσω μιας προγραμματιστικής διεπαφής (API) και να εκτελεί τις λειτουργίες εκείνες που επιτρέπονται από το blockchain κοινοπραξίας. Το blockchain κοινοπραξίας διαχειρίζεται από μια ομάδα, που αποτελεί την κοινοπραξία. Αυτή η ομάδα αποφασίζει πως θα λειτουργήσει το blockchain. Επίσης, υπάρχει περιορισμένη πρόσβαση και η ομάδα αποφασίζει ποιος την αποκτά. Τα οφέλη της περιορισμένης πρόσβασης είναι οι ταχύτερες συναλλαγές, η καλύτερη κλιμάκωση, και το καλύτερο απόρρητο συναλλαγών. Από την άλλη, το υβριδικό blockchain μπορεί να περιγραφτεί ως ένα δημόσιο blockchain που φιλοξενείται σε ένα ιδιωτικό δίκτυο. Η περιορισμένη συμμετοχή ελέγχεται μέσω του ίδιου του ιδιωτικού δικτύου. Τεχνικά, το υβριδικό blockchain λειτουργεί δημιουργώντας τα μπλοκ δεδομένων με τις τιμές κατακερματισμού τους (hashes) χρησιμοποιώντας το ιδιωτικό δίκτυο και στη συνέχεια αποθηκεύοντας αυτά τα δεδομένα στο δημόσιο blockchain, χωρίς να διακυβεύεται το απόρρητο των δεδομένων. Σε αντίθεση με το blockchain κοινοπραξίας (consortium), το υβριδικό blockchain παρέχει έναν ευέλικτο έλεγχο του blockchain. Αυτό σημαίνει ότι ο έλεγχος της κοινοποίησης των δεδομένων δεν είναι ιδανικός και όχι καλύτερος από αυτόν στο blockchain κοινοπραξίας. Οι βασικές περιπτώσεις χρήσεις του υβριδικού blockchain είναι αυτές στις οποίες απαιτείται κλιμάκωση και αποκέντρωση.[55]

Πλεονεκτήματα του Υβριδικού Blockchain[55]

- **Λειτουργία της μορφής κλειστού οικοσυστήματος:** Δεν υπάρχει ανησυχία στις εταιρίες ή στους οργανισμούς που χρησιμοποιούν αυτό το είδος blockchain ότι θα υπάρξει διαρροή των πληροφοριών τους.
- **Προστασία από κακόβουλες επιθέσεις κατά 51%:** Τα υβριδικά blockchain έχουν κατά 51% «ανοσία» σε κακόβουλη επίθεση αφού οι κακόβουλοι χρήστες (hackers) δεν μπορούν να έχουν πρόσβαση σε ένα δίκτυο υβριδικού blockchain για να πραγματοποιήσουν την επίθεση.
- **Προστασία του απορρήτου των δεδομένων και επικοινωνία με τον «εξωτερικό κόσμο» ταυτόχρονα:** Παρόλο που το ιδιωτικό blockchain είναι το πιο αποδοτικό όσον αφορά σε θέματα απορρήτου δεδομένων, έχει περιορισμένες δυνατότητες επικοινωνίας με την κοινότητα εκτός του δικτύου. Πολλές εταιρίες έχουν την ανάγκη να διατηρούν το απόρρητο των συναλλαγών τους αλλά ταυτόχρονα να διαμορφώνουν με τέτοιο τρόπο το blockchain τους, που να τους επιτρέπει να επικοινωνούν με όλους τους μετόχους τους συμπεριλαμβανομένου και του κοινού.
- **Χαμηλό κόστος συναλλαγής:** Οι συναλλαγές είναι φθηνές καθώς απαιτούνται ολιγάριθμοι κόμβοι για την επαλήθευσή τους. Οι περισσότερο ισχυροί κόμβοι στο δίκτυο διευκολύνουν την επαλήθευση της κάθε συναλλαγής, η οποία ενδέχεται σε ένα δημόσιο blockchain να χρειαστεί εργασία από χιλιάδες κόμβους.

[1] https://101blockchains.com/hybrid-blockchain/

Περιπτώσεις Χρήσης του Υβριδικού Blockchain[1]

- **Internet of Things (IoT):** Οι περισσότερες πλατφόρμες IoT είναι κεντρικές υπολογιστικές υποδομές, βασισμένες στο cloud και έχουν σημαντικά μειονεκτήματα όπως το υψηλό κόστος συντήρησης του διακομιστή cloud και θέματα ασφάλειας και εμπιστοσύνης. Η χρήση της τεχνολογίας blockchain μπορεί να συμβάλει στην επίτευξη κατανεμημένης συναίνεσης σε ένα σύστημα IoT, που συμβάλει στην αντιμετώπιση αυτών των προβλημάτων.[23] Είναι δύσκολη η διαχείριση του Διαδικτύου των Πραγμάτων με μια δημόσια λύση blockchain, καθώς θα μπορούσε να δώσει στους κακόβουλους χρήστες ελεύθερα δεδομένα με τα οποία θα μπορούσαν να χαρτογραφήσουν τους κόμβους του δικτύου, ή ακόμα και να πραγματοποιήσουν κάποια επίθεση σε αυτούς. Με τη χρήση του υβριδικού blockchain σε ένα σύστημα IoT οι συσκευές μπορούν να τοποθετηθούν σε ιδιωτικό δίκτυο, και σε αυτές να έχουν πρόσβαση όσοι τις χρειάζονται. Ορισμένες πτυχές του δικτύου μπορούν να κοινοποιηθούν ανάλογα με τα δεδομένα που μπορούν να δημοσιοποιηθούν. Μια υβριδική λύση μπορεί να λύσει πολλά προβλήματα ασφαλείας.
- **Οικονομία και Εμπόριο:** Η πλατφόρμα XinFin βασίζεται σε ένα υβριδικό blockchain. Χρησιμοποιεί το Ethereum για το δημόσιο μέρος και το Quorum για το ιδιωτικό μέρος της υβριδικής λύσης. Στόχος είναι η παροχή μιας παγκόσμιας πλατφόρμας χρηματοδότησης και εμπορίου, χρησιμοποιώντας την υβριδική τεχνολογία. Ο μηχανισμός συναίνεσης που χρησιμοποιείται είναι η κατ' εξουσιοδότηση απόδειξη πονταρίσματος (delegated Proof-of-Stake – dPoS).
- **Τραπεζικές συναλλαγές:** Δεδομένου ότι οι τράπεζες πρέπει να επιλύσουν εσωτερικά προβλήματα και επίσης να διαφυλάξουν και τις πληροφορίες των χρηστών, μπορούν να χρησιμοποιήσουν αυτή την υβριδική προσέγγιση. Ακόμα και το Ripple, που αποτελεί ένα συγκεντρωτικό blockchain κρυπτονομισμάτων σχεδιάζει μια ενδεχομένως υβριδική προσέγγιση.
- **Εφοδιαστική αλυσίδα:** Η εφοδιαστική αλυσίδα είναι τεράστια. Συνεπώς, δεν μπορεί να επιλεχθεί σε αυτή την περίπτωση μια ιδιωτική ή δημόσια λύση. Πολλές εταιρίες εφοδιαστικής αλυσίδας (logistics) έχουν ήδη αρχίσει να την υλοποιούν. Ένα παράδειγμα είναι η εταιρία IBM Food Trust. Έχοντας βασιστεί στο υβριδικό blockchain, στοχεύουν στη βελτίωση της αποτελεσματικότητας σε ολόκληρη την αλυσίδα τροφίμων. Πρόκειται για ένα δίκτυο στο οποίο παίρνουν μέρος όλοι όσοι συμμετέχουν στην εφοδιαστική αλυσίδα συμπεριλαμβανομένων των αγροτών, των χονδρεμπόρων, των διανομέων και πολλών άλλων.
- **Κυβερνήσεις:** Οι κυβερνήσεις μπορούν να χρησιμοποιήσουν το blockchain για την πραγματοποίηση εκλογών, τη δημιουργία δημόσιας βάσης δεδομένων για αναγνώριση και ταυτοποίηση, την καταγραφή σύνθετων δεδομένων, την αυτοματοποίηση των εξαγορών, την παροχή ανθρωπιστικής βοήθειας κ.α. Για να πραγματοποιηθούν τα παραπάνω, πρέπει να χρησιμοποιηθεί υβριδική λύση. Παρέχει στην κυβέρνηση τη δυνατότητα ελέγχου που χρειάζεται και ταυτόχρονα επιτρέπει την πρόσβαση του κοινού.

Συνολικά, το υβριδικό blockchain μπορεί να χρησιμοποιηθεί σε έργα για τα οποία δεν είναι κατάλληλο ούτε το δημόσιο, ούτε το ιδιωτικό blockchain. Το δημόσιο blockchain μπορεί να χρησιμοποιηθεί σχεδόν σε κάθε κλάδο. Είναι κατάλληλο για δημόσια έργα και για τη δημιουργία κρυπτονομισμάτων για εμπορική χρήση.[56] Το ιδιωτικό blockchain είναι

[1] https://101blockchains.com/hybrid-blockchain/

κατάλληλο για κάποιον οργανισμό, ο οποίος απαιτεί πλήρη έλεγχο της ροής εργασιών του. Οι μηχανισμοί PoW και PoS είναι κατάλληλοι για δημόσια blockchain. Για τα blockchain κοινοπραξίας ή ιδιωτικά blockchain μπορεί να είναι καταλληλότεροι οι μηχανισμοί pBFT.[7]

2 Μετανάστευση και Blockchain

2.1 Μετανάστευση και προσφυγικό στην Ευρωπαϊκή Ένωση

2.1.1 Ιστορική Αναδρομή

Στο κεφάλαιο αυτό περιγράφονται οι γενικές εξελίξεις στο πεδίο των μεταναστευτικών και προσφυγικών ροών στην Ευρώπη καθώς και τα πρότυπα εγκατάστασης των μεταναστών από τη δεκαετία του 1950 και μετά, δηλαδή ουσιαστικά υστέρα από τη λήξη του Β΄ Παγκοσμίου Πολέμου. Η μετανάστευση στην ΕΕ έχει μακρά ιστορία, αλλά παρουσιάζει σημαντική αύξηση από τον εικοστό αιώνα και μετά. Ιδιαίτερα οι χώρες της Δυτικής Ευρώπης δέχθηκαν μεγάλο αριθμό μεταναστών μετά το Β' Παγκόσμιο Πόλεμο. Στο σύγχρονο περιβάλλον της παγκοσμιοποίησης, οι μεταναστεύσεις στην Ευρώπη έχουν επιταχυνθεί [24]. Ως αποτέλεσμα της συμφωνίας του Σένγκεν του 1985, οι πολίτες των κρατών μελών της ΕΕ και οι οικογένειές τους έχουν το δικαίωμα να ζουν και να εργάζονται οπουδήποτε εντός της ΕΕ λόγω της ιθαγένειας της ΕΕ. Όμως οι πολίτες των κρατών που δεν ανήκουν στην ΕΕ δεν έχουν αυτά τα δικαιώματα, εκτός εάν κατέχουν την άδεια παραμονής μακράς διαρκείας της ΕΕ ή είναι μέλη της οικογένειας πολιτών της ΕΕ. Ωστόσο, όλοι οι κάτοχοι έγκυρων αδειών διαμονής ενός κράτους Σένγκεν έχουν το δικαίωμα να ταξιδεύουν εντός του χώρου Σένγκεν μόνο για τουριστικούς σκοπούς και για έως και τρεις μήνες.[1]

Αφετηρία της ιστορικής αυτής αναδρομής αποτελούν οι συμφωνίες σχετικά με τη μετακίνηση μεταξύ των χωρών ενός αριθμού μεταναστών-εργαζομένων που υπογράφηκαν από πολλές ευρωπαϊκές χώρες στις δεκαετίες του 1950 και του 1960. Διακρίνουμε τρεις κύριες περιόδους από το σημείο αυτό και μετά. Η πρώτη περίοδος έχει διάρκεια από το 1950 έως το 1974, δηλαδή φτάνει μέχρι την πετρελαϊκή κρίση το 1973-1974. Η πετρελαϊκή κρίση του 1973 ξεκίνησε τον Οκτώβριο του 1973 όταν τα μέλη του Οργανισμού Αραβικών Χωρών Εξαγωγών Πετρελαίου (OAPEC) κήρυξαν εμπάργκο πετρελαίου. Το εμπάργκο στόχευε στις χώρες που υποστήριζαν το Ισραήλ (Καναδάς, Ιαπωνία, Ολλανδία, Ηνωμένο Βασίλειο) κατά τη διάρκεια του πολέμου του Yom Kippur, μιας στρατιωτικής επίθεσης που εξαπέλυσαν η Αίγυπτος και η Συρία με την υποστήριξη και άλλων αραβικών χωρών εναντίον του Ισραήλ. Μέχρι το τέλος του 1974, που τελείωσε το εμπάργκο, η τιμή του πετρελαίου είχε αυξηθεί κατά 300%, δηλαδή ανέβηκε από τα 3 δολάρια στα 12 δολάρια.[2] Η περίοδος αυτή χαρακτηρίστηκε από σταθερή οικονομική ανάπτυξη, την ανάπτυξη προγραμμάτων επισκεπτών εργαζομένων, την επιστροφή μεταναστών από πρώην αποικίες στις μητέρες-χώρες, και τη μετανάστευση προσφύγων, η οποία αποτυπώθηκε στις κινήσεις τους από την Ανατολή προς τη Δύση. Η δεύτερη περίοδος (1974-1980) ξεκίνησε με την πετρελαϊκή κρίση και τελείωσε με την πτώση του Σιδηρού Παραπετάσματος στα τέλη της δεκαετίας του 1980. Κατά τη διάρκεια αυτής της περιόδου οι βορειοδυτικές ευρωπαϊκές κυβερνήσεις περιόριζαν όλο και περισσότερο τη μετανάστευση και η βασική μέθοδος εισόδου των μεταναστών έγινε η οικογενειακή επανένωση. Επιπλέον, οι αιτήσεις ασύλου αυξήθηκαν. Μέχρι το τέλος αυτής της περιόδου, οι μεταναστευτικές ροές είχαν αρχίσει να στρέφονται προς χώρες μετανάστευσης στη Νότια

[1] https://en.wikipedia.org/wiki/Immigration_to_Europe
[2] https://en.wikipedia.org/wiki/1970s_energy_crisis

Ευρώπη. Η τρίτη περίοδος διήρκησε από την πτώση του Σιδηρού Παραπετάσματος μέχρι σήμερα, με την αυξανόμενη επιρροή της Ευρωπαϊκής Ένωσης (ΕΕ), τον έλεγχο της μετανάστευσης από τρίτες χώρες στην ΕΕ, καθώς και την ενθάρρυνση της ενδοευρωπαϊκής κινητικότητας. [25]

2.1.1.1 Περίοδος 1950-1974 : Μετακίνηση Μεταναστών-Εργαζομένων και Αποικιοκρατία

Την περίοδο μετά τον Δεύτερο Παγκόσμιο Πόλεμο, η βορειοδυτική Ευρώπη άνθισε οικονομικά. Για παράδειγμα, η βιομηχανική παραγωγή αυξήθηκε κατά 30% μεταξύ 1953 και 1958 [26]. Οι γηγενείς εργαζόμενοι σε αυτές τις χώρες της βορειοδυτικής Ευρώπης γινόταν ολοένα και πιο μορφωμένοι και έτσι δόθηκαν σε πολλούς από αυτούς οι ευκαιρίες να εργαστούν σε επιχειρησιακές και οργανωτικές θέσεις εργασίας. Οι ντόπιοι εργαζόμενοι δεν μπόρεσαν να καλύψουν τις θέσεις εργασίας καθώς και ο ντόπιος πληθυσμός δεν ήταν πλέον πρόθυμος να αναλάβει ανθυγιεινές και κακοπληρωμένες θέσεις εργασίας στη γεωργία, τον καθαρισμό, τις κατασκευές και την εξόρυξη. Ως αποτέλεσμα, οι βορειοδυτικές ευρωπαϊκές κυβερνήσεις (Βέλγιο, Γαλλία, Γερμανία, Λουξεμβούργο, Σουηδία, Ελβετία) άρχισαν να προσλαμβάνουν εργατικό δυναμικό από περιφερειακές χώρες.[25]

Οι αλλοδαποί εργαζόμενοι αναμενόταν να επιστρέψουν στην πατρίδα τους μετά την ολοκλήρωση της εργασίας τους. Ως εκ τούτου, είχαν λίγα δικαιώματα και λίγη ή καθόλου πρόσβαση στην υποστήριξη κοινωνικής πρόνοιας. Στο τέλος αυτής της περιόδου, οι περισσότεροι μετανάστες στη Βορειοδυτική Ευρώπη προέρχονταν από την Αλγερία, την Ελλάδα, την Ιταλία, το Μαρόκο, την Πορτογαλία, την Ισπανία, την Τυνησία, την Τουρκία και τη Γιουγκοσλαβία. Σχηματίστηκε, λοιπόν, ένα σύστημα μετανάστευσης με το οποίο οι περιφερειακές χώρες, όπως οι χώρες της Νότιας Ευρώπης, παρείχαν εργαζόμενους σε χώρες της Βορειοδυτικής Ευρώπης. Εκτός αυτού, οι μεταναστευτικές ροές καθοδηγούνταν έντονα από τις διαφορές στην οικονομική ανάπτυξη μεταξύ περιφερειών που χαρακτηρίζονται από αγροβιομηχανίες και από εκείνες με οικονομικά υψηλή βιομηχανία, τόσο σε διεθνές όσο και σε εθνικό επίπεδο [27]. Αντιπροσωπευτικό παράδειγμα αποτελεί η μετακίνηση ανειδίκευτων εργαζομένων από περιοχές της Νότιας Ιταλίας προς τα βιομηχανικά κέντρα της Βόρειας Ιταλίας. Οι περισσότεροι μετανάστες εργαζόμενοι προέρχονταν από φτωχές γεωργικές περιοχές όπου δεν υπήρχε επαρκής εργασία, όπως η Βόρεια Πορτογαλία, η Δυτική Ισπανία, η Νότια Ιταλία και η Βόρεια Ελλάδα.[25]

Ωστόσο, οι ευρωπαϊκές κυβερνήσεις διεύρυναν σταδιακά τις ζώνες πρόσληψης και σε χώρες εκτός Ευρώπης. Ένας από τους κύριους λόγους ήταν η περίοδος του Ψυχρού Πολέμου στην Ευρώπη που περιόρισε σοβαρά την κινητικότητα των μεταναστών από την Ανατολή προς τη Δύση. Στη Δυτική Γερμανία, για παράδειγμα, υπήρξε σημαντική εισροή εργαζομένων από την Ελλάδα, την Ιταλία και την Ισπανία, καθώς και από την Ανατολική Γερμανία. Η κατασκευή του Τείχους του Βερολίνου το 1961, ωστόσο, διέκοψε τη μετανάστευση εργαζομένων από την Ανατολική προς την Δυτική Γερμανία. Ως αποτέλεσμα, η Δυτική Γερμανία επαναπροσανατόλισε την πρόσληψή της προς άλλες χώρες. Έτσι, υπέγραψε διμερείς συμφωνίες με την Τουρκία (1961), το Μαρόκο (1963), την Πορτογαλία (1964), την Τυνησία (1965) και τη Γιουγκοσλαβία (1968). Ακολούθησαν και άλλες χώρες προορισμού, όπως το Βέλγιο, οι Κάτω Χώρες, η Γαλλία και η Ελβετία, που υπέγραψαν επίσης συμφωνίες μετανάστευσης εργασίας με αυτές τις χώρες στη δεκαετία του 1960. Η διεθνής μετανάστευση αυτής της περιόδου αντιμετωπίστηκε γενικά θετικά λόγω των οικονομικών της πλεονεκτημάτων τόσο για τις χώρες αποστολής όσο και για τις χώρες υποδοχής. Στην περιοχή της Μεσογείου, για παράδειγμα, η μετανάστευση βοήθησε στην ανακούφιση των πιέσεων

στην αγορά εργασίας, καθώς η περιοχή χαρακτηριζόταν από σημαντική δημογραφική πίεση, χαμηλή παραγωγικότητα και υψηλή ανεργία.[25]

Οι εκτιμήσεις του αριθμού των ατόμων που εγκατέλειψαν την Ιταλία, την Ισπανία, την Ελλάδα και την Πορτογαλία μεταξύ 1950 και 1970 κυμαίνονται από 7 έως 10 εκατομμύρια. Όπως φαίνεται από τον Πίνακας 6, το 1950 οι περισσότεροι πληθυσμοί μεταναστών βρέθηκαν στη Γαλλία, το Ηνωμένο Βασίλειο, τη Γερμανία και το Βέλγιο.

Χώρα	1950	1960	1970	Ποσοστό επί του πληθυσμού
Βέλγιο	354	444	716	8.5%
Γαλλία	2128	2663	3339	7.9%
Δυτική Γερμανία	548	686	2977	6.6%
Ολλανδία	77	101	236	2.6%
Σουηδία	124	191	411	5.0%
Ελβετία	279	585	983	16.0%
Ηνωμένο Βασίλειο	1573	2205	3968	7.8%

Πίνακας 6: Πληθυσμιακές μειονότητες μεταναστών στις Χώρες της Κεντρικής και Δυτικής Ευρώπης 1950-1970. Οι αριθμοί αντιπροσωπεύουν χιλιάδες μεταναστών.[28]

Οι αριθμοί για όλες τις χώρες, εκτός του Ηνωμένου Βασιλείου, είναι για αλλοδαπούς κατοίκους. Εξαιρούνται τα πολιτογραφημένα άτομα και οι μετανάστες από τις ολλανδικές και γαλλικές αποικίες. Τα στοιχεία του Ηνωμένου Βασιλείου είναι απογραφικά στοιχεία των ετών 1951, 1961 και 1971. Στις αρχές της δεκαετίας του 1970, οι αριθμοί αυτοί είχαν αυξηθεί σημαντικά τόσο σε απόλυτους όσο και σε σχετικούς όρους. Ένας στους επτά χειρώνακτες στο Ηνωμένο Βασίλειο και ένας στους τέσσερις βιομηχανικούς εργάτες στο Βέλγιο, τη Γαλλία και την Ελβετία ήταν ξένης προέλευσης στα μέσα της δεκαετίας του 1970. Ταυτόχρονα, η διαδικασία αποικιοποίησης οδήγησε σε σημαντικές μεταναστευτικές ροές προς τις (πρώην) αποικιακές δυνάμεις της Ευρώπης. Ένας σημαντικός αριθμός ατόμων από τις αποικίες ήρθαν στο Βέλγιο, τη Γαλλία, τις Κάτω Χώρες, το Ηνωμένο Βασίλειο και τη δεκαετία του 1970 στην Πορτογαλία. Σύμφωνα με εκτιμήσεις, μεταξύ του 1940 και του 1975 ο αριθμός των ατόμων ευρωπαϊκής καταγωγής που επέστρεψαν από αποικίες ήταν περίπου 7 εκατομμύρια. Οι κύριες μεταναστευτικές ροές ήταν από την Κένυα, την Ινδία και τη Μαλαισία στο Ηνωμένο Βασίλειο, από τη Βόρεια Αφρική στη Γαλλία και την Ιταλία, από το Κονγκό στο Βέλγιο και από την Ινδονησία προς τις Κάτω Χώρες. Τέλος, το Σιδηρούν Παραπέτασμα (Iron Curtain) περιόρισε σοβαρά την κινητικότητα Ανατολής-Δύσης, χωρίς όμως να τη σταματήσει. Σιδηρούν Παραπέτασμα ονομάστηκε η νοητή διαχωριστική γραμμή που τέθηκε μεταξύ της Σοβιετικής Ένωσης (και των χωρών της Ανατολικής Ευρώπης με κουμουνιστικά καθεστώτα όπως η Τσεχοσλοβακία, η Ρουμανία κ.τ.λ.) και των χωρών του Ν.Α.Τ.Ο και των συμμάχων τους. Συγκεκριμένα, μεταξύ του 1950 και του 1990, 12 εκατομμύρια άνθρωποι μετανάστευσαν από την Ανατολή στη Δύση και πολλοί από αυτούς στη Γερμανία. Η συντριπτική πλειοψηφία μεταναστών της Δυτικής Ευρώπης μετά την πτώση του Σιδηρού Παραπετάσματος προήλθε από την πρώην Σοβιετική Ένωση. Περιστασιακά, ωστόσο, υπήρχαν μεγαλύτερες εισροές Ανατολικών Ευρωπαίων, μετά από πολιτικές κρίσεις όπως από την Ουγγαρία (1956–1957), την Τσεχοσλοβακία (1968–1969) και την Πολωνία (1980–1981).[25]

2.1.1.2 Περίοδος 1974-Τέλος της δεκαετίας του 1980 : Πετρελαϊκή Κρίση και Έλεγχος της Μετανάστευσης

Η πετρελαϊκή κρίση του 1973-1974 είχε σημαντικό αντίκτυπο στο οικονομικό τοπίο της Ευρώπης, μειώνοντας την ανάγκη για εργασία. Η Ελβετία και η Σουηδία ήταν οι πρώτες χώρες που πραγματοποίησαν μια στάση μετανάστευσης το 1970 και το 1972 αντίστοιχα, και ακολούθησαν και άλλες όπως η Γερμανία το 1973 και η Γαλλία το 1974. Παρόλα αυτά, οι νέες αυτές πολιτικές δεν κατάφεραν να σταματήσουν τη μετανάστευση, αλλά την οδήγησαν σε μετασχηματισμό. Πιο συγκεκριμένα, οι μετανάστες μη Ευρωπαϊκών χωρών, που είχαν υπαχθεί σε προγράμματα πρόσληψης εργασίας εγκαταστάθηκαν με πιο μόνιμο τρόπο πλέον, φέρνοντας στην Ευρώπη και τις οικογένειες τους, μιας και πλέον η επιστροφή τους στη χώρα καταγωγής τους για μεγάλο χρονικό διάστημα ενείχε σημαντικό κίνδυνο απώλειας της άδειας παραμονής τους.[25]

Κατά τη διάρκεια αυτής της περιόδου άλλαξε και η σύσταση του μεταναστευτικού πληθυσμού, καθώς το μερίδιο των μη Ευρωπαίων μεταναστών αυξήθηκε σημαντικά. Για παράδειγμα, στη Σουηδία, το 1970 μόλις το 7,6% των γεννήσεων αλλοδαπών αφορούσαν μη Ευρωπαίους πολίτες, ενώ μέχρι το 1999 αυτό το ποσοστό έφτασε στο 40%. Το γεγονός αυτό αντανακλά και τη φυσική εσωτερική ανάπτυξη των πληθυσμών αυτών στη χώρα μετανάστευσης. Το γεγονός αυτό ήταν επίσης αποτέλεσμα της αυξανόμενης επιστροφής πληθυσμών μεταναστών της Νότιας Ευρώπης, δεδομένης της αυξημένης ποιότητας ζωής και ευκαιριών απασχόλησης στη Νότια Ευρώπη.[29]

Οι χώρες, την περίοδο αυτή, ελέγχουν όλο και περισσότερο τις εισόδους των αλλοδαπών. Η αύξηση των επιπέδων ανεργίας λόγω της οικονομικής ύφεσης πυροδότησε εχθρότητα, ρατσισμό και ξενοφοβία απέναντι σε ορισμένες «ορατές» ομάδες κατοίκων μεταναστών. Παρόλα αυτά έγινε, επίσης, κατανοητό σε πολιτικούς ηγέτες και λαό ότι οι ομάδες των μεταναστών είναι πλέον ένα μέρος του πληθυσμού και της κοινωνίας. Ως αποτέλεσμα, η ανάγκη για επαρκείς πολιτικές ένταξης έγινε εμφανής και αυτές οι πολιτικές άρχισαν αργά να αναπτύσσονται. [25]

Επιπλέον, ο αριθμός των αιτήσεων ασύλου άρχισε να αυξάνεται στην Ευρώπη, ειδικά τη δεκαετία του 1980 και μετά την πτώση του Τείχους του Βερολίνου. Στο χρονικό διάστημα μεταξύ των αρχών της δεκαετίας του 1970 και του τέλους του εικοστού αιώνα, ο αριθμός των αιτήσεων ασύλου στην ΕΕ (αποτελούμενη τότε από 15 κράτη μέλη) αυξήθηκε από 15 χιλιάδες σε 300 χιλιάδες ετησίως. Η Γερμανία αποτέλεσε τον μεγαλύτερο αποδέκτη αιτήσεων ασύλου στην Ευρώπη σε όλες τις περιόδους, όπως φαίνεται και στον Πίνακας 7. Η δραματική αύξηση των αιτήσεων ασύλου από την Ανατολική Ευρώπη στις αρχές της δεκαετίας του 1990 συνόδευε την αποσύνθεση της Σοβιετικής Ένωσης και των Γιουγκοσλαβικών πολέμων.[25]

Χώρες	1970-74	1980-84	1990-94	1995-99
Συνολικές αιτήσεις ασύλου στην Ε.Ε	64.5	540.2	2419.8	1613.5
Γερμανία	34.3	249.6	1374.7	749.6
Βέλγιο	1.7	14.5	87.0	93.4
Γαλλία	5.1	106.3	184.5	112.2
Ηνωμένο Βασίλειο	-	17.5	150.8	223.3
Ελλάδα	-	6.4	12.8	11.8

Πίνακας 7 Οι περιορισμοί στην είσοδο ξένων ατόμων στις χώρες της Βορειοδυτικής Ευρώπης είχαν, επίσης, ως αποτέλεσμα τη στροφή των μεταναστευτικών ροών προς τη Νότια Ευρώπη, από τα μέσα της δεκαετίας του 1980

και ιδιαίτερα κατά τη δεκαετία του 1990. Η Νότια Ευρώπη έγινε λοιπόν ένας ελκυστικός προορισμός για μη Ευρωπαίους μετανάστες, ιδίως εκείνους από τη Βόρεια Αφρική, τη Λατινική Αμερική, την Ασία και την Ανατολική Ευρώπη, μετά την πτώση του σιδηρού παραπετάσματος. Εκτός από τις μεταναστευτικές ροές από μη ευρωπαϊκές χώρες, οι ευνοϊκές οικονομικές συνθήκες στη Νότια Ευρώπη οδήγησαν επίσης στην επιστροφή της μετανάστευσης από τη Βόρεια στη Νότια Ευρώπη. Η Ελλάδα ήταν η τελευταία χώρα που πέρασε από μια χώρα με έξοδο μεταναστών προς άλλες ευρωπαϊκές χώρες σε μια χώρα επιστροφής μεταναστών. Μέχρι το 1973, περίπου 1 εκατομμύριο Έλληνες εργαζόταν στο εξωτερικό. Οι μισοί από αυτούς επέστρεψαν την περίοδο μετά την πετρελαϊκή κρίση.[30]

2.1.1.3 Περίοδος Δεκαετία 1990-2012 : Πρόσφατες τάσεις μετανάστευσης προς την Ευρώπη και εντός αυτής

Από το 1990 και μετά, το άνοιγμα των συνόρων της Ανατολικής Ευρώπης προκάλεσε νέες μεταναστευτικές ροές σε όλη την Ευρώπη. Ένα μεγάλο ποσοστό μεταναστών, προερχόμενων από πρώην κράτη του ανατολικού μπλοκ, κατά τη δεκαετία του 1990, μετακινήθηκε σε χώρες της Δυτικής Ευρώπης, ειδικά στην Ισπανία, την Ελλάδα, τη Γερμανία, την Ιταλία, την Πορτογαλία και το Ηνωμένο Βασίλειο. Υπάρχουν συγκεκριμένα μοτίβα μετανάστευσης που επαναλαμβάνονται και σχετίζονται σε πολύ μεγάλο βαθμό με τη γεωγραφία, τη γλώσσα και τον πολιτισμό. Για παράδειγμα, πολλοί Πολωνοί έχουν μεταναστεύσει στο Ηνωμένο Βασίλειο, την Ιρλανδία και την Ισλανδία, ενώ ένας μεγάλος αριθμός μεταναστών ρουμάνικης και βουλγάρικης καταγωγής έχουν επιλέξει την Ισπανία και την Ιταλία. Το τέλος του Ψυχρού Πολέμου, καθώς και οι πόλεμοι στην πρώην Γιουγκοσλαβία οδήγησαν σε νέες ροές αιτούντων άσυλο προς τη Δυτική Ευρώπη. Μεταξύ 1989 και 1992, για παράδειγμα, οι αιτήσεις ασύλου αυξήθηκαν από 320.000 σε 695.000, μειώθηκαν σε 455.000 έως το τέλος της δεκαετίας και αυξήθηκαν ξανά σε 471.000 το 2001. Δύο από τις κύριες χώρες καταγωγής κατά τη διάρκεια αυτής της περιόδου ήταν η Ομοσπονδιακή Δημοκρατία της Γιουγκοσλαβίας (836.000) και η Ρουμανία (400.000). Μεταξύ 2002 και 2006, οι αιτήσεις ασύλου στην Ευρώπη ακολούθησαν πτωτική πορεία. Ωστόσο, από το 2006 και μετά, οι αιτήσεις ασύλου αυξήθηκαν λόγω των συγκρούσεων στο Αφγανιστάν και στο Ιράκ. Μέχρι το 2010, οι 25 χώρες της ΕΕ (με επιπλέον τη Νορβηγία και την Ελβετία) είχαν λάβει 254.180 αιτήσεις και η ανθρωπιστική μετανάστευση αντιπροσώπευε το 6% των νεοεισερχόμενων στην ΕΕ. Οι περισσότερες αιτήσεις υποβλήθηκαν στη Γαλλία (47.800), στη Γερμανία (41.300) και στη Σουηδία (31.800).[25]

Κατά τη διάρκεια αυτής της περιόδου, η είσοδος στην ΕΕ περιορίστηκε σταδιακά λόγω της ενοποίησης της ευρωπαϊκής αγοράς, η οποία επέβαλε αυστηρούς συνοριακούς ελέγχους. Αυτοί οι έλεγχοι στην είσοδο των αλλοδαπών οδήγησαν και στην αυξημένη παράνομη μετανάστευση.

Κατά τη διάρκεια αυτής της τρίτης περιόδου, τα ζητήματα ένταξης έγιναν κεντρικό ζήτημα πολιτικής. Πολλές ευρωπαϊκές χώρες ενέτειναν τις προσπάθειες προσέλκυσης μεταναστών με υψηλή εξειδίκευση ή εκπαίδευση. Αυτός ο στόχος αντανακλάται ακόμη σε πολλά εθνικά προγράμματα σήμερα, όπως για παράδειγμα, στη Δανία, τη Γερμανία, τη Σουηδία και το Ηνωμένο Βασίλειο. Η ΕΕ καθιέρωσε το Σχέδιο Μπλε Κάρτας, μιας άδειας διαμονής και εργασίας σε ολόκληρη την ΕΕ. Έτσι, η μετανάστευση φοιτητών από χώρες εκτός ΕΕ έγινε ολοένα και μεγαλύτερη σε ορισμένα μέρη της ΕΕ. Τα ιδρύματα τριτοβάθμιας εκπαίδευσης έχουν συμμετάσχει σε αυτές τις προσπάθειες, υποκινούμενα από τα οικονομικά οφέλη της προσέλκυσης διεθνών φοιτητών με τη μορφή υψηλών διδάκτρων. Σε αυτό το πλαίσιο, αρκετές ευρωπαϊκές χώρες, όπως η Γαλλία, η Γερμανία, οι Κάτω Χώρες και το Ηνωμένο Βασίλειο απλοποίησαν τις διαδικασίες μετάβασης από την εκπαίδευση στην εργασία για τους διεθνείς φοιτητές. [31]

Αξίζει να σημειωθεί η διάκριση μεταξύ της κινητικότητας των ευρωπαίων πολιτών εντός της ΕΕ και της μετανάστευσης εντός και προς την ΕΕ υπηκόων τρίτων χωρών, καθώς αυτές οι δύο ομάδες υπόκεινται σε διαφορετική νομοθεσία. Η ενδοευρωπαϊκή κινητικότητα θεωρείται ως συμβολή στη ζωτικότητα και ανταγωνιστικότητα της ΕΕ. Επιπλέον, οι ευρωπαίοι πολίτες έχουν το δικαίωμα να κυκλοφορούν ελεύθερα εντός της ΕΕ χωρίς την ανάγκη έκδοσης κάρτας visa και ως εκ τούτου αντιμετωπίζουν λιγότερα θεσμικά εμπόδια στη διαδικασία μετανάστευσης. Η μετανάστευση προς την ΕΕ υπηκόων τρίτων χωρών , αντίθετα, παραμένει σε μεγάλο βαθμό συνδεδεμένη με μέτρα περιορισμού της πρόσβασης και ελέγχου των συνόρων. Η παγκόσμια οικονομική κρίση που ξεκίνησε το 2008 έφερε, τουλάχιστον προσωρινά, ένα τέλος στην ταχεία οικονομική ανάπτυξη, την επέκταση της ΕΕ και την υψηλή μετανάστευση. Η κρίση φαίνεται να επηρέασε κυρίως την ενδοευρωπαϊκή μετανάστευση με τη μείωση της κυκλοφορίας εντός της Ε.Ε και με τις περιφερειακές χώρες που επλήγησαν περισσότερο από την κρίση - ιδίως την Ελλάδα, την Ιρλανδία, την Ιταλία, την Πορτογαλία και την Ισπανία - να γίνουν και πάλι χώρες μετανάστευσης.[25]

2.1.2 Μετανάστες, αιτούντες άσυλο και πρόσφυγες

Οι όροι «πρόσφυγας», «αιτών άσυλο» και «μετανάστης» χρησιμοποιούνται για να περιγράψουν άτομα που έχουν εγκαταλείψει τις χώρες τους και έχουν περάσει τα σύνορα μιας άλλης χώρας. Ειδικά οι όροι «πρόσφυγας» και «μετανάστης» συχνά συγχέονται. Ωστόσο, είναι σημαντικό να γίνει διάκριση μεταξύ τους, καθώς υπάρχει νομική διαφορά. [61]

2.1.2.1 Πρόσφυγες

Οι πρόσφυγες είναι άτομα που έχουν εγκαταλείψει τη χώρα τους επειδή σε αυτή κινδυνεύουν από σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων και διώξεις. Οι κίνδυνοι για την ασφάλεια και τη ζωή τους είναι τόσο μεγάλοι που τους οδηγούν στο να φύγουν και να αναζητήσουν την ασφάλεια εκτός της χώρας τους, επειδή η δική τους κυβέρνηση δεν μπορεί να τους προστατεύσει από αυτούς τους κινδύνους. Οι πρόσφυγες έχουν δικαίωμα στη διεθνή προστασία.[1]

2.1.2.2 Αιτούντες άσυλο

Οι αιτούντες άσυλο είναι άτομα που, επίσης, έχουν εγκαταλείψει τη χώρα τους και ζητούν προστασία από διώξεις και σοβαρές παραβιάσεις των ανθρωπίνων δικαιωμάτων σε άλλη χώρα. Ωστόσο, τα άτομα αυτά δεν έχουν αναγνωριστεί ακόμη ως πρόσφυγες και περιμένουν να ληφθεί απόφαση σχετικά με την αίτησή τους για άσυλο. Η αναζήτηση ασύλου είναι ανθρώπινο δικαίωμα. Αυτό σημαίνει ότι πρέπει να επιτρέπεται σε όλους να εισέρχονται σε άλλη χώρα με σκοπό να ζητήσουν άσυλο.[59]

Άτομα που διαφεύγουν από πόλεμο ή διώξεις πρέπει να υποβάλουν αίτηση ασύλου στην πρώτη χώρα της ΕΕ στην οποία βρίσκονται. Με την υποβολή αυτή σημαίνει ότι γίνονται αιτούντες άσυλο. Λαμβάνουν καθεστώς πρόσφυγα ή διαφορετική μορφή διεθνούς προστασίας μόνο όταν ληφθεί θετική απόφαση από τις εθνικές αρχές. Αυτοί είναι άνθρωποι για τους οποίους η άρνηση ασύλου έχει δυνητικά θανατηφόρες συνέπειες. Οι πρόσφυγες ορίζονται και προστατεύονται στο διεθνές δίκαιο. Υπάρχει μια θεμελιώδης διαφορά μεταξύ των αιτούντων άσυλο που έχουν υποβάλει επίσημα αίτηση ασύλου, αλλά των οποίων η αίτηση εκκρεμεί και των προσφύγων. Στην πραγματικότητα, σύμφωνα με τη Σύμβαση για τους Πρόσφυγες του 1951, οι πρόσφυγες με αναγνωρισμένο καθεστώς προστασίας δεν

[1] https://www.amnesty.org/en/what-we-do/refugees-asylum-seekers-and-migrants/

πρέπει να απελαθούν ή να επιστρέψουν σε καταστάσεις όπου η ζωή και η ελευθερία τους θα απειλούνταν. [1]

2.1.2.3 Μετανάστες

Δεν υπάρχει διεθνώς αποδεκτός νομικός ορισμός του μετανάστη. Οι περισσότεροι οργανισμοί θεωρούν τους μετανάστες ως άτομα που μένουν εκτός της χώρας καταγωγής τους, αλλά δεν είναι αιτούντες άσυλο ή πρόσφυγες. Ένας σημαντικός αριθμός μεταναστών εγκαταλείπουν τη χώρα τους με σκοπό να σπουδάσουν ή να εργαστούν σε άλλη χώρα. Υπάρχει, βέβαια, και ένας αριθμός που αποφασίζουν να φύγουν λόγω φτώχειας, πολιτικών αναταραχών ή φυσικών καταστροφών. Με άλλα λόγια, οι μετανάστες εγκαταλείπουν τις χώρες τους στις περισσότερες περιπτώσεις λόγω της οικονομικής αστάθειας, πράγμα που σημαίνει ότι εάν επιλέξουν να επιστρέψουν στην πατρίδα τους, θα συνεχίσουν να λαμβάνουν την προστασία της κυβέρνησής τους.[61]

Πολλοί άνθρωποι δεν ταιριάζουν με τον νομικό ορισμό του πρόσφυγα. Παρόλα αυτά, θα μπορούσαν να διατρέχουν κίνδυνο εάν επέστρεφαν στη χώρα καταγωγής τους. Επίσης, είναι προφανές από τα παραπάνω ότι η διάκριση μεταξύ μεταναστών και προσφύγων είναι ζωτικής σημασίας για μεμονωμένες κυβερνήσεις και για την ΕΕ γενικότερα. Ο λόγος είναι ότι οι χώρες αντιμετωπίζουν τους μετανάστες βάσει των δικών τους νόμων και διαδικασιών μετανάστευσης, ενώ οι πρόσφυγες αντιμετωπίζονται μέσω νόμων που είναι ορίζονται τόσο στην εθνική όσο και στη διεθνή νομοθεσία. [2]

2.1.3 Παρούσα κατάσταση στην ΕΕ

2.1.3.1 Περίοδος 2012-2020

Το πιο σημαντικό γεγονός αυτής της περιόδου για την ΕΕ ήταν η μεταναστευτική κρίση (γνωστή και ως προσφυγική κρίση) των ετών 2015-2016. Ήταν μια περίοδος που χαρακτηρίστηκε από την άφιξη στην Ευρωπαϊκή Ένωση πολύ υψηλού αριθμού ατόμων που φθάνουν από όλη τη Μεσόγειο Θάλασσα ή από την ενδοχώρα μέσω της Νοτιοανατολικής Ευρώπης [13]. Σύμφωνα με την Ύπατη Αρμοστεία των Ηνωμένων Εθνών για τους Πρόσφυγες, τον Ιανουάριο του 2015 έως το Μάρτιο του 2016, οι τρεις κορυφαίες εθνικότητες μεταξύ ενός εκατομμυρίου προσφύγων που έφτασαν από τη Μεσόγειο Θάλασσα ήταν Σύριοι (46,7%), Αφγανοί (20,9%) και Ιρακινοί (9,4%) [16]. Πολλοί πρόσφυγες που έφτασαν στην Ιταλία και την Ελλάδα προέρχονταν από χώρες στις οποίες ήταν σε εξέλιξη ένοπλες συγκρούσεις με κύρια αυτή του εμφυλίου πολέμου της Συρίας (2011-σήμερα). Επιπλέον προσφυγικές ροές προήλθαν λόγω του πολέμου στο Αφγανιστάν που είχε ξεκινήσει το 2001 και της σύγκρουσης στο Ιράκ που ξεκίνησε το 2003. Οι ένοπλες αυτές συγκρούσεις συνεχίζουν μέχρι σήμερα, οπότε και συνεχίζουν οι ροές αιτούντων ασύλου από αυτές τις περιοχές προς την ΕΕ.[3]

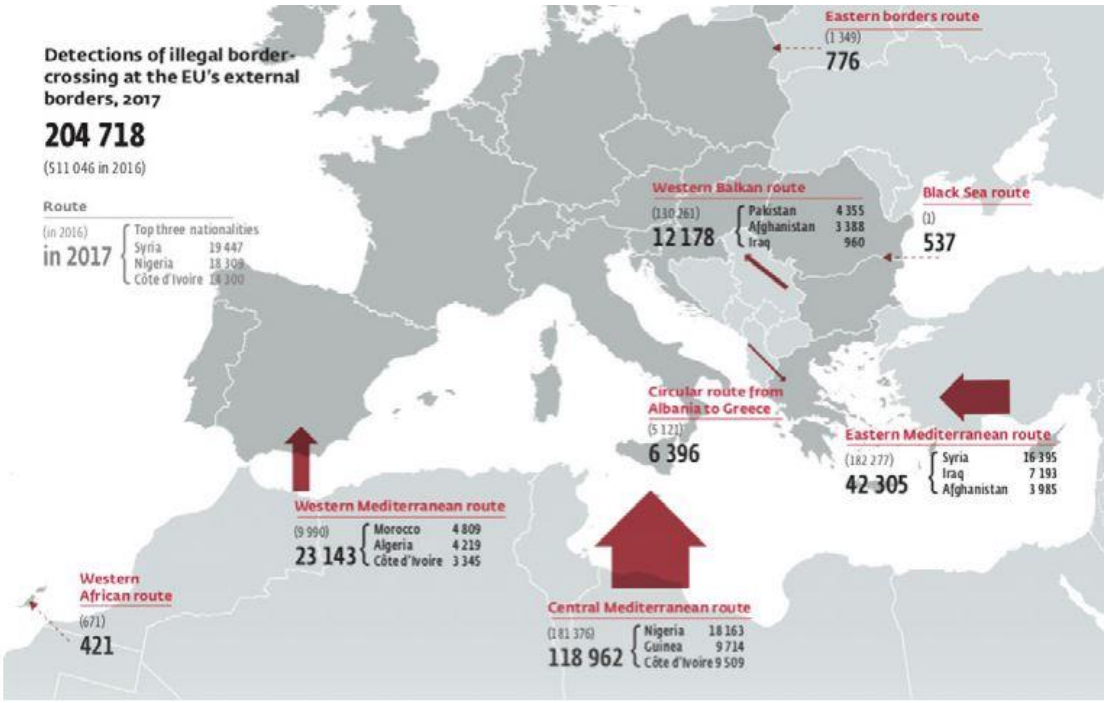
Η εισροή υπηκόων τρίτων χωρών, οι οποίοι κάνουν αίτηση ασύλου στην ΕΕ έχει πάρει πολύ μεγάλες διαστάσεις τα τελευταία έτη (με σημαντική αύξηση τα έτη 2015-2016). Παρατηρήθηκε κατακόρυφη μείωση του αριθμού αυτού το 2016, εξαιτίας κυρίως της σύμπραξης της Ευρωπαϊκής Ένωσης με την Τουρκία, η οποία οδήγησε στον περιορισμό των προσφυγικών κυμάτων διαμέσου των οδών της Ανατολικής Μεσογείου και των Δυτικών Βαλκανίων. Παρόλα αυτά, ακόμη και σήμερα οι χώρες μέλη της ΕΕ στη Νότια Ευρώπη

