ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

Σχολή Οικονομικών και Πολιτικών Επιστημών Τμήμα Επικοινωνίας και Μέσων Μαζικής Ενημέρωσης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΓΙΑ ΤΗΝ ΕΞΥΠΗΡΕΤΗΣΗ ΠΟΛΙΤΩΝ
Πρωτόκολλο Blockchain: Κρυπτονομίσματα και Ηλεκτρονική Ταυτοποίηση

ΓΙΑΝΝΑΚΟΥ ΜΑΡΙΑ-ΑΓΓΕΛΙΚΗ
Α.Μ.: 9983201500021

Πτυχιακή εργασία που κατατίθεται ως μέρος των απαιτήσεων του Προγράμματος Προπτυχιακών Σπουδών του Τμήματος Επικοινωνίας και Μέσων Μαζικής Ενημέρωσης (8ο εαρινό εξάμηνο)

Αθήνα, Ιούνιος, 2019

Επιτελική Σύνοψη

Η παρούσα εργασία μελετά την τεχνολογία του Πρωτοκόλλου Blockchain και παρουσιάζει τα πεδία στα οποία αυτό αναπτύσσεται, ήτοι, τις εφαρμογές Blockchain, τα κρυπτονομίσματα και την ανάπτυξη της τεχνολογίας στο πεδίο της Ηλεκτρονικής Ταυτοποίησης. Αναπτύσσονται οι έννοιες της δομής και της ασφάλειας του Blockchain, οι ‘έξυπνες’ ψηφιακές συμβάσεις, οι εφαρμογές στην τηλε-ιατρική, τα Bitcoins και τα εναλλακτικά κρυπτονομίσματα, η Ηλεκτρονική Ταυτοποίηση και η Ιδιωτικότητα με αναφορά σε παραδείγματα ψηφιακής ταυτοποίησης παγκοσμίως. Τέλος, γίνεται μια ‘επισκόπηση’ των δυνατοτήτων και των εγγενών χαρακτηριστικών της ελληνικής περίπτωσης σχετικά με το ενδεχόμενο να στηρίξει μια πρωτοβουλία όπως η ηλεκτρονική ταυτοποίηση, όντας ένα επίκαιρο κοινωνικό και πολιτικό ζήτημα της εποχής.

Ευχαριστίες

Θερμές ευχαριστίες στον επιβλέποντα Καθηγητή Δημήτρη Γκούσκο για όλες τις παρατηρήσεις, τις συμβουλές και τις κατευθύνσεις στο πλαίσιο της εργασίας, όπως και στον κο Νικόλαο Λάριο για την επικοινωνία, τις πληροφορίες και την πραγματοποίηση της συνέντευξης σχετικά με το σύστημα των ψηφιακών υπογραφών του ΕΚΠΑ.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Εισαγωγή

Η εργασία πραγματεύεται την ανάπτυξη, τη δομή και τις εφαρμογές του Πρωτοκόλλου Blockchain τη σημερινή εποχή. Σε πρακτικό επίπεδο, το Blockchain είναι ένα αποκεντρωμένο σύστημα που έχει ως στόχο την επίτευξη συμφωνίας μεταξύ χρηστών. Ειδικότερα, μια αλυσίδα Blockchain αποτελεί ένα διαμοιρασμένο δημόσιο κατάστιχο, όπως αποδίδεται στην ελληνική ορολογία, όπου οι συναλλαγές βρίσκονται κατανεμημένες σε ομάδες (blocks). Το δημόσιο κατάστιχο Blockchain μπορεί να λειτουργήσει ως μια πηγή δεδομένων για όλα τα μέλη που επιθυμούν να συναλλαχθούν, σε αντίθεση με το μοντέλο των ιδιωτικών βάσεων δεδομένων όπου κάθε μέλος διατηρεί τη δική του βάση. Όπως αναφέρει και ο Imran Bashir (2017, σελ. 219), "ο Κώδικας του ηλεκτρονικού υπολογιστή γίνεται ο Νόμος", με την κυριολεκτική έννοια του όρου.

Αν και η τεχνολογία έχει αναπτυχθεί ήδη εδώ και αρκετές δεκαετίες, τα αποτελέσματά της δεν φάνηκαν παρά τη στιγμή εμφάνισης του πρώτου κρυπτονομίσματος, του *Bitcoin*. Η σημασία έκτοτε είναι πολλαπλή τόσο σε τεχνικό επίπεδο, καθώς η τεχνολογία έχει επιτρέψει την ανάπτυξη ψηφιακών συμβολαίων και συναλλαγών με ισχύ μεταξύ των μερών, όσο και σε οικονομικό και παγκόσμιο επίπεδο, δεδομένης της χρήσης των κρυπτονομισμάτων και των πρωτοβουλιών για ηλεκτρονική ταυτοποίηση που αυξάνονται συνεχώς. Το Πρωτόκολλο, μέσω των χαρακτηριστικών στοιχείων της σταθερότητας, της διαφάνειας και της 'αποκεντροποίησης', χαρίζει κάτι "ανεπανάληπτο": 'την εμπιστοσύνη μέσω της ανωνυμίας', πράγμα που, όπως θα αναλυθεί και στα επόμενα κεφάλαια, αποτελεί τον ακρογωνιαίο λίθο του συστήματος. Σε αυτό το πλαίσιο, το ερευνητικό ερώτημα αφορά στη διερεύνηση των τομέων στους οποίους χρησιμοποιείται και θα μπορούσε εν δυνάμει να χρησιμοποιηθεί η τεχνολογία Blockchain για την εξυπηρέτηση πολιτών. Για την απάντηση στο ερευνητικό ερώτημα, θα ακολουθηθεί μια ποιοτική ανάλυση των ζητημάτων που θα αναπτυχθούν.

Ο δημιουργός του Bitcoin δεν έχει ακόμα ταυτοποιηθεί. Το σημαντικό, βέβαια, είναι μέσω της συνεισφοράς του νομίσματος αυτού να επιτευχθεί η δημιουργία ενός καλύτερου αύριο τόσο για την οικονομία, και δη τις αναπτυσσόμενες χώρες (όπως η Κένυα όπου η χρήση κρυπτονομισμάτων έχει γίνει πλέον ένα σταθερό μέσο συναλλαγής), όσο και για τον κόσμο και τα πεδία ανάπτυξής του γενικότερα. Έτσι, ο πολίτης καθίσταται στο κέντρο του ενδιαφέροντος καθώς, δεδομένης της σημαντικής θέσης του ηλεκτρονικού υπολογιστή σήμερα, ο ίδιος δύναται να αξιοποιήσει τις δυνατότητες του Πρωτοκόλλου Blockchain σε διοικητικό, οικονομικό και νομικό επίπεδο δίνοντας νέες λύσεις στις σχέσεις μεταξύ επιχειρήσεων και πολιτών, στις σχέσεις μεταξύ πολιτών και κράτους, πολιτών μεταξύ τους και δημόσιων ή ιδιωτικών οργανισμών μεταξύ τους. Στο πλαίσιο, άρα, της Ηλεκτρονικής Διακυβέρνησης το μέλλον αναμένεται, θα έλεγε κανείς, αρκετά επαναστατικό.

Στο πρώτο κεφάλαιο θα αναλυθούν οι πτυχές της τεχνολογίας Blockchain αναφορικά με τη δομή, τις εφαρμογές και τα θέματα ασφάλειας που προκύπτουν. Στο δεύτερο κεφάλαιο θα αναλυθούν τα κρυπτονομίσματα, με πρώτο φυσικά το Bitcoin. Ταυτόχρονα, θα μελετηθεί και η σχέση του με τα υπόλοιπα εναλλακτικά κρυπτονομίσματα (Altcoins). Στο τρίτο Κεφάλαιο, θα αναλυθούν οι έννοιες της Ασφάλειας, της Ιδιωτικότητας και της Ταυτοποίησης. Στο τέταρτο Κεφάλαιο θα γίνει αναφορά στην Ταυτοποίηση για Ανάπτυξη με μελέτες περίπτωσης ανά τον κόσμο και στο ελληνικό οικοσύστημα ηλεκτρονικής ταυτοποίησης.

Κεφάλαιο 1. Η τεχνολογία *Blockchain*

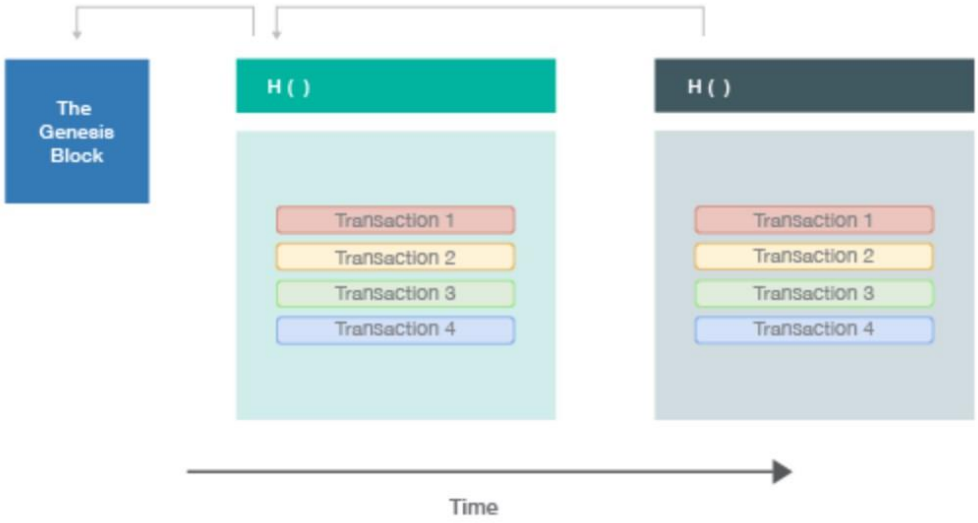
Υποκεφάλαιο 1.1 Η δομή και τα χαρακτηριστικά της τεχνολογίας

Η τεχνολογία Blockchain αποτελεί την *Πέμπτη επανάσταση* (Laurence, 2017, σελ. 7) των Η/Υ. Βασίζεται σε ένα αποκεντρωμένο σύστημα ομότιμης σύνδεσης μεταξύ υπολογιστών. Στην τεχνολογία αυτή στόχος είναι η αποτελεσματική διαχείριση δεδομένων μέσω της ύπαρξης εντός των διασυνδεδεμένων δικτύων ανεξάρτητων χρηστών[1]. Οι Η/Υ, που ονομάζονται *full nodes* (Quest, 2018, σελ. 177), δύνανται να βρίσκονται σε περισσότερες από μία τοποθεσίες αποδίδοντας έτσι την μέγιστη ασφάλεια στο σύστημα. Δεν είναι τυχαία η χρήση της τεχνολογίας από το Bitcoin[2]. Όταν μια πληροφορία έχει εγγραφεί στην αλυσίδα Blockchain, είναι σχεδόν αδύνατον αυτή να διαγραφεί. Έτσι, εμπορικές, εταιρικές και τραπεζικές συναλλαγές αποκτούν την μέγιστη επιθυμητή σταθερότητα[3] και ασφάλεια.

Η δομή της τεχνολογίας αποτελείται από *block*[4] (Laurence, 2017, σελ. 10 - 11), δηλαδή ομάδες καταχωρήσεων συναλλαγών που έχουν καταγραφεί στο δημόσιο κατάστιχο[5] και προς τούτο μοιάζουν με "μητρώα-λίστες" δεδομένων. Εν συνεχεία, αποτελείται από μια αλυσίδα (chain) που σχηματίζεται μέσω της μεθόδου σύνδεσης του ενός μπλοκ με το επόμενο (μέθοδος «σύναψης» - *hashing*). Η τεχνολογία σύνδεσηςσύναψης (hashing) υποβοηθά την ασφάλεια του συστήματος (Morabito, 2017, σελ. 70) καθώς κάθε «κρίκος» δημιουργείται μόνο από δεδομένα-κανόνες του προηγούμενου «κρίκου», κατά τρόπο ώστε ένα μπλοκ να αναγνωρίζει μόνο το προηγούμενό του κι όχι οποιοδήποτε άλλο. Γίνεται δηλαδή μια κρυπτογραφική

[1] 'Distributed network of independent users', όπως αποδίδεται ο όρος στην αγγλική βιβλιογραφία. [2]
[2] Το Bitcoin (βλ. Κεφάλαιο 2) αποτελεί ένα ψηφιακό νόμισμα το οποίο διαθέτει αγοραία συναλλακτική αξία με αποτέλεσμα την εμπορική συναλλαγή του όπως ακριβώς γίνεται με τα αποθέματα. Γνωστά πρωτόκολλα Blockchain περιλαμβάνουν το Bitcoin, το Ethereum, το Ripple, το Hyperledger και το Factom.
[3] Ο αγγλικός όρος: 'Immutability'.
[4] Εφ'εξής: *μπλοκ*
[5] Κατά την αγγλική ορολογία: 'Ledger'. Θα μπορούσε να ειπωθεί ότι αποτελεί ένα καθολικό οικονομικών συναλλαγών. Στην επίσημη ιστοσελίδα αναφέρεται ως κοινόχρηστο δημόσιο λογιστικό βιβλίο (https://bitcoin.org/el/how-it-works)

διαδικασία-"αυθεντικοποίηση". Εν τοις πράγμασι, τα ελαττώματα εντός της αλυσίδας λύνονται με την μέθοδο *forking* κατά την οποία επανεγγράφονται οι κανόνες που ένας κόμβος θα πρέπει να ακολουθήσει ώστε να καταστήσει ένα μπλοκ έγκυρο[6]. Τέλος, το σύστημα χρησιμοποιεί ένα δίκτυο κόμβων στους οποίους εγγράφονται όλες οι συναλλαγές εντός της αλυσίδας (Laurence, 2017, σελ. 11).



Εικόνα 1 Σχηματοποίηση της αλυσίδας Blockchain (Bird, 2016)

Ο πυρήνας της τεχνολογίας βασίζεται στον αλγόριθμο που δημιουργεί "ειλικρινή" (Drescher, 2017, σελ. 177) συστήματα που αυτο-διορθώνονται χωρίς την επίδραση κάποιου τρίτου παράγοντα. Αυτό είναι το αλγοριθμικό *consensus* (συμφωνία) το οποίο είναι διαφορετικό για κάθε αλυσίδα. Η ισχύς κάθε αλγοριθμικής συμφωνίας στηρίζεται στην παρουσία/απουσία απειλών (threats) και εμπιστοσύνης (trust)[7] μεταξύ χρηστών (Drescher, 2017). Έτσι, διασφαλίζεται από το σύστημα όλοι οι συνδεόμενοι υπολογιστές να έχουν τα ίδια δεδομένα, ώστε εάν κάποιος τα χάσει ή του υποκλαπούν να τα επαναφέρει από το σύστημα. Καθένας διαθέτει μια διεύθυνση-κλειδί που μόνο ένας κάτοχος-δημιουργός διαθέτει. Δυνατότητα αλλαγής

[6] Εάν κάποιοι κόμβοι αναγνωρίσουν την αναβάθμιση και άλλα όχι τότε δύναται η αλυσίδα να χωριστεί σε δύο ακολουθίες (γνωστό ως 'blockchain fork').
[7] Έτσι το δίκτυο παρουσιάζει και μια υψηλή ανθεκτικότητα σε βλάβες τύπου 'Byzantine Fault Tolerance'.

της διεύθυνσης πραγματοποιείται μόνο από τον ίδιο μέσω του ιδιωτικού κλειδιού και παράλληλα ο καθένας μπορεί να δημιουργήσει άπειρους συνδυασμούς διευθύνσεων χωρίς κίνδυνο ομοιότητας με άλλες διευθύνσεις. Πολύ βασικό είναι το γεγονός ότι η αλυσίδα είναι *ψευδο-ανώνυμη* (Dresher, 2017, σελ. 193) καθώς η ταυτότητα αυτών που είναι εντός της συναλλαγής αναπαρίσταται με μια διεύθυνση αποτελούμενη από τυχαίες συστοιχίες στοιχείων. Έτσι, η αλυσίδα χρησιμοποιείται για αποθήκευση δεδομένων όπως αξίες, ταυτότητες, δικαιώματα ιδιοκτησίας και άλλα (Drescher, 2017).

Η τεχνολογία Blockchain διακρίνεται σε *δημόσιο blockchain*, *ιδιωτικό blockchain* και *consortium blockchain* (Bambara & Allen, 2018, σελ. 13-14). Στην πρώτη περίπτωση, εισχωρεί οποιοσδήποτε και αναβαθμίζει την αλυσίδα. Η δεύτερη περίπτωση αφορά αλυσίδες με μικρό αριθμό παραγόντων όπου η εγκυρότητα ελέγχεται από έναν από αυτούς. Η τρίτη κατηγορία αναφέρεται σε έναν 'συνασπισμό'/ένωση αλυσίδων που χρησιμοποιείται κι ελέγχεται μαζί με άλλους οργανισμούς. Τα σημαντικότερα πλεονεκτήματα της δημόσιας αλυσίδας περιλαμβάνουν, κατά πρώτον, την προστασία των χρηστών από ενέργειες των σχεδιαστών λογισμικού οι οποίοι θα πρέπει, ακόμα και αυτοί, να ακολουθήσουν ορισμένους κανόνες και, κατά δεύτερον, το γεγονός ότι οι αλυσίδες αυτές είναι ανοιχτές για χρήση από διαφορετικούς παράγοντες.

Η τεχνολογία Blockchain (Drescher, 2017, σελ. 99-100), αφενός, χρησιμοποιεί την ασύμμετρη κρυπτογραφία *public-to-private* [8] με στόχο την ταυτοποίηση των λογαριασμών ή των χρηστών ώστε να διατηρηθεί η σύνδεση μεταξύ ιδιοκτήτη και ιδιοκτησίας και να πραγματοποιούνται οι συναλλαγές και, αφετέρου, χρησιμοποιεί την *private-to-public* ασύμμετρη κρυπτογραφία για να επιτρέπει αυτές. Όντως, τα συναλλαγόμενα δεδομένα πρέπει να περιλαμβάνουν αποδεικτικά στοιχεία ότι ο

[8] Σε ένα πιο τεχνικό επίπεδο, η μέθοδος της συμμετρικής κρυπτογραφίας αρχικά αφορούσε στην ύπαρξη ενός μόνο κλειδιού το οποίο διενεργούσε τόσο την κωδικοποίηση όσο και την αποκωδικοποίηση. Η τεχνολογική εξέλιξη όμως δημιούργησε την ασύμμετρη κρυπτογράφηση στην οποία γίνεται λόγος για δυο συμπληρωματικά κλειδιά: ένα δημόσιο κλειδί που δίνεται στον καθένα ανεξαρτήτως εμπιστοσύνης και ένα δεύτερο ιδιωτικό κλειδί που δεν μοιράζεται. Είτε ο καθένας προσθέτει την πληροφορία η οποία μπορεί να ανοιχθεί μόνο από έναν (*Public to Private*), και η διαδικασία αυτή μοιάζει με το ηλεκτρονικό ταχυδρομείο, είτε η πληροφορία δημιουργείται και κωδικοποιείται ή μετασχηματίζεται από έναν παράγοντα αλλά όλοι όσοι έχουν το αντίγραφο του δημόσιου κλειδιού δύνανται να την «αναγνώσουν» (*Private to Public*).

ιδιοκτήτης του λογαριασμού που μεταβιβάζει την ιδιοκτησία συμφωνεί με την μεταφορά αυτού του a priori ιδιόκτητου πράγματος.

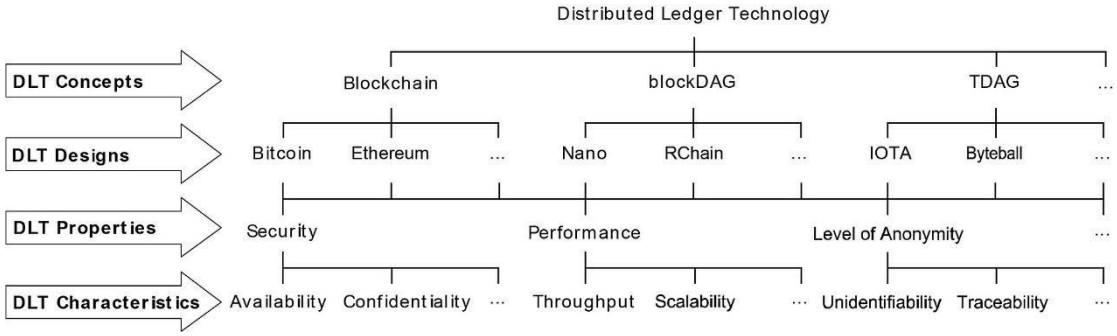
Επομένως, τα εν γένει 'συστατικά' της αλυσίδας (Bashir, 2017, σελ. 39-41) περιλαμβάνουν την ύπαρξη διευθύνσεων, συναλλαγών, διαφόρων μπλοκ, ομότιμης σύνδεσης, γλώσσας προγραμματισμού, μιας ψηφιακής μηχανής (virtual machine), μιας στατικής μηχανής (state machine), κόμβων-υπολογιστών και δυνατότητας δημιουργίας «έξυπνων» ηλεκτρονικών συμβάσεων[9].

Τα χαρακτηριστικά στοιχεία της τεχνολογίας, εν συνόψει, είναι: το πεδίο της διαμοιραζόμενης αλγοριθμικής συμφωνίας, η πιστοποίηση της συναλλαγής, οι βάσεις (platforms) των έξυπνων ηλεκτρονικών συμβάσεων, η μεταφορά αξιών μεταξύ ομότιμα συνδεδεμένων χρηστών, η δυνατότητα δημιουργίας κρυπτονομισμάτων, η δυνατότητα διασύνδεσης άυλου ή ενσώματου αγαθού στην αλυσίδα Blockchain κατά τρόπο αμετάκλητο, η παροχή προστασίας, η σταθερότητα και το αμετάβλητο των στοιχείων της αλυσίδας όπως και η μοναδικότητα κάθε συναλλαγής, στοιχεία που όπως ειπώθηκε και προηγουμένως δομούν την ασφάλεια[10].

[9] *Smart contracts*: Βλ. Υποκεφάλαιο 1.3

[10] Όπως θα γίνει αναφορά παρακάτω, ευαίσθητα στοιχεία όπως τα ιατρικής φύσεως δεδομένα δεν μεταβάλλονται.

Υποκεφάλαιο 1.2 Το πεδίο των *DLT* (Distributed Ledger Technologies)



Εικόνα 2 Οι Τεχνολογίες DLT. (Kannengießer et al., 2018)

Ένα δημόσιο κατάστιχο [11] αποτελεί μια μορφή ψηφιακών δεδομένων που αναβαθμίζεται και κρατείται από κάθε μέλος ξεχωριστά και ανεξάρτητα εντός του δικτύου. Υπάρχουν διαφορετικά είδη DLT[12]. Το Blockchain, εν προκειμένω, αποτελεί μια 'μακριά λίστα αρχείων'. Μόλις πραγματοποιηθεί μια συναλλαγή, οι κόμβοι στο δίκτυο την επιβεβαιώνουν για να ελέγξουν την πιστότητά της. Ύστερα, μετά την πιστοποίηση, η συναλλαγή λαμβάνει έναν μοναδικό κρίκο ταυτοποίησης (hash ID), συσχετιζόμενο με τον πρόσφατο κρίκο ταυτοποίησης της συναλλαγής, και αρχειοθετείται στο κατάστιχο (ledger). Μόλις εισχωρήσει στην αλυσίδα δεν μπορεί να διαγραφεί ή να τροποποιηθεί.

Το *DAG* [13] αποτελεί επίσης τεχνολογία DLT κατά την οποία κάθε συναλλαγή αποθηκεύεται στο καθολικό με ένα κριτήριο σειράς (Anwar, 2019). Η συχνότητα λειτουργεί έτσι ώστε κάθε συναλλαγή να κατευθύνεται από την προηγούμενη στην επόμενή της. Σε αυτήν την περίπτωση, η συναλλαγή πρέπει να πιστοποιηθεί και πάλι για να εισχωρήσει στην αλυσίδα. Αυτή τη φορά όμως θα πρέπει η ίδια να πιστοποιήσει τις δύο προηγούμενες συναλλαγές για να θεωρηθεί η ίδια έγκυρη. Όσο μεγαλύτερη είναι η αλυσίδα τόσο περισσότερο έγκυρες γίνονται οι συναλλαγές.

[11] 'Distributed ledger', στην αγγλική ορολογία.
[12] Το Blockchain είναι ένα είδος *DLT*.
[13] Βλ. Εικόνα 17 - Εικόνα 18 στο Παράρτημα Δ

Στο *HASHGRAPH* μπορούν να υπάρχουν περισσότερες συναλλαγές αποθηκευμένες σε ένα κατάστιχο στο ίδιο *timestamp*[14] και σε παράλληλες δομές (Anwar, 2019). Μόλις μια συναλλαγή λάβει χώρα, οι γειτονικοί κόμβοι μοιράζονται αυτήν την πληροφορία με στόχο τη γνώση από όλους τους κόμβους για τη συναλλαγή[15].

Το *HOLOCHAIN* ως DLT αποτελεί μια διαφορετική τεχνολογία που κινείται από μια πληροφοριο-κεντρική[16] σε μια ενεργο-κεντρική δομή[17]. Εδώ, κάθε κόμβος διαθέτει τη δική του αλυσίδα-καθολικό. Δεν υπάρχει κάποια συνολική διαδικασία πιστοποίησης των νέων συναλλαγών, όμως το *Holochain* δίκτυο διαθέτει μια σειρά κανόνων που ονομάζονται '*DNA'* για να ελέγξουν πάλι την πιστότητα του εκάστοτε κατάστιχου (Anwar, 2019).

Τέλος, άλλη μια τεχνολογία DLT είναι η *TEMPO* (*RADIX*) στην οποία οι συναλλαγές προστίθενται κατά χρονική σειρά στην αλυσίδα. Κάθε κόμβος στο δίκτυο διατηρεί ένα κομμάτι από την κύρια αλυσίδα και συγχρονίζεται. Για να πιστοποιηθεί μια συναλλαγή, οι κόμβοι ακολουθούν την συχνότητα των συναλλαγών και όχι την 'χρονοσήμανση'[18] (Anwar, 2019).

Η τεχνολογία *DLT* περιλαμβάνει επομένως το πρωτόκολλο Blockchain και όχι το αντίθετο [19] . Οι διαμοιραζόμενες τεχνολογίες συντίθενται πάνω σε ένα δίκτυο διαφορετικών υπολογιστικών συσκευών ή κόμβων. Κάθε κόμβος αποθηκεύει ένα ακριβές αντίγραφο της αλυσίδας. Η αλυσίδα αυτή δεν κρατείται ούτε ελέγχεται από κανενός είδους κεντρικό σύστημα. Οι κόμβοι συμφωνούν σε οποιαδήποτε αναβάθμιση γίνεται μονομερώς από τον καθένα. Μόλις η συμφωνία πραγματωθεί, το διαμοιραζόμενο σύστημα ενσωματώνει το συμπεφωνημένο σε κάθε ξεχωριστό κόμβο. Έτσι, η τεχνολογία αυτή μειώνει δραστικά το κόστος πιστότητας, επεκτείνει

[14] Δηλ. την ίδια χρονική στιγμή ή αλλιώς *χρονοσήμανση.*
[15] Εν προκειμένω, συντελείται η διαδικασία του *Virtual Voting,* ένα είδος ψηφιακής ψήφου, όπου κάθε κόμβος πιστοποιεί την συναλλαγή κι έτσι αυτή η τελευταία εισχωρεί στην αλυσίδα.
[16] 'Data-centric structure', στην αγγλική ορολογία.
[17] 'Agent-centric structure', στην αγγλική ορολογία.
[18] 'Timestamp', στην αγγλική ορολογία. [19]
[19] Όπως φαίνεται και στην Εικόνα 2.

την υπολογιστική δύναμη και παράλληλα διευρύνει την εφαρμογή της σε διαφορετικούς τομείς.

Βέβαια, το Blockchain διακρίνεται από τις άλλες τεχνολογίες καθώς τα δεδομένα ενώνονται και οργανώνονται σε ομάδες. Η δομή αυτή επιτρέπει την εισαγωγή μόνο πληροφοριών και όχι ενδεχόμενες αφαιρέσεις ή τροποποιήσεις[20].

Σε επιχειρηματικό επίπεδο, οι συναλλαγές δύναται να αφορούν πωλητές, αγοραστές και μεσάζοντες όπως συμβολαιογράφους και τράπεζες (Brakeville & Perepa, 2019) των οποίων οι συμφωνίες των επιχειρήσεων και οι συμβάσεις εγγράφονται σε κατάστιχα. Τυπικά, μια επιχείρηση χρησιμοποιεί πληθώρα αλυσίδων για να αποθηκεύει την ιδιοκτησία και την μεταφορά των αγαθών μεταξύ των εμπλεκόμενων παραγόντων. Οι αλυσίδες αυτές, όπως επισημάνθηκε, αποτελούν τα «μητρώα» των οικονομικών δραστηριοτήτων και συμφερόντων μιας εταιρείας.

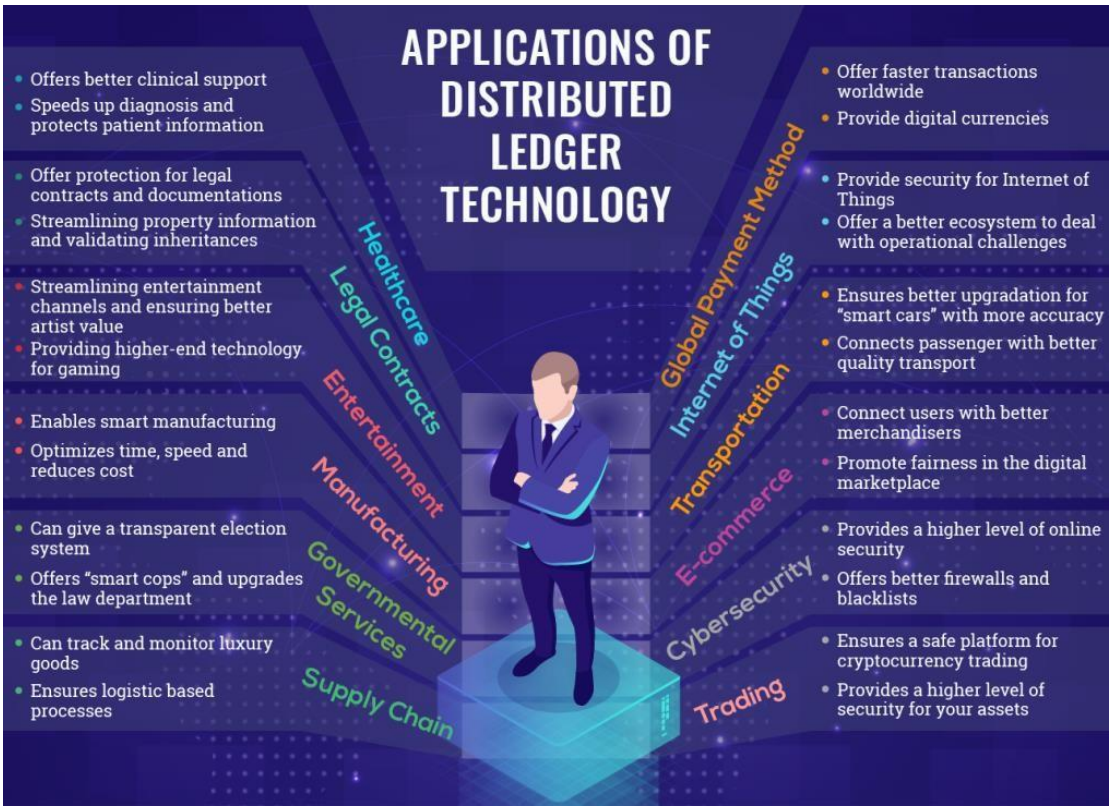
LEDGER

ACCOUNT TYPE	CASH				
TRANSACTION DATE	TRANSACTION DETAIL	REFERENCE	DEBIT	CREDIT	BALANCE
1/1/16	Expenses for Jan	Ref#1	$100.00		$100.00
2/1/16	Tax withheld	Ref#2		$110.00	($10.00)

Εικόνα 3 Μια τυπική εταιρική συναλλαγή με τα παρεπόμενα οικονομικά, λογιστικά και φορολογικά στοιχεία της. (Brakeville & Perepa, 2019)

Τα αρνητικά των τεχνολογιών DLT περιλαμβάνουν ζητήματα: ασφάλειας, μεγάλης εξάρτησης από το δίκτυο, δέσμευσης από την ύπαρξη ή όχι επικοινωνίας, χρόνου, κόστους και πολυπλοκότητας, καθώς κάθε κόμβος διενεργεί τις δικές του διεργασίες (Drescher, 2017).

[20] Ωστόσο, οφείλει κανείς να παραδεχθεί ότι τα κοινά σημεία μεταξύ του Blockchain και των διαμοιραζόμενων τεχνολογιών DLT εν γένει εξακολουθούν να υφίστανται, όπως η αποκέντρωση των διαδικασιών και η αλγοριθμική συμφωνία, δηλαδή το *consensus*, χρήσιμο για ενδεχόμενη τροποποίηση δεδομένων.



Εικόνα 4 Τα πλεονεκτήματα και οι καινοτομίες των τεχνολογιών DLT (Anwar, 2019)

Υποκεφάλαιο 1.3 Οι εφαρμογές 'Smart Contracts'– Η Κρυμμένη Νομική

Σύμφωνα με τον κατασκευαστή IBM (Gopie, 2018), οι έξυπνες συμβάσεις αποτελούν σειρές κώδικα που εκτελούνται μόλις πραγματοποιηθούν οι όροι και οι προϋποθέσεις τους. Αποθηκεύονται στην αλυσίδα κόμβων (Blockchain) και εκτελούνται αυτόματα ως μέρος της συναλλαγής. Πρακτικά, μια 'έξυπνη' σύμβαση δύναται να περιγράψει τις συμβατικές ρήτρες στις οποίες υπόκειται η μεταφορά ενός αγαθού. Θα μπορούσε επίσης να συγχωνεύσει τους όρους και τις προϋποθέσεις μιας ασφαλιστικής σύμβασης ταξιδιού η οποία θα μπορούσε να εκτελείται αυτόματα μόλις παρατηρείται καθυστέρηση πτήσης.

Ήδη το 1990, ο Nick Szabo (Bashir, 2017, σελ. 218) περιέγραψε τις συμβάσεις αυτές ως «*ένα πρωτόκολλο υπολογιστικής συναλλαγής που εκτελεί τους όρους μιας σύμβασης-συμφωνίας. Οι γενικοί στόχοι είναι να ικανοποιηθούν οι κοινές συμβατικές*

προϋποθέσεις[21]*, να ελαττωθούν οι κακόβουλες αλλά και οι αμελείς επεμβάσεις και να περιοριστεί η παρέμβαση μεσαζόντων*». Οι σχετικοί οικονομικοί στόχοι περιλαμβάνουν την καταπολέμηση της απάτης, των ζημιών, των διαιτησιών, των εξόδων κύρωσης και άλλων εξόδων της συναλλαγής (Bashir, 2017). Αυτή η ιδέα των 'έξυπνων' συμβάσεων εγκαθιδρύεται για πρώτη φορά και σε τεχνικό επίπεδο το 2009 με τα Bitcoins. Πλέον καθίσταται δυνατή η μεταφορά αγαθών και αξιών μεταξύ χρηστών που δεν εμπιστεύονται απαραίτητα τους εκάστοτε συμβαλλόμενους και όπου δεν υπάρχει ενδιάμεσος.

