



**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ:  
«ΔΙΑΧΕΙΡΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΒΙΒΛΙΟΘΗΚΕΣ, ΑΡΧΕΙΑ, ΜΟΥΣΕΙΑ»**

**ΤΜΗΜΑ ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ  
ΣΧΟΛΗ ΔΙΟΙΚΗΤΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**DEPARTMENT OF ARCHIVAL, LIBRARY AND INFORMATION STUDIES  
SCHOOL OF MANAGEMENT, ECONOMICS AND SOCIAL SCIENCES**

**Διπλωματική Εργασία**

**Ο τρόπος διαχείρισης των αρχειακών τεκμηρίων στον  
Ελληνικό στρατό και τα περιθώρια ενσωμάτωσης νέων  
τεχνολογιών με έμφαση στο Blockchain**

**Συγγραφέας**

**Αναστάσιος Καρνέζης (ΑΜ: 196682017)**

**Επιβλέπων: Ιωάννης Τριανταφύλλου**

**Αθήνα, Ιανουάριος 2023**

# Επιτροπή Εξέτασης

1. Ονοματεπώνυμο

2. Ονοματεπώνυμο

3. Ονοματεπώνυμο

## ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Αναστάσιος Καρνέζης του Κωνσταντίνου, με αριθμό μητρώου 196682017, φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «Διαχείριση Πληροφοριών σε Βιβλιοθήκες, Αρχεία, Μουσεία» του Τμήματος Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης της Σχολής Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».



Ο Δηλών

## Ευχαριστίες – Αφιερώσεις

Αυτή η διπλωματική εργασία είναι αφιερωμένη στην οικογένεια μου και σε όλους τους ανθρώπους που με στήριξαν μέσα σε αυτή τη δύσκολη συγκυρία που βιώνει όλη η ανθρωπότητα.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή κ. Ιωάννη Τριανταφύλλου για την υποστήριξη του, την καθοδήγηση του, την εξαιρετική συνεργασία και πολύτιμη συμβολή του στην ολοκλήρωση της παρούσας εργασίας. Η εμπιστοσύνη που μου έδειξε με την ανάθεση της συγκεκριμένης εργασίας αλλά και η άμεση ανταπόκριση και ανατροφοδότηση καθώς και η κατανόηση που έδειξε σε όλη τη διάρκεια εκπόνησης της εργασίας ήταν καθοριστικοί παράγοντες. Ειδική μνεία αξίζει και στον κ. Νικόλαο Καρεκλά για τη συμβολή του και την άμεση ανταπόκριση του σε οποιαδήποτε απορία προέκυψε κατά εκπόνηση της εργασίας. Εκτιμώ πολύ τη στήριξη, την υπομονή που έδειξαν σε όλη τη διάρκεια εκπόνησης της εργασίας και τη συγκαταβατικότητα τους στις αλλαγές που χρειάστηκε να γίνουν λόγω συνθηκών στο θεωρητικό καθώς και στο ερευνητικό μέρος. Ακόμη, ευχαριστώ το μόνιμο στρατιωτικό και πολιτικό προσωπικό της Υπηρεσίας Στρατιωτικών Αρχείων για την άψογη συνεργασία και σημαντική συνεισφορά τους στην εκπόνηση της ερευνητικής διαδικασίας.

## Περίληψη στα ελληνικά

Η παρούσα διπλωματική εργασία πραγματεύεται την ανάλυση του προγράμματος διαχείρισης αρχειακών εγγράφων του Ελληνικού στρατού, μέσα από έρευνα στην Υπηρεσία Στρατιωτικών Αρχείων (ΓΕΣ/ΥΣΑ), Αρχικά, θα γίνει μια παρουσίαση στο πρόγραμμα του παραπάνω οργανισμού άμυνας, αφού προηγηθούν οι ορισμοί σημαντικών όρων. Μέσα από τη μεθοδολογία του οργανισμού, θα παρουσιαστούν πληροφορίες όπως οι απαιτήσεις, ο τρόπος λειτουργίας και οι νέες συνθήκες που διαμορφώνονται σε τομείς όπως η προσβασιμότητα, η αποθήκευση και η διαχείριση των αρχειακών τεκμηρίων. Με αυτό τον τρόπο θα μπορέσουν να βγουν και ορισμένα συμπεράσματα, παρατηρήσεις και προκλήσεις ως προς τον τρόπο επεξεργασίας των αρχειακών τεκμηρίων. Πρόσθετα θα εξεταστούν τα περιθώρια ενσωμάτωσης στα προγράμματα διαχείρισης εγγράφων των δυο οργανισμών νέων τεχνολογιών όπως είναι το Blockchain.

**Λέξεις Κλειδιά:** Διαχείριση αρχείων, αρχειακά τεκμήρια, Υπηρεσία Στρατιωτικών Αρχείων, Αρχεία Ελληνικού στρατού, τεχνολογία Blockchain

## Περίληψη στα αγγλικά

This thesis deals with the analysis of the record management standard of the Greek Army, through research in the Military Archives Service. Initially, there will be a presentation of the program used by the defense agency, after defining important terms. Through the methodology of the organization, information such as requirements, way of operation and new conditions that are formed in areas such as accessibility, storage and management of archival documents will be presented. Therefore, some conclusions, observations and challenges regarding the way of processing the archival documents will be presented. Additionally, the possibility of the organization to integrate Blockchain technology will be investigated.

**Keywords:** Record management, archives, Military Archives Service, Greek army archival records, Blockchain technology

# Πίνακας περιεχομένων

ΕΠΙΤΡΟΠΗ ΕΞΕΤΑΣΗΣ .....	II
ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ .....	III
ΕΥΧΑΡΙΣΤΙΕΣ – ΑΦΙΕΡΩΣΕΙΣ .....	IV
ΠΕΡΙΛΗΨΗ ΣΤΑ ΕΛΛΗΝΙΚΑ .....	V
ΠΕΡΙΛΗΨΗ ΣΤΑ ΑΓΓΛΙΚΑ .....	VI
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ .....	VII
ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ .....	IX
ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ .....	X
<b>ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ .....</b>	<b>1</b>
1.1 ΠΛΑΙΣΙΟ, ΣΚΟΠΟΣ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ .....	1
1.2 ΕΡΕΥΝΗΤΙΚΕΣ ΥΠΟΘΕΣΕΙΣ .....	1
1.3 ΜΕΘΟΔΟΛΟΓΙΑ .....	2
1.4 ΠΕΡΙΟΡΙΣΜΟΙ .....	3
1.5 ΟΡΙΣΜΟΙ .....	3
1.6 ΟΡΓΑΝΩΣΗ ΚΕΦΑΛΑΙΩΝ Η ΔΙΑΡΘΡΩΣΗ ΤΗΣ ΕΡΓΑΣΙΑΣ .....	7
<b>ΚΕΦΑΛΑΙΟ 2. ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ .....</b>	<b>8</b>
2.1 ΠΡΟΛΟΓΟΣ .....	8
2.2 ΕΛΛΗΝΙΚΟΣ ΣΤΡΑΤΟΣ .....	16
2.2.1 <i>Ιστορικά στοιχεία</i> .....	16
2.2.2 <i>Εγκαταστάσεις</i> .....	17
2.2.3 <i>Αποστολή</i> .....	18
2.2.4 <i>Συλλογές</i> .....	19
2.2.5 <i>Κατηγορίες αρχείων</i> .....	21
2.2.6 <i>Ψηφιακή εποχή</i> .....	22
2.3 ΔΙΕΘΝΗΣ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ .....	25
2.3.1 <i>Ηνωμένο Βασίλειο</i> .....	25
2.3.2 <i>Ηνωμένες Πολιτείες της Αμερικής</i> .....	30
2.4 ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN .....	36
2.4.1 <i>Εισαγωγή</i> .....	36
2.4.2 <i>Εφαρμογές της τεχνολογίας Blockchain</i> .....	37

2.4.3	Περιπτώσεις χρήσης .....	42
2.4.4	Περιεχόμενο και κίνδυνοι.....	44
2.4.5	Πλατφόρμες Blockchain.....	44
2.4.6	Γενιές Blockchain .....	49
2.4.7	Τύποι Blockchain.....	52
2.4.8	Μέρη ενός Blockchain .....	59
2.4.9	Βασικές αρχές της τεχνολογίας Blockchain .....	60
2.4.10	Τεχνικά χαρακτηριστικά .....	62
2.4.11	Θεμελιώδη χαρακτηριστικά ενός συστήματος Blockchain .....	73
2.4.12	Στρατηγική ανάπτυξης ενός συστήματος διαχείρισης αρχείων που βασίζεται στην τεχνολογία Blockchain .....	81
2.4.13	Blockchain & Record Management.....	83
2.4.14	Σχεδιασμός και διασφάλιση ενός συστήματος Blockchain.....	92
2.4.15	Blockchain & GDPR.....	95
<b>ΚΕΦΑΛΑΙΟ 3. ΜΕΘΟΔΟΛΟΓΙΑ Η/ΚΑΙ ΣΧΕΔΙΟ ΕΡΓΑΣΙΩΝ– ΥΛΟΠΟΙΗΣΗ – ΕΦΑΡΜΟΓΗ .....</b>		<b>103</b>
3.1	ΣΧΕΔΙΟ ΕΡΓΑΣΙΩΝ .....	103
3.2	ΠΕΡΙΓΡΑΦΗ ΥΛΟΠΟΙΗΣΗΣ – ΕΦΑΡΜΟΓΗΣ.....	104
3.3	ΣΤΟΧΟΣ ΤΗΣ ΈΡΕΥΝΑΣ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ.....	104
<b>ΚΕΦΑΛΑΙΟ 4. ΑΠΟΤΕΛΕΣΜΑΤΑ – ΕΥΡΗΜΑΤΑ / ΕΠΙΤΕΥΓΜΑΤΑ .....</b>		<b>108</b>
4.1	ΑΝΑΛΥΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ.....	108
4.1.1	Δομή.....	108
4.1.2	Υλικοτεχνικός εξοπλισμός και υποδομές.....	108
4.1.3	Προσωπικό.....	109
4.1.4	Document Management System – «Πάπυρος».....	110
4.1.5	Διαχείριση και αξιοποίηση αρχειακού υλικού .....	111
4.1.6	Ψηφιοποίηση.....	113
4.1.7	Προτάσεις.....	115
<b>ΚΕΦΑΛΑΙΟ 5. ΣΥΖΗΤΗΣΗ – ΣΥΜΠΕΡΑΣΜΑΤΑ – ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ.....</b>		<b>118</b>
5.1	ΣΥΜΠΕΡΑΣΜΑΤΑ .....	118
5.2	ΠΡΟΒΛΗΜΑΤΑ.....	122
5.3	ΠΡΟΚΛΗΣΕΙΣ .....	134
5.4	ΕΠΙΛΟΓΟΣ.....	141
<b>ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ.....</b>		<b>143</b>
<b>ΠΑΡΑΡΤΗΜΑ.....</b>		<b>146</b>



## Πίνακας Σχημάτων

Σχήμα 1: Σχέση μεταξύ Blockchain και DLT.....	48
Σχήμα 2: Τυπολογία Blockchain.....	53
Σχήμα 3: Πλεονεκτήματα Blockchain.....	65
Σχήμα 4: Ενδεικτική δομή ενός Blockchain.....	68
Σχήμα 5: Απλή μορφή ενός Merkle Tree.....	69
Σχήμα 6: Σύνθετη μορφή ενός Merkle Tree.....	70
Σχήμα 7: Δημιουργία ενός μπλοκ σε ένα Blockchain.....	71
Σχήμα 8: Η διαδικασία εκτέλεσης μιας συναλλαγής σε ένα Blockchain.....	71
Σχήμα 9: Διάγραμμα soft και hard fork.....	74
Σχήμα 10: Μοντέλο εμπιστοσύνης τριών επιπέδων της τεχνολογίας Blockchain.....	78
Σχήμα 11: Η ταξινόμια της εμπιστοσύνης.....	78
Σχήμα 12: 6 στάδια διαχείρισης αρχείων σε ένα Blockchain.....	84
Σχήμα 13: Μοντέλο κύκλου ζωής.....	86
Σχήμα 14: Διεπαφή χρήστη κατά τη διάρκεια διαμόρφωσης μιας εγγραφής σε Blockchain περιβάλλον.....	94

## Πίνακας Πινάκων

Πίνακας 1: Αρμοδιότητες, παράγοντες και ενέργειες που οδηγούν στη δημιουργία ενεργού αρχειακού υλικού .....	29
Πίνακας 2: Σύγκριση Blockchain – παραδοσιακής βάσης δεδομένων.....	47
Πίνακας 3: Γενική σύγκριση δημόσιου και ιδιωτικού Blockchain .....	57
Πίνακας 4: Παράδειγμα ενός Hash.....	67
Πίνακας 5: Είδη, παραδείγματα και τοποθεσία εγγραφών σε ένα σύστημα Blockchain.	91
Πίνακας 6: Αντιστοίχιση αρχών GARP με άρθρα του GDPR.....	96
Πίνακας 7: Σύνοψη περιορισμών και ρίσκων ενός Blockchain συστήματος .....	127

# Κεφάλαιο 1. Εισαγωγή

## 1.1 Πλαίσιο, σκοπός και στόχοι της διπλωματικής εργασίας

Στόχος της διπλωματικής εργασίας είναι να παρουσιάσει το πρόγραμμα διαχείρισης αρχειακών εγγράφων του Ελληνικού στρατού και όχι μόνο να προβάλλει το περιεχόμενο του αλλά και να αναφέρει τομείς που χρήζουν βελτίωσης. Ως προς τον Ελληνικό στρατό η πληροφορία θα εξαχθεί μέσα από έρευνα στη Υπηρεσία Στρατιωτικών Αρχείων (ΓΕΣ/ΥΣΑ). Η πορεία των περιοριστικών μέτρων λόγω της πανδημίας του Covid19 θα παίξει σημαντικό ρόλο ως προς την ολοκλήρωση της έρευνας στην ΥΣΑ στον επιθυμητό βαθμό ώστε να μπορεί να γίνει όσο το δυνατόν εκτενέστερη ανάλυση της Ελληνικής. Ο τομέας της διαχείρισης της πληροφορίας στη σημερινή εποχή είναι ιδιαίτερα νευραλγικός, ειδικότερα στους οργανισμούς άμυνας που διαχειρίζονται διαβαθμισμένες/απόρρητες πληροφορίες καθημερινά. Για το λόγο αυτό θα γίνει απόπειρα να ερευνηθεί το κατά πόσο μια “state of art” τεχνολογία, όπως αυτή του Blockchain, μπορεί να διαδραματίσει σημαντικό ρόλο ως προς τη διαχείριση των αρχειακών τεκμηρίων καθ’ όλη τη διάρκεια του κύκλου ζωής τους.

## 1.2 Ερευνητικές υποθέσεις

Στην παρούσα διπλωματική θα γίνει προσπάθεια να παρουσιαστεί όσο το δυνατόν πιο αναλυτικά ο τρόπος λειτουργίας και διαχείρισης αρχείων στον Ελληνικό στρατό, μέσω της Υπηρεσίας Στρατιωτικών Αρχείων, καθώς δεν υπάρχουν διαθέσιμες πληροφορίες ούτε μέσω βιβλιογραφίας ούτε μέσω κάποιας επίσημης ιστοσελίδας. Έχοντας άμεση εμπειρία και επαφή με την παραπάνω υπηρεσία λόγω της στρατιωτικής μου θητείας, θεώρησα ενδιαφέρον να κάνω μια προσπάθεια προβολής της Ελληνικής πραγματικότητας ως προς τη διαχείριση αρχείων σε έναν οργανισμό άμυνας.