[1] http://www.europarl.europa.eu/news/en/headlines/society/20170629STO78630/eu-migrant-crisis-facts-and-figures

[2] https://www.amnesty.org/en/what-we-do/refugees-asylum-seekers-and-migrants/

[3] https://en.wikipedia.org/wiki/European_migrant_crisis

αποτελούν τις πιο συχνές πύλες εισόδου για μετανάστες και πρόσφυγες. Η πιο συνήθης τακτική των πληθυσμών αυτών είναι η διέλευσή τους από τα Βαλκάνια και μετέπειτα η προσπάθεια για εγκατάσταση σε αναπτυγμένα κράτη (π.χ. Γερμανία, Αυστρία, Γαλλία, Σουηδία). Οι πιο βασικοί δρόμοι διέλευσης των συνόρων προς την ΕΕ για τους πληθυσμούς αυτούς είναι ο δρόμος της Ανατολικής Μεσογείου, των Δυτικών Βαλκανίων και αυτός της Κεντρικής Μεσογείου, όπως φαίνεται και στην παρακάτω εικόνα. Το δρόμο της Ανατολικής Μεσογείου με πορεία από την Τουρκία προς την Ελλάδα, καθώς και το δρόμο των Βαλκανίων έχουν χρησιμοποιήσει πολλές φορές (με ιδιαίτερη ένταση το 2015) αιτούντες άσυλο από τη Συρία, το Αφγανιστάν και το Ιράκ. Αιτούντες άσυλο προερχόμενοι από τη δυτική Αφρική χρησιμοποιούν πολύ συχνά ως πύλη εισόδου στην ΕΕ το δρόμο της κεντρικής Μεσογείου από τη Λιβύη προς τη Μάλτα και την Ιταλία.[1]



Εικόνα 14 Εντοπισμός παράνομων παραβιάσεων στα εξωτερικά σύνορα της ΕΕ, 2017 [63]

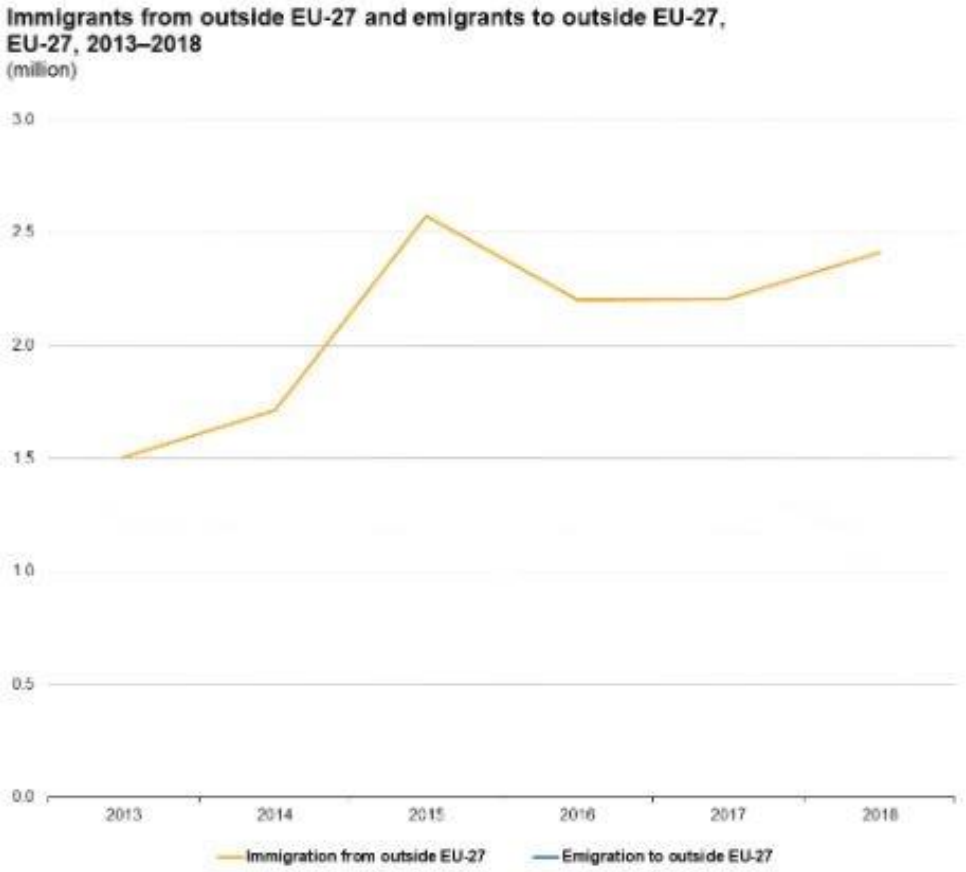
2.1.3.2 Στατιστικά στοιχεία σχετικά με τις ροές μεταναστών και προσφύγων (2018-2020)

2.1.3.2.1 Μετανάστες

Σύμφωνα με στατιστικές εκτιμήσεις, περίπου 2,4 εκατομμύρια μετανάστες ήλθαν στην ΕΕ-27 από χώρες εκτός ΕΕ-27 το 2018 (immigrants). Σύμφωνα με στατιστικές 21,8 εκατομμύρια άτομα (4,9%) από τα 446,8 εκατομμύρια άτομα που ζούσαν στην ΕΕ-27 την 1η Ιανουαρίου 2019 ήταν πολίτες εκτός ΕΕ-27. Επιπλέον, το ίδιο έτος 1,4 εκατομμύρια άτομα που κατοικούσαν προηγουμένως σε ένα κράτος μέλος ΕΕ-27 μετανάστευσαν σε άλλο κράτος μέλος (emigrants). Τα δεδομένα αυτά φαίνονται και στην Εικόνα 15. Το διάγραμμα απεικονίζει τη μεταναστευτική κρίση στην Ευρώπη των ετών 2015-2016 καθώς και την αυξημένη ροή μεταναστών από χώρες εκτός ΕΕ-27 από το 2017 και ύστερα. Τα κράτη μέλη

[1]https://www.emn.ee/en/news/migration-policy-situation-during-the-change-of-leadership-in-the-european-union/

της ΕΕ-27 χορήγησαν υπηκοότητα σε 672 χιλιάδες άτομα το 2018.[64]



Εικόνα 15: Αριθμός (σε εκατομμύρια) μεταναστών-πολιτών εκτός της ΕΕ προς την ΕΕ τα έτη 2013-2018.[1]

Οι χώρες προορισμού των μεταναστών που εισέρχονται στην ΕΕ από χώρες εκτός της ΕΕ (immigrants) είναι κυρίως η Γερμανία, η Ισπανία και η Γαλλία. Για παράδειγμα, το 2018 η Γερμανία ανέφερε το μεγαλύτερο συνολικό αριθμό μεταναστών εκτός της ΕΕ (893,9 χιλιάδες), ακολουθούμενη από την Ισπανία (643,7 χιλιάδες), τη Γαλλία (386,9 χιλιάδες) και την Ιταλία (332,3 χιλιάδες).[64]

Οι χώρες προορισμού των μεταναστών που προέρχονται από κράτη μέλη της ΕΕ (immigrants) είναι επίσης κυρίως η Γερμανία και η Γαλλία. Το 2018 ο υψηλότερος αριθμός σημειώθηκε στη Γερμανία (540,4 χιλιάδες) και ακολούθησε η Γαλλία (341,4 χιλιάδες), η Ισπανία (309,5 χιλιάδες), η Ρουμανία (231,7 χιλιάδες) και η Πολωνία (189,8 χιλιάδες). [64]

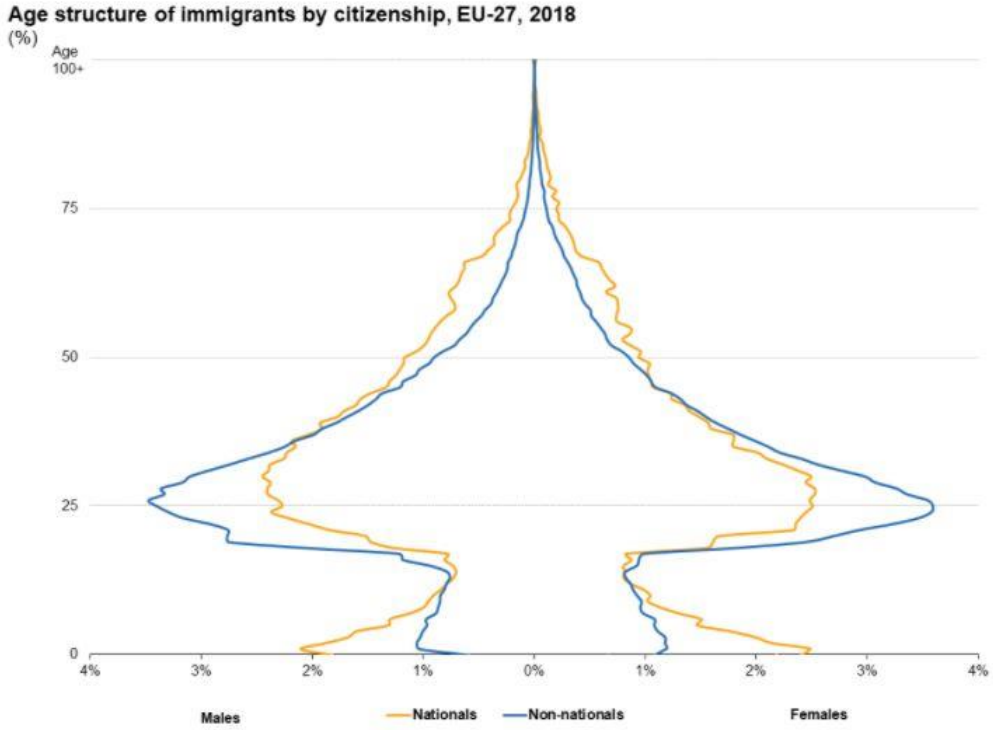
Συνολικά 22 από τα κράτη μέλη της ΕΕ-27 ανέφεραν, το 2018, ότι δέχθηκαν περισσότερους μετανάστες από χώρες εκτός της ΕΕ σε σχέση με αυτούς που προέρχονταν από χώρες μέλη της ΕΕ. Αντίθετα, σε κράτη όπως η Βουλγαρία, η Κροατία, η Λετονία, η Λιθουανία και η Ρουμανία οι μετανάστες από χώρες εντός της ΕΕ ήταν πολυπληθέστεροι.[64]

Σε σχέση με τον πληθυσμό των κατοίκων, η Μάλτα κατέγραψε τα υψηλότερα ποσοστά μετανάστευσης το 2018 (55 μετανάστες ανά 1.000 άτομα).[64]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics

Σε απόλυτους όρους, ο μεγαλύτερος αριθμός μη υπηκόων που ζουν στα κράτη μέλη της ΕΕ-27 την 1η Ιανουαρίου 2019 βρέθηκε στη Γερμανία (10,1 εκατομμύρια άτομα), στην Ιταλία (5,3 εκατομμύρια), στη Γαλλία (4,9 εκατομμύρια) και στην Ισπανία (4,8 εκατομμύρια) . Οι μη υπήκοοι σε αυτά τα τέσσερα κράτη μέλη αντιπροσώπευαν συλλογικά το 71% του συνολικού αριθμού των μη υπηκόων που ζουν σε όλα τα κράτη μέλη της ΕΕ-27, ενώ τα ίδια τέσσερα κράτη μέλη είχαν μερίδιο 58% του πληθυσμού της ΕΕ-27.[65]

Οι μετανάστες στα κράτη μέλη της ΕΕ-27 το 2018 ήταν, κατά μέσο όρο, πολύ νεότεροι από το συνολικό πληθυσμό που κατοικούσε ήδη, στη χώρα προορισμού τους. Αυτό φαίνεται και στην Εικόνα 16. Την 1η Ιανουαρίου 2019, η μέση ηλικία του συνολικού πληθυσμού της ΕΕ-27 ανήλθε σε 43,7 έτη, ενώ ήταν 29,2 έτη για τους μετανάστες στην ΕΕ-27 το 2018.[65]



Εικόνα 16: Ηλικιακή δομή των μεταναστών στην Ε.Ε (2018). Η σχηματική απεικόνιση με μπλε χρώμα αντιπροσωπεύει την ηλικία των μεταναστών που δεν είναι πολίτες της ΕΕ και αυτή με κίτρινο χρώμα την ηλικία των πολιτών της Ε.Ε [1]

Ο αριθμός των ατόμων που απέκτησαν την ιθαγένεια ενός κράτους μέλους της ΕΕ-27 το 2018 ήταν 672,3 χιλιάδες, που αντιστοιχεί σε μείωση 4% σε σχέση με το 2017. Η Γερμανία είχε τον υψηλότερο αριθμό ατόμων που απέκτησαν ιθαγένεια το 2018 (116,8 χιλιάδες ή 17% του συνόλου της ΕΕ-27). Τα επόμενα υψηλότερα επίπεδα απόκτησης ιθαγένειας ήταν στην Ιταλία (112,5 χιλιάδες), στη Γαλλία (110,0 χιλιάδες), στην Ισπανία (90,8 χιλιάδες) και στη Σουηδία (63,8 χιλιάδες). Σε απόλυτους όρους, οι υψηλότερες μειώσεις σε σύγκριση με το 2017 παρατηρήθηκαν στην Ιταλία και στην Ελλάδα.[65]

Οι πολίτες χωρών εκτός της ΕΕ αντιπροσώπευαν το 84% όλων των ατόμων που απέκτησαν την ιθαγένεια ενός κράτους μέλους της ΕΕ-27 το 2018. Αυτοί οι νέοι πολίτες της ΕΕ-27 προέρχονταν κυρίως από την Αφρική (28% του συνολικού αριθμού των υπηκόων που αποκτήθηκαν), την Ευρώπη εκτός της ΕΕ-27 (25%), την Ασία (16%), καθώς και τη Βόρεια και

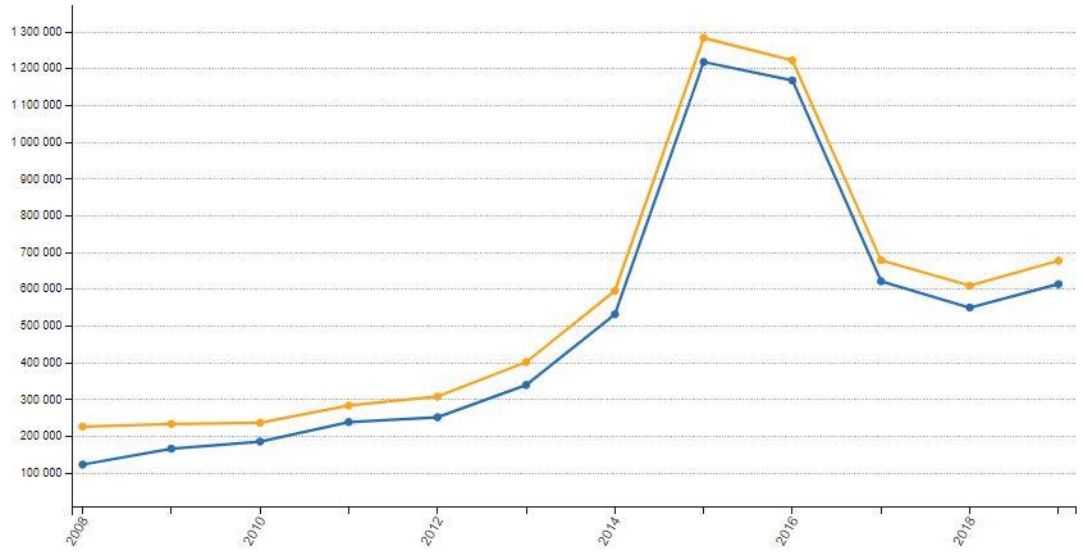
[1]https://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics

Νότια Αμερική (14%). Οι πολίτες κρατών μελών της ΕΕ-27 που απέκτησαν την ιθαγένεια άλλου κράτους μέλους της ΕΕ-27 αποτέλεσαν το 13% του συνόλου.[1]

Όπως και τα προηγούμενα χρόνια, η μεγαλύτερη ομάδα νέων πολιτών στα κράτη μέλη της ΕΕ-27 το 2018 ήταν πολίτες του Μαρόκου (67,2 χιλιάδες, που αντιστοιχούν στο 10% όλων των χορηγούμενων υπηκοότητας), ακολουθούμενη από πολίτες της Αλβανίας (47,4 χιλιάδες ή 7,1%), Τούρκοι (28,4 χιλιάδες ή 4,2%) και Βραζιλιάνοι (23,1 χιλιάδες ή 3,4%). Το μεγαλύτερο μέρος των Μαροκινών απέκτησαν τη νέα τους υπηκοότητα στην Ισπανία (38%), στην Ιταλία (23%) ή στη Γαλλία (23%), ενώ η πλειονότητα των Αλβανών έλαβε ελληνική ιθαγένεια (51%) ή ιταλική ιθαγένεια (46%). Η πλειοψηφία των Τούρκων (59%) έλαβε γερμανική ιθαγένεια και περίπου οι μισοί Βραζιλιάνοι έλαβαν ιταλική ιθαγένεια (46%).[66]

2.1.3.2.2 Αιτούντες άσυλο – Πρόσφυγες

Μεταξύ των ετών 2008 και 2012 σημειώθηκε σταδιακή αύξηση του αριθμού των αιτήσεων ασύλου προς την ΕΕ-27. Στη συνέχεια, ο αριθμός των αιτούντων άσυλο αυξήθηκε με ταχύτερο ρυθμό, με 400.500 αιτήσεις το 2013, 594.200 το 2014 και περίπου 1,3 εκατομμύρια το 2015. Ο αριθμός των αιτήσεων ασύλου ακολούθησε πτωτική πορεία τα έτη 2016,2017,2018. Ωστόσο, το 2019 παρουσίασε και πάλι αύξηση κατά 11,2% σε σύγκριση με το 2018. Τα δεδομένα αυτά φαίνονται και στο παρακάτω διάγραμμα.[67]



Εικόνα 17: Αριθμός των αιτήσεων ασύλου από πολίτες εκτός της ΕΕ προς χώρες της ΕΕ (2008-2019). Η διαγραμματική απεικόνιση με κίτρινο χρώμα αντιστοιχεί στο συνολικό αριθμό αιτήσεων ασύλου και αυτή με μπλε χρώμα αντιστοιχεί στους αιτούντες άσυλο για πρώτη φορά. [67]

Οι πρώτης φοράς αιτούντες άσυλο είναι πρόσωπα που υποβάλουν αίτηση ασύλου για πρώτη φορά σε ένα δεδομένο κράτος μέλος της ΕΕ. Οι αιτούντες άσυλο πρώτης φοράς για το έτος 2019 ήταν 612.700. Ο αριθμός των ατόμων που υπέβαλαν περισσότερες από μία αιτήσεις ασύλου στην ΕΕ-27 το 2019 ήταν 63.600, αντιπροσωπεύοντας το 9,4% του συνολικού αριθμού των αιτούντων. Το συντριπτικό ποσοστό των αιτήσεων ασύλου για το 2019 (90,6%) ήταν αιτήσεις πρώτης φοράς. Μάλιστα, σε σχέση με το 2018 οι αιτήσεις ασύλου πρώτης φοράς αυξήθηκαν και οι κύριες συνεισφορές σε αυτή την αύξηση ήταν ο υψηλότερος αριθμός αιτούντων από τη Βενεζουέλα, την Κολομβία και το Αφγανιστάν. [2]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Migration_and_migrant_population_statistics
[2] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

Χώρες προέλευσης των αιτούντων άσυλο

Σχετικά με την ιθαγένεια των αιτούντων για πρώτη φορά άσυλο, από το 2013, η Συρία παραμένει η κύρια χώρα προέλευσης των αιτούντων άσυλο στην ΕΕ-27. Επίσης, πολύ μεγάλο ποσοστό προέρχεται από το Αφγανιστάν και τη Βενεζουέλα.[1]

Για παράδειγμα, το μεγαλύτερο ποσοστό αιτούντων για πρώτη φορά άσυλο στην Ελλάδα προέρχεται από τέσσερα κράτη, τη Συρία, το Ιράκ, το Αφγανιστάν και το Πακιστάν. Αντίθετα, στην Ιταλία η εικόνα είναι διαφορετική, καθώς οι περισσότεροι αιτούντες άσυλο προέρχονται από τη Νιγηρία, το Μπαγκλαντές, το Πακιστάν και κάποια κράτη της δυτικής Αφρικής. Οι αιτούντες άσυλο από τη Συρία, το Αφγανιστάν και το Ιράκ καταλαμβάνουν πολύ μικρότερο ποσοστό. [2]

Στην Εικόνα 17*Εικόνα 18* φαίνονται οι πέντε μεγαλύτερες ομάδες ιθαγένειας αιτούντων άσυλο πρώτης φοράς σε καθένα από τα κράτη μέλη της ΕΕ-27, το Ηνωμένο Βασίλειο και τις χώρες της Ευρωπαϊκής Ζώνης Ελεύθερων Συναλλαγών, για το 2019. Οι Σύριοι αντιπροσωπεύουν το μεγαλύτερο αριθμό αιτούντων σε επτά από τα 27 κράτη μέλη της ΕΕ, συμπεριλαμβανομένων 39.300 αιτούντων στη Γερμανία. Περίπου 40.300 κάτοικοι Βενεζουέλας (ο υψηλότερος αριθμός αιτούντων από μία χώρα σε ένα από τα κράτη μέλη της ΕΕ-27 το 2019) και 28.900 Κολομβιανοί υπέβαλαν αίτηση προστασίας στην Ισπανία, ενώ οι Αφγανοί αντιπροσώπευαν 23.700 αιτούντες στην Ελλάδα. Οι επόμενοι υψηλοί αριθμοί αιτούντων μεμονωμένης ιθαγένειας το 2019 παρατηρήθηκαν επίσης στη Γερμανία (13.700 αιτούντες από το Ιράκ και 10.800 από την Τουρκία), την Ελλάδα (10 800 αιτούντες από τη Συρία) και τη Γαλλία (10.000 αιτούντες από το Αφγανιστάν). [68]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

[2]https://www.espon.eu/sites/default/files/attachments/espon_asylum-flows-response-policies-greece-online-gr_0.pdf

Belgium	
Syria	2 730
Palestine	2 320
Afghanistan	2 245
El Salvador	1 365
Eritrea	1 155
Other	13 290

Bulgaria	
Afghanistan	985
Syria	480
Iraq	280
Pakistan	90
Iran	80
Other	155

Czechia	
Armenia	330
Ukraine	215
Georgia	190
Vietnam	120
Kazakhstan	95
Other	625

Denmark	
Syria	490
Eritrea	480
Stateless (*)	200
Somalia	160
Morocco	155
Other	1 115

Germany	
Syria	39 270
Iraq	13 740
Turkey	10 785
Afghanistan	9 520
Nigeria	9 070
Other	60 060

Estonia	
Russia	30
Turkey	20
Ukraine	5
Syria	5
Afghanistan	5
Other	30

Ireland	
Albania	970
Georgia	635
Zimbabwe	445
Nigeria	385
South Africa	315
Other	1 995

Greece	
Afghanistan	23 665
Syria	10 750
Pakistan	6 420
Iraq	5 590
Turkey	3 795
Other	24 690

Spain	
Venezuela	40 305
Colombia	28 880
Honduras	6 730
Nicaragua	5 840
El Salvador	4 715
Other	28 705

France	
Afghanistan	9 995
Albania	8 010
Georgia	7 735
Guinea	6 600
Bangladesh	5 810
Other	81 760

Croatia	
Iraq	300
Afghanistan	240
Iran	165
Syria	135
Algeria	95
Other	330

Italy	
Pakistan	7 305
El Salvador	2 520
Peru	2 445
Ukraine	1 775
Albania	1 545
Other	19 415

Cyprus	
Syria	2 550
Georgia	1 490
India	1 425
Bangladesh	1 215
Cameroon	1 175
Other	4 840

Latvia	
Azerbaijan	35
Russia	25
India	15
Ukraine	10
Georgia	10
Other	80

Lithuania	
Russia	275
Tajikistan	205
Syria	15
Belarus	15
Turkey	15
Other	95

Luxembourg	
Eritrea	565
Syria	375
Afghanistan	170
Iraq	130
Algeria	75
Other	885

Hungary	
Afghanistan	185
Iraq	155
Pakistan	25
Iran	20
Syria	20
Other	55

Malta	
Sudan	1 045
Syria	430
Libya	255
Somalia	225
Nigeria	220
Other	1 830

Netherlands	
Syria	3 675
Nigeria	2 105
Iran	1 535
Turkey	1 250
Algeria	1 210
Other	12 710

Austria	
Syria	2 660
Afghanistan	2 515
Iran	655
Somalia	595
Iraq	590
Other	3 755

Poland	
Russia	1 770
Ukraine	215
Turkey	115
Tajikistan	80
Afghanistan	55
Other	525

Portugal	
Angola	305
Gambia, The	175
Guinea-Bissau	155
Guinea	120
Venezuela	95
Other	885

Romania	
Iraq	620
Syria	450
Afghanistan	190
Algeria	130
Somalia	120
Other	940

Slovenia	
Algeria	1 010
Morocco	720
Pakistan	520
Afghanistan	415
Bangladesh	175
Other	770

Slovakia	
Afghanistan	85
Iran	45
Armenia	15
Bangladesh	15
Ukraine	5
Other	50

Finland	
Turkey	360
Russia	285
Iraq	270
Somalia	140
Afghanistan	125
Other	1 260

Sweden	
Syria	5 015
Stateless (*)	1 165
Eritrea	1 155
Iran	985
Uzbekistan	965
Other	13 845

United Kingdom	
Iran	5 455
Albania	3 940
Iraq	3 895
Pakistan	2 565
Afghanistan	2 130
Other	26 270

Iceland	
Venezuela	180
Iraq	135
Nigeria	50
Albania	45
Afghanistan	45
Other	355

Liechtenstein	
Kosovo*	10
Georgia	5
Afghanistan	5
China including Hong Kong	5
Ukraine	5
Other	20

Norway	
Syria	535
Turkey	360
Eritrea	180
Stateless (*)	125
Afghanistan	95
Other	870

Switzerland	
Eritrea	2 500
Afghanistan	1 350
Turkey	1 225
Syria	945
Algeria	780
Other	5 745

Εικόνα 18: Οι πέντε πρώτες ιθαγένειες (εκτός ΕΕ) των αιτούντων άσυλο για πρώτη φορά, 2019.[1]

Χώρες προορισμού των αιτούντων άσυλο

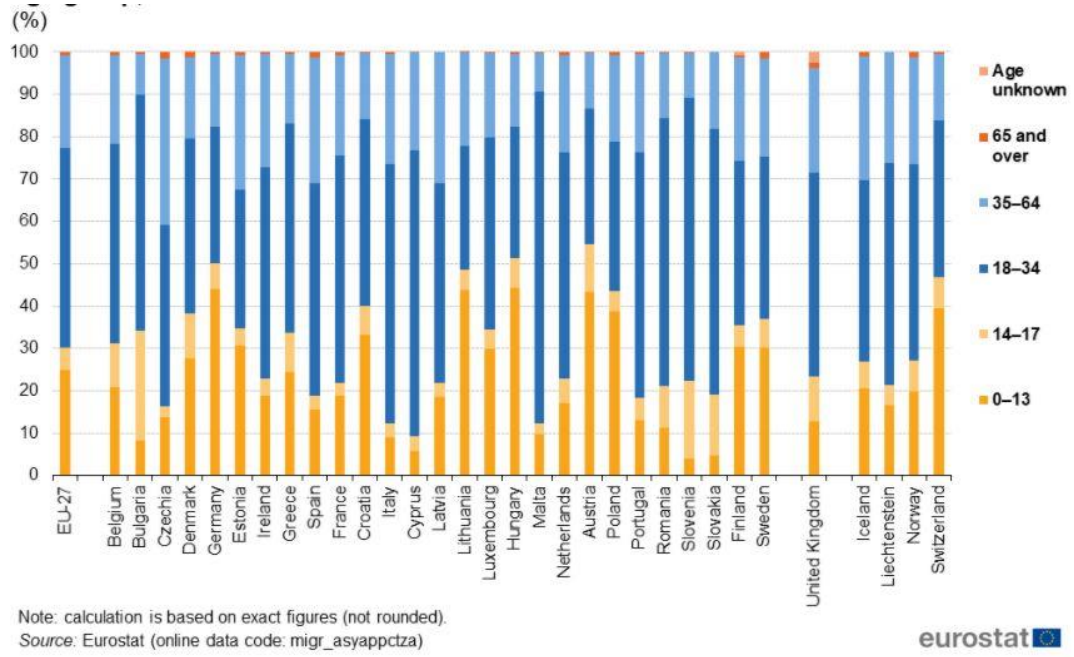
Οι χώρες εισόδου και διέλευσης των αιτούντων άσυλο, όπως η Δημοκρατία της Βόρειας Μακεδονίας έχουν την τάση να δέχονται ένα μεγάλο αριθμό αιτούντων άσυλο. Οι κοινωνικές και οικονομικές συνθήκες που επικρατούν σε κάθε χώρα είναι αυτές που επηρεάζουν τους αιτούντες άσυλο ως προς την επιλογή περιοχής εγκατάστασης , και οι οποίοι συνηθίζουν να εγκαθίστανται σε ανεπτυγμένα αστικά περιβάλλοντα. Για παράδειγμα, περιοχές που είναι ελκυστικές για τους αιτούντες άσυλο είναι η Λομβαρδία και το Λάτσιο στην Ιταλία, η Αττική και το Βόρειο Αιγαίο στην Ελλάδα.[70]

Οι κύριες χώρες προορισμού των αιτούντων άσυλο είναι η Γερμανία, η Γαλλία και η Ισπανία. Με 142.400 αιτούντες εγγεγραμμένους το 2019, η Γερμανία αντιπροσώπευε τη χώρα προορισμού του 23,3% των αιτούντων ασύλου πρώτης φοράς στην ΕΕ-27. Ακολούθησε η Γαλλία (119.900, ή 19,6%), η Ισπανία (115.200, ή 18,8%), μπροστά από την Ελλάδα (74.900, ή 12,2%) και την Ιταλία (35.000, ή 5,7%). Ο αριθμός των υποψηφίων πρώτης φοράς αυξήθηκε περισσότερο σε σχέση με το προηγούμενο έτος στην Ισπανία, την Κύπρο και την Ελλάδα.[70]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

Ηλικία και φύλο των αιτούντων πρώτης φοράς

Περισσότερα από τα τρία τέταρτα (77,3%) των αιτούντων άσυλο (για πρώτη φορά) στην ΕΕ-27 το 2019 ήταν ηλικίας κάτω των 35 ετών. Από αυτούς, λίγο λιγότεροι από τους μισούς (47,0%) ήταν στην ηλικιακή ομάδα 18–34 ετών, ενώ σχεδόν το ένα τρίτο (30,3%) του συνολικού αριθμού των αιτούντων άσυλο πρώτης φοράς ήταν ανήλικοι ηλικίας κάτω των 18 ετών. Αυτή η κατανομή ηλικίας των αιτούντων άσυλο ήταν κοινή σε όλα σχεδόν τα κράτη μέλη της ΕΕ-27, με το μεγαλύτερο ποσοστό των αιτούντων να είναι ηλικίας 18–34. Τα δεδομένα αυτά φαίνονται και στην παρακάτω σχηματική απεικόνιση της κατανομής των ηλικιακών ομάδων.[1]



Εικόνα 19: Κατανομή των αιτούντων άσυλο για πρώτη φορά ανά ηλικιακή ομάδα για το έτος 2019.[71]

Η κατανομή των αιτούντων άσυλο για πρώτη φορά ανά φύλο δείχνει ότι περισσότεροι άνδρες (61,9%) από γυναίκες (38,1%) ζητούσαν άσυλο.[71]

Αιτήσεις ασυνόδευτων ανηλίκων

Ένας ασυνόδευτος ανήλικος είναι ένα άτομο ηλικίας κάτω των 18 ετών που φτάνει στο έδαφος κράτους μέλους της ΕΕ-27 και δεν συνοδεύεται από ενήλικα υπεύθυνο για αυτόν ή ένας ανήλικος που αφήνεται ασυνόδευτος μετά την είσοδό του στην επικράτεια ενός κράτους μέλους. Το 2019 υποβλήθηκαν 14.100 αιτήσεις στην ΕΕ-27 από ασυνόδευτους ανηλίκους. Το 7,1% όλων των ανηλίκων ήταν ασυνόδευτοι. Στην πλειονότητα των κρατών μελών της ΕΕ-27, το 2019 το μερίδιο των ανηλίκων που ήταν ασυνόδευτοι ήταν μικρότερο από 20%. [71]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

Αποφάσεις σχετικά με τις αιτήσεις ασύλου

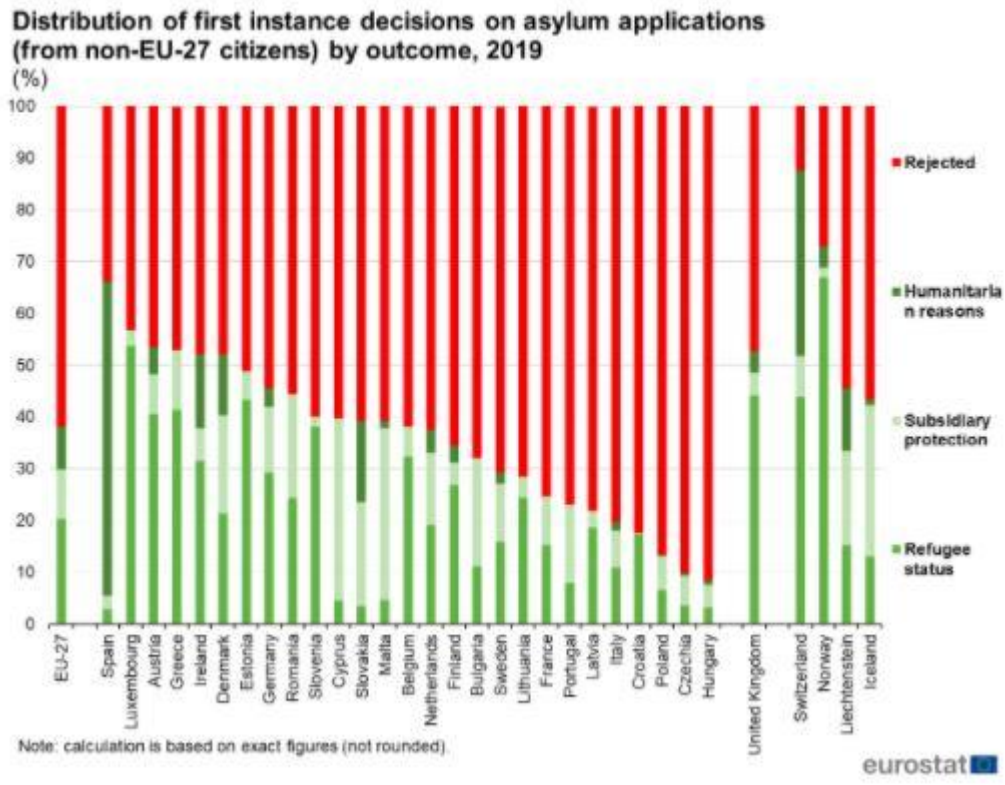
Τα δεδομένα των αποφάσεων σχετικά με τις αιτήσεις ασύλου είναι διαθέσιμα σε δύο επίπεδα. Συγκεκριμένα, αποτελούνται από τις πρωτοβάθμιες αποφάσεις και τις τελικές αποφάσεις που λαμβάνονται κατόπιν προσφυγής ή επανεξέτασης.[1]

Το 2019, 540.800 πρωτοβάθμιες αποφάσεις για αιτήσεις ασύλου ελήφθησαν στα κράτη μέλη της ΕΕ-27 και 296.600 τελικές αποφάσεις μετά από προσφυγή. Οι αποφάσεις που ελήφθησαν πρωτοδίκως οδήγησαν σε 206.000 άτομα σε καθεστώς προστασίας, ενώ άλλα 91.000 έλαβαν καθεστώς προστασίας κατόπιν προσφυγής.[72]

Μέχρι στιγμής, ο μεγαλύτερος αριθμός αποφάσεων (πρώτης και τελικής) εκδόθηκε στη Γερμανία, αντιπροσωπεύοντας το 28,5% των συνολικών πρωτοβάθμιων αποφάσεων και το 44,2% των συνολικών τελικών αποφάσεων στην ΕΕ-27 το 2019. [72]

Πρωτοβάθμιες αποφάσεις για αιτήσεις ασύλου

Στην παρακάτω εικόνα παρέχεται μια ανάλυση του αποτελέσματος των πρωτοβάθμιων αποφάσεων. Αν και το καθεστώς πρόσφυγα και επικουρικής προστασίας ορίζεται από το δίκαιο της ΕΕ, οι ανθρωπιστικοί λόγοι είναι ειδικοί για την εθνική νομοθεσία και δεν ισχύουν σε ορισμένα από τα κράτη μέλη της ΕΕ.[72]



Εικόνα 20: Κατανομή των αποφάσεων σχετικά με τις πρωτοβάθμιες αιτήσεις ασύλου, 2019 [72]

Το 2019, το 38,1% των πρωτοβάθμιων αποφάσεων ασύλου της ΕΕ-27 οδήγησε σε θετικά αποτελέσματα, δηλαδή σε επιχορηγήσεις πρόσφυγα ή επικουρική προστασία, ή άδεια παραμονής για ανθρωπιστικούς λόγους. Από τις θετικές αποφάσεις, περίπου το 52,9% στην

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

ΕΕ-27 το 2019 είχε ως αποτέλεσμα τη χορήγηση καθεστώτος πρόσφυγα. Δηλαδή, από τις συνολικές αιτήσεις περίπου το 20,1% καταλήγει σε χορήγηση καθεστώτος πρόσφυγα.[1]

Μεταξύ των κρατών μελών της ΕΕ-27, τα υψηλότερα ποσοστά θετικών πρωτοβάθμιων αποφάσεων από το συνολικό αριθμό πρωτοβάθμιων αποφάσεων το 2019 καταγράφηκαν στην Ισπανία (66,2%), ακολουθούμενη από το Λουξεμβούργο (56,7%), την Αυστρία (53,5%), την Ελλάδα (53,1%),την Ιρλανδία (52,1%) και τη Δανία (52,0%). Αντίθετα, η Ιταλία, η Κροατία, η Πολωνία, η Τσεχία και η Ουγγαρία κατέγραψαν η καθεμιά ένα μερίδιο θετικών πρωτοβάθμιων αποφάσεων μεταξύ 19,7% (Ιταλία) και 8,5% (Ουγγαρία). Το μερίδιο των θετικών τελικών αποφάσεων βάσει έφεσης ή επανεξέτασης ήταν χαμηλότερο στην ΕΕ-27 το 2019 από ό,τι για τις πρωτοβάθμιες αποφάσεις.[73]

2.1.3.3 Σχέδιο της ΕΕ για την αντιμετώπιση του μεταναστευτικού

Διαχείριση μεταναστευτικών ροών

Η ΕΕ έχει υιοθετήσει διάφορα σύνολα κανόνων και πλαισίων για τη διαχείριση των νόμιμων μεταναστευτικών ροών όσον αφορά τους αιτούντες ασύλου, τους εργαζόμενους με υψηλή εξειδίκευση, τους φοιτητές και ερευνητές, τους εποχιακούς εργαζόμενους, και όσους επιδιώκουν την οικογενειακή επανένωση. Όσον αφορά τις υπόλοιπες μεταναστευτικές ροές έχει υιοθετήσει κοινούς κανόνες για την επεξεργασία των αιτήσεων ασύλου καθώς και συμφωνίες επανεισδοχής για την επιστροφή των παράνομων μεταναστών. [74]

2.1.3.3.1 Νόμιμες μεταναστευτικές ροές

- Επανεγκατάσταση

Η επανεγκατάσταση επιτρέπει στους πρόσφυγες που χρειάζονται προστασία να εισέλθουν από χώρα εκτός της ΕΕ στην ΕΕ νόμιμα και με ασφάλεια χωρίς να χρειάζεται να διακινδυνεύσουν τη ζωή τους κάνοντας επικίνδυνα ταξίδια. [2]

- Μετεγκατάσταση

Η μετεγκατάσταση επιτρέπει στους πρόσφυγες να μετακινηθούν από μία χώρα ασύλου σε ένα άλλο κράτος που έχει συμφωνήσει να τους δεχθεί και τελικά να τους παραχωρήσει μόνιμη εγκατάσταση.[3]

- Εργαζόμενοι με υψηλή εξειδίκευση

Η μπλε κάρτα της ΕΕ εγκρίθηκε το 2009 για να διευκολύνει τη μετάβαση σε εργαζόμενους με υψηλά προσόντα εκτός ΕΕ. Τον Ιούνιο του 2016 η Επιτροπή πρότεινε μια μεταρρύθμιση της οδηγίας για τη μπλε κάρτα για να προσελκύσει περισσότερα από τα ταλέντα που χρειάζεται η ευρωπαϊκή οικονομία. Ο στόχος είναι να αντιμετωπιστούν οι ελλείψεις εργασίας και δεξιοτήτων και να καταστεί η ΕΕ πιο ανταγωνιστική προσελκύοντας εργαζομένους υψηλής ειδίκευσης. Οι νέοι κανόνες ευνόησαν τη δυνατότητα συμμετοχής σε παράλληλες επαγγελματικές δραστηριότητες και ενίσχυσαν την ευελιξία για την επαγγελματική κινητικότητα μεταξύ διαφορετικών κρατών μελών. [74]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics

[2] https://www.consilium.europa.eu/en/policies/migratory-pressures/managing-migration-flows/

[3]https://www.unhcr.org/resettlement.html https://ec.europa.eu/commission/presscorner/detail/el/IP_16_2178

- Φοιτητές και ερευνητές

Το 2016, το Συμβούλιο και το Κοινοβούλιο εξέδωσαν οδηγία που καθορίζει τους όρους εισόδου και διαμονής υπηκόων τρίτων χωρών για σκοπούς: έρευνας, σπουδών, κατάρτισης, εθελοντικής υπηρεσίας, προγραμμάτων ανταλλαγής μαθητών ή εκπαιδευτικών έργων. Ηγέτες της ΕΕ και της Αφρικής συμφώνησαν να προωθήσουν την κινητικότητα φοιτητών, ερευνητών και επιχειρηματιών μεταξύ των δύο ηπείρων. [76]

- Εποχιακοί εργαζόμενοι

Η οικονομία της ΕΕ βασίζεται σε μεγάλο αριθμό εποχιακών εργαζομένων εκτός ΕΕ καθώς αντιμετωπίζει αυξανόμενες ελλείψεις εργατικού δυναμικού. Το Συμβούλιο και το Κοινοβούλιο ενέκριναν την οδηγία για τους εποχιακούς εργαζομένους το 2014. Περιγράφει τις συνθήκες υπό τις οποίες οι υπήκοοι τρίτων χωρών μπορούν να εισέλθουν και να παραμείνουν στην ΕΕ ως εποχικά εργαζόμενοι. Αυτοί οι κανόνες βοηθούν στην εναρμόνιση και απλοποίηση των κανόνων εισδοχής στα κράτη μέλη, στην προστασία των εποχιακών εργαζομένων εκτός ΕΕ από την εκμετάλλευση και τις κακές συνθήκες εργασίας καθώς και στην αντιμετώπιση του προβλήματος των εποχιακών εργαζομένων εκτός ΕΕ που παραμένουν παράνομα στην ΕΕ. [76]

- Ενδοεταιρικές μεταφορές

Οι πολίτες εκτός ΕΕ μπορούν να υποβάλουν αίτηση για ένταξη στην ΕΕ ως διευθυντές, ειδικοί ή εκπαιδευόμενοι υπάλληλοι στα πλαίσια μιας ενδοεπιχειρησιακής μεταφοράς. [76]

- Οικογενειακή επανένωση

Η οικογενειακή επανένωση επιτρέπει σε αυτούς που έχουν συγγενείς, που διαμένουν νόμιμα στην ΕΕ να επανενωθούν με την οικογένειά τους. Η επανένωση βοηθά τους υπηκόους τρίτων χωρών να ενσωματωθούν καλύτερα στην κοινωνία. [76]