Η απουσία του ενδιάμεσου [22] που θα ελέγξει την εκτελεστότητα και τους όρους εκτέλεσης της σύμβασης, αποδεικνύει πως, πρώτον, ο Κώδικας είναι ο Νόμος[23] και πως, δεύτερον, δεν χρειάζεται κάποια ιδιαίτερη νομική διαδικασία επικύρωσης της πιστότητας και της εγκυρότητάς τους: είναι '*αυτο-εκτελεστά'* (Bashir, 2017, σελ. 221). Τα συγκεκριμένα προγράμματα διαθέτουν υψηλό σύστημα αντοχής και ανοχής ενδεχόμενων περιορισμών ή ελαττωμάτων του εξωτερικού περιβάλλοντος. Υπάρχουν συζητήσεις οι συμβάσεις αυτές να γίνουν όχι αυτόματα εκτελεστές αλλά *εκτελέσιμες* [24] εξαιτίας του ανθρώπινου παράγοντα που συχνά απαιτείται σε ορισμένες περιπτώσεις (Bashir, 2017, σελ. 221). Βέβαια, το κατά πόσο ένας κώδικας μπορεί να αποτελέσει αντικείμενο δικαστικής διαμάχης και αν αυτός ο πρώτος δύναται να σχεδιαστεί ώστε να είναι κατανοήσιμος από νομικούς παράγοντες, αυτό αποτελεί άλλο ένα επίσης αξιοσημείωτο θέμα συζήτησης.

Έτσι, οι 'έξυπνες συμβάσεις' είναι εγγενώς σχεδιασμένες να υπόκεινται σε ντετερμινιστικά πρότυπα. Εάν το αποτέλεσμα διαφέρει ελάχιστα μεταξύ των κόμβων, η συμφωνία δεν μπορεί να επιτευχθεί και όλη η αλυσίδα κόμβων μπορεί να καταρρεύσει. Γίνεται έτσι κατανοητό ότι αυτού του τύπου οι συμβάσεις καθορίζονται από τέσσερα συστατικά: την αυτόματη εκτελεστότητα, την δυνατότητα να αυτόεπικυρώνονται, την δυνατότητα να είναι *κατανοητά, ασφαλή και αδιάληπτα* (Bashir, 2017, σελ. 221). Άλλη μια συζήτηση αφορά στο ότι κάθε κώδικας πρέπει να

[21] Όπως όροι πληρωμής, εχεμύθεια, κύρωση της σύμβασης.
[22] Συνήθως ενός νομικού ή συμβολαιογράφου.
[23] Βλ. Bashir, 2017, σελ. 219, όπως παρατέθηκε και στην Εισαγωγή
[24] Εν δυνάμει εκτελέσιμες, δηλαδή εκτελεστές με την ανθρώπινη παρέμβαση.

είναι κατανοητός τόσο από τους Η/Υ όσο και από τους ανθρώπους. Γι' αυτό, βέβαια, εισήχθησαν οι συμβάσεις τύπου «Ricardian»[25] (Bashir, 2017, σελ. 222).

Οι πιο συχνές χρήσεις της έξυπνης σύμβασης πραγματοποιούνται στον εμπορικό και τον χρηματοπιστωτικό κόσμο. Έχει επίσης υποστηριχθεί η δημιουργία συμβάσεων προσχώρησης (Template contracts), δηλαδή 'προτύπων συμβάσεων' για ταχύτητα και αποτελεσματικότητα.

Ήδη, οι 'έξυπνες' συμβάσεις επεκτείνονται σε πληθώρα πεδίων. Η δυνατότητα δημιουργίας και ελέγχου ψηφιακής ταυτότητας για αναγνώριση πελατών από εταιρείες, η διευκόλυνση αυτόματης καταβολής εταιρικών μερισμάτων και αποπληρωμής αποθεμάτων, η διεθνής μεταφορά αγαθών μέσω πιστωτικών μηχανισμών, η απλοποίηση των διαδικασιών χωρίς περαιτέρω έξοδα, η διαύγεια στα χρηματοοικονομικά συστήματα και τις συναλλαγές, η διευκόλυνση και αποτελεσματικότητα σύνδεσης μεταξύ των μερών και των συναλλαγών συνδεόμενων με υποθήκες, όπως και οι εφαρμογές ασφαλιστικών συμβάσεων είναι μερικά[26] από τα σύγχρονα παραδείγματα που και σε παγκόσμιο δικαστικό επίπεδο (Digital Commercial Chamber, 2016) έχουν ξεκινήσει να εξετάζονται.

Ωστόσο, το οικοσύστημα των έξυπνων συμβάσεων βρίσκεται ακόμη σε εμβρυικά επίπεδα με αποτέλεσμα οι συμβάσεις αυτές να μην μπορούν να εισάγουν εξωτερικά δεδομένα που δύναται να χρειάζονται ή και να απαιτούνται για τον έλεγχο της

[25] Το σημείο-κλειδί σε αυτού του τύπου τις συμβάσεις, που χρησιμοποιούνται στον χρηματοπιστωτικό κόσμο, είναι η συγγραφή ενός εγγράφου που θα είναι κατανοητό και αποδεκτό τόσο από ένα δικαστήριο όσο και από ένα πρόγραμμα Η/Υ. Ταυτοποιεί τον εκδότη και διακρίνει τους όρους και τις ρήτρες της σύμβασης ώστε να το καταστήσει αποδεκτό ως μια νομικά δεσμευτική σύμβαση. Η διαφορά μεταξύ 'έξυπνων' συμβάσεων και τύπου «Ricardian» έγκειται στο ότι αυτές οι τελευταίες επικεντρώνονται περισσότερο στον σημασιολογικό πλούτο και την παραγωγή του εγγράφου περιλαμβάνοντας συμβάσεις προσχώρησης. Στο Bitcoin, η 'έξυπνη' σύμβαση αφορά αμιγώς στην εκτέλεση της σύμβασης ενώ η τύπου «Ricardian» σύμβαση αφορά στην παραγωγή ενός εγγράφου που είναι κατανοητό από ανθρώπους, και δη νομικούς.

[26] Επιπλέον παραδείγματα: ψηφιακή αρχειοθέτηση και αυτόματη αναβάθμιση ασφαλειών νομικού χαρακτήρα, εξάλειψη της απάτης διευκολύνοντας μεταφορές τίτλων ιδιοκτησίας και ασφάλεια ιατρικού απορρήτου.

εκτέλεσης της επιχειρηματικής λογικής (π.χ. η τιμή των αποθεμάτων μιας εγγύησης που απαιτείται από τη σύμβαση για την καταβολή των εταιρικών μερισμάτων)[27].

Επίσης, να σημειωθεί ότι η τεχνολογία των συμβάσεων αυτών δεν είναι απαραίτητο να βασίζεται στην αλυσίδα κόμβων (Blockchain). Ωστόσο, τα παραδείγματα δεν λείπουν: η τεχνολογία *Ethereum* βασίζεται στο σύστημα *Blockchain* και αναπτύσσει και 'έξυπνες' συμβάσεις.

Βέβαια, υπάρχει κάποιος σκεπτικισμός γύρω από το ζήτημα. Ειδικότερα, μέσω της ζημίας 50 εκατ. δολαρίων στο σύστημα ηλεκτρονικών επενδύσεων *smart contracts DAO* από κακόβουλη παρέμβαση τον Ιούνιο του 2016 (Bashir, 2017, σελ. 228), αποδεικνύεται πως ο χρυσός κανόνας '*code is law*' δεν είναι δυνατόν να εγγυάται πάντοτε πιστότητα και εμπιστοσύνη όπως τα παραδοσιακά πρότυπα νομικής εκτελεστότητας και ασφάλειας. Σύμφωνα με τους ειδικούς, η λύση βρίσκεται στη δημιουργία μιας ασφαλούς, κατά το μέγιστο, γλώσσας προγραμματισμού (Bashir, 2017).

Υποκεφάλαιο 1.4 Οι εν γένει εφαρμογές της τεχνολογίας *Blockchain*

1.4.1 e-health

Η τεχνολογία Blockchain προσφέρει ασφάλεια προσωπικών δεδομένων σε ό,τι αφορά τις απόρρητες πληροφορίες και τα ιατρικά δεδομένα που αντιστοιχούν σε ένα πρόσωπο. Ως γνωστόν, η ιδιωτικότητα των ασθενών συχνά διακινδυνεύεται όταν τα ιατρικά αρχεία διαμοιράζονται ή μεταφέρονται εκτός των πεδίων των αρμόδιων ιδρυμάτων και οργανισμών. Αντίστροφα, η πλήρης απομόνωση των πληροφοριών αυτών δεν λειτουργεί ευεργετικά για την σύγχρονη επιστήμη και την έρευνα. Ένα σύστημα Blockchain όμως δύναται να καλύψει αυτόν τον προβληματισμό και να επιτύχει σταθερότητα δεδομένων και ασφάλεια (Hussein et al., 2018) ως προς τη διαχείριση και την πρόσβαση σε τέτοιες ευαίσθητες πληροφορίες. Αποδεικνύεται

[27] Γι' αυτό το λόγο, εισάγονται τα συστήματα διεπαφής *Oracle* τα οποία μεταφέρουν δεδομένα από μια εξωτερική πηγή στις έξυπνες συμβάσεις.

πως με τον κατάλληλο σχεδιασμό συστήματος θα μπορεί η μεταφορά των δεδομένων μεταξύ διαφόρων περιβαλλόντων όπως κλινικές, νοσοκομεία και κέντρα υγείας να πραγματοποιείται αποτελεσματικά. Ένα σύστημα *cloud*, έτσι, θα βοηθούσε στην επέκταση των πηγών και στην καλύτερη ασφάλεια (Hussein et al., 2018, σελ. 10).

1.4.2. Άλλες εφαρμογές Blockchain

Όπως γίνεται αντιληπτό, το Blockchain 1.0 αφορά στην πρώτη γενιά της τεχνολογίας που δεν είναι άλλη από την εφαρμογή των ψηφιακών νομισμάτων. Η δεύτερη γενιά, Blockchain 2.0, αφορά στις θετικές επιρροές που πρόκειται να προκληθούν στο κομμάτι της διεθνούς οικονομίας. Η τρίτη γενιά αφορά σε εφαρμογές καθαρά προς τον πολίτη και την κοινωνία (Efanov & Roschin, 2018, σελ. 117-119).

Συχνές χρήσεις της τεχνολογίας αφορούν πρωτίστως *μεταφορές χρημάτων και άλλων αξιών γρήγορα και φτηνά* (Laurence, 2017, σελ. 14). Αυτές οι συναλλαγές περιλαμβάνουν επίσης εμπορικά αποθέματα και καταβολές πληρωμών μισθωτών. Ειδικότερα, η νέα τάση της τεχνολογίας *IoT*[28]*,* καθώς είναι ιδιαίτερα ευαίσθητη σε κακόβουλες επιθέσεις, ενισχύεται μέσω του Blockchain (Laurence, 2017, σελ. 15). Στα συστήματα δεδομένων προστίθενται τα αυτό-οδηγούμενα αυτόματα αυτοκίνητα, οι διεθνείς ταξιδιωτικές εφαρμογές και τα συστήματα ηλεκτρονικής διακυβέρνησης και ταυτοποίησης πολιτών.

Μια άλλη καινοτομία παρατηρείται στο πεδίο των νομικών πράξεων γύρω από τα ακίνητα προς υποθήκευση. Η ασφάλιση που εγγυάται τις ζημίες του υποθηκευμένου ακινήτου προστατεύει τις τράπεζες από τις επενδύσεις τους. Επίσης, συχνά τίτλοι ασφάλισης καταρτίζονται μεταξύ αγοραστή-πωλητή για να εγγυηθεί η καλή κατάσταση του αγαθού στα χέρια του αγοραστή[29] (Laurence, 2017, σελ. 144-146). Η τεχνολογία Blockchain θα μπορούσε να βοηθήσει στην αρχειοθέτηση του υλικού εξαιτίας του αμετάβλητου των δεδομένων. Βέβαια, ενδιάμεσοι παράγοντες όπως μεσίτες, επιθεωρητές κατοικιών, γραμματείς στο υποθηκοφυλακείο ενδέχεται να

[28] 'Internet of Things': το Διαδίκτυο των Πραγμάτων αποτελεί ένα δίκτυο επικοινωνίας μεταξύ διαφόρων συσκευών και ψηφιακών περιβαλλόντων.
[29] Κατά το κοινό δίκαιο.

επηρεαστούν από τη νέα τεχνολογία. Τα έξοδα υποθήκης έτσι μειώνονται σημαντικά. Η νέα 'μόδα' έχει ξεκινήσει και εφαρμόζεται σε Η.Π.Α., Κίνα, Ευρώπη και Αφρική (Laurence, 2017).

Στην ιδιωτική ασφάλιση επίσης αναμένονται μεταβολές. Η διαχείριση θα αποτελεί πλέον μια εύκολη διαδικασία και οι προτεραιότητες θα μετακινηθούν προς τον υπολογισμό ζημιών και την εύρεση του καταλληλότερου συνδυασμού προσφοράςζήτησης (Laurence, 2017). Η μικρο-ασφάλιση θα αποτελέσει ένα ενδιαφέρον στοιχείο για τις μικρο-μεσαίες τάξεις. Εν ολίγοις, ασφαλιστές και ασφαλιζόμενοι θα νιώσουν τα πλεονεκτήματα (Laurence, 2017).

Επίσης, πολύ σημαντική καινοτομία αποτελούν οι ηλεκτρονικές υπογραφές που χρησιμοποιούν ασύμμετρη κρυπτογράφηση. Μια ηλεκτρονική υπογραφή αποτελεί το ισοδύναμο της καθημερινής υπογραφής με τη διαφορά ότι "εισάγεται σε ένα σύστημα Blockchain που χρησιμοποιεί κρυπτογραφικό «hashing» και ιδιωτική-προς-δημόσια πληροφορία" (Drescher, 2017, σελ. 104) και φυσικά αριθμούς. Πλέον, για κάθε είδος συναλλαγής απαιτείται ο ιδιοκτήτης να είναι και ο *διαχειριστής-δημιουργός-συμβαλλόμενος* στη συναλλαγή Blockchain. Κατ'αυτόν τον τρόπο, μειώνεται στο μηδέν ο κίνδυνος εξαπάτησης αφού ο μηχανισμός εγγυάται αυτομάτως πως ο φορέας είναι και ο συμβαλλόμενος στη συναλλαγή μέσω της μοναδικότητας της ηλεκτρονικής υπογραφής (Drescher, 2017).

Αναλογικά με τις μεταβιβάσεις ακινήτων, έτσι και το επίπεδο των πνευματικών δικαιωμάτων, δύναται να αλλάξει προς μια θετικότερη κατεύθυνση. Πολύπλοκες διαδικασίες εγγραφής στα μητρώα, η απαίτηση να εγγραφούν διάφορα αρμόδια δικαστήρια, η απαιτούμενη εξειδίκευση νομικής κατάρτισης για την διαδικασία, η ήδη βαριά διαδικασία διαχείρισης των πνευματικών δικαιωμάτων πρόκειται να αναπτύξουν διαφορετική τροχιά με το σύστημα Blockchain. Πλέον θα γίνεται λόγος για μια ενιαία βάση δεδομένων, ένα ενιαίο αρχείο-εναποθετήριο σημάτων και

πνευματικής ιδιοκτησίας, όπου η διαχείριση αυτών θα αποτελεί μια απλούστερη διαδικασία[30] (Gürkaynak, Yılmaz, Yeşilaltay & Bengi, 2018).

Υποκεφάλαιο 1.5 Το πλαίσιο της τεχνικής και εν γένει ασφάλειας στο *Blockchain* και η θέση του νομικού κόσμου

Τα πρώτα προβλήματα σχετίζονται με την απάτη και τις διαδικτυακές επιθέσεις. Το 51% των επιθέσεων προκύπτει από την αδυναμία του συστήματος να αντιμετωπίσει την παρουσία δυο διαφορετικών μπλοκ που διεκδικούν τη θέση τους στην αλυσίδα, δημιουργώντας το λεγόμενο «πιρούνι[31]». Τελικά, αυτό που πρέπει να διατηρηθεί πάση θυσία στα χέρια του χρήστη είναι το ιδιωτικό κλειδί. Εάν αυτό "χαθεί ή κλαπεί, κανένας δεν μπορεί να το επανακτήσει" (Efanov & Roschin, 2018, σελ. 119). Όλα τα στοιχεία πλέον θα ανήκουν στον νέο κάτοχο, μαζί με τα αγαθά και τα δεδομένα (Volety, Saini, McGhin, Liu & Choo, 2018). Αυτό αποτελεί ίσως κάτι παραπάνω από αδυναμία, ίσως αποτελεί έναν λόγο που ακόμα η τεχνολογία δεν διευρύνεται «εκτός εταιρικών συνόρων».

Σε ό,τι αφορά τα *smart contracts*[32], αυτά θα χρειαστεί να συμβαδίσουν με τις εκάστοτε έννομες τάξεις. Το ζήτημα της ασφάλειας δικαίου παραμένει, καθώς για λόγους ασφάλειας τα αυτό-οδηγούμενα αυτοκίνητα θα πρέπει να ακολουθούν τους κανόνες των δρόμων, η δημιουργία αυτόνομων εταιρειών θα πρέπει να ακολουθεί επίσης ορισμένες νομικές διαδικασίες (Giancaspro, 2017) και αυτόνομες αγορές θα πρέπει να εφαρμόζουν την εγγενή τους λογική κάθε φορά. Κάποιοι ωστόσο, 'φοβούνται' πως η είσοδος της τεχνολογίας στο νομικό κόσμο θα επιφέρει και την αντικατάστασή του από τον νόμο της τεχνολογίας, πράγμα που σημαίνει κατά

[30] Παρά ταύτα, η έλλειψη γνώσης κώδικα από την πλευρά των νομικών όπως και η απουσία νομοθετικών ρυθμίσεων είναι οι δυο μεγάλες σύγχρονες προκλήσεις.
[31] 'Fork', στην αγγλική ορολογία.
[32] Και σε μια πιο ευρεία ερμηνεία της λέξης 'ασφάλεια'

μερικούς (Savelyev, 2018) υποκατάσταση του παρόντος νομικού καθεστώτος με κάποιο νέο τεχνολογικό κώδικα.

Επίσης, δεν θα πρέπει να λησμονηθεί ο πρόσφατος ευρωπαϊκός κανονισμός περί των προσωπικών δεδομένων (Millard, 2018) που αγγίζει και το κομμάτι 'αξιοπιστία-ασφάλεια' του Blockchain.

Στο πεδίο των ιατρικών εφαρμογών e-health, ενώ η εφαρμογή, η αποτελεσματικότητα και η απόκριση του συστήματος αποτελούν θετικά στοιχεία (Roehrs & al., 2018), η ασφάλεια των δεδομένων παραμένει σοβαρό ζήτημα. Παρ'όλο που στο πλαίσιο ερευνών έχουν σχεδιαστεί προγράμματα για την υποστήριξη της αποθήκευσης ιατρικών δεδομένων όπως το *Ancile* (Dagher, Mohler, Milojkovic & Marella, 2018), ωστόσο, προτείνεται η χρήση είτε κάποιου *smart contract* είτε κάποιου παρεπόμενου προγράμματος για λόγους αξιοπιστίας. Σε ένα σύστημα ακόμα εμβρυικής κατάστασης αναζητούνται 'ειλικρινείς χρήστες' (Chen, Lee, Chang, Chood & Zhang, 2019).

«Η ακεραιότητα στα δεδομένα και τις πληροφορίες όπως και η εμπιστευτικότητα είναι κάποια θεμελιώδη στοιχεία που ακόμα αναζητούνται εντός των δικτύων σε ομότιμη σύνδεση» παρατηρεί ο Drescher (2017, σελ. 162). Η ακεραιότητα εξαρτάται από τη γνώση του αριθμού των κόμβων ή τον ομότιμων χρηστών και τη γνώση της εμπιστευτικότητας αυτών των τελευταίων (Drescher, 2017, σελ. 30), προϋποθέσεις αρκετά δύσκολες για ένα διαμοιρασμένο μηχανισμό. Ελλείψει, το σύστημα κινδυνεύει από τεχνικές βλάβες και κακόβουλους ομότιμους χρήστες[33]. Από τεχνικής πλευράς, είναι φανερά δύσκολο να διορθωθούν ενδεχόμενα ελαττώματα εξαιτίας του στατικού πρωτοκόλλου της αλυσίδας. Ωστόσο, ήδη γίνονται προσπάθειες να ελαττωθεί το φαινόμενο αυτό και να σχεδιαστεί ένα μοντέλο εκούσιας διαγραφής των δεδομένων από την αλυσίδα Blockchain (Yang, Chen & Xiang, 2017).

[33] Είναι το πρόβλημα που αντιμετωπίζει η επιστήμη των Η/Υ: *Byzantine General Problem*.

Κεφάλαιο 2. Κρυπτονομίσματα: *Bitcoins* και *Altcoins*

Υποκεφάλαιο 2.1 *Bitcoins*

2.1.1 Ορισμός και λειτουργία του *Bitcoin*

Το κρυπτονόμισμα, ως έννοια, υπήρχε από τη δεκαετία του ’90. Ωστόσο, η τεχνολογία παρουσίαζε προβλήματα και δεν ήταν αρκετά εξελιγμένη και διαδεδομένη. Το 2009, η τεχνολογία δημιούργησε τα *Bitcoins*, χρησιμοποιώντας την αλυσίδα Blockchain. Το Blockchain, επομένως δομεί το *Bitcoin*. Όλα τα κρυπτονομίσματα είναι Blockchain, όχι όμως και το αντίθετο. Οι όροι Bitcoin-Blockchain συχνά χρησιμοποιούνται εναλλάξ.

Το *Bitcoin core* πρωτο-δημιουργήθηκε από τον Satoshi Nakamoto (Bambara & Allen, 2018, σελ. 11-12). Δεν είναι γνωστό αν αυτό είναι το αληθινό του όνομα ή αν κρύβονται περισσότερα άτομα πίσω από αυτό. Η διαφορά των κρυπτονομισμάτων από το τραπεζικό σύστημα έγκειται στη σύγκρουση μεταξύ του κεντροποιημένου τραπεζικού μηχανισμού με το δημόσιο καθολικό στην καρδιά του *Bitcoin,* γεγονός που έχει ως συνέπεια την αυτονομία και την αποδέσμευση από οποιαδήποτε κεντρική δομή. Η τεχνολογία Blockchain “εξελίχθηκε με τη δημιουργία του Bitcoin” (Laurence, 2017, σελ. 11). Σήμερα το δίκτυο *Bitcoin* διαθέτει περίπου 7000 διαμοιρασμένους κόμβους παγκοσμίως[34] (Bird, 2016).

Η εφαρμογή του κρυπτονομίσματος δύναται να χρησιμοποιηθεί σε πληθώρα συσκευών ως ένα λογισμικό ανοιχτού κώδικα. Οι χρήστες επικοινωνούν διαδικτυακά μεταξύ τους μέσω του Πρωτοκόλλου *Bitcoin*. Η πρωταρχική δραστηριότητα είναι η μεταφορά και η αποθήκευση αξιών μέσω του δικτύου αυτού. Πραγματοποιούνται αγορές αγαθών, πωλήσεις σε φυσικά ή νομικά πρόσωπα ακόμα και πιστώσεις[35], όπως ακριβώς και με τα παραδοσιακά νομίσματα. Επίσης, μπορούν να αγοραστούν,

[34] Εκτός από την κυκλοφορία των κρυπτονομισμάτων, γρήγορα έγινε αντιληπτή η επιτυχής χρήση της τεχνολογίας και σε άλλες εφαρμογές με μικρότερες αλυσίδες Blockchain.
[35] Όπως η εφαρμογή ‘*debit card’*

να πωληθούν και να ανταλλαχθούν με άλλα νομίσματα (Antonopoulos, 2016). Το *Bitcoin* είναι το 'ιδανικό' νόμισμα λόγω της ταχύτητας, της ασφάλειας και της απουσίας γεωγραφικών φραγμάτων. Γίνεται λόγος, επομένως, για ένα άυλο νόμισμα του οποίου οι χρήστες διαθέτουν δικά τους ιδιωτικά κλειδιά επιτρέποντάς τους να αποδεικνύουν την ιδιοκτησία των νομισμάτων στο δίκτυο. Τα κλειδιά συχνά αποθηκεύονται στο ψηφιακό πορτοφόλι σε οποιαδήποτε συσκευή του χρήστη. Η μόνη προϋπόθεση, άρα, για την υπογραφή μιας συναλλαγής είναι η κατοχή του κλειδιού[36].

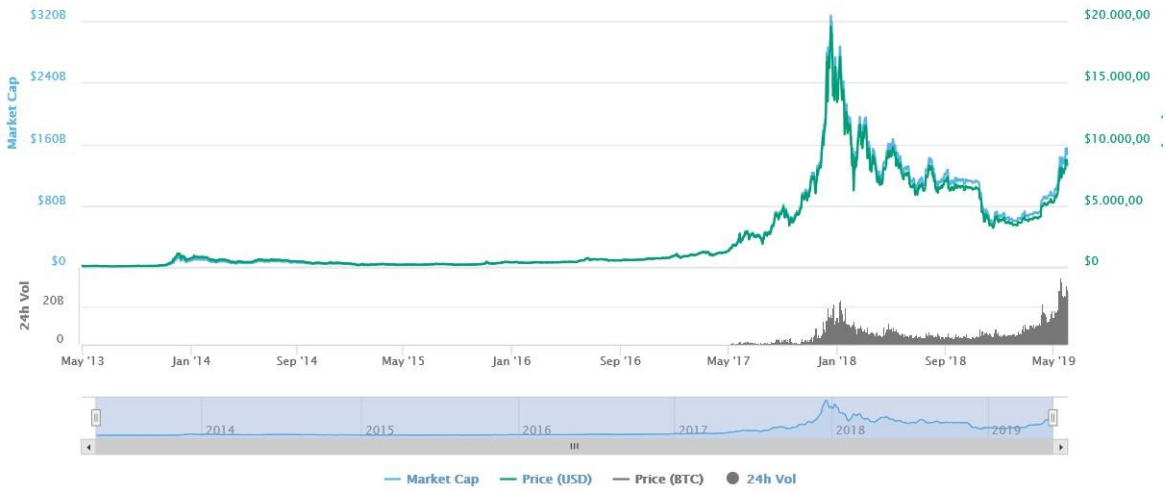
Πίνακας 1 Τι πρέπει να γνωρίζει ο χρήστης για τη χρήση του Bitcoin (Συλλογή δεδομένων (Κυρίτσης, 2019))

Απόκτηση Ψηφιακού Πορτοφολιού	Απόκτηση *Bitcoin* μέσω:	Παρατηρήσεις
•Μέσω δωρεάν εφαρμογής στον Η/Υ ή στο κινητό •Σε δωρεάν λογαριασμό κάποιου κέντρου Bitcoin συναλλαγών (Bitcoin Exchange) •Σε ειδικές συσκευές με αυξημένη ασφάλεια	•Ανταλλαγής Bitcoin με κάποιον •Αγοράς σε τρέχουσα ισοτιμία σε ευρώ ή δολάρια •Ανταγωνιστικής εξόρυξης: Mining	•Δεν χρειάζεται κανείς να ξοδέψει χιλιάδες χρήματα: μπορεί κανείς να αγοράσει και υποδιαιρέσεις του BTC (πχ. **0,00024993 BTC**) •Το ψηφιακό πορτοφόλι διαθέτει μια μοναδική αλφαριθμητική διεύθυνση •Για να πραγματοποιήσουμε μια συναλλαγή, όπως συμβαίνει και με το ηλεκτρονικό ταχυδρομείο, πολύ απλά χρησιμοποιούμε τις ανώνυμες ηλεκτρονικές διευθύνσεις για μόνο φορά όμως.

Το «mining»[37], δηλαδή η διαδικασία επιβεβαίωσης της συναλλαγής, αποτελεί ένα παιχνίδι *τύχης* (Szmigielski, 2016, σελ. 15). Το λογισμικό δημιουργεί ένα υποψήφιο μπλοκ το οποίο, εκτός από τον κρίκο που συνδέει το προηγούμενο μπλοκ με το υπάρχον, διαθέτει και όλες τις συναλλαγές όπως και ένα είδος μετρητή[38]. Κατά την τοποθέτηση του κρίκου, εάν το αποτέλεσμα δεν συναντά τα κριτήρια δυσκολίας, τότε

[36] Ονομάζεται και φύτρο – 'seed'.
[37] Αναφέρεται και ως *κατανεμημένο συναινετικό σύστημα.*
[38] 'Nonce', στην αγγλική ορολογία.

ο μετρητής αυτός καταστρέφεται και εισχωρεί άλλος κρίκος. Η διαδικασία εξόρυξης μπορεί να πραγματοποιήσει δισεκατομμύρια ή και τρισεκατομμύρια τέτοιων κρίκων το δευτερόλεπτο. Μόλις βρεθεί ο κατάλληλος κρίκος, το λογισμικό εισάγει το μπλοκ στο δίκτυο για έλεγχο. Είναι η λεγόμενη διαδικασία *Proof-of-work* (Antonopoulos, 2016). Ο υπολογιστής δοκιμάζει τυχαίους αριθμούς με μεγάλο αριθμό ψηφίων, τον ένα μετά τον άλλο: «*Όταν βρει τον "σωστό" αριθμό, με βάση την κρυπτογραφία, τότε η διαδικασία είναι επιτυχής*» (Κυρίτσης, 2019). Οι "εξορύκτες" [39] λαμβάνουν ως βραβείο για την επιτυχία στη διαδικασία *PoW*, την "κοπή" νέων *Bitcoins* κι έτσι νέα νομίσματα 'γεννιούνται' και 'βγαίνουν' στην κυκλοφορία. Άλλο κίνητρο γι' αυτούς αποτελεί η λήψη *Bitcoins* μέσω των εξόδων συναλλαγής[40]. Η συχνότητα κοπής των *Bitcoins* κάθε τέσσερα χρόνια περιορίζεται[41] καθώς ο αλγόριθμός είναι όλο και πιο δύσκολος να λυθεί, απαιτώντας παράλληλα τεράστια υπολογιστική δύναμη, γεγονός που γεννά ερωτήματα ως προς την ενέργεια και το περιβάλλον. Παλαιότερα, ένας απλός υπολογιστής μπορούσε να απαντήσει στον αλγόριθμο. Τώρα, απαιτείται η χρήση μεγάλων ταχυτήτων και ισχυρών συστημάτων GPU (Szmigielski, 2016).



Εικόνα 5 Γράφημα για την αξία του BTC σε δολάριο 2013-2019 (Coinmarket Cap, χ.η.)

[39] 'Miners': Ανεξάρτητα μέλη ή οργανισμοί που κινούν το δίκτυο Bitcoin και κυβερνούν την υπολογιστική δύναμη.
[40] 'Transaction fees', στην αγγλική ορολογία.
[41] Ο συνολικός αριθμός bitcoin θα φτάσει περίπου τα 21 εκατομμύρια κι εκεί θα παύσει η περαιτέρω «κοπή» του.

2.1.2 Θετικά σημεία και εφαρμογές του *Bitcoin*

Στον ελληνικό χώρο[42], ήδη υπάρχουν επιχειρήσεις που υποστηρίζουν πληρωμές με BTC[43]. Στην Κένυα αγαθά και υπηρεσίες διεκπεραιώνονται με ηλεκτρονικό χρήμα. Ωστόσο, πληθώρα ανεπτυγμένων κρατών έχουν ακόμα μείνει εκουσίως [44] στα "παρασκήνια". Κατ'άλλους, αποτελεί μια ιδιαίτερα εκπληκτική τεχνολογία η οποία πρόκειται να φέρει στο μέλλον πολύ ενδιαφέρουσες προτάσεις. Βέβαια, αυτό που έχει παρατηρηθεί είναι η ανάπτυξη της τεχνολογίας Blockchain κυρίως στο επίπεδο των εφαρμογών business-to-business. Εταιρείες όπως η *Ripple* και η *R3* εργάζονται σε αυτόν τον τομέα. Σε επίπεδο ασφάλειας, η απάτη ελαττώνεται και σε κοινωνικό επίπεδο το σύστημα εγγυάται ένα είδος δημοκρατικότητας καθώς *"απαιτείται τουλάχιστον το 51% για να πραγματοποιηθεί μια αλλαγή εντός του συστήματος των κόμβων"* (Laurence, 2017, σελ. 134). Στο μέλλον, οι χώρες προβλέπεται να ενδυναμώνουν το ελλιπές κεφάλαιό τους και οι ιδιοκτήτες αγαθών κινητών και ακινήτων πρόκειται να διαθέτουν το μεγάλο πλεονέκτημα να πουλούν σε όλον τον πλανήτη. Επίσης, οι μικρο-επενδύσεις θα αποτελούν μια εύκολη, χωρίς μεσολαβητές και πιο ελκυστική διαδικασία (Laurence, 2017). Η νέα τεχνολογική τάση πριμοδοτεί την ισότητα στο παγκόσμιο οικονομικό σύστημα ακριβώς εξαιτίας του αποκεντρωμένου χαρακτήρα της τεχνολογίας. Η ελευθερία πληρωμών, τα εμπορικά προνόμια, ο έλεγχος από την πλευρά του χρήστη, οι διακυμάνσεις του νομίσματος (Chuen & Nian, 2015) αποτελούν τις γενικές αρχές του συστήματος. Σε επιχειρηματικό επίπεδο, ιδιαίτερα ενδιαφέρουσα σύζευξη της τραπεζικής λογικής με την αλυσίδα Blockchain είναι το λεγόμενο *Consortium Banking*, το οποίο θεμελιώνει την επικοινωνία μεταξύ διαφόρων επενδυτικών παραγόντων με το διαμοιρασμένο δίκτυο. Επίσης, η τεχνολογία μπορεί να χρησιμοποιηθεί και για ηλεκτρονικές

[42] Βλ. Χάρτες στο Παράρτημα Γ

[43] Μεταξύ των οποίων φαρμακεία, δικηγορικά γραφεία, ασφαλιστικές υπηρεσίες, ηλεκτρονικό επιχειρείν, κομμωτήρια, Πανεπιστήμιο Κύπρου, ακόμα και οδοντιατρικές υπηρεσίες. Εκτός αυτού, ο απλός ιδιώτης πλέον είναι δυνατόν να αγοράσει bitcoin από τα εγκεκριμένα 'ATM bitcoin' τα οποία μέσω της δραστηριοποίησης της εταιρείας *Thess Cash Hellas* έχουν αρχίσει να αυξάνονται ανά την επικράτεια. Για περισσότερες πληροφορίες: http://thesscash.gr/en/info/about/

[44] Βλ. Υποενότητα 2.1.3

διατραπεζικές πληρωμές. Η διαδικασία ταυτοποίησης πελατών (KYC- Know Your Client) θα μπορούσε να ευδοκιμήσει και σε τραπεζικό επίπεδο (Shah & Jani, 2018).