Η λογική μας οδηγεί στο συμπέρασμα ότι η διαχείριση αρχείων σε έναν οργανισμό άμυνας στην Ελλάδα θα διαφέρει σε μεγάλο βαθμό με κάποιον αντίστοιχο του εξωτερικού. Με δεδομένη τη γραφειοκρατία και το χαμηλό ρυθμό εξέλιξης, καινοτομίας και αλλαγής στο δημόσιο τομέα, θα είναι τουλάχιστον ενθαρρυντικό να υπάρχει διαθέσιμη μια πρόταση που

θα μπορεί να αναβαθμίσει τεχνολογικά τον τρόπο λειτουργίας και τις παροχές ενός οργανισμού άμυνας

Μέσω της ερευνητικής διαδικασίας έγινε προσπάθεια διερεύνησης της τρέχουσας κατάστασης σε τομείς όπως οι παρακάτω:

- Ροή εργασιών της υπηρεσίας
- Αλληλεπίδραση και εξυπηρέτηση με το κοινό
- Διαδικασία ψηφιοποίησης αρχειακού υλικού
- Συνθήκες αποθήκευσης αρχειακού υλικού
- Τρόποι πρόσβασης σε αρχειακό υλικό και δικλίδες ασφαλείας
- Τρέχον λογισμικό διαχείρισης εγγράφων («Πάπυρος»), τα χαρακτηριστικά του και οι δυνατότητες που προσφέρει
- Επάρκεια τεχνολογικού εξοπλισμού με σκοπό την άρτια λειτουργία της υπηρεσίας

Αυτά αποτελούν τα βασικά ζητήματα, ωστόσο στην πορεία της έρευνας μπορεί να προκύψουν επιπλέον ερωτήματα οπότε τα επιπλέον δεδομένα/συμπεράσματα θα συμπεριληφθούν στην αντίστοιχη ενότητα.

### **1.3 Μεθοδολογία**

Στο πλαίσιο της διπλωματικής εργασίας θα γίνει αρχικά μια βιβλιογραφική ανασκόπηση σε άρθρα επιστημονικών περιοδικών από βάσεις δεδομένων εκδοτών του εξωτερικού (π.χ. Elsevier) αλλά και από την υπηρεσία «Μελετητής» της Google όπου θα αναζητηθούν ορισμένα εισαγωγικά στοιχεία και ορισμοί σχετικά με τη διαχείριση αρχειακών εγγράφων γενικότερα αλλά και την τεχνολογία Blockchain ειδικότερα. Στη συνέχεια, θα πραγματοποιηθεί έρευνα στην Υπηρεσία Στρατιωτικών Αρχείων, από όπου θα προκύψουν χρήσιμα συμπεράσματα για την υπηρεσία ως προς την κουλτούρα και τον τρόπο λειτουργίας της. Η εκπόνηση της έρευνας στην ΥΣΑ απαιτεί φυσική παρουσία οπότε η πορεία της πανδημίας του Covid19 στη χώρα μας θα παίξει σημαντικό ρόλο ως προς την άντληση σημαντικών στοιχείων και την τήρηση των χρονοδιαγραμμάτων. Παράλληλα, θα γίνει παρουσίαση των βασικών λειτουργιών και χαρακτηριστικών της τεχνολογίας Blockchain ώστε να χρησιμοποιηθούν και αυτά τα δεδομένα στην ερευνητική διαδικασία, να διερευνηθεί η πιθανότητα ενσωμάτωσης της τεχνολογίας αυτής από έναν οργανισμό άμυνας μέσω ενός

ολοκληρωμένου συστήματος διαχείρισης αρχειακών εγγράφων, το οποίο θα βασίζεται στην τεχνολογία Blockchain.

## 1.4 Περιορισμοί

Η Ελληνική πραγματικότητα αποτυπώνεται και παράλληλα περιορίζεται στην Υπηρεσία Στρατιωτικών Αρχείων, καθώς εκεί εστιάζει και το ερευνητικό μέρος. Εκτός από την Υπηρεσία Στρατιωτικών Αρχείων, αρχειακό υλικό διατηρούν επίσης η Διεύθυνση Ιστορίας Στρατού (ΔΙΣ), το Γενικό Επιτελείο Αεροπορίας (ΓΕΑ) και το Γενικό Επιτελείο Ναυτικού (ΓΕΝ), αλλά σε μικρότερο βαθμό και όγκο.

## 1.5 Ορισμοί

Bitcoin: Το Bitcoin είναι ένα σύστημα πληρωμών peer-to-peer που εφευρέθηκε από έναν μη αναγνωρισμένο προγραμματιστή ή ομάδα προγραμματιστών, υπό το όνομα Satoshi Nakamoto (Staples et al., 2017).

Block: Ένα μπλοκ σε ένα Blockchain είναι αυτό που περιέχει τις συναλλαγές. Κάθε μπλοκ περιέχει μια χρονική σήμανση και έναν σύνδεσμο προς το προηγούμενο μπλοκ (Staples et al., 2017).

Blockchain: Το Blockchain είναι μια κατακερματισμένη βάση δεδομένων εγγράφων (συναλλαγών) που αποθηκεύει τιμές κατακερματισμού δεδομένων, πληροφοριών, συναλλαγών, εγγράφων ή εγγραφών και συνδέεται με την έννοια της τεχνολογίας κατακερματισμένου καθολικού (Distributed Ledger Technology - DLT) (Stancic, 2018).

Blockchain Recordkeeping: η χρήση του Blockchain ως τεχνολογία για την αποθήκευση εγγραφών hash, όπως εγγραφές καθολικού (Lemieux, 2016a).

Consensus mechanism / Μηχανισμός συναίνεσης: Το νεότερο Blockchain πρέπει να είναι συνεπές και αποδεκτό από την πλειοψηφία των συνδεδεμένων ηλεκτρονικών υπολογιστών. Η μέθοδος με την οποία γίνεται αποδεκτό το νέο Blockchain καθορίζεται από τον αλγόριθμο που χρησιμοποιείται (National Archives and Records Administration (NARA), 2019).

Consortium Blockchain / Blockchain κοινοπραξίας: Ένα ιδιωτικό Blockchain που αναπτύσσεται και λειτουργεί από μια κοινοπραξία οργανισμών (Staples et al., 2017).

Cryptocurrency / Κρυπτονόμισμα: Ένα ψηφιακό νόμισμα που χρησιμοποιούν οι τεχνικές κρυπτογράφησης για να ρυθμίσουν τη δημιουργία μονάδων νομίσματος και να επαληθεύσουν τη μεταφορά κεφαλαίων, λειτουργώντας ανεξάρτητα από μια κεντρική τράπεζα (National Archives and Records Administration (NARA), 2019).

Decentralized applications / Αποκεντρωμένες εφαρμογές: Το Google Play και το Apple Store ελέγχουν κεντρικά τις εφαρμογές που προσφέρονται μέσω των καταστημάτων τους. Μια αποκεντρωμένη εφαρμογή είναι μια εφαρμογή που μπορεί να διατεθεί σε μια πλατφόρμα Blockchain χωρίς κεντρικό σημείο ελέγχου (National Archives and Records Administration (NARA), 2019).

Digital ID / Ψηφιακό αναγνωριστικό: Πληροφορίες για μια οντότητα που χρησιμοποιείται από συστήματα υπολογιστών για την αναπαράσταση ενός εξωτερικού παράγοντα. Αυτός ο παράγοντας μπορεί να είναι άτομο, οργανισμός, εφαρμογή ή συσκευή (National Archives and Records Administration (NARA), 2019).

Distributed Ledger Technology (DLT) / Τεχνολογία Κατανεμημένου Καθολικού: Μια ομοφωνία αναπαραγόμενων, κοινών και συγχρονισμένων ψηφιακών δεδομένων γεωγραφικά κατανεμημένων σε πολλούς ιστότοπους, χώρες ή/και ιδρύματα (Lemieux, 2016a).

Ethereum: Το Ethereum είναι μια δημόσια κατανεμημένη υπολογιστική πλατφόρμα που βασίζεται σε Blockchain, η οποία διαθέτει λειτουργικότητα έξυπνων συμβολαίων. Παρέχει μια αποκεντρωμένη εικονική μηχανή, την εικονική μηχανή Ethereum (Ethereum Virtual Machine), η οποία μπορεί να εκτελεί συμβόλαια peer-to-peer χρησιμοποιώντας ένα ειδικό νόμισμα που ονομάζεται ether (Staples et al., 2017).

Fixity / σταθερότητα: Η σταθερότητα του αρχείου διασφαλίζει ότι η ιδιοκτησία ενός ψηφιακού αρχείου είναι σταθερή ή αμετάβλητη. Ο έλεγχος σταθερότητας είναι η διαδικασία επαλήθευσης ότι ένα ψηφιακό αντικείμενο δεν έχει αλλοιωθεί ή καταστραφεί (National Archives and Records Administration (NARA), 2019).

Hash: Μια συνάρτηση που παίρνει μια συμβολοσειρά εισόδου (input string), η οποία μπορεί να είναι οποιουδήποτε μήκους, και δημιουργεί μια έξοδο σταθερού μήκους. Το αποτέλεσμα, ή hash, χρησιμοποιείται για την επαλήθευση των πληροφοριών. Οι τιμές που επιστρέφονται

από μια συνάρτηση hash ονομάζονται τιμές hash, κωδικοί hash, επιτομές ή απλά hashes (National Archives and Records Administration (NARA), 2019).

Merkle tree: Στην κρυπτογραφία, ένα δέντρο Merkle είναι ένα δέντρο στο οποίο κάθε κόμβος φύλλου (leaf node) επισημαίνεται με το hash ενός μπλοκ δεδομένων και κάθε κόμβος που δεν είναι φύλλου (non-leaf node) επισημαίνεται με το κρυπτογραφικό hash των ετικετών των θυγατρικών κόμβων του. Τα δέντρα hash επιτρέπουν την αποτελεσματική και ασφαλή επαλήθευση των περιεχομένων μεγάλων δομών δεδομένων (National Archives and Records Administration (NARA), 2019).

Miner / εξορύκτες: Σε ένα Blockchain Proof of Work (PoW), οι κόμβοι επεξεργασίας που λειτουργούν συλλογικά το Blockchain είναι γνωστοί ως εξορύκτες (miners) (Staples et al., 2017).

Mining / εξόρυξη: Η διαδικασία με την οποία οι κόμβοι ανταγωνίζονται για την προσθήκη εγγραφών ή μπλοκ συναλλαγών στο Blockchain (National Archives and Records Administration (NARA), 2019).

Node / κόμβος (Lemieux, 2016a):

- a. μια ξεχωριστή μονάδα (υπολογιστής) μέσα σε ένα δίκτυο
- b. μια ξεχωριστή μονάδα (υπολογιστής) μέσα σε ένα αποκεντρωμένο σύστημα Blockchain που διατηρεί ένα αντίγραφο του Blockchain και δαπανά την ισχύ της CPU για την κατασκευή του Blockchain.

Off-Chain: Αντικείμενα ή δεδομένα που αναφέρονται μέσω συνδέσμων ή δεικτών, αλλά αποθηκεύονται χωριστά από το Blockchain (National Archives and Records Administration (NARA), 2019).

Peer-to-peer: Ένα κατανεμημένο δίκτυο στο οποίο οι κόμβοι διασυνδέονται και μοιράζονται δεδομένα απευθείας μεταξύ τους χωρίς κεντρική υπηρεσία (National Archives and Records Administration (NARA), 2019).

Peer-to-peer Payment / Πληρωμή peer-to-peer: μια συναλλαγή με χρήση κρυπτονομίσματος μεταξύ δύο μερών που δεν βασίζεται σε τρίτο μέρος (όπως μια τράπεζα) για τη διεξαγωγή της συναλλαγής (Lemieux, 2016a).

Permissionless/Public Ledger / Καθολικό δημόσιο/χωρίς άδεια: Οποιοσδήποτε μπορεί να εισαγάγει συναλλαγές σε ένα μπλοκ που θα συμπεριληφθεί στο Blockchain (National Archives and Records Administration (NARA), 2019).

Permissioned/Private Ledger / Καθολικό εξουσιοδοτημένο/ιδιωτικό: Περιορίζεται σε ένα συγκεκριμένο σύνολο εξουσιοδοτημένων κόμβων και μόνο ένας εξουσιοδοτημένος χρήστης μπορεί να έχει πρόσβαση, να δημιουργήσει συναλλαγές και να ενημερώσει το καθολικό (National Archives and Records Administration (NARA), 2019).

Private Blockchain / Ιδιωτικό Blockchain: Ένα Blockchain που λειτουργεί από μια ιδιωτική οντότητα ή κοινοπραξία, χωρίς καθόλου ή με περιορισμένη πρόσβαση από άλλα μέρη, και συνήθως με μικρό αριθμό (δεκάδες ή εκατοντάδες) κόμβους επεξεργασίας που λειτουργούν το Blockchain. Σε αυτό το πλαίσιο, σε σύγκριση με τα δημόσια Blockchain, μπορούν να χρησιμοποιηθούν τεχνικές βελτιστοποιήσεις για τη βελτίωση του λανθάνοντος χρόνου και της απόδοσης του Blockchain και οι μηχανισμοί συναίνεσης μπορεί να χρησιμοποιηθούν για την παροχή ισχυρότερων εγγυήσεων σχετικά με την ολοκλήρωση των συναλλαγών (Staples et al., 2017).

Public Blockchain / Δημόσιο Blockchain: Ένα Blockchain που λειτουργεί ως δημόσιο σύστημα peer-to-peer. Τα μέρη προσδιορίζονται συνήθως με ψευδώνυμα δημόσια/ιδιωτικά κλειδιά και μια μορφή συναίνεσης Nakamoto χρησιμοποιείται συνήθως για να επιτρέψει σε μεγάλο αριθμό (χιλιάδες) κόμβους επεξεργασίας να λειτουργήσουν το Blockchain (Staples et al., 2017).

Public Key / Δημόσιο κλειδί: Στην κρυπτογραφία ένα δημόσιο κλειδί είναι ένας δημοσιευμένος αριθμός που χρησιμοποιείται ως παράμετρος σε μια συνάρτηση κρυπτογράφησης, για την κρυπτογράφηση και τον έλεγχο υπογεγραμμένων μηνυμάτων. Τα δημόσια κλειδιά συνδυάζονται με μυστικά ιδιωτικά κλειδιά, τα οποία χρησιμοποιούνται για την αποκρυπτογράφηση και την υπογραφή μηνυμάτων (Staples et al., 2017).

Public/Private Key Infrastructure / Υποδομή δημόσιου/ιδιωτικού κλειδιού: Κλειδιά που σχετίζονται μαθηματικά μεταξύ τους. Το δημόσιο κλειδί μπορεί να χρησιμοποιηθεί για την επαλήθευση μιας υπογραφής που δημιουργείται χρησιμοποιώντας ένα ιδιωτικό κλειδί (National Archives and Records Administration (NARA), 2019).