2.1.3.3.2 Υπόλοιπες μεταναστευτικές ροές

Κοινό ευρωπαϊκό σύστημα ασύλου

Το κοινό ευρωπαϊκό σύστημα ασύλου (CEAS) καθορίζει τα ελάχιστα κοινά πρότυπα για τη μεταχείριση των αιτούντων άσυλο. Στην πράξη, οι αιτούντες άσυλο δεν αντιμετωπίζονται ομοιόμορφα και τα ποσοστά αναγνώρισης ποικίλλουν μεταξύ των κρατών μελών. Ως αποτέλεσμα αυτού, πολλοί αιτούντες άσυλο μετακινούνται εντός της ΕΕ αναζητώντας την καλύτερη χώρα για να υποβάλουν αίτηση ασύλου. Οι αιτήσεις ασύλου μπορεί να οδηγήσουν σε επιχορηγήσεις πρόσφυγα ή επικουρική προστασία, ή άδεια παραμονής για ανθρωπιστικούς λόγους (οι οποίες ενδεχομένως πραγματοποιούνται μέσω των διαδικασιών επανεγκατάστασης και μετεγκατάστασης), ή σε επιστροφή. Κάποιες φορές, αιτούντες άσυλο φιλοξενούνται σε ειδικές δομές (π.χ. Μόρια). Η κρίση της μετανάστευσης επιδείνωσε αυτό το ζήτημα και τόνισε την ανάγκη για καλύτερη εναρμόνιση των διαδικασιών και των προτύπων ασύλου. [1]

Πολιτική επιστροφής και συμφωνίες επανεισδοχής

Η πολιτική επιστροφής της ΕΕ θέτει κανόνες για την επιστροφή παράνομα διαμενόντων υπηκόων τρίτων χωρών. Η οδηγία υπογραμμίζει επίσης την ανάγκη σύναψης συμφωνιών

[1] https://www.consilium.europa.eu/en/policies/migratory-pressures/managing-migration-flows/

επανεισδοχής με τρίτες χώρες. Αυτές οι συμφωνίες είναι ζωτικής σημασίας για την εφαρμογή της πολιτικής επιστροφής της ΕΕ. Καθορίζουν τους κανόνες για την επιστροφή ατόμων που διαμένουν παράνομα στην ΕΕ στη χώρα καταγωγής τους. Η ΕΕ διαπραγματεύεται και συνάπτει συμφωνίες επανεισδοχής με τρίτες χώρες. Μέχρι στιγμής, η ΕΕ έχει συνάψει 18 συμφωνίες επανεισδοχής .Εκτός από τις συμφωνίες επανεισδοχής, η ΕΕ έχει επίσης συνάψει συμφωνίες επιστροφής με ορισμένες τρίτες χώρες με τον ίδιο στόχο.[1]

2.1.3.4 Διαδικασία αίτησης ασύλου στην Ελλάδα

Το δικαίωμα υποβολής αίτησης διεθνούς προστασίας είναι δικαίωμα κάθε υπηκόου τρίτου κράτους. Πραγματοποιείται πλήρης καταγραφή από τις Αρχές Παραλαβής (όπως η Υπηρεσία Ασύλου). Ένας υπήκοος τρίτης χώρας μπορεί να καταθέσει αίτηση Διεθνούς Προστασίας είτε αυτοπροσώπως είτε ηλεκτρονικά. Επίσης, στους υπηκόους τρίτων χωρών δίνεται η δυνατότητα υποβολής αίτησης και για τα μέλη της οικογένειας τους. Είναι απαραίτητη η προσέλευση και αυτών στην Υπηρεσία Ασύλου.[78]

Σε περίπτωση εισόδου υπηκόου τρίτης χώρας στην Ελλάδα χωρίς νόμιμες διατυπώσεις, είναι υποχρεωτική η μεταφορά σε Κέντρο Υποδοχής και Ταυτοποίησης προκειμένου να πραγματοποιηθούν οι απαραίτητες διαδικασίες υποδοχής και ταυτοποίησης, με τη συμβολή κάποιου κλιμακίου της υπηρεσίας ασύλου στην περιοχή. Είναι υποχρεωτική η παραμονή στις εγκαταστάσεις του κέντρου όσο χρόνο διαρκεί η διαδικασία εξέτασης της αίτησης, με την προϋπόθεση ότι δεν υπάρχει χρονική υπέρβαση 25 ημερών. Η διάρκεια εξέτασης της αίτησης διαρκεί συνήθως από είκοσι ημέρες έως έξι μήνες. [78]

Τα στοιχεία ταυτότητας, η χώρα καταγωγής, το όνομα του πατέρα, μητέρας, συζύγου, τέκνων, βιομετρικά στοιχεία αναγνώρισης, η αναφορά των αιτιών αίτησης διεθνούς προστασίας, η επιθυμητή γλώσσα εξέτασης της αίτησης και η ενδεχόμενη επιθυμία για ορισμό εξουσιοδοτημένου εκπρόσωπου, είναι κάποια από τα στοιχεία που θα πρέπει να συμπεριληφθούν στην καταγραφή της αίτησης. Στην περίπτωση ασυνόδευτου ανηλίκου, μικρότερου των δεκαοκτώ ετών, χωρίς συνοδεία ενηλίκου, θα πρέπει να ενημερωθεί ο αρμόδιος Εισαγγελέας, ο οποίος θα ορίσει έναν επίτροπο για την προάσπιση των συμφερόντων του ανήλικου.[2]

Κατά τη διάρκεια υποβολής της αίτησης διεθνούς προστασίας, πραγματοποιείται φωτογράφηση των αιτούντων και λήψη δακτυλικών αποτυπωμάτων. [78]

Επίσης, ορίζεται μία ημερομηνία στην οποία ο αιτών θα δώσει συνέντευξη σε υπάλληλο της Υπηρεσίας Ασύλου. Οι αιτούντες κατά τη διάρκεια της συνέντευξης ερωτώνται κυρίως για τα στοιχεία που έχουνε δηλώσει στην αίτηση τους, για τον τρόπο εισόδου τους στην Ελλάδα, για τους λόγους που υποβάλλουν την αίτηση και αυτούς για τους οποίους δεν σκοπεύουν να επιστρέψουν στη χώρα τους.[78]

Με το πέρας της συνέντευξης η Υπηρεσία Ασύλου λαμβάνει την απόφαση για τη χορήγηση στον αιτών είτε καθεστώτος πρόσφυγα, είτε δικαίωμα επικουρικής προστασίας, είτε για την απόρριψη της αίτησης. Σε περίπτωση απόρριψης της αίτησης, ακολουθείται διαδικασία απομάκρυνσής από τη χώρα.[78]

Αν κάποιος αιτών, μετά την έκδοση της απόφασης σχετικά με την αίτηση του, αποκτήσει καθεστώς πρόσφυγα από την Ελληνική Δημοκρατία έχει τη δυνατότητα απόκτησης τριετούς άδειας διαμονής. Επίσης, του δίνεται η δυνατότητα απόκτησης ταξιδιωτικού εγγράφου της Ελληνικής Δημοκρατίας, ώστε να μπορεί να επισκέπτεται άλλες χώρες της ΕΕ για διάστημα έως ενενήντα ημέρες. Όσον αφορά τους δικαιούχους επικουρικής προστασίας, αυτοί

[1] https://www.consilium.europa.eu/en/policies/migratory-pressures/managing-migration-flows/

[2] https://migration.gov.gr/gas/diadikasia-asyloy/

αποκτούν άδεια διαμονής για ένα έτος. Υπάρχει η δυνατότητα ανανέωσης για επιπλέον δύο χρόνια, ύστερα από επανεξέταση. Οι πρόσφυγες και όσοι είναι δικαιούχοι επικουρικής προστασίας μπορούν να έχουν πρόσβαση στην αγορά εργασίας, στην κοινωνική πρόνοια, στην ιατρική περίθαλψη και στη μόρφωση όλων των βαθμίδων και σε προγράμματα κατάρτισης. Θα πραγματοποιηθεί μεταβολή του Προσωρινού Αριθμού Ασφάλισης και Υγειονομικής Περίθαλψης Αλλοδαπού (Π.Α.Α.Υ.Π.Α.) σε ΑΜΚΑ. Δίνεται επιπλέον η δυνατότητα αίτησης οικογενειακής επανένωσης με τα μέλη της οικογένειάς τους που είναι στη χώρα καταγωγής τους ή σε άλλη τρίτη χώρα στους αναγνωρισμένους πρόσφυγες.[78]

Οι πρόσφυγες είναι υποχρεωμένοι να παρακολουθούν τα προγράμματα κοινωνικής ένταξης των αρμόδιων υπηρεσιών. Υπάρχει, επίσης, η δυνατότητα υποβολής αίτησης απόκτησης ελληνικής υπηκοότητας, με την προϋπόθεση ότι έχουν συμπληρωθεί για τον υπήκοο είτε τρία συνεχόμενα έτη σε καθεστώς πρόσφυγα, είτε επτά χρόνια σε καθεστώς επικουρικής προστασίας. Θα πρέπει, ακόμη, να ισχύουν οι νομικές προϋποθέσεις για την κοινωνική ένταξη. [78]

Σε περίπτωση απόρριψης της αίτησης ή χορήγησης καθεστώτος επικουρικής προστασίας και ο αιτών κρίνει ότι δικαιούται καθεστώς πρόσφυγα, έχει δικαίωμα άσκησης προσφυγής ενώπιον της Αρχής Προσφυγών. Η προσφυγή αυτή κατατίθεται στο Περιφερειακό Γραφείο Ασύλου ή στο Αυτοτελές Κλιμάκιο Ασύλου, στο οποίο εκδόθηκε η απορριπτική απόφαση. Αφού ο αιτών καταθέσει προσφυγή, του χορηγείται εκ νέου Δελτίο Αιτούντος Διεθνή Προστασία. Η εξέταση της προσφυγής πραγματοποιείται από την Ανεξάρτητη Επιτροπή Προσφυγών. Ο αιτών έχει τη δυνατότητα παραίτησης από την προσφυγή, όσο αυτή βρίσκεται ακόμη σε εκκρεμότητα. Η Ανεξάρτητη Επιτροπή Προσφυγών παίρνει την απόφαση σχετικά με τη χορήγηση είτε καθεστώτος πρόσφυγα, είτε δικαιούχου επικουρικής προστασίας είτε απόρριψης της προσφυγής. Η έκδοση της απόφασης μπορεί να πραγματοποιηθεί σε διάστημα από δεκαπέντε μέρες έως τρεις μήνες.[78]

Εάν απορριφθεί η αίτηση για προσφυγή, τότε ο αιτών κρατείται σε Προαναχωρησιακό Κέντρο Κράτησης μέχρι την ολοκλήρωση της απομάκρυνσής του ή την έκδοση τελεσίδικης θετικής απόφασης για την αίτησή του. Σε περίπτωση απόρριψης της προσφυγής, η Ανεξάρτητη Επιτροπή Προσφυγών προχωρά στην έκδοση απόφασης για την επιστροφή του αιτούντος πίσω στη χώρα του.[1]

2.1.3.5 Πολιτική κατανομής των προσφύγων στα κράτη μέλη της ΕΕ

Μία από τις κύριες προκλήσεις σχετικά με αυτήν την κατάσταση στην Ευρώπη σήμερα σχετίζεται με την κοινωνική ένταξη των εν λόγω ομάδων. Η κοινωνική ένταξη είναι μια διαδικασία που διασφαλίζει ότι όσοι διατρέχουν κίνδυνο φτώχειας και κοινωνικού αποκλεισμού αποκτούν τις απαραίτητες ευκαιρίες και πόρους για να συμμετάσχουν πλήρως στην οικονομική, κοινωνική, πολιτική και πολιτιστική ζωή και να αποκτήσουν ένα βιοτικό επίπεδο που θεωρείται φυσιολογικό στην κοινωνία όπου ζουν. Διασφαλίζει ότι έχουν μεγαλύτερη συμμετοχή στη λήψη αποφάσεων που επηρεάζει τη ζωή τους και την πρόσβαση στα θεμελιώδη δικαιώματά τους.[2] Επιπλέον, η κοινωνική ένταξη καταγράφεται στους 17 Αναπτυξιακούς Στόχους της Χιλιετίας και στην Ατζέντα 2030. [3]

Με σημείο εκκίνησης τη μεταναστευτική και προσφυγική κρίση του 2015 η Ευρώπη, τα τελευταία χρόνια αντιμετωπίζει τη μεγαλύτερη κρίση από οποιαδήποτε προηγούμενη

[1] https://migration.gov.gr/gas/diadikasia-asyloy/

[2] http://ec.europa.eu/employment_social/social_inclusion/docs/final_joint_inclusion_report_2003_en.pdf

[3] http://www.un.org/sustainabledevelopment/sustainable-development-goals/

ευρωπαϊκή κρίση προσφύγων μετά τον Β 'Παγκόσμιο Πόλεμο[1]. Η κατάσταση είναι τόσο επιβαρυμένη, που παρόλο που έχουν ληφθεί αρκετά μέτρα για τη διαχείριση της κρίσης καθώς και για τη βελτίωση του συστήματος ασύλου, σύμφωνα με τη δημοσκόπηση του Ευρωβαρόμετρου του 2017, το 73% των Ευρωπαίων εξακολουθεί να θέλει η ΕΕ να προχωρήσει σε περισσότερες ενέργειες για τη διαχείριση της κατάστασης[2]. Παρόλο που υπάρχει σαφής συναίνεση ότι το πρόβλημα της μετανάστευσης είναι υψίστης σημασίας, υπάρχουν διάφοροι παράγοντες που εμποδίζουν την πραγματική πρόοδο. Πρώτα απ 'όλα, εκτός από την τεράστια εισροή αιτούντων άσυλο από το 2015, πρέπει να αναφερθεί ότι αυτοί οι πληθυσμοί είναι πολύ διαφορετικοί, δηλαδή υπάρχει μεγάλη ετερογένεια. Επίσης, ο αριθμός των ασυνόδευτων παιδιών είναι υψηλότερος από ποτέ. Το μεγαλύτερο μέρος των αιτούντων άσυλο είναι χαμηλής ειδίκευσης (επαγγελματικές δεξιότητες) αλλά έχουν υψηλό κίνητρο, κάτι που είναι θετικό επειδή η ένταξη στην αγορά εργασίας είναι ο πιο σημαντικός παράγοντας που ευνοεί τη μακροπρόθεσμη ένταξη στην κοινωνία [32]. Επιπλέον, η Υπηρεσία Προσφύγων του ΟΗΕ πιστεύει ότι τα παιδιά αποτελούν το 55% του συνολικού πληθυσμού προσφύγων [3].

Σημαντικό πρόβλημα αποτελεί, επίσης, η άνιση κατανομή των προσφύγων μεταξύ των κρατών μελών της ΕΕ. Αυτό βασίζεται σε ένα πρόγραμμα προσωρινής μετεγκατάστασης / επανεγκατάστασης που πρότεινε η Επιτροπή το 2015. Το πρόγραμμα αυτό πρότεινε ότι η μετεγκατάσταση / επανεγκατάσταση υπηκόων τρίτων χωρών ανά χώρα της ΕΕ πρέπει να βασίζεται στα εξής. [4]

1. Στο μέγεθος του πληθυσμού της χώρας της ΕΕ (40%)
2. Στο συνολικό ΑΕΠ (40%)
3. Στο μέσο αριθμό αιτήσεων ασύλου και στον αριθμό επανεγκατεστημένων / μετεγκατεστημένων προσφύγων ανά εκατομμύριο κατοίκους (10%) και
4. Στο ποσοστό ανεργίας (10%)

2.1.3.6 Κριτική ανάλυση του σχεδίου της Ε.Ε

Παρόλο που οι παραπάνω παράμετροι φαίνεται να έχουν νόημα, το τελικό αποτέλεσμα φαίνεται να είναι μη ισορροπημένο βλέποντας πώς η Γερμανία, η Ιταλία και η Γαλλία προβλέπεται να δεχτούν πάνω από το 40% των μετεγκατεστημένων και πάνω από το 35% των επανεγκατεστημένων. Ωστόσο, αυτό φαίνεται να συμβαίνει επειδή υπάρχουν διαφορετικά επίπεδα ετοιμότητας μεταξύ των κρατών μελών της ΕΕ, όπως άνισες υποδομές, οικονομικοί πόροι και εμπειρία στην αντιμετώπιση του συγκεκριμένου ζητήματος. Εντός της ΕΕ, η Ιταλία, η Ελλάδα και η Ουγγαρία βρίσκονται στην πρώτη γραμμή, αλλά οι κύριες χώρες προορισμού είναι η Γερμανία, η Σουηδία και η Αυστρία, σε σχέση με τον πληθυσμό τους. Σε αυτές τις χώρες αντιστοιχεί περισσότερο από το 75% όλων των αιτούντων, ενώ σε ορισμένες χώρες της Ανατολικής Ευρώπης (Σλοβακία, Κροατία, Σλοβενία, Λιθουανία, Εσθονία και Λετονία) αντιστοιχούν λιγότεροι από 100 αιτούντες άσυλο. Κατά συνέπεια, καθίσταται προφανές ότι για την επιτυχή διανομή και ένταξη των προσφύγων μεταξύ των χωρών της ΕΕ, απαιτούνται ριζικές αλλαγές σε ένα πιο βασικό επίπεδο.[5]

[1] http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_eipre&lang=en

[2] http://www.europarl.europa.eu/news/en/headlines/priorities/20150831TST91035/20170505STO73515/migration-crisis-73-of-europeans-wants-eu-to-do-more

[3] http://www.unhcr.org/globaltrends2016/

[4] http://ec.europa.eu/employment_social/social_inclusion/docs/final_joint_inclusion_report_2003_en.pdf

[5] https://www.eesc.europa.eu/resources/docs/common-basic-principles_en.pdf

Σύμφωνα με τα αποτελέσματα των ερευνών σχετικά με την πρόθεση εγκατάστασης των προσφύγων, η πλειονότητα των προσφύγων θα παραμείνει για μεγάλο χρονικό διάστημα στις χώρες υποδοχής και η ένταξη στην αγορά εργασίας αποτελεί την πιο βιώσιμη λύση. Σύμφωνα με τις κοινές βασικές αρχές των χωρών της ΕΕ για την ένταξη των μεταναστών, «η απασχόληση αποτελεί βασικό μέρος της διαδικασίας ένταξης και έχει κεντρική σημασία για τη συνεισφορά των μεταναστών στην κοινωνία υποδοχής». Επιπλέον, η πλήρης ένταξη των προσφύγων μπορεί να συμβάλει στην κάλυψη των δημογραφικών κενών και στην προσφορά εργασίας στα πλαίσια των γηράσκουσων κοινωνιών με ελλείψεις δεξιοτήτων κάποιων χωρών της ΕΕ[86]. Η πλήρης ένταξη των προσφύγων στη χώρα υποδοχής μέσω της παροχής στέγασης, εκπαίδευσης, υγειονομικής περίθαλψης, κατάρτισης και πρόσβασης στην αγορά εργασίας είναι μια πολύ δαπανηρή διαδικασία. Ωστόσο, μια λιγότερο δαπανηρή στρατηγική συνεπάγεται τον κίνδυνο μιας μακροπρόθεσμης αποτυχίας ολοκλήρωσης του σχεδίου ένταξης, το πολιτικό κόστος μιας μαζικής πολιτικής πόλωσης, καθώς και την αύξηση μιας ημι-ενταγμένης μεταναστευτικής υποκατηγορίας μέσα στην κοινωνία. [33]

Το κύριο ζήτημα είναι ότι, σε αντίθεση με τα πρότυπα της ΕΕ για την υποδοχή και την προστασία, η αποτελεσματική ένταξη των προσφύγων δεν βρίσκεται στην πρώτη γραμμή της ευρωπαϊκής μεταναστευτικής πολιτικής. Η πολιτική ένταξης των προσφύγων ενσωματώνεται στις πολιτικές ένταξης των μεταναστών για υπηκόους τρίτων χωρών. Ως εκ τούτου, δεν υπάρχουν κοινά συμφωνημένα πρότυπα και οδηγίες βάσει των οποίων να αξιολογούνται οι πολιτικές ένταξης για τους πρόσφυγες. Οι οδηγίες και οι συστάσεις είναι προσαρμοσμένες για μετανάστες και όχι για πρόσφυγες. Επιπλέον, μόνο λίγες χώρες τηρούν πλήρως τα ελάχιστα πρότυπα υποδοχής προσφύγων. Ακόμη και στις περιπτώσεις που οι χώρες λαμβάνουν μέτρα για τη βελτίωση της κατάστασης (για παράδειγμα, στο Ηνωμένο Βασίλειο οι πρώην πρόσφυγες έχουν εκπαιδευτεί να ενεργούν ως σύμβουλοι για νέους πρόσφυγες), υπάρχει και η έλλειψη εμπειρικής έρευνας για την ένταξη των προσφύγων, καθώς και η έλλειψη συγκριτικών πληροφοριών σχετικά με τις πολιτικές και τις πρακτικές σε όλα τα κράτη μέλη της ΕΕ.[1]

2.1.3.7 Στοιχεία από το νέο σύμφωνο μετανάστευσης και ασύλου (Σεπτέμβριος 2020)

Σύμφωνα με το νέο σύμφωνο, η έλλειψη ολοκλήρωσης των διαδικασιών οφείλεται πολύ συχνά στην απώλεια εντοπισμού κάποιου αιτούντα μεταξύ μιας αρνητικής απόφασης ασύλου και μιας διαδικασίας επιστροφής. Επίσης, όσοι αναγνωρίστηκαν πρόσφατα ως πρόσφυγες συχνά αντιμετωπίζουν υπερβολικές δυσκολίες μεταξύ της εγκατάλειψης του συστήματος υποδοχής των αιτούντων άσυλο και της εισόδου στην οικονομική και κοινωνική ζωή του κράτους μέλους υποδοχής τους. [2]

Προκειμένου να βελτιωθούν οι διαδικασίες, η ΕΕ με το νέο σύμφωνο στοχεύει στη δημιουργία ολοκληρωμένων διαδικασιών ξεκινώντας από τα σύνορα. Αυτές οι διαδικασίες, που περιλαμβάνουν έλεγχο πριν από την είσοδο, διαδικασία ασύλου και, κατά περίπτωση, διαδικασία ταχείας επιστροφής, στοχεύουν στην επιτάχυνση της λήψης αποφάσεων. Σε απλές περιπτώσεις όπου κάποιος δεν έχει δικαίωμα διαμονής, το άτομο μπορεί να επιστραφεί μετά από μια σύντομη διαδικασία. Αυτές οι διαδικασίες συνοδεύονται από ειδική παρακολούθηση και νομικές διασφαλίσεις για να διασφαλιστεί η πλήρης αξιολόγηση κάθε ατόμου. Ο έλεγχος, που θα πραγματοποιείται στα σύνορα, θα περιλαμβάνει

[1] http://europa.eu/rapid/press-release_IP-15-5699_en.htm

[2] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1707#eurodac

αναγνώριση, ελέγχους υγείας και ασφάλειας, δακτυλικά αποτυπώματα και εγγραφή στη βάση δεδομένων Eurodac. [1]

Το Eurodac (European Dactyloscopy) είναι η βάση δεδομένων δακτυλικών αποτυπωμάτων της ΕΕ για τον εντοπισμό αιτούντων άσυλο και ατόμων που διασχίζουν παράτυπα τα σύνορα. Οι αιτούντες άσυλο και οι παράτυποι διασυνοριακοί διαβάτες άνω των 14 ετών δίνουν τα δακτυλικά τους αποτυπώματα σύμφωνα με τη νομοθεσία της ΕΕ. Στη συνέχεια αποστέλλονται ψηφιακά σε μια κεντρική μονάδα της Ευρωπαϊκής Επιτροπής και ελέγχονται αυτόματα έναντι άλλων αποτυπωμάτων στη βάση δεδομένων. Αυτό δίνει τη δυνατότητα στις αρχές να προσδιορίσουν εάν οι αιτούντες άσυλο έχουν ήδη υποβάλει αίτηση ασύλου σε άλλο κράτος μέλος της ΕΕ ή έχουν περάσει παράνομα μέσω άλλου κράτους μέλους της ΕΕ («αρχή της πρώτης επαφής»). Όλα τα κράτη μέλη της ΕΕ συμμετέχουν επί του παρόντος στο πρόγραμμα, καθώς και τρεις επιπλέον ευρωπαϊκές χώρες: Νορβηγία, Ισλανδία και Ελβετία. [2]

Με βάση το σύμφωνο, η οικογενειακή επανένωση θα ενισχυθεί με τη διεύρυνση του ορισμού των μελών της οικογένειας ώστε να περιλαμβάνονται τα αδέλφια και οι οικογένειες που σχηματίζονται σε χώρες διέλευσης. Προτεραιότητα θα δίνεται στη μετεγκατάσταση ασυνόδευτων παιδιών. Σε συγκεκριμένες περιπτώσεις, η ομάδα αλληλεγγύης που δημιουργείται για επιχειρήσεις έρευνας και διάσωσης μπορεί να χρησιμοποιηθεί για μετεγκατάσταση ευάλωτων ατόμων. Επίσης, ένα επιπλέον κριτήριο θα ορίζει ότι αν κάποιος αιτών άσυλο έχει λάβει δίπλωμα από ένα κράτος μέλος τότε αυτό το κράτος μέλος θα είναι υπεύθυνο για την αίτησή του για άσυλο. [89]

Το νέο σύμφωνο έχει ως στόχο, οι αναγνωρισμένοι πρόσφυγες να έχουν ισχυρότερα δικαιώματα για να διευκολυνθεί η ένταξή τους στην ευρωπαϊκή κοινωνία. Θα έχουν ιδίως το δικαίωμα να αποκτήσουν το καθεστώς κατοίκου μακράς διαρκείας στην ΕΕ μετά από 3 χρόνια αντί για 5 μέσω της τροποποίησης της οδηγίας για τους επί μακρόν διαμένοντες, και κατά συνέπεια να μπορούν να ζουν και να εργάζονται σε άλλο κράτος μέλος.[89]

Επιπλέον, η βάση δεδομένων Eurodac θα είναι σε θέση να παρακολουθεί καλύτερα τις κινήσεις των ατόμων που εισήλθαν και παραμένουν παράνομα στην ΕΕ και μετακινούνται από ένα κράτος μέλος σε άλλο και υποδεικνύουν την αλλαγή ευθύνης μεταξύ των κρατών μελών, συμπεριλαμβανομένων των περιπτώσεων μετεγκατάστασης. Οι αλλαγές στη βάση δεδομένων Eurodac περιλαμβάνουν καταμέτρηση μεμονωμένων αιτούντων και όχι αιτήσεων. Αυτό θα βοηθήσει στην εφαρμογή νέων διατάξεων σχετικά με τη μετατόπιση της ευθύνης εντός της ΕΕ, την αποτροπή μη εξουσιοδοτημένων μετακινήσεων σε άλλα κράτη μέλη, τη διευκόλυνση της μετεγκατάστασης και την εξασφάλιση καλύτερης παρακολούθησης των επιστρεφόμενων. [89]

Σχετικά με το για πόσο καιρό είναι υπεύθυνο ένα κράτος μέλος για μια αίτηση ασύλου μετά από παράνομη είσοδο και το ποιες είναι οι συνθήκες με βάσει τις οποίες ένα άλλο κράτος μέλος θα αναλάβει την ευθύνη, εφαρμόζονται κάποια κριτήρια με τη σειρά. Το πιο σημαντικό κριτήριο είναι η διασφάλιση των καλύτερων συμφερόντων όσον αφορά στα παιδιά. Το δεύτερο κριτήριο υποδεικνύει ότι ως υπεύθυνο κράτος μέλος θα ορίζεται εκείνο στο οποίο ένα μέλος της οικογένειας έχει διεθνή προστασία ή εξακολουθεί να είναι αιτών. Σε αντίθετη περίπτωση, υπεύθυνο είναι το κράτος μέλος που εξέδωσε έγγραφο διαμονής ή θεώρηση. Αν δεν ισχύει το προηγούμενο, υπεύθυνο είναι το κράτος μέλος από το οποίο ο αιτών έχει λάβει

[1] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1707#eurodac
[2] https://en.wikipedia.org/wiki/Eurodac

δίπλωμα ή τίτλο σπουδών εκπαιδευτικού ιδρύματος. Μόνον εάν δεν ισχύει κανένα από αυτά τα κριτήρια, το κράτος μέλος παράτυπης εγγραφής είναι υπεύθυνο για την εξέταση της αίτησης. [1]

2.2 Το Blockchain ως λύση στη διαχείριση του μεταναστευτικού

Από τα παραπάνω συμπεραίνουμε ότι προκειμένου να επιτευχθεί ο στόχος της αποτελεσματικής ένταξης των προσφύγων στην ΕΕ, θα πρέπει να λαμβάνονται υπόψη πολλά και διαφορετικά χαρακτηριστικά κάθε υπηκόου τρίτης χώρας. Δεδομένου ότι κάθε μετανάστης έχει διαφορετικές ανάγκες, για να ενσωματωθεί επιτυχώς σε μια ευρωπαϊκή κοινωνία, κάθε μεμονωμένη περίπτωση πρέπει να αντιμετωπίζεται με προσοχή. Σήμερα, τα δεδομένα σχετικά με τους μετανάστες συλλέγονται κυρίως από κυβερνητικούς φορείς και ΜΚΟ. Η κύρια πρόκληση είναι οι τεράστιες ποσότητες δεδομένων που αφορούν τους μετανάστες, οι οποίες είναι και σε μεγάλο βαθμό μη οργανωμένες και κάποιες φορές αμφίβολες. Αυτό οφείλεται και στο γεγονός ότι υπάρχουν πολλά σημεία εισόδου των υπηκόων τρίτων χωρών στην ΕΕ (π.χ. μέσω της Μαύρης Θάλασσας, της Ανατολικής Μεσογείου όπως τα νησιά του Αιγαίου, της Κεντρικής και Δυτικής Μεσογείου). Η μεγάλη ποσότητα των εν λόγω δεδομένων, σε συνδυασμό με την έλλειψη εργαλείων ΤΠΕ, καθώς και την έλλειψη αλγορίθμων ανάλυσης και συστημάτων αποφάσεων, αποτελεί σημαντικό εμπόδιο στον επιτυχημένο σχεδιασμό στρατηγικών που θα εκμεταλλευτούν τα εν λόγω δεδομένα, για να βοηθήσουν την ΕΕ να χωρίσει και να ενσωματώσει αποτελεσματικά τους πρόσφυγες στα μέλη της, ανάλογα με τις δεξιότητες, τις ανάγκες τους και πολιτιστικούς περιορισμούς.

Πρέπει να σημειωθεί ότι μόνο οι πρόσφυγες μπορούν να μετεγκατασταθούν. Όσον αφορά τους μετανάστες, η ΕΕ δεν μπορεί να τους υπαγορεύσει σε ποια χώρα θα ζήσουν. Το πλεονέκτημα της πληροφόρησης για αυτούς είναι ότι μπορούν να λάβουν πιο ενημερωμένες αποφάσεις εάν θα μείνουν ή θα πάνε σε άλλη ευρωπαϊκή χώρα όπου οι δεξιότητές τους ταιριάζουν καλύτερα, σχετικά με τις υπηρεσίες που είναι διαθέσιμες στη χώρα που έχουν μετακομίσει. Επιπλέον, και για τις αρχές και τους υπεύθυνους χάραξης της πολιτικής είναι πιο εύκολο να προσαρμόσουν και να κατευθύνουν τους πόρους όπου είναι αναγκαίοι, όσον αφορά στην πληθυσμιακή ομάδα των μεταναστών [2]. Το κοινό ευρωπαϊκό σύστημα ασύλου καθορίζει κοινά ελάχιστα πρότυπα για τη μεταχείριση των αιτούντων άσυλο. Στην πράξη, οι αιτούντες άσυλο δεν αντιμετωπίζονται ομοιόμορφα και τα ποσοστά αναγνώρισης ποικίλλουν μεταξύ των κρατών μελών. Ως αποτέλεσμα αυτού, πολλοί αιτούντες άσυλο μετακινούνται εντός της ΕΕ αναζητώντας την καλύτερη χώρα για να υποβάλουν αίτηση ασύλου. Αυτό το φαινόμενο είναι γνωστό ως «αγορές ασύλου» [3]. Η κρίση της μετανάστευσης επιδείνωσε αυτό το ζήτημα και τόνισε την ανάγκη για καλύτερη εναρμόνιση των διαδικασιών και των προτύπων ασύλου. Το φαινόμενο αυτό μπορεί να αποφευχθεί με τη χρήση ενός αποθετηρίου, στο οποίο θα συλλέγονται τα χαρακτηριστικά των υπηκόων τρίτων χωρών και με βάση κάποια κριτήρια όπως η ενδεχόμενη μόρφωση ή η συγγένεια με άτομα που κατοικούν στην ΕΕ θα αποφασίζεται πιο κράτος μέλος θα είναι υπεύθυνο γι' αυτούς.

Είναι ιδιαίτερα σημαντικό να τονιστεί, επίσης, ότι η πολιτική αντιμετώπισης των προσφυγικών και μεταναστευτικών ροών αφορά στη διαχείριση των ευαίσθητων προσωπικών δεδομένων των υπηκόων τρίτων χωρών. Όπως συνεπάγεται από τα παραπάνω,

[1] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1707#eurodac

[2] http://europa.eu/rapid/press-release_IP-15-5699_en.htm

[3] https://www.consilium.europa.eu/en/policies/migratory-pressures/managing-migration-flows/

οι υπάρχουσες δομές δε μπορούν να εξασφαλίσουν σε ικανοποιητικό βαθμό την ασφάλεια των δεδομένων ή θα πρέπει να δαπανηθούν μεγάλα χρηματικά ποσά για την επίτευξη αυτού του στόχου.

Προκειμένου να αντιμετωπιστούν αυτές οι προκλήσεις, μπορεί να χρησιμοποιηθεί η τεχνολογία του Blockchain. Όπως αναλύθηκε διεξοδικά και στο *κεφάλαιο 1.4* το Blockchain εξασφαλίζει την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, μέσω της τεχνολογίας της ψηφιακής υπογραφής (digital signature). Πιο συγκεκριμένα, θα ήταν ωφέλιμο προς αυτή την κατεύθυνση να δημιουργηθεί ένα επιμελημένο και σημασιολογικά βελτιωμένο αποθετήριο blockchain, όπου τα διαφορετικά ενδιαφερόμενα μέρη θα μπορούν να συνεισφέρουν με δεδομένα προκειμένου να υποστηρίξουν τους δικούς τους στόχους και λειτουργίες, αλλά ταυτόχρονα θα επιτρέπει και στους τελικούς χρήστες (υπηκόους τρίτων χωρών) να επωφεληθούν από τις λειτουργίες του. Ακόμη ένα βασικό πλεονέκτημα της τεχνολογίας του blockchain είναι η δυνατότητα αποκεντρωμένης αποθήκευσης αρχείων, γεγονός που συμβάλει στη διατήρηση της ασφάλειας των δεδομένων των υπηκόων τρίτων χωρών και τα προστατεύει από ενδεχόμενη παραβίαση. Δεδομένου ότι κάθε μία από τις συναλλαγές στο blockchain επικυρώνεται και αποκτά χρονική επισήμανση, είναι εύκολο να επαληθευτούν και να εντοπιστούν κινήσεις και καταγραφές των υπηκόων τρίτων χωρών. Έτσι, με τη χρήση της τεχνολογίας του Blockchain είναι δυνατό να δημιουργηθεί ένα ψηφιακό πορτφόλιο (ατομικός ψηφιακός φάκελος) για κάθε έναν υπήκοο τρίτης χώρας που φτάνει στην ΕΕ και το οποίο θα χρησιμοποιεί ο ίδιος αλλά και τα ενδιαφερόμενα μέρη, υπηρεσίες και ΜΚΟ σε όλη την πορεία της ένταξης του ή μη στην ΕΕ.

3 European Blockchain Services Infrastructure (EBSI)

3.1 Εισαγωγή στο EBSI

Η «Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain» (EBSI) αποτελεί κοινή πρωτοβουλία της Ευρωπαϊκής Επιτροπής και της «Ευρωπαϊκής Σύμπραξης Blockchain» - European Blockchain Partnership (EBP) - με στόχο την αξιοποίηση της τεχνολογίας Blockchain για την παροχή υπηρεσιών, ιδίως διασυνοριακών, στην Ευρωπαϊκή Ένωση. Η πλατφόρμα EBSI υλοποιείται ως ένα peer-to-peer δίκτυο διασυνδεδεμένων κόμβων. Η Ευρωπαϊκή Επιτροπή διατηρεί σε λειτουργία ένα ελάχιστο αριθμό τέτοιων κόμβων σε ευρωπαϊκό επίπεδο και τα κράτη μέλη της ΕΕ μπορούν να λειτουργήσουν κόμβους διασυνδεδεμένους στο δίκτυο σε εθνικό επίπεδο. Το σύνολο των κόμβων δύναται να δημιουργούν και να προωθούν συναλλαγές οι οποίες ενημερώνουν το ledger. Όλοι οι κόμβοι είναι συγχρονισμένοι μοιράζοντας την ίδια κατάσταση του ledger και των μέσων αποθήκευσης εκτός blockchain.[1, 2]

3.1.1 Η πορεία προς το EBSI

Το 2017, τα κράτη μέλη και οι χώρες της ΕΖΕΣ (Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών) υπέγραψαν τη δήλωση του Ταλίν για την ηλεκτρονική διακυβέρνηση, τονίζοντας τη σημασία αποτελεσματικών και ασφαλών ψηφιακών δημόσιων υπηρεσιών προκειμένου να αξιοποιηθούν πλήρως οι δυνατότητες της Ψηφιακής Ενιαίας Αγοράς. [94]

Το 2018, 27 κράτη μέλη της ΕΕ, η Νορβηγία και το Λιχτενστάιν υπέγραψαν μια δήλωση για τη δημιουργία της Ευρωπαϊκής Σύμπραξης Blockchain (EBP) με στόχο την παροχή ψηφιακών υπηρεσιών που να ανταποκρίνονται στα απαιτούμενα επίπεδα ψηφιακής ασφάλειας και τις ανάγκες της σημερινής κοινωνίας. [94]

Στις 14 Φεβρουαρίου 2019, η Ευρωπαϊκή Επιτροπή δημοσίευσε το Πρόγραμμα Εργασίας Τηλεπικοινωνιών 2019 του μηχανισμού «Συνδέοντας την Ευρώπη» - Connecting Europe Facility (CEF), δημιουργώντας τις αρχικές προϋποθέσεις χρηματοδότησης του EBSI. Ο μηχανισμός «Συνδέοντας την Ευρώπη» αποτελεί χρηματοδοτικό πρόγραμμα για στρατηγικές επενδύσεις στους τομείς των μεταφορών, των τηλεπικοινωνιών και της ενέργειας. [94,3]

Το 2020 το EBSI προορίζεται να προστεθεί στη λίστα με τα διαθέσιμα CEF building blocks, ώστε να προσφέρει μια επαναχρησιμοποιούμενη λύση λογισμικού και μια βάση κοινών προδιαγραφών προς υιοθέτηση από τα θεσμικά όργανα της ΕΕ και τις Ευρωπαϊκές διοικήσεις για την ταχεία εκμετάλλευση των δυνατοτήτων του EBSI. [94]

Τα CEF building blocks μπορούν να χρησιμοποιηθούν σε Ευρωπαϊκά projects ώστε να διευκολυνθεί η ανάπτυξη δημόσιων ψηφιακών υπηρεσιών. Βασίζονται σε συμφωνίες διαλειτουργικότητας μεταξύ των κρατών μελών της ΕΕ εξασφαλίζοντας κατά αυτόν τον τρόπο και τη διαλειτουργικότητα των πληροφοριακών συστημάτων. Για να μπορέσει ένα building block να αξιοποιηθεί από τους ενδιαφερόμενους παρέχεται μία «Πλατφόρμα Βασικής Υπηρεσίας» (Core Service Platform) η οποία αποτελείται από [4]:

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/EBSI+Documentation+home
[3] https://ec.europa.eu/transport/themes/infrastructure/cef_en
[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+a+Building+Block

- Το σύνολο των τεχνικών προδιαγραφών και προτύπων πάνω στα οποία βασίζεται η υπό ανάπτυξη υπηρεσία
- Λογισμικό που βρίσκεται σε συμφωνία με τις ανωτέρω προδιαγραφές, ως δείγμα για τη διευκόλυνση της υλοποίησης της λύσης (προαιρετικά)
- Ένα σύνολο υπηρεσιών όπως υπηρεσίες υποστήριξης και ελέγχου συμμόρφωσης, προς διευκόλυνση της εφαρμογής των ανωτέρω προδιαγραφών

3.1.2 Στόχοι και οφέλη EBSI

Η ανάπτυξη του EBSI απορρέει από το όραμα της Ευρωπαϊκής Επιτροπής για την παροχή υψηλού επιπέδου υπηρεσιών προς διευκόλυνση των πολιτών και των θεσμικών οργάνων της ΕΕ. Συνοπτικά αναφέρονται παρακάτω οι στρατηγικοί στόχοι του EBSI [1]:

- Παροχή και βελτίωση των διασυνοριακών υπηρεσιών από τις κυβερνήσεις προς τους πολίτες
- Συμμόρφωση και τήρηση της νομοθεσίας και των κανονισμών, όπως ενδεικτικά αναφέρονται οι κανονισμοί GDPR (*General Data Protection Regulation),* eIDAS (*electronic IDentification, Authentication and trust Services*)
- Ώθηση στην ανάπτυξη εφαρμογών και προγραμμάτων στην Ευρώπη και αξιοποίηση των δυνατοτήτων που παρέχει η τεχνολογία του Blockchain
- Ενίσχυση της επιχειρησιακής κινητικότητας
- Υποστήριξη της αειφόρου ανάπτυξης

Η ανάπτυξη του EBSI δημιουργεί οφέλη για α) τους πολίτες, παρέχοντάς τους διευκολύνσεις και μέγιστη ασφάλεια για την εκτέλεση διασυνοριακών συναλλαγών, β) τα ευρωπαϊκά θεσμικά όργανα και τις ευρωπαϊκές κοινότητες, απλοποιώντας τις διοικητικές διαδικασίες, επιτρέποντας τη συμμόρφωση με τους κανονισμούς και αυξάνοντας την αποτελεσματικότητα των διασυνοριακών δημοσίων υπηρεσιών, γ) τις εθνικές διοικήσεις, διευκολύνοντας τις διοικητικές διαδικασίες, αυξάνοντας την απόδοση και την αξιοπιστία των υπηρεσιών, δ) τον τεχνολογικό κλάδο δίνοντας τη δυνατότητα στους παρόχους υπηρεσιών και εφαρμογών να αξιοποιούν ένα κυβερνητικά πιστοποιημένο δίκτυο blockchain.[2]

3.1.3 Αρχιτεκτονική EBSI

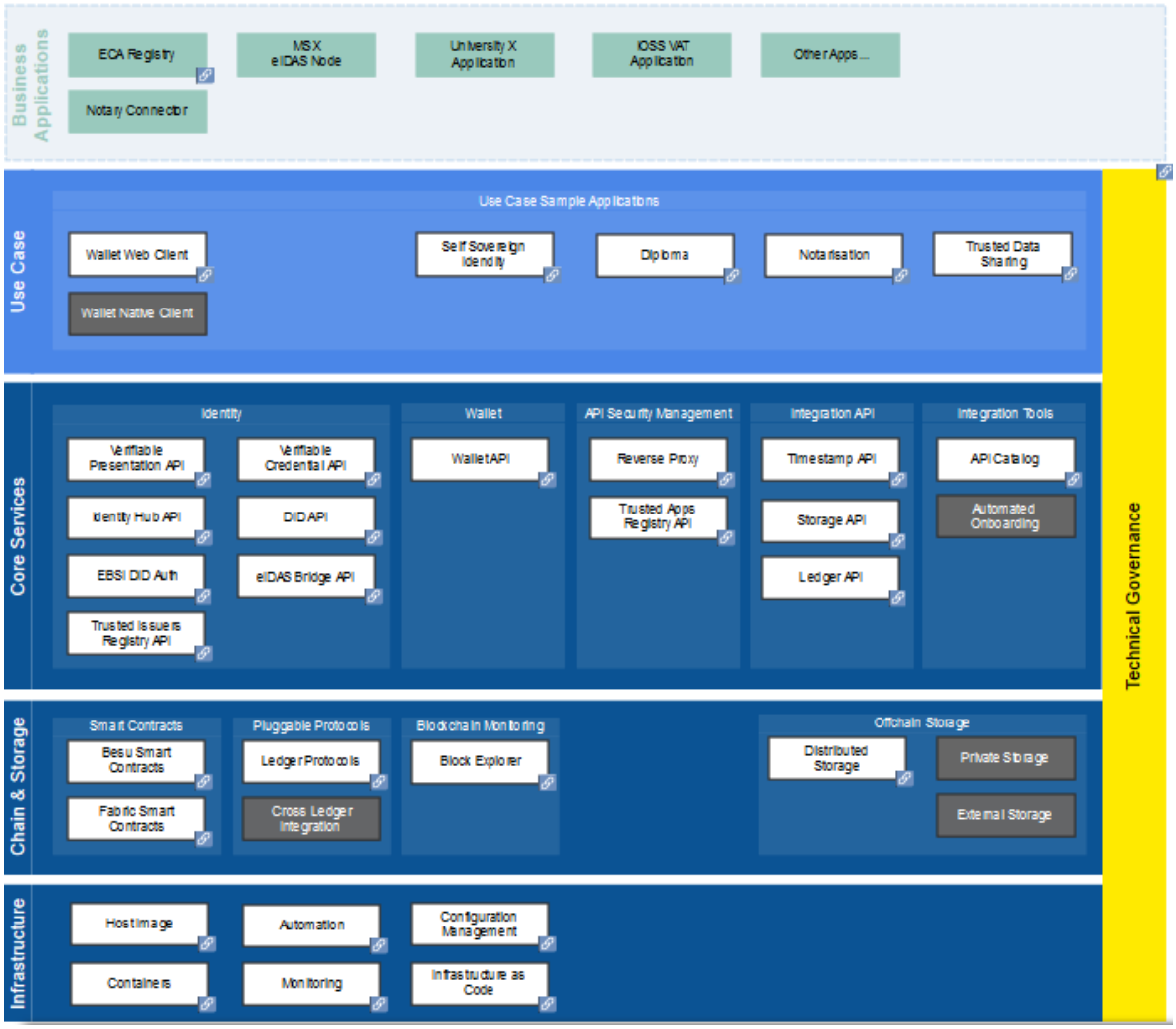
Η αρχιτεκτονική του EBSI χωρίζεται σε επίπεδα, που το καθένα από αυτά εξυπηρετεί μία γενική κατηγορία λειτουργικοτήτων. Κατά αυτόν τον τρόπο οι υπηρεσίες που αναπτύσσονται εντάσσονται βάσει των λειτουργιών που επιτελούν σε ένα από αυτά τα επίπεδα. Η υλοποίηση του EBSI βασίζεται σε microservices αρχιτεκτονική.