Οι εφαρμογές του κρυπτονομίσματος έχουν προχωρήσει και πλέον έχει αρχίσει η συζήτηση για χρήση ενός *carbon coin* (βλ. Κίνα) στο πλαίσιο ανάπτυξης μιας ενεργειακής πολιτικής (Pan & al., 2018). Εκτός αυτού, έχει υποστηριχθεί πως σε ό,τι αφορά τα οικονομικά χαρακτηριστικά τους, ο χρυσός και το δολάριο σε σχέση με το Bitcoin παρουσιάζουν πολλά κοινά χαρακτηριστικά. Βέβαια, η επιλογή ένταξης του κρυπτονομίσματος εντός της εταιρικής πολιτικής έχει ως πλεονεκτήματα την καλύτερη γνώση της αγοράς και την καλύτερη λήψη αποφάσεων, όντας ένα εργαλείο για αντιμετώπιση "αντίθετων" επενδυτών [45] (Dyhrberg, 2015, σελ. 92). Το κρυπτονόμισμα από τη μία παρουσιάζει τα σημαντικά πλεονεκτήματα μιας αποθηκευμένης νομισματικής αξίας [46] και από την άλλη διαθέτει όλα τα θετικά στοιχεία των ελεύθερων συναλλαγών (Dyhrberg, 2015a). Επιπλέον, το κρυπτονόμισμα κυκλοφορεί σε υψηλές συχνότητες με καθόλου περιορισμό ημερών για εμπορικές συναλλαγές γεγονός που δίνει τεράστιες ταχύτητες σε αυτές (Dyhrberg, 2015b). Η τεχνολογία βοηθά, επίσης, στο να εξαλειφθούν όχι μόνο τα εθνικά όρια αλλά και οι ενδεχόμενες απαγορεύσεις κεφαλαίων (capital controls) (Dwyer, 2014).

2.1.3 Προβληματισμοί και ανοιχτά ζητήματα του *Bitcoin*

Εντούτοις, η σύζευξη χρηματοπιστωτικού μηχανισμού και Blockchain φαντάζει ιδιαίτερα απίθανη έως και επικίνδυνη (ΤτΕ, 2018) κυρίως λόγω της εγγενούς φύσης του νομίσματος αλλά και του τραπεζικού μηχανισμού καθώς για μια συναλλαγή απαιτούνται ειδικά έξοδα σε κάθε μεταφορά.

[45] Σε περίπτωση ματαίωσης κάποιας εταιρικής επένδυσης, το κρυπτονόμισμα μπορεί να καλύψει την απώλεια αυτή.
[46] Όπως το δολάριο.

Ένα από τα αρνητικά της τεχνολογίας αφορά στη μεγάλη επεξεργαστική ισχύ για το κλείσιμο ενός μεμονωμένου μπλοκ [47]. Αυτό θέτει ζητήματα ενεργειακά και περιβαλλοντικά. Επίσης, υπάρχει χρονικός περιορισμός που υπολογίζεται περίπου στα δέκα λεπτά, εάν επιθυμείται αλλαγή κάποιου μπλοκ (1DayDude Team, 2018). Αλλαγές δεν χωρούν πέρα των δέκα λεπτών αλλιώς σε αντίθετη περίπτωση αναγκάζεται κανείς να ξεκινήσει τη διαδικασία κλεισίματος των μπλοκ από την αρχή (Κυρίτσης, 2019).

Πίνακας 2 Τα θετικά και τα αρνητικά της διαδικασίας εξόρυξης σύμφωνα με τον Szmigielski (2016, σελ. 32-33)

Τα θετικά της διαδικασίας εξόρυξης	Τα αρνητικά της διαδικασίας εξόρυξης
•Δεν χρειάζεται εξειδικευμένο εξοπλισμό •Αποτελεί μια καλή εισαγωγή για να ξεκινήσει κανείς τη διαδικασία εξόρυξης για πρώτη φορά •Αξιοσημείωτη εκπαιδευτική εμπειρία •Είναι διασκεδαστικό	•Υψηλό κόστος σε κατανάλωση ηλεκτρικού ρεύματος •Δεν είναι προσοδοφόρο •Φθορά στον επεξεργαστή

Επίσης, άλλο ένα αρνητικό χαρακτηριστικό αφορά στον περιορισμένο αριθμό του κρυπτονομίσματος ακριβώς για τη διατήρηση της αξίας του. Το νόμισμα είναι σχεδιασμένο έτσι ώστε ο συνολικός αριθμός όλων των *Bitcoin* που θα δημιουργηθούν ποτέ να είναι ακριβώς 21 εκατομμύρια περίπου το έτος 2140 (Κυρίτσης, 2019). Έτσι, τα *Bitcoin* ως προς τον τρόπο παραγωγής τους, προσομοιάζουν με την παραγωγή

[47] Αυτή τη στιγμή το Bitcoin δύναται να πραγματοποιεί ταυτόχρονα μόλις 7 με 10 συναλλαγές σε αντίθεση με άλλους τρόπους πληρωμής (π.χ. μέσω e-banking).

χρυσού και μετάλλων. Ανάλογα με τη διαθεσιμότητά τους παγκοσμίως στον πλανήτη θα υπάρξει και η αντίστοιχη παραγωγή.

Σε τεχνικό επίπεδο, κάθε μπλοκ δεν μπορεί να ξεπεράσει το 1MB, ήτοι τις επτά συναλλαγές, και παράλληλα κάθε δέκα λεπτά εισχωρούν στην αλυσίδα νέα μπλοκ. Στον οικονομικό κόσμο, παγκόσμιοι οργανισμοί ενημερώνουν για απειλές στα 'πορτοφόλια' των πολιτών. Ήδη, εταιρείες όπως αυτή στην Ιαπωνία, *Mt. Gox*, και μια από τις μεγαλύτερες εταιρείες συναλλαγών *Bitcoin*, κήρυξε διαδικασία εξυγίανσης λόγω χρέους μισού δις δολαρίων σε ψηφιακά νομίσματα (Sapovadia, 2015).

Πίνακας 3 Οι κίνδυνοι της νέας 'Άγριας Δύσης'[48]

Σύμφωνα με την *Tiana Laurence (2017, σελ. 47)*	Σύμφωνα με τον *Imran Bashir (2017, σελ. 30-33)*	Σύμφωνα με την ΤτΕ (2018) σε συνεργασία με την Ε.Α.Τ.
•Θύματα διαδικτυακής απάτης •Απατηλοί- μη πραγματικοί ιστοχώροι •Εφαρμογές με δυνατότητες για γρήγορο *bitcoin* κέρδος χωρίς ρίσκο – ισχύει κυρίως για τις επενδύσεις (πρόσκληση και άλλων συγγενών σε επένδυση)	•Δεν υπάρχουν συμπληρωματικά μέτρα προστασίας της εκάστοτε ιδιοκτησίας (κινητής ή ακίνητης) πέραν από έναν αριθμό •Ευάλωτη δομή σε ό,τι αφορά τα δεδομένα •Πολύ υψηλά κόστη •Θέματα χρόνου, υψηλής κατανάλωσης, ενέργειας και περιβάλλοντος.	•Μπορεί να χαθούν χρήματα στην πλατφόρμα ανταλλαγής •Τα χρήματα μπορεί να κλαπούν από το ψηφιακό πορτοφόλι •Δεν υπάρχει προστασία όταν χρησιμοποιούνται εικονικά νομίσματα ως μέσο πληρωμής •Η αξία του εικονικού νομίσματος μπορεί να αλλάξει ταχέως και μπορεί ακόμη και να μηδενιστεί •Οι συναλλαγές σε εικονικό νόμισμα μπορεί να αποτελέσουν αντικείμενο κατάχρησης για εγκληματικές δραστηριότητες, συμπεριλαμβανομένης της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες •Ενδέχεται να υπέχει ο χρήστης φορολογικές υποχρεώσεις

Σε νομικό επίπεδο, δικαστήρια των Η.Π.Α. είχαν να αποφανθούν περί της αρμοδιότητάς τους για διαμάχες στον *Bitcoin* κόσμο[49]. Το τοπίο χαρακτηρίζεται από

[48] Ο όρος χρησιμοποιήθηκε από την Laurence (2017, σελ. 47).

[49] SEC v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013, Gordon v. Dailey, No. 14-cv-7495 (JHR) (JS) (D.C.N.J., July 25, 2016

πληθώρα δυσκολιών λόγω της δυσχέρειας να καταστεί έγκυρη μια συναλλαγή. Σε περίπτωση κάποιας αδικίας, το θύμα δύσκολα θα μπορέσει να φέρει τις κατάλληλες αποδείξεις. Είναι κατανοητό ότι, τελικά, θα χρειαστεί ένα ρυθμιστικό πλαίσιο[50] για τους χρήστες και τις εκάστοτε έννομες τάξεις (Girasa, 2018). Έχουν υπάρξει πολλές δικαστικές υποθέσεις για εξαπάτηση, παράνομο εμπόριο και εγκληματικές ενέργειες (Girasa, 2018).

Πίνακας 4 Η ασφάλεια των Bitcoin (Συλλογή δεδομένων από την βιβλιογραφία)

Η ασφάλεια του κρυπτονομίσματος απειλείται από τα εξής στοιχεία	Συνήθεις εγκληματικές δραστηριότητες με *CSC contracts*
• Την δημιουργία συμφωνίας consensus- με 51%, γεγονός που υπονοεί τον έλεγχο του συστήματος από ενδεχόμενους 'δράστες-attackers' • Την αδυναμία αποκατάστασης του ιδιωτικού κλειδιού σε περίπτωση απώλειάς του • Τις εγκληματικές δραστηριότητες	• Cracking ψηφιακών πορτοφολιών • Παράνομο εμπόριο ναρκωτικών • Το πρόβλημα των διπλοπληρωμών (δηλ. να πληρώνει κανείς με τα ίδια Bitcoin διαφορετικά πράγματα) • Ξέπλυμα μαύρου χρήματος

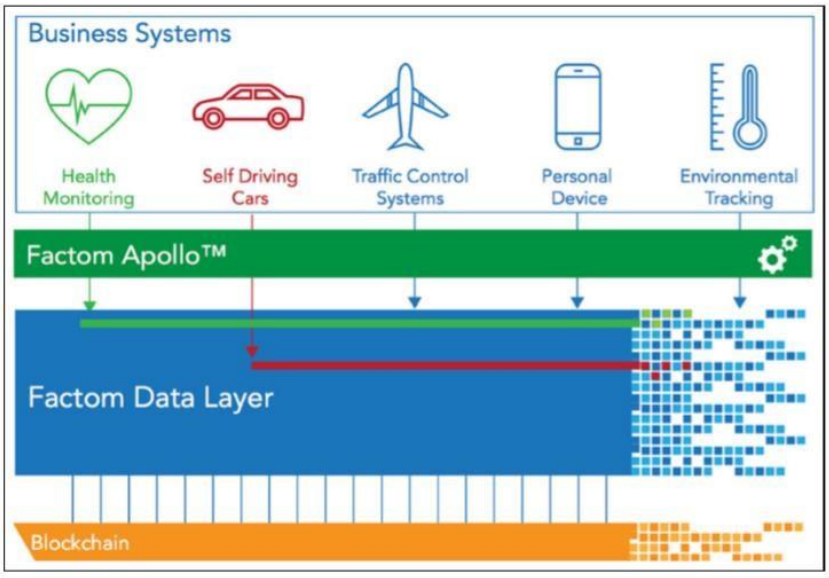
Ο όρος *CSC* αναφέρεται στα *criminal smart contracts*, συμβάσεις που μπορούν να διευκολύνουν τον διαμοιρασμό εμπιστευτικών πληροφοριών, την κλοπή κρυπτογραφημένων κλειδιών και διάφορα εγκλήματα του πραγματικού κόσμου όπως δολοφονίες, τρομοκρατία κ.λπ. (Li, Jiang, Chen, Luo & Wen, 2017). Οι αδυναμίες των έξυπνων συμβάσεων για χακάρισμα είναι δυνατόν να προκύψουν λόγω της ιδιαίτερης ευαισθησίας τους (Wang, Qin, Hu & Xiao, 2017). Σύμφωνα με ορισμένους ερευνητές, «*η ηθελημένη ασφάλεια των νομισμάτων περιορίζεται μόνον στην πρόληψη των διπλών πληρωμών*» (Low & Teo, 2016) και πουθενά αλλού.

[50] Έχει παρατηρηθεί πως ο πολίτης χρειάζεται και μια καθαρά νομική αλλά και μια φοροτεχνική ρύθμιση στα κρυπτονομίσματα.

Υποκεφάλαιο 2.2 *Altcoins*

2.2.1 Ορισμός και λειτουργία των *Altcoins*

Όπως με το *Bitcoin*, το δίκτυο *Ethereum* αποτελεί την δεύτερη επανάσταση της λογικής Blockchain. Χρησιμοποιεί την τεχνολογία *PoW* για να επιτύχει διαμοιρασμένη συναίνεση και υποστηρίζει τα *smart contracts* μέσω αποκεντρωμένων αυτόνομων δικτύων [51]. Με το λογισμικό αυτό μπορούν να δημιουργηθούν πληθώρα νέων κρυπτονομισμάτων συγκρατώντας υψηλά τα επίπεδα ασφάλειας σε δεδομένα και σύστημα [52]. Το *Factom* είναι η "τρίτη επανάσταση" με ελαφρύτερο σύστημα συμφωνίας ενσωματώνοντας την τεχνολογία ηλεκτρονικής ψήφου και αποθηκεύοντας πολλή περισσότερη πληροφορία (Laurence, 2017, σελ 12).



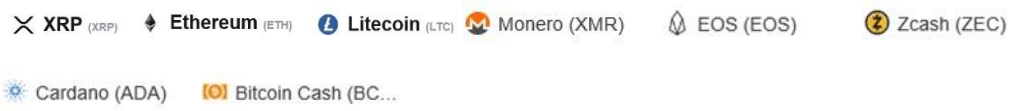
Εικόνα 6 Τα smart contracts στο Factom Blockchain (Laurence, 2017, σελ. 79)

[51] 'Decentralized Autonomous Organisations' (DAOs) στην αγγλική ορολογία.
[52] Όπως το *Namecoin*.

Το *Ethereum* βγάζει και δικά του κρυπτονομίσματα: ETH και ETC (Karame & Androulaki, 2016, σελ. 184). Το *Hyperledger,* αν και δεν θεωρείται Blockchain, ξεκίνησε από την *Linux foundation* το 2015 με πεδία εφαρμογής τις παγκόσμιες εταιρικές και βιομηχανικές συναλλαγές[53]. Σε ό,τι αφορά τα κρυπτονομίσματα, κυκλοφορούν πάνω από 2000[54], χάνουν όμως συνεχώς την αξία τους.

Κατά τον Imran Bashir: "*Εάν ο στόχος είναι να δημιουργηθεί ένα διαμοιρασμένοαποκεντρωμένο σύστημα blockchain τότε γίνεται αναφορά στα εναλλακτικά blockchain. Εάν όμως ο στόχος είναι η παρουσίαση ενός καινούργιου νομίσματος, τότε μιλάμε για altcoin*" (2017, σελ. 180).

Ουσιαστικά, από την δομή *Bitcoin* έχουν προκύψει πολλά διαφορετικά κρυπτονομίσματα. Το *Namecoin*, με εμφάνιση το 2011, είναι ένα εναλλακτικό νόμισμα που προέρχεται από αυτό και διαμοιράστηκε μετά από αυτό. Έχει σχεδιαστεί για να παρέχει ένα υποκατάστατο σύστημα του *DNS*[55] ενώ επεκτείνει το Πρωτόκολλο *Bitcoin* και στους λεγόμενους τύπους συναλλαγών[56]. Μετά το 2013, πολλά altcoins εμφανίστηκαν στην αγορά. Το *Litecoin* αποτελεί άλλο ένα παράδειγμα που χρησιμοποιεί την κρυπτογραφία στους κρίκους όντας ανθεκτικό στη συγκράτηση μνήμης. Άλλη μια τεχνολογία είναι αυτή του *Dogecoin* που επεκτάθηκε[57] από το *Litecoin* (Judmayer et al., 2017, σελ. 50).



Εικόνα 7 Παραδείγματα altcoins: Bitcoin Cash, Cardano, Zcash, EOS, Monero, Litecoin, Ethereum, Ripple (XRP). Σύνθεση εικονιδίων που ανακτήθηκαν από: https://coinmarketcap.com/currencies/

[53] Εναλλακτικές τεχνολογίες Blockchain που προσφέρουν νέες λύσεις είναι : *Kadena, Ripple, Stellar, Rootstock, Quorum, Tezos, Storj, Maidsafe, BigChainDB, Multichain, Tendermint*.

[54] Βλ. για περισσότερες πληροφορίες : https://graphics.reuters.com/CRYPTO-CURRENCIESCONFLICTS/0100818S2BW/index.html

[55] Το 'Domain Name System' (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών, που χρησιμοποιούν το πρωτόκολλο IP. Αντιστοιχίζει τα ονόματα των υπολογιστών υπηρεσίας σε διευθύνσεις IP.

[56] 'Transaction Types' στην αγγλική ορολογία

[57] Μέσω της μεθόδου 'forking' (βλ. *Γλωσσάρι απόδοσης ξενόγλωσσων όρων*)

Το *PoW* σχήμα πρωτοχρησιμοποιήθηκε στο *Bitcoin* και αξιοποιήθηκε ως ένας μηχανισμός "εγγύησης" για την εύρεση του κατάλληλου μπλοκ κατά τη διαδικασία εξόρυξης (Bashir, 2017, σελ. 184). Το *Primecoin* είναι άλλη μια τεχνολογία που εναντιώθηκε κατά κάποιο τρόπο με το *Bitcoin* σε ό, τι αφορά το νέο σύστημα *PoW* (τον αλγόριθμο για την εύρεση του κατάλληλου κρίκου-hash) που εισήγαγε. Το *Zcash* κυκλοφόρησε το 2016 και είναι το πρώτο κρυπτονόμισμα που χρησιμοποιεί συγκεκριμένου είδους μηδενική γνώση *proofs*, γνωστό ως 'zero-knowledge Succinct Non-interactive Arguments of Knowledge' (zk-SNARKs) έχοντας ως στόχο την παροχή πλήρους ιδιωτικότητας στον χρήστη (Bashir, 2017).

2.2.2 Θετικά σημεία και εφαρμογές των *Altcoins*

Τεχνικά, το σχήμα PoW που χρησιμοποιήθηκε στο *Bitcoin* παρέχει την εγγύηση στον "μεταλλωρύχο" ότι έχει ολοκληρώσει την απαιτούμενη εργασία για την εύρεση ενός μπλοκ. Με τα εναλλακτικά νομίσματα έχουν εισαχθεί νέες τεχνολογίες στο πεδίο της αλυσίδας κόμβων και της συναινετικής διαδικασίας όπως: *Proof of Storage*, που απαιτεί από τους χρήστες να εισάγουν ένα μεγάλο όγκο δεδομένων για την εύρεση του μπλοκ και *Proof of Stake*[58], το οποίο αφορά σε εναλλακτικά σχήματα *PoW* και αξιοποιήθηκε με το κρυπτονόμισμα *PeerCoin* (Bashir, 2017, σελ. 186). Η τελευταία κατηγορία περιλαμβάνει την ανάπτυξη διαφόρων υποκατηγοριών όπως: *Proof of Coinage, Proof of Deposit, Proof of Burn, Proof of Activity*. Φυσικά, η ανάλυση αυτών δεν αφορά στην παρούσα μελέτη όμως είναι σημαντική η αναφορά τους για να αναδειχθούν οι "αδύναμες" πτυχές του πρωτοεμφανιζόμενου *Bitcoin* σε σχέση με τις εξελίξεις της τεχνολογίας. Επίσης, τα εναλλακτικά νομίσματα αναφορικά με την ανάπτυξη διαφόρων αλγορίθμων με στόχο την καλυτέρευση ορισμένων παραμέτρων της διαδικασίας *hashing* έχουν παρουσιάσει τους εξής αλγορίθμους: Kimoto Gravity Well, Dark Gravity Wave, DigiShield, MIDAS (Multi Interval Difficulty Adjustment

[58] Στην περίπτωση αυτή, οι κάτοχοι κρυπτονομισμάτων επιλέγονται τυχαία από το σύστημα να συναινέσουν στο κλείσιμο ενός μπλοκ συναλλαγών.

System), το οποίο απαντά ταχύτερα και αποδοτικότερα στις επιθέσεις όντας πολύ πιο ανθεκτικό (Bashir, 2017, σελ. 190). Εννοείται πως κάθε altcoin αναλόγως της φύσης του διαθέτει αναλογικά και εφαρμογές *smart contracts*.

2.2.3 Συγκριτική παράθεση των *Altcoins* με τα *Bitcoins*

Οι λόγοι που εμφανίστηκαν τα altcoins εκπηγάζουν από ορισμένα ελαττώματα του *Bitcoin*. Εν γένει, το *Bitcoin* δεν είναι ευρέως γνωστό, πολλοί άνθρωποι δεν είναι ενήμεροι και οι λίστες των συνεργαζόμενων επιχειρήσεων είναι ακόμη μικρές[59]. Υπάρχει μια σχετική αστάθεια καθώς το νόμισμα είναι βέβαια καινούργιο όχι όμως *ώριμο*, με αποτέλεσμα να μην γνωρίζουν αρκετοί την παγκόσμια εξέλιξή του, πράγμα που το καθιστά, κατ'αλλους, *συναρπαστικό*. Σε λειτουργικό επίπεδο, το νόμισμα έχει ακόμα προβλήματα πρωτίστως στην ιδιωτικότητα γιατί υπάρχει η πιθανότητα μέσω των συναλλαγών να βρεθεί η IP διεύθυνση (Laurence, 2017, σελ. 196) και ως εκ τούτου η ταυτότητα του χρήστη. Με τον ίδιο τρόπο πληροφορίες συναλλαγών, όπως στοιχεία συναλλαγής, καθολικά και κρυπτογραφήσεις, μπορούν να αποκτηθούν. Για το λόγο αυτό, δημιουργήθηκαν ορισμένα πρωτόκολλα, όπως: μικτά πρωτόκολλα[60], τριτομερή μικτά δίκτυα[61] και εσωτερικής ανωνυμίας (Bashir, 2017, σελ. 190). Εκτός αυτού, η παραγωγή του *Bitcoin* θα παύσει κάπου στα 21 εκατομμύρια νομίσματα (Volkering, 2017) ενώ σε ορισμένα altcoins όπως το *DogeCoin* η παραγωγή είναι απεριόριστη. Επίσης, ο ρυθμός κλειδώματος ενός μπλοκ, όπως προειπώθηκε, είναι κατά μέσο όρο 10 λεπτά ενώ στο *LiteCoin* ο χρόνος περιορίζεται στα 2,5 λεπτά. Σημαντικό είναι να προσθέσουμε πως το *Bitcoin* πια έχει υψηλά έξοδα [62] συνδράμοντας έτσι στην ανάπτυξη των altcoins. Υπάρχει επίσης η εντύπωση πως το *Bitcoin* έχει σοβαρά τεχνικά προβλήματα με διάφορα ζητήματα ανωνυμίας. Σύμφωνα με πολλούς κριτικούς και χρήστες, όλα αυτά τα στοιχεία δεν σημαίνουν ότι το *Bitcoin* σε λίγο καιρό θα ξεχαστεί. Σίγουρα θα υπάρξουν αλλαγές και σίγουρα δεν γνωρίζει

[59] Τουλάχιστον στον ελληνικό χώρο.
[60] 'Mixing Protocols', με την αγγλική ορολογία
[61] 'Third-Party Mixing', με την αγγλική ορολογία.
[62] 'Fees', όπως είναι ευρέως γνωστά.

κανείς αν το νόμισμα αυτό θα εξαφανιστεί ή θα συνεχίσει την πορεία του. Με οικονομικούς όρους, όποτε κατεβαίνει η αξία του *Bitcoin* ομοίως συμπεριφέρονται και τα άλλα κρυπτονομίσματα, φανερώνοντας πως το *Bitcoin* με τα altcoins είναι πολύ στενά συνδεδεμένα (Hoffman, 2018). Όντως, σύμφωνα με μια έρευνα, ένα μεικτό ψηφιακό πορτοφόλι – *Bitcoin* με άλλα κρυπτονομίσματα – προσφέρει περισσότερα θετικά για τους επενδυτές και διαχειριστές (Mensi, Rehman, AlYahyaee, Al-Jarrah & Kang, 2019, σελ. 283). Ένα *Ethereum-Bitcoin* πορτοφόλι διακρίνεται για σημαντική μείωση των ρίσκων και διαχειρισιμότητα. Σημειωτέον πως η αλληλεξάρτηση των κρυπτονομισμάτων μεταξύ τους αποτελεί τη βάση όχι μόνο για τεχνολογική εξέλιξη αλλά και για οικονομική ανάπτυξη, όπως παρατηρείται από πρόσφατη έρευνα που διεξήχθη το διάστημα 2015-2018. Εκεί, παρατηρήθηκε ραγδαία αύξηση κατά 10% των «διμερών σχέσεων» μεταξύ των εξής νομισμάτων: *Bitcoin–Dash, Ethereum–Litecoin, Ethereum–Dash, Ethereum–Monero, Ripple–Stellar* (Cagli, 2018, σελ. 4). Παρά το ό,τι το *Bitcoin* δεν έχει την πρωτοκαθεδρία (Yi, Xu & Wang, 2018), σίγουρα όμως αποτελεί ένα ‘καλό’ εργαλείο για επενδύσεις (Volkering, 2017) με σιγουριά και διαχειρισιμότητα. Από άλλης πλευράς, τα altcoins δεν έχουν αυτό που έχει το παραδοσιακό *Bitcoin*: ιστορία και κοινότητα (Krawisz, 2013).

Μεγάλο μέρος της εμπιστοσύνης στο *Bitcoin* προέρχεται από το γεγονός ότι δεν απαιτεί καμιά απολύτως εμπιστοσύνη. Είναι ανοιχτού κώδικα και αποκεντρωμένο. Ο καθένας έχει πρόσβαση σε ολόκληρο τον κώδικα ανά πάσα στιγμή (Bitcoin Project, 2019). Όλες οι συναλλαγές και τα *Bitcoins* που δημιουργούνται μπορεί να τα ανατρέξει ο καθένας με διαφάνεια σε πραγματικό χρόνο. Όλες οι πληρωμές μπορούν να γίνουν χωρίς εξάρτηση από τρίτους (Bitcoin Project, 2019). Αυτή η απλότητα της φράσης στηρίζεται στην παραδοχή ότι η ‘άγνοια προσφέρει εμπιστοσύνη’. Θα λέγαμε, καλύτερα, ότι τελικά αυτή ‘υποχρεώνει’ στην εμπιστοσύνη.

2.2.4 Προβληματισμοί και ανοιχτά ζητήματα των *Altcoin*s

Ήδη, τα αρνητικά σημεία διαφαίνονται στον ορίζοντα. Το altcoin *Monero* έχει σχεδιαστεί για να είναι ασφαλές, ιδιωτικό, και μη ανιχνεύσιμο (Bambara & Allen, 2018, σελ. 171). Όπως είναι κατανοητό, οι συναλλαγές του δεν είναι δυνατόν να

ανιχνευτούν αναδρομικά πράγμα που το καθιστά σίγουρο εργαλείο για παράνομο εμπόριο ναρκωτικών. Στο πεδίο αυτό, οι τιμές προσφοράς-ζήτησης ουσιών είναι οι υψηλότερες στην Αυστραλιανή χώρα από οπουδήποτε αλλού (Broséus, Morelato, Tahtouh & Roux, 2017).

Η πολυπλοκότητα του συστήματος όπως και η εμφάνιση πολλών διαφορετικών κρυπτονομισμάτων έχει οδηγήσει και σε ορισμένες *απώλειες*: ήδη ιστοσελίδες και επικοινωνιακά fora ενημερώνουν τους χρήστες για τα κρυπτονομίσματα που θα πρέπει να αποφευχθούν για επενδύσεις. Πρόσφατα βγήκε ανακοίνωση για τα εξής: *Verge* (XVG), *Tether* (USDT) και *Dogecoin* (DOGE) κυρίως λόγω των ζημιών που έχουν αυτά υποστεί (iBankCrypto, 2018). Βέβαια, η αγορά είναι σε εξέλιξη και τα δεδομένα μεταβάλλονται συνεχώς και δεν γνωρίζει κανείς που θα κινηθεί η «αγορά» τα επόμενα χρόνια.

Ας μην ξεχνάμε βέβαια και το ρυθμιστικό πλαίσιο που, έχοντας αγγίξει και το ευρωπαϊκό ‘τραπέζι’, κατά μερικούς οφείλει να τεθεί σε εφαρμογή. Σύμφωνα με την ευρωπαϊκή νομοθετική πρόταση για τους χρήστες αυτών των υπηρεσιών, η ανωνυμία και η ψευδωνυμία, που είναι συνημμένες με τα ψηφιακά νομίσματα, καταργείται (Vandezande, 2018). Οι χρήστες θα πρέπει να είναι ταυτοποιήσιμοι και διαφανείς με τις αρμόδιες αρχές. Βέβαια, αυτή η πρόταση βρίσκεται ακόμα στην αρχή υιοθέτησης και ψήφισης από τα αρμόδια ευρωπαϊκά όργανα (Vandezande, 2018). Το μέλλον θα δείξει πού θα κινηθεί η ανάγκη αυτή για ρύθμιση των ψηφιακών νομισμάτων.

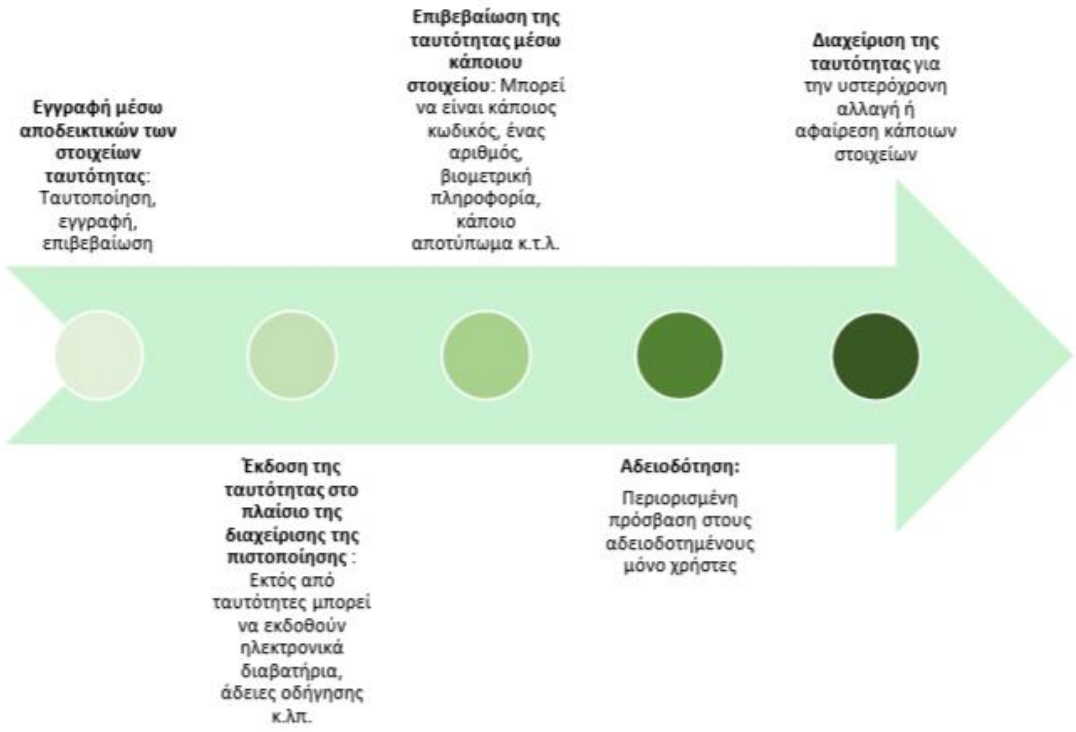
Κεφάλαιο 3. Ασφάλεια, Ιδιωτικότητα, Ταυτοποίηση και Πρωτόκολλο Blockchain

Υποκεφάλαιο 3.1 Ψηφιακή Ασφάλεια και Ιδιωτικότητα

3.1.1 Ασφάλεια (Security)

Πάνω από 1,5 δισεκατομμύρια άτομα σε αναπτυσσόμενες χώρες σε όλον τον πλανήτη δεν διαθέτουν αστικές ταυτότητες και κατά συνέπεια αυτό οδηγεί στον αποκλεισμό από την κοινωνική, πολιτική και οικονομική ζωή (World Bank Group & GSMA, 2016). Η ιδέα της ηλεκτρονικής ταυτότητας αναδεικνύει την τεχνολογική εξέλιξη, τις ταχείες και αποτελεσματικές συναλλαγές οικονομικού, τραπεζικού και φορολογικού περιεχομένου στις σχέσεις μεταξύ πολιτών και κράτους και αποτελεί ένα εν δυνάμει εργαλείο εξοικονόμησης σε κυβερνητικό και επιχειρηματικό επίπεδο. Σε αυτό το πλαίσιο, η ηλεκτρονική ταυτότητα, όπως έχει αποδοθεί σε ορισμό από την πρωτοβουλία '*ID4D*' είναι μια "*συλλογή από αποθηκευμένα και καταχωρημένα δεδομένα που περιγράφουν ένα μοναδικό πρόσωπο με στόχο διαφόρων ειδών ηλεκτρονικές συναλλαγές*" (World Bank Group & GSMA, 2016, σελ. 11).

Πίνακας 5 Ο τυπικός κύκλος ζωής της ηλεκτρονικής ταυτοποίησης



Το πεδίο της ασφάλειας σε ό,τι αφορά την ταυτοποίηση περιλαμβάνει αρχικά τα στάδια της ίδιας της ταυτοποίησης του προσώπου με τα πραγματικά στοιχεία. Αρκετά συχνά τα παρεχόμενα από τους πολίτες στοιχεία είναι ανεπαρκή ή αμφισβητήσιμα. Στην περίπτωση αυτή, αναλαμβάνει την ταυτοποίηση ένας “μάρτυρας” (Introducer). Κατά το στάδιο της πιστοποίησης της αυθεντικότητας (Authentication) (Forouzan, 2014, σελ. 642) της πληροφορίας αποδεικνύεται ότι ο χρήστης είναι με αυθεντικό τρόπο αυτός που υποστηρίζει ότι είναι[63] (World Bank Group, 2018a). Αμέσως μετά, προβλέπεται η αδειοδότηση (Authorization), κατά την οποία προστατεύονται κύρια δεδομένα και στοιχεία μέσω της περιορισμένης πρόσβασης για αδειοδοτημένους μόνο χρήστες.

[63] Μπορεί να είναι μέσω κάποιου PIN, βιομετρικής πληροφορίας κ.τ.λ.

Σε επίπεδα ασφάλειας, η διαδικασία της *ακρόασης* (Auditing) είναι ο μηχανισμός της εγγραφής και της εξέτασης στοιχείων για την ανίχνευση απρόβλεπτης ή μη αδειοδοτημένης ενέργειας (IBM Knowledge Center, 2019). Άλλο ένα σημαντικό εργαλείο αποτελεί η έννοια της εμπιστευτικότητας που προστατεύει ευαίσθητες πληροφορίες από μη αδειοδοτημένη διαρροή δεδομένων. Επίσης, η ακεραιότητα των πληροφοριών ανιχνεύει οποιαδήποτε ενδεχόμενη μεταβολή αυτών (IBM Knowledge Center, 2019).

Τεχνικά, οι τεχνολογίες που χρησιμοποιούνται για την ασφάλεια είναι οι ακόλουθες. Αρχικά, αναπτύσσεται η *κρυπτογράφηση*, που στηρίζεται στην μετατροπή ενός μηνύματος σε ακατάληπτη μορφή, η οποία δεν μπορεί να αναγνωστεί εάν δεν αποκρυπτογραφηθεί. Σύμφωνα με τον ορισμό της IBM (IBM Knowledge Center, 2019), η κρυπτογράφηση είναι η διαδικασία της μετατροπής ενός απλού κειμένου (plaintext) σε ένα κρυπτοκείμενο (ciphertext). Εν συνεχεία, υπάρχει η λεγόμενη *σύνοψη μηνύματος* (message digest) η οποία δίνει μια αριθμητική αναπαράσταση του περιεχομένου του μηνύματος. Η σύνοψη μηνύματος κατακερματίζεται (hash) και κρυπτογραφείται δημιουργώντας μια ψηφιακή υπογραφή. Άλλοι μηχανισμοί ασφαλείας αποτελούν τα *ψηφιακά πιστοποιητικά* που εγγυώνται ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια ορισμένη οντότητα. Όντως, τα κλειδιά αυτά εκδίδονται από μια συγκεκριμένη Αρχή Πιστοποίησης. Τέλος, υπάρχει το σύστημα *Public Key Infrastructure* που αφορά σε διευκολύνσεις, πολιτικές και υπηρεσίες που υποστηρίζουν τη χρήση κρυπτογράφησης δημόσιων κλειδιών για την ταυτοποίηση των μερών σε μια συναλλαγή (IBM Knowledge Center, 2019).