Smart Contract / Έξυπνο συμβόλαιο/σύμβαση: Ένας αυτοεκτελούμενος αλγόριθμος υπολογιστή που ενσωματώνει τους όρους και τις προϋποθέσεις ενός συμβολαίου/σύμβασης ως πηγαίο κώδικα που μεταγλωττίζεται σε εκτελέσιμο κώδικα υπολογιστή (Lemieux, 2016a).

Timestamp / Χρονοσήμανση: τρέχουσα ώρα ενός συμβάντος που καταγράφεται από υπολογιστή (Lemieux, 2016a).

Trustless Transfer: ένα σύστημα όπου τα δικαιώματα της εγγραφής διαχειρίζονται και διαμεσολαβούνται από μια τεχνολογία, εξαιρώντας ένα αξιόπιστο ίδρυμα ή τρίτο μέρος (Lemieux, 2016a).

## **1.6 Οργάνωση Κεφαλαίων ή Διάρθρωση της Εργασίας**

Η εργασία περιλαμβάνει πρώτα την παρουσίαση της Ελληνικής πραγματικότητας ως προς τη διαχείριση αρχειακών τεκμηρίων σε έναν οργανισμό άμυνας στην Ελλάδα, μέσω της Υπηρεσίας Στρατιωτικών Αρχείων με ορισμένα ιστορικά στοιχεία και πληροφορίες όπως οι εγκαταστάσεις, η αποστολή, οι συλλογές, οι κατηγορίες των αρχείων που διατηρεί αλλά και η παρουσία της στην ψηφιακή εποχή. Έπειτα γίνεται αναφορά στη διεθνή πραγματικότητα με παραδείγματα από το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες της Αμερικής. Στη συνέχεια, παρουσιάζεται εκτενώς η τεχνολογία Blockchain, ιστορικά στοιχεία, εφαρμογές και περιπτώσεις χρήσης, πλατφόρμες, γενιές, μέρη, περιεχόμενο, αρχές, τεχνικά και θεμελιώδη χαρακτηριστικά και διάφοροι τύποι Blockchain, η σχέση μεταξύ της τεχνολογίας Blockchain με την αρχειονομία αλλά και με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (GDPR). Έπειτα, παρουσιάζονται τα ευρήματα του ερευνητικού μέρους και γίνονται και οι αντίστοιχες προτάσεις. Τέλος, γίνεται αναφορά σε συμπεράσματα, προβλήματα και προκλήσεις που προκύπτουν μέσα από τη διεθνή βιβλιογραφία.

## Κεφάλαιο 2. Θεωρητικό μέρος

### 2.1 Πρόλογος

Σύμφωνα με τα Vermont State Archives (2019), οι τεχνολογίες και οι διαδικασίες που περιλαμβάνουν την τήρηση δημόσιων αρχείων πρέπει να διασφαλίζουν ότι τα αρχεία παραμένουν αυθεντικά, αξιόπιστα, ακέραια και προσβάσιμα, ειδικά για αρχειακά έγγραφα, τα οποία πρέπει να διατηρούνται επ' αόριστον. Η τεχνολογία που επιλέγεται για χρήση σε κυβερνητικές εφαρμογές πρέπει να ελεγχθεί διεξοδικά και να συμμορφώνεται με τις απαιτήσεις που στηρίζουν τις βασικές λειτουργίες της κυβέρνησης, ειδικά αν αφορούν έναν οργανισμό άμυνας που διαχειρίζεται διαβαθμισμένα και απόρρητα έγγραφα.

Όπως αναφέρεται και από τους Lemieux et al. (2019), στην παραδοσιακή τήρηση αρχείων σε χαρτί, τα στοιχεία μπορούν να βρεθούν σε μια ενιαία οντότητα. Στην πρώιμη εποχή του ψηφιακού αρχείου, η κωδικοποίηση των ψηφιακών αρχείων δεν παρήγαγε πλέον μια σταθερή μορφή τεκμηρίωσης και, ως αποτέλεσμα, οι ψηφιακές εγγραφές δεν μπορούσαν πλέον να διατηρηθούν ως φυσικά αντικείμενα. Έπρεπε να διατηρηθούν ως ροές bit που θα μπορούσαν να υποστούν σωστή επεξεργασία από υπολογιστές για να αποδοθούν στην κατάλληλη μορφή τεκμηρίωσης. Αυτό ισχύει επίσης για τις εγγραφές Blockchain, των οποίων η μορφή διαμεσολαβείται υπολογιστικά.

Η τεχνολογία γενικά παίζει μεγάλο ρόλο στη διαχείριση των δημόσιων αρχείων, ειδικά τις τελευταίες δεκαετίες, καθώς βρίσκεται σε εξέλιξη η μετάβαση από τα παραδοσιακά συστήματα τήρησης αρχείων που βασίζονται σε χαρτί σε αυτά που είναι πλήρως ψηφιακά και συχνά βασισμένα στο διαδίκτυο (web-based) ή φιλοξενούνται απομακρυσμένα (remotely hosted). Η απόκτηση τεχνολογίας για την καλύτερη διαχείριση πληροφοριών και αρχείων αποτελεί τομέα ιδιαίτερου ενδιαφέροντος, καθώς απαιτείται σημαντικό ποσό δαπανών για την αγορά, συντήρηση και λειτουργία τέτοιων συστημάτων (Vermont State Archives, 2019). Ένα τέτοιο παράδειγμα αποτελεί η τεχνολογία Blockchain, στην οποία θα γίνει ιδιαίτερη μνεία παρακάτω.

Γενικά μια εκ των αρμοδιοτήτων μιας κυβέρνησης αποτελεί η διατήρηση δεδομένων ατόμων/πολιτών. Η διαχείριση και η χρήση αυτών των δεδομένων μπορεί να αποδειχθεί δύσκολη, ακόμη και για προηγμένες κυβερνήσεις. Διαφορετικές κρατικές υπηρεσίες

επιβολής του νόμου διαθέτουν ξεχωριστές βάσεις δεδομένων, γεγονός που μπορεί να αποτελέσει εμπόδιο στην ομαλή ροή δεδομένων μεταξύ διαφορετικών κρατικών υπηρεσιών. Η ύπαρξη τέτοιων πολλαπλών βάσεων δεδομένων αυξάνει επίσης το κόστος της ασφάλειάς τους και έτσι η πιθανότητα παράνομων αλλαγών αυξάνεται σταδιακά (Al Omar et al., 2018). Η ασφάλεια των δεδομένων αποτελεί ιδιαίτερα σημαντικό τομέα για την ορθή και ομαλή λειτουργία ενός συστήματος διαχείρισης αρχειακών εγγράφων, ειδικά για τη σημερινή εποχή που οι κυβερνοεπιθέσεις είναι πολύ συχνό φαινόμενο.

Σύμφωνα με την Lemieux (2016b), επιστήμονες υπολογιστών ανά τον κόσμο έχουν ασχοληθεί με ορισμούς και μέτρα απόδοσης αξιόπιστων στρατιωτικών συστημάτων για σχεδόν 20 χρόνια. Την τελευταία δεκαετία, η πρωτοποριακή εργασία από αρχειονόμους σε Αυστραλία, Βόρεια Αμερική και Ευρώπη είχε ως αποτέλεσμα την ανακάλυψη θεμελιωδών νέων προσεγγίσεων και εργαλείων που προσδιορίζουν τη φύση και την απόδοση αξιόπιστων συστημάτων διαχείρισης αρχειακών εγγράφων.

Τα τελευταία χρόνια ειδικοί στις ψηφιακές βιβλιοθήκες έχουν συνεισφέρει την εμπειρία τους σε ένα αυξανόμενο σύνολο βιβλιογραφίας και εφαρμογών που σχετίζονται με την κατασκευή και τη συντήρηση ασφαλών συστημάτων που φιλοξενούν μεγάλες ποσότητες ψηφιακών πόρων. Μεγάλο μέρος της συζήτησης σχετικά με τα αξιόπιστα αρχεία ή συστήματα συνοψίζεται σε δύο έννοιες αλληλένδετες: αξιοπιστία και αυθεντικότητα και στενά συνδεδεμένες έννοιες όπως ταυτότητα, ακεραιότητα και προέλευση (Lemieux, 2016b).

Επιπλέον, το πρότυπο ISO 15489 ορίζει μια τέταρτη βασική πτυχή, τη χρηστικότητα, η οποία δεν σχετίζεται με της αξιοπιστίαν ενός αρχείου αλλά με την πρακτική χρησιμότητα αυτού του αρχείου στο πλαίσιο χρήσης του (Vermont State Archives, 2019).

Σύμφωνα με τη Lemieux (2016b), η **αξιόπιστία** των αρχείων ως προς τη δήλωση γεγονότων ξεκινά με τη διαδικασία δημιουργίας του αρχείου: το δημιουργό του και τον τρόπο δημιουργίας του. Ένα αξιόπιστο αρχείο είναι αυτό του οποίου το περιεχόμενο μπορεί να αποτελέσει πλήρη και ακριβή αναπαράσταση των συναλλαγών, δραστηριοτήτων ή γεγονότων που πιστοποιούν και μπορεί να εξαρτηθεί από αυτά κατά τη διάρκεια των επόμενων συναλλαγών ή δραστηριοτήτων. Τα αρχεία είναι πιθανό να είναι πιο αξιόπιστα εάν δημιουργούνται κατά τη συνήθη και κοινή πορεία των εργασιών: δηλαδή, τη στιγμή της συναλλαγής ή του συμβάντος με το οποίο σχετίζονται, ή αμέσως μετά, από άτομα που έχουν

άμεση γνώση των γεγονότων ή από μέσα που χρησιμοποιούνται συνήθως εντός της επιχείρησης για τη διεξαγωγή της συναλλαγής.

Για την παραγωγή αξιόπιστων αρχείων τα συστήματα αρχείων πρέπει να (Lemieux, 2016b):

- καταγράφουν τακτικά όλα τα αρχεία εντός του πεδίου των επιχειρηματικών τους δραστηριοτήτων.
- οργανώνουν τα αρχεία με τρόπο που να αντικατοπτρίζει τις επιχειρηματικές διαδικασίες του οργανισμού.
- προστατεύουν τα αρχεία από μη εξουσιοδοτημένη τροποποίηση ή διάθεση.
- λειτουργούν τακτικά ως η κύρια πηγή πληροφοριών σχετικά με ενέργειες που τεκμηριώνονται στα αρχεία.
- παρέχουν άμεση πρόσβαση σε όλες τις εγγραφές και τα μεταδεδομένα.

Οι πιθανές συνέπειες των αναξιόπιστων αρχείων που εμπλέκονται σε νομικές διαδικασίες είναι καταστροφικές. Η απώλεια της πίστης στην κρατική διαχείριση αρχείων θα υπονόμει την εμπιστοσύνη στην ίδια την κυβέρνηση. Οι παραβιάσεις δεδομένων στην κυβέρνηση τα τελευταία χρόνια έχουν αναγκάσει τα νομοθετικά όργανα να εφαρμόσουν μέτρα προστασίας, όπως ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, επιδιώκοντας να αποκαταστήσουν την εμπιστοσύνη στη διαχείριση δεδομένων από τη μεριά της κυβέρνησης (Vermont State Archives, 2019).

Η **αυθεντικότητα**, σύμφωνα με την Lemieux (2016b), εξαρτάται από την καθιέρωση και τη διατήρηση της ταυτότητας και της ακεραιότητας ενός αρχείου από το σημείο της δημιουργίας του και έπειτα. Όταν δημιουργούνται ψηφιακά αρχεία, συχνά διατηρούνται για ένα χρονικό διάστημα στα συστήματα που δημιουργήθηκαν. Αυτή η περίοδος μπορεί να διαφέρει ανάλογα με το σκοπό του αρχείου, όπως σε περιβάλλοντα που διαθέτουν ένα σταθερό πρόγραμμα διαχείρισης αρχείων με χρονοδιαγράμματα διατήρησης ή μπορεί απλώς να συνδέεται με τον παροπλισμό του αρχικού συστήματος, ειδικά σε οργανισμούς όπου δεν υπάρχουν τυπικοί έλεγχοι των αρχείων. Στο πλαίσιο των αρχικών συστημάτων, ο καθορισμός της ταυτότητας των αρχείων περιλαμβάνει διαδικασίες καταχώρισης, όπου οι εγγραφές καταχωρούνται σε μητρώο και αντιστοιχούνται με μοναδικά αναγνωριστικά, και ταξινόμησης, όπου τα αρχεία συνδέονται λογικά με άλλα αρχεία που σχετίζονται με την ίδια λειτουργία σύμφωνα με ένα σχήμα ταξινόμησης. Αυτά τα αναγνωριστικά ενδέχεται να είναι

ενσωματωμένα ή λογικά συνδεδεμένα με το αρχείο. Η διασφάλιση της ακεραιότητας σε τέτοια συστήματα περιλαμβάνει μέτρα όπως ο έλεγχος πρόσβασης, η επαλήθευση χρήστη, ο έλεγχος των διαδρομών καθώς και η τεκμηρίωση που αποδεικνύει την κανονική λειτουργία, την τακτική συντήρηση και τη συχνότητα των αναβαθμίσεων των συστημάτων αρχείων.

Όπως αναφέρεται και από τα Vermont State Archives (2019), η **ακεραιότητα** ενός αρχείου αποτελεί μέτρηση τόσο της πληρότητάς του όσο και της διασφάλισης ότι το αρχείο παραμένει αναλλοίωτο από την αρχική του μορφή. Η διατήρηση της ακεραιότητας στην ηλεκτρονική τήρηση αρχείων μπορεί να αποδειχθεί εξαιρετικά δύσκολη καθώς ακόμη και μικρές αλλαγές μπορούν να προκαλέσουν σημαντική ζημιά στα ηλεκτρονικά αρχεία, ακόμη και να τα καταστήσουν μη αναγνώσιμα. Συνεπώς, η διατήρηση της ακεραιότητας ενός αρχείου είναι άκρως σημαντική ως προς τη διασφάλιση ότι το αρχείο μπορεί να χρησιμοποιηθεί και αξιοποιηθεί. Επιπλέον, με την ευκολία τόσο ακούσιας όσο και εκούσιας αλλαγής ψηφιακών αρχείων και τη δυσκολία εντοπισμού αλλαγών σε αρχεία εντός συστημάτων που δεν έχουν σχεδιαστεί για τον πλήρη έλεγχο των ενεργειών των χρηστών τους, μπορεί να αποδειχθεί δύσκολο ή αδύνατο να εντοπιστούν αλλαγές σε αρχεία χωρίς ισχυρά συστήματα που παρακολουθούν την ακεραιότητα αυτών των αρχείων. Επιπλέον, χωρίς το πλήρες αρχείο, μπορεί να χαθεί πολύτιμο περιεχόμενο, καθιστώντας άκυρη τη σημασία του αρχείου.