Η αρχιτεκτονική του EBSI διακρίνεται στα τρία επίπεδα που αναφέρονται επιγραμματικά παρακάτω και αναλύονται στη συνέχεια:

- Βασικές Υπηρεσίες (Main Services)
- Σενάρια χρήσης (Use Cases)
- Επιχειρησιακές εφαρμογές (Business Applications)

[1]https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Mapping+of+Vision%2C+Mission%2C+and+Goals

[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI



Εικόνα 21 Αρχιτεκτονική EBSI [1]

3.1.3.1 Βασικές Υπηρεσίες (Main Services)

Το επίπεδο των Βασικών Υπηρεσιών μπορεί να διακριθεί περεταίρω στα εξής τρία υποεπίπεδα:

- Υποδομή (Infrastructure). Στο υποεπίπεδο της υποδομής ανήκουν τα απαραίτητα στοιχεία για την εγκατάσταση και λειτουργία του EBSI κόμβου, όπως είναι η υπολογιστική ισχύς, η δικτύωση καθώς επίσης τα στοιχεία και εργαλεία παραμετροποίησης, εγκατάστασης, αυτοματοποίησης και παρακολούθησης της λειτουργίας του κόμβου.[2]
- Chain-Storage. Το υποεπίπεδο αυτό περιλαμβάνει τα blockchain πρωτόκολλα που υποστηρίζονται από το EBSI, καθώς και τις επιπλέον δυνατότητες που παρέχονται για off-chain μέσα αποθήκευσης, συμβάλλοντας στη διαλειτουργικότητα του EBSI δικτύου με πλήθος διαφορετικών εφαρμογών και ενδεχομένως με διαφορετικά Blockchain δίκτυα.[3]
- Υπηρεσίες πυρήνα (Core Services). Στο υποεπίπεδο αυτό ανήκουν οι διεπαφές που παρέχουν τις βασικές υπηρεσίες-λειτουργικότητες στις εφαρμογές του ανωτέρου

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Architecture
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Infrastructure+Layer
[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Chain+and+Storage+Layer

επιπέδου (use cases) αξιοποιώντας τις λειτουργικότητες του EBSI. Κατά αυτόν τον τρόπο εξωτερικές εφαρμογές δεν έχουν απευθείας πρόσβαση στις χαμηλότερες από άποψη αρχιτεκτονικής λειτουργικότητες του EBSI, αλλά μέσα των διεπαφών που ορίζονται συμβάλλοντας έτσι στην ασφάλεια του δικτύου και στην παροχή αρθρωτών λύσεων.[1]

3.1.3.2 Σενάρια χρήσης (Use cases)

Στο επίπεδο αυτό συναντάται πλήθος σεναρίων χρήσης που αποτελούν έφαρμογες-δείγματα. Κατά αυτόν τον τρόπο γίνονται ευκολότερα κατανοητές οι δυνατότητες του δικτύου EBSI. Επίσης, επεξηγούνται οι υπηρεσίες-λειτουργικότητες που παρέχει η διεπαφή του κατώτερου επιπέδου (Core Service API) και ο τρόπος χρήσης τους. Τέλος, δημιουργείται αξία από τις ίδιες τις εφαρμογές (use cases) που έχουν αναπτυχθεί.[2]

3.1.3.3 Επιχειρησιακές εφαρμογές (Business Applications)

Το επίπεδο αυτό περιλαμβάνει επιχειρησιακές εφαρμογές που δεν βρίσκονται στην υποδομή των EBSI κόμβων ωστόσο επιτρέπουν στους οργανισμούς να αναπτύσσουν εφαρμογές που συνδέονται στους EBSI κόμβους και αξιοποιούν τις υπηρεσίες που διατίθενται. [3]

3.1.4 Παρεχόμενες υπηρεσίες

Με την ένταξη της λύσης που βασίζεται στο EBSI στη λίστα με τα διαθέσιμα CEF Building Blocks, ένα σύνολο υπηρεσιών θα παρέχονται, διευκολύνοντας τα κράτη μέλη και τις δημόσιες διοικήσεις για την υιοθέτηση των προσφερόμενων λύσεων αλλά και την ανάπτυξη νέων εφαρμογών. Οι υπηρεσίες αυτές μπορούν να ομαδοποιηθούν συνοπτικά σε α) Βασικές Υπηρεσίες (Core Services), που αφορούν τη δημιουργία και τη συντήρηση των τεχνικών προδιαγραφών του EBSI, β) Υποστηρικτικές Υπηρεσίες (Enabling Services) προς διευκόλυνση της αξιοποίησης των δυνατοτήτων του EBSI, όπως πακέτα εγκατάστασης, πακέτα ελέγχου, υλικό εκπαίδευσης, γ) Enhancing Services που επιταχύνουν την υιοθέτηση λύσεων βασισμένων στο EBSI βελτιώνοντας την εμπειρία χρήσης των Δημόσιων Διοικήσεων. [105]

3.1.4.1 Σενάρια Χρήσης EBSI v1

Με την έναρξη της λειτουργίας του EBSI στην πρώτη έκδοση το τέλος του πρώτου τριμήνου του έτους 2020, παρέχονται οι παρακάτω εφαρμογές ως αντιπροσωπευτικά σενάρια χρήσης

Wallet Web Client

Οι πολίτες, τα ιδρύματα και κατ' επέκταση οι ενδιαφερόμενοι χρήστες μπορούν μέσω της εφαρμογής του Wallet, να χρησιμοποιούν τις υπόλοιπες εφαρμογές που έχουν υλοποιηθεί και να διαχειρίζονται τα προσωπικά στοιχεία και δεδομένα τους. Περιλαμβάνει τη σελίδα ταυτοποίησης του χρήστη, και μία κεντρική σελίδα που εμφανίζει τις υπάρχουσες εφαρμογές μαζί με προσωποποιημένα τμήματα όπως ιστορικό και ειδοποιήσεις.[4]

European Self Sovereign Identity

Ο όρος «Αυτοδύναμη Ταυτότητα» - Self Sovereign Identity (SSI) συνδέεται με τον τρόπο διαχείρισης των ταυτοτήτων στον ψηφιακό κόσμο. Συγκεκριμένα, δίνεται η δυνατότητα στους χρήστες να δημιουργούν και να διαχειρίζονται την ταυτότητά τους χωρίς να βασίζονται

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Core+Services+Layer
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Use+Case+Layer
[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Wallet+Web+Client

σε κάποια κεντρική αρχή. Με το SSI το υποκείμενο-χρήστης είναι σε θέση να αποκτά διαπιστευτήρια που σχετίζονται με αυτό και έχουν τα χαρακτηριστικά εκείνα ώστε να μπορούν να πιστοποιούν τον ισχυρισμό του χρήστη, αλλά και των οποίων η εγκυρότητα μπορεί να επαληθευτεί. Μέσω της υπηρεσίας ο χρήστης είναι σε θέση να αιτείται και να αποκτά ένα ψηφιακό αναγνωριστικό, Verifiable (digital) ID, που μπορεί να χρησιμοποιηθεί για την αναγνώριση και πιστοποίησή του. Η Ευρωπαϊκή Αυτοδύναμη Ταυτότητα ESSI βασίζεται στην χρήση Αποκεντρωμένων Αναγνωριστικών – Decentralized Identifiers (DIDs) που είναι σύμφωνα με το πρότυπο W3C (World Wide Web Consortium), και αποτελούν ένα είδος ψηφιακών αναγνωριστικών που είναι αποκλειστικά υπό τον έλεγχο του υποκειμένου και δεν έχουν εξάρτηση από καμία κεντρική αρχή ή μητρώο.[1, 2]

Diplomas

Μέσω της συγκεκριμένης υπηρεσίας οι πολίτες έχουν τον έλεγχο των εκπαιδευτικών διαπιστευτηρίων τους μειώνοντας έτσι τα κόστη που απαιτούνται για την πιστοποίηση εγγράφων αλλά και αυξάνοντας την αξιοπιστία τους. Συγκεκριμένα έχουν τη δυνατότητα να αιτούνται και να αποκτούν βεβαιώσεις για τα διπλώματα που έχουν στην κατοχή τους και στη συνέχεια να αποθηκεύουν και να διαχειρίζονται τις βεβαιώσεις αυτές.

Στα πλαίσια του συγκεκριμένου σεναρίου χρήσης, έχουν υλοποιηθεί δύο web εφαρμογές προσομοιώνοντας τη διαδικασία έκδοσης επαληθεύσιμων βεβαιώσεων (Verifiable Attestation - VA), εκ μέρους της κυβέρνησης της Φλαμανδικής περιοχής και ενός ισπανικού πανεπιστημίου. Ένα VA αποτελεί ένα είδος διαπιστευτηρίου το οποίο μια οντότητα μπορεί να χρησιμοποιήσει ως ένα αποδεικτικό για κάποια ιδιότητα ή ισχυρισμό. Στην προκειμένη περίπτωση τα διαπιστευτήρια αφορούν την κατοχή διπλωμάτων Bachelor και Master. [3,4]

Συγκεκριμένα, ο χρήστης μπορεί να αιτηθεί την έκδοση ενός διαπιστευτηρίου (VA) για το Bachelor δίπλωμά του, επιδεικνύοντας το διαπιστευτήριο του ψηφιακού αναγνωριστικού (eID VC) που έχει αποκτήσει μέσω της υπηρεσίας ESSI. Η προσομοιωμένη για την Φλαμανδική Κυβέρνηση εφαρμογή εφόσον ελέγξει ότι το διαπιστευτήριο που ο χρήστης υποδεικνύει πληροί τις απαραίτητες συνθήκες, όπως εγκυρότητα, γνησιότητα, ακεραιότητα, θα εκδώσει το ζητούμενο διαπιστευτήριο. [110]

Κατά αντιστοιχία, ο χρήστης μπορεί να αιτηθεί την έκδοση ενός διαπιστευτηρίου (VA) για το Master δίπλωμά του. Στην προκειμένη περίπτωση, μαζί με το eID VC επιδεικνύεται και το διαπιστευτήριο που αποκτήθηκε για το Bachelor δίπλωμα. Η προσομοιωμένη εφαρμογή για το ισπανικό πανεπιστήμιο θα επικυρώσει τον έλεγχο των διαπιστευτηρίων και στη συνέχεια θα εκδώσει το ζητούμενο διαπιστευτήριο. [5]

Notarisation

Με την υπηρεσία Notarisation παρέχεται η δυνατότητα για συμβολαιογραφική θεώρηση εγγράφων, για επαλήθευση θεωρημένων εγγράφων, για δημιουργία διαδρομών ελέγχων (audit-trail) καθώς και για έλεγχο της ακεραιότητας και της πιστότητας των εγγράφων.

[1]https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Technical+Specification+%282%29+-+DID+Modelling

[2] https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers

[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Terminology

[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Diplomas

[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Diplomas

Για το συγκεκριμένο σενάριο χρήσης του EBSI, έχει δημιουργηθεί μια web εφαρμογή που προσομοιώνει λειτουργικότητες ενός ευρωπαϊκού χρηματοδοτικού ιδρύματος, στα πλαίσια της οποίας παρέχεται η δυνατότητα για υποβολή και χρονοσήμανση εγγράφων σχετιζόμενων με δαπάνες συμβάσεων επιχορήγησης, όπως τιμολόγια και συμβόλαια καθώς επίσης και η δυνατότητα για την επικύρωση της γνησιότητας αυτών των εγγράφων. [1]

Trusted Data Sharing

Η αξιόπιστη κοινή χρήση δεδομένων (Trust Data Sharing), βασίζεται σε μια νέα προσέγγιση για τη δημιουργία ενός κατανεμημένου και αποκεντρωμένου συστήματος, διασυνδέοντας τους δημόσιους και ιδιωτικούς φορείς των κρατών μελών σε μια πλατφόρμα με στόχο την κοινή χρήση δεδομένων αντί της ανταλλαγής αυτών, προσφέροντας ταυτόχρονα πλήρη ιχνηλασιμότητα και διαχείριση της ιδιοκτησίας και του κύκλου ζωής δεδομένων. [2]

Στην προκειμένη περίπτωση, αξιοποιούνται οι τεχνικές δυνατότητες που προσφέρει το EBSI για τη δημιουργία μιας εφαρμογής που εξυπηρετεί την αξιόπιστη κοινή χρήση δεδομένων. Συγκεκριμένα στα πλαίσια αυτής της web εφαρμογής παρέχονται οι δύο εξής λειτουργικότητες. [3]

- Οι φορολογικές αρχές των κρατών μελών μπορούν να υποβάλουν προς κοινοποίηση στο σύστημα στοιχεία (όπως εν προκειμένω το αναγνωριστικό φόρου προστιθέμενης αξίας «import one-stop-shop» -IOSS VAT Id)
- Οι τελωνειακές αρχές των άλλων κρατών μελών μπορούν να έχουν πρόσβαση στα κοινοποιημένα δεδομένα. Κατά αυτόν τον τρόπο μπορούν να ελέγξουν την εγκυρότητα των IOSS VAT Ids που εμφανίζονται στα δελτία εισαγωγής των προϊόντων κατά το χρόνο εισαγωγής.

3.1.4.2 Υποστηρικτικές Υπηρεσίες

Επιπροσθέτως των υπηρεσιών που αφορούσαν τα σενάρια χρήσης που αναφέρθηκαν παραπάνω παρέχεται και ένα σύνολο υποστηρικτικών υπηρεσιών.

Υπηρεσία Κοινοτικής Διαχείρισης CEF EBSI

Στόχος της υπηρεσίας Κοινοτικής Διαχείρισης είναι να υποστηρίξει τους χειριστές κόμβων του EBSI, τους υπεύθυνους για τους ελέγχους και δοκιμές, τα μέλη του EBP και άλλους ενδιαφερόμενους παρέχοντάς τους ένα σύνολο κοινών και ανοικτών κατευθυντήριων γραμμών για την περεταίρω ανάπτυξη του EBSI. Μέσω της κοινότητας οι χρήστες μπορούν να μοιράζονται τις απορίες τους και τα σχόλια τους με την τεχνική ομάδα, την ομάδα υποστήριξης και άλλους συμμετέχοντες ενισχύοντας έτσι την αλληλεπίδραση μεταξύ των χρηστών και κατ' επέκταση τη βαθύτερη κατανόηση του EBSI. [4]

Υπηρεσία Γνωσιακής Βάσης CEF EBSI

Η συγκεκριμένη υπηρεσία αποσκοπεί στην παροχή ενός αποθετηρίου αναφορών που συνδέονται με πληροφορίες σχετικές με το CEF EBSI building block. [5]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Trusted+Data+Sharing+User+Stories
[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Trusted+Data+Sharing
[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+Community+Management
[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+Community+Management

Υπηρεσία Εξυπηρέτησης (Service Desk)

Η υπηρεσία υποστήριξης παρέχει καθοδήγηση στους χρήστες σχετικά με το εύρος των υπηρεσιών που προσφέρονται στα πλαίσια του EBSI. Αποτελεί ένα ενιαίο σημείο επαφής για την απάντηση ερωτημάτων, τη διαχείριση περιστατικών, αιτημάτων και αλλαγών που αναφέρονται από τους χρήστες. [1]

Υπηρεσία Εκπαίδευσης

Η υπηρεσία εκπαίδευσης του EBSI προσφέρει ένα πακέτο εκμάθησης που παρέχει βοήθεια στους ενδιαφερόμενους που επιθυμούν τη χρησιμοποίηση του CEF EBSI building block. [2]

Υπηρεσία Ελέγχου Συνδεσιμότητας CEF EBSI

Μέσω της υπηρεσίας ελέγχου συνδεσιμότητας δύναται να επικυρωθεί εάν ένας νεοεγκατεστημένος κόμβος του EBSI, ο οποίος είναι σύμφωνος με τις προδιαγραφές του EBSI, μπορεί να επικοινωνήσει επιτυχώς με κόμβο του EBSI ο οποίος διαχειρίζεται από την Ευρωπαϊκή Επιτροπή, καθώς και άλλους κόμβους του δικτύου. Η συνδεσιμότητα ελέγχεται σε επίπεδο υποδομής και όχι σε επίπεδο εφαρμογών. Συνεπώς, μία επιτυχημένη δοκιμή υποδεικνύει ότι κατά πάσα πιθανότητα η εγκατάσταση και παραμετροποίηση του κόμβου έχουν γίνει σωστά. [3]

Κατάλογος Προγραμματιστικών Διεπαφών CEF EBSI v1

Ο κατάλογος των Προγραμματιστικών Διεπαφών που την τρέχουσα στιγμή αφορά την πρώτη έκδοση του EBSI παρέχει μία κεντρική πύλη για όλες τις διαθέσιμες διεπαφές που είναι προσβάσιμες και βρίσκονται στο επίπεδο βασικών διεπαφών (Core Services) του EBSI. Με αυτόν τον τρόπο οι χρήστες έχουν τη δυνατότητα να πληροφορηθούν για τον τρόπο αλληλεπίδρασης του λογισμικού που αναπτύσσουν ή χρησιμοποιούν με το EBSI. Επιπλέον, ενημερώνονται για τα είδη των κλήσεων που μπορούν να πραγματοποιήσουν, τον τρόπο που μπορούν να τις πραγματοποιήσουν καθώς και την μορφή των δεδομένων που ανταλλάσσονται. [4]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+Service+Desk
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+Training+Service
[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+Connectivity+Testing
[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI+v1+APIs

3.1.5 Μηχανισμός συναίνεσης και τύπος Blockchain του EBSI

3.1.5.1 Μηχανισμός Συναίνεσης

Η συναίνεση του δικτύου EBSI επιτυγχάνεται μέσω του μηχανισμού συναίνεσης απόδειξης εξουσίας (ή απόδειξη φήμης) – Proof of Authority-(PoA) με έναν κόμβο (node) ανά κράτος μέλος [1]. Σε δίκτυα, τα οποία βασίζονται στο μηχανισμό συναίνεσης PoA, οι συναλλαγές και τα block επικυρώνονται από εγκεκριμένους λογαριασμούς, γνωστούς ως «επικυρωτές» (validators)[122]. Οι επικυρωτές εκτελούν λογισμικό που τους επιτρέπει να τοποθετούν συναλλαγές σε μπλοκ. Η διαδικασία είναι αυτοματοποιημένη και δεν απαιτεί οι επικυρωτές (validators) να παρακολουθούν συνεχώς τους υπολογιστές τους. Ωστόσο, απαιτεί τη συντήρηση του υπολογιστή - κόμβου εξουσίας (authority node) [2]. Ο όρος επινοήθηκε από τον Gavin Wood, συνιδρυτή της Ethereum και της Parity Technologies.[122]

Με το μηχανισμό συναίνεσης PoA, οι οντότητες κερδίζουν το δικαίωμα να γίνουν επικυρωτές, επομένως υπάρχει ένα κίνητρο να διατηρήσουν τη θέση που έχουν αποκτήσει. Με την προσκόλληση μιας «φήμης» στην ταυτότητα τους, οι επικυρωτές ενθαρρύνονται να υποστηρίξουν τη διαδικασία συναλλαγής, καθώς δεν επιθυμούν να συνδέσουν τις ταυτότητές τους σε μια αρνητική φήμη [122]. Ο αλγόριθμος συναίνεσης PoA επωφελείται από την αξία των ταυτοτήτων, πράγμα που σημαίνει ότι οι επικυρωτές block δεν ποντάρουν νομίσματα (coins) αλλά τη «φήμη» τους. Επομένως, ένα blockchain που λειτουργεί με μηχανισμό PoA διασφαλίζεται από τους κόμβους επικύρωσης (validators) που επιλέγονται αυθαίρετα ως αξιόπιστες οντότητες. Το μοντέλο απόδειξης εξουσίας βασίζεται σε περιορισμένο αριθμό επικυρωτών μπλοκ και αυτό το καθιστά ένα εξαιρετικά κλιμακώσιμο (scalable) σύστημα. Τα μπλοκ και οι συναλλαγές επαληθεύονται από προ-εγκεκριμένους συμμετέχοντες, οι οποίοι ενεργούν ως συντονιστές του. Αυτή η προσέγγιση θεωρείται πιο ισχυρή από την προσέγγιση του μηχανισμού συναίνεσης απόδειξης πονταρίσματος PoS (Proof-of-Stake). Αυτό συμβαίνει γιατί ενώ το πονταρισμα μεταξύ δύο μερών μπορεί να είναι ισόπαλο, ο μηχανισμός PoS δεν λαμβάνει υπόψη τις συνολικές συμμετοχές κάθε μέρους. Αυτό σημαίνει ότι μπορεί να μην υπάρχει ισορροπία στα κίνητρα. Από την άλλη πλευρά, ο μηχανισμός PoA επιτρέπει τη μη διαδοχική έγκριση block από οποιονδήποτε επικυρωτή, γεγονός που σημαίνει ότι ο κίνδυνος σοβαρής ζημιάς συγκεντρώνεται στον κόμβο εξουσίας (authority node). Ο μηχανισμός PoA είναι κατάλληλος τόσο για ιδιωτικά όσο και για δημόσια δίκτυα. Στον μηχανισμό απόδειξης εξουσίας, η εμπιστοσύνη διανέμεται. Με άλλα λόγια, μπορούμε να πούμε ότι η εξουσία (authority) είναι αποκεντρωμένη[3].

Ύστερα από τους μηχανισμούς συναίνεσης απόδειξης εργασίας (PoW) και απόδειξης πονταρίσματος (PoS), οι οποίοι αντιμετωπίζουν σημαντικό πρόβλημα κλιμάκωσης, η απόδειξη εξουσίας (PoA) εφαρμόζεται επί του παρόντος ως μια πιο αποτελεσματική εναλλακτική λύση επειδή είναι σε θέση να εκτελεί πολύ περισσότερες συναλλαγές ανά δευτερόλεπτο (transactions per second -TPS). [123]

Προϋποθέσεις του μηχανισμού συναίνεσης «Απόδειξη Εξουσίας» (PoA):

- Έγκυρες και αξιόπιστες ταυτότητες: Οι επικυρωτές (validators) πρέπει να επικυρώσουν τις πραγματικές τους ταυτότητες. [123]

[1] https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12
[2] https://en.wikipedia.org/wiki/Proof_of_authority
[3] https://academy.binance.com/en/articles/proof-of-authority-explained

- Ύπαρξη δυσκολίας για να γίνει κάποιος επικυρωτής: οι υποψήφιοι πρέπει να είναι πρόθυμοι να επενδύσουν χρήματα και να διακυβεύσουν τη φήμη τους. Μια «σκληρή» διαδικασία επιλογής μειώνει τους κινδύνους επιλογής αμφισβητήσιμων επικυρωτών και ενθαρρύνει μια μακροπρόθεσμη δέσμευση. [1]
- Πρότυπο έγκρισης επικυρωτή: Η μέθοδος επιλογής επικυρωτών πρέπει να αντιμετωπίζει ισάξια τους υποψήφιους. [124]

Η ουσία πίσω από αυτόν το μηχανισμό που στηρίζεται στη φήμη είναι η βεβαιότητα πίσω από την ταυτότητα του επικυρωτή. Αυτή δεν μπορεί να είναι μια εύκολη διαδικασία ούτε μια διαδικασία που θα παραμεριζόταν εύκολα. Ο μηχανισμός θα πρέπει να είναι ικανός να αποβάλει τους κακόβουλους συμμετέχοντες. Τέλος, η διασφάλιση ότι όλοι οι επικυρωτές ακολουθούν την ίδια διαδικασία εγγυάται την ακεραιότητα και την αξιοπιστία του συστήματος. [124]

3.1.5.2 Τύπος Blockchain

Όπως είδαμε και στο κεφάλαιο 1, το μεγαλύτερο μέρος των δημόσιων (public) blockchains είναι ανοιχτά στο κοινό και μπορεί να συμμετέχει οποιοσδήποτε ως κόμβος σε αυτά χωρίς κάποια άδεια (permissionless). Ωστόσο, υπάρχει και η κατηγορία των public permissioned blockchains. Σε αυτόν τον τύπο blockchain ανήκει και το EBSI [2]. Ένα public permissioned δίκτυο blockchain είναι ένας νέος τύπος δικτύου, ο οποίος «βρίσκεται» μεταξύ των δικτύων public permissionless (όπως το Bitcoin ή το Ethereum) και των ιδιωτικών δικτύων κοινοπραξίας (private consortium blockchains). Ένα public permissioned δίκτυο blockchain συνδυάζει την ανάγκη παροχής άδειας για συμμετοχή που περιλαμβάνει το ιδιωτικό δίκτυο κοινοπραξίας με το αποκεντρωμένο μοντέλο διακυβέρνησης του δημόσιου δικτύου, προσπαθώντας να επωφεληθεί από τις ιδιότητες και των δύο μοντέλων. Σε ένα public permissioned blockchain η ταυτότητα όλων των συμμετεχόντων κόμβων είναι γνωστή[3].

[1] https://academy.binance.com/en/articles/proof-of-authority-explained

[2] https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12

[3] https://www.r3.com/blog/how-public-permissioned-blockchains-are-not-an-oxymoron-2/

3.1.6 Ορολογία EBSI

Στον

Self-Sovereign Identity (SSI) – «Αυτοδύναμη Ταυτότητα»	Η αυτοδύναμη ταυτότητα – Self-Sovereign Identity βασίζεται στην ιδέα ότι ο χρήστης πρέπει να είναι αυτός που διαχειρίζεται την ταυτότητα του. Ο χρήστης πρέπει να έχει την δυνατότητα να χρησιμοποιεί την ταυτότητα του σε πολλαπλά σημεία, και να έχει τον πλήρη έλεγχο της. Συνεπώς μια τέτοια ταυτότητα θα πρέπει να είναι μεταφέρσιμη. Επίσης θα πρέπει να επιτρέπει στο χρήστη να προβεί σε αξιώσεις-ισχυρισμούς (claims).
Subject-Υποκείμενο	Ο όρος υποκείμενο αναφέρεται σε οποιαδήποτε υπαρκτή οντότητα. Στα πλαίσια που χρησιμοποιείται ο όρος, πρέπει να είναι εφικτή η αναφορά στη συγκεκριμένη οντότητα με την έννοια ότι μπορεί να αναγνωριστεί μοναδικά.[127]
(Digital) identity – (Ψηφιακή) ταυτότητα	(Ψηφιακή) ταυτότητα είναι το σύνολο των χαρακτηριστικών/δηλώσεων/ιδιοτήτων που επιτρέπουν την αναγνώριση μιας οντότητας.[127]
Verifiable Credential (VC)	Ένα επαληθεύσιμο διαπιστευτήριο, που μπορεί να επαληθευτεί κρυπτογραφικά. Μπορεί να χρησιμοποιηθεί για τη δημιουργία επαληθεύσιμων παρουσιάσεων (Verifiable Presentations). Αποτελεί έναν «ισχυρισμό» όπως εξηγείται και στον επόμενο όρο. [127,]
Claim – Ισχυρισμός	Με τον όρο «ισχυρισμός» αναφερόμαστε στο αντικείμενο που αναπαριστά ένα σύνολο χαρακτηριστικών ή κάποια δήλωση μιας οντότητας. Δύο εξειδικεύσεις ισχυρισμών που αναφέρονται στα πλαίσια της διπλωματικής είναι α) Verifiable Claim, που αποτελεί έναν «ισχυρισμό» που η εγκυρότητα, η ακεραιότητα και η γνησιότητα του μπορούν να επαληθευτούν και από άλλα μέρη εκτός του μέρους που τον δημιουργεί, β) Verifiable Credential «επαληθεύσιμο διαπιστευτήριο», που αποτελεί έναν ισχυρισμός σύμφωνα με το W3C verifiable Credential standard. [127,128]
DID (Decentralized Identifier)	Τα αποκεντρωμένα αναγνωριστικά (DIDs) είναι ένας νέος τύπος αναγνωριστικού που επιτρέπει την επαληθεύσιμη, αποκεντρωμένη ψηφιακή ταυτότητα. Ένα DID προσδιορίζει οποιοδήποτε θέμα (π.χ. ένα άτομο, οργανισμό, μοντέλο δεδομένων, αφηρημένη οντότητα κ.λπ.) που ο υπεύθυνος επεξεργασίας του DID αποφασίζει ότι προσδιορίζει. Σε αντίθεση με τα τυπικά, ενοποιημένα αναγνωριστικά, τα DID έχουν σχεδιαστεί έτσι ώστε να μπορούν να αποσυνδεθούν από κεντρικά μητρώα, παρόχους ταυτότητας και αρχές έκδοσης πιστοποιητικών. Συγκεκριμένα, ενώ άλλα μέρη ενδέχεται να χρησιμοποιηθούν για να βοηθήσουν στην ανακάλυψη πληροφοριών που σχετίζονται με ένα DID και κατ' επέκταση τον κάτοχό του, ο σχεδιασμός επιτρέπει στον ελεγκτή ενός DID να αποδείξει ότι έχει τον έλεγχο του χωρίς να απαιτείται άδεια από οποιοδήποτε άλλο μέρος. Τα DIDs είναι URIs (Uniform Resource Identifiers) που συσχετίζουν για παράδειγμα έναν κάτοχο DID με ένα έγγραφο DID, το οποίο επιτρέπει αξιόπιστες αλληλεπιδράσεις που σχετίζονται με αυτόν τον κάτοχο. Κάθε έγγραφο DID μπορεί να εκφράζει κρυπτογραφικό υλικό, μεθόδους επαλήθευσης ή τα endpoints μιας υπηρεσίας, τα οποία παρέχουν ένα σύνολο μηχανισμών που επιτρέπουν σε έναν ελεγκτή DID να αποδείξει τον έλεγχο του DID. Τα endpoints μιας υπηρεσίας επιτρέπουν αξιόπιστες αλληλεπιδράσεις που σχετίζονται με τον κάτοχο του DID.
ESSIF digital ID	Μια ψηφιακή ταυτότητα (ακολουθούμενη και από το αντίστοιχο αναγνωριστικό) με την οποία μια οντότητα μπορεί να αναγνωριστεί στα πλαίσια του European Self-Sovereign Framework.[131]
Verifiable (digital) ID	Αποτελεί μία ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» (verifiable credential) που επιτρέπει όχι μόνο την αναγνώριση μίας οντότητας αλλά επίσης και την πιστοποίησή της. Μπορεί να το

	παρουσιάσει μια οντότητα ως απόδειξη του ποιος είναι (συγκρίσιμο με διαβατήριο, δελτίο ταυτότητας κ.λπ.).
Verifiable attestation – Επαληθεύσιμη Βεβαίωση	Η επαληθεύσιμη βεβαίωση είναι μια ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» που μπορεί να προβάλει μια οντότητα ως απόδειξη ορισμένων ιδιοτήτων ή ως απόδειξη άδειας / βεβαίωσης / εξουσιοδότησης που έχει λάβει, με τη διαφορά όμως ότι δεν χρησιμοποιείται για την πιστοποίηση της οντότητας.
Verifiable Consent/Mandate (VC)-Επαληθεύσιμη Συγκατάθεση/Εντολή	Ειδική μορφή διαπιστευτηρίου που επιτρέπει στον κάτοχο να παρουσιάζεται σε τρίτο μέρος με διαπιστευτήρια και εντολή (και βεβαιώσεις σχετικά με ένα αντίστοιχο θέμα).[131]
Verifiable presentation	Με τον όρο verifiable presentation αναφερόμαστε στα δεδομένα που μεταβιβάζονται από μια οντότητα σε ένα εμπιστευτικό μέρος (που συχνά είναι το μέρος που επαληθεύει τα δεδομένα).[131]
Verifiable Supporting Docs	Οποιοσδήποτε τύπος «παραρτημάτων» στα οποία αναφέρονται τα επαληθεύσιμα διαπιστευτήρια. [130]
eIDAS	Ο κανονισμός (EU) N°910/2014 για τις υπηρεσίες ηλεκτρονικής αναγνώρισης και πιστοποίησης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.[131]
Registry (Μητρώο Εγγραφών)	Μια υπηρεσία notarisation στο blockchain είναι ουσιαστικά ένα στατικό μητρώο που αποθηκεύει αμετάβλητα δεδομένα αναφοράς που μπορούν να χρησιμοποιηθούν σε μεταγενέστερο στάδιο ως απόδειξη γνησιότητας / ακεραιότητας των ψηφιακών αντικειμένων. Αναφερόμαστε στο "Μητρώο" ως η εφαρμογή / σύστημα που θα προσφέρει τις υπηρεσίες συμβολαιογραφικής θεώρησης.
Document (Έγγραφο)	Ένα «έγγραφο» είναι οποιαδήποτε ψηφιακή πληροφορία, συμπεριλαμβανομένων αρχείων κειμένου, μηνυμάτων ηλεκτρονικού ταχυδρομείου, φωτογραφιών και βημάτων / συμβάντων επεξεργασίας, από ένα σύστημα πληροφοριών.[132]
NID (Notarisation Identifier)	Αναφορά σε notarisation.
eID	eID είναι ένα σύνολο υπηρεσιών που παρέχονται από την Ευρωπαϊκή Επιτροπή με στόχο την αναγνώριση των διαφορετικών σχημάτων ηλεκτρονικής αναγνώρισης (electronic identification schemes) των χρηστών ανά την Ευρώπη. Επιτρέπει στους ευρωπαίους πολίτες να χρησιμοποιούν τις εθνικές τους ηλεκτρονικές ταυτότητες κατά την πρόσβαση σε διαδικτυακές υπηρεσίες από άλλες ευρωπαϊκές χώρες.
Ευρωπαϊκό Πλαίσιο Επαγγελματικών Προσόντων (ΕΠΕΠ)-European Qualifications Framework (EQF)	Το ΕΠΕΠ αποτελεί ένα πλαίσιο με 8 επίπεδα αναφοράς που βασίζεται στα μαθησιακά αποτελέσματα για όλους τους τύπους των προσόντων. Χρησιμεύει ως μηχανισμός μετατροπής μεταξύ των διαφόρων εθνικών πλαισίων επαγγελματικών προσόντων. Συμβάλλει στη βελτίωση της διαφάνειας, της συγκρισιμότητας και της φορητότητας των επαγγελματικών προσόντων και καθιστά δυνατή τη σύγκριση προσόντων από διαφορετικές χώρες και ιδρύματα. Το ΕΠΕΠ καλύπτει όλους τους τύπους και όλα τα επίπεδα προσόντων και η χρήση μαθησιακών αποτελεσμάτων καθιστά σαφές τι γνωρίζει, τι κατανοεί και τι είναι σε θέση να κάνει ένα άτομο. Το επίπεδο αυξάνεται ανάλογα με το επίπεδο επάρκειας, το επίπεδο 1 είναι το χαμηλότερο και το 8 το υψηλότερο. Το σημαντικότερο είναι ότι το ΕΠΕΠ συνδέεται στενά με τα εθνικά πλαίσια επαγγελματικών προσόντων. Η σύνδεση αυτή του επιτρέπει να χαρτογραφεί όλους τους τύπους και τα επίπεδα προσόντων στην Ευρώπη, τα οποία καθίστανται όλο και περισσότερο προσβάσιμα με τη βοήθεια βάσεων δεδομένων για τα επαγγελματικά προσόντα.
Εθνικό Πλαίσιο Προσόντων (ΕΠΠ) -	Τα Εθνικά Πλαίσια Προσόντων ταξινομούν τα προσόντα ανά επίπεδο, με βάση τα μαθησιακά αποτελέσματα. Αυτή η ταξινόμηση αντικατοπτρίζει το περιεχόμενο και το προφίλ των προσόντων - δηλαδή, τι αναμένεται να

National Qualifications Framework (NQF)	γνωρίζει, να κατανοεί και να είναι σε θέση να κάνει ο κάτοχος ενός πιστοποιητικού ή διπλώματος.
GDPR	Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
Deep link	Ο όρος deep link αναφέρεται στη χρήση υπερσυνδέσμων οι οποίοι οδηγούν σε ένα συγκεκριμένο μέρος πληροφορίας ή περιεχομένου

Πίνακας 8 παρατίθενται συγκεντρωτικά όροι που εν μέρει αναφέρθηκαν και αναλύθηκαν νωρίτερα αλλά και όροι που θα χρησιμοποιηθούν στα ακόλουθα υποκεφάλαια.

Self-Sovereign Identity (SSI) – «Αυτοδύναμη Ταυτότητα»	Η αυτοδύναμη ταυτότητα – Self-Sovereign Identity βασίζεται στην ιδέα ότι ο χρήστης πρέπει να είναι αυτός που διαχειρίζεται την ταυτότητα του. Ο χρήστης πρέπει να έχει την δυνατότητα να χρησιμοποιεί την ταυτότητα του σε πολλαπλά σημεία, και να έχει τον πλήρη έλεγχο της. Συνεπώς μια τέτοια ταυτότητα θα πρέπει να είναι μεταφέρσιμη. Επίσης θα πρέπει να επιτρέπει στο χρήστη να προβεί σε αξιώσεις-ισχυρισμούς (claims). [1]
Subject-Υποκείμενο	Ο όρος υποκείμενο αναφέρεται σε οποιαδήποτε υπαρκτή οντότητα. Στα πλαίσια που χρησιμοποιείται ο όρος, πρέπει να είναι εφικτή η αναφορά στη συγκεκριμένη οντότητα με την έννοια ότι μπορεί να αναγνωριστεί μοναδικά.[127]
(Digital) identity – (Ψηφιακή) ταυτότητα	(Ψηφιακή) ταυτότητα είναι το σύνολο των χαρακτηριστικών/δηλώσεων/ιδιοτήτων που επιτρέπουν την αναγνώριση μιας οντότητας.[127]
Verifiable Credential (VC)	Ένα επαληθεύσιμο διαπιστευτήριο, που μπορεί να επαληθευτεί κρυπτογραφικά. Μπορεί να χρησιμοποιηθεί για τη δημιουργία επαληθεύσιμων παρουσιάσεων (Verifiable Presentations). Αποτελεί έναν «ισχυρισμό» όπως εξηγείται και στον επόμενο όρο. [127,2]
Claim – Ισχυρισμός	Με τον όρο «ισχυρισμός» αναφερόμαστε στο αντικείμενο που αναπαριστά ένα σύνολο χαρακτηριστικών ή κάποια δήλωση μιας οντότητας. Δύο εξειδικεύσεις ισχυρισμών που αναφέρονται στα πλαίσια της διπλωματικής είναι α) Verifiable Claim, που αποτελεί έναν «ισχυρισμό» που η εγκυρότητα, η ακεραιότητα και η γνησιότητα του μπορούν να επαληθευτούν και από άλλα μέρη εκτός του μέρους που τον δημιουργεί, β) Verifiable Credential «επαληθεύσιμο διαπιστευτήριο», που αποτελεί έναν ισχυρισμός σύμφωνα με το W3C verifiable Credential standard. [127,128]
DID (Decentralized Identifier)	Τα αποκεντρωμένα αναγνωριστικά (DIDs) είναι ένας νέος τύπος αναγνωριστικού που επιτρέπει την επαληθεύσιμη, αποκεντρωμένη ψηφιακή ταυτότητα. Ένα DID προσδιορίζει οποιοδήποτε θέμα (π.χ. ένα άτομο, οργανισμό, μοντέλο δεδομένων, αφηρημένη οντότητα κ.λπ.) που ο υπεύθυνος επεξεργασίας του DID αποφασίζει ότι προσδιορίζει. Σε αντίθεση με τα τυπικά, ενοποιημένα αναγνωριστικά, τα DID έχουν σχεδιαστεί έτσι ώστε να μπορούν να αποσυνδεθούν από κεντρικά μητρώα, παρόχους ταυτότητας και αρχές έκδοσης πιστοποιητικών. Συγκεκριμένα, ενώ άλλα μέρη ενδέχεται να χρησιμοποιηθούν για να βοηθήσουν στην ανακάλυψη πληροφοριών που σχετίζονται με ένα DID και κατ' επέκταση τον κάτοχό του, ο σχεδιασμός επιτρέπει στον ελεγκτή ενός DID να αποδείξει ότι έχει τον έλεγχο του χωρίς να απαιτείται άδεια από οποιοδήποτε άλλο μέρος. Τα DIDs είναι URIs (Uniform Resource Identifiers) που συσχετίζουν για παράδειγμα έναν κάτοχο DID με ένα έγγραφο DID, το οποίο επιτρέπει αξιόπιστες αλληλεπιδράσεις που σχετίζονται με αυτόν τον κάτοχο. Κάθε έγγραφο DID μπορεί να εκφράζει κρυπτογραφικό υλικό, μεθόδους επαλήθευσης ή τα endpoints μιας υπηρεσίας, τα οποία παρέχουν ένα

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Terminology

[2] https://www.w3.org/TR/vc-data-model/#terminology

	σύνολο μηχανισμών που επιτρέπουν σε έναν ελεγκτή DID να αποδείξει τον έλεγχο του DID. Τα endpoints μιας υπηρεσίας επιτρέπουν αξιόπιστες αλληλεπιδράσεις που σχετίζονται με τον κάτοχο του DID. [1]
ESSIF digital ID	Μια ψηφιακή ταυτότητα (ακολουθούμενη και από το αντίστοιχο αναγνωριστικό) με την οποία μια οντότητα μπορεί να αναγνωριστεί στα πλαίσια του European Self-Sovereign Framework.[131]
Verifiable (digital) ID	Αποτελεί μία ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» (verifiable credential) που επιτρέπει όχι μόνο την αναγνώριση μίας οντότητας αλλά επίσης και την πιστοποίησή της. Μπορεί να το παρουσιάσει μια οντότητα ως απόδειξη του ποιος είναι (συγκρίσιμο με διαβατήριο, δελτίο ταυτότητας κ.λπ.). [2]
Verifiable attestation – Επαληθεύσιμη Βεβαίωση	Η επαληθεύσιμη βεβαίωση είναι μια ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» που μπορεί να προβάλει μια οντότητα ως απόδειξη ορισμένων ιδιοτήτων ή ως απόδειξη άδειας / βεβαίωσης / εξουσιοδότησης που έχει λάβει, με τη διαφορά όμως ότι δεν χρησιμοποιείται για την πιστοποίηση της οντότητας. [3]
Verifiable Consent/Mandate (VC)-Επαληθεύσιμη Συγκατάθεση/Εντολή	Ειδική μορφή διαπιστευτηρίου που επιτρέπει στον κάτοχο να παρουσιάζεται σε τρίτο μέρος με διαπιστευτήρια και εντολή (και βεβαιώσεις σχετικά με ένα αντίστοιχο θέμα).[131]
Verifiable presentation	Με τον όρο verifiable presentation αναφερόμαστε στα δεδομένα που μεταβιβάζονται από μια οντότητα σε ένα εμπιστευτικό μέρος (που συχνά είναι το μέρος που επαληθεύει τα δεδομένα).[131]
Verifiable Supporting Docs	Οποιοσδήποτε τύπος «παραρτημάτων» στα οποία αναφέρονται τα επαληθεύσιμα διαπιστευτήρια. [130]
eIDAS	Ο κανονισμός (EU) N°910/2014 για τις υπηρεσίες ηλεκτρονικής αναγνώρισης και πιστοποίησης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.[131]
Registry (Μητρώο Εγγραφών)	Μια υπηρεσία notarisation στο blockchain είναι ουσιαστικά ένα στατικό μητρώο που αποθηκεύει αμετάβλητα δεδομένα αναφοράς που μπορούν να χρησιμοποιηθούν σε μεταγενέστερο στάδιο ως απόδειξη γνησιότητας / ακεραιότητας των ψηφιακών αντικειμένων. Αναφερόμαστε στο "Μητρώο" ως η εφαρμογή / σύστημα που θα προσφέρει τις υπηρεσίες συμβολαιογραφικής θεώρησης. [4]
Document (Έγγραφο)	Ένα «έγγραφο» είναι οποιαδήποτε ψηφιακή πληροφορία, συμπεριλαμβανομένων αρχείων κειμένου, μηνυμάτων ηλεκτρονικού ταχυδρομείου, φωτογραφιών και βημάτων / συμβάντων επεξεργασίας, από ένα σύστημα πληροφοριών.[132]
NID (Notarisation Identifier)	Αναφορά σε notarisation.[5]
eID	eID είναι ένα σύνολο υπηρεσιών που παρέχονται από την Ευρωπαϊκή Επιτροπή με στόχο την αναγνώριση των διαφορετικών σχημάτων ηλεκτρονικής αναγνώρισης (electronic identification schemes) των χρηστών ανά την Ευρώπη. Επιτρέπει στους ευρωπαίους πολίτες να χρησιμοποιούν τις εθνικές τους ηλεκτρονικές ταυτότητες κατά την πρόσβαση σε διαδικτυακές υπηρεσίες από άλλες ευρωπαϊκές χώρες.[6]
Ευρωπαϊκό Πλαίσιο Επαγγελματικών	Το ΕΠΕΠ αποτελεί ένα πλαίσιο με 8 επίπεδα αναφοράς που βασίζεται στα μαθησιακά αποτελέσματα για όλους τους τύπους των προσόντων.