3.1.2 Ιδιωτικότητα (Privacy)

Η έννοια της ιδιωτικότητας αναφέρεται με τον όρο ‘*privacy’* και διαφέρει από την προϋπόθεση της ασφάλειας στο σύστημα. Η ιδιωτικότητα είναι ένα θεμελιώδες

ανθρώπινο δικαίωμα συνταγματικώς, ευρωπαϊκώς[64] και διεθνώς[65] θεσμοθετημένο το οποίο περιλαμβάνει τα αξιώματα της ανθρώπινης αξιοπρέπειας και της ανθρώπινης ελευθερίας. Παρά ταύτα, παρατηρείται ασάφεια και δυσκολία στον ορισμό της. Το 1890 ο δικηγόρος Louis Brandeis ενώπιον του Ανωτάτου Δικαστηρίου των Η.Π.Α. όρισε το δικαίωμα στην ιδιωτικότητα ως το 'δικαίωμα στη λήθη', όπως χαρακτηριστικά έχει μείνει στην ιστορία : «the right to be left alone» (The Public Voice, χ.η.). Υπάρχουν, έτσι, τα εξής πεδία ιδιωτικότητας: η πληροφοριακή ιδιωτικότητα που σχετίζεται με δημόσια έγγραφα και μητρώα, η σωματική ιδιωτικότητα που σχετίζεται με τη ακεραιότητα του ανθρώπινου σώματος[66], την ιδιωτικότητα των τηλεπικοινωνιών και τέλος την ιδιωτικότητα σε ό,τι αφορά το άσυλο της κατοικίας και την οριοθέτηση των προσωπικών και εργασιακών περιβαλλόντων[67] (The Public Voice, χ.η.).

Ειδικά για το σύστημα της ηλεκτρονικής ταυτοποίησης, ο εκάστοτε κυβερνητικός φορέας θα πρέπει να αναπτύξει ένα κατάλληλο πλαίσιο πολιτικής στρατηγικής σχετικά με το ποια δεδομένα καταχωρούνται, πότε, πώς προστατεύεται η πληροφορία από επιθέσεις και παρεμβολές, πώς η εμπιστευτικότητα των πολιτών διασφαλίζεται, για ποιους σκοπούς θα χρησιμοποιηθούν τα δεδομένα, ποιος θα έχει πρόσβαση σε αυτά όπως και τον κατάλληλο σχεδιασμό της αδειοδότησης[68] (World Bank Group, 2018a). Όλη αυτή η διαδικασία οδηγεί στην καταμέτρηση των δικαιωμάτων και των υποχρεώσεων του χρήστη με απώτερο στόχο την ίδια τη χρήση. Χωρίς αυτές τις εγγυήσεις στο πεδίο της ιδιωτικότητας δεν θα υπάρχει εμπιστοσύνη στο σύστημα. Το σημαντικό είναι, εν τέλει, να διασφαλιστεί η διαδικασία με κατάλληλο προγραμματισμό και αποτελεσματική σχεδίαση, καθώς οι δυνατότητες αποθήκευσης και καταχώρησης των πληροφοριών είναι αμέτρητες, δεδομένων των σύγχρονων τεχνικών δομών. Έτσι, στον ψηφιακό κόσμο είναι αδύνατον κάποιος να

[64] European Convention on Human Rights (Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου, ΕΣΔΑ)
[65] Διεθνές Σύμφωνο για τα αστικά και πολιτικά Δικαιώματα (International Covenant on Civil and Political Rights, ICCPR)
[66] Γενετικά τεστ, ιατρικές έρευνες σε ανθρώπινα όργανα κ.λπ.
[67] Όπως έρευνες, κάμερες παρακολούθησης κ.λπ.
[68] Η αδειοδότηση πραγματοποιείται από την πλευρά του πολίτη προς τον εκάστοτε φορέα.

«κρυφτεί», εκτός κι αν αναπτυχθούν συστήματα ασφαλείας όπως η κρυπτογράφηση (Capurro et al., 2013). Εντούτοις, ο στόχος δεν περιορίζεται μόνο στο σχεδιασμό μιας ελκυστικής τεχνολογίας, αλλά αφορά και στην απαίτηση για ορθή διαχείριση πόρων και χρημάτων από τους οργανισμούς.

Υποκεφάλαιο 3.2 Οι τεχνολογίες ταυτοποιήσεων εν γένει

Η ταυτοποίηση ορίζεται από τον John Hartley (2011) ως μια "διαδικασία που εμπλέκει στοιχεία ταυτότητας με στόχο την εννοιοδότηση του εαυτού". Για την ταυτοποίηση του ατόμου χρησιμοποιούνται τεχνολογίες πιστοποίησης ή αλλιώς τρόποι πιστοποίησης γνωστοί ως *Credential Technologies*. Ειδικότερα, υπάρχουν ορισμένες κατηγορίες τεχνολογιών πιστοποίησης: βιομετρική πληροφορία, κάρτες, έξυπνες κάρτες και κινητά τηλέφωνα (World Bank Group, 2018a).

Σε πρώτο επίπεδο, η βιομετρική πληροφορία συνίσταται στην αναγνώριση των μοναδικών φυσικών ή συμπεριφορικών στοιχείων του ατόμου για την ταυτοποίηση και την "αυθεντικοποίηση" της ταυτότητάς του [69] (Das, 2016). Η βιομετρική καταχώρηση της πληροφορίας διακρίνεται σε πρωτεύουσα βιομετρική πληροφορία (δαχτυλικό αποτύπωμα, πρόσωπο, αναγνώριση ίριδας κ.λπ.) και σε απλή βιομετρική πληροφορία (όπως η υπογραφή) (World Bank Group, 2018a, σελ. 18). Οι βιομετρικές μέθοδοι είναι οι εξής: δαχτυλικό αποτύπωμα, αναγνώριση παλάμης, φλεβών, αναγνώριση προσώπου, ίριδος, αμφιβληστροειδούς, φωνής, συμπεριφοράς, δαχτυλογραφίας (Keystroke) υπογραφής. Στο μέλλον θα έχουν αναπτυχθεί και τρόποι καταμέτρησης βιομετρικής πληροφορίας μέσω της αναγνώρισης DNA, της αναγνώρισης της βάδισης και του λοβού (Das, 2016, σελ. 15-25). Εν γένει, η

[69] Εδώ θα πρέπει να διακριθεί το στάδιο της ανίχνευσης και καταχώρησης της πληροφορίας (Capturing) από το στάδιο της ταυτοποίησης (Matching) ότι η πληροφορία ως είσοδος στο σύστημα αντιστοιχεί με την ήδη καταχωρημένη πληροφορία σε αυτό. Οι τεχνολογίες σχεδιασμού και ανάπτυξης διαφέρουν σ' αυτά τα δυο στάδια.

βιομετρική πληροφορία αποτελεί ένα στοιχείο μοναδικό, πανταχού παρόν, μετρήσιμο, πρακτικό και *μη-διαμοιράσιμο* (Das, 2016).

Μία δεύτερη μέθοδος ταυτοποίησης αφορά στις κάρτες που μπορούν να αναγνωστούν από εξειδικευμένες συσκευές εισόδου ή αναγνώστες καρτών[70].

Σε πρώτη φάση, οι μη ηλεκτρονικές κάρτες[71] αναπαριστούν βασικές δημογραφικές πληροφορίες συνήθως με κάποια φωτογραφία, αριθμό, διεύθυνση, ημερομηνία γέννησης κ.λπ. Σε δεύτερη φάση, υπάρχουν η μη έξυπνες ψηφιακές κάρτες RFID, που χρησιμοποιούν ηλεκτρομαγνητική ενέργεια για την ανάγνωση πληροφοριών και βρίσκονται αποθηκευμένες στις RFID ετικέτες ταυτοποίησης[72] (World Bank Group, 2018a). Η τεχνολογία RFID φημίζεται για την πρακτικότητά της και την ευρεία της απήχηση δεδομένης της χρήσης της ήδη από το 1943 για τη διενέργεια διαφόρων διαδικασιών όπως το άνοιγμα κάποιας πόρτας, την ανίχνευση πυρηνικών στοιχείων κ.λπ. (Yang & Hancke, 2017, σελ. 352). Σήμερα, μια ευρέως διαδεδομένη πρακτική είναι αυτή της ταυτότητας *Electronic Product Code* (EPC) για την ανίχνευση των εμπορευμάτων, τις παρτίδας και των προϊόντων[73]. Μια πραγματική επανάσταση έχει πραγματοποιηθεί με την σύζευξη RFID και IoT τεχνολογίας για τον έλεγχο κάθε προϊόντος μιας επιχείρησης και τη διαχείριση των εμπορευμάτων (Mašek, Kolarovszki & Čamaj, 2016) σε πραγματικό χρόνο. Έτσι, η τεχνολογία χρησιμοποιείται για την "ταυτοποίηση πραγμάτων ή ανθρώπων αποθηκεύοντας ένα μοναδικό στοιχείο που αφορά στο εν λόγω αντικείμενο" (προϊόν ή άνθρωπο) (Yang & Hancke, 2017, σελ. 355). Στην περίπτωση της ανθρώπινης ταυτοποίησης, για την απόδειξη της ταυτότητας του κατόχου πρέπει να διατίθεται η κατάλληλη πληροφορία ώστε να

[70] Αυτοί χρησιμοποιούν τεχνολογίες που δύνανται να ανιχνεύσουν σειριακούς αριθμούς ή κείμενο μέσω συστημάτων οπτικής αναγνώρισης χαρακτήρων (optical character recognition), μαγνητικές ταινίες, συσκευές ανάγνωσης με ανέπαφες ή μη έξυπνες κάρτες και άλλους αναγνώστες RFID.

[71] Αυτές αποτελούν απλές κάρτες ταυτότητας.

[72] Εν προκειμένω, γίνεται λόγος για κάρτες που χρησιμοποιούν ραδιο-μαγνητικές συχνότητες για την ταυτοποίηση και την αναγνώρισή τους.

[73] Χρησιμοποιούνται από κυβερνητικούς φορείς και μεγάλες εταιρείες όπως *Tesco* και *Walmart.* Η τεχνολογία αυτή χρησιμοποιείται και για ποικίλες άλλες δραστηριότητες όπως σε υπηρεσίες διαχείρισης βιβλιοθηκών, διαδικασιών ανακύκλωσης, ανίχνευσης φαρμακευτικών προϊόντων και αεροπορικώς ταξιδιωτικών αντικειμένων και τοποθέτησής τους κ.λπ.

επιτραπεί στο σύστημα η ταυτοποίηση αυτού. Επομένως, μια κάρτα RFID δύναται να διαθέτει και βιομετρικές πληροφορίες[74].

Σε τρίτο επίπεδο, υπάρχουν οι έξυπνες κάρτες που αποτελούν πιστοποιήσεις με ενσωματωμένο μικροτσίπ και μια επεξεργαστική μονάδα που έχει σχεδιαστεί για να λειτουργεί όταν έρχεται σε επαφή με έναν αναγνώστη. Χρησιμοποιούνται ευρέως ήδη σε πολλές χώρες[75] σε διαδικασίες ψήφου, ανοίγματος τραπεζικού λογαριασμού, αιτήσεων αδειών οδήγησης και άλλες υπηρεσίες (World Bank Group, 2018a). Έχουν σχεδιαστεί τεχνολογίες καρτών που συνδυάζουν τις έξυπνες κάρτες με βιομετρικές πληροφορίες για την καλύτερη ταυτοποίηση όπως και με τις ραδιοσυχνότητες για την επίτευξη της μέγιστης ασφάλειας. Η τρίτη μέθοδος ταυτοποίησης, εκτός των βιομετρικών στοιχείων και των καρτών, είναι η ταυτοποίηση μέσω κινητού τηλεφώνου με την ανάπτυξη διαφόρων τεχνολογιών (βλ. εικόνα).

Εικόνα 8 Οι κατηγορίες τεχνολογιών στις κινητές συσκευές (World Bank Group, 2018a, σελ. 46)

[74] Η τεχνολογία αυτή χρησιμοποιείται κυρίως σε διακυβερνητικό επίπεδο όπως έχει προχωρήσει η Κίνα, για την έκδοση ταξιδιωτικών εγγράφων (e-passports) που μπορούν να αναγνωστούν από ορισμένους αναγνώστες (MRTD), για τραπεζικές υπηρεσίες πληρωμών.
[75] Όπως σε Πακιστάν, Σαουδική Αραβία, Κουβέιτ και Αφρική

Υποκεφάλαιο 3.3 Πρωτόκολλο Blockchain[76] και Ταυτοποίηση

Η τεχνολογία Blockchain αναλύθηκε στο Κεφάλαιο 1. Το ιδιαίτερο πλεονέκτημα του Πρωτοκόλλου για την ταυτοποίηση συνίσταται στο ότι δεν υπάρχει εξάρτηση από κάποιον κεντρικό μηχανισμό και ότι τα προσωπικά στοιχεία δεν μπορούν να αφαιρεθούν. Αυτή η "αυτό-κυρίαρχη" ταυτότητα αναφέρεται ως 'Self-Sovereign Digital Identity' (SSID). Στα συστήματα ταυτοποίησης, χρησιμοποιείται ο μηχανισμός των εξουσιοδοτημένων κατάστιχων[77] μεταξύ των μερών εφόσον αυτή η λογική προσφέρει ταχύτητα στις συναλλαγές και καλύτερη ασφάλεια δεδομένων. Ένα ψηφιακό πορτοφόλι, δηλαδή, ή φάκελος διαθέτει πληροφορίες ταυτότητας ή επιβεβαιωμένα στοιχεία. Ο εκδότης[78] είναι ένας οργανισμός[79] που παρέχει αίτημα με χαρακτηριστικά ταυτοποίησης σχετικά με τον κάτοχο του φακέλου. Ο 'επιβεβαιωτής' (Verifier) είναι μια οντότητα με την οποία ο κάτοχος του φακέλου επιθυμεί να πραγματοποιήσει μια συναλλαγή. Ο κάτοχος 'μοιράζεται έναν αποκεντρωμένο 'ταυτοποιητή' συσχετιζόμενο με το αίτημα του 'επιβεβαιωτήVerifier' ο οποίος μπορεί να επιβεβαιώσει την νομιμότητα του αιτήματος επί της αλυσίδας" (World Bank Group, 2018a). Η εμπιστοσύνη διατηρείται καθ' όλη τη διάρκεια της διαδικασίας χρησιμοποιώντας κρυπτογράφηση δημόσιου και ιδιωτικού κλειδιού ενώ τα ιδιωτικά κλειδιά του κατόχου μένουν αποθηκευμένα και φυλαγμένα στο ψηφιακό πορτοφόλι[80].

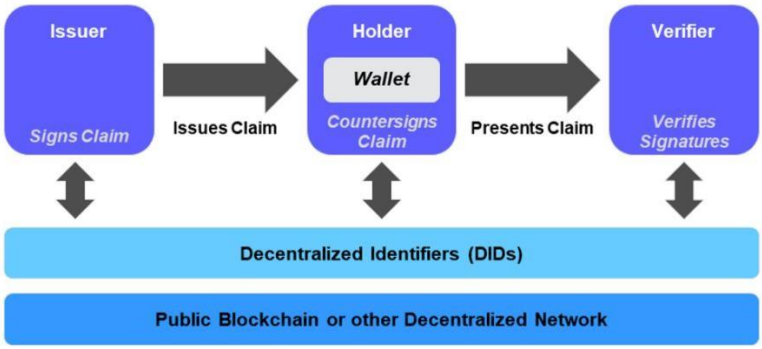
[76] Η ταυτοποίηση δεν εξαρτάται μόνο από την τεχνική μέθοδο αλλά και από το Πρωτόκολλο που χρησιμοποιείται κάθε φορά. Έτσι, έχουν αναπτυχθεί τα εξής πρωτόκολλα ταυτοποίησης : *FIDO Fast Identity Online Universal Authentication Framework* (UAF) που έχει ως στόχο την καταπολέμηση του φαινομένου των πολλών κωδικών (password) στο διαδίκτυο, το *FIDO Universal Second Factor* (U2F) ως μια βελτιωμένη έκδοση του πρώτου ως προς την ευχρηστία και την ασφάλεια, το *OAuth 2.0* για εξουσιοδοτημένη αδειοδότηση εφαρμογών πελατών στο Διαδίκτυο, το *OpenID Connect* για συστήματα πιστοποίησης αυθεντικότητας σε κινητές συσκευές, το *SAML* για χρήση μεταξύ επιχειρηματικών παραγόντων και τέλος, φυσικά, το Πρωτόκολλο Blockchain.

[77] 'Ledgers', όπως αναφέρθηκε στο Κεφάλαιο 1.

[78] 'Issuer', όπως αναφέρεται στην εικόνα.

[79] Η κόμβος-διακομιστής.

[80] Επί της τεχνολογίας αυτής μπορούν να χρησιμοποιηθούν για καθαρά πρακτικούς λόγους και τεχνολογίες ταυτοποίησης μέσω κινητών συσκευών.



Εικόνα 9 Το πλαίσιο εμπιστοσύνης του συστήματος Blockchain (World Bank Group, 2018a, σελ. 66)

Όπως αποδεικνύεται, η ασφάλεια και η ιδιωτικότητα είναι δυο στοιχεία που διασφαλίζονται εν προκειμένω σε πολύ μεγαλύτερο βαθμό από τις υπόλοιπες τεχνολογίες που μελετήθηκαν επί του παρόντος κεφαλαίου. Φυσικά, έχει τις 'τεχνικές' αδυναμίες του: λ.χ., εάν ένας χρήστης χάσει τους κωδικούς δεν υπάρχει κάποιος κεντρικός διακομιστής με τον οποίο να πραγματοποιηθεί ανάδραση με στόχο την επίλυση του προβλήματος. Επίσης, σε επίπεδο πολυπλοκότητας, η δομή του συστήματος δεν εγγυάται πως ένας χρήστης δεν θα είναι κάτοχος περισσότερων κλειδιών. Και πάλι το ζήτημα είναι η ιδιωτικότητα, καθώς το δικαίωμα να μπορεί κάποιος να 'ξεχαστεί' δεν διασφαλίζεται από τη στιγμή που τα δεδομένα είναι αναλλοίωτα στην αλυσίδα. Για το λόγο αυτό πολλοί πιστεύουν ότι "σε μια αλυσίδα ποτέ δεν θα πρέπει να αποθηκευτούν βιομετρικές πληροφορίες ή αμιγώς προσωποποιημένα δεδομένα" (World Bank Group, 2018a, σελ. 67). Αν και η τεχνολογία δεν αναπτύχθηκε με σκοπό την ηλεκτρονική ταυτοποίηση, η πρακτική έχει στραφεί προς αυτήν την κατεύθυνση, και δη προς τον σχεδιασμό αυτού που σημειώθηκε προηγουμένως ως 'αυτο-κυρίαρχη ταυτότητα' (SSID) (World Bank Group, 2018b). Αυτή παρουσιάζεται ως μια υπηρεσία προς ένα άτομο ή οντότητα που θα αξιώνει την ταυτότητά του χωρίς την παρέμβαση κάποιου τρίτου παράγοντα. Βέβαια, η εγκυρότητα του όρου αμφισβητείται, διότι η αστική ταυτότητα επιβεβαιώνεται από μια εκδοτική εξουσιοδοτημένη αρχή πριν γίνει αντικείμενο διαχείρισης από τον

κάτοχο. Έτσι, γίνεται περισσότερο αναφορά για μια *αυτό-διαχειριζόμενη* ταυτότητα παρά για μια *αυτό-κυρίαρχη* ταυτότητα[81] (World Bank Group, 2018b).

Σύγχρονες πρακτικές της τεχνολογίας περιλαμβάνουν τα εξής πεδία: Σχέδια για έξυπνες πόλεις στο πλαίσιο της ηλεκτρονικής διακυβέρνησης, IoT (Bashir, 2017, σελ. 432), ιστοσελίδες, μέσα κοινωνικής δικτύωσης, τηλεπικοινωνίες, την Βιομηχανία 4.0, την τεχνητή νοημοσύνη, την τηλε-ιατρική, τη κινητή τηλεφωνία, την ηλεκτρονική ψήφο (Noizat, 2015). Επιπροσθέτως, η τεχνολογία χρησιμοποιείται και για συμβολαιογραφικές πράξεις, πιστοποιητικά γέννησης, συμβόλαια [82] όπου τα έγγραφα είναι συνδεδεμένα με την ηλεκτρονική ταυτότητα του μέρους της συναλλαγής για την απόδειξη της ταυτότητάς του (Bashir, 2017, σελ. 432).

Όπως διαφαίνεται, πραγματοποιείται ήδη σε πολλές χώρες του κόσμου ο σχεδιασμός και ο προγραμματισμός της χρήσης της τεχνολογίας Blockchain για την ηλεκτρονική ταυτοποίηση[83].

Υποκεφάλαιο 3.4 Θετικά στοιχεία της ταυτοποίησης

Με την ταυτοποίηση οι πολίτες του κόσμου μπορούν πλέον να ασκούν τα πολιτικά τους δικαιώματα, να διενεργούν συναλλαγές στο πλαίσιο των σχέσεων μεταξύ πολιτών και κρατικών μηχανισμών και να έχουν την πρόσβαση σε πληθώρα άλλων υπηρεσιών. Αυτό είναι δυνατό χάρη στην ηλεκτρονική ταυτοποίηση η οποία διαθέτει πολλά πλεονεκτήματα και παράλληλα λύνει προβλήματα κοινωνικού, οικονομικού και διοικητικού περιεχομένου.

Αρχικά, εξασφαλίζεται η ταχύτητα σε ό,τι αφορά τα επίπεδα της ταυτοποίησης (Matching). Πλέον δε χρειάζεται το 'χαρτί' για να ταυτοποιηθεί ένα άτομο αλλά συνήθως μια απλή κάρτα. Αυτό αναδεικνύει τον οικολογικό χαρακτήρα της πρωτοβουλίας. Έπειτα, η τεχνολογία βρίσκεται σε αρκετά υψηλό επίπεδο σε ό,τι

[81] '*Self-managed'* παρά '*self-sovereign'* ID ταυτότητα.
[82] Εφαρμογές που πραγματοποιούνται ήδη στην Κίνα.
[83] Βλ. Παράρτημα Α για ορισμένα μελλοντικά παραδείγματα που ίσως αποτελέσουν και μελέτες περίπτωσης στο προσεχές μέλλον.

αφορά τα τεχνικά της χαρακτηριστικά. Η τεχνολογία είναι αρκετά ώριμη και εξελιγμένη καθιστώντας την κατάλληλη για διακυβερνητική και διασυνοριακή χρήση (World Bank Group, 2018a). Ειδικά, το δαχτυλικό αποτύπωμα ως βιομετρικό στοιχείο είναι ένα από τα λιγότερο δαπανηρά μέσα ταυτοποίησης εξασφαλίζοντας ταυτόχρονα και αποτελεσματικότητα. Το γεγονός ότι η βιομετρική πληροφορία δύναται να εισχωρήσει σε ηλεκτρονικές κάρτες δίνει ένα ασύγκριτο πλεονέκτημα.

Στον κοινωνικο-πολιτικό τομέα, περιορίζεται ο οικονομικός αποκλεισμός. Ήδη, σε αναπτυσσόμενες χώρες, λιγότερο του μισού των ενηλίκων διαθέτει τραπεζικό λογαριασμό. Επιπροσθέτως, διασφαλίζεται η ισότητα των φύλων καθώς ο "γυναικείος πληθυσμός κατά πάσα πιθανότητα τις περισσότερες φορές δεν έχει πρόσβαση στην προσωπική ταυτοποίηση σε αντίθεση με τον ανδρικό πληθυσμό" (Dahan & Hanmer, χ.η., σελ. 8). Ως αποτέλεσμα αυτού, οι γυναίκες δεν μπορούν να ασκήσουν όχι μόνο πολιτικά δικαιώματα αλλά και καθημερινές αστικές πράξεις σε περιουσιακά στοιχεία όπως ακίνητα. Με την ηλεκτρονική ταυτοποίηση, ενδυναμώνονται τόσο οι γυναίκες όσο και τα παιδιά αποκτώντας πρόσβαση στις κοινωνικο-οικονομικο-πολιτικές διαδικασίες (Dahan & Hanmer, χ.η.). Το επόμενο πλεονέκτημα χαρίζει πρόσβαση σε υπηρεσίες πρόνοιας. Για την παροχή από τα κράτη υπηρεσιών ιατρικής περίθαλψης, ασφάλισης και συνολικότερης κάλυψης θα πρέπει οι εκάστοτε κεντρικές αρχές να έχουν προχωρήσει στη ταυτοποίηση των πολιτών τους. Εκτός αυτού, η ηλεκτρονική ταυτοποίηση θα αναλαμβάνει και τον ρόλο της πρόληψης ιατρικών ασθενειών ή γεγονότων ανιχνεύοντας ενδεχόμενα ιατρικά στοιχεία. Οι πιθανότητες απάτης ελαχιστοποιούνται και παράλληλα διευκολύνονται οι σχέσεις μεταξύ ασθενή και ιατρικής υπηρεσίας. Επίσης, το ανθρωπιστικό έργο και τα κοινωνικά δίκτυα θα αναπτυχθούν και θα εξελιχθούν ραγδαία και αποτελεσματικότερα. Σε κυβερνητικό επίπεδο, όπως έχει ήδη τονιστεί, τα θετικά περιλαμβάνουν αξιοπιστία, διαφάνεια και αποτελεσματικότητα. Η ταυτοποίηση δίνει επίσης τη λύση στον επιχειρηματικο-εργατικό τομέα με προτάσεις ταυτοποίησης και αδειοδότησης (Mansfield-Devine, 2015). Ειδικά, η τεχνολογία RFID όταν συνδυάζεται με καλή ενδο-επιχειρηματική διαχείριση, αυξάνει τα επίπεδα των υπηρεσιών των

πελατών, της παραγωγικότητας και της διαχείρισης προϊόντων (Reyes, Li & Visich, 2016, σελ. 11).

Αξιοσημείωτη είναι η ταυτοποίηση στο πλαίσιο της μετανάστευσης. Η ενάσκηση των δικαιωμάτων ασύλου και προστασίας είτε στη χώρα που φιλοξενεί είτε κατά τη διάρκεια της μετακίνησης καθίσταται σχεδόν αδύνατη χωρίς στοιχεία ταυτότητας (Manby, 2016). Παρομοίως, η ταυτοποίηση και η πιστοποίηση θα λύσουν το κοινωνικό πρόβλημα των γάμων με ανήλικα παιδιά δίνοντάς τους όχι μόνο νομική προστασία αλλά και ανιχνεύοντας ενδεχόμενες παρανομίες στο πλαίσιο των εκάστοτε ορίων ηλικίας (Hanmer & Elefante, 2016).

Υποκεφάλαιο 3.5 Αρνητικά ζητήματα της ταυτοποίησης

Φυσικά, τα προβλήματα δεν απουσιάζουν. Εκτός από τις ψυχο-φιλοσοφικές θεωρίες περί της ταύτισης του ανθρώπινου προσώπου με έναν αριθμό (Capurro et al., 2013) και τους γενικότερους προβληματισμούς γύρω από τη διαδικτυακή λογική, στον πρακτικό τομέα γεννιούνται ορισμένα ερωτήματα.

Αρχικά, υπάρχει περίπτωση τα βιομετρικά στοιχεία να είναι αδύνατον να αναγνωστούν από τις συσκευές ανάγνωσης λόγω φυσικών ανωμαλιών όπως: καταστροφή της επιδερμικής επιφάνειας (Labati, Genovese, Piuri & Scotti, 2014), μεταβολές στην ίριδα ή ακόμα και λόγω της μικρής ηλικίας ενός παιδιού όπου τα φυσικά στοιχεία ταυτοποίησης δεν έχουν ακόμα αναπτυχθεί. Να σημειωθεί ότι η βιομετρική πληροφορία από μόνη της δεν μπορεί να επιτύχει τον στόχο της ταυτοποίησης αν δεν συνδυαστεί και με άλλες πληροφορίες (Laurent & Bouzefrane, 2015). Άλλο πρόβλημα παρουσιάζεται στην αποδοχή από το κοινό τέτοιων τεχνολογιών συνήθως λόγω του ανθυγιεινού χαρακτήρα ή του βαθμού ιδιωτικότητας που παρέχουν (World Bank Group, 2018a), πράγμα που οδηγεί κατ' επέκταση στην γενικότερη αμφισβήτηση της ηλεκτρονικής ταυτοποίησης.

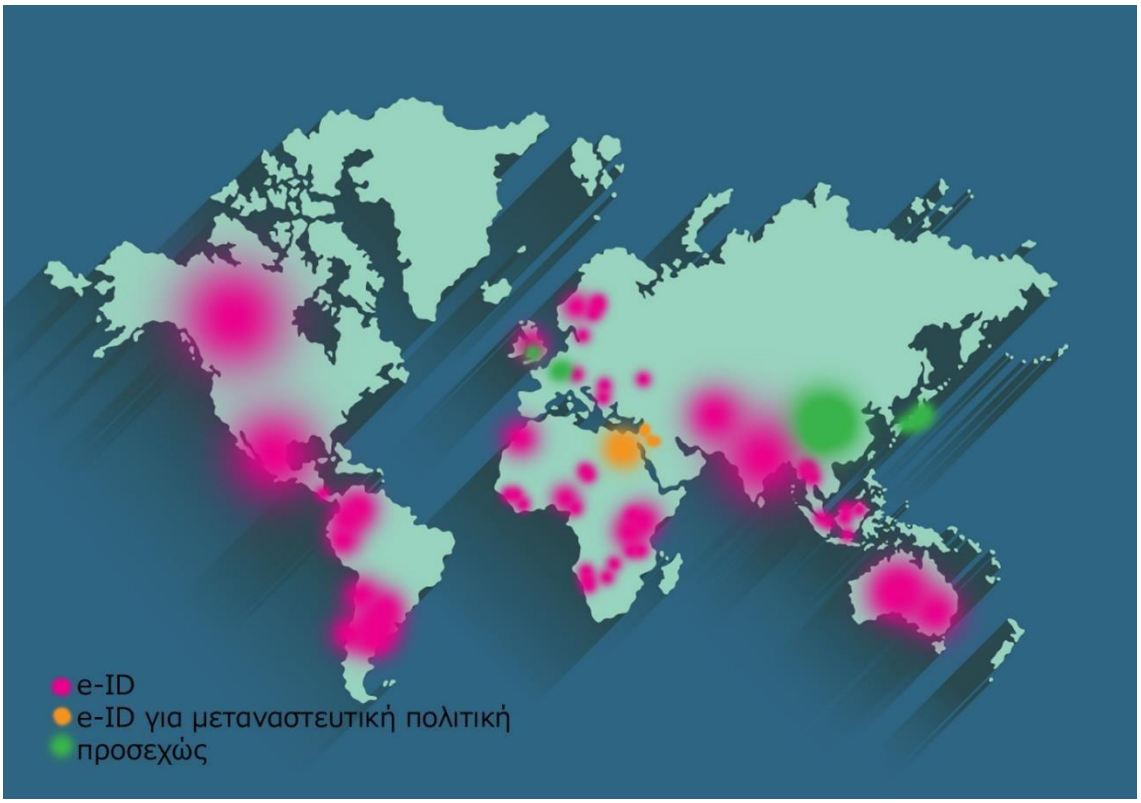
Επίσης, το κόστος αποτελεί αρκετά μεγάλο ζήτημα καθώς λειτουργεί τις περισσότερες φορές ως "φρένο". Σε κάθε περίπτωση, η έρευνα βρίσκεται ακόμη σε πειραματικό και δοκιμαστικό στάδιο και ως εκ τούτου τα πραγματικά αποτελέσματα δεν έχουν

ακόμα φανεί εν συνόλω. Γι' αυτό εξάλλου και στο ερώτημα εάν η ηλεκτρονική ταυτοποίηση θα λύσει το πρόβλημα των ανθρωπιστικών βοηθειών η απάντηση είναι «όχι, όχι ακόμα» (Twelves, χ.η.). Επίσης, τις περισσότερες φορές συστήματα ταυτοποίησης μέσω κινητών συσκευών λαμβάνουν ως δεδομένη την κατάσταση οι πολίτες να κάνουν χρήση των κινητών τηλεφώνων γεγονός που πολλές φορές δεν απαντά στην πραγματικότητα (World Bank Group, 2018a, σελ. 56). Να προστεθεί ότι θα υπάρξουν ζητήματα μεγάλης χωρητικότητας δεδομένων και κατά συνέπεια αρνητικά θέματα σε ταχύτητα και αποτελεσματικότητα των συσκευών (Jiang & Meng, 2017, σελ. 165-166).

Εν τέλει, το ζήτημα παραμένει πάντα το ίδιο: η ιδιωτικότητα. Ο πολίτης ποτέ δεν μπορεί να είναι σίγουρος για το πού αποθηκεύονται τα συλλεγόμενα δεδομένα και το πού χρησιμοποιούνται. Εξάλλου, και από τεχνικής πλευράς, το αξιακό πρόταγμα του δικαιώματος στη λήθη δεν διασφαλίζεται. Έρευνες έχουν φέρει στο φως ζητήματα ασφαλείας των βιομετρικών στοιχείων (Ring, 2015) και ζητήματα μεταξύ αυτών και της τεχνολογίας RFID, ειδικά σε ό,τι αφορά την εγκαθίδρυση μιας ευρείας δομής παρακολούθησης των ανθρώπων, γεγονός που θέτει σε κίνδυνο και τα αστικά δικαιώματα (Laurent & Bouzefrane, 2015). Θυμίζουμε πως οι κάρτες RFID με τσιπ μπορούν να αναγνωστούν ακόμη και από απόσταση από εξειδικευμένους αναγνώστες.

Σε αυτό το πλαίσιο, η ανάπτυξη τέτοιων συστημάτων για τον σχεδιασμό των λεγόμενων 'έξυπνων πόλεων' διαθέτει ακόμη πολλά σημεία που χρήζουν επίλυσης (Curzona, Almehmadi & El-Khatib, 2019).

Κεφάλαιο 4. Ταυτοποίηση για ανάπτυξη[84] – Μελέτες Περίπτωσης



Εικόνα 10 Δημιουργήθηκε με Photoshop CS2[85]

Υποκεφάλαιο 4.1 Αναπτυσσόμενες χώρες

[84] Η πρωτοβουλία του World Bank Group Identification for Development (ID4D) κάνει πραγματικότητα σε παγκόσμια κλίμακα την εφαρμογή της ταυτοποίησης για ανάπτυξη με διεθνείς πρακτικές με στόχο την κοινωνική ανέλιξη, την υγεία, την καλύτερη πρόσβαση σε αγαθά και υπηρεσίες και την αποτελεσματικότητα στις σχέσεις κράτους-πολίτη. Η πρωτοβουλία είναι δυνατή χάρη στις προσπάθειες των εξής φορέων: *World Bank Group, Bill & Melinda Gates Foundation, Omidyar Network* και την Κυβέρνηση της Αυστραλίας.