Άλλο ένα σημαντικό χαρακτηριστικό αποτελεί η **χρηστικότητα** ενός αρχείου, δηλαδή το πόσο εύκολα μπορεί να εντοπιστεί, να ανακτηθεί, να παρουσιαστεί και να ερμηνευτεί, και συχνά αυτό μπορεί να είναι η πιο απαιτητική απαίτηση. Πιο συγκεκριμένα, για να είναι χρήσιμα τα αρχεία, πρέπει να είναι διαθέσιμα και ερμηνεύσιμα. Τα αρχεία σε μη αναγνώσιμες γλώσσες, κωδικοποιήσεις ή μορφότυπα παλαιού τύπου μπορεί μεν να είναι αυθεντικά, αξιόπιστα και να έχουν ακεραιότητα, αλλά μπορεί να μην είναι πλέον αξιοποιήσιμα. Μια μεγάλη πρόκληση τόσο για τη διαχείριση αρχείων όσο και για τη μακροπρόθεσμη ψηφιακή διατήρηση είναι η συνεχής παροχή της ίδιας ποιότητας πρόσβασης στην πληροφορία, παρά τις συνεχώς μεταβαλλόμενες συνθήκες.

Σύμφωνα με τα Vermont State Archives (2019), ως τώρα η πλειονότητα των αρχείων έχει γίνει σε αναλογική μορφή που δεν έχει σχεδόν καμία σύνδεση με τον Ιστό ή με οποιοδήποτε ηλεκτρονικό σύστημα οπότε θα πρέπει να γίνουν αλλαγές σε αυτή την τεχνολογική υποδομή.

Αρχικά το κράτος θα πρέπει να εξετάσει το ενδεχόμενο να ξεκινήσει με μια ηλεκτρονική λογιστική/τήρηση αρχείων. Ωστόσο, η υλοποίηση του θα απαιτούσε πραγματικό συντονισμό και συνεργασία από όλους τους κρατικούς φορείς καθώς και έναν κρατικό φορέα που θα επιβλέπει τη μετάβαση από τη φυσική μορφή (χαρτί) στην ηλεκτρονική και θα διασφαλίζει ότι οι προσπάθειες ψηφιοποίησης έγιναν με συνέπεια.

Η τεχνολογία αποτελεί εργαλείο και, όπως κάθε εργαλείο, μπορεί να αποδειχθεί αποτελεσματική εάν χρησιμοποιηθεί κατάλληλα. Όταν δεν εφαρμόζεται, ωστόσο, μπορεί να προκαλέσει αύξηση του κόστους, αναποτελεσματικότητα, μακροπρόθεσμες εξαρτήσεις και συνέπειες που απαιτούν ακόμη περισσότερες επενδύσεις για να αναιρεθούν. Μια καλώς αυτοματοποιημένη διαδικασία δημιουργεί αποτελεσματικότητα ενώ μια κακώς αυτοματοποιημένη διαδικασία δημιουργεί αναποτελεσματικότητα. Επομένως, η αξιολόγηση και η βελτίωση της διαδικασίας είναι ζωτικής σημασίας και ακολουθεί η απόκτηση της τεχνολογίας.

Η χρήση της τεχνολογίας στην κρατική διαχείριση αρχείων έχει επεκταθεί τα τελευταία χρόνια και έτσι πολλοί δημόσιοι φορείς σήμερα χρησιμοποιούν ηλεκτρονικά συστήματα για τη διαχείριση των πληροφοριών τους. Τα αρχεία που διατηρούνταν αρχικά σε αναλογική μορφή, όπως βιβλία ή καθολικά, τώρα σαρώνονται τακτικά σε ηλεκτρονικά συστήματα διαχείρισης αρχείων, καταχωρούνται χειροκίνητα ή επεξεργάζονται ψηφιακά σε βάσεις δεδομένων ή απλώς αποτελούν πλέον ηλεκτρονικά δεδομένα.

Όπως αναφέρεται στα Vermont State Archives (2019), η πρόκληση της τήρησης αρχείων σε ηλεκτρονική μορφή είναι η αυξανόμενη προσδοκία παροχής, κατά παραγγελία, δεδομένων που έχουν αναδιοργανωθεί και έχουν γίνει προσβάσιμα σε διάφορες μορφές και περιβάλλοντα, καθώς και η προσαρμογή στις συνεχώς μεταβαλλόμενες ανάγκες του κοινού. Η συνέπεια αυτής της μεταφοράς δεδομένων μέσω διαφορετικών μορφών και μορφοτύπων είναι συχνά ότι πολλά υπολείμματα, όπως έντυπες εφαρμογές των οποίων η χρησιμότητα έχει εξαντληθεί μετά την καταχώρηση τους στη βάση δεδομένων, υπερβολικές αναφορές ή συλλεγμένα δεδομένα που δεν εξυπηρετούν πλέον κανένα σκοπό, μένουν πίσω. Η διαχείριση αυτού του μεγάλου όγκου δεδομένων έχει γίνει όλο και πιο περίπλοκη και επαχθής για κάθε είδους δημόσιο φορέα. Επιπλέον, το εύρος αυτού του μετασχηματισμού δεδομένων δεν περιλαμβάνει μόνο τα φυσικά ή ψηφιακά χαρακτηριστικά του ίδιου του αρχείου, αλλά και το περιβάλλον στο οποίο βρίσκονται τα αρχεία.

Ωστόσο, ακόμη και μέσα σε τμήματα και μονάδες του ίδιου οργανισμού, δύο ηλεκτρονικά συστήματα μπορεί να έχουν πολύ διαφορετικά περιβάλλοντα αποθήκευσης, λαμβάνοντας υπόψη ότι το λειτουργικό σύστημα, η μορφή βάσης δεδομένων, τα μορφότυπα των αρχείων και άλλες πτυχές μπορεί να διαφέρουν. Η διασφάλιση της διαλειτουργικότητας μεταξύ ηλεκτρονικών συστημάτων αποτελεί πρόκληση, ειδικά όταν τα δεδομένα διαβιβάζονται τακτικά μεταξύ διαφορετικών υπηρεσιών και διαφορετικών δικαιοδοσιών. Σε αντίθετη περίπτωση, τα δεδομένα μπορεί να χαθούν, οι διαδικασίες μπορεί να καθυστερήσουν και οι υπηρεσίες να διακοπούν. Κάθε πρόσθετη μορφή αρχείου, περιβάλλον λογισμικού ή ανάγκη υλικού, προσθέτει μια άλλη απαίτηση στον περίπλοκο ιστό των αλληλοεπιδρώντων τεχνολογικών λύσεων.

Σύμφωνα με την Lemieux (2016a), Στο ψηφιακό περιβάλλον, μια ηλεκτρονική εγγραφή αποτελείται από οκτώ θεμελιώδη στοιχεία:

1. μέσο: το φυσικό φορέα του περιεχομένου του μηνύματος.
2. φυσική μορφή: τα τυπικά χαρακτηριστικά του ηλεκτρονικού αρχείου (π.χ. γραφή, γλώσσα και ειδικοί χαρακτήρες) που είναι απαραίτητα για να γίνει κατανοητό το αρχείο από τον χρήστη.
3. πνευματική μορφή: τα τυπικά χαρακτηριστικά που αντιπροσωπεύουν και επικοινωνούν τη δράση στην οποία εμπλέκεται η εγγραφή και περιλαμβάνει διαμόρφωση πληροφοριών, άρθρωση περιεχομένου και σχολιασμούς.
4. περιεχόμενο: το ίδιο το μήνυμα που προορίζεται να μεταφέρει η εγγραφή.
5. δράση: η πράξη και η πρόθεση που οδηγούν στη δημιουργία του αρχείου.
6. πρόσωπα: τα άτομα που συμμετέχουν στη δημιουργία του αρχείου, συμπεριλαμβανομένου του συγγραφέα, του παραλήπτη, του συντάκτη και του δημιουργού (ταυτότητες που αποσαφηνίζονται πάντα στα ηλεκτρονικά αρχεία).
7. αρχειακός δεσμός: το σύμπλεγμα σχέσεων μεταξύ εγγραφών που σχετίζονται με την ίδια ενέργεια που εκφράζεται μέσω φυσικής τοποθεσίας, κωδικών ταξινόμησης ή αριθμών μητρώου.
8. πλαίσιο, το πλαίσιο δράσης στο οποίο συμμετέχει η εγγραφή.

Είναι σημαντικό να σημειωθεί ότι στα ηλεκτρονικά αρχεία, το περιεχόμενο, η μορφή και το μέσο μπορούν να υπάρχουν χωριστά.

Η διασφάλιση της ικανότητας εξακρίβωσης, επαλήθευσης και ελέγχου αξιόπιστων αρχείων είναι απαραίτητη για την αξιολόγηση της τεχνολογίας Blockchain, ειδικά αφού η δυναμική της θεωρείται ότι διαταράσσει μια σειρά βιομηχανιών, όπως η διαχείριση δεδομένων και ταυτότητας, η υγειονομική περίθαλψη, η ασφάλιση και οι οικονομίες peer-to-peer.

Στη συνέχεια, και με βάση τα Vermont State Archives (2019), μετά τη συγκέντρωση των απαιτήσεων, κάθε υποψήφια τεχνολογία πρέπει στη συνέχεια να αξιολογηθεί για να καθοριστεί εάν οι δυνατότητές της είναι σε θέση να ανταποκριθούν στις διαδικαστικές, οικονομικές, νομικές, τεχνολογικές ή άλλες απαιτήσεις. Ορισμένες απαιτήσεις δεν είναι υποχρεωτικές και μπορούν να γίνουν συμβιβασμοί, ωστόσο πολλές (π.χ. θεσμοθετημένες ή ρυθμιστικές) πρέπει να ικανοποιηθούν και ενδέχεται να απαιτούν περίπλοκες λύσεις. Το σύνολο των απαιτήσεων, οι οποίες χωρίζονται σε λειτουργικές και μη λειτουργικές, μπορεί εύκολα να είναι εκατοντάδες ή χιλιάδες στοιχεία, ανάλογα με το μέγεθος, την εμβέλεια και τον αντίκτυπο του συστήματος.

Έτσι, οι νέες τεχνολογίες, και συγκεκριμένα, η τεχνολογία Blockchain, αδιαμφισβήτητα μπορούν να συμβάλλουν στη συνολική βελτίωση και εκσυγχρονισμό της διαχείρισης αρχείων εν γένει και στη μετάβαση στη νέα εποχή. Οι θεμελιώδεις έννοιες και τεχνολογίες που απαρτίζουν την τεχνολογία Blockchain έγιναν γνωστές στις αρχές της δεκαετίας του 1980, ωστόσο η ανάπτυξη της και το ουσιαστικό ενδιαφέρον του κοινού ξεκίνησε το 2008, με τη δημοσίευση της λευκής βίβλου Bitcoin από τον Satoshi Nakamoto. Στο βιβλίο αυτό, ο Nakamoto περιέγραψε το Bitcoin ως μοντέλο συναλλαγών νομισμάτων peer-to-peer. Έκτοτε, έχουν αναπτυχθεί πληθώρα άλλων νομισμάτων και υπηρεσιών χρησιμοποιώντας την τεχνολογία Blockchain, ενώ παράλληλα έχουν γίνει μεγάλες επενδύσεις σε νομίσματα, υπηρεσίες και εταιρείες που την χρησιμοποιούν.

Επιπλέον, λόγω του συνεχούς ενδιαφέροντος για την τεχνολογία Blockchain, τα κρυπτονομίσματα, τα έξυπνα συμβόλαια και άλλες υπηρεσίες που βασίζονται στην παραπάνω τεχνολογία, έχουν οδηγηθεί σε περαιτέρω ανάπτυξη και μελέτη, η οποία έχει αποσαφηνίσει σε ένα βαθμό τόσο την ίδια την τεχνολογία όσο και τα πλαίσια, τα μοντέλα και τις διαδικασίες που μπορούν να αξιοποιήσουν την τεχνολογία. Το συνεχές ενδιαφέρον ιδιωτικών εταιρειών, συμπεριλαμβανομένων τραπεζών και άλλων χρηματοπιστωτικών ιδρυμάτων, ηγετών της τεχνολογίας πληροφοριών, εργολάβων στον τομέα της άμυνας, κατασκευαστών κ.α. έχει οδηγήσει στην περαιτέρω ανάπτυξη και χρηματοδότηση ερευνών



σχετικά με το ενδιαφέρον και την αποτελεσματικότητα στη χρήση του Blockchain απέναντι σε προκλήσεις, όπως η εταιρική διακυβέρνηση, οι οικονομικές συναλλαγές και η διαχείριση ταυτότητας.

Έτσι, το Blockchain δημιουργήθηκε με τη σύνθεση ήδη υπάρχοντων μεθόδων όπως η κρυπτογραφία δημόσιου κλειδιού (public-key cryptography) και η δικτύωση peer-to-peer για να λειτουργήσει ως μια λύση που θα βασίζεται στην κρυπτογραφική απόδειξη και όχι στην εμπιστοσύνη σε οργανισμούς ή άτομα.

Γενικά κάθε χρήστης μπορεί να έχει δύο σετ κλειδιών, ένα δημόσιο και ένα ιδιωτικό, τα οποία συνδέονται μαθηματικά μεταξύ τους. Το ιδιωτικό κλειδί του χρήστη χρησιμοποιείται για την υπογραφή (κρυπτογράφηση) μηνυμάτων και διατηρείται μυστικό, ενώ το δημόσιο κλειδί μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση αυτών των μηνυμάτων και κοινοποιείται δημόσια. Ακόμη, η προέλευση ενός μηνύματος μπορεί να εξακριβωθεί με την προϋπόθεση το μήνυμα να είναι υπογεγραμμένο με το ιδιωτικό κλειδί του χρήστη.

Ένας από τους πρωταρχικούς στόχους, αν όχι ο πρωταρχικός στόχος, της τεχνολογίας Blockchain είναι να μην υπάρχει πλέον ανάγκη για ένα αξιόπιστο τρίτο μέρος. Η ύπαρξη και οι υπηρεσίες ενός διαμεσολαβητή προσθέτουν κόστος και χρόνο διεκπεραίωσης και εκθέτουν τα εμπλεκόμενα μέρη μιας συναλλαγής σε έναν νέο κίνδυνο: κακόβουλη ή επιθετική συμπεριφορά εκ μέρους του διαμεσολαβητή.

Χρησιμοποιώντας την επαλήθευση συναλλαγών peer-to-peer, ο διαμεσολαβητής αντικαθίσταται από ένα δίκτυο, το οποίο κατόπιν συμφωνίας των εμπλεκόμενων μερών αποτελεί πλέον τον ενδιάμεσο. Δεδομένου ότι οι συναλλαγές είναι κρυπτογραφημένες, ο φυσικός ρόλος των μελών αυτού του δικτύου (γνωστοί ως κόμβοι) είναι να αποκρυπτογραφούν αυτές τις συναλλαγές επαληθεύοντάς τις (καθώς σε περίπτωση που δημιουργήθηκαν εσφαλμένα οι συναλλαγές, δεν θα γινόταν σωστά η αποκρυπτογράφηση). Αυτοί οι κόμβοι στο Blockchain του Bitcoin αντισταθμίζονται για αυτό το έργο μέσω της «εξόρυξης» επιπλέον νομισμάτων. Έτσι, το δίκτυο, μέσω του πρωτοκόλλου Blockchain, αντικαθιστά τον ενδιάμεσο. Το τελευταίο κομμάτι αυτής της μεθόδου είναι το λεγόμενο «πρωτόκολλο συναίνεσης» το οποίο αναγκάζει το δίκτυο να συμφωνήσει για την ορθότητα και την οργάνωση των συναλλαγών για να προχωρήσει. Για να το θέσουμε πιο απλά, το έργο της επαλήθευσης των συναλλαγών δεν μπορεί να ολοκληρωθεί από έναν μόνο κόμβο, αλλά η πλειοψηφία πρέπει να επαληθεύσει μεμονωμένες συναλλαγές προτού καταστούν έγκυρες

και μπορούν να προστεθούν στην αλυσίδα. Η απαίτηση πολλαπλών επαληθεύσεων μειώνει σημαντικά την πιθανότητα εσφαλμένων συναλλαγών.