[1] https://www.w3.org/TR/did-core/

[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

[3] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Terminology

[4] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

[5] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=155385948

[6] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

Προσόντων (ΕΠΕΠ)- European Qualifications Framework (EQF)	Χρησιμεύει ως μηχανισμός μετατροπής μεταξύ των διαφόρων εθνικών πλαισίων επαγγελματικών προσόντων. Συμβάλλει στη βελτίωση της διαφάνειας, της συγκρισιμότητας και της φορητότητας των επαγγελματικών προσόντων και καθιστά δυνατή τη σύγκριση προσόντων από διαφορετικές χώρες και ιδρύματα. Το ΕΠΕΠ καλύπτει όλους τους τύπους και όλα τα επίπεδα προσόντων και η χρήση μαθησιακών αποτελεσμάτων καθιστά σαφές τι γνωρίζει, τι κατανοεί και τι είναι σε θέση να κάνει ένα άτομο. Το επίπεδο αυξάνεται ανάλογα με το επίπεδο επάρκειας, το επίπεδο 1 είναι το χαμηλότερο και το 8 το υψηλότερο. Το σημαντικότερο είναι ότι το ΕΠΕΠ συνδέεται στενά με τα εθνικά πλαίσια επαγγελματικών προσόντων. Η σύνδεση αυτή του επιτρέπει να χαρτογραφεί όλους τους τύπους και τα επίπεδα προσόντων στην Ευρώπη, τα οποία καθίστανται όλο και περισσότερο προσβάσιμα με τη βοήθεια βάσεων δεδομένων για τα επαγγελματικά προσόντα.[1]
Εθνικό Πλαίσιο Προσόντων (ΕΠΠ) - National Qualifications Framework (NQF)	Τα Εθνικά Πλαίσια Προσόντων ταξινομούν τα προσόντα ανά επίπεδο, με βάση τα μαθησιακά αποτελέσματα. Αυτή η ταξινόμηση αντικατοπτρίζει το περιεχόμενο και το προφίλ των προσόντων - δηλαδή, τι αναμένεται να γνωρίζει, να κατανοεί και να είναι σε θέση να κάνει ο κάτοχος ενός πιστοποιητικού ή διπλώματος.[2]
GDPR	Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.[3]
Deep link	Ο όρος deep link αναφέρεται στη χρήση υπερσυνδέσμων οι οποίοι οδηγούν σε ένα συγκεκριμένο μέρος πληροφορίας ή περιεχομένου [4]

Πίνακας 8: Ορολογία EBSI

[1] https://europa.eu/europass/el/european-qualifications-framework-eqf

[2] https://www.cedefop.europa.eu/en/events-and-projects/projects/national-qualifications-framework-nqf

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

[4] https://en.wikipedia.org/wiki/Deep_linking

3.2 ESSIF & Notarisation of actions

3.2.1 ESSIF (European Self Sovereign Identity)

3.2.1.1 Η χρησιμότητα της Αυτοδύναμης ταυτότητας (SSI) για τους Ευρωπαίους Πολίτες

Με τον κανονισμό eIDAS, η Ευρώπη δημιούργησε πρόσφατα ένα ισχυρό πλαίσιο για την ψηφιακή ταυτότητα και τις υπηρεσίες εμπιστοσύνης. Έχοντας ως στόχο την εξασφάλιση ενός ικανοποιητικού επιπέδου ασφάλειας στα μέσα ηλεκτρονικής ταυτοποίησης και στις υπηρεσίες εμπιστοσύνης, το πρωτόκολλο eIDAS καθορίζει τους όρους αναγνώρισης των μέσων ηλεκτρονικής ταυτοποίησης φυσικών και νομικών προσώπων, οι οποίοι εντάσσονται σε σύστημα ψηφιακής ταυτοποίησης άλλου κράτους μέλους. Ορίζει κανόνες για τις υπηρεσίες εμπιστοσύνης με έμφαση στις ηλεκτρονικές συναλλαγές. Επίσης, ορίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές, τις ηλεκτρονικές σφραγίδες, τα ηλεκτρονικά έγγραφα και τις υπηρεσίες πιστοποιητικών για την επαλήθευση της ταυτότητας ιστοτόπων. Ενώ το eIDAS δίνει τη δυνατότητα στους πολίτες να χρησιμοποιούν τα διαπιστευτήριά τους σε όλα τα κράτη μέλη, δεν εξυπηρετεί τη χρήση περιπτώσεων που απαιτούν διαφοροποιημένα διαπιστευτήρια (credentials) ή εκείνων που προέρχονται εκτός των κρατών μελών της ΕΕ. Σε επίπεδο υποδομής, το eIDAS λειτουργεί ως μηχανισμός εναρμόνισης των κεντρικών συστημάτων ταυτότητας των κρατών μελών. [1,2]

Τα νέα χαρακτηριστικά πιστοποίησης του SSI, πέρα από τα χαρακτηριστικά ταυτότητας που παρέχει το eIDAS, μπορούν να γίνουν ένα εξαιρετικό συμπλήρωμα για τη διόρθωση των ελλιπών δυνατοτήτων των κυβερνήσεων και άλλων οργανισμών όσον αφορά την απόκτηση ψηφιακών επαληθευμένων δεδομένων σχετικά με τους πολίτες. Οι οργανισμοί χρειάζονται έγκυρα δεδομένα για χρήση τους σε διοικητικές ή επιχειρηματικές διαδικασίες για να αποφασίζουν εάν ένα αίτημα πρόκειται να εξυπηρετηθεί ή να απορριφθεί. Οι διαδικασίες δημόσιας υπηρεσίας παραμένουν σε επίπεδο τέτοιο όπου χρειάζονται πολύ χρόνο, παρουσιάζονται ξεπερασμένες και χαμηλής ποιότητας στους πολίτες και σε πολλές περιπτώσεις αυξάνουν τις δαπάνες των δημόσιων πόρων με την ανάγκη των δημοσίων υπαλλήλων να διαχειρίζονται αναποτελεσματικές, φυσικές διαδικασίες συμπλήρωσης φορμών και σάρωσης. Οι πολίτες εισέρχονται και εξέρχονται από πολλούς οργανισμούς (εκπαίδευση, απασχόληση, δήμος, πολιτεία κ.λπ.) κατά τη διάρκεια της ζωής τους και λαμβάνουν πιστοποιητικά από τον καθέναν οργανισμό, τα οποία απαιτούν διαχείριση. Από την άλλη όμως πλευρά, το όραμα της ΕΕ είναι να επιτρέπεται στον πολίτη τον ίδιο να διαχειρίζεται τα πιστοποιητικά του. Οι τρέχουσες πρακτικές IdM (Identity Management) οδηγούν τους πολίτες στο να μην έχουν τον έλεγχο της ανταλλαγής προσωπικών δεδομένων τους (δηλαδή ποιος το χρησιμοποιεί, για ποιο σκοπό και ούτω καθεξής). Το γεγονός αυτό οφείλεται στην έλλειψη αξιόπιστων και εύχρηστων εργαλείων διαχείρισης και ανταλλαγής προσωπικών δεδομένων για την επιβολή των δικαιωμάτων του πολίτη, όπως αυτό ορίζεται στο GDPR (General Data Protection Regulation). [140]

Ένα ενδιαφερόμενο μέρος, για την απόκτηση επαληθευμένων δεδομένων ενός πολίτη από ένα ψηφιακό σύστημα, πρέπει να δημιουργήσει και να διατηρήσει μια αξιόπιστη και ψηφιακά εξουσιοδοτημένη σύνδεση με την πηγή δεδομένων. Αυτό θα σήμαινε την υλοποίηση ενός point-to-point συστήματος, δηλαδή την ενοποίηση συστήματος από σημείο σε σημείο με πολύ διαφορετικές τεχνικές προσεγγίσεις και γραφειοκρατία για τη διευκόλυνση του συστήματος, ακόμη και μεταξύ τμημάτων μιας μεμονωμένης δημόσιας υπηρεσίας ή οργανισμού. Για πολλούς λόγους, δεν υπάρχει επιχειρηματική υπόθεση που να δικαιολογεί αυτήν την προσπάθεια. Υπάρχουν επίσης νομικοί περιορισμοί για την περαιτέρω

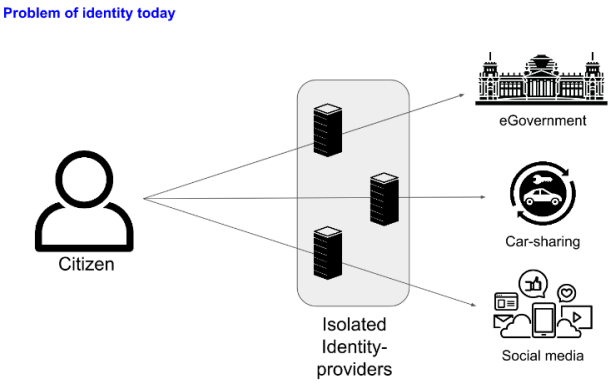
[1] http://www.aped.gov.gr/thesmiko-plaisio/eu-frame/18-topic/40-eidas.html
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text

χρήση των δεδομένων των πολιτών που συλλέγονται αρχικά για έναν νομικά καθορισμένο σκοπό από κυβερνητικές οργανώσεις. [1]

Διαμέσου της μίμησης των μοντέλων συναλλαγών βεβαίωσης του φυσικού κόσμου, το SSI επιτρέπει στους πολίτες να παρουσιάζουν και να χρησιμοποιούν ψηφιακές βεβαιώσεις κυβερνητικού επιπέδου οπουδήποτε θέλουν, χωρίς να εμπλέκουν τις κυβερνήσεις, οι οποίες ενδεχομένως να πρέπει να επενδύσουν σε υλικό και λογισμικό για να υποστηρίξουν τους πολίτες τους. Επιτρέπει στους πολίτες - καθώς και στους μη κατοίκους της ΕΕ - να παρέχουν στις κυβερνήσεις βεβαιώσεις τόσο από κυβερνητικούς όσο και από μη κυβερνητικούς οργανισμούς, όπως τράπεζες, ΜΚΟ, εταιρείες κοινής ωφέλειας, φορείς εκμετάλλευσης κινητής τηλεφωνίας, εκδότες αδειών, κ.λπ. Το μοντέλο SSI επιτρέπει σε κυβερνητικούς φορείς και άλλους παρόχους υπηρεσιών να έχουν πολύ μεγαλύτερη διαβεβαίωση ότι οι πολίτες είναι, για παράδειγμα επιλέξιμοι για συγκεκριμένο ζητούμενο-υπηρεσία (π.χ πρόνοια, παροχές υγείας, πρόσβαση σε συστήματα πληροφορικής) ή για το αν επιτρέπεται να ενεργούν σε νομοθετικά κατοχυρωμένο επάγγελμα ή θέση (π.χ. ιατρός, δικηγόρος, οδηγός φορτηγού για επικίνδυνα φορτία κ.λπ.). Το SSI υποστηρίζει την ένταξη των πολιτών, όπως για παράδειγμα μεταναστών που επιδιώκουν ένταξη στην κοινωνία της ΕΕ, καθώς οι πολίτες δεν χρειάζεται πλέον να γνωρίζουν τι τους ζητείται καθώς συμπληρώνουν μια φόρμα, πού να λάβουν τις πληροφορίες και πώς να γνωρίζουν ότι οι πληροφορίες που παρέχουν είναι σωστές. Επιπλέον, οι πολίτες δεν χρειάζεται πλέον να επισκέπτονται φυσικά μέρη για να συλλέγουν δεδομένα (π.χ. σε ιατρικό ειδικό ή δημοτικό γραφείο) που είναι δύσκολο για άτομα με ορισμένες αναπηρίες και περιορισμούς, και επίσης αποτελεί μία χρονοβόρα διαδικασία. [141]

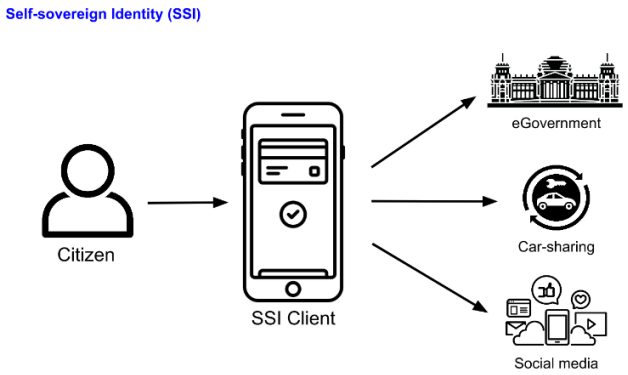
Το μοντέλο υποδομής του SSI

Σε ένα μοντέλο δεδομένων υποδομής SSI, κάθε φορά που οι ταυτότητες και τα σχετικά χαρακτηριστικά πρέπει να συνδέονται για μια διαδικασία, αυτή η σύνδεση πρέπει να γίνεται αποδεκτή από το μέρος του οποίου τα δεδομένα ταυτότητας πρόκειται να συνδεθούν, δηλαδή του πολίτη (Εικόνα 23), μέσω μιας εφαρμογής Wallet. Με αυτόν τον τρόπο, τα δεδομένα δεν μπορούν να συνδεθούν χωρίς ενεργή συμμετοχή του εκπροσωπούμενου μέρους, σε αντίθεση με τα συστήματα ομόσπονδης διαχείρισης ταυτότητας που υπάρχουν σήμερα (Εικόνα 22).[141]



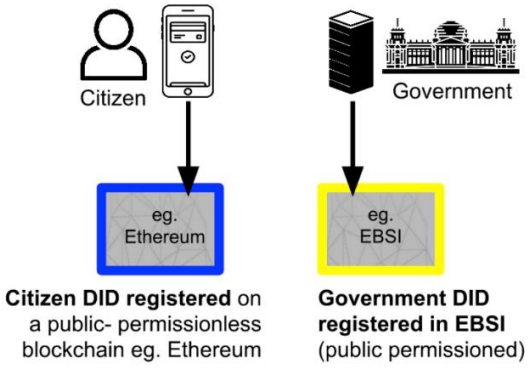
Εικόνα 22: Οι μεμονωμένοι πάροχοι ταυτότητας μπορούν να επιτύχουν διαλειτουργικότητα μόνο μέσω της ομοσπονδίας [141]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text



Εικόνα 23: Το αυτόνομο μοντέλο ταυτότητας με την κοινή χρήση χαρακτηριστικών ταυτότητας ελέγχεται από το SSI Client, που ελέγχεται μόνο από τον πελάτη (υποκείμενο δεδομένων). [1]

Η παραχώρηση στους πολίτες του ελέγχου της ταυτότητάς τους απαιτεί να γίνουν ιδιοκτήτες και κάτοχοι των ιδιωτικών κρυπτογραφικών κλειδιών τους, τα οποία απαιτούνται κατά την υπογραφή βεβαιώσεων ταυτότητας προς τους νόμιμους παραλήπτες τους. Τα μέσα για τη διαχείριση αυτού έχουν τη μορφή μιας εφαρμογής πορτοφολιού ταυτότητας (δηλαδή του SSI Client). Τα κρυπτογραφικά κλειδιά δεν είναι ορατά για τους πολίτες, αλλά αποτελούν τη βασική ασφάλεια πίσω από τις εσωτερικές λειτουργίες του SSI του πορτοφολιού (Wallet) που απαιτείται για την άσκηση ελέγχου δεδομένων ταυτότητας. Καθώς η κατοχή αυτών των κλειδιών σε μια προσωπική συσκευή θα αποτελούσε σημαντική ευθύνη για τον πολίτη, οποιεσδήποτε λύσεις SSI που χρησιμοποιούνται πρέπει να παρέχουν ταυτόχρονα εύκολους και αξιόπιστους μηχανισμούς δημιουργίας αντιγράφων ασφαλείας για την ανάκτηση των κλειδιών (π.χ. σε περίπτωση απώλειας ή καταστροφής μιας έξυπνης συσκευής).[142]



Εικόνα 24: Η καταχώριση των αναγνωριστικών μπορεί να διαφέρει, με βάση την οντότητα που αντιπροσωπεύεται. Τα DID των πολιτών μπορεί να μην χρειάζεται να εγγραφούν σε ένα δημόσιο blockchain.[142]

Το SSI επιτρέπει την αποσύνδεση της απόκτησης αναγνωριστικών (identifiers) από την πράξη έκδοσης εμπιστοσύνης. Η έκδοση εμπιστοσύνης εξακολουθεί να υπόκειται στον πάροχο εμπιστοσύνης (γνωστός και ως εκδότης – Issuing Service) που μπορεί να εκδίδει διαπιστευτήρια και βεβαιώσεις στο αναγνωριστικό μιας οντότητας. Ένας κάτοχος διαπιστευτηρίων μπορεί αργότερα να χρησιμοποιήσει αυτό το διαπιστευτήριο με διαφορετικούς επαληθευτές, με δική του βούληση και ανεξάρτητα από τον εκδότη.[142]

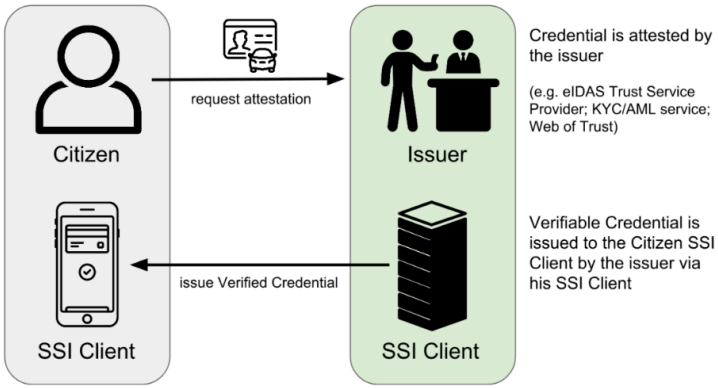
Ενώ τα πρωτόκολλα SSI διασφαλίζουν τεχνική διαλειτουργικότητα σε διαφορετικά δίκτυα, τα χρησιμοποιούμενα πλαίσια εμπιστοσύνης (π.χ. eIDAS ή Web of Trust) παρέχουν το καθένα

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text

τις δικές τους εγγυήσεις σχετικά με τη σημασία και την ορθότητα των αντιπροσωπευόμενων δεδομένων. Ένας κάτοχος του πορτοφολιού (Wallet) μπορεί να λάβει ένα επαληθεύσιμο πιστοποιητικό (Verifiable Credential) που έχει εκδοθεί από κάποιο ενδιαφερόμενο μέρος, το οποίο συνδέεται με το γνωστό DID του κατόχου - ή άλλο κομμάτι δεδομένων που ελέγχεται από τον κάτοχο- με το εκδοθέν διαπιστευτήριο (από μέρους του εκδότη). Με βάση το πλαίσιο εμπιστοσύνης που βασίζεται σε μια συγκεκριμένη περίπτωση χρήσης, αυτό μπορεί να απαιτεί ο εκδότης (συνήθως ένας οργανισμός, όχι πολίτης) να είναι «αγκυροβολημένος» σε ένα συγκεκριμένο αποκεντρωμένο δίκτυο. Όσον αφορά τον παραλήπτη των διαπιστευτηρίων, αυτή η εξάρτηση δεν απαιτείται. Η ακριβής χαρτογράφηση των αναγνωριστικών (DID) και των επαληθεύσιμων διαπιστευτηρίων εξακολουθεί να αποτελεί αντικείμενο συζητήσεων, καθώς διαφορετικές αρχιτεκτονικές προσφέρουν διαφορετικές προσεγγίσεις για την επίτευξη προστασίας δεδομένων.[1]

Ένα παράδειγμα μιας διαδικασίας έκδοσης περιγράφεται παρακάτω στην Εικόνα 25. Ο πολίτης πιστοποιείται (authentication) και ζητά βεβαίωση της άδειας οδήγησης με τη μορφή Επαληθεύσιμης Διαπίστευσης από την Υπηρεσία Εκδόσεων Πιστοποιητικών (Υπηρεσία Εμπιστοσύνης) της κυβερνητικής υπηρεσίας που διατηρεί μητρώο τέτοιων αδειών. Η Υπηρεσία Έκδοσης (Issuing Service) θα μπορούσε να είναι μια Πιστοποιημένη υπηρεσία εμπιστοσύνης eIDAS ή μια απλή υπηρεσία στο Διαδίκτυο. Με βάση την επιτυχή (και επαρκή) πιστοποίηση του Πολίτη και τον εσωτερικό έλεγχο της άδειας οδήγησης, μπορεί να χορηγηθεί βεβαίωση (εάν δεν έχει ανακληθεί ή δεν υπάρχει καθόλου) δεδομένου ότι η Υπηρεσία-Εκδότης παρέχει στον πολίτη ένα verifiable credential που κρυπτογραφικά προσδιορίζει τον Εκδότη ως μη αξιόπιστη πηγή της βεβαίωσης (το Επαληθεύσιμο Πιστοποιητικό – Verifiable Credential- περιέχει το DID του Εκδότη). [143]

Έτσι, ο πολίτης μπορεί τώρα να χρησιμοποιήσει αυτό το επαληθεύσιμο πιστοποιητικό σε κάθε αλληλεπίδραση όπου ένα τρίτο μέρος, ένας επαληθευτής (Verifier), ζητά απόδειξη α) κατοχής του συγκεκριμένου τύπου διαπιστευτηρίων και β) ότι ο επαληθευτής (Verifier) αποδέχεται το πλαίσιο εμπιστοσύνης του αντίστοιχου Εκδότη (Issuer). Οι πολίτες μπορούν να χρησιμοποιήσουν τις εφαρμογές Wallet για να διαχειριστούν και να αποθηκεύσουν ένα ευρύ φάσμα διαπιστευτηρίων. Τα διαπιστευτήριά τους μπορούν να χρησιμοποιηθούν όχι μόνο σε μία αλληλεπίδραση, αλλά και να επαναχρησιμοποιηθούν σε άλλα περιβάλλοντα (π.χ. ως πελάτης μιας επιχείρησης). [143]



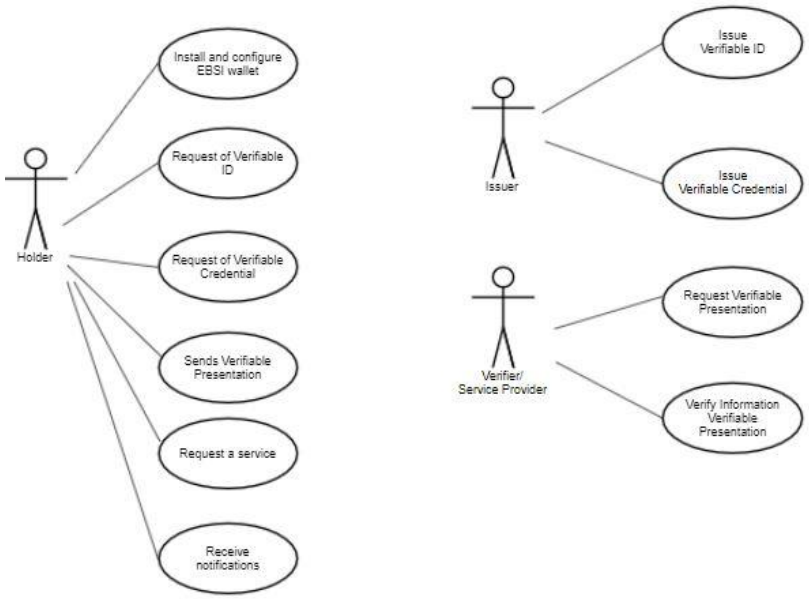
Εικόνα 25: Παράδειγμα πιστοποίησης του πολίτη και της ακόλουθης έκδοσης επαληθεύσιμης πιστοποίησης.[143]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+Orientation+Vision+Text

3.2.1.2 Γενική Περίπτωση Χρήσης του ESSIF

3.2.1.2.1 Use Case View

Το Ευρωπαϊκό Πλαίσιο Αυτοδύναμης Ταυτότητας (ESSIF) στοχεύει στην ανάπτυξη προτύπων και λειτουργικότητας για να επιτρέψει στους Ευρωπαίους πολίτες και στα ιδρύματα να αξιοποιήσουν μια πραγματική ψηφιακή ταυτότητα που βρίσκεται υπό τον έλεγχο του κατόχου της. Εντός του EBSI V1 (Version 1), η βασική λειτουργικότητα του ESSIF αναπτύσσεται και ευθυγραμμίζεται με το πορτοφόλι EBSI έτσι ώστε να υπάρχει μια αξιοποιήσιμη επαληθεύσιμη πιστοποίηση και δυνατότητα παρουσίασης, που υποστηρίζεται από ένα ασφαλές προσωπικό αναγνωριστικό GDPR και μια υποδομή ιδιωτικού / δημόσιου κλειδιού. Το κεφάλαιο αυτό περιγράφει την επισκόπηση του γενικού σεναρίου χρήσης του ESSIF. Το σύμβολο V1 συμβολίζει την πρώτη έκδοση του EBSI (Version 1), το V2 συμβολίζει τη δεύτερη έκδοση (Version 2), και το V2+ συμβολίζει μεταγενέστερες εκδόσεις. [1]



Εικόνα 26: Η προβολή της γενικής περίπτωσης χρήσης επιτρέπει την κατανόησή της οπτικά. Επισημαίνονται οι ενέργειες του κάθε ρόλου στο σενάριο χρήσης, οι οποίες εξηγούνται και στη συνέχεια.[144]

Οι ειδικοί όροι του ESSIF έχουν εξηγηθεί στον

Self-Sovereign Identity (SSI) – «Αυτοδύναμη Ταυτότητα»	Η αυτοδύναμη ταυτότητα – Self-Sovereign Identity βασίζεται στην ιδέα ότι ο χρήστης πρέπει να είναι αυτός που διαχειρίζεται την ταυτότητα του. Ο χρήστης πρέπει να έχει την δυνατότητα να χρησιμοποιεί την ταυτότητα του σε πολλαπλά σημεία, και να έχει τον πλήρη έλεγχο της. Συνεπώς μια τέτοια ταυτότητα θα πρέπει να είναι μεταφέρσιμη. Επίσης θα πρέπει να επιτρέπει στο χρήστη να προβεί σε αξιώσεις-ισχυρισμούς (claims).
Subject-Υποκείμενο	Ο όρος υποκείμενο αναφέρεται σε οποιαδήποτε υπαρκτή οντότητα. Στα πλαίσια που χρησιμοποιείται ο όρος, πρέπει να είναι εφικτή η αναφορά στη συγκεκριμένη οντότητα με την έννοια ότι μπορεί να αναγνωριστεί μοναδικά.[127]
(Digital) identity – (Ψηφιακή) ταυτότητα	(Ψηφιακή) ταυτότητα είναι το σύνολο των χαρακτηριστικών/δηλώσεων/ιδιοτήτων που επιτρέπουν την αναγνώριση μιας οντότητας.[127]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

Verifiable Credential (VC)	Ένα επαληθεύσιμο διαπιστευτήριο, που μπορεί να επαληθευτεί κρυπτογραφικά. Μπορεί να χρησιμοποιηθεί για τη δημιουργία επαληθεύσιμων παρουσιάσεων (Verifiable Presentations). Αποτελεί έναν «ισχυρισμό» όπως εξηγείται και στον επόμενο όρο. [127,]
Claim – Ισχυρισμός	Με τον όρο «ισχυρισμός» αναφερόμαστε στο αντικείμενο που αναπαριστά ένα σύνολο χαρακτηριστικών ή κάποια δήλωση μιας οντότητας. Δύο εξειδικεύσεις ισχυρισμών που αναφέρονται στα πλαίσια της διπλωματικής είναι α) Verifiable Claim, που αποτελεί έναν «ισχυρισμό» που η εγκυρότητα, η ακεραιότητα και η γνησιότητα του μπορούν να επαληθευτούν και από άλλα μέρη εκτός του μέρους που τον δημιουργεί, β) Verifiable Credential «επαληθεύσιμο διαπιστευτήριο», που αποτελεί έναν ισχυρισμός σύμφωνα με το W3C verifiable Credential standard. [127,128]
DID (Decentralized Identifier)	Τα αποκεντρωμένα αναγνωριστικά (DIDs) είναι ένας νέος τύπος αναγνωριστικού που επιτρέπει την επαληθεύσιμη, αποκεντρωμένη ψηφιακή ταυτότητα. Ένα DID προσδιορίζει οποιοδήποτε θέμα (π.χ. ένα άτομο, οργανισμό, μοντέλο δεδομένων, αφηρημένη οντότητα κ.λπ.) που ο υπεύθυνος επεξεργασίας του DID αποφασίζει ότι προσδιορίζει. Σε αντίθεση με τα τυπικά, ενοποιημένα αναγνωριστικά, τα DID έχουν σχεδιαστεί έτσι ώστε να μπορούν να αποσυνδεθούν από κεντρικά μητρώα, παρόχους ταυτότητας και αρχές έκδοσης πιστοποιητικών. Συγκεκριμένα, ενώ άλλα μέρη ενδέχεται να χρησιμοποιηθούν για να βοηθήσουν στην ανακάλυψη πληροφοριών που σχετίζονται με ένα DID και κατ' επέκταση τον κάτοχό του, ο σχεδιασμός επιτρέπει στον ελεγκτή ενός DID να αποδείξει ότι έχει τον έλεγχο του χωρίς να απαιτείται άδεια από οποιοδήποτε άλλο μέρος. Τα DIDs είναι URIs (Uniform Resource Identifiers) που συσχετίζουν για παράδειγμα έναν κάτοχο DID με ένα έγγραφο DID, το οποίο επιτρέπει αξιόπιστες αλληλεπιδράσεις που σχετίζονται με αυτόν τον κάτοχο. Κάθε έγγραφο DID μπορεί να εκφράζει κρυπτογραφικό υλικό, μεθόδους επαλήθευσης ή τα endpoints μιας υπηρεσίας, τα οποία παρέχουν ένα σύνολο μηχανισμών που επιτρέπουν σε έναν ελεγκτή DID να αποδείξει τον έλεγχο του DID. Τα endpoints μιας υπηρεσίας επιτρέπουν αξιόπιστες αλληλεπιδράσεις που σχετίζονται με τον κάτοχο του DID.
ESSIF digital ID	Μια ψηφιακή ταυτότητα (ακολουθούμενη και από το αντίστοιχο αναγνωριστικό) με την οποία μια οντότητα μπορεί να αναγνωριστεί στα πλαίσια του European Self-Sovereign Framework.[131]
Verifiable (digital) ID	Αποτελεί μία ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» (verifiable credential) που επιτρέπει όχι μόνο την αναγνώριση μίας οντότητας αλλά επίσης και την πιστοποίησή της. Μπορεί να το παρουσιάσει μια οντότητα ως απόδειξη του ποιος είναι (συγκρίσιμο με διαβατήριο, δελτίο ταυτότητας κ.λπ.).
Verifiable attestation – Επαληθεύσιμη Βεβαίωση	Η επαληθεύσιμη βεβαίωση είναι μια ειδική μορφή ενός «επαληθεύσιμου διαπιστευτηρίου» που μπορεί να προβάλει μια οντότητα ως απόδειξη ορισμένων ιδιοτήτων ή ως απόδειξη άδειας / βεβαίωσης / εξουσιοδότησης που έχει λάβει, με τη διαφορά όμως ότι δεν χρησιμοποιείται για την πιστοποίηση της οντότητας.
Verifiable Consent/Mandate (VC)-Επαληθεύσιμη Συγκατάθεση/Εντολή	Ειδική μορφή διαπιστευτηρίου που επιτρέπει στον κάτοχο να παρουσιάζεται σε τρίτο μέρος με διαπιστευτήρια και εντολή (και βεβαιώσεις σχετικά με ένα αντίστοιχο θέμα).[131]
Verifiable presentation	Με τον όρο verifiable presentation αναφερόμαστε στα δεδομένα που μεταβιβάζονται από μια οντότητα σε ένα εμπιστευτικό μέρος (που συχνά είναι το μέρος που επαληθεύει τα δεδομένα).[131]
Verifiable Supporting Docs	Οποιοσδήποτε τύπος «παραρτημάτων» στα οποία αναφέρονται τα επαληθεύσιμα διαπιστευτήρια. [130]

eIDAS	Ο κανονισμός (EU) N°910/2014 για τις υπηρεσίες ηλεκτρονικής αναγνώρισης και πιστοποίησης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.[131]
Registry (Μητρώο Εγγραφών)	Μια υπηρεσία notarisation στο blockchain είναι ουσιαστικά ένα στατικό μητρώο που αποθηκεύει αμετάβλητα δεδομένα αναφοράς που μπορούν να χρησιμοποιηθούν σε μεταγενέστερο στάδιο ως απόδειξη γνησιότητας / ακεραιότητας των ψηφιακών αντικειμένων. Αναφερόμαστε στο "Μητρώο" ως η εφαρμογή / σύστημα που θα προσφέρει τις υπηρεσίες συμβολαιογραφικής θεώρησης.
Document (Έγγραφο)	Ένα «έγγραφο» είναι οποιαδήποτε ψηφιακή πληροφορία, συμπεριλαμβανομένων αρχείων κειμένου, μηνυμάτων ηλεκτρονικού ταχυδρομείου, φωτογραφιών και βημάτων / συμβάντων επεξεργασίας, από ένα σύστημα πληροφοριών.[132]
NID (Notarisation Identifier)	Αναφορά σε notarisation.
eID	eID είναι ένα σύνολο υπηρεσιών που παρέχονται από την Ευρωπαϊκή Επιτροπή με στόχο την αναγνώριση των διαφορετικών σχημάτων ηλεκτρονικής αναγνώρισης (electronic identification schemes) των χρηστών ανά την Ευρώπη. Επιτρέπει στους ευρωπαίους πολίτες να χρησιμοποιούν τις εθνικές τους ηλεκτρονικές ταυτότητες κατά την πρόσβαση σε διαδικτυακές υπηρεσίες από άλλες ευρωπαϊκές χώρες.
Ευρωπαϊκό Πλαίσιο Επαγγελματικών Προσόντων (ΕΠΕΠ)- European Qualifications Framework (EQF)	Το ΕΠΕΠ αποτελεί ένα πλαίσιο με 8 επίπεδα αναφοράς που βασίζεται στα μαθησιακά αποτελέσματα για όλους τους τύπους των προσόντων. Χρησιμεύει ως μηχανισμός μετατροπής μεταξύ των διαφόρων εθνικών πλαισίων επαγγελματικών προσόντων. Συμβάλλει στη βελτίωση της διαφάνειας, της συγκρισιμότητας και της φορητότητας των επαγγελματικών προσόντων και καθιστά δυνατή τη σύγκριση προσόντων από διαφορετικές χώρες και ιδρύματα. Το ΕΠΕΠ καλύπτει όλους τους τύπους και όλα τα επίπεδα προσόντων και η χρήση μαθησιακών αποτελεσμάτων καθιστά σαφές τι γνωρίζει, τι κατανοεί και τι είναι σε θέση να κάνει ένα άτομο. Το επίπεδο αυξάνεται ανάλογα με το επίπεδο επάρκειας, το επίπεδο 1 είναι το χαμηλότερο και το 8 το υψηλότερο. Το σημαντικότερο είναι ότι το ΕΠΕΠ συνδέεται στενά με τα εθνικά πλαίσια επαγγελματικών προσόντων. Η σύνδεση αυτή του επιτρέπει να χαρτογραφεί όλους τους τύπους και τα επίπεδα προσόντων στην Ευρώπη, τα οποία καθίστανται όλο και περισσότερο προσβάσιμα με τη βοήθεια βάσεων δεδομένων για τα επαγγελματικά προσόντα.
Εθνικό Πλαίσιο Προσόντων (ΕΠΠ) - National Qualifications Framework (NQF)	Τα Εθνικά Πλαίσια Προσόντων ταξινομούν τα προσόντα ανά επίπεδο, με βάση τα μαθησιακά αποτελέσματα. Αυτή η ταξινόμηση αντικατοπτρίζει το περιεχόμενο και το προφίλ των προσόντων - δηλαδή, τι αναμένεται να γνωρίζει, να κατανοεί και να είναι σε θέση να κάνει ο κάτοχος ενός πιστοποιητικού ή διπλώματος.
GDPR	Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
Deep link	Ο όρος deep link αναφέρεται στη χρήση υπερσυνδέσμων οι οποίοι οδηγούν σε ένα συγκεκριμένο μέρος πληροφορίας ή περιεχομένου

Πίνακας 8.

3.2.1.2.2 Ρόλοι

Όρος	Ορισμός
Holder (Κάτοχος)	Ένα φυσικό πρόσωπο που επιθυμεί ένα προϊόν / υπηρεσία. Ως φυσικό πρόσωπο, είναι δυνατόν να εκπροσωπεί ένα νομικό πρόσωπο και να ενεργεί για λογαριασμό του.

Issuer (Εκδότης)	Ένα φυσικό ή νομικό πρόσωπο που είναι σε θέση να παρέχει ένα τέτοιο προϊόν ή υπηρεσία και να εκδίδει επαληθεύσιμα διαπιστευτήρια.
Verifier (Επιβεβαιωτής)	Ένα φυσικό ή νομικό πρόσωπο που είναι σε θέση να παρέχει ένα τέτοιο προϊόν ή υπηρεσία και χρειάζεται επαληθεύσιμες πληροφορίες για να παρέχει αυτήν την υπηρεσία.
Webservice (Υπηρεσία διαδικτύου – πάροχος)	Υλικό / λογισμικό που μπορεί να παρέχει το ζητούμενο προϊόν ή υπηρεσία ή μπορεί να ωθήσει άλλους φορείς να παρέχουν το ζητούμενο προϊόν ή υπηρεσία (π.χ. ιστότοπος).
Browser (Περιηγητής-ελεγχόμενος από κάτοχο)	Υλικό / λογισμικό που χρησιμοποιεί ο Αιτών για περιήγηση στο Διαδίκτυο και για επικοινωνία με τις διαδικτυακές υπηρεσίες διαφορετικών παρόχων (π.χ. τυπικό πρόγραμμα περιήγησης σε φορητό υπολογιστή ή τηλέφωνο).
Agent (Πράκτορας)	Μέρος υλικού / λογισμικού, συμμορφωμένο με ESSIF, που βοηθά τον ιδιοκτήτη του στη διεξαγωγή ψηφιακών συναλλαγών. Και οι δύο, ο Αιτών και ο Πάροχος διαθέτουν έναν Πράκτορα-Αντιπρόσωπο (Agent), τον οποίο ονομάζουμε «Πράκτορα-Αιτών» - “Agent Requester”- (π.χ. μια εφαρμογή σε κινητή συσκευή ή ένα plugin προγράμματος περιήγησης) και "Πράκτορα-Πάροχο"- “Agent Provider” (π.χ. διακομιστής μεσολάβησης-proxy server-για μια υπηρεσία Web).

Πίνακας 9: Ρόλοι ESSIF[1]

3.2.1.2.3 Δυνατότητες του χρήστη

3.2.1.2.3.1 Βασικές Δυνατότητες (Core Capabilities)

Σε αυτό το κεφάλαιο εξηγούνται οι δυνατότητες που είναι μοναδικές και απολύτως απαραίτητες σε αυτή τη γενική περίπτωση χρήσης.

I. Ο Κάτοχος (Holder) εγκαθιστά και διαμορφώνει το Wallet (V1)

Ρόλος : Κάτοχος (Holder)

Ιστορικό : Για να μπορέσει κάποιος να χρησιμοποιήσει το ESSIF, η πρώτη προϋπόθεση είναι να αποκτήσει τα πιο βασικά εργαλεία που συμμορφώνονται με αυτό. Οι χρήστες - συνήθως στους ρόλους τους ως «Κάτοχοι»- πρέπει συνήθως να κατεβάσουν μια εφαρμογή στο τηλέφωνό τους ή σε άλλη συσκευή που μπορεί να χρησιμοποιηθεί ως αναπαράσταση στον «ψηφιακό κόσμο». Πιθανώς, στο μέλλον, ο χρήστης θα είναι σε θέση να επιλέξει μία από αυτές τις εφαρμογές από διαφορετικούς προμηθευτές. Ενώ όλες αυτές οι εφαρμογές θα έχουν την απαιτούμενη βασική λειτουργικότητα ESSIF, ενδέχεται να διαφέρουν στην εμφάνιση (π.χ. εμπειρία χρήστη, ασφάλεια κ.λπ.) και θα πρέπει να διαμορφωθούν ξεχωριστά (π.χ. για να διασφαλιστεί επαρκής έλεγχος πρόσβασης και ευθυγράμμιση με την επιθυμητή εμπειρία του χρήστη ή προτιμήσεις ασφάλειας και απορρήτου).

Στόχος : Ο στόχος είναι η απόκτηση ενός Πράκτορα (Agent) ESSIF.

Διαδρομή του χρήστη :

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

1. Μια ποικιλία εφαρμογών (Agent Requesters) διατίθεται στην αγορά.
2. Ο χρήστης επιλέγει, κατεβάζει και εγκαθιστά μια κατάλληλη εφαρμογή ESSIF (Agent Requester) σε μία συσκευή (π.χ smartphone).
3. Ο χρήστης ανοίγει / ξεκινά την εφαρμογή ESSIF και διαμορφώνει τις προτιμήσεις χρήστη και ασφάλειας.
4. Η διαμόρφωση της εφαρμογής που γίνεται για πρώτη φορά προκαλεί τη δημιουργία ιδιωτικού κλειδιού ρίζας ESSIF και την αποθήκευσή του στον ασφαλή «θύλακα» του κινητού του χρήστη.[1]

II. Onboarding (V1)

Ρόλοι : Κάτοχος (Holder) και Εκδότης (Issuer)

Ιστορικό : Ο κάτοχος έχει ήδη εγκαταστήσει και διαμορφώσει το πορτοφόλι (Wallet) EBSI.

Στόχος : Ο χρήστης έχει στόχο να αποκτήσει ένα Verifiable ID συνδεδεμένο με το DID του χρήστη.

Διαδρομή του χρήστη :

1. Ο χρήστης επισκέπτεται τον ιστότοπο της κυβέρνησης.
2. Ο ιστότοπος εμφανίζει ένα deep link.
3. Ο ιστότοπος απαιτεί ισχυρή πιστοποίηση (authentication).
4. Ο Κάτοχος επικυρώνει τον εαυτό του μέσω της εθνικής ηλεκτρονικής ταυτότητας (eID).
5. Η εφαρμογή (Agent Requester) και ο ιστότοπος (Agent Provider) δημιουργούν ασφαλή σύνδεση.
6. Η εφαρμογή ζητά την έκδοση του Verifiable ID.
7. Εκδίδεται Verifiable ID στον κάτοχο. Το Verifiable ID θα περιλαμβάνει μόνο χαρακτηριστικά eIDAS.
8. Το Verifiable ID αποθηκεύεται.
9. Ο κάτοχος λαμβάνει μια ειδοποίηση με το Verifiable ID .[146]

III. Αίτημα και έκδοση Verifiable Credential (Verifiable Attestation) (V1)

Ρόλοι : Κάτοχος (Holder) και Εκδότης (Issuer)

Ιστορικό : Ο κάτοχος διαθέτει πορτοφόλι (wallet) EBSI με Verifiable ID, μεταξύ άλλων πιθανών Verifiable Credentials αποθηκευμένων στο πορτοφόλι.

Στόχος : Ο κάτοχος στοχεύει να αποκτήσει μια νέα επαληθεύσιμη πιστοποίηση (Verifiable Credential).

Διαδρομή του χρήστη :

1. Ο κάτοχος επισκέπτεται τον ιστότοπο του Εκδότη και ζητά την έκδοση ενός Verifiable Credential .
2. Ο ιστότοπος εμφανίζει ένα deep link.
3. Ο κάτοχος κάνει κλικ στο deep link.
4. Ο εκδότης ζητά συγκεκριμένη απόδειξη της ταυτότητας του κατόχου και ζητά την παρουσίαση ορισμένων Verifiable Credentials.
5. Ο χρήστης ελέγχει τις ζητούμενες πληροφορίες (π.χ. eID) και τις εγκρίνει στην εφαρμογή.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

6. Δημιουργείται και κοινοποιείται το Verifiable Credential.
7. Οι πληροφορίες που παρουσιάζονται επαληθεύονται από τον εκδότη.
8. Ο εκδότης εκδίδει το Verifiable Credential.
9. Το Verifiable Credential («ψηφιακά υπογεγραμμένο διαπιστευτήριο») αποθηκεύεται (π.χ. στην εφαρμογή).
10. Ο κάτοχος λαμβάνει ειδοποίηση με το νέο Verifiable Credential.[1]

IV. Επαληθεύσιμη Παρουσίαση-Verifiable Presentation (V1)

Ρόλοι : Κάτοχος (Holder) και Επαληθευτής (Verifier).

Ιστορικό : Θεωρείται δεδομένο ότι υπάρχει κάτοχος και επαληθευτής με ταυτότητες ESSIF, με τα αντίστοιχα επαληθεύσιμα διαπιστευτήριά τους (Verifiable credentials).

Στόχος : Ο κάτοχος θέλει να αποκτήσει μια υπηρεσία και ο πάροχος υπηρεσιών χρειάζεται κάποιες πληροφορίες για να παρέχει την υπηρεσία.

Διαδρομή του χρήστη :

1. Ο χρήστης επισκέπτεται τον ιστότοπο του επαληθευτή (Verifier).
2. Ο ιστότοπος εμφανίζει ένα deep link.
3. Ο κάτοχος κάνει κλικ στον παρεχόμενο σύνδεσμο σε βάθος.
4. Ο επαληθευτής ζητά συγκεκριμένη απόδειξη της ταυτότητας του κατόχου και ζητά την παρουσίαση ορισμένων επαληθεύσιμων διαπιστευτηρίων.
5. Ο χρήστης ελέγχει τις ζητούμενες πληροφορίες (π.χ. eID) και εγκρίνει στην εφαρμογή.
6. Δημιουργείται και κοινοποιείται η επαληθεύσιμη παρουσίαση (Verifiable Presentation).
7. Η παρουσίαση επαληθεύεται από τον επαληθευτή (Verifier).[147]

3.2.1.2.3.2 Υποστηρικτικές δυνατότητες (Supporting Capabilities)

Αυτή η ενότητα περιέχει μη απαραίτητες δυνατότητες για τη γενική περίπτωση χρήσης που περιγράφτηκε παραπάνω. Περιλαμβάνει επιπλέον δυνατότητες ή δυνατότητες από άλλες περιπτώσεις χρήσης.

I. Offline Onboarding (V2+)

Ρόλοι : Τελικός χρήστης και Πάροχος υπηρεσιών (Service provider)

Ιστορικό : "Offline Onboarding" μέσω φυσικής ταυτοποίησης (authentication). Ο κάτοχος πηγαίνει φυσικά σε κυβερνητικό γραφείο.

Στόχος : Ο στόχος του χρήστη είναι να δημιουργήσει μια ταυτότητα στο σύστημα.

Διαδρομή του χρήστη :

1. Ο χρήστης επισκέπτεται ένα κυβερνητικό γραφείο και ζητά την έκδοση ταυτότητας ως Verifiable Credential (VC).
2. Ο δημόσιος υπάλληλος ταυτοποιεί τον χρήστη (π.χ. έγκυρο διαβατήριο ή άλλου είδους ταξιδιωτικό έγγραφο) και παρουσιάζει ένα deep link.
3. Ο χρήστης συνδέει την εφαρμογή της (Agent Requester) με την κυβέρνηση (Agent Provider) μέσω ενός deep link. Η εφαρμογή της βρίσκει το τελικό σημείο όπου ο κυβερνητικός πράκτορας εκδίδει VC και ο χρήστης ζητά ένα VC.
4. Πραγματοποιεί έκδοση Verifiable ID.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

5. Το Verifiable ID αποθηκεύεται (π.χ. στην εφαρμογή).[147]

II. Εγκατάσταση και διαμόρφωση ενός (Κυβερνητικού / Επιχειρησιακού) Πράκτορα-Παρόχου- "Agent Provider" (web service proxy) (V1)

Ρόλοι : Εκδότης και Επαληθευτής.