[85] Βλ. Παράρτημα Γ για τις αναπαριστώμενες χώρες.

4.1.1 Ινδία

Ως απάντηση στην ανεξέλεγκτη διαφθορά και την απάτη, η κυβέρνηση της Ινδίας παρουσίασε το 2016 το σύστημα *Aadhaar*, το μεγαλύτερο πρόγραμμα βιομετρικής ψηφιακής ταυτοποίησης του κόσμου (Nilekani, 2018). Η κυβέρνηση με αυτόν τον τρόπο επιθυμεί να αυξήσει την οικονομική και κοινωνική ένταξη μέσω ενός οικοσυστήματος που ονομάζεται *JAM Trinity* που εντάσσει *Unique Digital Ids* και τραπεζικούς λογαριασμούς χρησιμοποιώντας και κινητές συσκευές. Τεχνικά, το *Aadhaar* είναι ένας 12-ψήφιος τυχαίος αριθμός (Nilekani, 2018) που εκδίδεται από τον κυβερνητικό μηχανισμό *UIDAI* (Unique Identification Authority of India) με στόχο την εξάλειψη της απάτης και την δυνατότητα ταυτοποίησης και επιβεβαίωσης με χαμηλό κόστος. Η τεχνολογία χρησιμοποιεί δημογραφικά στοιχεία όπως όνομα, διεύθυνση, ημερομηνία γέννησης, φύλο, μαζί με βιομετρικά δεδομένα: 10 δαχτυλικά αποτυπώματα, δυο φωτογραφίες ίριδας, ψηφιακή φωτογραφία προσώπου. Τα τελευταία συλλέγονται με σαρωτές δαχτυλικών αποτυπωμάτων, σαρωτές ίριδας και κάμερες για αναγνώριση προσώπου (World Bank Group, 2018c). Όλη η ταυτοποίηση, επομένως, γίνεται μέσω των βιομετρικών στοιχείων.

Πίνακας 6 Το 'Aadhaar' στις καθημερινές συναλλαγές (συλλογή στοιχείων από World Bank Group, 2018c)

1.20 δις Αριθμοί *Aadhaar*
339 εκατ. *Aadhaar* αριθμοί συνδέθηκαν με τραπεζικούς λογαριασμούς
1.7 δις ταυτοποιήσεις έγιναν με *Aadhaar* τα τελευταία 3 χρόνια
Οι συνολικές ψηφιακές συναλλαγές άγγιξαν τα 17.57 δις το 2017-18, 70 % περισσότερο από το προηγούμενο έτος 2016-2017
4.9 δις συναλλαγές 'e-KYC transactions' πραγματοποιήθηκαν με *Aadhaar*

Το σύστημα *Aadhaar* [86] συνοδεύτηκε από την ηλεκτρονική υπηρεσία e-KYC επιταχύνοντας την επιβεβαίωση ταυτότητας ενός πελάτη. Η μέθοδος αυτή επιτρέπει στον κάτοχο της ταυτότητας και του αριθμού να ενεργοποιήσει υπηρεσίες όπως κινητή τηλεφωνία, τραπεζικούς λογαριασμούς κ.λπ. Τα δεδομένα της κάρτας επικοινωνούνται άμεσα μόνο με τη συγκατάθεση του πελάτη εξασφαλίζοντας την ιδιωτικότητα. Οι πολίτες μπορούν να χρησιμοποιήσουν το σύστημα για να ανοίξουν τραπεζικούς λογαριασμούς, να αγοράσουν sim κάρτες, να δεχθούν επιστροφές από την κυβέρνηση, να υπογράφουν αιτήσεις ηλεκτρονικά, να επενδύουν σε αμοιβαία κεφάλαια, να λαμβάνουν πιστώσεις και άλλες ενέργειες και υπηρεσίες.

Η πρακτική αυτή θα φέρει την επανάσταση εντός του τραπεζικού συστήματος, με τα έγγραφα μητρώα KYC να ελαχιστοποιούνται δίνοντας χώρο σε μια νέα χρηματοπιστωτική οντότητα, και στις σχέσεις με τους πολίτες-πελάτες μέσω των διατραπεζικών πληρωμών. Το σύστημα συνεπικουρείται από το πρόγραμμα *Bharat Interface for Money* (BHIM) για αμεσότητα και ταχύτητα στις τραπεζικές συναλλαγές (World Bank Group, 2018c).

Πίνακας 7 Οι τραπεζικές συναλλαγές στην Ινδία μέσω του BHIM συστήματος (συλλογή στοιχείων από World Bank Group, 2018c)

BHIM αποθηκεύτηκε σε ηλεκτρονικές συσκευές 23.8 εκατ. φορές από τον Δεκέμβριο 2016
Από τις αρχές του 2018 ο αριθμός των συναλλαγών στο BHIM-UPI ξεπέρασε σε αξία το 1 δις δολάρια

Πολλοί μιλούν για το καλύτερο σύστημα στον κόσμο που συνδυάζει δημογραφικά στοιχεία και βιομετρικά δεδομένα. Βέβαια, και πάλι τα ερωτήματα περί της ιδιωτικότητας δεν λείπουν (Nilekani, 2018). Η αλλαγή αυτή στις ηλεκτρονικές ταυτότητες ήρθε σε μια εποχή όπου νόμος στην Ινδία για τα προσωπικά δεδομένα και τα δικαιώματα και τις υποχρεώσεις των εμπλεκομένων δεν είχε τεθεί ακόμα σε ισχύ. Έχουν ήδη φτάσει σχετικές υποθέσεις στο Ανώτατο Δικαστήριο και το σίγουρο

[86] Στα αγγλικά αποδίδεται με τον όρο '*Foundation*'.

είναι πως η κυβέρνηση οφείλει να ενημερώσει τους πολίτες για τα ζητήματα και τα δικαιώματά τους (Nilekani, 2018). Ο προβληματισμός είναι ο ίδιος ο αριθμός, που δίνει ίσως υπέρμετρες δυνατότητες στο κράτος για παρακολούθηση σε πληθώρα πεδίων. Παρά ταύτα, πρόσφατη έρευνα[87] στο πεδίο της ιδιωτικότητας έχει φέρει στο φως σημαντικά στοιχεία για μελέτη. Ενδεικτικά παραθέτουμε τους παράγοντες της ελαχιστοποίησης των δεδομένων, της ασφάλειας και της συγκατάθεσης.

[87] Βλ. Πίνακα 13 (Παράρτημα Δ) για τα ολοκληρωμένα αποτελέσματα.

Πίνακας 8 Ο περιορισμός των συλλεγόμενων δεδομένων, η ασφάλεια και η συγκατάθεση στο ινδικό μοντέλο. Οι πίνακες προέρχονται από τη μελέτη 'Privacy by Design: Current Practices in Estonia, India, and Austria' (World Bank Group, 2018c, σελ. 8-11)

Data minimization	**Zero Semantics UIN**—The UIN (Aadhaar number) is a **random number** and does not on its own convey any meaning/information about the user. Linking of data across various systems/databases up until early 2018 was based on the Aadhaar number. In the light of increasing privacy and surveillance concerns, UIDAI recently launched the **virtual ID and tokenization features** discussed further in Box 1. • With the **tokenization** feature, instead of a UIN, a token which is calculated based on service provider code and Aadhaar number is used to identify the user in the service provider database, thus avoiding linkability of data across databases. • A **virtual ID** is a temporary ID number mapped to the UIN, that can be generated and used by a user instead of exposing the Aadhaar number. **Fingerprint and iris data are never shared.** **UIDAI certified biometric devices** used by service providers for authentication encrypt **the biometric** data captured from the user in the device itself before it reaches the service provider system, thus securing it. Data, when used for analytics purposes, are **anonymized** before sharing.
Security	The digital signature on the electronic Aadhaar ensures integrity and authenticity of the electronic Aadhaar document—enabling detection of any forgery of the Aadhaar document. This security feature enables it to be used for offline authentication and identity verification with a higher level of assurance. The Aadhaar also has two digitally signed Quick Response (QR) codes, one with photograph and demographic data and the other with demographic data only. The QR code, in both electronic Aadhaar or printed Aadhaar document, can be used for electronic capture of demographic data during offline KYC/authentication. The QR code prevents the data to be read visually without a QR code reader and the digital signature validation of the QR code enables detection of fake /forged Aadhaar's. All the data are **encrypted** and **digitally signed** and transmitted over a secure communication channel when sharing data between systems. Data is stored in **encrypted f**ormat and not exposed/available even for admin user or other type of user in plain text format The transaction logs are time stamped and digitally signed making them **tamper proof.** Any change would make the digital signature invalid. Users and systems are **authenticated and authorization** rules enforced before providing access to services (API's) or administrative functions. **Data tampering** is prevented by ensuring that data updates can only be done by authorized applications and not through command line queries/scripts. **Data is partitioned** and held in multiple database systems, with a random alias being the only link, which ensures that there is no centralised data table where all resident data is available. Access to the API's and hence to the CIDR is through a **network of trusted service providers (AUA and ASA)** only. Users can **lock/unlock** the use of **biometrics** to disable/enable biometric-based authentication.
Consent	User **authentication** while accessing a service serves as consent to the service provider to access data from Aadhaar. Only trusted registered services (AUA/KUA) can access the Aadhaar system API's and can access it only through a trusted secure network of service agencies (ASA). User consent is captured during registration for digital ID on paper forms.

4.1.2 Ουγκάντα: Η ηλεκτρονική ταυτοποίηση για τη μεταναστατευτική πολιτική

Η Ουγκάντα, όπως και η Ιορδανία, το Λίβανο και η Αίγυπτος, αποτελεί ένα ισχυρό μεταναστευτικό κέντρο λόγω του πολέμου στη Συρία. Το τμήμα εγγραφής και ταυτοποίησης μεταναστών φιλοξενεί πάνω από ένα εκατομμύριο μετανάστες προερχόμενους κυρίως από το Νότιο Σουδάν και το *DRC*[88].

Η Ουγκάντα είναι μέλος της Μεταναστευτικής Συμφωνίας του 1951 και αναγνωρίζεται ως ένα από τα πιο φιλόξενα κράτη για μετανάστες στον κόσμο. Η κυβέρνηση παρέχει ελευθερία διακίνησης, πρόσβαση σε υπηρεσίες και παρέχει κομμάτια γης για στέγαση και αγροτικές καλλιέργειες.

Το 2014, το *Office of the Prime Minister*[89] εισήγαγε το δικό του σύστημα : το *Refugee Information Management System* (RIMS). Το RIMS αποτελεί ένα σύστημα βασισμένο στην επιγραμμική σύνδεση που περιλαμβάνει την εγγραφή, την καταχώρηση βιομετρικής πληροφορίας, τη διαχείριση των στοιχείων και την παραγωγή-έκδοση καρτών. Το σύστημα αποθηκεύει δυο δαχτυλικά αποτυπώματα, δεν διενεργεί αυτό που ονομάζεται βιομετρική *deduplication* ή *authentication* και δεν είναι συμβατή με την εθνική ταυτότητα της χώρας που εκδίδεται από την Εθνική Αρχή *NIRA (*National Identification and Registration Agency) (World Bank Group, 2018b, σελ. 53). Η Αρχή *NIRA*, βέβαια, παρέχει υπηρεσίες πολιτικής εγγραφής σε μετανάστες και αιτούντες άσυλο. Η κυβέρνηση βρίσκεται στη διαδικασία να ταυτοποιήσει περίπου πάνω από ένα εκατομμύριο μετανάστες με το σύστημα RIMS. Η κάρτα *refugee ID card* και τα ανάλογα πιστοποιητικά που εκδίδονται είναι ευρέως αναγνωρισμένα και επιτρέπουν την πρόσβαση σε όλες τις υπηρεσίες στις οποίες ένας μη-κάτοικος έχει δικαίωμα. Στόχος είναι η εγγραφή για την παροχή υπηρεσιών και την απαιτούμενη υποστήριξη. Το 2017, όταν η κυβέρνηση προχώρησε σε υποχρεωτική σύνδεση της κάρτας SIM με

[88] *Danish Refugee Council:* Το Δανέζικο Συμβούλιο Προσφύγων για την φιλανθρωπική υποστήριξη και τη βοήθεια προς τους μετανάστες ιδρύθηκε στη Δανία το 1956 κι έκτοτε πραγματοποιεί διεθνές έργο.
[89] Δηλαδή, ο Πρωθυπουργός της εν λόγω χώρας

τον αριθμό της εθνικής ταυτότητας ID, εισήχθη ο αριθμός της ταυτότητας *refugee ID*. Έτσι, η κάρτα αυτή χρησιμοποιείται και για το άνοιγμα ενός τραπεζικού λογαριασμού.

Γενικότερα, η κάρτα αυτή δίνει τη δυνατότητα σε μετανάστες να έχουν πρόσβαση σε πληθώρα δράσεων σχεδιασμένων και προγραμματισμένων αποκλειστικά για εκείνους συμπεριλαμβανομένων υπηρεσιών εκπαίδευσης και ιατρικής περίθαλψης. Η κυβέρνηση χρησιμοποιεί το λογισμικό της UNHCR's βιομετρικής εγγραφής, το οποίο έχει ήδη τεθεί σε εφαρμογή για την εγγραφή μεταναστών από 48 χώρες παγκοσμίως (Bond, 2018). Η πρωτοβουλία αυτή στην Ουγκάντα αποτελεί την ευρύτερη στον πλανήτη.

Όπως έχει ήδη γίνει αναφορά αρκετές φορές από ειδικούς και διάφορους παράγοντες, οι προκλήσεις στο πεδίο της εγκατάστασης του συστήματος είναι αρκετές. Ωστόσο, η προοδευτική πολιτική της Ουγκάντα, η πρακτική της να δοθεί ταυτότητα σε μετανάστες και αιτούντες άσυλο και η διασφάλιση ότι αυτές η ταυτότητες αναγνωρίζονται ευρέως συνιστούν άξιες πρωτοβουλίες (World Bank Group, 2018b, σελ. 53).

Υποκεφάλαιο 4.2 Ανεπτυγμένες χώρες

4.2.1 Εσθονία

Η Εσθονία αποτελεί ένα πολύ ιδιαίτερο παράδειγμα. Η χώρα φιλοξενεί μόλις 1,3 κατοίκους και είναι μια από τις περισσότερο ψηφιακά ενταγμένες χώρες στον κόσμο. Ο μηχανισμός της ηλεκτρονικής διακυβέρνησης της Εσθονίας δομείται από ένα υψηλής εμπιστευτικότητας σύστημα διευρυμένο στις περισσότερες υπηρεσίες μεταξύ πολιτών και κράτους[90].

[90] Το νομικό οικοσύστημα, σε ό,τι αφορά την ιδιωτικότητα, θεμελιώνεται από το εθνικό Σύνταγμα και από το νόμο περί προστασίας των προσωπικών δεδομένων. Σε διοικητικό επίπεδο, υπάρχει η Αρχή Προστασίας Δεδομένων από το 1999 και η Αρχή Πληροφοριακών Συστημάτων. Νομοθετικά καθορίζονται οι προϋποθέσεις πρόσβασης στην ιδιωτική πληροφορία, στις βάσεις δεδομένων και στο μηχανισμό διαχείρισης της κρατικής και διοικητικής πρόσβασης στα δεδομένα. Επίσης,

Τρία συστήματα συγκροτούν τον μηχανισμό της ηλεκτρονικής διακυβέρνησης: η εσθονική ψηφιακή ταυτότητα, το σύστημα 'X-Road' και το 'RIHA'. Η ψηφιακή ταυτότητα είναι το κλειδί πρόσβασης σε όλες τις ιδιωτικές και δημόσιες υπηρεσίες είτε μιλάμε για ψηφιακή κάρτα είτε για ταυτότητα συνδεδεμένη σε συσκευή κινητής τηλεφωνίας ή σε κινητές συσκευές εν γένει με ειδική ταυτοποίηση SIM (Mobile ID) είτε για ταυτοποίηση μέσω της εφαρμογής *smart-ID7* που μπορεί να ενεργοποιηθεί από Android και iOS λογισμικό (Smart ID) (World Bank Group, 2018c). Και στις τρεις περιπτώσεις το κάθε διαπιστευτήριο έχει δυο ψηφιακά πιστοποιητικά: μια για ταυτοποίηση και μια για ψηφιακή υπογραφή εγγράφων ενώ και οι δυο καταστάσεις ενεργοποιούνται με έναν PIN αριθμό. Όλοι οι πολίτες άνω των 15 υποχρεώνονται να έχουν ένα από τα τρία είδη ταυτοποίησης (World Bank Group, 2018c, σελ. 7).

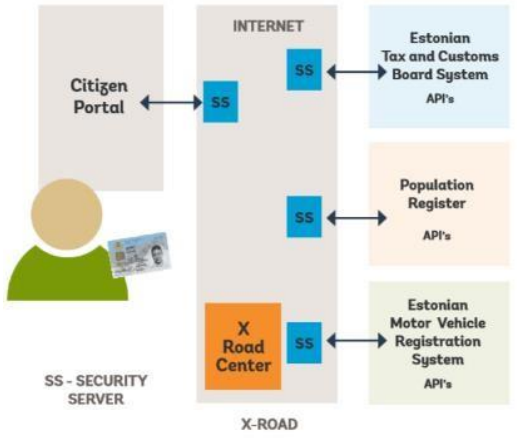
Το σύστημα X-Road διασφαλίζει την μεταφορά των δεδομένων ταυτοποίησης από και προς διαφορετικές βάσεις δεδομένων για τις ανάγκες των υπηρεσιών[91]. Το RIHA αποτελεί το διοικητικό σύστημα για την κρατική υποδομή πληροφοριών της Εσθονίας και κατά κάποιον τρόπο τον κατάλογο για τις βάσεις δεδομένων του Κράτους[92] (World Bank Group, 2018c, σελ. 8).

κατοχυρώνονται το δικαίωμα στο απαράβατο της ιδιωτικής και οικογενειακής ζωής σε ό,τι αφορά τη χρήση προσωπικών δεδομένων και το δικαίωμα πρόσβασης στην προσωπική πληροφορία.

[91] Η μεταφορά γίνεται μέσω του Unique Identification Number (UIN).

[92] Μεταξύ άλλων συγκρατούνται και καταχωρούνται πληροφοριακά συστήματα, βάσεις δεδομένων και στοιχεία που επεξεργάζονται σε συλλέγονται σε αυτά, υπηρεσίες και λίστα χρηστών, νομικές βάσεις και πιστοποιήσεις των διαδικασιών και της επεξεργασίας των βάσεων δεδομένων.

Πίνακας 9 Η αρχιτεκτονική του εσθονικού μοντέλου. Η φωτογραφία προέρχεται από την έρευνητική μελέτη 'Privacy by Design: Current Practices in Estonia, India, and Austria' (World Bank Group, 2018c, σελ. 13)



1. A user wanting to use an online service "XYZ" of Department "ABC" authenticates their identity by using the citizen portal using their digital ID (smart card or mobile ID). (Single sign -on solution enables the user to request service from any department seamlessly.)
2. Using X-Road, the service being accessed itself obtains the data needed to process the service request from other databases.
3. The Security Server component of the requesting system encrypts the data and sends it to the system (database) from which data are desired over the Internet.
4. The security server at the data provider system end authenticates the requesting system, and if the authorization check succeeds, forwards the request to the system.
5. The security server time stamps, digitally signs, and logs the transaction and sends an encrypted response, provided by, the data provider system to the requestor system.
6. The security server decrypts the response, and then the service processes the request based on data fetched in real-time and returns the response to the user.

Παρακάτω (Πίνακας 10) παρατίθενται τα στοιχεία του περιορισμού των δεδομένων, της ασφάλειας και της αδειοδότησης από το χρήστη στο εσθονικό μοντέλο. Υπάρχει ένας 11ψήφιος αριθμός, το φύλο και η ημερομηνία γέννησης. Τα δεδομένα είναι κρυπτογραφημένα και υπογεγραμμένα ηλεκτρονικά και παράλληλα το σύστημα ενισχύεται από το Πρωτόκολλο Blockchain για την επιτυχία στην ασφάλεια των συναλλαγών με χρήση του συστήματος κρυπτογράφησης hashing[93] (World Bank Group, 2018c). Το εσθονικό μοντέλο έτσι αναπτύσσει ένα πρωτοπόρο σύστημα ηλεκτρονικής υγείας και δίνει νέο νόημα στην έννοια της ιδιωτικότητας με τον χρήστη-πολίτη να είναι πάντα ενήμερος για την οποιαδήποτε χρήση των δεδομένων του από την κυβέρνηση.

[93] Βλ. Κεφάλαιο 1.1

Πίνακας 10 Ο περιορισμός των δεδομένων, η ασφάλεια και η συγκατάθεση στο εσθονικό σύστημα ταυτοποίησης. Από την ερευνητική μελέτη 'Privacy by Design: Current Practices in Estonia, India, and Austria' (World Bank Group, 2018c, σελ. 14-16)

Data minimization	• **UIN (Universal Identification Number)** an 11-digit number, referred to as a **Personal Identification Code in Estonia**, consists of gender, century of birth, date of birth, serial number separating persons born on a same date, and a checksum. It is simple, both from technical design (easy to generate) and usability perspective (easy to remember), but it does **reveal gender and date of birth** information of the individual. This is in contrast to random number UINs adopted by other countries. • **Link**—The data of a citizen is **linked** across systems/**databases through UIN** which provides complete 360 views of the user. Estonia has leveraged this knowledge for efficiencies in service delivery with due regard to user privacy and data protection. The privacy and data protection risks are mitigated through strong technology-enabled checks and controls, and a strong regulatory environment.
Security	• All the data are **encrypted** and **digitally signed** and transmitted over a secure communication channel when sharing data between systems. • The transaction logs are time stamped and digitally signed making them **tamper proof.** Any change would make the digital signature invalid. • The logs are **hash chained** to further enhance the immutability of the logs and make changing logs at a later date an extremely tedious and difficult task. • **Block chain technology** has also been deployed for enhancing the integrity of transaction logs. The log is pseudonymized to protect privacy but can trace the user in the event a transaction is contested. • As the authentication holds the key to all data of the user, strong **multi-factor authentication** using the smart card with digital certificates (something you have) + PIN (something you know) ensures that someone else cannot impersonate you. • The **machine to machine interaction** involving data access by one system from another system or user-initiated data access is allowed only after **authentication and authorization** of systems using digital certificates and access rules (done by the security servers of X-Road).
Consent	• User **authentication** while accessing a service serves as consent to the service provider to access data from other databases. • The authentication and transaction logs at each system are time stamped to match the consent of the user with data access.

Η ψηφιακή ταυτότητα [94] διαθέτει τσιπ (chip) με ενσωματωμένα αρχεία και, χρησιμοποιώντας μια κρυπτογράφηση των 2048-bit με δημόσιο κλειδί, δύναται να αξιοποιηθεί για την ταυτοποίηση σε ψηφιακό περιβάλλον. Οι εφαρμογές της e-ID περιλαμβάνουν εν γένει την ταυτοποίηση, τις ηλεκτρονικές υπογραφές και την

[94] Το εσθονικό σύστημα, σύμφωνα με τα δεδομένα του επίσημου φορέα, έχει εκδώσει ψηφιακές ταυτότητες για το 98% των πολιτών και παράλληλα έχει υποβοηθήσει στην πραγματοποίηση πάνω από 500 εκατομμύρια ψηφιακές υπογραφές Να σημειωθεί ότι στη χώρα 88% των πολιτών χρησιμοποιούν το Διαδίκτυο.

κρυπτογράφηση. Ειδικά για την τελευταία, στόχος είναι η πληροφορία να μην μπορεί να αναγνωστεί από τρίτους. Τεχνικά, υπάρχει ένα δημόσιο κλειδί και ένα μυστικό ιδιωτικό κλειδί με τις λειτουργίες της κωδικοποίησης και αποκωδικοποίησης αντίστοιχα. Έτσι, αν χαθεί μια e-ID πληροφορία δεν μπορεί να αποκρυπτογραφηθεί. Επίσης, εάν ο χρήστης κρυπτογραφήσει την πληροφορία με ορισμένα πιστοποιητικά, με την έκδοση νέων πιστοποιητικών της e-ID κάρτας η πληροφορία που έχει κρυπτογραφηθεί με τα προγενέστερα πιστοποιητικά δεν μπορεί να αποκρυπτογραφηθεί από τα νέα πιστοποιητικά (Estonian Information System Authority, χ.η.). Οι χρήσεις της e-ID κάρτας περιλαμβάνουν: μετακινήσεις εντός της ΕΕ, έκδοση ιατρικής κάρτας ασφάλισης, απόδειξη για είσοδο σε τραπεζικούς λογαριασμούς, ηλεκτρονική ψήφο, έλεγχο ιατρικών μητρώων και φορολογικών αιτημάτων και τηλε-ιατρικές εφαρμογές (Estonian Information System Authority, χ.η.). Στο μοντέλο Mobile-ID τα ιδιωτικά κλειδιά αποθηκεύονται στην κάρτα SIM. Επιπλέον, η ψηφιακή κάρτα διαμονής απευθύνεται σε παράγοντες από όλον τον πλανήτη στον κλάδο της επιχειρηματικότητας.

4.2.2 Αυστρία

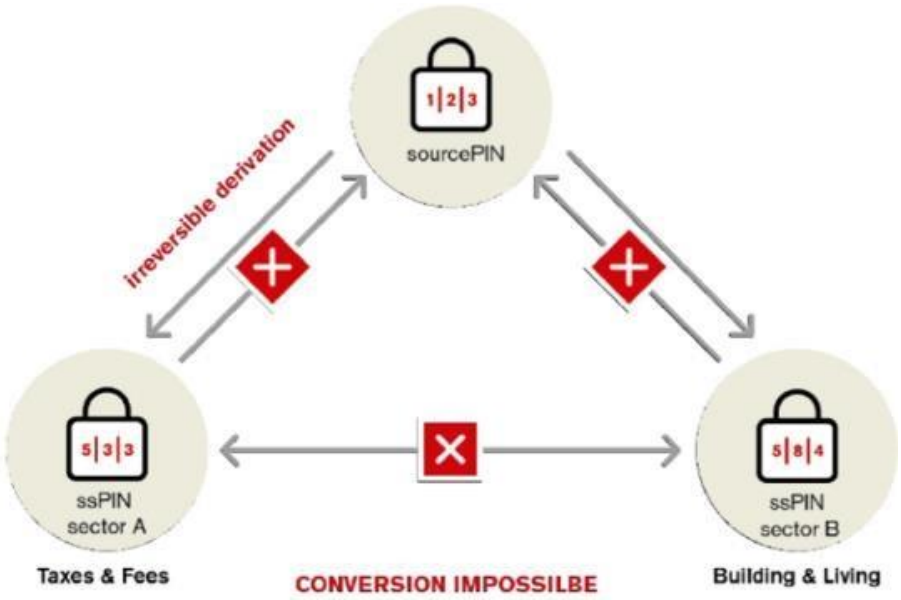
Η Αυστρία, μια από τις ευρωπαϊκές χώρες με 8.7 εκατομμύρια κατοίκους, προχώρησε στο σύστημα εναρμόνισης eIDAS [95] (European Commission, 2017) ενώ ήδη από το 2003 η χώρα εκδίδει ψηφιακές ταυτότητες. Η αυστριακή e-ID αποθηκεύει ελάχιστο αριθμό δεδομένων στο ενσωματωμένο τσιπ (chip) και εκδίδεται για την πρόσβαση σε εφαρμογές ηλεκτρονικής διακυβέρνησης. Να σημειωθεί ότι σε αντίθεση με το

[95] Στις 29 Σεπτεμβρίου 2018 τίθεται σε ισχύ η νομοθεσία για την ηλεκτρονική ταυτοποίηση σε όλη την Ε.Ε., γνωστή ως κανονισμός eIDAS, η οποία επιτρέπει τη διασυνοριακή αναγνώριση των ηλεκτρονικών αναγνωριστικών στοιχείων και θα επιτρέψει στους πολίτες και τις επιχειρήσεις της ένωσης να έχουν πρόσβαση σε διαδικτυακές υπηρεσίες διασυνοριακά. Πρόκειται για μια σειρά από αρχές περί της ψηφιακής ταυτοποίησης και εργαλείων εμπιστευτικότητας για ηλεκτρονικές συναλλαγές (*Electronic Trust Services - eTS*) εντός της ενωσιακής ενιαίας αγοράς που εντάσσει τις ψηφιακές υπογραφές και την ψηφιακή ταυτοποίηση υπό μια ενιαία νομική βάση. Η πρωτοβουλία δεν καθιστά υποχρεωτική την υπαγωγή σε ένα καθεστώς e-ID αλλά επιτάσσει την αναγνώριση αυτής από όλα τα κράτη-μέλη της ΕΕ με στόχο την διασυνοριακή επιχειρηματική δραστηριότητα, την διευκόλυνση των διασυνοριακών διοικητικών διαδικασιών και την ίδια νομική ισχύ των επί χάρτου εγγράφων με τα ψηφιακά έγγραφα υπό ταυτοποίηση.

'κεντροποιημένο' σύστημα της Ινδίας, το σύστημα της Αυστρίας είναι αποκεντρωμένο.

Η Αυστρία υπόκειται στην οδηγία GDPR όπως και στην εθνική νομοθεσία περί των προσωπικών δεδομένων. Φορέας για τη νομική διασφάλιση της ιδιωτικότητας και την έκδοση των ψηφιακών ταυτοτήτων είναι η *SourcePIN Register Authority* που συνεπικουρείται από την Ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων[96] (World Bank Group, 2018c). Εντός της χώρας, η εγγραφή στα τοπικά μητρώα[97] είναι υποχρεωτική είτε για τους κατοίκους είτε για τους μη-κατοίκους. Κάθε εγγραφή δεδομένων έχει έναν αριθμό ταυτοποίησης δώδεκα ψηφίων, με ονοματεπώνυμο, φύλο, ημερομηνία γέννησης, υπηκοότητα, διεύθυνση. Ωστόσο, η απόκτηση μιας φυσικής ταυτότητας δεν είναι υποχρεωτική αφού, αντ' αυτής, το κράτος εκδίδει την ψηφιακή *Citizen Card* (CC) που δύναται να εγκατασταθεί σε πληθώρα συσκευών (κινητά τηλέφωνα, έξυπνες κάρτες, USB συσκευές κ.λπ.) (World Bank Group, 2018c). Ήδη, η ψηφιακή υπογραφή μέσω κινητού τηλεφώνου και οι έξυπνες κάρτες χρησιμοποιούνται κατά κόρον. Κάθε κάρτα CC εκτός από όνομα, ημερομηνία γέννησης και ένα PIN, διαθέτει και κρυπτογραφημένα κλειδιά για κρυπτογράφηση και ψηφιακή υπογραφή. Ο χρήστης πραγματοποιεί συναλλαγές εντός των 26 τομέων υπηρεσιών, μεταξύ των οποίων φορολογία, υγεία, εκπαίδευση κ.λπ. Ο χρήστης έχει απλώς ανάγκη από την κάρτα CC, από έναν αναγνώστη, έναν Η/Υ με σύνδεση στο Διαδίκτυο και ένα ειδικό λογισμικό 'MOAID' (World Bank Group, 2018c, σελ. 19). Οι δημόσιες υπηρεσίες χρησιμοποιούν το ειδικό αλγοριθμικό πιστοποιητικό *ssPIN*. Εκείνο δίνει φυσικά την πρόσβαση να χρησιμοποιηθεί η πληροφορία από τον αρμόδιο δημόσιο φορέα για τη συμπλήρωση κάποιων διοικητικών εγγράφων του φυσικού προσώπου, αλλά όχι τη δυνατότητα να μεταφέρει την πληροφορία σε άλλους δημόσιους φορείς. Για να γίνει αυτό, θα πρέπει ο δημόσιος φορέας να αιτηθεί στον κεντρικό φορέα *SourcePIN Register Authority* την αποστολή των δεδομένων *ssPIN* σε κρυπτογραφημένη μορφή και στη συνέχεια το *ssPIN* να αποκρυπτογραφηθεί μόνο από τον αιτούντα φορέα (World Bank Group, 2018c, σελ. 20).

[96] *Data Protection Authority* (DPA)
[97] Δηλαδή στο *Central Register of Residents* (CRR)

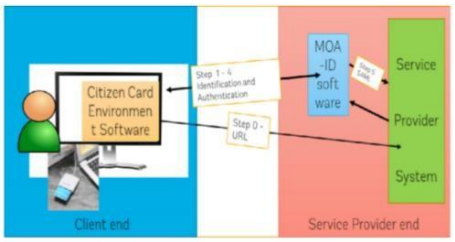


Εικόνα 11 Το σύστημα ssPIN (Digital Austria, Federal Chancellery) από τη μελέτη 'Privacy by Design: Current Practices in Estonia, India, and Austria' (World Bank Group, 2018c, σελ. 19)

Αντιλαμβάνεται κανείς πως με αυτό το σύστημα η προστασία προσωπικών δεδομένων εγγυάται σε αρκετά υψηλό επίπεδο. Υπό τη βάση αυτή, η Αυστρία έχει προχωρήσει και στην ανάπτυξη σχεδίων έξυπνων πόλεων στο πλαίσιο της ηλεκτρονικής διακυβέρνησης με πολλούς ιδιωτικούς παράγοντες να δραστηριοποιούνται στο χώρο (Fernandez-Anez, Fernández-Güell & Giffinger, 2017). Η στρατηγική της ψηφιακής ταυτοποίησης αποτελεί τη βάση για την κυβερνητική πολιτική δίνοντας έμφαση στην ιδιωτικότητα, μείζον ζήτημα της εποχής. Το αποκεντρωμένο σύστημα της αυστριακής κυβέρνησης λειτουργεί αποτελεσματικά για την ασφάλεια των δεδομένων, ακόμα κι αν έχει υποστηριχθεί ότι τόσο σε επίπεδο κόστους συντήρησης των τεχνικών υποδομών όσο και σε επίπεδο πρακτικότητας ένα κεντροποιημένο σύστημα λειτουργεί ίσως καλύτερα (Zwattendorfer & Slamanig, 2016).

Πίνακας 11 Οι αποθηκευμένες ή αποθηκεύσιμες πληροφορίες της κάρτας CC – Citizen Card (συλλογή στοιχείων από το World Bank Group, 2018c)

Κάθε πολίτης δίνει τις απαραίτητες προσωπικές πληροφορίες
Κάθε άτομο έχει έναν ειδικό κωδικό *sourcePIN* από το *Central Register of Residents*
Ενσωματωμένη εφαρμογή για ηλεκτρονικές υπογραφές που μπορεί να συνδυαστεί με μια ηλεκτρονική διεύθυνση
Εφαρμογή μιας ψηφιακής νομικής 'εντολής' για όποιον πολίτη διαθέτει την κάρτα να πράξει αντ' αυτού (φυσικού ή νομικού προσώπου)
Δύναται να αποθηκεύονται και πληροφορίες όπως: τραπεζικών λογαριασμών, φοιτητικής ακαδημαϊκής ταυτότητας



1. When a user requests a service, MOA-ID checks the integrity and authenticity of the CC.
2. MOA-ID calculates the ssPIN by applying a cryptographic hash function H (SHA-1) to the concatenation of the SourcePIN and the sector-specific identifier of the service provider.
3. MOA-ID requests consent of the user for the service by requesting electronic signature of the user.
4. MOA-ID verifies the citizen's qualified signature.
5. The user can now avail the service (MOA-ID sends SAML response to service provider system).