Κάθε συναλλαγή αποτελείται γενικά από:

- i. μια λίστα εισροών (αναφορές σε προηγούμενες συναλλαγές)
- ii. μια λίστα εκροών (αποτελέσματα των συναλλαγών)
- iii. επαληθεύσεις
- iv. χρονικές σημάνσεις

Αυτά τα δεδομένα μαζί παρέχουν ένα συνοπτικό αρχείο συναλλαγών. Μια δέσμη αρχείων που έχουν συγκεντρωθεί, επαληθευτεί, και έχει επόμενες συναλλαγές αφού γίνει μπλοκ. Όλα τα μπλοκ μαζί αποτελούν ένα Blockchain. Αυτά τα μπλοκ σώζονται, αποθηκεύονται και αναφέρονται από τους κόμβους κατά την προσθήκη νέων μπλοκ. Παράμετροι όπως το μέγεθος της συναλλαγής, ο αλγόριθμος κρυπτογράφησης, το μοντέλο συναίνεσης, η δομή του μπλοκ, ποικίλλουν από Blockchain σε Blockchain. Μια αλλαγή σε κάποια από αυτές τις παραμέτρους μπορεί να αλλάξει ριζικά τη φύση του Blockchain (Vermont State Archives, 2019). Αναλυτικότερη παρουσίαση της τεχνολογίας Blockchain θα γίνει στο αντίστοιχο κεφάλαιο παρακάτω.

## **2.2 Ελληνικός Στρατός**

### **2.2.1 Ιστορικά στοιχεία**

Σύμφωνα με τα Γενικά Αρχεία του Κράτους (2018), μέχρι την εποχή του Β' παγκοσμίου πολέμου, τα αρχεία του Στρατού παρέμεναν στους εκδότες τους ή σε φορείς του ενεργού Στρατού (επιτελεία, σχηματισμούς, διοικήσεις, μονάδες, σχολές και υπηρεσίες). Κατά το Β' Παγκόσμιο Πόλεμο, με την κατάρρευση του μετώπου το 1941, η κυβέρνηση κατοχής με τον κίνδυνο απώλειας των αρχείων από τη γενικευμένη διάλυση των φορέων του Στρατού, προχώρησε με ρυθμιστικές υπουργικές αποφάσεις στη συγκρότηση της ΥΣΑ, (για μια περίοδο Υπηρεσία Αρχείων Στρατολογικών και Οικονομικών Βιβλίων Πολέμου 1940 – 1941 (ΥΑΣΟΒ)), με σκοπό να συγκεντρωθούν εκεί όλα τα αρχεία των υπό διάλυση στρατιωτικών φορέων σε πρωτότυπη μορφή για ταξινόμηση και εκμετάλλευση.

Σε συνέχεια της παραπάνω ΕΔΥΕΘΑ, το Υπουργείο Στρατιωτικών (ΥΣ) στις 26 Μαΐου 1941, με την υπ' αριθμ. 29398/ΕΔΥΕΘΑ 29/26 Μαΐου 1941 «Σύσταση Υπηρεσίας Στρατιωτικών

Αρχείων (ΥΣΑ)», συγκρότησε την Υπηρεσία Στρατιωτικών Αρχείων (ΥΣΑ), ως ανεξάρτητη Αρχή υπαγόμενη απ' ευθείας στον Υπουργό Στρατιωτικών, «ἐπὶ σκοπῷ περισυλλογῆς, ταξινομήσεως, διαφυλάξεως τῶν ἀπανταχοῦ τοῦ Κράτους εὑρισκομένων πάσης φύσεως Ἀρχείων Στρατ. Μονάδων, Καταστημάτων καὶ ὑπηρεσιῶν τοῦ Στρατοῦ καὶ Ἀεροπορίας, εἰς τρόπον ὥστε νὰ εἶναι δυνατὴ εὐκόλος καὶ ταχεῖα ἡ παροχὴ ἀναγκαιούντων εἰς τὴν ὑπηρεσίαν ὠφελίμων στοιχείων καὶ πρὸς ἐξυπηρέτησιν τῶν ἀτόμων» (Γενικό Επιτελεῖο Στρατοῦ (ΓΕΣ), 2021).

«Με ρυθμιστικὴ Εγκύκλιο του Γενικοῦ Επιτελεῖου Στρατοῦ (ΓΕΣ) το 1951, καθορίστηκε ὅτι στην ΥΣΑ θα αποστέλλονταν τα αρχεῖα μόνο των διαλυομένων φορέων του Στρατοῦ. Το 1966 ἐκδόθηκε νεότερη ρυθμιστικὴ υπουργικὴ ἀπόφαση, που προέβλεπε ἐκκαθάριση σε τακτικὴ βάση ὅλων των αρχείων των φορέων του Στρατοῦ και ἀποστολὴ τους στην ΥΣΑ. Στα αρχεῖα αὐτὰ συμπεριλήφθηκαν στα τέλη του 1967 και τα ατομικὰ ἐγγράφα του στρατιωτικοῦ και πολιτικοῦ προσωπικοῦ.» (Γενικά Αρχεῖα του Κράτους, 2018).

Ἡ ΥΣΑ ἐφαρμόζει ἀπὸ το 1969 τὴ διαδικασία μικροφωτογράφισης για τους φορεῖς του ΓΕΣ, χωρὶς να καταστρέφει τα πρωτότυπα. Ἡ μικροφωτογράφιση, διαθέτοντας ἀποδεικτικὴ ἰσχὺ και δυνατότητα καταστροφῆς των πρωτοτύπων, θεσμοθετήθηκε ἐπίσημα το 1972 ως το σύστημα ἀρχειοθέτησης ὅλου του δημοσίου τομέα. Τέλος, με τὴν ρυθμιστικὴ υπουργικὴ ἀπόφαση (ΝΔΑ 6/2005 (Γενικό Επιτελεῖο Στρατοῦ (ΓΕΣ), 2021)) το 2005, πραγματοποιήθηκε ἡ συστηματοποίηση τῆς διαδικασίας τήρησης των αρχείων του Στρατοῦ. Ἡ ΥΣΑ ἀποτελεῖ το φορέα ἀρχείων του ΓΕΣ και γενικότερα του Στρατοῦ, και διοικητικὰ υπάγεται στην Διεύθυνση Γραμματειακῆς και Μεταφραστικῆς Ὑποστήριξης του ΓΕΣ (ΓΕΣ / ΔΓΜΥ). (Γενικά Αρχεῖα του Κράτους, 2018).

### **2.2.2 Εγκαταστάσεις**

Σύμφωνα με στοιχεία που παρέχονται ἀπὸ τὴν υπηρεσία (Γενικό Επιτελεῖο Στρατοῦ (ΓΕΣ), 2021), ἡ ΥΣΑ, το 1941 ἐγκαταστάθηκε στο Ἀβερῶφειο Μέγαρο τῆς Σχολῆς Ευελπίδων (νυν ΣΕΘΑ), το 1955 μεταστάθμευσε σε κτήριο στη Ν. Χαλκηδόνα, που εἶχαν κτίσει τα ἰταλικά στρατεύματα κατοχῆς, και το 1965 στο Γαλάτσι, στον χώρο ὅπου στεγάζεται σήμερα το Δημαρχεῖο. Ἀπὸ το 1985 ἕως και σήμερα στεγάζεται σε τρία ἱστορικὰ κτήρια στον Β' Ὑποτομέα του Στρατοπέδου «Ἰλάρχου Νικολάου Βαρύτη», στο Ἄλσος Στρατοῦ. Τα κτήρια τῆς ΥΣΑ, ἐκ των ὁποίων τέσσερα ἔχουν χαρακτηριστεῖ διατηρητέα, περιλαμβάνουν:

- Το διοικητήριο, το οποίο είναι διώροφο σε μορφή προστατευμένου κτηρίου (bunker), κατασκευάστηκε από τον Γερμανικό Στρατό κατοχής το 1941 και υπήρξε το Διοικητήριο και η κατοικία του Γερμανού Φρούραρχου της Αττικής.
- Τις δύο δίδυμες αποθήκες, στις οποίες αποθηκεύεται το φυσικό αρχείο και στεγάζονται το 2ο και 3ο Τμήμα. Κτίστηκαν το 19ο αιώνα (περί το 1880-1890) ως στάβλοι της Ανακτορικής Φρουράς.
- Το πρώην αντλιοστάσιο της πηγής του νερού, που τροφοδοτούσε όλη τη γύρω κατοικημένη περιοχή, περιμετρικά της οποίας συγκεντρώθηκαν τα στρατεύματα υπό τον Σ/χη Ζορμπά κατά το κίνημα του «Στρατιωτικού Συνδέσμου», την 15η Αυγούστου 1909.
- Τη «Φυλακή των Έξι», στην οποία κατά ορισμένους ιστορικούς, κρατήθηκαν για λίγες ώρες οι θεωρούμενοι ως υπεύθυνοι για τις συνέπειες της Μικρασιατικής Καταστροφής, πολιτικοί και στρατιωτικοί, Χατζηανέστης Γεώργιος, Γούναρης Δημήτριος, Γούδας Μιχαήλ, Στρατηγός Ξενοφών, Στράτος Νικόλαος, Πρωτοπαπαδάκης Πέτρος, μέχρι την εκτέλεσή τους, την 15η Νοεμβρίου 1922.

### 2.2.3 Αποστολή

Η Υπηρεσία Στρατιωτικών Αρχείων έχει ως αποστολή (Γενικά Αρχεία του Κράτους, 2018):

- την τήρηση των αρχείων του Στρατού Ξηράς και ορισμένων φορέων του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ) (Σχολών, Υπηρεσιών).
- την τήρηση των ατομικών εγγράφων όλων των στελεχών του Στρατού, του Δικαστικού Σώματος των Ενόπλων Δυνάμεων και των Κοινών Σωμάτων του ΓΕΕΘΑ καθώς και των μονίμων πολιτικών υπαλλήλων του Υπουργείου Εθνικής Άμυνας (ΥΠΕΘΑ) / ΓΕΣ.

Σύμφωνα με τα Γενικά Αρχεία του Κράτους (2018), η ΥΣΑ παρέχει αρχειακό υλικό:

- στο ΓΕΣ και γενικότερα στο ΥΠΕΘΑ και τους φορείς του.
- σε Δικαστικές και Αστυνομικές Αρχές.
- σε Στρατιωτικούς και πολίτες.
- σε λοιπούς δημόσιους και ιδιωτικούς φορείς.

«Συνεργάζεται με τη Διεύθυνση Ιστορίας του Γενικού Επιτελείου Στρατού (ΓΕΣ / ΔΙΣ) και επιστημονικούς φορείς στην Ελλάδα και το εξωτερικό. Παράλληλα, είναι ανοικτή στην έρευνα του κοινού και δίνει στοιχεία από το μη διαβαθμισμένο αρχείο σε ενδιαφερομένους, μετά από αίτημά τους, εφόσον δεν εμπíπτουν στην προστασία των προσωπικών δεδομένων (συμπεριλαμβανομένων των ειδικών αρχείων του στρατιωτικού και πολιτικού προσωπικού). Η απομάκρυνση των αρχείων από τους χώρους της ΥΣΑ απαγορεύεται, πλην των ατομικών εγγράφων που αποστέλλονται για διοικητική / δικαστική χρήση. Τα έγγραφα διακινούνται αποκλειστικά από το υπεύθυνο προσωπικό.».

Ακόμη, όπως αναφέρεται και στα Γενικά Αρχεία του Κράτους (2018), στο πλαίσιο του εκτελούμενου έργου της, η ΥΣΑ, μέσα από μία σειρά αλληλένδετων, συμπληρωματικών ενεργειών στοχεύει:

- στη διαφύλαξη του συνόλου του αρχειακού υλικού σε μορφή μικροφίλμ καθώς και μέρους του έντυπου υλικού με κατάλληλες συνθήκες αποθήκευσης.
- στη δημιουργία ψηφιακής βιβλιοθήκης όλων των αρχείων του Στρατού και των μητρώων όλων των στελεχών του Στρατού.
- στην προβολή στοιχείων για τη Στρατιωτική Ιστορία σημαντικών χρονικών περιόδων.
- στην έρευνα του αρχειακού υλικού και την διάθεση του προς τους φορείς του Δημοσίου και το κοινό.
- στην άριστη εξυπηρέτηση του πολίτη και των Υπηρεσιών η οποία έγκειται στην εύκολη και άμεση αναζήτηση πρωτογενών πληροφοριών από κάθε ερευνητή και πολίτη στην Ελλάδα και στο εξωτερικό.
- στην ολοκλήρωση ενός μοναδικού, μεγάλης ιστορικής αξίας ψηφιακού πολιτιστικού αποθέματος και στην εύκολη πρόσβαση των ενδιαφερομένων σ' αυτό.
- στην προβολή και ανάδειξη σε εθνικό και παγκόσμιο επίπεδο της Στρατιωτικής Ιστορίας του Ελληνικού Στρατού, με τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών.

#### **2.2.4 Συλλογές**

Σύμφωνα με τα Γενικά Αρχεία του Κράτους (2018), οι συλλογές της ΥΣΑ περιλαμβάνουν:

- αρχειακό υλικό του Γενικού Επιτελείου Στρατού (ΓΕΣ) και των υφισταμένων σε αυτό Σχηματισμών, Διοικήσεων, Εθνικών Αντιπροσωπειών, Μονάδων, Σχολών,

Καταστημάτων και Οργανισμών, καθώς και των Μονάδων και των σχολών του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ).

- αρχεία ειδικών θεμάτων (δικαστικά, στρατολογίας, επιστρατεύσεως, πληροφοριών, επιχειρήσεων, όπως και τα αρχεία στρατιωτικών σχολών, ειρηνευτικών αποστολών και ορισμένων ειδικών υπηρεσιών, κτλ).
- ελλιπή γενικά στρατιωτικά αρχεία κυρίως από το 1863.
- πλήρη στρατιωτικά αρχεία περιόδων 1912-13, 1918-19, 1921-22 και στρατιωτικά αρχεία της περιόδου 1940-41.
- πλήρες αρχείο στρατιωτικών νοσοκομείων από το 1920.
- πλήρες στρατιωτικό αρχείο από το 1966 και μετέπειτα.

Από το 1951, στην ΥΣΑ τηρούνται τα αρχεία των διαλυομένων φορέων του Στρατού. Μετά το 1966, τηρούνται όλα τα αρχεία των φορέων του Στρατού, καθώς και τα ατομικά έγγραφα του αποστρατευμένου στρατιωτικού και συνταξιοδοτημένου πολιτικού προσωπικού. Επίσης, τηρούνται αντίγραφα σε φυσική μορφή των ΕΔΥΣ-ΕΔΥΕΘΑ από το 1880 έως και 2010 (Γενικό Επιτελείο Στρατού (ΓΕΣ), 2021).