Ιστορικό : Οι κυβερνήσεις, οι επιχειρήσεις και άλλοι οργανισμοί (π.χ. η Ελληνική Κυβέρνηση, κάποιο Πανεπιστήμιο ή άλλο Εκπαιδευτικό Ίδρυμα) που θέλουν οι υπηρεσίες τους στο διαδίκτυο να γίνουν "ESSIF enabled", θα πρέπει να περάσουν από μια παρόμοια διαδικασία. Θα πρέπει επίσης να αποκτήσουν τα πιο βασικά εργαλεία που συμμορφώνονται με το ESSIF, τα οποία μπορούν να εγκαταστήσουν «παρακείμενα» στους δικούς τους υπάρχοντες διακομιστές ιστού (Agent Provider). Οι οργανισμοί θα πρέπει επίσης να δώσουν μεγαλύτερη προσοχή στις «πολιτικές τις οποίες διαβάζουν οι μηχανές», τις οποίες τα στοιχεία ESSIF θα απαιτήσουν για την αυτοματοποίηση και τον εξορθολογισμό των ψηφιακών διαδικασιών. Η δημιουργία και εγκατάσταση τέτοιων πολιτικών θα είναι μέρος της εγκατάστασης και της διαμόρφωσης των αντίστοιχων agent providers.

Στόχος : Ο στόχος του ελεγκτή / εκδότη είναι να αποκτήσει έναν πράκτορα ESSIF.

Διαδρομή του χρήστη :

1. Μια ποικιλία εφαρμογών (agent providers) για κυβερνήσεις και επιχειρήσεις (π.χ. διακομιστής μεσολάβησης για υπηρεσίες Web) είναι διαθέσιμες σε μια αγορά.
2. Η κυβέρνηση / επιχείρηση κατεβάζει και εγκαθιστά έναν agent provider.
3. Η κυβέρνηση / επιχείρηση διαμορφώνει την εφαρμογή (agent provider), για παράδειγμα θέτοντας επιχειρηματικές πολιτικές για αυτοματοποίηση / απλοποίηση διαδικασιών που σχετίζονται με υπηρεσίες και ρόλους. Η διαδικασία αυτή περιλαμβάνει τη δημιουργία ιδιωτικών κλειδιών και αποθήκευσή τους στο HSM (Hardware Security Module) σε διακομιστή που εκτελεί τον agent provider για την κυβέρνηση ή την επιχείρηση. Η μονάδα ασφάλειας υλικού (HSM) είναι μια φυσική υπολογιστική συσκευή που προστατεύει και διαχειρίζεται ψηφιακά κλειδιά, εκτελεί λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης για ψηφιακές υπογραφές, ισχυρό έλεγχο ταυτότητας και άλλες κρυπτογραφικές λειτουργίες.
4. Πραγματοποιείται μια καταχώριση / δημιουργία ενός (δημόσιου) DID σε ένα επιλεγμένο μητρώο -κατανεμημένο ημερολόγιο-DLT (π.χ. EBSI).
5. Πραγματοποιείται καταχώριση πιστοποιητικών που έχουν εκδοθεί με (τουλάχιστον μία) υπηρεσία καταλόγου διαπιστευτηρίων.
6. Η κυβέρνηση / επιχείρηση μπορεί να διαμορφώσει την ανάκληση και την αναστολή σε επιλεγμένες υπηρεσίες.
7. Η κυβέρνηση / επιχείρηση αποκτά μια ασφαλή αποθήκευση ορισμένων επαληθεύσιμων αναγνωριστικών -Verifiable IDs- που ενδέχεται να απαιτούνται σε μελλοντικές αλληλεπιδράσεις / συναλλαγές (π.χ. για διαπίστευση).[1]

III. Δημιουργία σύνδεσης για πρώτη φορά : Κάτοχος / Χρήστης <-> Εκδότης ή Επαληθευτής (V2 +)

Ρόλοι : Κάτοχος, Εκδότης, Επαληθευτής.

Ιστορικό : Προτού μπορέσει να δημιουργηθεί μια σύνδεση μεταξύ δύο μερών για πρώτη φορά, οι πράκτορές τους πρέπει να "εισαχθούν" (δηλαδή να δημιουργήσουν μια σχέση)

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

μεταξύ τους, έτσι ώστε να μπορούν να ανταλλάσσουν δεδομένα και να βρίσκουν ο ένας τον άλλο στο μέλλον. Ανάλογα με την περίπτωση χρήσης, ενδέχεται να μην είναι απαραίτητο για οποιοδήποτε μέρος να γνωρίζει ποιος εκπροσωπεί τον άλλο πράκτορα. Επί της ουσίας, αρκεί να γνωρίζουμε ότι οι πράκτορες έχουν "συναντηθεί" στο παρελθόν. Αυτό μοιάζει με αυτό που κάνουν οι εφαρμογές επαφών (δηλ. με την πληκτρολόγηση ενός αριθμού τηλεφώνου και τον καθορισμό κάποιου ονόματος ή συντομογραφίας, όταν πραγματοποιείται μια κλήση, η εφαρμογή επαφής γνωρίζει ότι υπήρξε σύνδεση πριν και μπορεί να δημιουργήσει αρχεία καταγραφής κ.λπ.).

Στόχος : Ο στόχος είναι η επίτευξη σύνδεσης σε έναν πάροχο υπηρεσιών για πρώτη φορά.

Διαδρομή του χρήστη :

1. Τα μέρη έχουν ήδη εγκαταστήσει και διαμορφώσει τους αντίστοιχους πράκτορές τους.
2. Ο κάτοχος επισκέπτεται το γραφείο ή τον ιστότοπο του εκδότη ή του επαληθευτή.
3. Ο Agent Requester ανακαλύπτει τα στοιχεία σύνδεσης του εκδότη ή του επαληθευτή κάνοντας κλικ σε ένα deep link σε έναν ιστότοπο.
4. Οι πράκτορες ανακαλύπτουν έγγραφο DID και το σχετικό endpoint (μέσω ανάλυσης DID).
5. Πραγματοποίηση αιτήματος σύνδεσης (δηλ. κοινή χρήση εγγράφου DID)
6. Απόκριση σύνδεσης (π.χ. μεταφορά ετικέτας παρόχου).
7. Αναγνώριση σύνδεσης.
8. Επικοινωνία μεταξύ πρακτόρων (μεταφορά πληροφοριών κρυπτογραφημένων με δημόσια κλειδιά).
9. Αποθήκευση νέας σχέσης (δηλαδή επαφή) με τον Εκδότη ή τον Επαληθευτή (χωρίς σχετική εμπιστοσύνη) στο πορτοφόλι.

Από τη στιγμή που τα μέρη έχουν δημιουργήσει μία σύνδεση μεταξύ των αντιπροσώπων-πρακτόρων τους, ο κάτοχος περιηγείται στην εφαρμογή και επιλέγει την επαφή που εμφανίζεται από την εφαρμογή (Agent Requester). Ο agent requester στέλνει ένα μήνυμα σε έναν άλλο πράκτορα (π.χ. Agent Provider) διασφαλίζοντας τη διαθεσιμότητα. Ο άλλος πράκτορας απαντά και έτσι πραγματοποιείται η επικοινωνία μεταξύ πρακτόρων (με κρυπτογραφημένα με δημόσια κλειδιά).[1]

IV. Αίτημα και Έκδοση Verifiable ID (ή βεβαίωσης - Attestation) με φυσική / εκτός σύνδεσης πιστοποίηση (Authentication) (V2 +)

Ρόλοι : Κάτοχος και Εκδότης.

Ιστορικό : Ο κάτοχος και ο εκδότης έχουν δημιουργήσει σχέση μεταξύ των «πρακτόρων» τους.

Στόχος : Ο στόχος του κατόχου είναι να αποκτήσει ένα Verifiable ID.

Διαδρομή του χρήστη :

1. Τα μέρη έχουν ήδη δημιουργήσει μια σύνδεση μεταξύ των αντιπροσώπων τους.
2. Ο κάτοχος επισκέπτεται το γραφείο του Εκδότη και ζητά Verifiable ID (ή βεβαίωση, VC).
3. Ο κάτοχος παρέχει τα απαιτούμενα αποδεικτικά ταυτότητας (π.χ. έγκυρο διαβατήριο) που ελέγχονται από την Κυβέρνηση / Επιχείρηση.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

4. Πραγματοποιείται σύνδεση μεταξύ πρακτόρων μέσω deep link. Η εφαρμογή (Agent Requester) βρίσκει το αντίστοιχο deep link όπου η κυβέρνηση / επιχείρηση (Agent Provider) εκδίδει VC και πραγματοποιεί ένα αίτημα: ο αντιπρόσωπος κάνει μια «προσφορά διαπιστευτηρίων» σχετικά με την ταυτότητα.
5. Δημιουργείται ασφαλής σύνδεση μεταξύ των αντιπροσώπων. Ο Agent Provider κάνει μια προσφορά VC.
6. Ο κάτοχος ζητά μια έκδοση επαληθεύσιμης πιστοποίησης VC (επαληθεύσιμη βεβαίωση) μέσω της εφαρμογής (agent requester).
7. Ο Agent Provider εκδίδει το VC.
8. Το VC αποθηκεύεται.[1]

V. **Αίτημα προϊόντος / υπηρεσίας και Παρουσίαση αιτήματος και κατασκευής (και έκδοση VC) – εντός εφαρμογής.**

Ρόλοι : Κάτοχος, Επαληθευτής, Εκδότης.

Ιστορικό : Ο κάτοχος και ο επαληθευτής έχουν διαμορφώσει το πορτοφόλι EBSI, το οποίο λειτουργεί κανονικά.

Στόχος : Ο στόχος είναι η απόκτηση ενός Verifiable Credential και η πραγματοποίηση μιας παρουσίασης προκειμένου να αποκτήσει ο κάτοχος ένα προϊόν / υπηρεσία, αποκτώντας ένα νέο Verifiable Credential ως αποτέλεσμα της διαδικασίας.

Διαδρομή του χρήστη :

1. Ο επαληθευτής / εκδότης έχει καθορίσει την πολιτική με την οποία οι διακομιστές Web πρέπει να εγκρίνουν / να απορρίπτουν αιτήματα για προϊόντα / υπηρεσίες.
2. Ο κάτοχος ανοίγει / ξεκινά την εφαρμογή (Agent Provider).
3. Ο κάτοχος περιηγείται σε υπάρχουσες επαφές και επιλέγει έναν Επαληθευτή / Εκδότη.
4. Πραγματοποιείται η σύνδεση μεταξύ των αντιπροσώπων.
5. Ο κάτοχος ζητά ένα προϊόν / υπηρεσία.
6. Ο Επαληθευτής (agent provider) ζητά μια επαληθεύσιμη παρουσίαση (VP), για να αποφασίσει για την αποδοχή / απόρριψη του αιτήματος.
7. Ο αιτών πράκτορας δημιουργεί και μοιράζεται μια επαληθεύσιμη παρουσίαση (VP), συμπεριλαμβανομένων όλων των ζητούμενων δεδομένων.
8. Ο Επαληθευτής / Εκδότης (agent provider) επαληθεύει την παρουσίαση (VP) και εγκρίνει / απορρίπτει το αίτημα σύμφωνα με τις πολιτικές.
9. Ενδέχεται να ενεργοποιηθούν μεταγενέστερες διεργασίες (π.χ. Υπηρεσίες Web).
10. Ο Agent Provider μπορεί να εκδώσει ένα Verifiable Credential επιβεβαιώνοντας ορισμένες πληροφορίες (π.χ. τη συναλλαγή).
11. Το VC αποθηκεύεται (π.χ. στην συσκευή).[150]

3.2.1.3 Ειδικές Περιπτώσεις Χρήσης του ESSIF

3.2.1.3.1 Ανάλυση Περιπτώσεων Χρήσης στο Δημόσιο Τομέα

Κάθε χώρα - ή κράτος μέλος της ΕΕ- προσφέρει ένα μοναδικό κοινωνικό, πολιτικό, νομικό, οικονομικό και τεχνολογικό περιβάλλον. Αυτές οι ρυθμίσεις μεμονωμένων κρατών δημιουργούν διαφορές ως προς τους κανονισμούς, τις πολιτικές προτεραιότητες, τα οικονομικά μέσα, τις υποδομές και τη δημιουργία οικονομικής αξίας. Λόγω αυτών των διαφορών, ορισμένες περιπτώσεις χρήσης του SSI είναι πιο σημαντικές και έχουν τη δυνατότητα να δημιουργήσουν μεγαλύτερη αξία για ορισμένες κυβερνήσεις και διοικήσεις,

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+User+Stories

παρά για άλλες. Επομένως, δεν είναι δυνατή η αναγνώριση ορισμένων περιπτώσεων χρήσης SSI ως κατάλληλες για κάθε κράτος. Λαμβάνοντας το γεγονός αυτό υπόψη, προσδιορίζονται πέντε περιπτώσεις χρήσης του SSI στο δημόσιο τομέα που φαίνεται να είναι υποσχόμενες για πολλές ευρωπαϊκές χώρες. Τα κριτήρια επιλογής βασίστηκαν σε διάφορους παράγοντες, όπως το κόστος, η ασφάλεια, η αποτελεσματικότητα των διαδικασιών, ζητήματα συμμόρφωσης, ο πιθανός αντίκτυπος στους πολίτες (δηλαδή ο αριθμός των ατόμων που επηρεάζονται και η συχνότητα της αντίστοιχης αλληλεπίδρασης) και βελτίωση της αλληλεπίδρασης των πολιτών (δηλ. ικανοποίηση πολιτών με την παροχή δημόσιων υπηρεσιών). Επιπλέον, αυτές οι περιπτώσεις χρήσης είναι πολύ σχετικές με μια σαφώς διακριτή ομάδα χρηστών που έχει την τάση να υιοθετεί νέες τεχνολογίες όπως το SSI λόγω της τεχνογνωσίας και της χαμηλής ανοχής για την απογοήτευση που σχετίζεται με τις δημόσιες διαδικασίες. Αυτή η ομάδα χρηστών είναι μαθητές. Παρουσιάζεται, λοιπόν, στα επιμέρους σενάρια χρήσης η διαδρομή μιας Ευρωπαίας υπηκόου, η οποία φοιτά και σε εκπαιδευτικό ίδρυμα υψηλού επιπέδου.[1]

Η φοιτήτρια είναι μια ευρωπαία πολίτης 25 ετών . Έχει γερμανική ιθαγένεια, όμως έχει ζήσει σε διαφορετικά κράτη-μέλη για διαφορετικούς λόγους στο καθένα. Επιθυμεί να αποκτήσει SSI (μέσω μιας εφαρμογής πορτοφολιού -wallet- ως διεπαφή χρήστη), προκειμένου να το χρησιμοποιήσει σε διάφορες περιπτώσεις χρήσης στο δημόσιο τομέα. Ο στόχος διαφέρει στα διαφορετικά σενάρια χρήσης.[151]

Διαδρομή του χρήστη (φοιτήτρια):

1. Set-up: Η φοιτήτρια «στήνει» την ψηφιακή της ταυτότητα με σκοπό να χρησιμοποιήσει το SSI στο μέλλον.
2. Authentication: Η φοιτήτρια πιστοποιεί τον εαυτό της απέναντι στην ψηφιακή πύλη (portal) του δημόσιου τομέα χρησιμοποιώντας το SSI.
3. Diplomas (1): Η φοιτήτρια κάνει αίτηση και λαμβάνει τα ψηφιακά της διπλώματα και τις πιστοποιήσεις.
4. Diplomas (2): Η φοιτήτρια ξαναχρησιμοποιεί το ψηφιακό της δίπλωμα προκειμένου να κάνει αίτηση σε άλλο πανεπιστήμιο ή σε κάποια θέση εργασίας.[151]

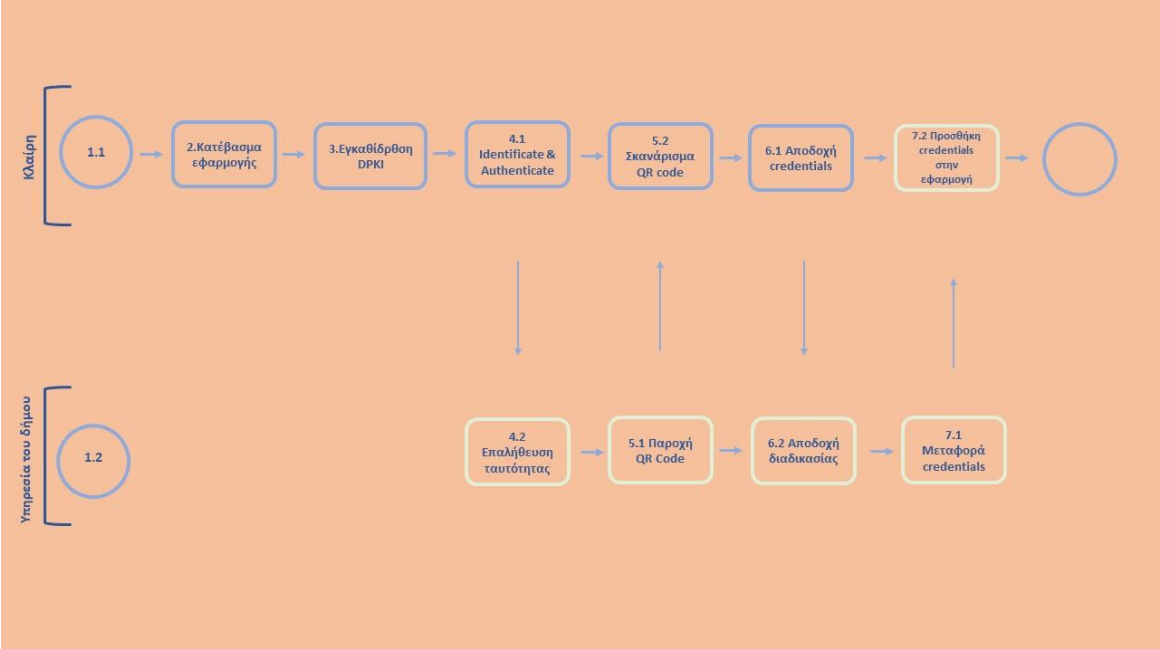
Setup-Digital Identity

- Οπτική-Στόχοι: Η φοιτήτρια επιθυμεί να «στήσει» την ταυτότητά της που θα βασίζεται στο SSI. Θα πρέπει να εγκαταστήσει μια εφαρμογή wallet, να δημιουργήσει μία ψηφιακή ταυτότητα και να την εμπλουτίζει με προσωπικές της πληροφορίες. Μπορεί να επιλέξει έναν από τους δύο τρόπους: online ή offline, όπως και στην ανάλυση της γενικής περίπτωσης χρήσης. Ο στόχος είναι η δημιουργία ενός DID και η εγκαθίδρυση ενός DPKI (Decentralized Public Key Infrastructure), η δημιουργία επαφής με άλλη οντότητα, και η λήψη και αποθήκευση των credentials.
- Εμπειρία του χρήστη:
    1. Κατέβασμα και «στήσιμο» -set up- της εφαρμογής SSI, μέσω επιλογών («κουμπιών») στην εφαρμογή
    2. Επίσκεψη στο γραφείο του Δήμου ή log in στη διαδικτυακή σελίδα του.
    3. Πιστοποίηση μέσω φυσικών εγγράφων ή μέσω βίντεο και «ανεβάσματος» αρχείων
    4. Επίτευξη σύνδεσης με το Δήμο (Issuer), μέσω link ή QR code
    5. Αποδοχή των ψηφιακών διαπιστευτηρίων
- Επιπλέον σχόλια : Στην περίπτωση που εμπλέκεται μία τέτοιου είδους αξιόπιστη οντότητα (όπως ένας δήμος), η πιστοποίηση μέσω επίσκεψης σε φυσικό γραφείο ή

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

μέσω της διαδικτυακής σελίδας είναι πολύ πιθανό να μην χρειαστεί να πραγματοποιηθεί ξανά, ύστερα από αυτή τη διαδικασία. Η σύνδεση πραγματοποιείται μέσω QR code.

- Διάγραμμα ροής :
  1.1: Η φοιτήτρια επιθυμεί να ταυτοποιηθεί χρησιμοποιώντας το SSI.
  1.2: Ο Δήμος διαθέτει την απαιτούμενη υποδομή SSI.
  3: Δημιουργείται ένα αναγνωριστικό, μία υποδομή αποκεντρωμένου δημόσιου κλειδιού, και αποθηκεύεται στη συσκευή το κρυπτογραφικό υλικό.[1]



Εικόνα 27: Διάγραμμα ροής για την απόκτηση ψηφιακής ταυτότητας με χρήση του SSI για μία Ευρωπαία πολίτη. Οι καταστάσεις με πράσινο περίγραμμα είτε είναι προαιρετικές, είτε συμβαίνουν στο παρασκήνιο χωρίς να τις πραγματοποιεί ο χρήστης.[152]

Authentication

Κάθε ευρωπαίος πολίτης φαίνεται να επηρεάζεται από αυτήν την περίπτωση χρήσης, επειδή όλοι οι πολίτες αλληλοεπιδρούν με την κυβέρνησή τους. Η εξάλειψη του αριθμού των διαφορετικών ονομάτων χρήστη, και κωδικών πρόσβασης που χρησιμοποιούνται σε αυτές τις επανειλημμένες περιπτώσεις και η αντικατάστασή τους με έναν ενιαίο, καθολικό, γρήγορο, εύκολο στη χρήση και ασφαλή τρόπο πρόσβασης σε όλους τους τύπους υπηρεσιών ηλεκτρονικής διακυβέρνησης έχει τη δυνατότητα να δημιουργήσει μια μεγάλη διευκόλυνση για τους πολίτες που μπορεί να επηρεάσουν σημαντικά τη συνολική αντίληψή τους για το SSI στο δημόσιο τομέα. Επιπλέον, σε σύγκριση με άλλες περιπτώσεις χρήσης, οι πολίτες έχουν πρόσβαση σε υπηρεσίες ηλεκτρονικής διακυβέρνησης σχετικά συχνά.[152]

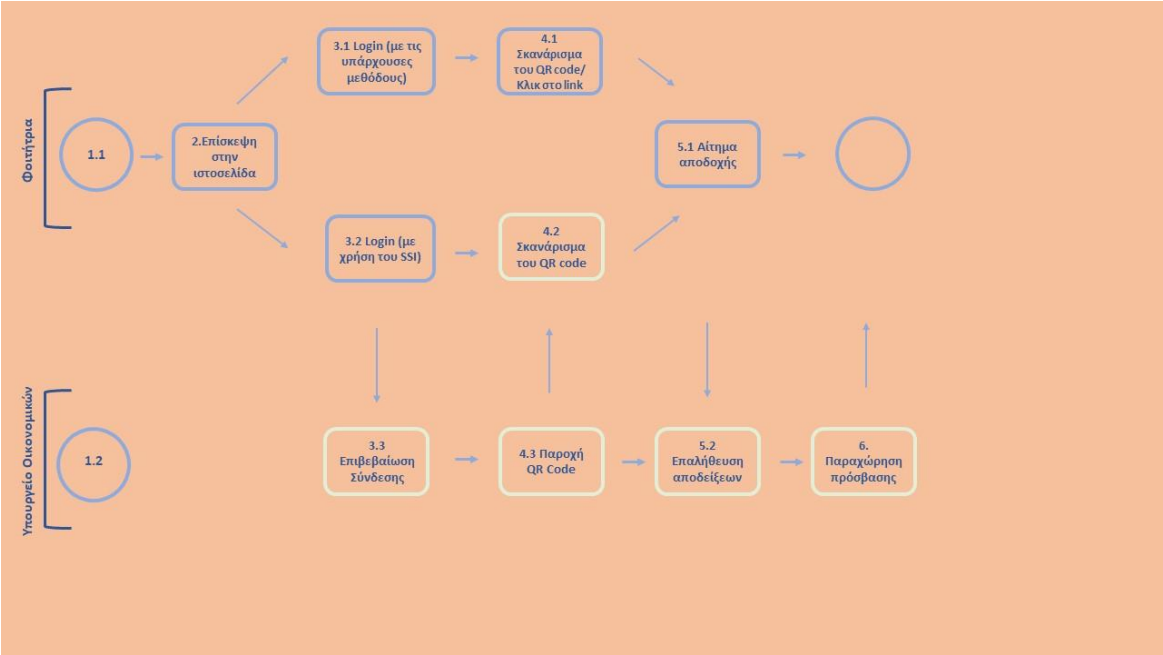
Οπτική-Στόχοι: Η φοιτήτρια επιθυμεί να πιστοποιείται (authenticate) απέναντι στις δημόσιες υπηρεσίες της ΕΕ και της Γερμανίας. Σε αυτήν την περίπτωση, επιθυμεί να έχει πρόσβαση στην «πύλη» (portal) του Υπουργείου Οικονομικών της Γερμανίας για να δημιουργήσει τη δική της επιχείρηση (π.χ. υποβολή βεβαίωσης από την εφορία). Έχει ήδη δημιουργήσει, όπως είδαμε στο προηγούμενο βήμα, την ψηφιακή της ταυτότητα. [152]

Διαδρομή του χρήστη:

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

1. Επίσκεψη στην ιστοσελίδα του Υπουργείου.
2. Login στην ιστοσελίδα του Υπουργείου Οικονομικών. Αντί για το παραδοσιακό login με τη χρήση username και password, γίνεται «κλικ» σε πεδίο με τίτλο «Login with SSI app». Πραγματοποιείται, δηλαδή, λειτουργία «Single sign-on (SSO)».[154] Πρόκειται για ένα σχήμα ελέγχου ταυτότητας που επιτρέπει σε έναν χρήστη να συνδεθεί με ένα μόνο αναγνωριστικό και κωδικό πρόσβασης σε οποιοδήποτε από τα πολλά σχετικά, αλλά ανεξάρτητα, συστήματα λογισμικού. Επιτρέπει στο χρήστη να συνδεθεί μία φορά και να αποκτήσει πρόσβαση σε υπηρεσίες χωρίς να εισαγάγει ξανά παράγοντες ελέγχου ταυτότητας. [1]
3. Σύνδεση με το Υπουργείο Οικονομικών. Προαιρετικά μπορεί να χρειάζεται το «σκανάρισμα» ενός QR code, στην περίπτωση που η διαδικασία δεν πραγματοποιείται στη συσκευή στην οποία είναι αποθηκευμένα τα σχετικά κλειδιά και αναγνωριστικά.
4. Δημιουργία επιπλέον αιτήματος προς το Υπουργείο Οικονομικών (προαιρετικό). Η διαδικασία του authentication μπορεί να πραγματοποιηθεί με βάση τα DIDs, εφόσον ο λογαριασμός είναι ήδη συνδεδεμένος με τα DIDs.[2]

Διάγραμμα ροής:



Εικόνα 28: Διάγραμμα ροής για τη διαδικασία του authentication με χρήση του SSI για μία Ευρωπαία πολίτη. Οι καταστάσεις με πράσινο περίγραμμα είτε είναι προαιρετικές, είτε συμβαίνουν στο παρασκήνιο χωρίς να τις πραγματοποιεί ο χρήστης.[154]

Diplomas & Educational Credentials

Οπτική-Στόχοι: Η φοιτήτρια έχει ένα Μεταπτυχιακό Δίπλωμα σπουδών (έχει σπουδάσει στην Ολλανδία και στην Αυστρία). Διαθέτει τα κατάλληλα αποδεικτικά έγγραφα σε μη επίσημη μορφή. Τώρα επιθυμεί να αποκτήσει τα πιστοποιητικά του μεταπτυχιακού της διπλώματος σε ψηφιακή μορφή και να τα ξαναχρησιμοποιήσει προκειμένου να πάρει μέρος σε ένα πρόγραμμα MBA μερικής απασχόλησης (στο Πανεπιστήμιο HEC στη Γαλλία) καθώς και να κάνει αίτηση σε μία μερικής απασχόλησης δουλειά σε μία γαλλική εταιρία. Έχει ήδη «στήσει»

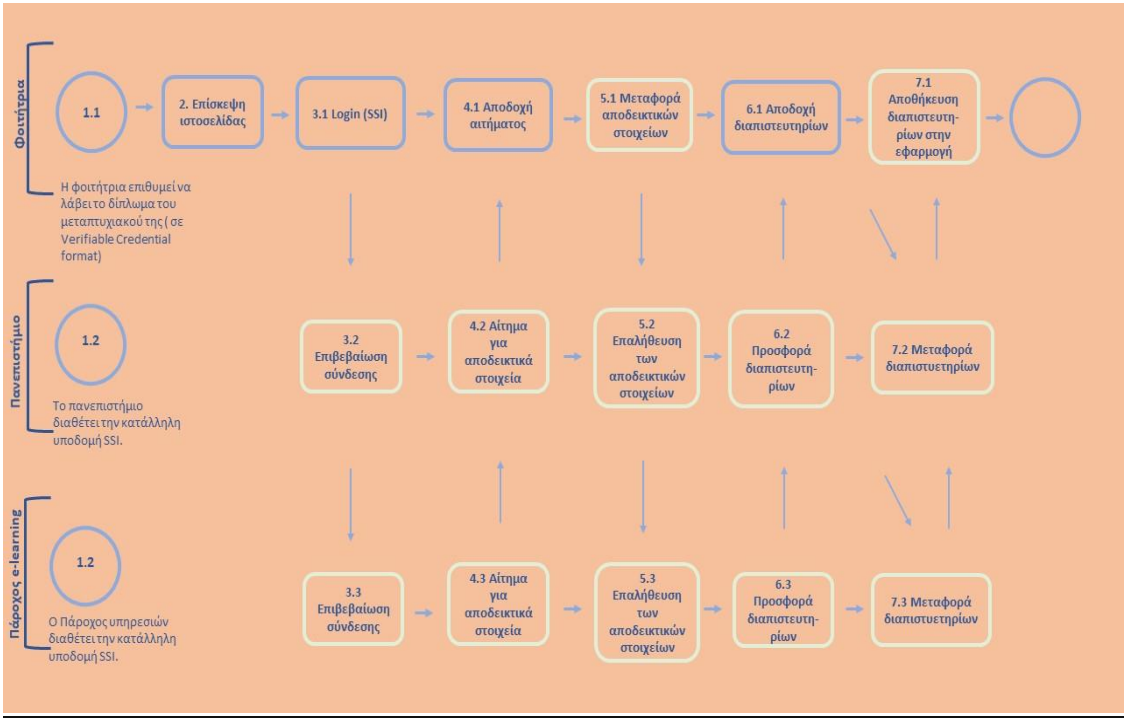
[1] https://en.wikipedia.org/wiki/Single_sign-on
[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

την ψηφιακή της ταυτότητα. Αρχικά στοχεύει να δημιουργήσει τη σύνδεση με τις (άλλες) οντότητες που την ενδιαφέρουν. Στη συνέχεια, επιθυμεί να λάβει και να αποθηκεύσει ένα credential (που πιστοποιεί το πρώτο μεταπτυχιακό της δίπλωμα). Έπειτα θέλει να μεταφέρει το αποδεικτικό αυτό στοιχείο (δίπλωμα) και να το επικυρώσει (valid diploma). Τέλος, αποθηκεύει τα διαπιστευτήρια στην εφαρμογή.[1]

Διαδρομή του χρήστη:

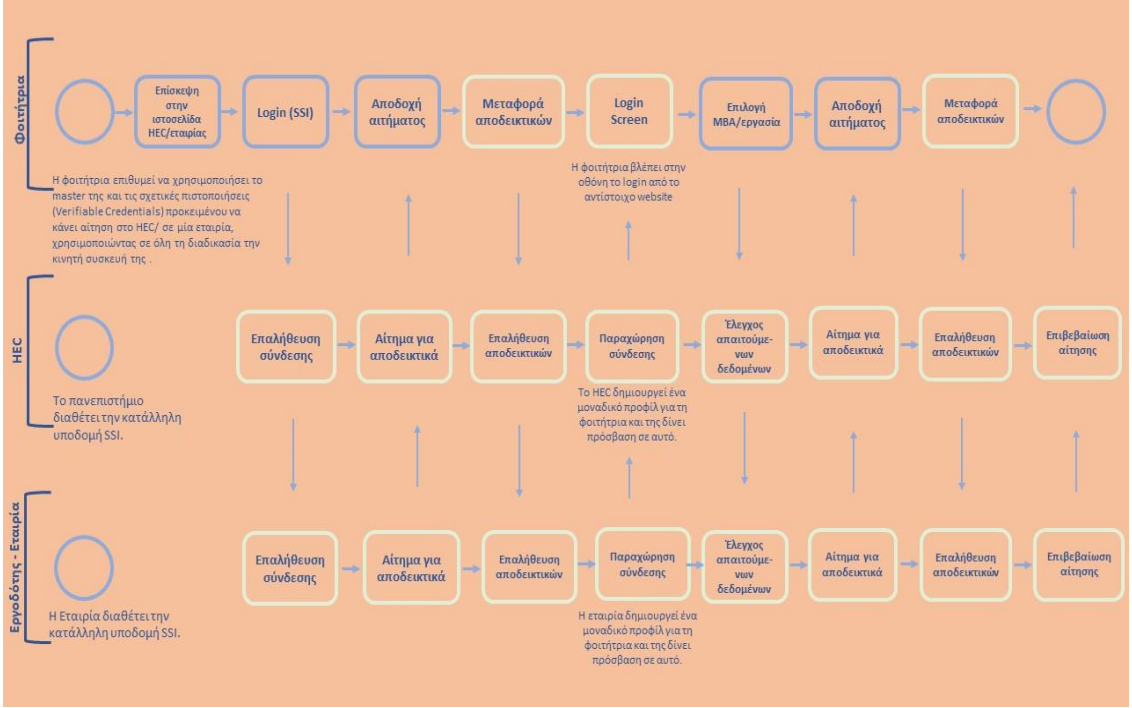
1. Login στην ιστοσελίδα του Παρόχου του Εκπαιδευτικού Ιδρύματος (service provider). Αντί για το παραδοσιακό login με τη χρήση username και password, γίνεται «κλικ» σε πεδίο με τίτλο «Login with SSI app». Πραγματοποιείται, δηλαδή, λειτουργία «Single sign-on (SSO)».
2. Σύνδεση με τον Πάροχο – Εκπαιδευτικό Ίδρυμα
3. Αποδοχή ψηφιακών διπλωμάτων (μέσω αντίστοιχου πεδίου στην εφαρμογή). Δεν απαιτείται επικοινωνία με τον πάροχο του εκπαιδευτικού ιδρύματος (τηλεφωνήματα, meetings) ή εκτύπωση έντυπων πιστοποιητικών.
4. Login στην ιστοσελίδα του πανεπιστημίου HEC – Login στην ιστοσελίδα της γαλλικής εταιρίας που επιθυμεί να υποβάλει αίτηση. Να σημειωθεί ότι μπορεί να απαιτούνται κάποια πιστοποιητικά για τη διαδικασία του authentication, ανάλογα με το επίπεδο διασφάλισης της υπηρεσίας.
5. Σύνδεση με το HEC – Σύνδεση με την εταιρία
6. Αποδοχή αιτήματος από το HEC - Αποδοχή αιτήματος από την εταιρία. [155]

Διαγράμματα ροής:



Εικόνα 29: Διάγραμμα ροής για τη διαδικασία της απόκτησης σε ψηφιακή μορφή διπλώματος και σχετικών αποδεικτικών (Verifiable Credentials) με χρήση του SSI για μία Ευρωπαία φοιτήτρια. Οι καταστάσεις με πράσινο περίγραμμα είτε είναι προαιρετικές, είτε συμβαίνουν στο παρασκήνιο χωρίς να τις πραγματοποιεί ο χρήστης.[155]

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

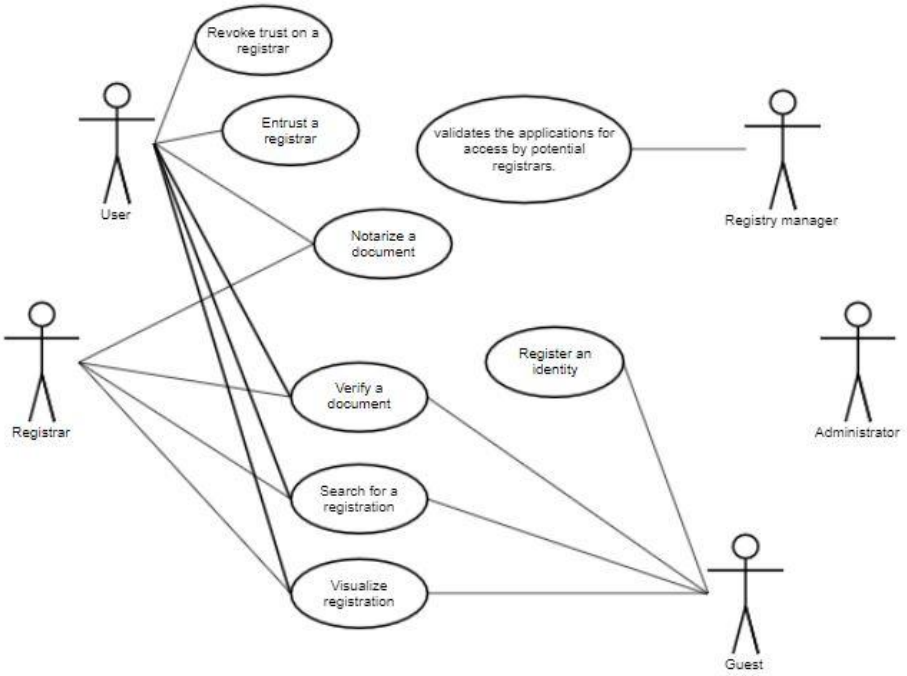


Εικόνα 30: Διάγραμμα ροής για τη διαδικασία αίτησης σε πανεπιστήμιο ή εργασία με χρήση του SSI για μία Ευρωπαία φοιτήτρια. Οι καταστάσεις με πράσινο περίγραμμα είτε είναι προαιρετικές, είτε συμβαίνουν στο παρασκήνιο χωρίς να τις πραγματοποιεί ο χρήστης.

3.2.2 Notarisation & Digital trail

Η υπηρεσία «Notarisation» επιτρέπει στους χρήστες την εγγραφή ψηφιακών εγγράφων, την επαλήθευση της αυθεντικότητάς τους και τη δημιουργία μιας ασφαλούς διαδρομής ελέγχου. Επίσης, επιτρέπει την εγγραφή και τη σύνδεση ψηφιακών αποτυπωμάτων (footprints) των αρχείων και των μεταδεδομένων τους. Δημιουργεί, ουσιαστικά, ένα digital trail. Ακόμη, επιτρέπει την αμφίδρομη ανταλλαγή ψηφιακών αποτυπωμάτων με τρίτα μέρη, με τρόπο συμβατό με το GDPR. Το κεφάλαιο αυτό περιγράφει την επισκόπηση του γενικού σεναρίου χρήσης του Notarisation.

3.2.2.1 Use Case View



Εικόνα 31 Η προβολή της γενικής περίπτωσης χρήσης επιτρέπει την κατανόησή της οπτικά. Επισημαίνονται οι ενέργειες του κάθε ρόλου στο σενάριο χρήσης, οι οποίοι εξηγούνται και στη συνέχεια. [1]

Οι ειδικοί όροι του ESSIF έχουν εξηγηθεί στον Πίνακας 8.

3.2.2.2 Ρόλοι

Μετά την εγγραφή (registry), οι χρήστες μπορούν να έχουν τους ακόλουθους ρόλους:

Όρος	Ορισμός
Χρήστης (User)	Μπορεί να είναι φυσικό ή νομικό πρόσωπο που μπορεί να εγγράψει (notarise) τα δικά του έγγραφα, να επαληθεύσει την αυθεντικότητα / ακεραιότητα του εγγράφου του και να περιηγηθεί στο δικό του ιστορικό εγγραφής.
Καταχωρητής (Registrar)	Συνήθως ένα δημόσιο ίδρυμα, αλλά επίσης πιθανώς μια λογιστική ή παρόμοια εταιρεία. Αυτός ο καταχωρητής έχει όλα τα δικαιώματα ενός χρήστη. Επιπλέον ένας καταχωρητής μπορεί να έχει πρόσβαση στις εγγραφές χρηστών, οι οποίοι έχουν δώσει τη ρητή συγκατάθεσή τους και να πραγματοποιήσει εγγραφή (notarisation) για λογαριασμό ενός χρήστη.
Διαχειριστής (Administrator)	Ένας διαχειριστής διαχειρίζεται τις «διαμορφώσεις» του συστήματος.
Διευθυντής του μητρώου εγγραφών (Registry Manager)	Ένας διευθυντής μητρώου επικυρώνει τις αιτήσεις πρόσβασης από πιθανούς καταχωρητές.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

Επισκέπτης (Guest)	Ένας επισκέπτης μπορεί να έχει πρόσβαση σε διαθέσιμες στο κοινό λειτουργίες.

Πίνακας 10: Ρόλοι notarisation.[1]

3.2.2.3 Δυνατότητες του χρήστη

3.2.2.3.1 Βασικές Δυνατότητες (Core Capabilities)

I. Βασική συμβολαιογραφική θεώρηση εγγράφου (V1)

Ρόλοι : Χρήστης

Ιστορικό : Ένας ελεγχόμενος έχει δημιουργήσει έγγραφα που ενδέχεται να σχετίζονται με μελλοντικούς ελέγχους (π.χ. τιμολόγιο, συμβόλαιο) και θέλει να τα ενημερώσει.

Στόχος : Να θεωρήσει συμβολαιογραφικά τα αρχεία που υπέβαλε ο χρήστης και να δημιουργήσει μια αξιόπιστη διαδρομή ελέγχου (audit trail).

Διαδρομή :

- Ο χρήστης αποθηκεύει τα αρχεία που πρέπει να θεωρηθούν συμβολαιογραφικά σε έναν χώρο αποθήκευσης εκτός αλυσίδας (π.χ. EBSI off-chain storage component)
- Ο χώρος αποθήκευσης είναι προσβάσιμος μέσω του component Ελέγχου -Audit Component-(περιπτώσεις χρήσης επιπέδου εφαρμογής -application layer- του EBSI).
- Ο χρήστης συνδέεται στο μητρώο με τα διαπιστευτήριά του.
- Ο χρήστης επιλέγει τα αρχεία που θέλει να θεωρηθούν συμβολαιογραφικά.

Στη συνέχεια, ο χρήστης ενεργοποιεί τη συμβολαιογραφική θεώρηση εγγράφου (notarisation). Το audit component παράγει τα hashes (τιμές κατακερματισμού) των εγγράφων και, στη συνέχεια, τα αποθηκεύει στην αλυσίδα. Η συμβολαιογραφική θεώρηση ενός αρχείου είναι δυνατή μέσω του audit component (διαδικτυακή εφαρμογή) και μέσω ενός αποκλειστικού API που μπορεί να κληθεί από μια εξωτερική εφαρμογή (π.χ. ECA Registry). Η εγγραφή περιλαμβάνει μόνο το χρήστη που ξεκίνησε τη διαδικασία και το πορτοφόλι του (wallet) ("από" και "έως" αναπαριστούν το ίδιο πορτοφόλι).[157]

ECA Registry Service

Η εφαρμογή ECA (EBSI V1) αξιοποιεί το Core Services Layer προκειμένου να επωφεληθεί από το blockchain EBSI και τον κατανεμημένο χώρο αποθήκευσης. Το μητρώο ECA δημιουργεί ένα ψηφιακό αποτύπωμα ελέγχου που επισημαίνεται χρονικά (audit trail), επιτρέπει την εγγραφή και σύνδεση μεταξύ των «ψηφιακών αποτυπωμάτων» αρχείων και των μεταδεδομένων τους και, επίσης, επιτρέπει την αμφίδρομη ανταλλαγή αποτυπωμάτων με τρίτους με τρόπο συμβατό με το GDPR. Το μητρώο ECA (EBSI V1) χρησιμοποιεί τις υπηρεσίες Timestamp API και Storage API για την καταχώριση τιμών κατακερματισμού στο EBSI.[2]

II. Πλήρης συμβολαιογραφική θεώρηση εγγράφου (V2+)

Ρόλοι : Χρήστης ή Καταχωρητής

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

[2] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=155385948

Ιστορικό : *Περίπτωση 1*: Ένας ελεγχόμενος έχει δημιουργήσει έγγραφα που ενδέχεται να σχετίζονται με μελλοντικούς ελέγχους (π.χ. τιμολόγιο, συμβόλαιο κ.λπ.) και θέλει να τα ενημερώσει.

Περίπτωση 2: Κατά τη διάρκεια ενός ελέγχου, ο ελεγκτής συλλέγει αρχεία που αφορούν έναν συγκεκριμένο ελεγχόμενο και θέλει να τα γνωστοποιήσει (εκ μέρους του).

Περίπτωση 3: Ο ελεγχόμενος έχει δημιουργήσει μια νέα έκδοση ενός εγγράφου που έχει στο παρελθόν θεωρήσει συμβολαιογραφικά ή αντιλαμβάνεται ότι είχε στο παρελθόν θεωρήσει συμβολαιογραφικά λάθος αρχείο. Ο ελεγκτής θέλει να θεωρήσει συμβολαιογραφικά τη νέα έκδοση συνδέοντάς τη με την παλιά έκδοση.

Στόχος : Να θεωρήσει συμβολαιογραφικά τα αρχεία που υπέβαλε ο χρήστης μαζί με τα σχετικά μεταδεδομένα (metadata) και να δημιουργήσει μια αξιόπιστη διαδρομή ελέγχου (audit trail).

Διαδρομή :

Περιπτώσεις 1 και 2 :

- Ο χρήστης αποθηκεύει τα αρχεία που πρέπει να θεωρηθούν συμβολαιογραφικά σε αποθηκευτικό χώρο της επιλογής του (εκτός αλυσίδας).
- Ο χώρος αποθήκευσης είναι προσβάσιμος μέσω του Registry, αλλά δεν χρειάζεται να είναι μέρος αυτού. Ο χρήστης συνδέεται (login) στο Registry με τα διαπιστευτήριά του.
- Ο χρήστης επιλέγει τα αρχεία που θέλει να θεωρήσει συμβολαιογραφικά.