Εικόνα 12 Η διαδικασία αυθεντικοποίησης. Από την ερευνητική μελέτη 'Privacy by Design: Current Practices in Estonia, India, and Austria' (World Bank Group, 2018c, σελ. 19)

4.2.3 Ελλάδα: Ακαδημαϊκή ταυτότητα ΕΚΠΑ[98]

Η ψηφιακή υπογραφή περιλαμβάνει "*προσωπικά ψηφιακά πιστοποιητικά αυθεντικοποίησης/υπογραφής και κρυπτογράφησης τα οποία ο υπογράφων διατηρεί υπό τον αποκλειστικό του έλεγχο*[99] " (Λάριος, Ν., Συνέντευξη, 3 Ιουνίου 2019[100]). Έτος 'γέννησης' της ψηφιακής υπογραφής είναι το 2008 και, αργότερα, το 2015 επεκτάθηκε στον ακαδημαϊκό τομέα με την απόκτηση της Ακαδημαϊκής Ταυτότητας. Οι ψηφιακές υπογραφές "*απευθύνονται σε όλα τα μέλη της Πανεπιστημιακής Κοινότητας που χρειάζονται ασφαλή ανταλλαγή εγγράφων και ηλεκτρονικού*

[98] Από τη Συνέντευξη που πραγματοποιήθηκε με τον κο Ν. Λάριο
[99] Μέσω κάρτας ή ειδικής συσκευής USB.
[100] Βλ. Παράρτημα Β για Συνέντευξη

ταχυδρομείου, υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων, ασφαλή προσδιορισμό της ηλεκτρονικής ταυτότητας, έλεγχο πρόσβασης σε κατάλληλες εφαρμογές κ.α." (Λάριος, Ν., Συνέντευξη, 3 Ιουνίου 2019).

Σε τεχνικό επίπεδο, η ψηφιακή υπογραφή ΕΚΠΑ βασίζεται στο εξής σύστημα. Χρησιμοποιείται η κρυπτογραφία δημοσίου κλειδιού σύμφωνα με την οποία ο χρήστης διαθέτει δύο κλειδιά (ένα δημόσιο, ένα ιδιωτικό). Εάν κάποιος γνωρίζει το ένα κλειδί πρακτικά είναι αδύνατον να ανασύρει το άλλο[101]. Η διαφορά από την κρυπτογράφηση αφορά στο ότι στην ψηφιακή υπογραφή "*ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα*" (Λάριος, Ν., Συνέντευξη, 3 Ιουνίου 2019). Έτσι, μέσω της συνάρτησης κατακερματισμού [102], από ένα μήνυμα ανεξαρτήτου μεγέθους παράγεται η «σύνοψή του», με τη μορφή μιας σειράς από bits[103]. Η σύνοψη μηνύματος[104] είναι μία ψηφιακή αναπαράσταση του μηνύματος και μοναδική για το μήνυμα και το αντιπροσωπεύει [105]. Έτσι, το κόστος της τεχνολογίας είναι πολύ χαμηλό. Οι ταυτότητες προμηθεύονται δωρεάν από το Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων. Ο αναγνώστης της κάρτας έχει κόστος σαράντα ευρώ, το λογισμικό εγκατάστασης παρέχεται δωρεάν και, κατά συνέπεια, το κόστος συντήρησης, εκτός της προβλεπόμενης διετούς ανανέωσης της κάρτας, είναι αμελητέο.

Ωστόσο, από το 2016 υπάρχουν αρκετά προβλήματα κυρίως αδυναμίας ενεργοποίησης εξαιτίας χαμένου κωδικού ή μηνύματος ενεργοποίησης. Ένα αρνητικό γνώρισμα αφορά στην ανάγκη "*εξοικείωσης* των μελών της Πανεπιστημιακής Κοινότητας με την νέα τεχνολογία" όπως αναφέρει ο κ. Λάριος.

Η αλλαγή στην ταυτοποίηση, βέβαια, έχει ήδη γίνει εμφανής καθώς πλέον

[101] Όπως αναφέρεται χαρακτηριστικά: "*Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της*" (Λάριος, Ν., 3 Ιουνίου 2019, Συνέντευξη) [102]
[102] 'One way hash', στην αγγλική ορολογία.
[103] Π.χ. 128 ή 160 bits
[104] 'Fingerprint ή message digest', στην αγγλική ορολογία.
[105] Βλ. Παράρτημα Β για περισσότερες πληροφορίες.

"*προμήθειες και διαγωνισμοί του δημοσίου δεν νοούνται χωρίς την χρήση της ψηφιακής υπογραφής*" [106] (Λάριος, Ν., Συνέντευξη, 3 Ιουνίου 2019). Ένα βασικό θετικό γνώρισμα της τεχνολογίας αφορά στην ασφάλεια. Με την ψηφιακή υπογραφή, εξασφαλίζεται η διαφύλαξη εμπιστευτικών πληροφοριών, η βελτίωση της ροής των ψηφιακών εργασιών, η εξοικονόμηση χρόνου, χαρτιού αλλά και κόστους[107].

Υποκεφάλαιο 4.3 Συμπεράσματα από τις μελέτες περίπτωσης

4.3.1 Συμπεράσματα από τις μελέτες περίπτωσης

Οι μελέτες περίπτωσης που παρουσιάστηκαν έχουν ένα κοινό γνώρισμα: την ταυτοποίηση στο πλαίσιο της ηλεκτρονικής διακυβέρνησης και των υπηρεσιών προς τον πολίτη. Οι χώρες αποτελούν ενδεικτικά παραδείγματα των οποίων ένα μεγάλο ποσοστό σε παγκόσμιο επίπεδο έχει προχωρήσει στην υλοποίηση τέτοιων πρωτοβουλιών, όπως αναπαρίσταται στον χάρτη του παρόντος κεφαλαίου (Εικόνα 10).

Η σημασία της ταυτοποίησης, όπως τονίστηκε και στο υποκεφάλαιο 3.4, δεν είναι μόνο οι εν γένει λύσεις που προτείνει αλλά και το γεγονός ότι τα παραδείγματα αυτά δύνανται να αποτελέσουν το έναυσμα για μια παγκόσμια, και δη ελληνική, πορεία ανάπτυξης και προόδου στο επίπεδο της επικοινωνίας μεταξύ πολίτη και κρατικών μηχανισμών[108]. Έχουν υπάρξει περιπτώσεις όπου η ηλεκτρονική ταυτοποίηση δεν πέτυχε, όπως στο μοντέλο της Ελβετίας κυρίως εξαιτίας θεμάτων υποδομής και κόστους. Όμως αυτό έχει προωθήσει περαιτέρω τις τεχνολογικές εξελίξεις και στο ελβετικό οικοσύστημα έχουν προταθεί προγράμματα που εντάσσουν την τεχνολογία Blockchain στην ψηφιακή ταυτοποίηση. Έτσι, δυο δημοτικές ομοσπονδιακές

[106] Τόσο από τις αναθέτουσες αρχές όσο και από τους προμηθευτές.
[107] Σύμφωνα με τον ΙΟΒΕ υπάρχει εξοικονόμηση 400 εκ. ευρώ ανά έτος με την κατάργηση του χαρτιού και των παράπλευρων διαδικασιών κατά την έκδοση διοικητικών εγγράφων και πράξεων (Λάριος, Ν., Συνέντευξη, 3 Ιουνίου 2019).
[108] Το πρόβλημα της συνολικότερης γραφειοκρατίας και των χρονοβόρων διαδικασιών παρατηρείται σε παγκόσμια κλίμακα.

περιφέρειες από το φθινόπωρο 2017 προτείνουν μια βασισμένη στο Blockchain Ethereum λύση για ψηφιακή ταυτότητα, την *Zug ID*, παίρνοντας το όνομα της ελβετικής πόλης (Young & Verhulst, 2018). Τα δεδομένα ταυτοποίησης βρίσκονται αποθηκευμένα στην ιδιωτική κλειδαριά της ηλεκτρονικής εφαρμογής ενώ ο χρήστης χρειάζεται για την ταυτοποίησή του να παρουσιαστεί στη διοικητική υπηρεσία της περιοχής του μια μόνο φορά. Αντίστοιχα, το καντόνιο Schaffhauser, προτείνει τη λύση του eID+, επίσης μια ψηφιακή ταυτότητα που βασίζεται στο Blockchain. Αυτές οι πρωτοβουλίες *τρέχουν* από το 2018 (Young & Verhulst, 2018).

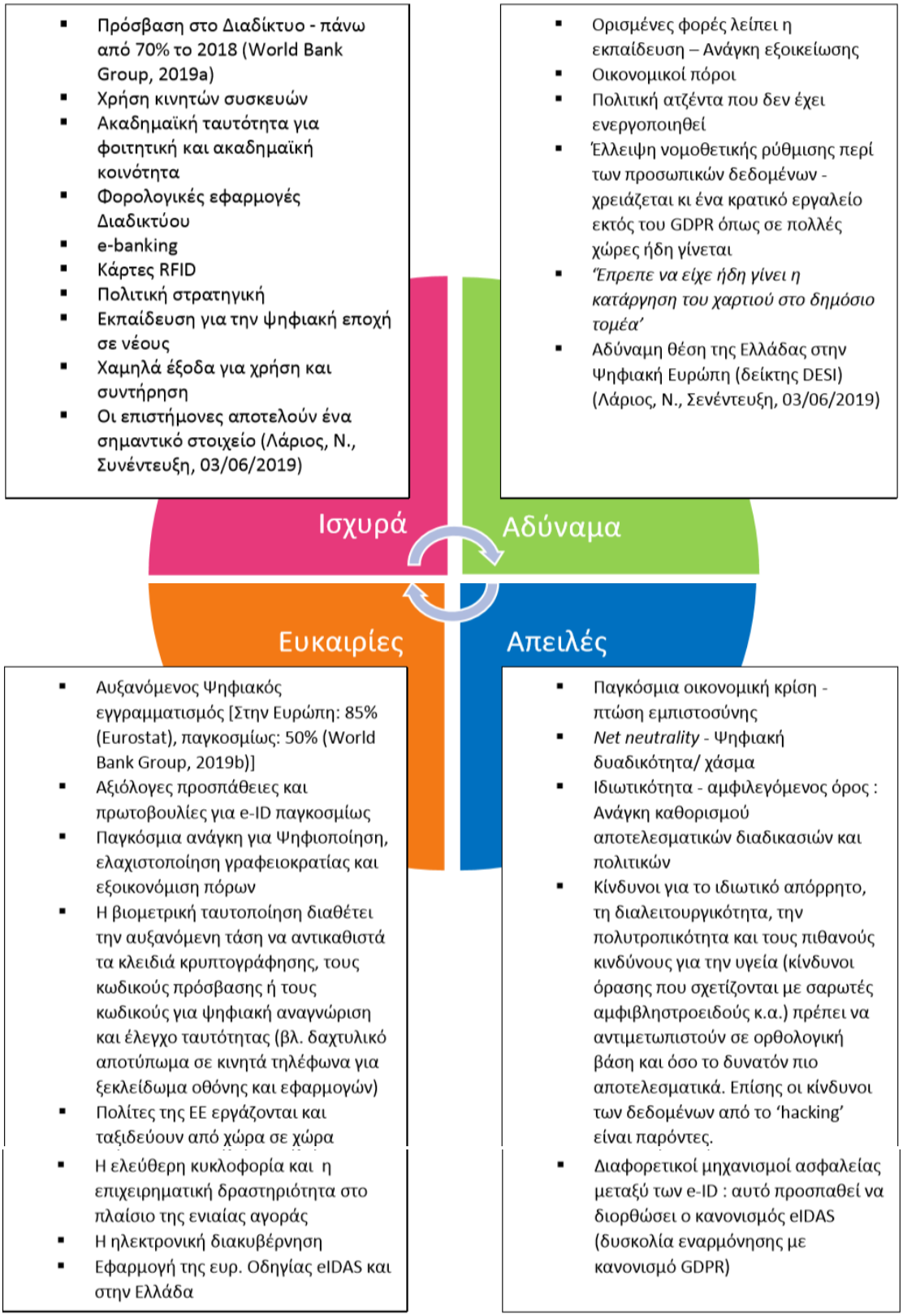
Όλες αυτές οι περιπτώσεις αποτελούν πολύτιμα μαθήματα για την Ελλάδα στο μέτρο που προτείνουν λύσεις για αποτελεσματικότητα και ταχύτητα στις σχέσεις πολίτη-Κράτους. Η τεχνολογία ταυτοποίησης με Blockchain, παρά τα λίγα παραδείγματα μέχρι στιγμής παγκοσμίως, αποτελεί τον ασφαλέστερο και ίσως τον ελκυστικότερο τρόπο και προς τους πολίτες αλλά και προς τους κρατικούς οργανισμούς για τη διαχείριση δεδομένων και τη διασφάλιση της ιδιωτικότητας. Το μόνο σίγουρο είναι ότι αν και εφόσον αξιοποιηθεί και σχεδιαστεί ορθά, η τεχνολογία θα δώσει πολύ ικανοποιητικά αποτελέσματα. Ήδη, πολλές χώρες εμπιστεύονται την αλυσίδα Blockchain για ψηφιακή ταυτοποίηση και υπηρεσίες προς τους πολίτες. Το επιχείρημα, επομένως, του παρόντος κεφαλαίου είναι ότι δίνοντας περισσότερες ευκαιρίες στην τεχνολογία Blockchain, πιστεύουμε ότι θα αυξηθούν οι δυνατότητες εξέλιξης και ανέλιξης της τεχνολογίας σε επίπεδο ηλεκτρονικής διακυβέρνησης και όχι μόνο. Σε αυτό το πλαίσιο, μένει να μελετηθεί ειδικότερα η θέση της Ελλάδας σχετικά με το ενδεχόμενο επιλογής της ηλεκτρονικής ταυτοποίησης.

4.3.2 Η θέση της Ελλάδας και η ψηφιακή ταυτοποίηση[109]

Με το εργαλείο της ανάλυσης SWOT, θα επιχειρήσουμε να περιγράψουμε το συνολικότερο πλαίσιο της ελληνικής περίπτωσης σε ό,τι αφορά μια ενδεχόμενη πολιτική στρατηγική επιλογή ηλεκτρονικής ταυτοποίησης.

[109] Αξιοποιήθηκαν και οι πολύτιμες πληροφορίες της Συνέντευξης

Πίνακας 12 Ανάλυση SWOT για ανάπτυξη e-ID στην Ελλάδα: Στην Ελλάδα εάν εφαρμοστεί η πολιτική για την ηλεκτρονική ταυτοποίηση, ποιά είναι τα ισχυρά/αδύναμα σημεία και ποιές οι ευκαιρίες/απειλές;



Συμπεράσματα

Στην παρούσα εργασία μελετήθηκε η τεχνολογία Blockchain ως προς την δομή, τα κρυπτονομίσματα και την ταυτοποίηση. Η αρχική υπόθεση του αν το Πρωτόκολλο Blockchain μπορεί να υποστηρίξει σύγχρονες εφαρμογές όπως και να υποβοηθήσει το σύστημα της ηλεκτρονικής διακυβέρνησης φαίνεται να οδηγεί σε μια επιχειρηματολογία υπέρ της τεχνολογίας αυτής. Το μέλλον αναμένεται τελικά *ενδιαφέρον*. Η τεχνολογία *Blockchain* θα μπορούσε να επιφέρει πολλές λύσεις και στην Ελλάδα. Η τεχνολογία διασυνδεδεμένων/διαμοιρασμένων κόμβων έχει επικρατήσει κατά κάποιο τρόπο λόγω της υψηλής ασφάλειας που αναζητείται συχνά στο Διαδίκτυο. Όταν τα δεδομένα είναι αμετάκλητα και σταθερά, οι εμπορικές συναλλαγές τουλάχιστον γίνονται κατά τρόπο πιο σίγουρο και ελέγξιμο. Ο,τιδήποτε αναλογικό, όπως μια εμπράγματη αξία ενός αγαθού ή η προσωπική ταυτότητα, τώρα μπορεί να καταχωρηθεί και να διατηρηθεί επιγραμμικά (Laurence, 2017). Η ασφαλής μεταφορά ψηφιακών αρχείων δεδομένων, χρημάτων και αγαθών είναι πια δυνατή. Με το Πρωτόκολλο Blockchain τα εθνικά, διοικητικά ακόμη και δικαστικά σύνορα δεν αποτελούν πια εμπόδια. Παρατηρούνται βέβαια ελλείψεις νομοθετικών ρυθμίσεων, γεγονός που καθιστά τις ιδιωτικές συναλλαγές αβέβαιες και ριψοκίνδυνες, απουσία ενός παγκόσμιου κινήματος, καθώς το παράδειγμα παραμένει θεωρητικό, θέματα ωρίμανσης της τεχνολογίας, ζητήματα ιδιωτικότητας και, τέλος, συγκρούσεις με άλλες τεχνολογίες που βασίζονται σε διαφορετικά πρωτόκολλα αλλά διενεργούν παρόμοιες διαδικασίες. Σε ό,τι αφορά τα Bitcoins, αυτά αποτελούν ένα ξεχωριστό εργαλείο που, παρά τις διάφορες ανακοινώσεις διεθνών τραπεζών περί ενημέρωσης της ασφάλειας, δίνουν μια εξαιρετική ‘απάντηση’ στην παγκόσμια κρίση ωθώντας φτωχότερες κοινωνικές τάξεις στην ανάπτυξη. Βέβαια, όπως αναφέρει ο Volkering (2017, σελ. 140), “το Bitcoin είναι όντως το πρώτο κρυπτονόμισμα, όχι όμως αυτό που αναγκαστικά θα επικρατήσει στο μέλλον”. Αναμένεται με την επερχόμενη ευρωπαϊκή

οδηγία PSD2 [110] η τεχνολογία Blockchain να ενδυναμώσει τα εκάστοτε σχέδια ανάπτυξης στο πλαίσιο του *Fintech*[111] και να ενδυναμωθεί από αυτά (Bambara & Allen, 2018). Επιπλέον, η ταυτοποίηση με Blockchain σιγά-σιγά γίνεται πραγματικότητα καθώς χώρες όπως η Μεγάλη Βρετανία, η Σιγκαπούρη, τα Ηνωμένα Αραβικά Εμιράτα, η Ελβετία, ήδη ξεκινούν την εγκατάσταση Blockchain λύσεων[112]. Δια τούτο, στο επίπεδο της ταυτοποίησης προτείνεται η συνεργασία μεταξύ των κυβερνητικών μηχανισμών για νομοθετική ρύθμιση και του ιδιωτικού τομέα για τις καινοτομίες, τις οικονομικές λύσεις, τις εξελίξεις και τις προτάσεις που μπορεί να τεθούν (World Bank Group & GSMA, 2016).

Σε αυτό το σημείο, είναι σκόπιμο να σημειωθεί η σημασία και το ενδιαφέρον για περαιτέρω έρευνα και μελέτη τόσο του πεδίου εφαρμογής των κρυπτονομισμάτων στην Ελλάδα, δεδομένης της ανάπτυξής τους στην επικράτεια, όσο και της ανάλυσης της δυνατότητας να υπάρξει εφαρμογή της τεχνολογίας Blockchain στον τομέα της ηλεκτρονικής ταυτοποίησης, θέμα που συζητείται παγκοσμίως μόλις τα τελευταία δυο χρόνια.

[110] Αναθεωρημένη οδηγία για τις υπηρεσίες πληρωμών εντός της ΕΕ
[111] Όρος που περιγράφει την σύζευξη τεχνολογίας και χρηματοπιστωτικού τομέα
[112] Βλ. Παράρτημα Α για περισσότερες πληροφορίες

Βιβλιογραφικές Αναφορές

Επιστημονικά βιβλία

Antonopoulos, A. (2016). *Mastering Bitcoin Unlocking Digital Cryptocurrencies-O'Reilly* (2η έκδοση). Sebastopol, CA: O'Reilly Media

Bambara, J. J. & Allen, P. R. (2018). *Blockchain A practical Guide to Developing Business, Law and Technology Solutions*. McGraw-Hill Education

Bashir, I. (2017). *Mastering Blockchain. Distributed ledgers, decentralization and smart contracts explained*. BIRMINGHAM – MUMBAI: Packt Publishing

Capurro, R., Eldred, M. & Nagel, D. (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. Heusenstamm: Ontos Verlag

Για μια γενικότερη κριτική ματιά στα συστήματα ταυτοποίησης

Das, R. (2016). *ADOPTING BIOMETRIC TECHNOLOGY Challenges and Solutions*. CRC Press.

Drescher, D. (2017). *Blockchain Basics A Non-Technical Introduction in 25 Steps*. Birmingham: Packt Publishing

Girasa, R. J. (2018). *Regulation of Cryptocurrencies and Blockchain Technologies National and International Perspectives.* DOI: 10.1007/978-3-319-78509-7

Hartley, J. (2011). *COMMUNICATION, CULTURAL AND MEDIA STUDIES. The Key Concepts.* London - New York: Routledge

Για τον ορισμό της ταυτότητας στο πεδίο της Επικοινωνίας

Jiang, L. & Meng, W. (2017). Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities. Στο: Jiang, R. et al. (επιμ.). *Biometric Security and Privacy. Opportunities & Challenges in The Big Data Era* (σελ. 163-178). DOI: 10.1007/978-3-319-47301-7_7

Judmayer, A., Stifter, N., Krombholz, K. & Weippl, E. (2017). *Blocks and Chains. Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanism.* DOI: 10.2200/S00773ED1V01Y201704SPT020

Karame, G. & Androulaki, E. (2016). *Bitcoin and Blockchain Security*. Norwood, MA: ARTECH HOUSE

Kuo Chuen, D. L. & Pak Nian, L. (2015). Introduction to Bitcoin. Στο: Kuo Chuen, D. L. (επιμ.). *Handbook of Digital Currency* (σελ. 5-29). USA: Elsevier.

Laurence, T. (2017). *Blockchain For Dummies*. NEW JERSEY: John Wiley & Sons, Inc.

Laurent, M. & Bouzefrane, S. (2015). *Digital Identity Management*. Great Britain - United States: ISTE Press & Elsevier

Morabito, V., (2017). *Business Innovation Through Blockchain*. DOI 10.1007/978-3-319-48478-5

Noizat, P. (2015). Blockchain Electronic Vote. Στο: Kuo Chuen, D. L. (επιμ.). *Handbook of Digital Currency* (σελ. 453-461). USA: Elsevier.

Quest, M. (2018). *Cryptocurrency Master Bundle: The Art of holding crypto mining mindset, The ICO approach, Cryptocurrency 101, Blockchain Dynamics*. Martin Quest

Sapovadia, V. (2015). Legal Issues in Cryptocurrency. Στο: Kuo Chuen, D. L. (επιμ.). *Handbook of Digital Currency* (σελ. 253-266). USA: Elsevier.

Szmigielski, A. (2016). *Bitcoin Essentials. Gain insights into Bitcoin, a cryptocurrency and a powerful technology, to optimize your Bitcoin mining techniques*. BIRMINGHAM – MUMBAI: Packt Publishing

Volkering, S. (2017). *Crypto Revolution: Bitcoin, Cryptocurrency and the Future of Money*. Southbank Investment Research

Yang, A. & Hancke, G. P (2017). RFID and Contactless Technology. Στο: Mayes, K. & Markantonakis, K. (επιμ.). *Smart Cards, Tokens, Security and Applications* (2η έκδοση) (σελ. 351-383). DOI: 10.1007/978-3-319-50500-8

Επιστημονική Αρθρογραφία

Chen, L., Lee, W.- K., Chang, C. C., Chood, K. K. R. & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems, 95*, 420–429. DOI: https://doi.org/10.1016/j.future.2019.01.018

Curzona, J., Almehmadi, A. & El-Khatib, K. (2019). A survey of privacy enhancing technologies for smart cities. *Pervasive and Mobile Computing, 55*, 76–95. DOI: https://doi.org/10.1016/j.pmcj.2019.03.001

Dwyer, P. G. (2014). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability, 17*, 81–91. DOI: 10.1016/j.jfs.2014.11.006

Efanov, D. & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science, 123*, 116-121. DOI: 10.1016/j.procs.2018.01.019

Fernandez-Anez, V., Fernández-Güell, J.-M. & Giffinger, R. (2017). Smart City implementation and discourses: An integrated conceptual model. The case of Vienna. *Cities, 78*, 4–16. DOI: 10.1016/j.cities.2017.12.004

Giancaspro, M., (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer law & security review, 33*, 825–835. DOI: 10.1016/j.clsr.2017.05.007

Gürkaynak, G., Yılmaz, I., Yeşilaltay, B. & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review, 34*, 847–862. DOI: 10.1016/j.clsr.2018.05.027

Hussein, A. F., ArunKuman, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M. R. S. & de Albuquerque, V. H. C. (2018). A medical records managing and securing Blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cognitive Systems Research, 52*, 1–11. DOI: 10.1016/j.cogsys.2018.05.004

Labati, R. D., Genovese, A., Piuri, V. & Scotti, F., (2014). Touchless Fingerprint Biometrics: A Survey on 2D and 3D Technologies. *Journal of Internet Technology, 15* (3328), 327-334. DOI: 10.6138/JIT.2014.15.3.01

Mansfield-Devine, S., (2015). Biometrics in developing Countries. *Biometric Technology Today*. *Biometric Technology Today, 2015* (4), 5-8. DOI: 10.1016/S0969-4765(15)30060-6

Mašek, J., Kolarovszki, P. & Čamaj, J., (2016). Applications of RFID Technology in Railway Transport Services and Logistics Chains. *Procedia Engineering, 164*, 231 – 236. DOI: 10.1016/j.proeng.2016.01.064

Millard, Ch. (2018). Blockchain and law: Incompatible codes?. *Computer Law & Security Review, 34*, 843–846. DOI: 10.1016/j.clsr.2018.06.006

Nilekani, N., (2018). Data to the People, India's Inclusive Internet. *FOREIGN AFFAIRS, 97* (5), 19-26

Pan, Y., Zhang, X., Wang, Y., Yan, J., Zhou, S., Li, G. & Bao, J. (2018). Application of Blockchain in Carbon Trading. *Energy Procedia, 158*, 4286–4291. DOI: 10.1016/j.egypro.2019.01.509

Ring, T. (2015). Spoofing: are the hackers beating biometrics?. *Biometric Technology Today, 2015* (7), 5-9. DOI: 10.1016/S0969-4765(15)30119-3

Savelyev, A. (2018). Some risks of tokenization and blockchainizaition of private law. *Computer Law & Security Review*, *34,* 863–869. DOI: 10.1016/j.clsr.2018.05.010

Shah, T. & Jani, Sh. (2018). Applications of Blockchain in Banking Finance.

Ανακτήθηκε από: https://www.researchgate.net/publication/327230927_Applications_of_Blockchain_Technology_in_Banking_Finance

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer law & Security review, 34,* 341–353. DOI: 10.1016/j.clsr.2017.03.011

Volety, T., Saini, S., McGhin, T., Liu, C. Z. & Choo, K. K. R. (2018). Cracking Bitcoin wallets: I want what you have in the wallets. *Future Generation Computer Systems, 91*, 136-143. DOI: 10.1016/j.future.2018.08.029

Έρευνες δημοσιευμένες σε επιστημονικά περιοδικά

Broséus, J., Morelato, M., Tahtouh, M. & Roux, C. (2017). Forensic Drug Intelligence and the rise of cryptomarkets. Part 1: Studying the Australian virtual market. *Forensic Science International, 279,* 288-301. DOI: 10.1016/j.forsciint.2017.08.026 0379-0738/

Cagli, E. C. (2018). Explosive behavior in the prices of Bitcoin and altcoins. *Finance Research Letters.* DOI: 10.1016/j.frl.2018.09.007

Dagher, G. G., Mohler, J., Milojkovic, M. & Marella, P. B. (2018). Ancile*:* Privacypreserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297. DOI: 10.1016/j.scs.2018.02.014

Dyhrberg, A. H. (2015a). Bitcoin, gold and the dollar – A GARCH volatility analysis. *Finance Research Letters*, *16,* 85–92. DOI: 10.1016/j.frl.2015.10.008

Dyhrberg, A. H. (2015b). Hedging capabilities of bitcoin. Is it the virtual gold?. *Finance Research Letters, 16,* 139–144. DOI: 10.1016/j.frl.2015.10.025

Li, X., Jiang, P., Chen, T., Luo, X. & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems.* DOI: http://dx.doi.org/10.1016/j.future.2017.08.020.

Low, K. F. K. & Teo, E. (2016). Legal Risks of Owning Cryptocurrencies. *Handbook of Blockchain, Digital Finance, and Inclusion, 1,* 225-247. DOI: 10.2139/ssrn.2856137

Mensi, W., Rehman, M. U., Al-Yahyaee, K. H., Al-Jarrah, I. M. W. & Kang, S. H. (2019). Time frequency analysis of the commonalities between Bitcoin and major Cryptocurrencies : Portfolio risk management implications. *North American Journal of Economics and Finance, 48,* 283-294. DOI: 10.1016/j.najef.2019.02.013

Reyes, P. M., Li, S. & Visich, J. K. (2016). Determinants of RFID adoption stage and perceived benefits. *European Journal of Operational Research, 254,* 801–812. DOI: 10.1016/j.ejor.2016.03.051

Roehrs, A., Da Costa, C. A., da Rosa Righi, R., Ferreira da Silva, V., Goldim, J. R. & Schmidt, D. C. (2019). Analyzing the performance of a blockchain – based personal health record implementation. *Journal of Biomedical Informatics*, *92,* 1-9. DOI: 10.1016/j.jbi.2019.103140

Wang, Q., Qin, B., Hu, J. & Xiao, F. (2017). Preserving transaction privacy in bitcoin. *Future Generation Computer Systems.* DOI: 10.1016/j.future.2017.08.026

Yang, Ch., Chen, X. & Xiang, Y. (2017). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *Journal of Network and Computer Applications, 103*, 185–193. DOI: 10.1016/j.jnca.2017.11.011

Yi, S., Xu, Z. & Wang, G.-J. (2018). Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?. *International Review of Financial Analysis, 60,* 98-114. DOI: 10.1016/j.irfa.2018.08.012

Zwattendorfer, B. & Slamanig, D. (2016). The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality. *Journal of Information Security and Applications*, *27-28*, 35–53. DOI: 10.1016/j.jisa.2015.11.004

Έγγραφα εργασίας - Working Papers για την πρωτοβουλία 'ID4D'

Dahan, M. & Hanmer, L. (χ.η.). *THE IDENTIFICATION FOR DEVELOPMENT (ID4D) AGENDA: Its Potential for Empowering Women and Girls*. Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/22795

Hanmer, L. & Elefante, M. (2016). *The Role of Identification in Ending Child Marriage: Identification for Development (ID4D)*. Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/25184

Manby, B. (2016). *Identification in the Context of Forced Displacement Identification for Development (ID4D).* Ανακτήθηκε από: https://openknowledge.worldbank.org/bitstream/handle/10986/24941/Identification0r0development00ID4D0.pdf?sequence=4&isAllowed=y

World Bank Group (2018a). *Technology Landscape for Digital Identification*. Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/31825

World Bank Group (2018b). *G20 Digital Identity Onboarding*. Ανακτήθηκε από: https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

World Bank Group (2018c). *Privacy by Design: Current Practices in Estonia, India, and Austria.* Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/31053

World Bank Group & GSMA (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/24920

Young, A. & Verhulst, S. (2018). *Self Sovereign Identity for Government Services in Zug, Switzerland.* Ανακτήθηκε από: https://blockchan.ge/blockchangegovernment-services.pdf

Έγγραφα κρατικών οργανισμών – 'Λευκές Βίβλοι'

Digital Commercial Chamber (2016). *Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction*. Ανακτήθηκε από: https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf

Τράπεζα της Ελλάδος (2018). *Ενημέρωση για τη χρήση εικονικών νομισμάτων*. Ανάκτηση από: https://www.bankofgreece.gr/Pages/el/Bank/News/Announcements/DispItem.aspx?Item_ID=5981&List_ID=1af869f3-57fb-4de6-b9ae-bdfd83c66c95

Στοιχεία Βάσεων Δεδομένων

Eurostat (2019). *Internet use by individuals, % of individuals aged 16 to 74. 2007 to 2018.* [Data set]. Ανακτήθηκε από: https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00 028&plugin=1

World Bank Group (2019a). *Individuals using the Internet (% of population).* Ανακτήθηκε από: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&start=2014

World Bank Group (2019b). *World Development Indicators. Individuals using the Internet (% of population). 2017 to 2018* [Data set]. Ανακτήθηκε από: https://databank.worldbank.org/data/reports.aspx?source=worlddevelopmentindicators

Διαδικτυακές πηγές

Ελληνικοί Ιστότοποι

Κυρίτσης, Α. (2019). *Πώς Λειτουργεί Το Bitcoin Και Πώς Είναι Ασφαλές Σαν Νόμισμα.* Ανακτήθηκε από: https://www.pcsteps.gr/13813-bitcoin/#__block

Bitcoin Project, (2019). *Γιατί οι άνθρωποι εμπιστεύονται το Bitcoin;*. Ανάκτηση από: https://bitcoin.org/el/faq#what-are-the-disadvantages-of-bitcoin

Ξενόγλωσσοι Ιστότοποι

1DayDude Team, (2018). *What is the Blockchain? Simply Explained*. Ανακτήθηκε από: https://www.1daydude.com/what-is-the-blockchain-simply-explained/

Anwar, H. (2019). *Distributed Ledger Technology: Where Technological Revolution Starts*. Ανακτήθηκε από: https://101blockchains.com/distributed-ledgertechnology-dlt/

Bird, G. (2016). *Block chain technology, smart contracts and Ethereum*. Ανάκτηση από: https://developer.ibm.com/clouddataservices/2016/05/19/block-chaintechnology-smart-contracts-and-ethereum/

Bond, K. (2018). *Uganda launches major refugee verification operation*. Ανακτήθηκε από: https://www.unhcr.org/news/latest/2018/3/5a9959444/uganda-launchesmajor-refugee-verification-operation.html

Brakeville, S. & Perepa, B. (2019). *Blockchain basics: Introduction to distributed ledgers. Get to know this game-changing technology and how to start using it*. Ανακτήθηκε από: https://developer.ibm.com/tutorials/cl-blockchain-basics-introbluemix-trs/

Estonian Information System Authority (χ.η.). *Applications of electronic identity*. Ανακτήθηκε από: https://www.ria.ee/en/state-informationsystem/eid/applications.html

European Commission (2017). *Access to the European public services with national eID is becoming possible*. Ανακτήθηκε από: https://ec.europa.eu/digital-singlemarket/en/news/access-european-public-services-national-eid-becomingpossible

Hoffman, Ch. (2018). *What Are Altcoins, and Why Do They Exist?.* Ανακτήθηκε από: https://www.howtogeek.com/341972/what-are-altcoins-and-why-do-they-exist/

Gopie, N. (2018). *What are smart contracts on blockchain?.* Ανακτήθηκε από: https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-onblockchain/

iBankCrypto (2018). *3 Altcoins That You Should Avoid Investing in 2019*. Ανακτήθηκε από: https://globalcoinreport.com/3-altcoins-avoid-investing-2019/

IBM Knowledge Center (2019). *Security concepts and mechanisms*. Ανακτήθηκε από: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.sec.doc/q009730_.htm

Krawisz, D. (2013). *The Problem with Altcoins*. Ανακτήθηκε από: https://nakamotoinstitute.org/mempool/the-problem-with-altcoins/

The Public Voice, (χ.η.). *Privacy: Background*. Ανακτήθηκε από: https://thepublicvoice.org/issues_and_resources/privacy-background/

Twelves, R. (χ.η.). *THE PROMISE AND PERIL OF DIGITAL IDENTIFICATION FOR AID DISTRIBUTION*. Ανακτήθηκε από: https://future-rcrc.com/2019/01/15/thepromise-and-peril-of-digital-identification-for-aid-distribution/

Πηγή για αγγλοελληνικό λεξικό όρων

Forouzan, B. (2014). *Εισαγωγή στην Επιστήμη των Υπολογιστών* (3η έκδοση). Αθήνα: Κλειδάριθμος

Εικόνες

Anwar, H. (2019). *Τα πλεονεκτήματα και οι καινοτομίες των τεχνολογιών DLT*. Ανάκτηση από: https://101blockchains.com/distributed-ledger-technology-dlt/

Bird, G. (2016). *Block chain technology, smart contracts and Ethereum*. Ανάκτηση από: https://developer.ibm.com/clouddataservices/2016/05/19/block-chaintechnology-smart-contracts-and-ethereum/

Brakeville, S. & Perepa, B. (2018). *Blockchain basics*. Ανάκτηση από: https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemix-trs/

Coinmarket Cap. (χ.η.). *Bitcoin*. Τελευταία προσπέλαση στις 19/5/2019: https://coinmarketcap.com/currencies/bitcoin/

Kannengießer, N., Lins, S., Dehling, T. & Sunyaev, A. (2018). *What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology*. Ανάκτηση από: http://www.aifb.kit.edu/web/Inproceedings3728

Laurence, T. (2017). *Blockchain For Dummies*. NEW JERSEY: John Wiley & Sons, Inc.