Σύμφωνα με την ΥΣΑ (2021), η υπηρεσία τηρεί αρχεία σε φυσική μορφή και σε μικροφίλμ, τα οποία έχουν αποδεικτική ισχύ ίση με το πρωτότυπο, σύμφωνα με την κείμενη νομοθεσία. Επίσης, τηρεί μέρος του αρχείου σε ψηφιακή μορφή και είναι υπεύθυνη για την εργασία ψηφιοποίησης του συνόλου του τηρούμενου αρχείου, δηλαδή να μετατρέπει το φυσικό αρχείο και το εγγεγραμμένο σε μικροφίλμ σε ψηφιακό, ώστε να είναι εύκολα προσβάσιμο και διαχειρίσιμο από την Υπηρεσία, και τους εκάστοτε αιτούντες Στρατιωτικούς και Δημόσιους Φορείς, όπως επίσης τους ερευνητές, ιστορικούς και λοιπούς ιδιώτες.

Ενδεικτικά το αρχείο περιλαμβάνει:

- Διοικητικό αρχείο που περιλαμβάνει Ημερήσιες Διαταγές, Φάκελους Σχεδίων Εγγράφων-Σημάτων, Πορίσματα προανακρίσεων-ΕΔΕ, Βιβλία απολεσθέντων κ.λπ.
- Αρχείο στρατολογικής φύσεως των τελευταίων 100 κλάσεων (121 χρόνια από το έτος γέννησης)
- Αρχείο υγειονομικής φύσεως όπως Φύλλα νοσηλείας νοσηλευθέντων σε νοσοκομεία, Βιβλία ασθενών, Βιβλία παραπομπής ασθενών σε επιτροπές

απαλλαγών, Βιβλία εισερχομένων και εξερχομένων ασθενών σε νοσοκομεία, Βιβλία γνωματεύσεων ή αποφάσεων επιτροπών απαλλαγών κ.λπ.

- Ειδικό Αρχείο Στρατιωτικών Υπηρεσιών, όπως Στρατιωτικών Δικαστηρίων (πλην αποφάσεων), Στρατολογίας, Επιστρατεύσεως, Πληροφοριών, Επιχειρήσεων, Εκπαιδεύσεως, Οργανώσεως, Διαχειρίσεως Υλικού-Εφοδίων, Οικονομικών, Γεωγραφικής Υπηρεσίας Στρατού κ.λπ.

Το συνολικό αρχείο της ΥΣΑ διαθέτει περίπου:

- 91.000 ατομικούς φάκελους αποστρατευμένου στρατιωτικού και συνταξιοδοτημένου πολιτικού προσωπικού του στρατού ξηράς
- 70.000.000 σελίδες φυσικού αρχείου Φορέων και Μονάδων του στρατού ξηράς
- 65.000 μικροφίλμ που αντιστοιχούν σε 400.000.000 σελίδες αρχείου
- 20.895.746 σελίδες ηλεκτρονικού αρχείου.

### **2.2.5 Κατηγορίες αρχείων**

Το αρχείο της ΥΣΑ, αναλόγως της φύσεως και του θέματος, ταξινομείται στις ακόλουθες κατηγορίες:

- Διοικητικής Φύσης: Προσωπικού, Δικαστικών Θεμάτων, Στρατολογίας και Επιστράτευσης)
- Πληροφοριών
- Επιχειρήσεων-Εκπαίδευσης-Οργάνωσης
- Υγειονομικής Φύσης (φάκελοι υγειονομικής κατάστασης)
- Διαχειριστικής Φύσης: Διαχείρισης Υλικών και Εφοδίων, Χρηματικού και Ειδικό Αρχείο Χρηματικού
- Αρχεία Διαφόρων Θεμάτων και Υπηρεσιών: Γεωγραφικής Υπηρεσίας Στρατού (ΓΥΣ), Στρατιωτικών Σχολών, Ειρηνευτικών Αποστολών.

Διευκρινίζεται ότι, σε ό,τι αφορά στα «Διατηρητέα Ιστορικά Στοιχεία» του Γενικού Επιτελείου Στρατού (ΓΕΣ), υπεύθυνος φορέας τήρησης είναι η Διεύθυνση Ιστορίας Στρατού (ΓΕΣ/Δ4) (Γενικό Επιτελείο Στρατού (ΓΕΣ), 2021).

## 2.2.6 Ψηφιακή εποχή

Σύμφωνα με το Υπουργείο Εθνικής Άμυνας (2016), η Υπηρεσία Στρατιωτικών Αρχείων (ΥΣΑ) διατηρεί αρχείο που εκτείνεται ως το 1895 και γίνεται καθημερινά αποδέκτης πλήθους αιτημάτων τόσο από ερευνητές – μελετητές – ιστορικούς, όσο και από απλούς πολίτες και διάφορες δημόσιες υπηρεσίες. Έτσι κατέστη αναγκαία η τεχνολογική εξέλιξη της υπηρεσίας μέσω της ψηφιοποίησης των συλλογών της.

Πιο συγκεκριμένα, την χρονική περίοδο μεταξύ Ιουνίου 2012 και Ιανουαρίου 2014 υλοποιήθηκε έργο ψηφιοποίησης με τίτλο «Ψηφιοποίηση, Τεκμηρίωση και Ανάδειξη Ιστορικού Αρχείου Υπηρεσίας Στρατιωτικών Αρχείων». Μέσω του έργου αυτού και της ανάγκης για διατήρηση του ιστορικού αυτού αρχείου, χωρίς τον κίνδυνο της φθοράς του χρόνου, το υλικό της ΥΣΑ ψηφιοποιήθηκε, οργανώθηκε και αρχειοθετήθηκε με τρόπο τέτοιο, που η πρόσβαση σε αυτό έγινε πιο εύκολη, ενώ παράλληλα διασώθηκαν παλαιά έγγραφα, στα οποία η φθορά του χρόνου ήταν εμφανής.

Στα πλαίσια του έργου, έγινε προμήθεια του απαραίτητου υλικού και λογισμικού, ενώ αναπτύχθηκε διαδικτυακός τόπος και ψηφιακές υπηρεσίες Δημόσιας Διοίκησης. Παράλληλα το ιστορικό αρχείο επεξεργάστηκε ψηφιακά και τεκμηριώθηκε, με τέτοιο τρόπο ώστε να είναι εύκολα προσβάσιμο για κάθε ενδιαφερόμενο. Σε ειδικά σχεδιασμένες Βάσεις Δεδομένων, βρίσκονται πλέον οργανωμένα έγγραφα Διοικητικής, Υγειονομικής και Στρατολογικής φύσεως, ενώ με τις ψηφιακές υπηρεσίες δίνεται η δυνατότητα έκδοσης προσωπικών εγγράφων (πιστοποιητικά προϋπηρεσίας, συνταξιοδότησης) με μεγαλύτερη ευελιξία και αξιοπιστία. Παράλληλα όμως προβάλλεται και το εθνικό πολιτιστικό απόθεμα, κάτι που μέχρι τώρα δεν γινόταν εύκολα, λόγω του ευαίσθητου ως προς τη συντήρηση χαρακτήρα του.

Όπως αναφέρεται και από την ίδια την υπηρεσία (Γενικό Επιτελείο Στρατού (ΓΕΣ), 2021), η ψηφιοποίηση αποτελεί ως γνωστόν καθοριστικό παράγοντα για την επιβίωση και την ενίσχυση της ιστορίας, του πολιτισμού, της επιστήμης και όλων των στοιχείων που καθορίζουν την καλούμενη συλλογική και εξελισσόμενη μνήμη των διαφόρων κοινωνιών, εθνοτήτων, λαών ενώ είναι επίσης καθοριστική και για την οικονομική ανάπτυξη. Πιο συγκεκριμένα, η ψηφιοποίηση αποτελεί ένα μέσο για την προώθηση σημαντικών στόχων, στους οποίους περιλαμβάνονται και οι ακόλουθοι:



- Η διατήρηση της πολύτιμης πληροφορίας που περιέχουν μέσα όπως οι εικόνες, οι φωτογραφίες, τα έργα τέχνης, τα βιβλία, οι εφημερίδες, τα σχέδια, οι χάρτες, τα αφίσες, τα χειρόγραφα, τα κινηματογραφικά έργα κλπ. Μερικά από τα προαναφερόμενα αντικείμενα καταστρέφονται ή αλλοιώνονται από τη φθορά του χρόνου ή από κάποιο συμβάν. Άλλα πολιτιστικά αγαθά, όπως παραδόσεις και μύθοι, σβήνουν στο πέρασμα του χρόνου. Η ψηφιοποίηση δημιουργεί ψηφιακά υποκατάστατα των υλικών και άυλων αγαθών, περισώζοντας την πολύτιμη πληροφορία που περιέχουν.
- Η ενίσχυση του ρόλου που έχει το πολιτιστικό αγαθό, αφού η αντίστοιχη πληροφορία μπορεί να ανευρεθεί πιο εύκολα και να συνδυαστεί με διαφορετικές πηγές, έτσι ώστε να καταστεί χρήσιμη για την έρευνα, τη μελέτη, την εκπαίδευση κ.λπ.
- Η προβολή (που συμβάλλει καθοριστικά και στην προαναφερόμενη ενίσχυση) των πολιτιστικών αγαθών, μέσα από το Διαδίκτυο αλλά και με την παραγωγή ηλεκτρονικών εκδόσεων (CD, DVD, εφαρμογές, αφιερώματα) για την εκπαίδευση και τον πολιτισμό, την παραγωγή έντυπου υλικού (π.χ. βιβλία και αφίσες) και άλλες παρουσιάσεις/εκδηλώσεις.
- Η οικονομική ανάπτυξη μέσω και της προβολής των πολιτιστικών αγαθών και της αξιοποίησης του πολιτιστικού περιεχομένου σε αχανείς αγορές, όπως η Εκπαίδευση, η Ψυχαγωγία και ο Τουρισμός.
- Η προστασία και η διασφάλιση της πρόσβασης στο ψηφιακό περιεχόμενο που έχει δημιουργηθεί. Για την εκπλήρωσή του είναι απαραίτητη η αντιμετώπιση προβλημάτων, όπως οι απαρχαιωμένοι τύποι αρχείων ή αποθηκευτικών μέσων. Το ψηφιακό περιεχόμενο, όμως, κινδυνεύει και από φυσικές καταστροφές, περιβαλλοντικούς παράγοντες και ανθρώπινες παρεμβάσεις. Για την περίπτωση που συμβεί κάτι τέτοιο, καλό είναι να υπάρχει ένα σχέδιο αντιμετώπισης καταστροφών.
- Η μακροπρόθεσμη διατήρηση του ψηφιακού αντιγράφου και των μεταδεδομένων του αποτρέπει την επανάληψη της ψηφιοποίησης, συμβάλλοντας στην προστασία των ευαίσθητων πρωτοτύπων και στην αποφυγή επένδυσης επιπλέον χρημάτων και χρόνου για τον ίδιο σκοπό. Το θέμα αυτό απασχολεί τη διεθνή κοινότητα και

αποτελεί θέμα έρευνας τα τελευταία χρόνια, ωστόσο σαφής λύση δεν έχει δοθεί μέχρι τώρα.

Όπως προκύπτει από το Υπουργείο Εθνικής Άμυνας (2016), στους ωφελούμενους του παρόντος έργου περιλαμβάνονται:

- Επιστημονικός κόσμος (ερευνητές, μελετητές): Ο επιστημονικός κόσμος αποκτά μια πληρέστατη και έγκυρη ψηφιακή βιβλιοθήκη. Το σημαντικό ιστορικό αρχείο της Υ.Σ.Α. έχει τεθεί στη διάθεση κάθε ενδιαφερόμενου, παρέχοντας ένα ανεκτίμητο εργαλείο για την επιτέλεση του ερευνητικού έργου τους.
- Εκπαιδευτικοί / Ακαδημαϊκοί φορείς: Ο ακαδημαϊκός κόσμος που ασχολείται με τη νεότερη και σύγχρονη ελληνική ιστορία αποκτά μια πληρέστατη πηγή με άμεσο αποτέλεσμα την τεκμηριωμένη υποστήριξη των καθηγητών στη διδασκαλία των συγκεκριμένων θεμάτων αλλά και την παροχή προς τους σπουδαστές και φοιτητές απεριόριστου ψηφιοποιημένου υλικού σχετικού με το αντικείμενο των σπουδών τους.
- Απλοί πολίτες και Ειδικές ομάδες κοινού (ΑΜΕΑ, σύλλογοι): Κάθε ενδιαφερόμενος μπορεί να αποκτήσει πλήρη πρόσβαση σε σημαντικά ιστορικά αρχεία και σε ανεκτίμητη και δυσεύρετη γνώση. Ειδικά οι άρρενες πολίτες έχουν τη δυνατότητα να λαμβάνουν πιστοποιητικά προϋπηρεσίας, πιστοποιητικά για συνταξιοδότηση και άλλα χρήσιμα έγγραφα με μεγαλύτερη ευελιξία και αξιοπιστία, χαμηλότερο κόστος, υψηλότερη ποιότητα και ταχύτητα. Έτσι θα αναπτυχθεί αίσθημα εμπιστοσύνης έναντι του ΥΠΕΘΑ.
- Υπουργεία και φορείς του ευρύτερου Δημόσιου τομέα: Λόγω της άμεσης πρόσβασής τους στο αρχείο της Υ.Σ.Α. απλοποιείται ροή των εργασιών τους.

Συνεπώς, τα αναμενόμενα αποτελέσματα από την υλοποίηση του έργου περιλαμβάνουν:

- Τη δημιουργία άρτια οργανωμένης ψηφιακής βιβλιοθήκης με το περιεχόμενο των ως άνω αρχείων αποθηκευμένο σε ψηφιακή μορφή, οργανωμένο σε θεματικούς καταλόγους και με πλήρη κωδικοποίηση και τεκμηρίωση κάθε αντικειμένου, έτσι ώστε να καλύψει τις ανάγκες του καθηγητή, του ιστορικού, του μελετητή, του ερευνητή, του δημοσιογράφου, του απλού πολίτη.

- Τη δημιουργία έξυπνου μηχανισμού αναζήτησης και εύρεσης υλικού πληροφόρησης και τεκμηρίωσης.
- Την ενίσχυση του επιστημονικού ενδιαφέροντος και την υποβοήθηση της έρευνας στο πεδίο της πολεμικής ιστορίας.
- Την προσέλκυση του ενδιαφέροντος από το ευρύ κοινό σε θέματα πολεμικής ιστορίας.
- Την ενίσχυση της πρόσβασης των μελών της εκπαιδευτικής κοινότητας, προκειμένου να ενημερώνεται, να αιτείται και να λαμβάνει έγγραφα.
- Την απλοποίηση και τον επανακαθορισμό σύγχρονων ηλεκτρονικών διαδικασιών για τη χορήγηση πιστοποιητικών με σκοπό τη μείωση χρόνου και του λειτουργικού κόστους εξυπηρέτησης, τον περιορισμό των λαθών και την αύξηση αξιοπιστίας.
- Την εξασφάλιση ενιαίας και ισότιμης εξυπηρέτησης των πολιτών.
- Την αποτελεσματική διαφύλαξη του υλικού της ΥΣΑ που υπάρχει σε αναλογική μορφή από τη φθορά του χρόνου μέσω της ψηφιοποίησής του.
- Τη βελτίωση της ποιότητας ζωής των πολιτών με την ανάπτυξη ψηφιακών υπηρεσιών Δημόσιας Διοίκησης καθώς και την ενιαία και ισότιμη συμμετοχή τους μέσω της σχεδιαζόμενης διαδικτυακής πρόσβασης στις πληροφορίες.
- Τη βελτίωση των σχέσεων ΥΣΑ – πολίτη.
- Την ανάπτυξη των δυνατοτήτων αμφίδρομης επικοινωνίας, με όλους τους πολίτες σε εθνικό και διεθνές επίπεδο.