Το Registry προτείνει να συμπληρωθεί ένα σύνολο μεταδεδομένων:

- Τα πεδία των μεταδεδομένων εξαρτώνται από το πλαίσιο στο οποίο πραγματοποιείται η εγγραφή και τα σχετικά πρότυπα.
- Ο χρήστης συμπληρώνει τα πεδία μεταδεδομένων και τα επισημαίνει είτε ως δημόσια (διαθέσιμα σε όλους), είτε ως ιδιωτικά (διατίθενται μόνο στον τρέχοντα καταχωρητή) ή ως περιορισμένα (διατίθενται μόνο στον τρέχοντα καταχωρητή και στους εξουσιοδοτημένους καταχωρητές). Το επίπεδο ορατότητας εξαρτάται επίσης από το πλαίσιο, καθώς ενδέχεται να υπάρχουν νομικές απαιτήσεις για ορισμένα από τα πεδία μεταδεδομένων, οι οποίες υποδεικνύουν να είναι «δημόσια».
- Η προσθήκη της μοναδικής αναφοράς μιας προηγούμενης εγγραφής ως μεταδεδομένων για μια νέα θα δημιουργήσει έναν λογικό σύνδεσμο μεταξύ των δύο. Το Registry δημιουργεί μια λογική αλυσίδα εγγραφών που αποτελεί μια αξιόπιστη χρονολογική διαδρομή ελέγχου (audit trail). Κατά την προσθήκη του λογικού συνδέσμου, το μητρώο εγγραφών ζητά την περιγραφή του συνδέσμου (π.χ. νεότερη έκδοση, αντικαθιστά το προηγούμενο αρχείο, μέρος της ίδιας διαδικασίας) και επιτρέπει στο χρήστη να προσθέσει ένα σχόλιο κειμένου.

Στη συνέχεια, ο χρήστης ενεργοποιεί τη συμβολαιογραφική θεώρηση. Το μητρώο δημιουργεί ψηφιακά αποτυπώματα των εγγράφων και των σχετικών μεταδεδομένων και, στη συνέχεια, αποθηκεύει ένα συνδυασμένο ψηφιακό αποτύπωμα (έγγραφο + μεταδεδομένα) στο blockchain. Εάν ο χρήστης είναι καταχωρητής (registrar), το μητρώο εγγραφών θα προσφέρει

τη δυνατότητα πραγματοποίησης της εγγραφής εκ μέρους ενός χρήστη που έχει προηγουμένως δώσει την άδειά του.[1]

Η εγγραφή καταγράφεται, με χρονική επισήμανση που παρέχεται από το μητρώο (ή συνδεδεμένη υπηρεσία χρονικής σήμανσης) και η κατάστασή της παραμένει «σε εκκρεμότητα» έως ότου ληφθούν επιβεβαιώσεις για τις συναλλαγές blockchain. Μόλις ληφθούν οι επιβεβαιώσεις, η διαδικασία του notarisation ολοκληρώνεται και ο χρήστης μπορεί να συμβουλευτεί τις σχετικές πληροφορίες που έχουν καταχωρηθεί στις σχετικές πλατφόρμες blockchain.

Η διαδικασία του notarisation ενός αρχείου θα είναι δυνατή μελλοντικά, μέσω του EBSI, μέσω ενός web interface (μη αυτόματη εγγραφή όπως περιγράφεται σε αυτήν την αφήγηση) ή μέσω ενός αποκλειστικού API (αυτοματοποιημένη εγγραφή).

Περίπτωση 3:

Υπάρχουν δύο λόγοι για να πραγματοποιηθεί μια νέα διαδικασία notarisation ενός εγγράφου:

1. Το λάθος έγγραφο είχε αρχικά θεωρηθεί συμβολαιογραφικά, κατά λάθος.
2. Ως αποτέλεσμα μιας επιχειρηματικής διαδικασίας, δημιουργήθηκε μια νέα έκδοση του εγγράφου.

Ο χρήστης προχωρά στη διαδικασία του notarisation του νέου εγγράφου με την ίδια διαδικασία που περιγράφεται για τις περιπτώσεις 1 και 2, αλλά παρέχει αναφορά στην προηγούμενη καταχώριση (μοναδικό αναγνωριστικό). Αυτή η αναφορά προστίθεται από το σύστημα μεταξύ των μεταδεδομένων και δημιουργεί μια λογική σύνδεση μεταξύ των δύο καταχωρίσεων. Κατά την προσθήκη του λογικού συνδέσμου, το μητρώο εγγραφών ζητά την περιγραφή του συνδέσμου (π.χ. νεότερη έκδοση, αντικαθιστά το προηγούμενο αρχείο, μέρος της ίδιας διαδικασίας) και επιτρέπει επίσης στο χρήστη να προσθέσει ένα σχόλιο κειμένου.[159]

III. Βασική επαλήθευση γνησιότητας / ακεραιότητας ενός αρχείου (V1)

Ρόλοι : Όλοι, συμπεριλαμβανομένων των μη εγγεγραμμένων χρηστών (επισκεπτών) για δημόσια έγγραφα.

Ιστορικό :

Περίπτωση 1: Ένας ελεγκτής λαμβάνει ορισμένα αρχεία μέσω email από έναν ελεγχόμενο και επιθυμεί να ελέγξει την αυθεντικότητα / ακεραιότητά τους.

Περίπτωση 2: Ένας δημοσιογράφος ή ένας πολίτης βρίσκει μια αναφορά από ένα δημόσιο ίδρυμα σε ένα φόρουμ και θέλει να επαληθεύσει εάν το έγγραφο, στο οποίο γίνεται η αναφορά, είναι «αυθεντικό».

Στόχος : Να επιτραπεί στους χρήστες να δημιουργήσουν ένα ψηφιακό αποτύπωμα ενός αρχείου και να ανακτήσουν οποιαδήποτε υπάρχουσα εγγραφή (στο Registry) που σχετίζεται με το ψηφιακό αυτό αποτύπωμα και τα σχετικά μεταδεδομένα.[159]

Διαδρομή :

Υπάρχουν δύο τύποι ρόλων που μπορούν να χρησιμοποιήσουν αυτή τη λειτουργικότητα:

1. Χρήστες που συνδέονται με τα διαπιστευτήριά (credentials) τους.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

2. Επισκέπτες που δεν έχουν λογαριασμό και συνδέονται μέσω δημόσιου ιστοτόπου προσφέροντας μία υπηρεσία επαλήθευσης συνδεδεμένη στο EBSI.

Ο χρήστης επιλέγει το έγγραφο που θέλει να επαληθεύσει και το υποβάλει. Η εφαρμογή δημιουργεί ένα αποτύπωμα (τιμή κατακερματισμού) του εγγράφου και εκτελεί αναζήτηση για μια αντίστοιχη εγγραφή. Εάν υπάρχει αντιστοιχία, επιβεβαιώνεται ότι υπάρχει εγγραφή και επιστρέφεται ένας σύνδεσμος προς αυτήν. Εάν δεν υπάρχει αντιστοιχία, το σύστημα επιστρέφει ένα μήνυμα που δηλώνει ότι δεν μπόρεσε να βρεθεί εγγραφή για το έγγραφο εισαγωγής. Επί της αρχής, εάν βρεθεί μια αντίστοιχη εγγραφή, το έγγραφο είναι «αυθεντικό» (δηλαδή είναι αυτό που έχει καταχωρηθεί). Εάν όχι, τότε υπάρχει λόγος να αμφισβητηθεί η αυθεντικότητα / ακεραιότητά του.

Για να πραγματοποιήσει μια βασική επαλήθευση, ο χρήστης μπορεί να ανοίξει την εγγραφή και να ελέγξει: την τιμή κατακερματισμού (hash), τη χρονική σήμανση της εγγραφής (timestamp), το πορτοφόλι - wallet - με το οποίο καταγράφηκε το έγγραφο, τη συναλλαγή στον block explorer.[1]

IV. Onboarding ενός φυσικού προσώπου στο Notarisation

Στόχος : Ένα φυσικό πρόσωπο στοχεύει στη χρήση υπηρεσιών του Notarisation και πιθανώς άλλων υπηρεσιών EBSI που χρειάζονται ταυτότητα ESSIF και πορτοφόλι (wallet) για τη διαχείρισή του. Η συμμετοχή στο ESSIF θα επιτρέψει στο φυσικό πρόσωπο να αποκτήσει πρόσβαση στις δυνατότητες συμβολαιογραφικής θεώρησης με τη δική του ψηφιακή ταυτότητα. Με τη συμμετοχή στο ESSIF, το φυσικό πρόσωπο θα διατηρεί και θα διαχειρίζεται όλα τα δεδομένα του.

Ιστορικό : Θεωρείται δεδομένο ότι το φυσικό πρόσωπο διαθέτει υποστηριζόμενα περιβάλλοντα χρήστη (smartphone, eID) και έχει πρόσβαση στο Διαδίκτυο (όχι στο πεδίο της εφαρμογής EBSI).

Διαδρομή :

Για να χρησιμοποιεί τις υπηρεσίες συμβολαιογραφικής θεώρησης, ένα φυσικό πρόσωπο πρέπει να έχει ταυτότητα ESSIF.

Ρύθμιση του πορτοφολιού (wallet) στο ESSIF.

1. Το φυσικό πρόσωπο δημιουργεί και αποθηκεύει με ασφάλεια το DID και τα σχετικά δημόσια / ιδιωτικά κλειδιά.
2. Το έγγραφο DID είναι καταχωρημένο στο EBSI Ledger.
3. Το φυσικό άτομο μπορεί να αρχίσει να χρησιμοποιεί υπηρεσίες συμβολαιογραφικής θεώρησης EBSI με το DID του και το πορτοφόλι του (wallet).

Παρατήρηση: Κάθε πολίτης που έχει DID μπορεί να χρησιμοποιήσει την υπηρεσία notarisation.[2]

3.2.2.3.2 Επιμέρους Δυνατότητες

I. Αίτηση για Εγγραφή

Ρόλοι : Επισκέπτης, Registry Manager.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

[2] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=155385948

Ιστορικό : Ένας νέος χρήστης επιθυμεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει το μητρώο εγγραφών (registry).

Στόχος : Να είναι δυνατή η εγγραφή της ταυτότητάς του.

Διαδρομή : Ένας νέος χρήστης κάνει αίτηση στη Διαχείριση Μητρώου Εγγραφών (Registry Manager) για πρόσβαση στο σύστημα. Κάνει ένα αίτημα στην πύλη συμπληρώνοντας τις απαιτούμενες πληροφορίες. Ο διαχειριστής μητρώου ελέγχει το αίτημα και αποφασίζει αν το εγκρίνει ή το απορρίπτει.[1]

II. Εγγραφή ταυτότητας

Ρόλος : Χρήστης

Ιστορικό : Ένας νέος χρήστης επιθυμεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει το μητρώο εγγραφών (registry) και χρειάζεται να αποδείξει την ταυτότητά του.

Στόχος : Να καταχωρήσει μια ταυτότητα νέου χρήστη, η οποία θα συνδεθεί με μελλοντική καταχώριση / συμβολαιογραφική θεώρηση εγγράφων.

Διαδρομή : Μόλις εγκριθεί το αίτημα, ο χρήστης λαμβάνει έναν αποκλειστικό σύνδεσμο εγγραφής. Ο χρήστης μπορεί στη συνέχεια να αποφασίσει αν θα:

- Καθορίσει την ταυτότητα με βάση μία υπάρχουσα (π.χ. εθνικά συστήματα ηλεκτρονικής αναγνώρισης (eIDAS) ή ESSIF),
- Δημιουργήσει μια νέα ταυτότητα στο μητρώο συμπληρώνοντας μια φόρμα με τα προσωπικά του στοιχεία.

Στη συνέχεια, η ταυτότητα επαληθεύεται και εγκρίνεται. Μόλις δημιουργηθεί ο λογαριασμός με βάση την αρχική ταυτότητα, ο χρήστης μπορεί να συνδέσει και άλλες πρόσθετες ταυτότητες. Το μητρώο θεωρεί συμβολαιογραφικά τη νέα ταυτότητα, αποθηκεύει και διατηρεί τους δεσμούς μεταξύ της ταυτότητας και των καταχωρίσεων εγγράφων που έγιναν από αυτήν την ταυτότητα. Αυτή η ταυτότητα γίνεται ένας καταχωρητής (registrar), έτσι ώστε να μπορεί να θεωρήσει συμβολαιογραφικά έγγραφα και οι άλλοι χρήστες να μπορούν να δώσουν τη συγκατάθεση τους έτσι ώστε ο διαχειριστής (Administrator) να εγγράψει έγγραφα για λογαριασμό του.[162]

III. Καταχώρηση των τιμών κατακερματισμού (hashes) στο Ledger

Στόχος : Ο χρήστης επαληθεύει εάν η συναλλαγή με το ίδιο ακριβώς περιεχόμενο (ίδια hashes εγγράφου και ίδιο hash μεταδεδομένων) έχει ήδη υποβληθεί στο ίδιο ημερολόγιο blockchain (ledger).

Διαδρομή :

1. Προκειμένου να επαληθεύσει εάν ένα έγγραφο έχει ήδη θεωρηθεί συμβολαιογραφικά, ως χρήστης, μπορεί να επαληθεύσει εάν η τιμή κατακερματισμού (hash) του αρχείου είναι καταχωρημένη στο ledger.
2. Σε περίπτωση που δεν έχει καταχωρηθεί στο παρελθόν τέτοια τιμή κατακερματισμού, ο χρήστης μπορεί να εισαγάγει μια νέα εγγραφή στο ledger.
3. Για να καταχωρήσει μία τιμή κατακερματισμού μπορεί να υποβάλλει μια συναλλαγή χρονικής σήμανσης.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

4. Αφού υποβληθεί η συναλλαγή, επικυρωθεί και συμπεριληφθεί στο ledger, ο χρήστης μπορεί να ελέγξει την εγγραφή του στο ledger.
5. Προκειμένου να επαληθεύσει την ύπαρξη εγγραφής μπορεί να ελέγξει το περιεχόμενο του δημόσιου ledger, σε λειτουργία μόνο για ανάγνωση, παρέχοντας το κατακερματισμό του εγγράφου ως είσοδο.
6. Ο χρήστης καταχώρησε επιτυχώς ένα hash στο ledger. Δεν είναι δυνατή η τροποποίηση ή η διαγραφή της εγγραφής.

Παρατηρήσεις: Για μια έγκυρη συναλλαγή, απαιτείται ο κατακερματισμός (hashing) του εγγράφου. Ο κατακερματισμός των μεταδεδομένων είναι προαιρετικός. Το αναγνωριστικό συμβολαιογραφικής θεώρησης (NID) πρέπει να είναι αποθηκευμένο εκτός αλυσίδας και πρέπει να δείχνει τη συναλλαγή που έχει καταχωρήσει το hash του εγγράφου στο ledger.[1]

IV. Ο χρήστης έχει τη δυνατότητα να δει το ιστορικό των εγγράφων του που έχει θεωρήσει συμβολαιογραφικά, ταξινομημένων με βάση την ημερομηνία.

Στόχος : Ο χρήστης θα δει μια λίστα (πίνακας) με τις συμβολαιογραφικές θεωρήσεις του (notarisations).

Διαδρομή :

1. Για να δει τη λίστα όλων των εγγράφων του που έχουν θεωρηθεί συμβολαιογραφικά (notarized), ως επικυρωμένος χρήστης, μπορεί να υποβάλει αίτημα στο ledger, χρησιμοποιώντας το DID του.
2. Ο χρήστης βλέπει μια πλήρη λίστα των εγγράφων του, με χρονολογική σειρά.
3. Η λίστα περιέχει το αναγνωριστικό NID, την ημερομηνία της συμβολαιογραφικής θεώρησης και το hash του σχετικού εγγράφου.

Παρατηρήσεις: Όλα τα συμβολαιογραφικά θεωρημένα έγγραφα που σχετίζονται με το hash ενός εγγράφου πρέπει να αναγνωρίζονται από το αναγνωριστικό (NID) τους.[163]

3.3 Roadmap – Η συνολική πορεία ενός χρήστη στο EBSI

Σε αυτό το κεφάλαιο, οι λειτουργίες που είναι διαθέσιμες στο EBSI εξηγούνται δημιουργώντας ένα ταξίδι χρήστη που ενσωματώνει όλες τις αρχικές περιπτώσεις χρήσης, οι οποίες με τη σειρά τους αξιοποιούν τις κοινές εφαρμογές EBSI και τις βασικές διεπαφές υπηρεσιών. Με αυτόν τον τρόπο, οι επιχειρηματίες και οι τεχνικοί μπορούν να καταλάβουν πώς θα μπορούσε να χρησιμοποιηθεί η πλατφόρμα και να αποκτήσουν μια εικόνα για τη χρήση των δυνατοτήτων της (περιλαμβάνονται οι λειτουργίες του «SSI» και του «Notarisation»). Εξηγείται λεπτομερώς η διαδρομή του χρήστη. Έπειτα κάθε βήμα της διαδρομής του χρήστη περιγράφεται με περισσότερες λεπτομέρειες.

Ο χρήστης είναι ένας εικοσιτριάχρονος Βέλγος που έχει αποκτήσει ένα Bachelor's degree από το πανεπιστήμιο του Ghent στο Βέλγιο. Επιθυμεί να υποβάλει αίτηση σε ένα μεταπτυχιακό πρόγραμμα σπουδών στην Ισπανία. Υποβάλλει την αίτηση και γίνεται δεκτός στο πανεπιστήμιο. Κατά τη διάρκεια των σπουδών του στο μεταπτυχιακό πρόγραμμα, ο χρήστης επιθυμεί να συμμετάσχει σε ένα πρόγραμμα πρακτικής άσκησης σε μία ισπανική εταιρία. Όταν τελειώνει το μεταπτυχιακό πρόγραμμα και την πρακτική άσκηση, λαμβάνει μία νέα βεβαίωση (verifiable attestation) για να εμπλουτίσει την SSI ταυτότητά του. Στη συνέχεια, αποφασίζει να ξεκινήσει μία επιχείρηση στην Ιταλία. Κάνει αίτηση για χρηματοδότηση από

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Notarisation+User+Stories

την ΕΕ. Λαμβάνει μία χρηματοδότηση και θεωρεί συμβολαιογραφικά όλα τα έγγραφα που σχετίζονται με τις δαπάνες της χρηματοδότησης, έτσι ώστε οι ελεγκτικοί μηχανισμοί να μπορούν να επαληθεύσουν τις πληροφορίες.[1]

Διαδρομή του χρήστη[164]**:**

- Εγκατάσταση Wallet: Προκειμένου να διαχειριστεί τα εκπαιδευτικά του διαπιστευτήρια, ο χρήστης θα πρέπει να δημιουργήσει μία ταυτότητα SSI. Γι' αυτό το λόγο θα πρέπει να εγκαταστήσει και να διαμορφώσει ένα πορτοφόλι EBSI με έγκυρες βεβαιώσεις (Agent Requester). Εγκαθιστώντας το πορτοφόλι, αποκτά και ένα αναγνωριστικό DID στο EBSI.
- Onboarding & Έκδοση Διπλώματος: Ο χρήστης πραγματοποιεί ένα αίτημα στην Κυβέρνηση του Βελγίου για την έκδοση του Verifiable ID του, καθώς και την έκδοση του Verifiable attestation (βεβαίωση), για το Bachelor's degree. Η κυβέρνηση επαληθεύει το αίτημα και εκδίδει και τα δύο διαπιστευτήρια (Verifiable Credentials).
- Αίτηση σε μεταπτυχιακό πρόγραμμα σπουδών: Ο χρήστης κάνει αίτηση στο μεταπτυχιακό πρόγραμμα σπουδών χρησιμοποιώντας το πορτοφόλι του στο EBSI. Το πανεπιστήμιο ζητά τα απαραίτητα διαπιστευτήρια και επικυρώνει τις πληροφορίες.
- Ο χρήστης γίνεται δεκτός στο μεταπτυχιακό πρόγραμμα σπουδών: Το ισπανικό πανεπιστήμιο αποδέχεται το αίτημα του χρήστη. Έπειτα, εκδίδει για τον χρήστη έναν αριθμό μητρώου ως ένα Verifiable Credential για την εσωτερική ταυτοποίησή του.
- Αίτηση σε πρόγραμμα πρακτικής άσκησης : Η ισπανική εταιρία εξετάζει την αίτηση του χρήστη και τα απαιτούμενα διαπιστευτήρια και εκδίδει την απαραίτητη βεβαίωση (Verifiable Attestation) με την επιβεβαίωση εγγραφής στο πρόγραμμα.
- Αποφοίτηση από το μεταπτυχιακό πρόγραμμα σπουδών: Το ισπανικό πανεπιστήμιο εκδίδει μια βεβαίωση στο χρήστη με το μεταπτυχιακό του δίπλωμα (Verifiable Attestation). Κατά τον ίδιο τρόπο, μετά το πέρας της πρακτικής άσκησης ο χρήστης λαμβάνει ένα διαπιστευτήριο από την εταιρία.
- Χρηματοδότηση: Ο χρήστης καταθέτει μία αίτηση για χρηματοδότηση στην ΕΕ. Ο χρήστης επιλέγεται για χρηματοδότηση και λαμβάνει την επιχορήγηση. Τέλος, προκειμένου να δικαιολογήσει τη δαπάνη της επιχορήγησης, θεωρεί συμβολαιογραφικά τα έγγραφα (notarisation) των εξόδων, έτσι ώστε οι ελεγκτές της ΕΕ να πραγματοποιήσουν τον απαιτούμενο έλεγχο.

Ανάλυση των βημάτων στο EBSI:

Βήμα 1ο - Εγκατάσταση του Wallet: Ο χρήστης επιλέγει, εγκαθιστά και διαμορφώνει μία εφαρμογή πορτοφολιού (Agent requester) στη συσκευή του. Αυτή η πράξη πυροδοτεί τη δημιουργία ιδιωτικών κλειδιών ρίζας (root private keys), τα οποία αποθηκεύονται στην αλυσίδα κλειδιών που αποθηκεύεται στην συσκευή. Μέχρι το σημείο αυτό, ο χρήστης διαθέτει ένα πορτοφόλι EBSI και ένα αναγνωριστικό DID. [164]

Βήμα 2ο- Onboarding :

I. Ο χρήστης στέλνει ένα αίτημα στην ομοσπονδιακή κυβέρνηση του Βελγίου για έκδοση της επαληθεύσιμης ταυτότητάς της (Verifiable ID) και πιστοποιητικό επαλήθευσης διπλώματος (Verifiable Attestation), δηλαδή το ψηφιακά υπογεγραμμένο διαπιστευτήριο για το πτυχίο του. Το πλαίσιο των διπλωμάτων για το EBSI V1 θα περιοριστεί στην τυπική εκπαίδευση, με σαφή αναφορά στο EQF / NQF.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Eva%27s+User+Journey

Στο Βέλγιο, δεν υπάρχει αλληλεπίδραση της κυβέρνησης με τα πανεπιστήμια για την έκδοση διπλωμάτων. Για έναν γερμανόφωνο φοιτητή, η περιφερειακή κυβέρνηση της Φλάνδρας στο Βέλγιο εκδίδει το δίπλωμα.

II. Η φλαμανδική κυβέρνηση επαληθεύει την ταυτότητα του χρήστη (eID) και ότι ο χρήστης έχει αποφοιτήσει από το Βελγικό Πανεπιστήμιο.

III. Η Κυβέρνηση του Βελγίου εκδίδει στο χρήστη την επαληθεύσιμη ταυτότητά του - Verifiable ID- (θα περιλαμβάνει μόνο χαρακτηριστικά eIDAS, τουλάχιστον όνομα και επώνυμο). Το επαληθεύσιμο αναγνωριστικό (Verifiable ID) περιλαμβάνει τα εξής:

- Credential ID (προαιρετικά)
- Credential Type: Verifiable ID
- Εκδότης
- Credential Subject
- Ισχυρισμοί : Σχετικά με την ταυτοποίηση / έλεγχο ταυτότητας
- Ημερομηνία έκδοσης
- Αποδείξεις: πχ eSignature

Τώρα ο χρήστης διαθέτει ένα EBSI ESSIF DID. Εάν γίνει αποδεκτό από το χρήστη το VC που αντιπροσωπεύει το δίπλωμα θα αποθηκευτεί στο προσωπικό του αποθετήριο, το οποίο μπορεί να αποθηκευτεί σε διαφορετική τοποθεσία από το πορτοφόλι.

IV. Η περιφερειακή κυβέρνηση της Φλαμανδικής Δημοκρατίας εκδίδει στο χρήστη ένα verifiable attestation (ψηφιακή υπογραφή διαπιστευτηρίου του πτυχίου της). Αυτό το VC μεταφέρεται στο πορτοφόλι που είναι συμβατό με το EBSI του χρήστη, υπογεγραμμένο από τη φλαμανδική κυβέρνηση, σε μορφή βασισμένη στην οντολογία του EBSI. Η επαληθεύσιμη βεβαίωση (Verifiable Attestation) περιλαμβάνει τα εξής:

- Credential ID (προαιρετικά)
- Credential Type: Verifiable Attestation
- Εκδότης
- Credential Subject
- Ισχυρισμοί : Πέρα από την ταυτοποίηση / έλεγχο ταυτότητας
- Ημερομηνία έκδοσης
- Αποδείξεις: πχ eSignature

Εάν η διαδικασία έκδοσης δεν μπορεί να γίνει σε πραγματικό χρόνο όταν το δημιουργούμενο Verifiable Credential είναι ακόμα διαθέσιμο, ο χρήστης θα λάβει μια ειδοποίηση μέσω email ή κινητού για τη διαθεσιμότητα της έκδοσης της επαληθεύσιμης πιστοποίησής της (ψηφιακά υπογεγραμμένο διαπιστευτήριο του πτυχίου της) από τη Φλαμανδική Κυβέρνηση.[1]

<u>Βήμα 3ο - Αίτηση σε μεταπτυχιακό πρόγραμμα σπουδών:</u>

I. Ο χρήστης περιηγείται στον ιστότοπο του ισπανικού Πανεπιστημίου και επιλέγει το πρόγραμμα για το οποίο θέλει να υποβάλει αίτηση.

II. Το ισπανικό Πανεπιστήμιο στέλνει στο χρήστη μια σελίδα προορισμού για να δημιουργήσει ένα αίτημα επαληθεύσιμης παρουσίασης (Verifiable Presentation) , μαζί με την αποδοχή του GDPR και άλλους όρους και προϋποθέσεις, καθώς και τη λίστα των απαιτούμενων Verifiable Credentials.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Eva%27s+User+Journey

III. Με βάση τα απαιτούμενα έγγραφα, ο χρήστης παρουσιάζει μέσω του πορτοφολιού του στο ισπανικό πανεπιστήμιο τα εξής :
    - Το Verifiable ID του
    - Την αποδοχή του GDPR και των άλλων όρων και προϋποθέσεων
    - Τα απαραίτητα Verifiable Credentials

IV. Το πανεπιστήμιο στέλνει έναν αριθμό αναφοράς αιτήματος στο πορτοφόλι του χρήστη, που σχετίζεται με το αίτημά του.

V. Ο χρήστης λαμβάνει μία ειδοποίηση (πχ μέσω e-mail) με αυτήν την πληροφορία.[1]

Βήμα 4ο – Αποδοχή αίτησης από το μεταπτυχιακό πρόγραμμα σπουδών[166]:

I. Το ισπανικό πανεπιστήμιο εξετάζει τις πληροφορίες που έχει λάβει από το χρήστη:
- Επαληθεύει όλα τα απαραίτητα έγγραφα (διαπιστευτήρια), που έχουν ληφθεί.
- Επαληθεύει την ταυτότητα του χρήστη (μέσω ESSIF).
- Επαληθεύει ότι η πιστοποίηση του χρήστη ταιριάζει με το απαιτούμενο επίπεδο.

II. Το Ισπανικό Πανεπιστήμιο - μέσω του συμβατού με το EBSI πορτοφολιού του - υπογράφει και στέλνει μια ειδοποίηση μέσω email / κινητής τηλεφωνίας στο χρήστη για λήψη και αποδοχή επαληθεύσιμης βεβαίωσης (Verifiable Attestation) του Αριθμού Μητρώου του Πανεπιστημίου (URN). Αυτό το VC θα χρησιμεύσει ως εσωτερική ταυτότητα για το πανεπιστήμιο και θα εκτυπωθεί στο δίπλωμα.

III. Μια επιπλέον επαληθεύσιμη βεβαίωση με την Ευρωπαϊκή Κάρτα Φοιτητών - European Student Card- του χρήστη (ESC) θα εκδοθεί σε αυτόν με τις ακόλουθες λεπτομέρειες:
    - Αριθμός ESC
    - Ημερομηνία Λήξης
    - European Student Identifier
    - Διεύθυνση e-mail φοιτητή

Βήμα 5ο - Αίτηση σε πρόγραμμα πρακτικής άσκησης:

I. Ο χρήστης περιηγείται στον ιστότοπο της ισπανικής εταιρείας, βρίσκει την πρακτική άσκηση και την επιλέγει.

II. Ένα αίτημα παρουσίασης αποστέλλεται από την ισπανική εταιρεία στο προφίλ του χρήστη, συμπεριλαμβανομένου του σκοπού (όροι και προϋποθέσεις) και μια λίστα με τις απαιτούμενες Verifiable Attestations (συμπεριλαμβανομένης της επαληθεύσιμης βεβαίωσης ότι πρόκειται για επίσημα εγγεγραμμένο φοιτητή).

III. Ο χρήστης αποστέλλει την εγγραφή του στο ισπανικό πανεπιστήμιο με την αίτηση του στο πρόγραμμα πρακτικής άσκησης.

IV. Η ισπανική εταιρεία λαμβάνει το αίτημα του χρήστη μέσω του συμβατού με το EBSI πορτοφολιού της.

V. Η ισπανική εταιρεία επαληθεύει ότι:
    - Η ταυτότητα του χρήστη είναι σωστή (Verifiable ID, το διαπιστευτήριο eIDAS συνδέεται με το Verifiable ID).
    - Ο χρήστης είναι εγγεγραμμένος στο Ισπανικό Πανεπιστήμιο.

VI. Η ισπανική εταιρεία, μέσω του συμβατού με το EBSI πορτοφολιού της, στέλνει μια ειδοποίηση στο χρήστη για λήψη και αποδοχή επαληθεύσιμης βεβαίωσης με την

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Eva%27s+User+Journey

επιβεβαίωση εγγραφής και τις λεπτομέρειες (αυτές μπορεί να είναι ημερομηνία έναρξης, ημερομηνία λήξης κ.λπ.)[1]

Βήμα 6ο - Αποφοίτηση από το μεταπτυχιακό πρόγραμμα σπουδών[167]:

I. Μόλις ο χρήστης ολοκληρώσει την πορεία των σπουδών του, το Ισπανικό Πανεπιστήμιο σφραγίζει την επαληθεύσιμη βεβαίωση (Verifiable Attestation) που αντιπροσωπεύει το δίπλωμά του (ψηφιακά υπογεγραμμένο διαπιστευτήριο για το πτυχίο) και τον ειδοποιεί για τη διαθεσιμότητα της επαληθεύσιμης πιστοποίησης. Όταν γίνει αποδεκτή, ο χρήστης θα αποθηκεύσει τα ψηφιακά υπογεγραμμένα διαπιστευτήρια με το μεταπτυχιακό του στο πορτοφόλι EBSI του (ήδη συνδεδεμένο με το DID του).

II. Με την ολοκλήρωση της πρακτικής άσκησης , ο χρήστης έχει τη δυνατότητα να ζητήσει πιστοποιητικό ψηφιακής υπογραφής με επιστολή σύστασης από τον εργοδότη της:

- Ο εργοδότης εκδίδει επαληθεύσιμη αξίωση / διαπιστευτήριο που αντιπροσωπεύει τη συστατική επιστολή στο πορτοφόλι EBSI του χρήστη.
- Ο χρήστης λαμβάνει μια ειδοποίηση (μέσω email ή κινητού).

Βήμα 7ο - Χρηματοδότηση[167]:

I. Ο χρήστης επιθυμεί να δημιουργήσει μία επιχείρηση startup στην Ιταλία και συμμετέχει σε μία πρόσκληση υποβολής προτάσεων από τις ιταλικές αρχές προκειμένου να λάβει κεφάλαια της ΕΕ για την εκκίνησή της. Συμπληρώνει μια αίτηση επιχορήγησης και στη συνέχεια σαρώνει και θεωρεί συμβολαιογραφικά την αίτηση μέσω του Notarisation Component.

II. Οι ιταλικές αρχές επιλέγουν την πρότασή του χρήστη και αυτός λαμβάνει επιχορήγηση χρηματοδοτούμενη από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης (ΕΤΠΑ). Η συμφωνία επιχορήγησης θεωρείται συμβολαιογραφικά μέσω του Notarisation Component.

III. Ο χρήστης ανταλλάσσει έγγραφα με τη Διαχειριστική Αρχή ηλεκτρονικά. Αυτά τα έγγραφα, που δικαιολογούν τον τρόπο με τον οποίο δαπανάται η επιχορήγηση, θεωρούνται συμβολαιογραφικά από τον χρήστη μέσω του Notarisation Component. Δείγματα συμβολαιογραφικών εγγράφων είναι τα εξής: τιμολόγια,
απόδειξη πληρωμής, εκθέσεις υλοποίησης έργου, φωτογραφίες και άλλα στοιχεία πολυμέσων.

IV. Στο πλαίσιο ενός ελέγχου, οι ελεγκτές της ΕΕ μπορούν να επαληθεύσουν την ακεραιότητα και τη χρονική σήμανση των θεωρημένων εγγράφων.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Eva%27s+User+Journey

4 Σχεδιασμός διαδικασίας ένταξης πρόσφυγα στην ΕΕ με τη χρήση του EBSI

4.1 Σενάριο χρήσης: Η πορεία ένταξης ενός πρόσφυγα στην κοινωνία της ΕΕ

4.1.1 Γιατί το EBSI αποτελεί ένα χρήσιμο εργαλείο για τη διαχείριση των μεταναστευτικών και προσφυγικών ροών

Όπως είδαμε και στο *κεφάλαιο 3*, το EBSI έχει ως στόχο την αξιοποίηση της τεχνολογίας Blockchain για την παροχή υπηρεσιών, ιδίως διασυνοριακών, στην Ευρωπαϊκή Ένωση. Η διαχείριση των μεταναστευτικών και προσφυγικών ροών αποτελεί μια από τις μεγαλύτερες προκλήσεις για την Ε.Ε, ως διασυνοριακή διαδικασία και ως διαδικασία που επηρεάζει σε γενικότερο πλαίσιο την κοινωνία και την οικονομία της Ε.Ε.

Οι διαδικασίες μετανάστευσης και ασύλου απαιτούν επί του παρόντος φυσικά έγγραφα όπως διαβατήρια, όπως έγινε κατανοητό στο *κεφάλαιο 2*. Επίσης, οι αιτούντες άσυλο συνήθως απαιτείται να παρέχουν πρόσθετες πληροφορίες προκειμένου να λάβουν συγκεκριμένα έγγραφα (π.χ. θεωρήσεις, άδειες διαμονής) για να εισέλθουν και να παραμείνουν σε άλλη χώρα. Εκτός από ζητήματα χρηστικότητας (π.χ. επιπτώσεις από την απώλεια φυσικών εγγράφων, τη συμπλήρωση εντύπων, υποχρεωτικές επισκέψεις σε πρεσβείες και υπηρεσίες), απαιτείται σημαντική εργασία για την επαλήθευση των δεδομένων των ατόμων και στη συνέχεια για την έκδοση και επικύρωση των αντίστοιχων εγγράφων. Αυτά τα βήματα έχουν ως αποτέλεσμα περιττό κόστος τόσο για τους πολίτες όσο και για τις κυβερνήσεις, καθώς και σπατάλη χρόνου σε δυνητικά ενοχλητικές και χρονοβόρες διαδικασίες εφαρμογής. Όπως έγινε κατανοητό και στο *κεφάλαιο 3*, το SSI του EBSI έχει τη δυνατότητα να εξορθολογήσει τον έλεγχο των συνόρων παρέχοντας στους πολίτες και τους μη πολίτες ψηφιακά ισοδύναμα (δηλαδή verifiable authentications, attestations) στα δημόσια έγγραφα που απαιτούνται για είσοδο, έξοδο ή παραμονή σε μια χώρα. Επιπλέον, το SSI έχει τη δυνατότητα να μειώσει τους χρόνους επεξεργασίας για τέτοιου είδους διαπιστευτήρια όπως ταυτότητες και ταξιδιωτικά έγγραφα από εβδομάδες ή και περισσότερο επί του παρόντος, σε λεπτά ή και δευτερόλεπτα, αυξάνοντας τη συνολική ασφάλεια και αποτρέποντας την πλαστογράφηση εγγράφων.[1]

Επιπλέον, πολίτες οι οποίοι αιτούνται άσυλο και τους χορηγείται καθεστώς πρόσφυγα, έχουν τη δυνατότητα να αποκτήσουν ένα σύνολο επίσημων και ανεπίσημων εκπαιδευτικών διαπιστευτηρίων κατά τη διάρκεια της ένταξής τους στην κοινωνία της Ε.Ε, όπως για παράδειγμα διπλώματα γυμνασίου, λυκείου ή πανεπιστημίου, επαγγελματικές πιστοποιήσεις - πιθανώς νόμιμα εξουσιοδοτημένα ή διπλώματα από ιδιωτικά ή κρατικά εκπαιδευτικά προγράμματα. Παρόλο που τέτοια διαπιστευτήρια χρησιμοποιούνται αμέτρητες φορές (π.χ. για αιτήσεις εργασίας, εφαρμογές σε εκπαιδευτικά προγράμματα, εφαρμογές για απόκτηση συγκεκριμένων δημόσιων αδειών), επί του παρόντος βασίζονται σε φυσικά έγγραφα, καθιστώντας άσκοπα δύσκολη και επίπονη την παροχή τους σε ψηφιακές αλληλεπιδράσεις. Επιπλέον, οι τρέχουσες πιστοποιήσεις εξακολουθούν να είναι ευάλωτες σε πλαστογραφίες λόγω των μορφών τους. Όπως είδαμε και στο *κεφάλαιο 3*, ωστόσο, με τη χρήση του SSI του EBSI όλοι οι τύποι εκπαιδευτικών διαπιστευτηρίων θα

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

μπορούσαν να εκδοθούν σε ψηφιακή μορφή, καθιστώντας εύκολη την παροχή τους σε πολλαπλές αλληλεπιδράσεις με δημόσιους ή ιδιωτικούς φορείς, διευκολύνοντας παράλληλα την επικύρωση και ενισχύοντας την ακεραιότητα τέτοιων εγγράφων για την αποτροπή δόλιας συμπεριφοράς. [1]

Εκτός από τα παραπάνω, οι αιτούντες άσυλο και πρόσφυγες υποβάλουν σε κρατικές υπηρεσίες νομικά έγγραφα. Ένα τέτοιο παράδειγμα είναι η άσκηση προσφυγής, ενώπιον της Αρχής Προσφυγών, από έναν αιτούντα άσυλο, του οποίου το αίτημα για απόκτηση καθεστώτος πρόσφυγα έχει απορριφθεί. Εκτός αυτού, κατά την πορεία ένταξης του στην κοινωνία ΕΕ, ένας πρόσφυγας έχει τη δυνατότητα δημιουργίας επιχείρησης. Για αυτό το σκοπό επίσης θα πρέπει να καταθέσει νομικά έγγραφα, τα οποία διατίθενται για έλεγχο από τους κατάλληλους ελεγκτικούς μηχανισμούς. Όπως αναλύθηκε στο *κεφάλαιο 3*, σε αυτήν την κατεύθυνση μπορεί να συμβάλει η υπηρεσία Notarisation του EBSI, η οποία παρέχει τη δυνατότητα για συμβολαιογραφική θεώρηση εγγράφων, για επαλήθευση θεωρημένων εγγράφων, για δημιουργία διαδρομών ελέγχων (audit-trail) καθώς και για έλεγχο της ακεραιότητας και της πιστότητας των εγγράφων.

Η ασφάλεια, στις διαδικασίες έκδοσης επαληθεύσιμων διαπιστευτηρίων και συμβολαιογραφικής θεώρησης εγγράφων, εξασφαλίζεται αξιοποιώντας την τεχνολογία της ψηφιακής υπογραφής (digital Signature) του blockchain, μέσω του EBSI. Το γεγονός αυτό εξηγήθηκε στο *κεφάλαιο 3*, σύμφωνα με το οποίο, εντός του EBSI V1 η βασική λειτουργικότητα του ESSIF αναπτύσσεται και ευθυγραμμίζεται με το πορτοφόλι EBSI (wallet). Με την εγκατάσταση και διαμόρφωση του πορτοφολιού, δίνεται η δυνατότητα αξιοποιήσιμης επαληθεύσιμης πιστοποίησης, δυνατότητα παρουσίασης και, επίσης, συμβολαιογραφικής θεώρησης εγγράφων, που υποστηρίζονται από μια υποδομή ιδιωτικού / δημόσιου κλειδιού.

Εκτός των άλλων, τα στοιχεία ταυτότητας και τα διαπιστευτήρια που ενδεχομένως μπορεί να κληθεί ένας αιτών άσυλο ή πρόσφυγας να καταθέσει, εμπεριέχουν σε μεγάλο βαθμό προσωπικά δεδομένα. Προκειμένου οι υπάρχουσες δομές να εξασφαλίσουν σε ικανοποιητικό βαθμό την ασφάλεια των δεδομένων, θα πρέπει να δαπανηθούν μεγάλα χρηματικά ποσά. Επιπλέον, στον τομέα της διαχείρισης του μεταναστευτικού, από την πλευρά των κρατών, ο οποίος πάσχει από την παράνομη μετακίνηση υπηκόων τρίτων χωρών σε χώρες της ΕΕ, η διαφάνεια που προσφέρει η τεχνολογία του Blockchain έχει μεγάλη σημασία. Σε ένα δίκτυο Blockchain στο οποίο συμμετέχουν υπήκοοι τρίτων χωρών (αιτούντες άσυλο, πρόσφυγες), ενώ η πραγματική τους ταυτότητα είναι ασφαλής, καθώς αποκρύπτεται με τη χρήση μεθόδων σύνθετης κρυπτογραφίας, η δημόσια διεύθυνσή τους δίνει τη δυνατότητα σε άλλους συμμετέχοντες να γνωρίζουν όλες τις ενέργειες που πραγματοποιούν με αποτέλεσμα να είναι υπόλογοι για τις ενέργειες τους. Το τελευταίο επιτυγχάνεται και μέσω της ελεγξιμότητας, καθώς κάθε ενέργεια ενός χρήστη- ενδεχομένως πρόσφυγα- επισημαίνεται χρονικά και μπορεί να ελεγχθεί. Το blockchain, επίσης, χαρακτηρίζεται από σταθερότητα. Από τη στιγμή που καταγράφεται σε αυτό μια ενέργεια-συμφωνία, δεν μπορεί έπειτα να τροποποιηθεί. Συνεπώς, με τη χρήση του blockchain, από τη στιγμή που έχει αναγνωριστεί καθεστώς πρόσφυγα σε έναν υπήκοο τρίτης χώρας, δεν είναι δυνατό έπειτα να του στερηθεί.

Επίσης, όσον αφορά στο μηχανισμό συναίνεσης του EBSI (Proof-of-Authority) είναι συμβατός με τη διαδικασία διαχείρισης του προσφυγικού. Από τη μία πλευρά, θα πρέπει να υπάρχει

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/ESSIF+How+we+use+SSI

μία κεντρική εξουσία που αποφασίζει σχετικά με τα θέματα των εισροών μεταναστών και τον αριθμό αιτούντων άσυλο που μπορούν να αναγνωριστούν ως πρόσφυγες (πχ η κυβέρνηση ενός κράτους μέλους), καθώς αυτές οι αποφάσεις σχετίζονται άμεσα με το ίδιο το κράτος, την κοινωνική και οικονομική ζωή του. Από την άλλη πλευρά όμως, η κεντρική εξουσία είναι αποκεντρωμένη πολιτικά, δηλαδή εκτός από την κυβέρνηση ενός κράτους μέλους μπορεί να συμμετέχουν σε αυτή και Μ.Κ.Ο, που έχουν στόχο την προάσπιση των δικαιωμάτων των προσφύγων. Επίσης, με το μηχανισμό συναίνεσης PoA, ενώ οι επικυρωτές (που βρίσκονται στην εξουσία) έχουν ισχυρό κίνητρο να διατηρήσουν τη θέση που έχουν αποκτήσει, δεν επιθυμούν να συνδέσουν τις ταυτότητές τους σε μια αρνητική φήμη.

Συμπερασματικά, η χρήση της τεχνολογίας blockchain του EBSI για τη διαχείριση του προσφυγικού προβλήματος που ταλανίζει την ΕΕ τα τελευταία χρόνια, αποτελεί μία εποικοδομητική λύση.

Στη συνέχεια, περιγράφεται ένα σενάριο-διαδρομή ενός πρόσφυγα από τη στιγμή που φτάνει στα σύνορα ενός κράτους μέλους της ΕΕ, μέχρι και την πλήρη ένταξή του στην κοινωνία της ΕΕ. Στο κεφάλαιο 4.2 αναλύεται ο σχεδιασμός του σεναρίου αυτού μέσω του EBSI.

4.1.2 Ανάλυση σεναρίου χρήσης

Ο χρήστης είναι ένας 25χρονος Σύριος, ο οποίος αποφασίζει να εγκαταλείψει τη χώρα του για να ζήσει στην Ευρωπαϊκή Ένωση. Για αυτό το σκοπό, φτάνει στα σύνορα της Ελλάδας με την Τουρκία, στη περιοχή του Έβρου, προκειμένου να καταθέσει αίτηση ασύλου στην Ελλάδα με στόχο να του χορηγηθεί καθεστώς πρόσφυγα.