World Bank Group (2018a). *Technology Landscape for Digital Identification*. Ανακτήθηκε από: https://openknowledge.worldbank.org/handle/10986/31825

World Bank Group (2018c). *Privacy by Design: Current Practices in Estonia, India, and Austria*. Ανάκτηση από: https://openknowledge.worldbank.org/handle/10986/31053

Κατάλογος Συντομογραφιών

CSC: Criminal Smart Contracts

DLT: Distributed Ledger Technologies

eID: Electronic Identity

eIDAS: Electronic IDentification, Authentication and trust Services

IoT: Internet of Things

Η/Υ: Ηλεκτρονικός Υπολογιστής

ΤτΕ: Τράπεζα της Ελλάδος

Γλωσσάρι απόδοσης ξενόγλωσσων όρων

Agent-centric structure: Ενεργο-κεντρική δομή δεδομένων

Authentication: Πιστοποίηση αυθεντικότητας

Block: Ομάδα καταχωρήσεων

Ciphertext: Κρυπτοκείμενο

Chain: Αλυσίδα

Cloud: Υπολογιστικό 'νέφος' για αποθήκευση δεδομένων

Consensus: Συμφωνία εντός της αλυσίδας *Blockchain*

Credentials: Διαπιστευτήρια/πιστοποιητικά

Data-centric structure: Πληροφοριο-κεντρική δομή δεδομένων

Decentralized Autonomous Organisations (DAOs): Αποκεντρωμένοι Αυτόνομοι Οργανισμοί

Distributed ledger: Δημόσιο κατάστιχο

Distributed network of independent users: Αποκεντρωμένο δίκτυο ανεξάρτητων χρηστών

DLT (**Distributed Ledger Technology)**: Τεχνολογία σε δημόσιο κατάστιχο

DNS (**Domain Name System)**: Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών

EBA: Ευρωπαϊκή Αρχή Τραπεζών (Ε.Α.Τ.)

Fees: Έξοδα συναλλαγής

Fingerprint ή message digest: Σύνοψη μηνύματος

Fork: 'Πιρούνι' από το οποίο χωρίζουν δυο διαφορετικές αλυσίδες *Blockchain*

Hashing: Μέθοδος σύνδεσης του ενός block με το επόμενο

ID (**identity)**: Αστική ταυτότητα

ID4D - **Identification for Development:** Ταυτοποίηση για Ανάπτυξη

Identification: Ταυτοποίηση

Immutability: Σταθερότητα/ Στατικότητα

Κρυπτοκείμενο: Κρυπτογραφημένα δεδομένα

Message Digest: Σύνοψη μηνύματος

Miners: Ανεξάρτητα μέλη ή οργανισμοί που κινούν το δίκτυο Bitcoin και κυβερνούν την υπολογιστική δύναμη

Mining: Κατανεμημένο συναινετικό σύστημα ή αλλιώς διαδικασία εξόρυξης

Mining Pool: Συγκέντρωση μεμονωμένων χρηστών δημιουργώντας ομάδες για την πραγμάτωση περισσότερο αποτελεσματικής διαδικασίας εξόρυξης.

Mixing Protocols: Μικτά πρωτόκολλα

Node: Κόμβος

Nonce: Μετρητής εντός της διαδικασίας εξόρυξης

One way hash: Συνάρτηση κατακερματισμού

P2P (**peer-to-peer)**: Ομότιμη σύνδεση

Plaintext: Απλό κείμενο

PoW (**Proof of work)**: Βλ. Γλωσσάρι ερμηνείας κύριων όρων

Privacy: Ιδιωτικότητα

RFID (Radio Frequency Identification): Ταυτοποίηση μέσω ραδιοσυχνοτήτων

Security: Ασφάλεια

Seed: Φύτρο

Template contracts: Συμβάσεις - πρότυπα, συμβάσεις προσχώρησης.

Third-Party Mixing: Τριτομερή μικτά δίκτυα

Timestamp: Χρονοσήμανση

Transaction fees: Έξοδα συναλλαγής

Transaction Types: Τύποι συναλλαγών

Γλωσσάρι ερμηνείας κύριων όρων

Byzantine fault tolerance: Αποτελεί μια συνθήκη ενός υπολογιστικού συστήματος, ειδικά ενός αποκεντρωμένου, όπου κάποιοι κόμβοι δύναται να αποτύχουν στην επικοινωνία και όπου δύναται να υπάρχει ελλιπής πληροφόρηση ως προς το γεγονός αυτό. Ο ορισμός αυτός έχει πάρει το όνομα από μια αλληγορία, εκείνη του 'Byzantine Generals Problem', όπου διάφοροι παράγοντες συμφωνούν ως προς μια συγκεκριμένη στρατηγική, κάποιοι από αυτούς όμως δεν είναι ''έμπιστοι'.

Consortium Blockchain: Αποτελεί ένα ημι-ιδιωτικό σύστημα μιας ελεγχόμενης ομάδας χρηστών που λειτουργεί διαμέσου διαφορετικών οργανισμών και ειδικότερα εταιρειών για την προώθηση της εργασίας, της λογιστικής και της διαφάνειας.

DAOs (Decentralized Autonomous Organisations): Πρόγραμμα Η/Υ που χρησιμοποιεί το Blockchain τηρώντας καθαρά επιχειρηματικής λογικής κανόνες (Business logic).

Distributed consensus: Η 'αποκεντρωμένη συμφωνία' αποτελεί τον ακρογωνιαίο λίθο της αλυσίδας Blockchain καθώς επιτρέπει σ'αυτήν την τελευταία να παρουσιάσει μια μόνο 'αλήθεια' που έχει συμφωνηθεί από όλους τους χρήστες χωρίς καμία ειδική αδειοδότηση ή έλεγχο από οποιαδήποτε κεντρική αρχή.

DNS: Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών, που χρησιμοποιούν το πρωτόκολλο IP. Αντιστοιχίζει τα ονόματα των υπολογιστών υπηρεσίας σε διευθύνσεις IP[113].

Mining (Διαδικασία εξόρυξης): Κάθε συναλλαγή που γίνεται στο δίκτυο του Bitcoin, ελέγχεται για την εγκυρότητά της και στη συνέχεια τοποθετείται σ' ένα μπλοκ μαζί με άλλες συναλλαγές που έχουν ελεγχθεί. Κάθε δέκα λεπτά, δημιουργείται και ένα νέο block για να φιλοξενήσει αυτές τις συναλλαγές, το οποίο σχετίζεται με το αμέσως προηγούμενο. Ένας μαθηματικός αλγόριθμος χρησιμοποιείται για να γίνει ο συσχετισμός του νέου μπλοκ με τα προηγούμενα. Μόλις βρεθεί η λύση του αλγόριθμου τότε θα δημιουργηθεί το νέο αυτό μπλοκ και μαζί με αυτό θα δημιουργηθεί κι ένας συγκεκριμένος αριθμός νέων Bitcoins, τα οποία θα αποδοθούν σε αυτόν ή αυτούς που βρήκαν τη λύση. Αυτή η διαδικασία ονομάζεται «Mining» κι έχει πάρει το όνομά της ως μια σύγχρονη αναπαράσταση των χρυσωρύχων του περασμένου αιώνα[114].

Nodes (Κόμβος): Ένας κόμβος σε μια αλυσίδα Blockchain μπορεί να διενεργεί διάφορες λειτουργίες. Δύναται να επιβεβαιώνει συναλλαγές και να πραγματοποιεί τη διαδικασία της εξόρυξης για να διευκολύνει τη συμφωνία και να διασφαλίσει την αλυσίδα συνήθως μέσω ενός Πρωτοκόλλου συμφωνίας (όπως το PoW).

[113] Ανάκτηση από: www.cerebrux.net
[114] Ανάκτηση από: www.bitcoinx.gr

Peer-to-peer network (Δίκτυο ομότιμης σύνδεσης): Δίκτυο όπου όλα τα μέρη μπορούν να επικοινωνήσουν μεταξύ τους στέλνοντας και λαμβάνοντας μηνύματα.

Proof of work (PoW): Εμπλέκει πληθώρα ενεργοποιημένων κόμβων του δικτύου ώστε να επιλυθεί σε πρώτο χρόνο ένα περίπλοκο μαθηματικό πρόβλημα και σε δεύτερο χρόνο να επιβραβευθεί ο χρήστης με το κλείσιμο της συναλλαγής του στο μπλοκ.

Proof of stake: Εμπλέκει χρήστες που διαθέτουν μεγάλες ποσότητες από 'tokens' (νομίσματα) ώστε εντός του συστήματος να επιλεγούν τυχαία για να συμφωνήσουν να κλείσουν ένα μπλοκ από συναλλαγές.

Proof of authority: Εμπλέκει την έκδοση ενός είδους αδειοδότησης στο δίκτυο κάποιων μελών τα οποία θα αναλάβουν να κλείσουν ένα μπλοκ συναλλαγών.

Scripting/programming language (Γλώσσα προγραμματισμού ή κρυπτογράφησης): Διενεργεί διάφορες λειτουργίες εντός μιας συναλλαγής. Οι κρυπτογραφήσεις της συναλλαγής είναι προκαθορισμένα πρότυπα εντολών ώστε οι κόμβοι να μεταφέρουν νομίσματα (tokens) από μια διεύθυνση σε μια άλλη. Η ασφάλεια της γλώσσας προγραμματισμού συνδέεται άμεσα με την ασφάλεια στο δίκτυο της αλυσίδας κόμβων.

Transaction (Συναλλαγή): Θεμέλιος λίθος της αλυσίδας μπλοκ (Blockchain). Μια συναλλαγή αναπαριστά μια μεταφορά αξιών από μια διεύθυνση σε μια άλλη.

Αυθεντικοποίηση: Διαδικασία επιβεβαίωσης των προσωπικών δεδομένων με την είσοδο αυτών στο σύστημα. Αποδίδεται με τον όρο 'πιστοποίηση αυθεντικότητας'.

Αδειοδότηση: Στην ορολογία της ταυτοποίησης, η αδειοδότηση αναφέρεται στο ρόλο των παραγόντων που κρατούν την προσωπική πληροφορία. Το σημαντικό είναι η σωστή διαχείριση των δεδομένων, η κατά το δυνατόν ελαχιστοποίηση των δεδομένων προς αποθήκευση και πρόσβαση από αυτούς τους τρίτους παράγοντες και ο προγραμματισμός και η τήρηση μιας ορθής πολιτικής προσωπικών δεδομένων από τη πλευρά αυτών.

Βιομετρική πληροφορία : Τα ανθρώπινα γνωρίσματα που συνθέτουν την ταυτότητα ενός ατόμου, όπως τα χαρακτηριστικά του προσώπου, τα μάτια, ακόμη και ο σφυγμός.

Κρυπτονόμισμα: Είναι μία *peer-to-peer* αποκεντρωμένη ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών[115].

Κρυπτογράφηση: Στηρίζεται στη μετατροπή ενός μηνύματος σε ακατάληπτη μορφή η οποία δεν μπορεί να αναγνωστεί εάν δεν αποκρυπτογραφηθεί.

[115] Ανάκτηση από: www.iml-greece.gr/crypto/

Παράρτημα Α : Θέματα

- Το οικοσύστημα του κρυπτονομίσματος Bitcoin στην Ελλάδα

Στο σύστημα *Bitcoin*, ο καθένας έχει πρόσβαση σε ολόκληρο τον κώδικα ανά πάσα στιγμή. Όλες οι πληρωμές μπορούν να γίνουν χωρίς εξάρτηση από τρίτους και ολόκληρο το σύστημα προστατεύεται από έντονα επιθεωρημένους από ομότιμους κρυπτογραφικούς αλγόριθμους όπως εκείνους που χρησιμοποιούνται στις online τραπεζικές συναλλαγές, όπως αναφέρει και η επίσημη ιστοσελίδα του Bitcoin Project[116].

Στην Ελλάδα, οι επιχειρήσεις είναι εκείνες που έχουν δώσει το παρόν σε ό,τι αφορά τα κρυπτονομίσματα ενώ πραγματική 'επανάσταση' ακόμα δεν υπάρχει. Ίσως λόγω της άγνοιας πολλών, της έλλειψης εμπιστοσύνης στο σύστημα ίσως ακόμη λόγω των συχνών ανακοινώσεων τόσο τραπεζικών φορέων (ΤτΕ) όσο και οργάνων της ΕΕ που δηλώνουν το 'επικίνδυνο' της διαδικασίας. Ειδικότερα, η Ευρωπαϊκή Κεντρική Τράπεζα απορρίπτει την υπαγωγή του *Bitcoin* στις διατάξεις της άνω Οδηγίας. Επίσης, δεν θεωρεί τα εικονικά νομίσματα πλήρεις μορφές χρήματος, στο βαθμό που δεν πληρούν τη λειτουργία του χρήματος ως μονάδας μέτρησης, ως μέσου ανταλλαγής και ως μέσου αποθήκευσης αξίας (https://www.capital.gr/meapopsi/3272145/bitcoin-kai-kruptonomismata). Η Ευρωπαϊκή Αρχή Τραπεζών προτείνει το χαρακτηρισμό «προϊόν» σε ο,τι αφορά το Bitcoin (*commodity*) και επισημαίνει τους κινδύνους που προέρχονται από την αγορά, την κατοχή ή την εμπορία εικονικών νομισμάτων (https://www.capital.gr/meapopsi/3272145/bitcoin-kai-kruptonomismata).

Το σημαντικό είναι ότι έχουν ειπωθεί κάποια σχέδια και πρωτοβουλίες για 'έξυπνες πόλεις' στη χώρα με έμφαση στο Blockchain, χωρίς να έχουν υλοποιηθεί ακόμη κυρίως λόγω της περαιτέρω ανάπτυξης που χρειάζεται η τεχνολογία. Παρά ταύτα, το 'επιχειρείν' εντάσσει όλο και περισσότερο την χρήση του Bitcoin, κυρίως λόγω της ταχύτητας και της αξιοπιστίας του, ιστορικά και τεχνικά. Έχει υποστηριχθεί μάλιστα ότι κατά την περίοδο των 'καπιταλ κοντρόλ' στην Ελλάδα είχε παρατηρηθεί αύξηση στις συναλλαγές με Bitcoin *(*https://www.insider.gr/hristika/ependyseis/68904/oiellines-agorazoyn-bitcoin-para-ta-capital-controls).

[116] www.bitcoin.org

- Μελλοντικές πρωτοβουλίες για ηλεκτρονική ταυτοποίηση με Blockchain

Η πρωτοβουλία της κυβέρνησης του Ντουμπάι βασιζεται σε ένα αρκετά φιλόδοξο σχέδιο μετατροπής και μετακίνησης όλων των κυβερνητικών εγγράφων και συστημάτων στο Blockchain μέχρι το 2020. Η πρωτοβουλία να καταργηθεί το 'χαρτί' ενισχύει την αποτελεσματικότητα σε όλους τους επικείμενους τομείς. Η τεχνολογία, που θα βασίζεται στην απλή καταχώρηση προσωπικών στοιχείων, θα ευνοεί τις διασυνοριακές δραστηριότητες, άλλη μια επιτυχία του Blockchain . Πρακτικά, αυτό που θα αποθηκεύεται δεν θα είναι η ταυτότητα αυτή καθεαυτή αλλά μια ταυτοποιημένη συναλλαγή ή επιβεβαίωση της ταυτότητας. Ένα άλλο παράδειγμα αποτελεί αυτό της Εσθονίας. Μετά την έξοδό της από τη Σοβιετική Ένωση η χώρα ανέπτυξε το πεδίο της τεχνολογίας μέχρι να παρέχει στους ενδιαφερομένους σχεδόν όλες τις υπηρεσίες της ηλεκτρονικά. Έχει προσκαλέσει διάφορους παράγοντες και σχεδιαστές λογισμικού για την ανάπτυξη εφαρμογών προς τους πολίτες με την τεχνολογία Blockchain. "Εντός σχεδίου" βρίσκεται και η Μεγάλη Βρετανία όπου υποστηρίζεται και προωθείται η ιδέα η τεχνολογία να αξιοποιηθεί για την πρόληψη της απάτης, της διαφθοράς, αλλά και την βελτίωση των σχέσεων πολίτη-κρατικού μηχανισμού.

- Η πρωτοβουλία *SINGPASS*

Σε ένα αντίστοιχο επίπεδο, κινείται και η Σιγκαπούρη και το Smart Nation project το οποίο αφορά πρωτοβουλίες για πρακτικές πληρωμών. Εν προκειμένω, τα κρυπτονομίσματα θα μπορούν να χρησιμοποιούνται για να εγγυάται η ιδιωτικότητα μετά από πραγματοποιημένες συναλλαγές. Και η τεχνολογία του 'ίντερνετ-των-πραγμάτων' δεν θα μείνει βέβαια εκτός. Αν και η Σιγκαπούρη δεν έχει παρουσιάσει ακόμα την ηλεκτρονική ταυτοποίηση (e-id) ως την επίσημη αστική ταυτοποίηση, ωστόσο, έχει ήδη ξεκινήσει η λειτουργία εφαρμογών για τις συναλλαγές μεταξύ πολιτών και κράτους. Έτσι, στο πλαίσιο της πρωτοβουλίας Smart Nation και μέσω της ταυτοποίησης *singpass*, φορολογικές, οικονομικές, διοικητικές και κρατικού τύπου συναλλαγές πραγματοποιούνται μέσω του συστήματος. Η πρωτοβουλία της ηλεκτρονικής πλέον ταυτοποίησης θα ξεκινήσει το 2020. Για περισσότερες πληροφορίες στις επίσημες ιστοσελίδες:

https://www.singpass.gov.sg/singpass/common/aboutus

https://www.smartnation.sg/what-is-smart-nation/initiatives/Strategic-NationalProjects/national-digital-identity-ndi

Παράρτημα Β : Συνέντευξη για τις Ψηφιακές Υπογραφές ΕΚΠΑ

Συνέντευξη Πτυχιακής εργασίας με τον κο *Νικόλαο Λάριο*

Ψηφιακές Υπογραφές ΕΚΠΑ

Γιαννάκου Μαρία-Αγγελική (Συν.)

Συνεντεύκτρια: Ψηφιακές υπογραφές στον ακαδημαϊκό χώρο : τι είναι, πότε ξεκίνησε, σε ποιους απευθύνεται και ποια τα κίνητρα/αίτια αυτής της τεχνολογίας;

Νικόλαος Λάριος: Η ψηφιακή υπογραφή είναι προσωπικά ψηφιακά πιστοποιητικά αυθεντικοποίησης / υπογραφής και κρυπτογράφησης που μπορεί ο υπογράφων, να διατηρήσει υπό τον αποκλειστικό του έλεγχο (κάρτα ή ειδική συσκευή usb) σύμφωνα με τα όσα ορίζει το άρθρο 2 του ΠΔ 150/2001, όπως αναφέρει και η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)[117]. Στον ακαδημαϊκό χώρο ξεκίνησε το 2008 έγινε όμως ευρέως διαδεδομένη το 2015 που δόθηκε η δυνατότητα στα μέλη της ακαδημαϊκής κοινότητας να αποκτήσουν δωρεάν Ακαδημαϊκή Ταυτότητα[118]. Οι ψηφιακές υπογραφές απευθύνονται σε όλα τα μέλη της Πανεπιστημιακής Κοινότητας που χρειάζονται ασφαλή ανταλλαγή εγγράφων και ηλεκτρονικού ταχυδρομείου, υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων, ασφαλή προσδιορισμό της ηλεκτρονικής ταυτότητας, έλεγχο πρόσβασης σε κατάλληλες εφαρμογές κ.α, όπως γίνεται αναφορά και στην επίσημη ιστοσελίδα του Υπουργείου Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης[119]. Το μεγαλύτερο κίνητρο είναι η διασφάλιση της ταυτότητας των διακινούμενων εγγράφων καθώς και η εξοικονόμηση 400 εκ. ευρώ ανά έτος με την κατάργηση του χαρτιού και των παράπλευρων διαδικασιών κατά την έκδοση διοικητικών εγγράφων και πράξεων σύμφωνα με τον ΙΟΒΕ.

Συν.: Σε τεχνικό επίπεδο, σε ποια τεχνολογία βασίζεται;

Ν. Λ.: Όπως αναφέρει και η ιστοσελίδα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων [120], οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού κατά την οποία ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια ώστε αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να

[117] www.aped.gov.gr
[118] https://ellak.r/2015/07/psifiaki-ipografi-engrafon-me-ti-chrisi-tis-akadimaikis-taftotitas/
[119] www.yap.gov.gr
[120] eett.gr

υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος και μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από τη σύνοψη, που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά τη μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Συν. : Έγινε γρήγορα αποδεκτό από τους χρήστες;

Ν. Λ.: Το 2015 που τα περισσότεροι μέλη της Πανεπιστημιακής Κοινότητας ξεκίνησαν να δημιουργούν τις ακαδημαϊκές τους ταυτότητες, δυστυχώς δεν υπήρχαν οι διαδικασίες ταυτοποίησης και έκδοσης των ψηφιακών υπογραφών στο Ίδρυμα μας με την μορφή που αυτό γίνεται σήμερα. Οι περισσότεροι παρέλαβαν τις κάρτες χωρίς καταρχήν να αντιληφθούν ότι χρειάζονται ενεργοποίηση. Με αποτέλεσμα από το 2016 που άρχισε να γίνεται γνωστή η χρήση της ακαδημαϊκής κάρτας για ψηφιακή υπογραφή να υπάρχουν αρκετά προβλήματα κυρίως αδυναμίας ενεργοποίησης εξαιτίας χαμένου κωδικού ή μηνύματος ενεργοποίησης.

Συν. : Ποιο το κόστος της τεχνολογίας για την κατασκευή, την εγκατάσταση, τη συντήρηση και τον τελικό χρήστη;

Ν. Λ.: Το κόστος της τεχνολογίας για το Ίδρυμα μας είναι το ελάχιστο δυνατό. Οι ακαδημαϊκές ταυτότητες προμηθεύονται δωρεάν από το Υπουργείο Παιδείας, Έρευνας και Θρησκευμάτων. Ενδεικτικά αναφέρεται ότι ο card reader της κάρτας που δίδεται μαζί με την κάρτα έχει κόστος περίπου σαράντα ευρώ. Το λογισμικό για την εγκατάσταση παρέχεται επίσης δωρεάν. Συντήρηση δεν χρειάζεται πέρα από την ανανέωση της ψηφιακής υπογραφής κάθε δύο χρόνια.

Συν. : Πιστεύετε ότι θα φέρει την αλλαγή στην 'ταυτοποίηση';

Ν. Λ.: Έχει ήδη φέρει την αλλαγή στην 'ταυτοποίηση' και φυσικά ενδεικτικό είναι ότι όλες οι προμήθειες και οι διαγωνισμοί του δημοσίου δεν νοούνται πλέον χωρίς την χρήση της ψηφιακής υπογραφής τόσο από τις αναθέτουσες αρχές όσο και από τους προμηθευτές. Το ίδιο φυσικά ισχύει και στο ΕΚΠΑ σε λίγο μικρότερο φυσικά βαθμό.
Συν. : Τι θετικά γνωρίσματα έχει η τεχνολογία των ψηφιακών υπογραφών;

Ν. Λ.: Τα θετικά γνωρίσματα είναι αρκετά με βασικότερο όμως την ενίσχυση της ασφάλειας. Ειδικά όταν πρόκειται για τη διαφύλαξη εμπιστευτικών πληροφοριών, μια ηλεκτρονική υπογραφή είναι το σημαντικότερο πράγμα που μπορεί κάποιος να έχει. Φυσικά άμεσο επακόλουθο είναι και η βελτίωση της ροή των ψηφιακών εργασιών και η εξοικονόμηση χρόνου αλλά και χαρτιού με το αντίστοιχο κόψιμο του κόστους. Τόσο το χαρτί όσο και το κόστος εκτύπωσης απορροφούν τμήμα της χρηματοδότησης του ΕΚΠΑ που θα μπορούσε να πάει σε άλλες υποδομές.

Συν.: Τι αρνητικά στοιχεία μπορεί να υπάρχουν και τι προβλήματα προκύπτουν ή ενδεχομένως να προκύψουν;

Ν. Λ.: Μέχρι στιγμής δεν υπάρχουν κάποια αρνητικά στοιχεία ή προβλήματα πέρα από την ανάγκη εξοικείωσης των μελών της Πανεπιστημιακής Κοινότητας με την συγκεκριμένη τεχνολογία. Είναι κάτι που δεν το γνωρίζουν πλήρως παρόλο που είναι πολύ εύκολο στην χρήση.

Συν.: Ποιος είναι ο επόμενος 'στόχος' των ψηφιακών υπογραφών και της ηλεκτρονικής ταυτοποίησης εν γένει σύμφωνα με την δική σας εμπειρία;

Ν. Λ.: Από τις αρχές του έτους θα έπρεπε να είχε ξεκινήσει η κατάργηση του χαρτιού στο δημόσιο. Αυτό ουσιαστικά σημαίνει ότι τουλάχιστον 23.000 φορείς δεν θα διακινούν χαρτί μεταξύ τους. Προς το παρόν τόσο σε επίπεδο ΕΚΠΑ όσο και λοιπής δημόσιας διοίκησης κάτι τέτοιο δεν έχει γίνει.

Συν.: Ποια τα αδύναμα/δυνατά σημεία της Ελλάδας σε ό,τι αφορά την υποστήριξη της τεχνολογίας αυτής;

Ν. Λ.: Μια εικόνα μόνο στον δείκτη DESI (https://ec.europa.eu/digital-singlemarket/en/desi) δείχνει την πολύ αδύναμη θέση της Ελλάδας στην Ψηφιακή Ευρώπη του σήμερα. Είμαστε στην προτελευταία θέση με χώρες σαν την Βουλγαρία μπροστά από εμάς. Δυστυχώς δεν δεχόμαστε καθολικές αλλαγές σαν λαός παρά μόνο υπό πίεση και κάτι τέτοιο συμβαίνει και στην υιοθέτηση των νέων τεχνολογιών. Το μόνο δυνατό σημείο μας σαν χώρα είναι ότι έχουμε τους επιστήμονες για να φέρουν την αλλάγή σε αυτή την τάση αν φυσικά το θελήσουμε.

Συν .: Ποιες είναι οι παγκόσμιες τάσεις/απειλές στο επίπεδο των ηλεκτρονικών υπογραφών;

Ν. Λ.: Παγκόσμια τάση είναι η μετάβαση από την ψηφιακή υπογραφή στην βιομετρική ταυτοποίηση με επακόλουθο την πιστοποίηση της ταυτότητας που αναγνωρίζει και εξακριβώνει τα άτομα με βάση τα φυσικά τους χαρακτηριστικά.

Δεδομένου του γεγονότος ότι τα βιομετρικά στοιχεία αποτελούν εγγενές τμήμα του κάθε ανθρώπου, τροφοδοτούν μια αυξανόμενη τάση να αντικαταστήσουν τα κλειδιά κρυπτογράφησης, τους κωδικούς πρόσβασης ή τους κωδικούς για ψηφιακή αναγνώριση και έλεγχο ταυτότητας. Από την αναγνώριση των δακτυλικών αποτυπωμάτων, την αναγνώριση των ίριδων και του αμφιβληστροειδούς, την αναγνώριση προσώπου, το βάδισμα, τη φωνή, το DNA, τα εγκεφαλικά κύματα και πολλά άλλα, κάθε μία από αυτές τις βιομετρικές τεχνολογίες μπορεί να χρησιμοποιηθεί για την αποτελεσματική αναγνώριση και εξακρίβωση της ταυτότητας του ανθρώπου, συνδυάζοντας φυσιολογικά ή συμπεριφορικά χαρακτηριστικά οποιουδήποτε ατόμου με τις πληροφορίες από ψηφιακές βάσεις δεδομένων που περιγράφουν την ταυτότητα του ατόμου. Καθώς οι νέες εφαρμογές βιομετρικών δεδομένων εξαπλώνονται, υπάρχει η ανάγκη καθορισμού αποτελεσματικών διαδικασιών και πολιτικών όπως έγινε στην περίπτωση των ψηφιακών υπογραφών. Λαμβάνοντας υπόψη τον αντίκτυπο που μπορεί να έχει στην ανθρώπινη κοινωνία, οι κίνδυνοι για το ιδιωτικό απόρρητο, τη διαλειτουργικότητα, την πολυτροπικότητα και τους πιθανούς κινδύνους για την υγεία (κίνδυνοι όρασης που σχετίζονται με σαρωτές αμφιβληστροειδούς κ.α.) πρέπει να αντιμετωπιστούν σε ορθολογική βάση και όσο το δυνατόν πιο αποτελεσματικά. Επίσης οι κίνδυνοι των δεδομένων από το hacking τέτοιον δικτύων εγείρουν επίσης ανησυχίες καθώς και η ικανότητα συστημάτων τεχνητής νοημοσύνης να θέτουν σε κίνδυνο τους βιομετρικούς δείκτες.

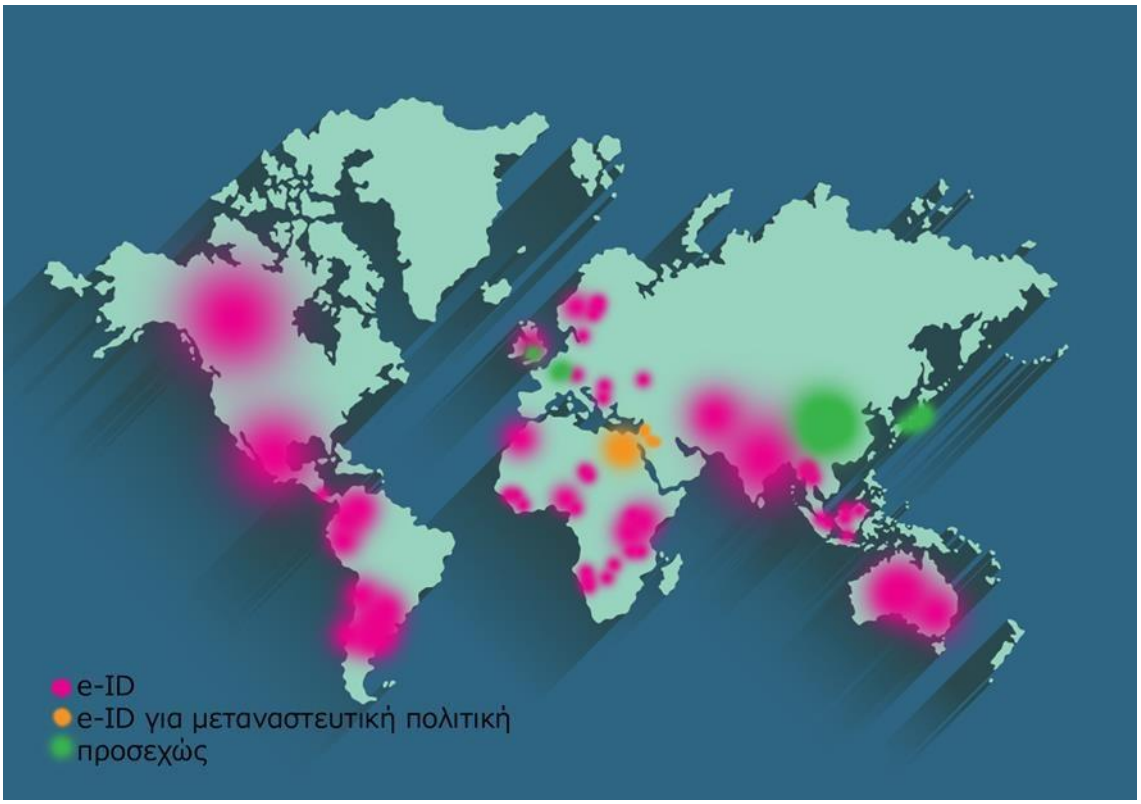
Συν.: Εάν η Ελλάδα προχωρούσε στο πεδίο της ηλεκτρονικής ταυτοποίησης (e-ID, digital ID) ποια πιστεύετε ότι θα ήταν τα θετικά σημάδια και ποια τα αρνητικά;

Ν. Λ.: Εντός της ΕΕ, περισσότεροι άνθρωποι από ποτέ ζουν, εργάζονται και ταξιδεύουν πέρα από χώρα σε χώρα. Ενώ όμως υπάρχει ελεύθερη κυκλοφορία και επιχειρηματική δραστηριότητα, ο διοικητικός φόρτος πρόσβασης σε δημόσιες και ιδιωτικές υπηρεσίες σε άλλες χώρες εξακολουθεί να είναι υψηλός. Περισσότερες από είκοσι ευρωπαϊκές χώρες διαθέτουν επί του παρόντος συστήματα eID, ωστόσο έχουν όλα διαφορετικούς μηχανισμούς ασφαλείας για τον εντοπισμό και την εξακρίβωση της γνησιότητας και βασίζονται σε διαφορετικές φιλοσοφίες που δεν διαθέτουν διασυνοριακή αναγνώριση και επικύρωση. Είναι προφανές ότι η πανευρωπαϊκή διαθεσιμότητα ευρείας και ασφαλούς πρόσβασης στις ηλεκτρονικές υπηρεσίες είναι απαραίτητη για τη συνεχιζόμενη οικονομική ανάπτυξη στην Ευρώπη και αποτελεί, ως εκ τούτου, ακρογωνιαίο λίθο στο δρόμο για την Ψηφιακή Ενιαία Αγορά (DSM). Βοηθώντας λοιπόν τα κράτη μέλη και ανάμεσα σε αυτά και την Ελλάδα να συμμορφωθούν με τον κανονισμό eIDAS, και eID της CEF προωθείται σημαντικά η επίτευξη του DSM. Στα θετικά σημάδια λοιπόν θα είναι ότι Έλληνες πολίτες θα έχουν την ελευθερία να έχουν πρόσβαση σε πολλές ηλεκτρονικές δημόσιες υπηρεσίες εντός της ΕΕ με άνευ προηγουμένου ευκολία, ενώ οι κυβερνήσεις και οι επιχειρήσεις θα είναι σε θέση να επεκτείνουν την εμβέλειά τους περισσότερο από ποτέ. Επιπλέον, οι κυβερνήσεις, οι επιχειρήσεις και οι πολίτες θα μπορούν να έχουν εμπιστοσύνη στα πρότυπα και τη διασφάλιση των συστημάτων eID στο δίκτυο eIDAS.

(https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Benefits+of+eID)

Αρνητικά σημάδια πέρα από παρόμοιες απειλές που αναφέραμε σε επίπεδο ψηφιακών υπογραφών δεν υπάρχουν.