## **2.3 Διεθνής πραγματικότητα**

### **2.3.1 Ηνωμένο Βασίλειο**

Όπως τονίζεται από το Ministry Of Defence (2014), το Υπουργείο Άμυνας και οι υπηρεσίες των ενόπλων δυνάμεων αποτελούν μεγάλες, ετερογενείς και σύνθετες οργανώσεις των οποίων οι αποφάσεις και οι ενέργειες επηρεάζουν πολλούς ανθρώπους, συχνά για μεγάλες περιόδους. Οι διάφορες επιχειρηματικές μονάδες του Υπουργείου έχουν ανάγκη να καταγράφουν αποφάσεις και ενέργειες όχι μόνο για δική τους χρήση αλλά και για ευρύτερη χρήση. Ωστόσο, αυτές οι αποφάσεις και ενέργειες είναι ανοιχτές σε νομική, κοινοβουλευτική,

προσωπική αλλά και αμφισβήτηση μέσω των μέσων ενημέρωσης, συχνά πολλά χρόνια μετά το γεγονός. Οι επιχειρηματικές μονάδες, είτε είναι οι δημιουργοί της δράσης είτε οι διάδοχοι, πρέπει να γνωρίζουν τι συνέβη και γιατί.

Το παραπάνω εγχειρίδιο προορίζεται για όλο το προσωπικό του Υπουργείου Άμυνας, στρατιωτικό και πολιτικό. Όπου υπάρχουν νόμιμες διαφορές στη διαδικασία, αυτές καθίστανται σαφείς, αλλά κατά κύριο λόγο η πολιτική και οι διαδικασίες προορίζονται να ισχύουν για όλους. Καθορίζεται έτσι η πολιτική που εφαρμόζεται σε όλο το Υπουργείο Άμυνας, δηλαδή στα κεντρικά γραφεία του Υπουργείου, στα TLB (“Top Level Budget/δημοσιονομικές περιοχές ανωτάτου επιπέδου”: οργανωτικές ομάδες του Υπουργείου Άμυνας άμεσα υπεύθυνες για τον προγραμματισμό, τη διαχείριση και τη διανομή των δυνατοτήτων του οργανισμού), στους σχηματισμούς και τις μονάδες Υπηρεσίας και στις Υπηρεσίες Άμυνας. Όπου οι κανονισμοί που διέπουν τα διάφορα μέρη του Υπουργείου Άμυνας διαφέρουν, αυτό γίνεται σαφές.

#### 2.3.1.1 Είδη αρχείων που δημιουργούνται στο πλαίσιο των δραστηριοτήτων ενός οργανισμού άμυνας

- Λειτουργικές πληροφορίες: Όλες οι πληροφορίες και τα αρχεία που δημιουργούνται σε λειτουργίες/επιχειρήσεις, συμπεριλαμβανομένων των «βασικών λειτουργικών αρχείων» (βλ. παρακάτω).
- Βασικά λειτουργικά αρχεία: Πρόκειται για αρχεία μεγάλης σημασίας. Αποτελούν υποσύνολο των λειτουργικών πληροφοριών και ορίζονται από τις πολιτικές τήρησης βασικών λειτουργικών αρχείων. Παρέχουν ένα σύνολο πληροφοριών που μπορούν να χρησιμοποιηθούν από τα τμήματα ιστορίας στην ιστορική επιχειρησιακή ανάλυση για να υποστηρίξουν τη λήψη αποφάσεων του Υπουργείου, την ανάπτυξη της επιχειρησιακής ικανότητας και τις διεργασίες μαθημάτων, καθώς και την παροχή μιας βάσης για μεγάλο μέρος του αρχείου που απαιτείται για να υποστηρίξει τις νομικές δραστηριότητες του τμήματος. Αποτελούν επίσης τα αρχεία που το υπουργείο θα μεταφέρει στα Εθνικά Αρχεία για μόνιμη διατήρηση.

Οι μονάδες και οι σχηματισμοί πρέπει να διατηρούν αρχείο των δραστηριοτήτων τους ενώ αναπτύσσονται σε επιχειρήσεις (συμπεριλαμβανομένων των Επιχειρήσεων στο Ηνωμένο

Βασίλειο). Αυτό περιλαμβάνει το βασικό λειτουργικό αρχείο και οποιαδήποτε άλλα αρχεία κρίνεται απαραίτητο να διατηρηθούν προκειμένου να εκπληρώσουν τα καθήκοντά τους ή να λογοδοτήσουν για τις ενέργειές τους. Αυτό το αρχείο συνεισφέρει σε ένα ευρύ φάσμα δραστηριοτήτων του Υπουργείου Άμυνας, από την επικύρωση αιτημάτων συντάξεων πολέμου έως τη σύνταξη επίσημων ιστοριών. Παρέχει:

- Πληροφορίες για την υποστήριξη των τρεχουσών και μελλοντικών επιχειρήσεων.
- Αποδεικτικά στοιχεία ενεργειών και αποφάσεων που μπορεί αργότερα να αποτελέσουν αντικείμενο πειθαρχικής έρευνας.
- Προστασία Μονάδων και Διοικητών έναντι διαφορών.

Παρακάτω παρουσιάζονται ορισμένες ενέργειες, οι οποίες εντάσσονται σε κάποιο ευρύτερο σύνολο αρμοδιοτήτων, χωρίζονται ανάλογα με την αρμοδιότητα του κάθε ατόμου/τμήματος και μπορούν να οδηγήσουν στην παραγωγή ενεργού αρχειακού υλικού στα πλαίσια της ροής εργασιών ενός οργανισμού άμυνας.

<b>Λειτουργική κατηγορία</b>	<b>Είδος/περιεχόμενο παραγόμενου αρχείου</b>
Διαχείριση της μονάδας	<ul style="list-style-type: none"> <li>○ Διαχείριση εγκαταστάσεων</li> <li>○ Υπηρεσίες μεταφορών</li> <li>○ Μετακομίσεις</li> <li>○ Δραστηριότητες επιτροπών</li> <li>○ Διαμονή αξιωματικών/προσωπικού</li> <li>○ Τεχνικά ζητήματα</li> </ul>
Διαχείριση συμμόρφωσης	<ul style="list-style-type: none"> <li>○ Διακυβέρνηση</li> <li>○ Έλεγχος</li> <li>○ Ασφάλεια εγγράφων</li> <li>○ Νομικά ζητήματα</li> <li>○ Διαχείριση και διασφάλιση ποιότητας</li> <li>○ Ασφάλεια [Έλεγχος / Προσωπικό / Φυσική / Πληροφοριών]</li> <li>○ SHEF - Υγεία και ασφάλεια</li> <li>○ Αποκατάσταση καταστροφών</li> </ul>

	<ul style="list-style-type: none"> <li>○ Δώρα και φιλοξενία</li> <li>○ Επιθεωρήσεις</li> <li>○ Ιστορική καταγραφή</li> <li>○ Μηνιαία έκθεση μονάδας</li> </ul>
Διαχείριση προσωπικού	<ul style="list-style-type: none"> <li>○ Προσλήψεις</li> <li>○ Επιλογή προσωπικού</li> <li>○ Εργατικό δυναμικό</li> <li>○ Θέματα προσωπικού</li> <li>○ Ασφάλεια προσωπικού</li> <li>○ Τιμές και Βραβεία</li> <li>○ Επιδόματα</li> <li>○ Θύματα</li> </ul>
Διαχείριση σχέσεων	<ul style="list-style-type: none"> <li>○ Επικοινωνίες</li> <li>○ Εσωτερικές και εξωτερικές εκδηλώσεις</li> <li>○ Συναντήσεις</li> <li>○ Επισκέψεις</li> <li>○ Πληροφορίες διαχείρισης δημοσίων σχέσεων</li> <li>○ Υποθέσεις Πολιτικής Στρατιωτικής Συνεργασίας (CIMIC)</li> <li>○ Συνεργασίες μονάδων</li> <li>○ MoUs (Μνημόνια Συμφωνίας)</li> </ul>
Διαχείριση πόρων	<ul style="list-style-type: none"> <li>○ Διαχείριση προϋπολογισμού</li> <li>○ Προϋπολογισμός και οικονομικά στοιχεία</li> <li>○ Οργανωτικές δομές</li> <li>○ Δημόσιοι και μη δημόσιοι πόροι</li> </ul>

Διοίκηση της μονάδας	<ul style="list-style-type: none"> <li>○ Επικοινωνία της μονάδας (τόσο εσωτερικά/ενδο-υπηρεσιακά όσο και εξωτερικά)</li> <li>○ Προσωπική αλληλογραφία διοικητών</li> <li>○ Έκδοση οδηγιών και εντολών</li> <li>○ Επιχειρηματικές συμβάσεις</li> <li>○ Διαχείριση υπηρεσιών επικοινωνίας</li> <li>○ Διαχείριση έργων</li> <li>○ Συμβόλαια</li> </ul>
Οικονομική διαχείριση	<ul style="list-style-type: none"> <li>○ Τραπεζικά αντίγραφα</li> <li>○ Μισθοί</li> <li>○ Ταχυδρομικά αρχεία / βιβλία</li> <li>○ Οφειλές/υπερπληρωμές/διαγραφές</li> <li>○ Ιστορικά αμοιβών εργαζομένων</li> </ul>

**Πίνακας 1: Αρμοδιότητες, παράγοντες και ενέργειες που οδηγούν στη δημιουργία ενεργού αρχειακού υλικού (Ministry Of Defence, 2014).**

Η σωστή διαχείριση αρχείων είναι απαραίτητη. Υποστηρίζει τις καθημερινές εργασίες εντός εκείνων των οργανισμών που παράγουν αρχεία αλλά και την ευρύτερη ανάγκη του τμήματος για πληροφορία. Δίνει τη δυνατότητα στο Υπουργείο Άμυνας να ανταποκρίνεται στις προκλήσεις και να υποστηρίζει τις ενέργειές του. Χωρίς αυτή, η συμμόρφωση με τις νομοθετικές πράξεις περί Δημοσίων Αρχείων, Προστασίας Δεδομένων και Ελευθερίας της Πληροφορίας είναι αδύνατη.

Συνολικά η κακή και ανεπαρκής διαχείριση αρχείων μπορεί να δημιουργήσει κινδύνους για έναν οργανισμό άμυνας. Ορισμένοι αποτελούν οι εξής (Ministry Of Defence, 2014):

- κίνδυνος για τις τρέχουσες ή μελλοντικές δραστηριότητες.
- κίνδυνος ρήξης με Υπουργούς ή Ανώτερους Στρατιωτικούς Αξιωματικούς.
- κίνδυνος άμεσης ή έμμεσης οικονομικής ζημίας.
- κίνδυνος μειωμένης εμπιστοσύνης του κοινού.
- κίνδυνος ότι το Υπουργείο Άμυνας δεν συμμορφώνεται με νομοθεσία ή/και κανονισμούς ή δεν είναι σε θέση να υποστηρίξει νομικές διαδικασίες.

### 2.3.2 Ηνωμένες Πολιτείες της Αμερικής

Όσα αναφέρονται παρακάτω έχουν δημοσιευθεί από το Department of the Army (2008) και αφορούν τον Ενεργό Στρατό, την Εθνική Φρουρά Στρατού/Εθνοφρουρά Στρατού των Ηνωμένων Πολιτειών και την Εφεδρεία Στρατού των ΗΠΑ, εκτός εάν αναφέρεται διαφορετικά.

#### 2.3.2.1 Ομοσπονδιακά αρχεία

Όπως αναφέρεται από το Department of the Army (2008), σύμφωνα με την ισχύουσα νομοθεσία, τα ομοσπονδιακά αρχεία αποτελούν υλικό τεκμηρίωσης, συμπεριλαμβανομένων:

- γραμμάτων
- μνημονίων
- συμπληρωμένων εντύπων
- στατιστικών και αφηγηματικών εκθέσεων
- γραφικών
- φωτογραφιών
- εγγραφών ήχου και βίντεο
- χαρτών
- αρχιτεκτονικών, μηχανικών και άλλων σχεδίων.

Τα ομοσπονδιακά αρχεία, ανεξάρτητα από τις φυσικές μορφές, περιλαμβάνουν:

- ηλεκτρονικές εγγραφές (e-mail, ψηφιοποιημένες εικόνες κ.λπ.)
- φωτογραφικές εκτυπώσεις και αρνητικά
- ταινίες κινηματογράφου
- ηχογραφήσεις μαγνητοφώνου.

Ακόμη, στα ομοσπονδιακά αρχεία συμπεριλαμβάνονται υλικά που παράγονται ή λαμβάνονται από μια υπηρεσία της κυβέρνησης των ΗΠΑ σύμφωνα με την ομοσπονδιακή νομοθεσία ή σε σχέση με τη συναλλαγή δημόσιας επιχείρησης ενώ προστίθενται σε αυτά και υλικά που διατηρούνται ή είναι κατάλληλα για διατήρηση ως αποδεικτικά στοιχεία



λειτουργιών, οργάνωσης και δραστηριοτήτων της εταιρείας ή που διατηρούνται λόγω της αξίας των πληροφοριών που περιέχουν.

Γενικά, τα έντυπα αρχεία μπορεί να είναι πρωτότυπα ή αντίγραφα, όπως αντίγραφα αρχείων εξερχόμενης αλληλογραφίας ή αντίγραφα που προωθούνται για ενέργεια. Πολλαπλά αντίγραφα του ίδιου εγγράφου μπορεί το καθένα να είναι αρχείο, εάν το καθένα εξυπηρετεί ξεχωριστό διοικητικό σκοπό και εάν φυλάσσονται σε χωριστά συστήματα αρχειοθέτησης ή τήρησης αρχείων. Εάν τα αρχεία που δημιουργούνται ηλεκτρονικά διατηρούνται σε σύστημα τήρησης αρχείων σε έντυπη μορφή (χαρτί), πρέπει να εκτυπωθούν οι απαραίτητες πληροφορίες για να διαμορφωθεί ένα πλήρες αρχείο.

Οι ηλεκτρονικές εγγραφές μπορεί να περιλαμβάνουν δεδομένα σε αυτοματοποιημένα συστήματα πληροφοριών (αρχεία δεδομένων, βάσεις δεδομένων), αρχεία επεξεργασίας κειμένου, ηλεκτρονικά υπολογιστικά φύλλα, μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) και ηλεκτρονικά μηνύματα, αρχεία εικόνας (αντιστοιχισμένα με bit) και άλλες πληροφορίες κειμένου ή αριθμών.