Ο χρήστης μεταφέρεται στο Κέντρο Υποδοχής και Ταυτοποίησης του Έβρου. Η παραμονή του στις εγκαταστάσεις του κέντρου είναι υποχρεωτική για όσο χρόνο διαρκεί η διαδικασία εξέτασης της αίτησης ασύλου του, όπως εξηγήθηκε και στο κεφάλαιο 2.1.3.4. Στη συνέχεια, καταθέτει την αίτηση ασύλου στην Υπηρεσία Ασύλου (η οποία υπάγεται στο Υπουργείο Μετανάστευσης και Ασύλου). Μετά την εξέταση της αίτησής του από την Υπηρεσία Ασύλου, ενημερώνεται ότι αυτή έχει απορριφθεί. Για το λόγο αυτό, ο χρήστης-αιτών άσυλο αποφασίζει να ασκήσει προσφυγή ενώπιον της Αρχής Προσφύγων του Υπουργείου Μετανάστευσης και Ασύλου. Καταθέτει αυτή την προσφυγή στην Υπηρεσία Ασύλου. Η εξέταση της προσφυγής πραγματοποιείται από την Ανεξάρτητη Επιτροπή Προσφύγων (κεφάλαιο 2.1.3.4). Αυτή παίρνει την απόφαση σχετικά με τη χορήγηση καθεστώτος πρόσφυγα η όχι. Η απόφαση εκδίδεται και χορηγείται καθεστώς πρόσφυγα στο χρήστη. Ο χρήστης αναχωρεί από το Κέντρο Υποδοχής και Ταυτοποίησης στον Έβρο και εγκαθίσταται σε αστική περιοχή (π.χ. Αθήνα).

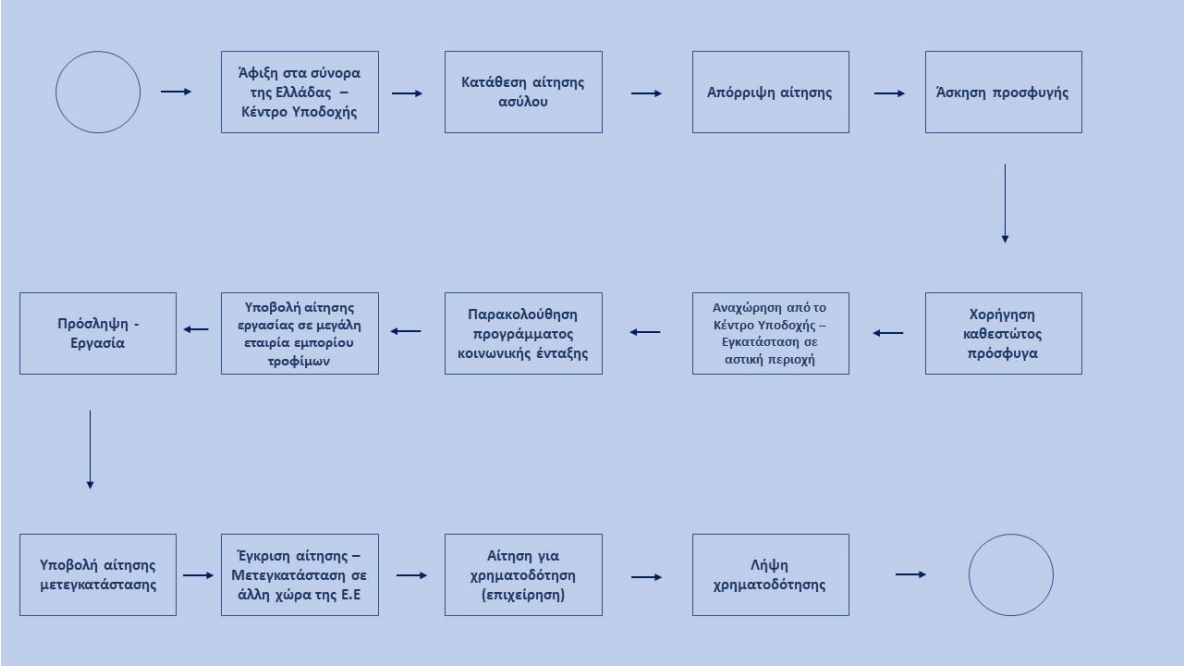
Ο χρήστης, που πλέον είναι αναγνωρισμένος πρόσφυγας, είναι υποχρεωμένος να παρακολουθήσει πρόγραμμα κοινωνικής ένταξης από την αρμόδια υπηρεσία. Υποβάλλει την αίτηση και γίνεται δεκτός στο πρόγραμμα κοινωνικής ένταξης. Παράλληλα με την παρακολούθηση αυτού του προγράμματος, αποφασίζει να δουλέψει ως πωλητής σε κατάστημα μίας μεγάλης εταιρίας εμπορίου τροφίμων. Υποβάλει αίτηση στην εταιρία εμπορίου τροφίμων και προσλαμβάνεται.

Ύστερα από κάποια χρόνια, ο χρήστης-πρόσφυγας, επιθυμεί να συμμετέχει σε πρόγραμμα μετεγκατάστασης σε άλλη χώρα της ΕΕ. Συγκεκριμένα, λόγω του ότι μετά τη λήξη της σύμβασής του με την εταιρία τροφίμων αντιμετωπίζει δυσκολίες στην εύρεση εργασίας, ο χρήστης υποβάλει σχετική αίτηση μετεγκατάστασης, έτσι ώστε να μετεγκατασταθεί στη

Γερμανία. Μέλη της οικογένειας του χρήστη-πρόσφυγα διαμένουν στη Φρανκφούρτη της Γερμανίας. Η αίτηση εξετάζεται από Αρμόδια Υπηρεσία της Γερμανίας. Η μετεγκατάσταση του χρήστη εγκρίνεται και αυτός μετεγκαθίσταται στη Φρανκφούρτη.

Ο χρήστης αποφασίζει να δημιουργήσει μία επιχείρηση στη Φρανκφούρτη. Κάνει αίτηση σε πρόγραμμα χρηματοδότησης της Ε.Ε. Λαμβάνει τη χρηματοδότηση και θεωρεί συμβολαιογραφικά όλα τα έγγραφα που σχετίζονται με τις δαπάνες της χρηματοδότησης, έτσι ώστε οι ελεγκτικοί μηχανισμοί να μπορούν να επαληθεύσουν τις πληροφορίες.

Το παραπάνω σενάριο χρήσης απεικονίζεται στο παρακάτω διάγραμμα:



Εικόνα 32: Σενάριο χρήσης : Η διαδρομή ένταξης ενός πρόσφυγα στην κοινωνία της Ε.Ε

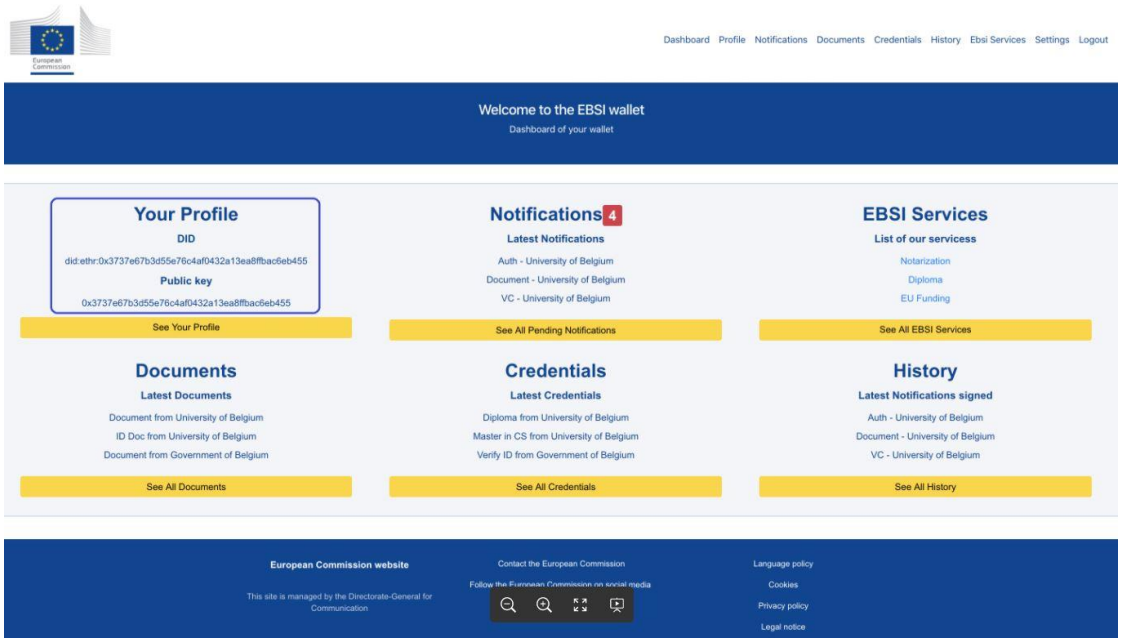
4.2 Περιγραφή υλοποίησης του σεναρίου χρήσης με τη χρήση του EBSI

Σε αυτό το κεφάλαιο, η διαδρομή του χρήστη παρουσιάζεται με τη χρήση των λειτουργιών που είναι διαθέσιμες στο EBSI. Το ταξίδι αυτό του χρήστη ενσωματώνει αρκετές από τις περιπτώσεις χρήσης που αναλύθηκαν στο κεφάλαιο 3, οι οποίες αξιοποιούν τις κοινές εφαρμογές EBSI και τις βασικές διεπαφές υπηρεσιών. Ο σχεδιασμός προϋποθέτει ότι ο χρήστης διαθέτει έξυπνη κινητή συσκευή. Επίσης, προκειμένου να εγκαταστήσει την εφαρμογή wallet του EBSI θα πρέπει να έχει δημιουργήσει προηγουμένως ένα λογαριασμό EU Login, ο οποίος για να δημιουργηθεί απαιτεί μόνο ως είσοδο το ονοματεπώνυμο, ένα e-mail, και επιλογή γλώσσας. [1]

Βήμα 1ο

Εγκατάσταση του Wallet EBSI	
1	Ο χρήστης (Holder) επιλέγει και εγκαθιστά μία εφαρμογή wallet (Agent Requester) στην συσκευή του.
2	Ο χρήστης ξεκινά την εφαρμογή και τη διαμορφώνει εισάγοντας password (συμπεριλαμβάνεται η αποδοχή όρων και προϋποθέσεων). Αυτή η πράξη πυροδοτεί τη δημιουργία ιδιωτικών κλειδιών (private keys), τα οποία αποθηκεύονται στην αλυσίδα κλειδιών που αποθηκεύεται στην συσκευή. Μέχρι το σημείο αυτό, ο χρήστης διαθέτει ένα πορτοφόλι EBSI και ένα αναγνωριστικό DID.

Στην παρακάτω εικόνα φαίνεται το dashboard του χρήστη. Εμφανίζονται, για παράδειγμα, το αναγνωριστικό DID του, το δημόσιο κλειδί του, οι παρεχόμενες από το EBSI υπηρεσίες καθώς και τα διαπιστευτήρια (credentials) που διαθέτει. [2]



Εικόνα 33: Wallet Dashboard [171]

[1] https://webgate.ec.europa.eu/cfcas3/tracesnt-webhelp/Content/C_EU%20login/create-a-new-EU-login-account.htm

[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITALEBSI/Wireframes+and+Screens+Specification

Βήμα 2ο

Ο χρήστης, εξαιτίας του γεγονότος ότι είναι υπήκοος τρίτης χώρας, δεν διαθέτει eID. Επομένως, δεν μπορεί να ακολουθήσει τη βασική λειτουργία του Online Onboarding (V1). Αντίθετα, ακολουθεί τη διαδικασία του Offline Onboarding (V2+).

Offline Onboarding	
1	Ο χρήστης-υπήκοος τρίτης χώρας (Holder) βρίσκεται στο Κέντρο υποδοχής και Ταυτοποίησης και πραγματοποιεί τη διαδικασία Onboarding απευθυνόμενος σε υπαλλήλους του κλιμακίου ασύλου που βρίσκεται εκεί.
2	Ο στόχος του χρήστη είναι να δημιουργήσει μία επαληθεύσιμη ταυτότητα στο σύστημα.
3	Ο χρήστης απευθύνεται σε έναν υπάλληλο (service provider) της Υπηρεσίας Ασύλου και ζητά την έκδοση ενός Verifiable ID (ως Verifiable Credential).
4	Ο χρήστης-υπήκοος τρίτης χώρας επιδεικνύει την ταυτότητα του ή το διαβατήριο του ή κάποιο άλλο ταξιδιωτικό έγγραφο στον υπάλληλο.
5	Ο υπάλληλος ταυτοποιεί τον χρήστη και του παρέχει ένα «σύνδεσμο σε βάθος» - deep link.
6	Ο χρήστης χρησιμοποιεί αυτό το deep link έτσι ώστε να συνδέσει την εφαρμογή του (Agent requester) με τις υπηρεσίες του Υπουργείου Μετανάστευσης και Ασύλου (Agent Provider). Η εφαρμογή βρίσκει το endpoint, όπου το Υπουργείο Μετανάστευσης και Ασύλου (μέσω της Υπηρεσίας Ασύλου) εκδίδει VC, και δημιουργεί ένα αίτημα έκδοσης VC (Verifiable ID).
7	Πραγματοποιείται έκδοση της επαληθεύσιμης ταυτότητας του χρήστη (Verifiable ID).Η επαληθεύσιμη ταυτότητα περιλαμβάνει τα εξής: • Credential ID (προαιρετικά) • Credential Type: Verifiable ID • Εκδότης (Issuer - Υπουργείο Μετανάστευσης και Ασύλου) • Credential Subject • Ισχυρισμοί : Σχετικά με την ταυτοποίηση / έλεγχο ταυτότητας • Ημερομηνία έκδοσης • Αποδείξεις: πχ eSignature
8	Τώρα ο χρήστης διαθέτει ένα EBSI ESSIF με αναγνωριστικό DID.

Βήμα 3ο

Κατάθεση αίτησης ασύλου	
1	Ο χρήστης επισκέπτεται τον ιστότοπο της Υπηρεσίας Ασύλου και επιλέγει το αντίστοιχο πεδίο για τη δημιουργία αίτησης ασύλου.
2	Η Υπηρεσία Ασύλου αποστέλλει στο χρήστη μια σελίδα προορισμού για να δημιουργήσει ένα αίτημα επαληθεύσιμης παρουσίασης (Verifiable Presentation), μαζί με την αποδοχή του GDPR και άλλους όρους και προϋποθέσεις, καθώς και τη λίστα των απαιτούμενων Verifiable Credentials.
3	Με βάση τα απαιτούμενα έγγραφα, ο χρήστης παρουσιάζει μέσω του πορτοφολιού του (Verifiable Presentation) στην Υπηρεσία Ασύλου τα εξής : • Το Verifiable ID του • Την αποδοχή του GDPR και των άλλων όρων και προϋποθέσεων • Τα απαραίτητα Verifiable Credentials Κάποια από τα Verifiable Credentials μπορεί να είναι η χώρα καταγωγής, το όνομα πατέρα, μητέρας, τα αίτια αίτησης διεθνούς προστασίας, η επιθυμητή γλώσσα

	εξέτασης της αίτησης κ.α. Επίσης, η Υπηρεσία Ασύλου μπορεί να αποστείλει στο χρήστη μια σελίδα προορισμού για να πραγματοποιηθεί η συνέντευξη διαδικτυακά.
4	Η Υπηρεσία Ασύλου στέλνει έναν αριθμό αναφοράς αιτήματος στο πορτοφόλι του χρήστη, που σχετίζεται με το αίτημά του.
5	Ο χρήστης λαμβάνει μία ειδοποίηση (πχ μέσω e-mail) με αυτήν την πληροφορία.
6	Επίσης, η Υπηρεσία Ασύλου αποδίδει στο χρήστη, ως επαληθεύσιμη βεβαίωση (Verifiable Attestation), τον Προσωρινό Αριθμό Ασφάλισης και Υγειονομικής Περίθαλψης Αλλοδαπού (Π.Α.Α.Υ.Π.Α.), μιας και αυτός αποδίδεται σε όλους ανεξαιρέτως τους αιτούντες άσυλο.

Βήμα 4ο

Απόρριψη αίτησης ασύλου	
1	Η υπηρεσία ασύλου εξετάζει τις πληροφορίες που έχει λάβει από το χρήστη: • Επαληθεύει ότι όλα τα απαραίτητα έγγραφα (διαπιστευτήρια), έχουν ληφθεί. • Επαληθεύει την ταυτότητα του χρήστη (μέσω ESSIF). • Εξετάζει αν ο χρήστης, με βάσει τα στοιχεία που έχει προσκομίσει, δικαιούται καθεστώς πρόσφυγα.
2	Η Υπηρεσία Ασύλου αποφασίζει ότι δε θα χορηγήσει καθεστώς πρόσφυγα στον χρήστη-αιτούντα άσυλο.
3	Η Υπηρεσία Ασύλου- μέσω του συμβατού με το EBSI πορτοφολιού της - υπογράφει και στέλνει μια ειδοποίηση μέσω email στο χρήστη για να τον ενημερώσει για την απόρριψη της αίτησης.

Βήμα 5ο

Άσκηση προσφυγής	
1	Ο χρήστης επισκέπτεται τον ιστότοπο της Υπηρεσίας Ασύλου και επιλέγει το αντίστοιχο πεδίο για την κατάθεση της προσφυγής.
2	Η Υπηρεσία Ασύλου αποστέλλει στο χρήστη μια σελίδα προορισμού για να δημιουργήσει ένα αίτημα επαληθεύσιμης παρουσίασης (Verifiable Presentation), μαζί με την αποδοχή του GDPR και άλλους όρους και προϋποθέσεις, καθώς και τη λίστα των απαιτούμενων Verifiable Credentials.
3	Με βάση τα απαιτούμενα έγγραφα, ο χρήστης παρουσιάζει μέσω του πορτοφολιού του (Verifiable Presentation) στην Υπηρεσία Ασύλου τα εξής : • Το Verifiable ID του • Την αποδοχή του GDPR και των άλλων όρων και προϋποθέσεων • Τα απαραίτητα Verifiable Credentials (προσφυγή που υπογράφεται από τον ίδιο το χρήστη ή τον δικηγόρο του)
4	Η Υπηρεσία Ασύλου στέλνει έναν αριθμό αναφοράς αιτήματος στο πορτοφόλι του χρήστη, που σχετίζεται με το αίτημά του.
5	Ο χρήστης λαμβάνει μία ειδοποίηση (πχ μέσω e-mail) με αυτήν την πληροφορία.

Βήμα 6ο

Χορήγηση Καθεστώτος Πρόσφυγα	
1	Η υπηρεσία ασύλου εξετάζει τις πληροφορίες που έχει λάβει από το χρήστη κατά τη διαδικασία προσφυγής: • Επαληθεύει ότι όλα τα απαραίτητα έγγραφα (διαπιστευτήρια), έχουν ληφθεί. • Επαληθεύει την ταυτότητα του χρήστη (μέσω ESSIF). • Εξετάζει αν ο χρήστης, με βάσει τα στοιχεία που έχει προσκομίσει, δικαιούται καθεστώς πρόσφυγα.
2	Η Υπηρεσία Ασύλου αποφασίζει τη χορήγηση καθεστώτος πρόσφυγα στον χρήστη-αιτούντα άσυλο.
3	Η Υπηρεσία Ασύλου- μέσω του συμβατού με το EBSI πορτοφολιού της - υπογράφει και στέλνει μια ειδοποίηση μέσω email στο χρήστη για λήψη και αποδοχή της επαληθεύσιμης βεβαίωσης (Verifiable Attestation) αναγνώρισής του ως πρόσφυγα. Επίσης, λόγω του ότι ο χρήστης είναι πλέον αναγνωρισμένος πρόσφυγας μεταβάλλεται ο Π.Α.Α.Υ.Π.Α. του σε Α.Μ.Κ.Α, ο οποίος αποστέλλεται, επίσης, ως επαληθεύσιμη βεβαίωση στον χρήστη.

Βήμα 7ο

Παρακολούθηση προγράμματος κοινωνικής ένταξης	
1	Ο χρήστης περιηγείται στον ιστότοπο της υπηρεσίας που παρέχει το πρόγραμμα κοινωνικής ένταξης και επιλέγει το αντίστοιχο πεδίο προκειμένου να εγγραφεί σε αυτό.
2	Ένα αίτημα παρουσίασης αποστέλλεται από την υπηρεσία στο προφίλ του χρήστη, συμπεριλαμβανομένου του σκοπού (όροι και προϋποθέσεις) και μια λίστα με τις απαιτούμενες Verifiable Attestations (συμπεριλαμβανομένης της επαληθεύσιμης βεβαίωσης ότι πρόκειται για αναγνωρισμένο πρόσφυγα).
3	Ο χρήστης αποστέλλει την επαληθεύσιμη βεβαίωση, που έχει λάβει από την Υπηρεσία Ασύλου, η οποία επικυρώνει ότι είναι αναγνωρισμένος πρόσφυγας, καθώς και την αίτηση εγγραφής του στο πρόγραμμα κοινωνικής ένταξης.
4	Η υπηρεσία λαμβάνει το αίτημα του χρήστη μέσω του συμβατού με το EBSI πορτοφόλι της.
5	Η υπηρεσία επαληθεύει ότι: • Η ταυτότητα του χρήστη είναι σωστή (Verifiable ID). • Ο χρήστης είναι αναγνωρισμένος πρόσφυγας.
6	Η υπηρεσία, μέσω του συμβατού με το EBSI πορτοφολιού της, στέλνει μια ειδοποίηση στο χρήστη για λήψη και αποδοχή επαληθεύσιμης βεβαίωσης (VA) με την επιβεβαίωση εγγραφής και τις λεπτομέρειες (αυτές μπορεί να είναι ημερομηνία έναρξης, ημερομηνία λήξης κ.λπ.)

Βήμα 8ο

Αίτηση εργασίας και πρόσληψη σε εταιρία εμπορίου τροφίμων	
1	Ο χρήστης περιηγείται στον ιστότοπο της εταιρίας, βρίσκει τη θέση εργασίας που τον ενδιαφέρει (πωλητής) και επιλέγει το αντίστοιχο πεδίο προκειμένου να υποβάλλει αίτηση.
2	Ένα αίτημα παρουσίασης αποστέλλεται από την εταιρία στο προφίλ του χρήστη, συμπεριλαμβανομένου του σκοπού (όροι και προϋποθέσεις) και μια λίστα με τις απαιτούμενες Verifiable Attestations.
3	Ο χρήστης αποστέλλει

	• Το VA που έχει λάβει από την Υπηρεσία Ασύλου, το οποίο επικυρώνει ότι είναι αναγνωρισμένος πρόσφυγας. • Το VA από την υπηρεσία παροχής του προγράμματος κοινωνικής ένταξης, το οποίο επικυρώνει ότι έχει πραγματοποιήσει εγγραφή στο πρόγραμμα.
4	Η υπηρεσία λαμβάνει το αίτημα του χρήστη μέσω του συμβατού με το EBSI πορτοφόλι της.
5	Η υπηρεσία επαληθεύει ότι: • Η ταυτότητα του χρήστη είναι σωστή (Verifiable ID). • Ο χρήστης είναι αναγνωρισμένος πρόσφυγας και παρακολουθεί πρόγραμμα κοινωνικής ένταξης. • Είναι κατάλληλος για αυτή τη θέση εργασίας.
6	Η υπηρεσία, μέσω του συμβατού με το EBSI πορτοφολιού της, στέλνει μια ειδοποίηση στο χρήστη για λήψη και αποδοχή της επαληθεύσιμης βεβαίωσης (VA) με την επιβεβαίωση πρόσληψης και τις λεπτομέρειες.

Βήμα 9ο

Ολοκλήρωση παρακολούθησης προγράμματος ένταξης	
	Μόλις ο χρήστης ολοκληρώσει την παρακολούθηση του προγράμματος, η υπηρεσία που το παρέχει σφραγίζει την επαληθεύσιμη βεβαίωση (Verifiable Attestation) που αντιπροσωπεύει το πιστοποιητικό του (ψηφιακά υπογεγραμμένο διαπιστευτήριο) και τον ειδοποιεί για τη διαθεσιμότητα της επαληθεύσιμης πιστοποίησης. Όταν γίνει αποδεκτή, ο χρήστης θα την αποθηκεύσει στο EBSI πορτοφόλι του (ήδη συνδεδεμένο με το DID του).

Βήμα 10ο

Λήξη σύμβασης εργασίας	
	Η σύμβαση εργασίας του χρήστη-πρόσφυγα με την εταιρία τροφίμων λήγει. Η εταιρία, έχει τη δυνατότητα να παρέχει μια επαληθεύσιμη βεβαίωση (Verifiable Attestation) στο χρήστη που επιβεβαιώνει ότι εργάστηκε σε αυτή με όλες τις υπόλοιπες λεπτομέρειες (για πόσο χρονικό διάστημα, σε ποια θέση εργασίας κτλ.). Η εταιρία ειδοποιεί για τη διαθεσιμότητα της επαληθεύσιμης πιστοποίησης. Όταν γίνει αποδεκτή, ο χρήστης την αποθηκεύει στο EBSI πορτοφόλι του .

Βήμα 11ο

Μετεγκατάσταση	
1	Ο χρήστης επισκέπτεται τον ιστότοπο της αρμόδιας υπηρεσίας της Γερμανίας και επιλέγει το αντίστοιχο πεδίο για τη δημιουργία αίτησης μετεγκατάστασης.
2	Η γερμανική υπηρεσία αποστέλλει στο χρήστη μια σελίδα προορισμού για να δημιουργήσει ένα αίτημα επαληθεύσιμης παρουσίασης (Verifiable Presentation), καθώς και τη λίστα των απαιτούμενων Verifiable Credentials.
3	Με βάση τα απαιτούμενα έγγραφα, ο χρήστης παρουσιάζει μέσω του πορτοφολιού του (Verifiable Presentation) στη γερμανική υπηρεσία τα εξής : • Το Verifiable ID του • Το VA που έχει λάβει από την Υπηρεσία Ασύλου και επιβεβαιώνει ότι έχει αναγνωριστεί ως πρόσφυγας στην Ελλάδα

	• Το VA που επιβεβαιώνει ότι έχει ολοκληρώσει την παρακολούθηση προγράμματος κοινωνικής ένταξης στην Ελλάδα. • Το VA που επιβεβαιώνει την εργασία του σε ελληνική εταιρία. • Τα υπόλοιπα Verifiable Credentials (πχ το λόγο που αιτείται μετεγκατάσταση, την επιθυμητή γλώσσα εξέτασης της αίτησης).
4	Η Υπηρεσία Ασύλου στέλνει έναν αριθμό αναφοράς αιτήματος στο πορτοφόλι του χρήστη, που σχετίζεται με το αίτημά του.
5	Ο χρήστης λαμβάνει μία ειδοποίηση (πχ μέσω e-mail) με αυτήν την πληροφορία.
6	Η υπηρεσία ασύλου εξετάζει τις πληροφορίες που έχει λάβει από το χρήστη: • Επαληθεύει τα απαραίτητα έγγραφα (διαπιστευτήρια), που έχουν ληφθεί. • Επαληθεύει την ταυτότητα του χρήστη (μέσω ESSIF). • Εξετάζει αν θα δεχθεί τη μετεγκατάσταση του πρόσφυγα, με βάσει τα στοιχεία που έχει προσκομίσει.
7	Η υπηρεσία αποφασίζει να δεχθεί τον πρόσφυγα στη Γερμανία, μέσω μετεγκατάστασης από την Ελλάδα.
8	Μέσω του συμβατού με το EBSI πορτοφολιού της υπογράφει και στέλνει μια ειδοποίηση μέσω email στο χρήστη για λήψη και αποδοχή της επαληθεύσιμης βεβαίωσης (Verifiable Attestation) μετεγκατάστασης του πρόσφυγα.

Βήμα 12ο

Από τη στιγμή που ο χρήστης διαθέτει ήδη ένα EBSI ESSIF wallet με αναγνωριστικό DID (το έχει διαμορφώσει στα προηγούμενα βήματα), μπορεί να χρησιμοποιήσει τη λειτουργία της συμβολαιογραφικής θεώρησης εγγράφων (Notarisation) του EBSI.

Χρηματοδότηση	
1	Ο χρήστης επιθυμεί να δημιουργήσει μία επιχείρηση στην Γερμανία και συμμετέχει σε μία πρόσκληση υποβολής προτάσεων προκειμένου να λάβει κεφάλαια της ΕΕ για τη δημιουργία της.
2	Συμπληρώνει μια αίτηση επιχορήγησης και στη συνέχεια τη σαρώνει και τη θεωρεί συμβολαιογραφικά μέσω του Notarisation Component του EBSI. Γι' αυτό το σκοπό: • Ο χρήστης αποθηκεύει τα αρχεία που πρέπει να θεωρηθούν συμβολαιογραφικά σε έναν χώρο αποθήκευσης εκτός αλυσίδας (π.χ. EBSI off-chain storage component) • Ο χώρος αποθήκευσης είναι προσβάσιμος μέσω του component Ελέγχου -Audit Component-(application layer του EBSI).
3	Το Audit Component δημιουργεί και παράγει τα hashes (τιμές κατακερματισμού) των εγγράφων και, στη συνέχεια, τα αποθηκεύει στην αλυσίδα.
4	Η πρόταση του χρήστη επιλέγεται και αυτός λαμβάνει χρηματοδότηση από την Ε.Ε. Η συμφωνία χρηματοδότησης θεωρείται συμβολαιογραφικά μέσω του Notarisation Component, με όμοιο τρόπο.
5	Ο χρήστης αποστέλλει στη διαχειριστική αρχή έγγραφα τα οποία έχει θεωρήσει συμβολαιογραφικά (notarized), και τα οποία αιτιολογούν τη δαπάνη της χρηματοδότησης (πχ τιμολόγια, αποδείξεις πληρωμών).
6	Στα πλαίσια ενός μελλοντικού ελέγχου, είναι δυνατή η επαλήθευση της ακεραιότητας και της χρονικής σήμανσης των εγγράφων (audit trail).

5 Συμπεράσματα

Η ανακάλυψη του Blockchain αποτελεί μία από τις μεγαλύτερες τεχνολογικές ανακαλύψεις των τελευταίων ετών. Από την εφεύρεση του Bitcoin (2008) και ύστερα, η τεχνολογία του Blockchain άρχισε να χρησιμοποιείται ευρέως, και γρήγορα επεκτάθηκε σε πολλούς και διαφορετικούς τομείς πέραν των ψηφιακών νομισμάτων. Το Blockchain αποτελεί ένα αποκεντρωμένο δίκτυο κόμβων, γεγονός που έχει οδηγήσει στο μικρό κόστος και στη μεγάλη αποδοτικότητα των συναλλαγών που πραγματοποιούνται σε αυτό. Επίσης, προσδίδει στις συναλλαγές και στα έγγραφα χρονοσήμανση, με αποτέλεσμα εάν κάποιος προκαλέσει οποιαδήποτε αλλαγή σε αυτά, αυτό να γίνεται πάντα αντιληπτό. Ως εκ τούτου, είναι εύκολος ο εντοπισμός καθώς και η επαλήθευση των καταγραφών που έχουν επικυρωθεί από το blockchain. Το Blockchain, λοιπόν, είναι μια τεχνολογία, η οποία λόγω των βασικών χαρακτηριστικών της (αποκέντρωση, διαφάνεια, ελεγξιμότητα και σταθερότητα) δύναται να βρει εφαρμογή σε πολλούς τομείς της ανθρώπινης ζωής, όπως είναι ο δημόσιος τομέας, οι κυβερνητικές διεργασίες, η εφοδιαστική αλυσίδα προϊόντων, η αποθήκευση αρχείων και η διαχείριση των προσωπικών δεδομένων, ενισχύοντας την ακεραιότητα και την ασφάλεια των διάφορων τύπων συναλλαγών και την αποτροπή δόλιας συμπεριφοράς. Σημαντική βοήθεια, σε αυτήν την κατεύθυνση, προσφέρουν οι έξυπνες συμβάσεις (smart contracts), οι οποίες κάνουν δυνατή την αυτόματη ανταλλαγή ψηφιακών στοιχείων μεταξύ οντοτήτων. Η αξιοπιστία του δικτύου Blockchain εξασφαλίζεται με τη χρήση των αλγορίθμων συναίνεσης, οι οποίοι οδηγούν το κατανεμημένο δίκτυο σε επίτευξη συμφωνίας, ενώ η ασφάλεια των συναλλαγών επιτυγχάνεται μέσω της τεχνολογίας της ψηφιακής υπογραφής.

Όσον αφορά στο μηχανισμό συναίνεσης, θα πρέπει να δίνεται ιδιαίτερη σημασία στην επιλογή του για ένα συγκεκριμένο δίκτυο blockchain. Στον πεδίο των μηχανισμών συναίνεσης παρατηρείται μία χρονική εξέλιξη. Ο πρώτος αλγόριθμός, που χρησιμοποιήθηκε ήταν ο αλγόριθμος απόδειξης εργασίας (PoW). Όπως προκύπτει από την έρευνα του πρώτου κεφαλαίου της παρούσας διπλωματικής, αποτελεί τον πιο αξιόπιστο αλγόριθμο συναίνεσης που υπάρχει σήμερα. Αυτό οφείλεται στο γεγονός ότι οποιοδήποτε δίκτυο blockchain χρησιμοποιεί τον συγκεκριμένο αλγόριθμο συναίνεσης είναι σε μεγάλο βαθμό αποκεντρωμένο, καθώς προτού επιβεβαιωθεί ένα νέο block συναλλαγών, πρέπει να επαληθευτεί και να εγκριθεί από την πλειονότητα των κόμβων του δικτύου. Για αυτό το λόγο, ο μηχανισμός αυτός, πρώτον, δεν μπορεί να εφαρμοστεί σε μεγάλο αριθμό περιπτώσεων χρήσης, στις οποίες θα πρέπει να έχουν το μεγαλύτερο μερίδιο ευθύνης της λήψης αποφάσεων κάποιες κεντρικές αρχές και, δεύτερον, παρουσιάζει σημαντικό πρόβλημα κλιμάκωσης. Ακόμα και τα δίκτυα που χρησιμοποίησαν τον μεταγενέστερο αλγόριθμο απόδειξης πονταρίσματος (PoS), που ουσιαστικά αποτέλεσε τη βελτίωση του αλγορίθμου απόδειξης εργασίας, δεν κατάφεραν πραγματικά να λύσουν το πρόβλημα κλιμάκωσης. Στη συνέχεια, εφαρμόστηκε ο αλγόριθμος απόδειξης εξουσίας (PoA), ο οποίος είναι σε θέση να εκτελεί πολύ περισσότερες συναλλαγές ανά δευτερόλεπτο, σε σχέση με του δύο προγενέστερούς του. Ωστόσο, η ιδέα του μηχανισμού απόδειξης εξουσίας είναι ότι, επί της ουσίας, ξεπερνά την αποκέντρωση. Έτσι θα μπορούσε κανείς να πει ότι αυτό το μοντέλο αλγόριθμου συναίνεσης είναι απλώς μια προσπάθεια με στόχο να καταστούν τα κεντρικά συστήματα πιο αποτελεσματικά. Το γεγονός αυτό καθιστά αυτόν το μηχανισμό μια πολύ ενδιαφέρουσα λύση για μεγάλες εταιρείες και οργανισμούς. Ωστόσο, από την άλλη πλευρά, οι πτυχές του αμετάβλητου τίθενται υπό αμφισβήτηση όταν η λογοκρισία, στα πλαίσια της χρήσης του συγκεκριμένου μηχανισμού συναίνεσης, δεν είναι δύσκολο να επιτευχθεί.

Συμπεραίνουμε, λοιπόν, ότι ο τομέας των αλγορίθμων συναίνεσης παρουσιάζει ιδιαίτερο ερευνητικό ενδιαφέρον. Θα πρέπει να γίνεται ενδελεχής έρευνα για την επιλογή μηχανισμού συναίνεσης, ο οποίος θα πρέπει να προσαρμόζεται σε κάθε μοναδική περίπτωση χρήσης του Blockchain. Ανάλογα με το επίπεδο αποκέντρωσης που απαιτεί η κάθε περίπτωση εφαρμογής του Blockchain, θα πρέπει να επιλέγεται ή να υλοποιείται ο κατάλληλος αλγόριθμος συναίνεσης, ο οποίος βέβαια δεν θα επιτρέπει την ύπαρξη λογοκρισίας και, τελικά, την αμφισβήτηση της επίτευξης συμφωνίας στο σύστημα.

Από την έρευνα που πραγματοποιήθηκε στα κεφάλαια 3 και 4, προκύπτει το συμπέρασμα ότι η τεχνολογία του Blockchain μπορεί να χρησιμοποιηθεί εποικοδομητικά για τη διαχείριση των μεταναστευτικών και προσφυγικών ροών προς την Ευρωπαϊκή Ένωση, καθώς και την ένταξη των προσφύγων και μεταναστών στην ευρωπαϊκή κοινωνία. Ωστόσο, προκειμένου να καταστεί πλήρως αποτελεσματική η εφαρμογή της τεχνολογίας του Blockchain προς αυτήν την κατεύθυνση, θα πρέπει να γίνουν σημαντικά βήματα τόσο σε επίπεδο οργάνωσης του σχεδίου κατανομής και ένταξης των ξένων υπηκόων στην Ευρωπαϊκή Ένωση, όσο και σε επίπεδο τεχνολογικών υποδομών. Πρώτα από όλα, τα επίπεδα ετοιμότητας όσον αφορά στην αποδοχή μεταναστών και προσφύγων είναι διαφορετικά στα διάφορα κράτη της Ευρωπαϊκής Ένωσης, λόγω των άνισων υποδομών και οικονομικών πόρων, με αποτέλεσμα σε κάποιες χώρες να αντιστοιχεί μεγάλο ποσοστό των αιτούντων άσυλο και σε άλλες ένα πολύ μικρό ποσοστό. Επιπλέον, εξαιτίας της σημαντικής γραφειοκρατίας και την εμπλοκή διαφορετικών υπηρεσιών σε αυτές τις διαδικασίες, οι αιτούντες άσυλο και οι πρόσφυγες καταλήγουν να παραμένουν για μεγάλα χρονικά διαστήματα στις χώρες υποδοχής, πολλές φορές κάτω από άσχημες συνθήκες διαβίωσης. Καταλαβαίνουμε, λοιπόν, ότι και οι συνθήκες αυτές μπορούν να οδηγήσουν τους ξένους υπηκόους τόσο στην παράνομη μετανάστευση, όσο και στην ενίσχυση των λεγόμενων «αγορών ασύλου» στην προσπάθειά τους να βρουν μία χώρα να ζήσουν χωρίς φόβο για τη ζωή και την υγεία τους. Θα πρέπει, επομένως, οι διαδικασίες να καθοριστούν πλήρως και με σαφήνεια και να είναι προσβάσιμες σε όλους τους ξένους υπηκόους που φτάνουν στην Ευρωπαϊκή Ένωση.

Όσον αφορά στον τομέα των τεχνολογικών υποδομών, συμπεραίνουμε ότι το EBSI (European Blockchain Services Infrastructure), που έχει ως στόχο την αξιοποίηση της τεχνολογίας του Blockchain για την παροχή κυρίως διασυνοριακών υπηρεσιών, μπορεί να προσφέρει μια εποικοδομητική λύση στη διαχείριση των μεταναστευτικών και προσφυγικών ροών, οι οποίες αποτελούν σημαντικό ζήτημα για την Ευρωπαϊκή Ένωση, ιδίως τα τελευταία χρόνια. Οι μηχανισμοί SSI (European Self Sovereign Identity) και Notarisation, εξασφαλίζουν τη διαφάνεια, την ελεγξιμότητα και την ασφάλεια στις διαδικασίες έκδοσης επαληθεύσιμων διαπιστευτηρίων και συμβολαιογραφικής θεώρησης εγγράφων, τα οποία απαιτούνται σε μία διαδρομή εισόδου και ένταξης ενός πρόσφυγα στην κοινωνία της Ευρωπαϊκής Ένωσης. Για αυτό το σκοπό, θα πρέπει οι αρμόδιες υπηρεσίες, όπως για παράδειγμα η Υπηρεσία Ασύλου, να αποκτήσουν τις απαιτούμενες EBSI υποδομές. Η υλοποίηση του σεναρίου χρήσης της εισόδου και ένταξης ενός υπηκόου τρίτης χώρας στην Ευρωπαϊκή Ένωση περιγράφτηκε αναλυτικά και στο κεφάλαιο 4. Ωστόσο, το EBSI είναι περισσότερο προσανατολισμένο για να εξυπηρετεί άτομα τα οποία είναι ήδη πολίτες της Ευρωπαϊκής Ένωσης. Προκειμένου, μέσα από την αξιοποίησή του, να βελτιωθούν οι προσφυγικές και μεταναστευτικές διαδικασίες, θα πρέπει να τις διευκολύνει. Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι ένας υπήκοος τρίτης χώρας θα πρέπει να ακολουθήσει τη διαδικασία του offline onboarding, αντί του online onboarding, λόγω του ότι δεν διαθέτει ταυτότητα eID. Για το σκοπό αυτό, θα πρέπει να έρθει σε επαφή με αρμόδιο υπάλληλο και να ταυτοποιηθεί εν μέρει μέσω paper-based διαδικασιών. Επιπροσθέτως, ενώ ο μηχανισμός συναίνεσης που χρησιμοποιεί το EBSI

είναι κατάλληλος για τη διαχείριση του μεταναστευτικού, όπως εξηγήθηκε πιο πάνω είναι ευάλωτος στη λογοκρισία.

Συμπερασματικά, η χρήση της τεχνολογίας Blockchain του EBSI για τη διαχείριση των μεταναστευτικών και προσφυγικών ροών ΕΕ, αποτελεί μία εποικοδομητική λύση. Ωστόσο, για να γίνει πράξη με τον πιο αποδοτικό τρόπο απαιτείται η αναγκαία υποστήριξη από την Ευρωπαϊκή Ένωση, τόσο σε επίπεδο επιχειρησιακής πολιτικής, όσο και σε επίπεδο υποδομών blockchain.

6 Βιβλιογραφία

[1] Pattanayak, P., Verma, S., Crosby, M., Nachiappan, Kalyanaraman ,V.: Blockchain technology: beyond bitcoin. http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf , 2016.

[2] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," Journal of Cryptology, vol. 3, no. 2, pp. 99–111, 1991.

[3] N. Satoshi , "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf, 2008.

[4] U. W. Chohan, "The Double Spending Problem and Cryptocurrencies," SSRN Electronic Journal, 2017.

[5] Mark Ryan, "Digital Cash", School of Computer Science, University of Birmingham.

[6] I. Bashir, Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition, Birmingham: Packt Publishing Ltd, 2018.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services*, vol. 14, no. 4, 2018, pp. 357-358.

[8] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Frankfurt, Germany: Apress, 2017, pp.19-25.

[9] J. Mattila, "The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures", ETLA Working Papers, no. 38, The Research Institute of the Finnish Economy (ETLA), Helsinki, 2016.

[10] S. Underwood, "Blockchain beyond bitcoin," Communications of the ACM, vol. 59, no. 11, 2016, pp. 15–17.

[11] G. Becker, "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis", Ruhr University Bochum, 2008, p. 16.

[12] N. Koblitz and A. J. Menezes, "Cryptocash, cryptocurrencies, and cryptocontracts" Designs, Codes and Cryptography, vol. 78, no. 1, 2015, pp. 87–102.

[13] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency," RFC Editor, Jun. 2013.

[14] E. Andreeva, C. Bouillaguet, O. Dunkelman, and J. Kelsey, "Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård," in Selected Areas in Cryptography, Springer Berlin Heidelberg, 2009, pp. 393–414.

[15] Andreeva E. et al., Second Preimage Attacks on Dithered Hash Functions. In: Smart N. (eds) Advances in Cryptology – EUROCRYPT 2008, Lecture Notes in Computer Science, vol. 4965, Springer, Berlin, Heidelberg, 2008

[16] I. Pentland et al., "Re-encrypting data on a hash chain", 2019.

[17] M. Kleppmann, "Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems", 1th ed., O'Reilly Media. p. 203.

[18] M. Ciampa, "CompTIA Security+ 2008 in depth.", Australia ;United States: Course Technology/Cengage Learning, 2009, p. 290.

[19] C. Cimpanu, "A quarter of major CMSs use outdated MD5 as the default password hashing scheme", ZDNet, 2019.

[20] A. K. Lenstra, "Key Lengths: Contribution to The Handbook of Information Security"

[21] "Linux Foundation Unites Industry Leaders to Advance Blockchain Technology - The Linux Foundation", The Linux Foundation, 2015.

[22] H. Lu, K. Huang, M. Azimi and L. Guo, "Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks," in IEEE Access, vol. 7, 2019, pp. 41426-41444.

[23] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan and E. Ragnoli, "Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-Blockchains," 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), Halifax, NS, Canada, 2018, pp. 1007-1016.

[24]Marozzi, M. ,(2015),"Construction, Robustness Assessment and Application of an Index of Perceived Level of Socio-economic Threat from Immigrants: A Study of 47 European Countries and Regions",Social Indicators Research. 128: 413–437

[25]Van Mol C., de Valk H. (2016) Migration and Immigrants in Europe: A Historical and Demographic Perspective. In: Garcés-Mascareñas B., Penninx R. (eds) Integration Processes and Policies in Europe. IMISCOE Research Series. Springer, Cham.

[26]Dietz, B., & Kaczmarczyk, P. (2008). On the demand side of international labour mobility: The structure of the German labour market as a causal factor of seasonal Polish migration. In C. Bonifazi, M. Okólski, J. Schoorl, & P. Simon (Eds.), International migration in Europe: New trends and new methods of analysis (IMISCOE research, pp. 37–64). Amsterdam: Amsterdam University Press

[27]Bade, K. J. (2003). Europa en movimiento: Las migraciones desde finales del siglo XVIII hasta nuestros días. Barcelona: Crítica.

[28]Castles, S., De Haas, H., & Miller, M. J. (2014). The age of migration: International population movements in the modern world. Basingstoke: Palgrave Macmillan.

[29]Barou, J. (2006). Europe, terre d'immigration: Flux migratoires et intégration. Grenoble: Presses Universitaires de Grénoble

[30]Castles, S., De Haas, H., & Miller, M. J. (2014). The age of migration: International population movements in the modern world. Basingstoke: Palgrave Macmillan.

[31]Lange, T. (2013). Return migration of foreign students and non-resident tuition fees. Journal of Population Economics, 26(2), 703–718.

[32]Konle-Seidl, R. and Bolits, G., 2016. Labour Market Integration of Refugees: Strategies and Good Practices : Study, European Parliament.

[33]Offe, Claus; Preuss, Ulrich Klaus (2016): Citizens in Europe. Essays on democracy, constitutionalism and European integration. Colchester: ECPR Press (ECPR Press essays)