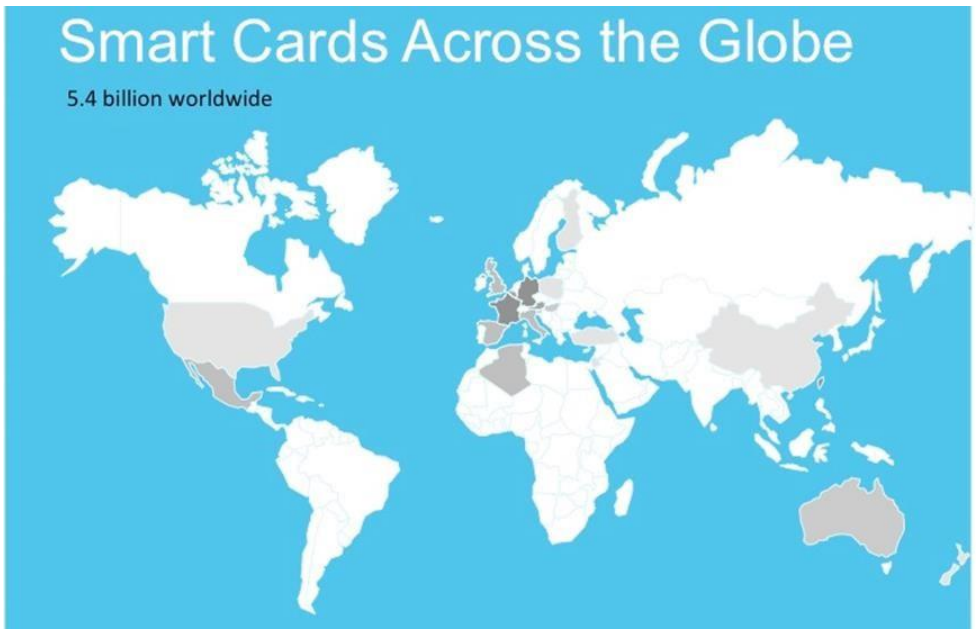
Παράρτημα Γ : Χάρτες



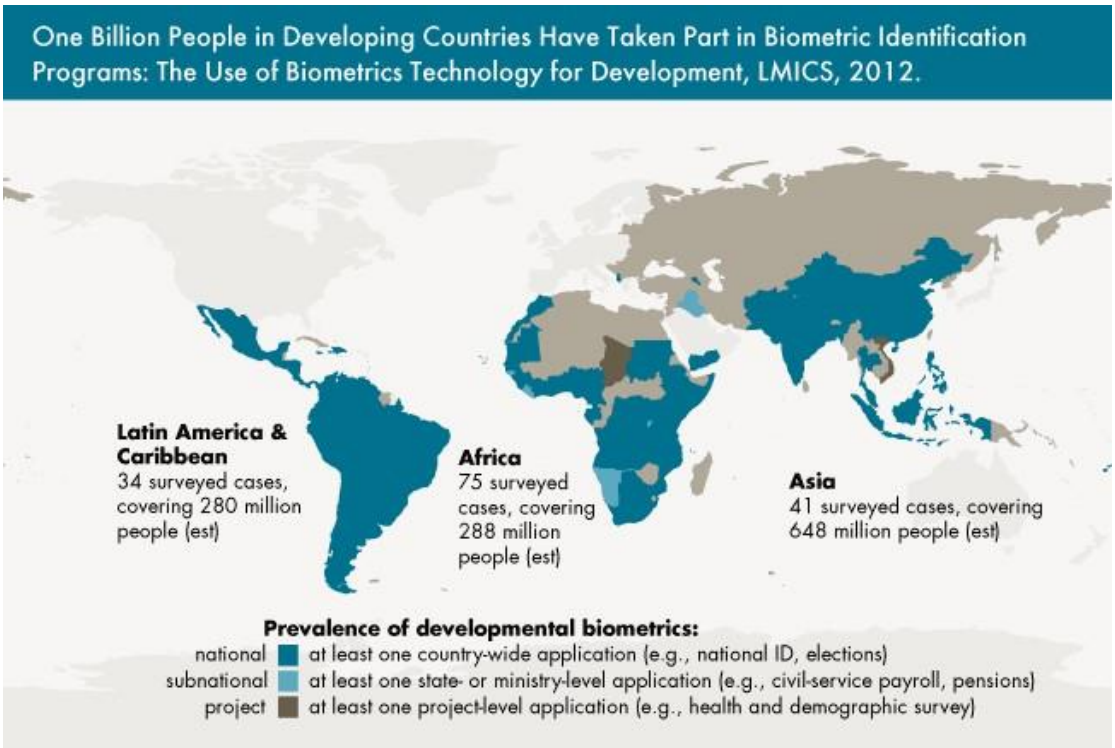
[Δημιουργήθηκε με Photoshop CS2]

Εικονίζονται οι εξής χώρες: Καναδάς, Μεξικό, Νορβηγία, Νιγηρία, Ινδία, Πακιστάν,, Ιορδανία, Λίβανο, Αίγυπτος, Μ. Βρετανία, Περού, Μορόκο, Ουγκάντα, Αργεντινή, Χιλή, Κολομβία, Εκουαδόρ, Κένυα, Μαλαισία, Παναμάς, Τανζανία, Ταϊλάνδη, Μολδαβία, Εσθονία, Αυστρία, Γουινέα, Καμερούν, Τσαντ , Μποτσουάνα, Ζάμπια, Ναμίμπια, Σιέρα Λεόνε, Ρουάντα, Λιβερία, Αλβανία, Φινλανδία, Σιγκαπούρη, Σερβία, Αυστραλία.

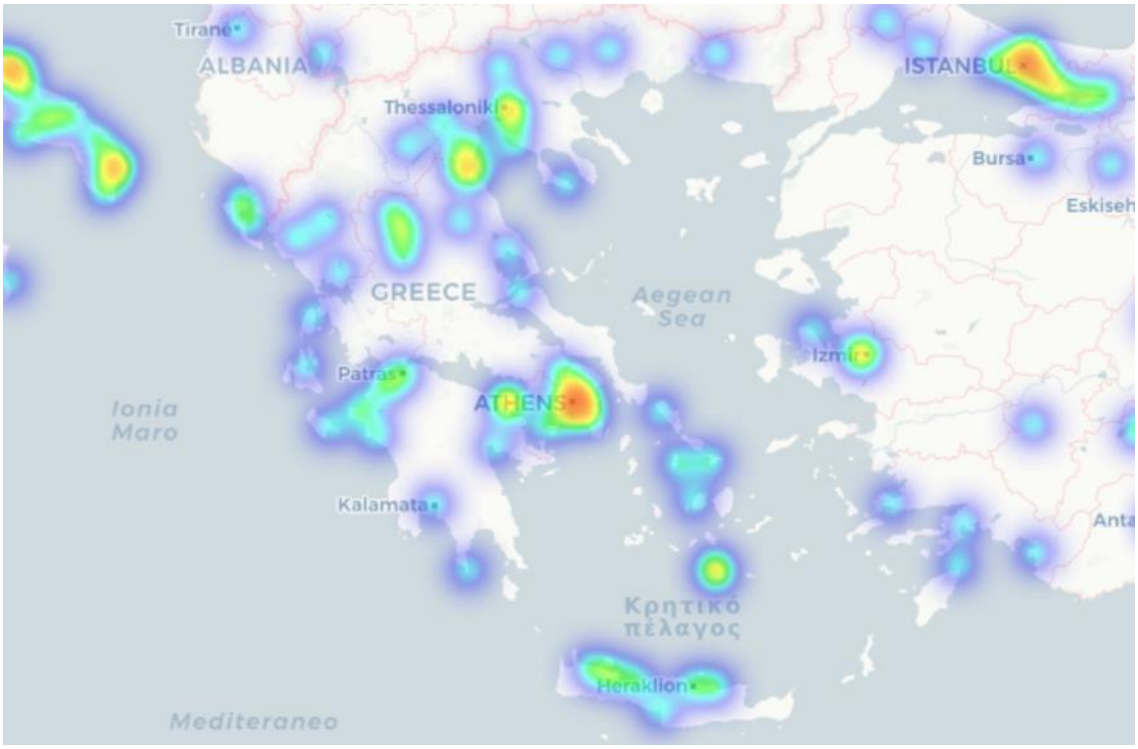
Προσεχώς: Ιαπωνία με Blockchain, Κίνα.



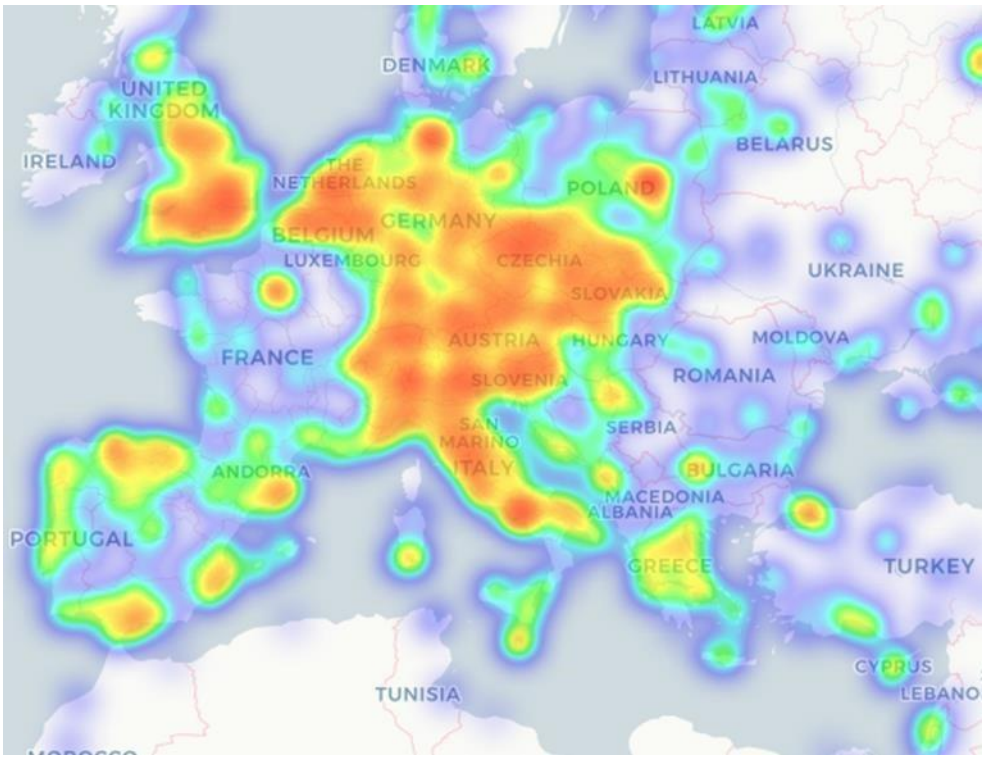
Εικόνα 13 Οι 'έξυπνες' κάρτες στον πλανήτη. Ανάκτηση από: http://itec200itreview.wikidot.com/team7spr10



Εικόνα 14 Οι αριθμοί για την ταυτοποίηση μέσω βιομετρικών δεδομένων. Ανάκτηση από: https://bioinformaticsknowledge.wordpress.com/worldwide/

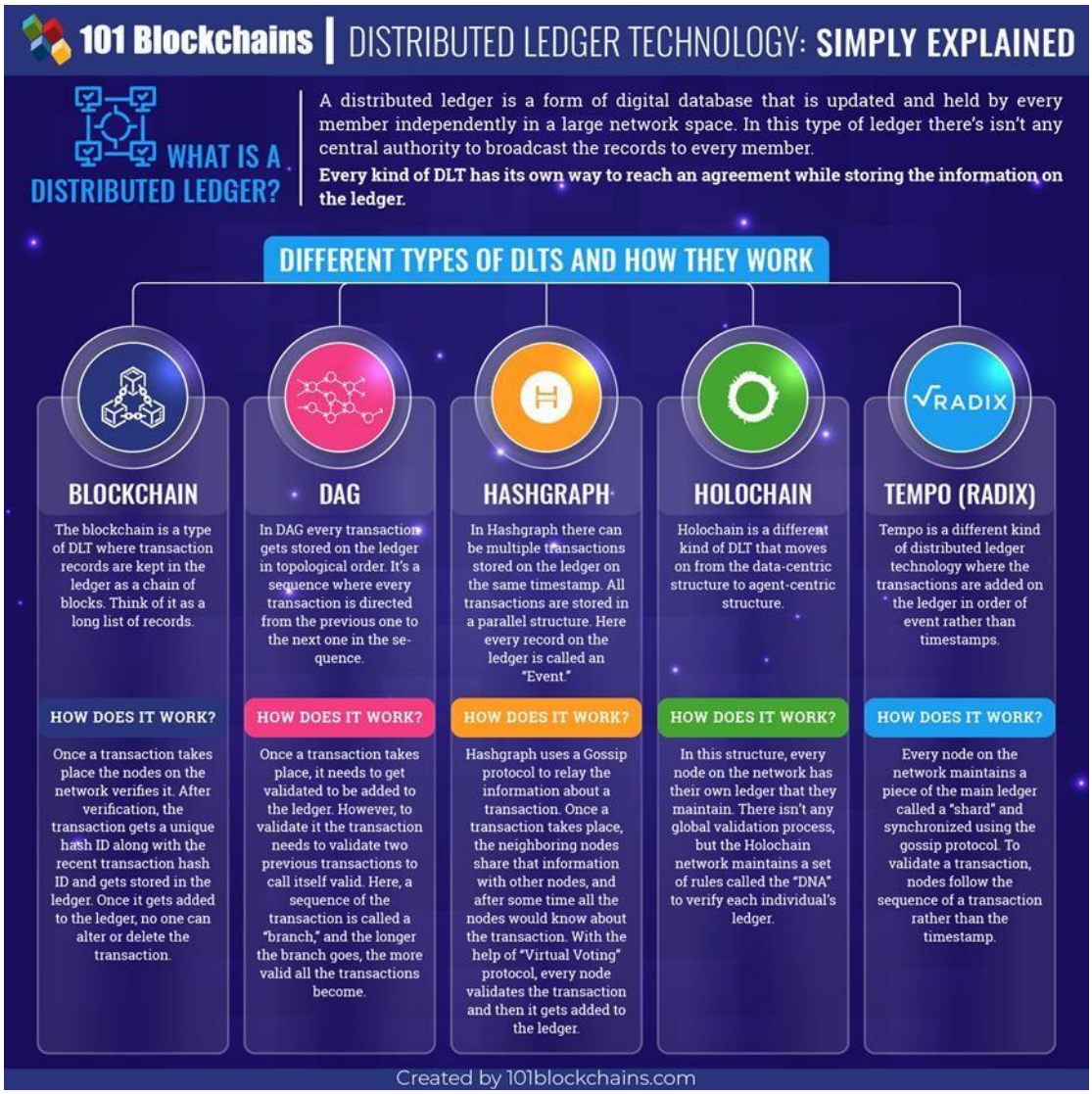


Εικόνα 15 Χρήση Bitcoin σε εθνικό επίπεδο. Ημερομηνία προσπέλασης 21/4/2019: https://coinmap.org/#/world/45.39844998/-0.52734375/3

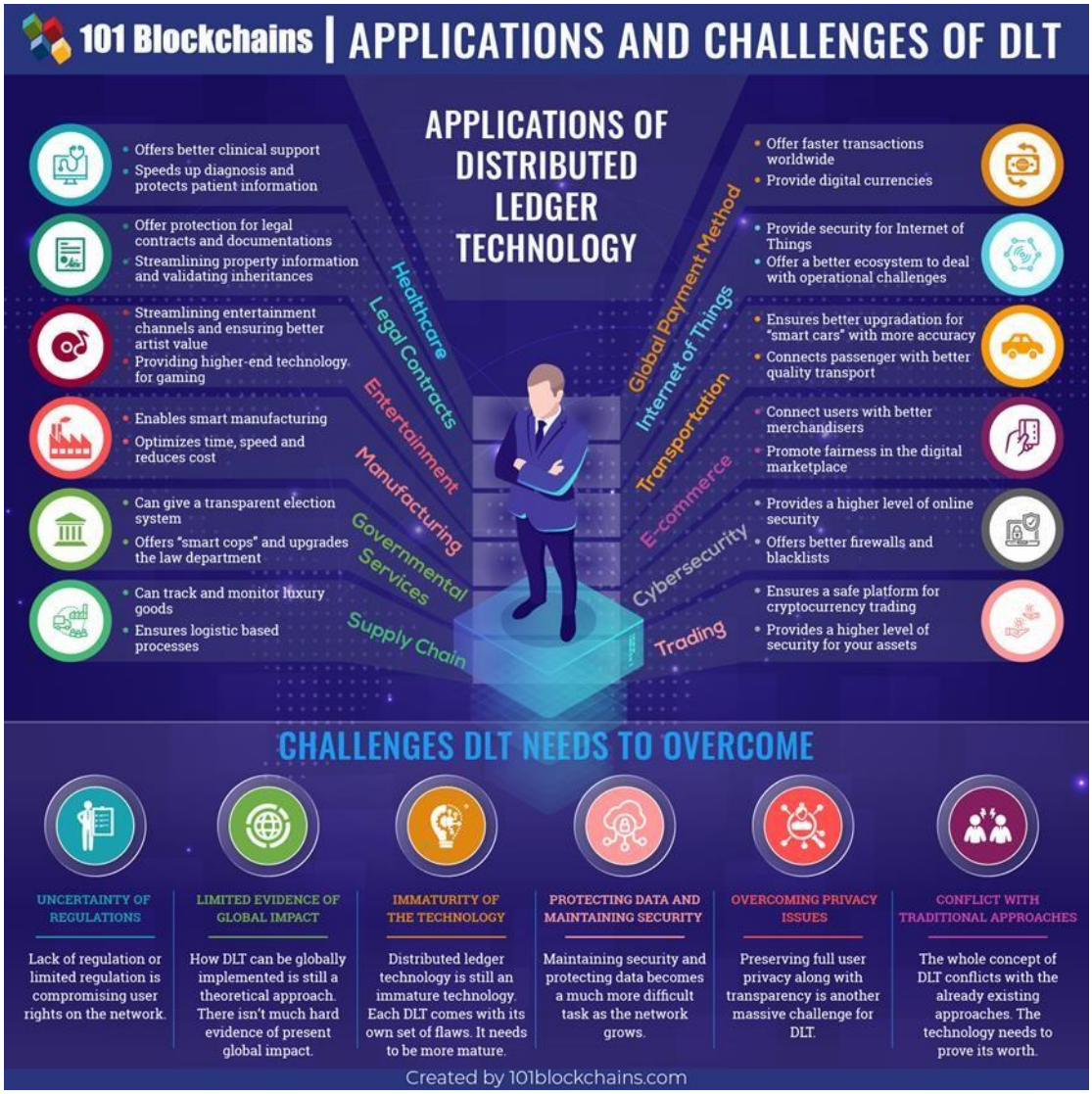


Εικόνα 16 Χρήση Bitcoin σε ευρωπαϊκό επίπεδο. Ημερομηνία προσπέλασης 21/4/2019: https://coinmap.org/#/world/45.39844998/-0.52734375/3

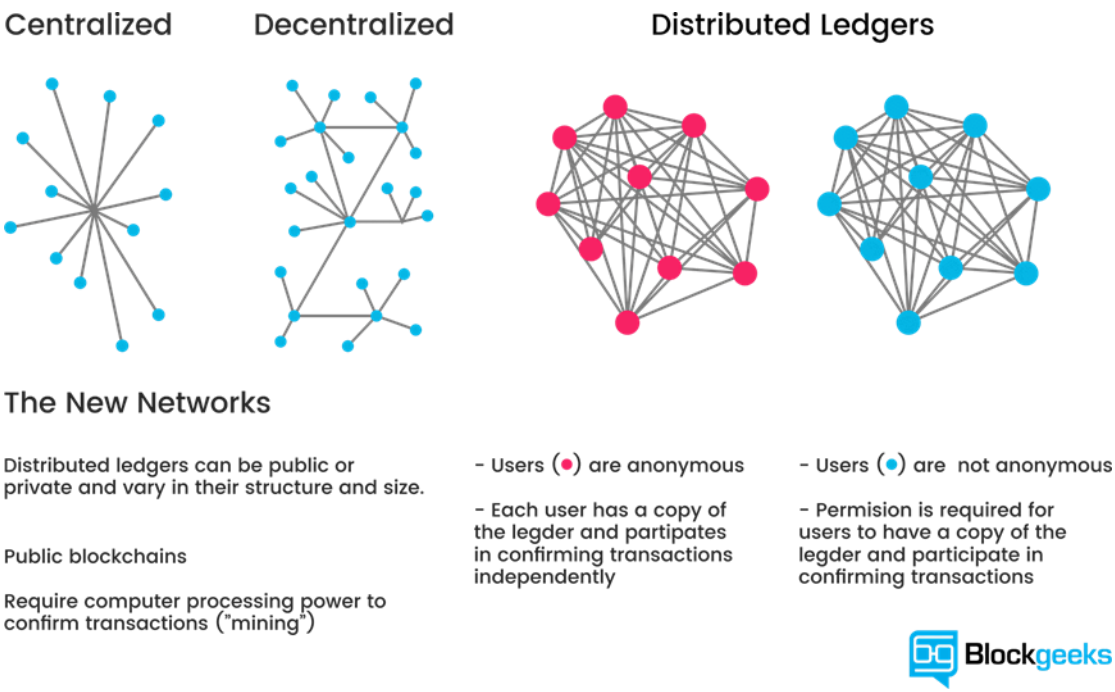
Παράρτημα Δ : Εικόνες – Πίνακες



Εικόνα 17 'Τι είναι η τεχνολογία DLT;' (Anwar, 2019)



Εικόνα 18 Εφαρμογές της τεχνολογίας DLT (Anwar, 2019)

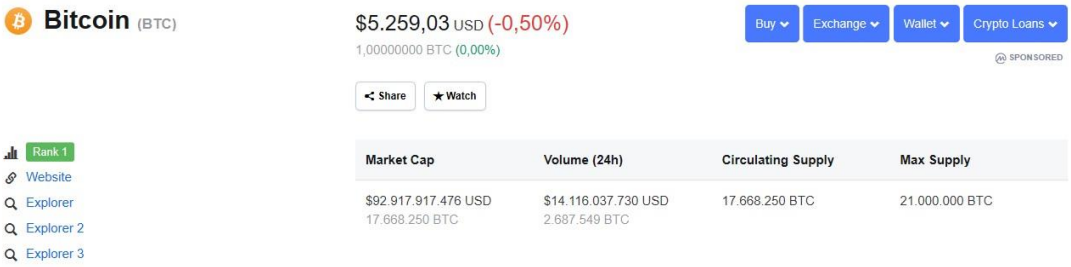


Εικόνα 19 Ένα αποκεντρωμένο και ένα κεντροποιημένο σύστημα. Ανάκτηση από: https://medium.com/@Brohit/helping-myself-understand-basics-of-blockchain-and-its-usecases-6f73fd40641

Bitcoin Statistics

Bitcoin Price	$5.259,03 USD
Bitcoin ROI	3.786,94%
Market Rank	#1
Market Cap	$92.917.917.476 USD
24 Hour Volume	$14.116.037.730 USD
Circulating Supply	17.668.250 BTC
Total Supply	17.668.250 BTC
Max Supply	21.000.000 BTC
All Time High	$20.089,00 USD (Dec 17, 2017)
All Time Low	$65,53 USD (Jul 05, 2013)
52 Week High / Low	$9.964,50 USD / $3.191,30 USD

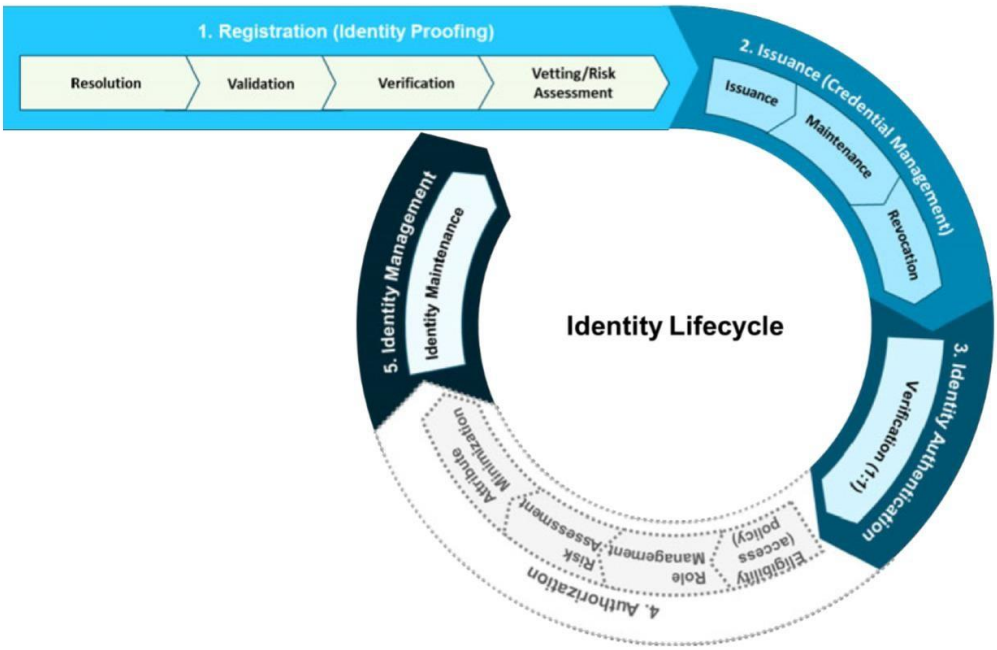
Εικόνα 20 Στατιστικά στοιχεία BTC, Ημερομηνία προσπέλασης 27/4/2019: https://coinmarketcap.com/currencies/bitcoin/



Εικόνα 21 Ισοτιμία BTC με δολάριο, Ημερομηνία προσπέλασης 27/4/2019: https://coinmarketcap.com/currencies/bitcoin/

#	Source	Pair	Volume (24h)	Price	Volume (%)	Category	Fee Type	Updated
1	BitMEX	XBT/USD	** $1.535.521.905	* $5.163,00	8,22%	Derivatives	No Fees	Recently
2	FCoin	BTC/USDT	** $1.368.959.338	$5.256,24	7,33%	Spot	Transaction Mining	Recently
3	Negocie Coins	BTC/BRL	$917.426.943	* $5.520,83	4,91%	Spot	Percentage	Recently
4	ZBG	BTC/USDT	** $556.367.474	$5.254,16	2,98%	Spot	Transaction Mining	Recently
5	Tidebit	BTC/USD	$503.672.140	* $5.012,50	2,70%	Spot	Percentage	Recently
6	CoinBene	BTC/USDT	$489.904.810	$5.255,25	2,62%	Spot	Percentage	Recently
7	BitForex	BTC/USDT	$441.962.168	$5.255,01	2,37%	Spot	Percentage	Recently
8	Coinall	BTC/USDT	** $401.096.842	$5.255,65	2,15%	Spot	Transaction Mining	Recently
9	BW.com	BTC/USDT	$397.895.133	$5.252,48	2,13%	Spot	Percentage	Recently
10	Coineal	LTC/BTC	$392.752.001	$5.263,79	2,10%	Spot	Percentage	Recently
11	OEX	BTC/USDT	$329.947.897	$5.256,26	1,77%	Spot	Percentage	Recently
12	DigiFinex	BTC/USDT	$264.062.832	$5.257,88	1,41%	Spot	Percentage	Recently
13	FCoin	ETH/BTC	** $254.226.669	$5.257,96	1,36%	Spot	Transaction Mining	Recently
14	LATOKEN	ETH/BTC	$237.186.297	$5.254,44	1,27%	Spot	Percentage	Recently
15	Bibox	BTC/USDT	$228.029.367	$5.255,46	1,22%	Spot	Percentage	Recently
16	IDAX	BTC/USDT	$222.326.383	$5.255,25	1,19%	Spot	Percentage	Recently

Εικόνα 22 Αγορά Bitcoin, Ημερομηνία προσπέλασης 27/4/2019: https://coinmarketcap.com/currencies/bitcoin/



Εικόνα 23 Ο κύκλος ζωής της ηλεκτρονικής ταυτοποίησης (World Bank Group, 2018α, σελ. 18)

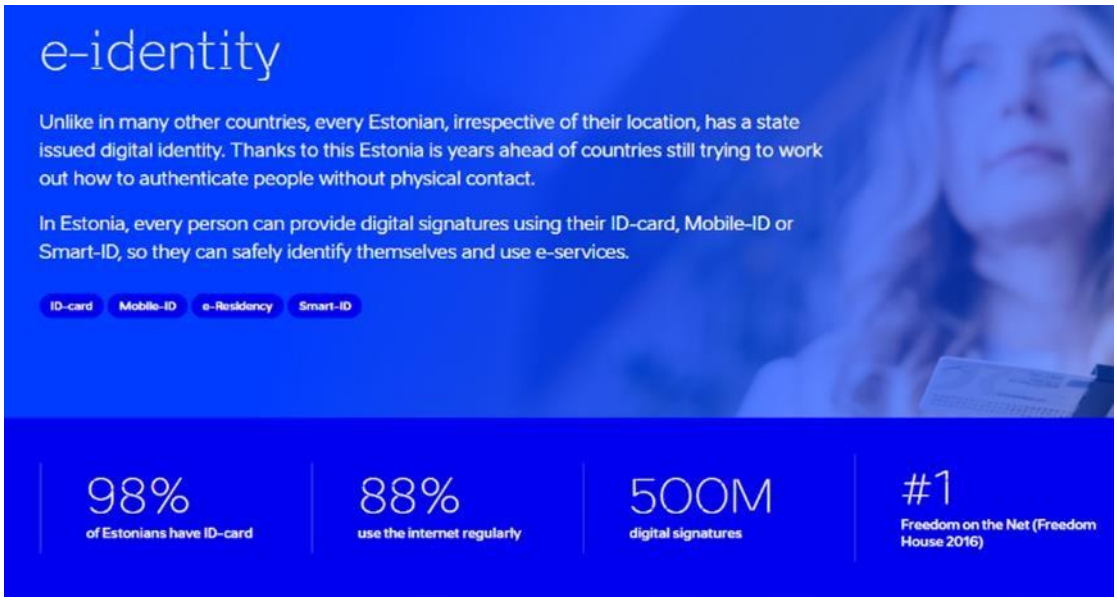
Πίνακας 13 Privacy by Design: Current Practices in Estonia, India, and Austria. (World Bank Group, 2018c., σελ. 8-11)

Table 3. Evaluation of India's Aadhaar Privacy by Design Features Based on Cavoukian's Eleven Fair Information Practices

S. No	Privacy principle	Indian system
1	**Purpose specification**	During the enrollment process, **the purposes** for which the data collected may be shared by UIDAI are explained and user consent and choice for sharing data captured. Demographic data sharing for electronic KYC is allowed for customer onboarding purposes only and requires user consent.
2	**Collection limitation**	**Minimal data are collected for enrolment for ID, namely** full name, address, date of birth and gender. The system also collects **multimodal biometrics**, namely. photograph, two irises, and ten fingerprints.
3	**Data minimization**	**Zero Semantics UIN**—The UIN (Aadhaar number) is a **random number** and does not on its own convey any meaning/information about the user. Linking of data across various systems/databases up until early 2018 was based on the Aadhaar number. In the light of increasing privacy and surveillance concerns, UIDAI recently launched the **virtual ID and tokenization features** discussed further in Box 1. • With the **tokenization** feature, instead of a UIN, a token which is calculated based on service provider code and Aadhaar number is used to identify the user in the service provider database, thus avoiding linkability of data across databases. • A **virtual ID** is a temporary ID number mapped to the UIN, that can be generated and used by a user instead of exposing the Aadhaar number. **Fingerprint and iris data are never shared.** **UIDAI certified biometric devices** used by service providers for authentication encrypt **the biometric** data captured from the user in the device itself before it reaches the service provider system, thus securing it. Data, when used for analytics purposes, are **anonymized** before sharing.

S. No	Privacy principle	Indian system
4	**Use, retention and disclosure limitation**	The biometric data are never shared by UIDAI with anyone. The biometric data provided by the user for authentication are not available to the service provider application as it is encrypted in the certified biometric devices before reaching the service provider application. KYC data consisting of demographic data and a photograph are shared by UIDAI with registered service providers only with user consent. No data are disclosed during authentication of users by UIDAI. Only a YES or NO response on an authentication request is given to service providers. The electronic Aadhaar, which is digitally signed by UIDAI, can be generated by the users on the portal. This can be used for offline authentication and KYC. The users can choose the demographic fields to be included in electronic Aadhaar, which enables them to limit the data that will be visible and shared with the service provider.
5	**Security**	The digital signature on the electronic Aadhaar ensures integrity and authenticity of the electronic Aadhaar document—enabling detection of any forgery of the Aadhaar document. This security feature enables it to be used for offline authentication and identity verification with a higher level of assurance. The Aadhaar also has two digitally signed Quick Response (QR) codes, one with photograph and demographic data and the other with demographic data only. The QR code, in both electronic Aadhaar or printed Aadhaar document, can be used for electronic capture of demographic data during offline KYC/authentication. The QR code prevents the data to be read visually without a QR code reader and the digital signature validation of the QR code enables detection of fake /forged Aadhaar's. All the data are **encrypted** and **digitally signed** and transmitted over a secure communication channel when sharing data between systems. Data is stored in **encrypted f**ormat and not exposed/available even for admin user or other type of user in plain text format The transaction logs are time stamped and digitally signed making them **tamper proof.** Any change would make the digital signature invalid. Users and systems are **authenticated and authorization** rules enforced before providing access to services (API's) or administrative functions. **Data tampering** is prevented by ensuring that data updates can only be done by authorized applications and not through command line queries/scripts. **Data is partitioned** and held in multiple database systems, with a random alias being the only link, which ensures that there is no centralised data table where all resident data is available. Access to the API's and hence to the CIDR is through a **network of trusted service providers (AUA and ASA)** only. Users can **lock/unlock** the use of **biometrics** to disable/enable biometric-based authentication.

S. No	Privacy principle	Indian system
6	**Accountability**	The **automated tamper proof logging** of transactions performed after successful authentication of users/systems holds people/systems accountable for data access. Internal system users also continuously monitor these logs/reports for violations. Users are **notified through registered e-mail/SMS of authentication attempts,** though access to e-mail/phones limits the universality of this feature. The **Aadhaar Act and IT Act** stipulates heavy penalties for unauthorized access to data. AUA and ASA sign agreements with UIDAI to access UIDAI services.
7	**Openness**	Access to the **time stamped and digitally signed** logs of all transactions where the user data was accessed ensures authenticity, integrity, and non-repudiation of transactions. The **resident portal** provides information regarding policies and procedures of data sharing and other information to the citizens.
8	**Consent**	User **authentication** while accessing a service serves as consent to the service provider to access data from Aadhaar. Only trusted registered services (AUA/KUA) can access the Aadhaar system API's and can access it only through a trusted secure network of service agencies (ASA). User consent is captured during registration for digital ID on paper forms.
9	**Accuracy**	Users can **view and update** their information on the Aadhaar resident portal and through various other channels to maintain its currency/accuracy.
10	**Access**	On the resident portal, citizens can **access authentication history** of when and where authentication was attempted. If they find authentication attempts to which they had not consented, they are able to contest these occurrences.
11	**Compliance**	Tamper proof **transaction logs** and availability of access history to the users help in maintaining and **demonstrating** compliance with the data protection and privacy laws.



Εικόνα 24 Τα στατιστικά του επίσημου φορέα ψηφιακής ταυτοποίησης της Εσθονίας. Προσπέλαση στις 22/5/2019: https://e-estonia.com/solutions/e-identity/id-card/