Αντιθέτως, ως «μη αρχεία» (non-records) θεωρούνται έγγραφα τεκμηρίωσης που ανήκουν στην κυβέρνηση των ΗΠΑ και εξαιρούνται από τον ορισμό των αρχείων που προκύπτει από τη νομοθεσία. Περιλαμβάνουν:

- επιπλέον αντίγραφα εγγράφων, όπως αυτά που χρησιμοποιούνται για λόγους αναφοράς
- αποθέματα εκδόσεων
- υλικό βιβλιοθηκών και μουσείων που έχει δημιουργηθεί/αποκτηθεί/διατηρηθεί αποκλειστικά για λόγους αναφοράς ή έκθεσης.

Πιο συγκεκριμένα, στην κατηγορία αυτή εντάσσονται:

- πληροφοριακά αντίγραφα αλληλογραφίας, οδηγιών, εντύπων και άλλων εγγράφων στα οποία δεν έχει καταγραφεί ή ληφθεί διοικητική ενέργεια
- έντυπα δρομολόγησης και φύλλα μετάδοσης που δεν προσθέτουν πληροφορίες σε αυτές που περιέχονται στο μεταδιδόμενο υλικό
- αντίγραφα αλληλογραφίας με υπενθύμιση, συμπλήρωμα ή αναστολή, υπό την προϋπόθεση ότι είναι επιπλέον αντίγραφα των πρωτοτύπων

- διπλότυπα αντίγραφα εγγράφων που τηρούνται στο ίδιο αρχείο
- επιπλέον αντίγραφα έντυπου ή επεξεργασμένου υλικού για τα οποία υπάρχουν πλήρη σύνολα αρχείων, όπως τρέχοντα και αντικατασταθέντα εγχειρίδια που διατηρούνται εκτός του γραφείου που είναι υπεύθυνο για τη διατήρηση του σετ αρχείων
- κατάλογοι, εμπορικά περιοδικά και άλλες δημοσιεύσεις που λαμβάνονται από άλλες κρατικές υπηρεσίες, εμπορικές εταιρείες ή ιδιωτικά ιδρύματα και που δεν απαιτούν καμία ενέργεια και δεν αποτελούν μέρος μιας υπόθεσης στην οποία λαμβάνονται μέτρα
- φυσικά εκθέματα, τεχνουργήματα και άλλα υλικά αντικείμενα χωρίς αποδεικτική αξία.

### 2.3.2.2 Αρχεία ζωτικής σημασίας

Αξίζει να σημειωθεί η εξέχουσα σημασία που έχουν τα αρχεία ζωτικής σημασίας. Αυτά αποτελούν αρχεία που περιέχουν πληροφορίες που μπορεί να χρειαστεί ο Στρατός για τη διεξαγωγή επιχειρήσεων σε συνθήκες έκτακτης ανάγκης ή για την προστασία των νομικών και οικονομικών δικαιωμάτων της Ομοσπονδιακής Κυβέρνησης και των ανθρώπων που εξυπηρετεί. Παραδοσιακά έχουν εντοπιστεί δύο τύποι αρχείων, τα “αρχεία λειτουργίας έκτακτης ανάγκης” (emergency operating records) και τα “αρχεία δικαιωμάτων και συμφερόντων” (rights and interest records) (Department of the Army, 2008).

A. Αρχεία λειτουργίας έκτακτης ανάγκης: αρχεία απαραίτητα για τη συνεχή λειτουργία και την ανασύσταση ενός οργανισμού πριν, κατά τη διάρκεια και μετά από μια έκτακτη ανάγκη εθνικής ασφάλειας ή σε συνθήκες έκτακτης ανάγκης ή καταστροφής. Τα κεντρικά γραφεία, οι κύριες διοικήσεις και ορισμένες δραστηριότητες διατηρούν αντίγραφα των αρχείων λειτουργίας έκτακτης ανάγκης σε προκαθορισμένα σημεία μετεγκατάστασης και εναλλακτικές τοποθεσίες. Τα αρχεία σε αυτήν την κατηγορία περιλαμβάνουν:

1. Σχέδια και οδηγίες έκτακτης ανάγκης, συμπεριλαμβανομένων των πληροφοριών που απαιτούνται για τη λειτουργία του κέντρου επιχειρήσεων έκτακτης ανάγκης και του εξοπλισμού του, σχέδια επαναφοράς αρχείων και σχέδια και διαδικασίες ανάκτησης.

2. Σειρά διαδοχής.
  3. Αντιπροσωπείες εξουσίας.
  4. Αποστολές στελέχωσης έκτακτης ανάγκης, συμπεριλαμβανομένων καταλόγων προσωπικού μαζί με τις διευθύνσεις και τους αριθμούς τηλεφώνου τους που έχουν εκχωρηθεί στο κέντρο επιχειρήσεων έκτακτης ανάγκης ή άλλα καθήκοντα έκτακτης ανάγκης ή εξουσιοδοτημένη πρόσβαση σε κατεστραμμένες εγκαταστάσεις για την εκτίμηση της έκτασης της ζημιάς.
  5. Διαπιστευτήρια πρόσβασης στο κέντρο επιχειρήσεων έκτακτης ανάγκης και διαβαθμισμένη ή περιορισμένη τεκμηρίωση κοντέινερ πρόσβασης, όπως απαιτείται.
  6. Εγχειρίδια λειτουργίας σχεδίων κτιρίων και κτιριακών συστημάτων για όλες τις εγκαταστάσεις της υπηρεσίας.
  7. Απογραφή εξοπλισμού για όλες τις εγκαταστάσεις της υπηρεσίας.
  8. Οι κατάλογοι αρχείων γραφείου που περιγράφουν τις σειρές αρχείων και τα ηλεκτρονικά συστήματα πληροφοριών που διατηρούνται στο γραφείο για όλες τις εγκαταστάσεις της υπηρεσίας.
  9. Απογραφές αρχείων ζωτικής σημασίας.
  10. Αντίγραφα των αρχείων προγράμματος της υπηρεσίας (σε οποιοδήποτε μέσο) που απαιτούνται για την εκτέλεση συνεχών κρίσιμων λειτουργιών.
  11. Τεκμηρίωση συστήματος για τυχόν ηλεκτρονικά συστήματα πληροφοριών που χαρακτηρίζονται ως λειτουργικά έκτακτης ανάγκης.
- B. Αρχεία δικαιωμάτων και συμφερόντων: αρχεία απαραίτητα για τη διατήρηση των νόμιμων δικαιωμάτων και συμφερόντων μεμονωμένων πολιτών (συμπεριλαμβανομένων των Στρατιωτών) και του Στρατού. Αυτά τα αρχεία απαιτούν προστασία, αλλά δεν χρειάζεται να διατηρούνται μέσα ή σε κοντινή εμβέλεια σε ένα χώρο λειτουργίας έκτακτης ανάγκης, καθώς δεν θα είναι άμεσα απαιτητά. Τα αρχεία σε αυτήν την κατηγορία περιλαμβάνουν:

1. Αρχεία εισπρακτέων λογαριασμών.
2. Αρχεία κοινωνικής ασφάλισης.
3. Αρχία μισθοδοσίας.
4. Αρχεία συνταξιοδότησης.
5. Αρχεία ασφάλειας.
6. Αρχεία που σχετίζονται με συμβόλαια, δικαιώματα, μισθώσεις ή υποχρεώσεις των οποίων η απώλεια θα αποτελούσε σημαντικό κίνδυνο για τα νομικά και οικονομικά δικαιώματα της Ομοσπονδιακής Κυβέρνησης ή προσώπων που επηρεάζονται άμεσα από τις ενέργειές της.
7. Τεκμηρίωση συστήματος για οποιοδήποτε ηλεκτρονικό σύστημα πληροφοριών που περιέχει αρχεία που ορίζονται ως απαραίτητα για την προστασία δικαιωμάτων.

### 2.3.2.3 Αρχεία συμβάσεων

Σύμφωνα με το Department of the Army (2008), η επίβλεψη διαχείρισης αρχείων των αρχείων των συμβάσεων είναι απαραίτητη για να διασφαλιστεί ότι όλες οι μακροπρόθεσμες ανάγκες τήρησης αρχείων ικανοποιούνται σύμφωνα με τις οδηγίες στο «Πρόγραμμα Τήρησης Αρχείων» του στρατού. Το κυβερνητικό προσωπικό θα εκχωρήσει τις κατάλληλες οδηγίες αναγνώρισης και απόρριψης αρχείων σε όλα τα αρχεία που παραδίδονται από τον εργολάβο. Επιπλέον, τα αρχεία και τα ηλεκτρονικά δεδομένα παρασκηνίου που είναι προς παράδοση στον αναθέτοντα οργανισμό πρέπει να συνοδεύονται από επαρκή τεχνική τεκμηρίωση που να επιτρέπει τη χρήση των αρχείων και των δεδομένων.

- i. Οι εργολάβοι που εκτελούν λειτουργίες προγράμματος που έχουν εξουσιοδοτηθεί από το Κογκρέσο πρέπει να δημιουργούν και να διατηρούν αρχεία για την τεκμηρίωση αυτών των προγραμμάτων. Η σύμβαση πρέπει να περιλαμβάνει απαιτήσεις για την παράδοση όλης της σχετικής τεκμηρίωσης για την εκτέλεση του προγράμματος του εργολάβου.
- ii. Πολλοί άλλοι τύποι συμβάσεων περιλαμβάνουν τη δημιουργία πληροφοριών παρασκηνίου που μπορεί να έχουν αξία για την κυβέρνηση. Όποτε χρειάζεται, οι

υπάλληλοι της υπηρεσίας θα πρέπει να απαιτούν την παράδοση τέτοιων βασικών πληροφοριών πέρα από το τελικό προϊόν. Για παράδειγμα:

1. Οι συμβάσεις για την παραγωγή στατιστικών αναλύσεων θα προσδιορίζουν την παράδοση πληροφοριών παρασκηνίου που μπορεί να έχουν αξία στον αναθέτοντα οργανισμό ή σε άλλους φορείς.
  2. Οι συμβάσεις για την παραγωγή εκθέσεων που αντιπροσωπεύουν την πολιτική του Στρατού θα προσδιορίζουν την παράδοση των πληροφοριών παρασκηνίου που απαιτούνται για την επαλήθευση των ισχυρισμών ή την αιτιολόγηση των συμπερασμάτων.
  3. Οι συμβάσεις έρευνας θα προσδιορίζουν την παράδοση πληροφοριών παρασκηνίου που έχουν αξία για τον αναθέτοντα οργανισμό.
- iii. Μια ρήτρα αναβολής παραγγελίας και παράδοσης πληροφοριών θα πρέπει να περιλαμβάνεται στη σύμβαση για την απόκτηση οποιωνδήποτε δεδομένων/πληροφοριών αρχείων που μπορεί να έχουν αξία για την κυβέρνηση, αλλά δεν έχουν προσδιοριστεί εκ των προτέρων.

#### 2.3.2.4 Αρχεία για μόνιμη ή αρχειακή διατήρηση

Όπως επισημαίνεται από το Department of the Army (2008), οι τύποι αρχείων που αξιολογούνται από τη NARA για μόνιμη ή αρχειακή διατήρηση αφορούν τα παρακάτω:

- Οργάνωση και λειτουργίες
- Επίσημα πρακτικά διοικητικών συμβουλίων και προμηθειών
- Αρχεία εσωτερικών επιτροπών, διυπηρεσιακών και μη ομοσπονδιακών επιτροπών
- Νομικές γνωμοδοτήσεις και σχόλια επί της νομοθεσίας
- Επίσημες οδηγίες, διαδικαστικές εκδόσεις και εγχειρίδια λειτουργίας που σχετίζονται με τις λειτουργίες του προγράμματος
- Επιλεγμένες αξιολογήσεις εσωτερικών λειτουργιών
- Αναλυτικές ερευνητικές μελέτες και περιοδικές εκθέσεις
- Ιστορικά υπηρεσιών και επιλεγμένο υλικό παρασκηνίου
- Ενημερωτικό υλικό
- Αρχεία δημοσίων σχέσεων
- Δημοσιεύσεις

- Επιλεγμένοι οπτικοακουστικοί και γραφικοί δίσκοι
- Αρχεία που τεκμηριώνουν ουσιώδη προγράμματα υπηρεσιών
- Ηλεκτρονικά αρχεία
- Ευρετήρια
- Πληροφορίες διοίκησης
- Κοινωνικοοικονομικές πληροφορίες
- Πληροφορίες φυσικών πόρων
- Πληροφορίες στρατιωτικών ή πολιτικών επιχειρήσεων
- Πολιτικές ή δικαστικές πληροφορίες
- Πληροφορίες ψηφιακής χαρτογράφησης
- Πληροφορίες ψηφιακής αρχιτεκτονικής και μηχανολογίας
- Πληροφορίες εθνικής ασφάλειας και διεθνών σχέσεων
- Επιλεγμένα αρχεία υποθέσεων
- Επιλεγμένες πληροφορίες
- Προσωρινά αρχεία

## 2.4 Τεχνολογία Blockchain

### 2.4.1 Εισαγωγή

Όπως αναφέρθηκε παραπάνω, και προκύπτει από τα Vermont State Archives (2019), «οι θεμελιώδεις έννοιες και τεχνολογίες που απαρτίζουν την τεχνολογία Blockchain έγιναν γνωστές στις αρχές της δεκαετίας του 1980, ωστόσο η ανάπτυξη της και το ουσιαστικό ενδιαφέρον του κοινού ξεκίνησε το 2008, με τη δημοσίευση της λευκής βίβλου Bitcoin από τον Satoshi Nakamoto». Παρόλο που η τεχνολογία Blockchain εφαρμόστηκε για πρώτη φορά σε μεγάλο βαθμό στον χρηματοπιστωτικό κλάδο ως η τεχνολογία που επέτρεψε στο Bitcoin να λειτουργεί, έχει εφαρμογές για πολλούς κλάδους όπως η υγειονομική περίθαλψη, η ασφάλιση, η φαρμακευτική, οι κατασκευές, η ηλεκτρονική ψηφοφορία, οι νομικές συμβάσεις, ο τουρισμός, η ενέργεια και η ταξιδιωτική βιομηχανία (Sadiku et al., 2018).

## 2.4.2 Εφαρμογές της τεχνολογίας Blockchain

### 2.4.2.1 Οικονομικές υπηρεσίες

Γενικά η εφαρμογή της τεχνολογίας Blockchain στον οικονομικό τομέα μπορεί να περιλαμβάνει την ανάπτυξη εφαρμογών σχετικών με τομείς όπως οι παρακάτω:

- Πληρωμές: Πραγματοποιούνται συνήθως με τη χρήση ψηφιακού νομίσματος σε Blockchain, με τοπικές ανταλλαγές μεταξύ του ψηφιακού νομίσματος και των παραστατικών (συνηθισμένων) νομισμάτων (Staples et al., 2017).
- Ψηφιακό συνάλλαγμα (κρυπτονόμισμα). Σύμφωνα με τους Staples et al. (2017), σε ένα Blockchain περιβάλλον μπορούν να αναπτυχθούν νέες μορφές χρημάτων αλλά και μια βάση για μοντέλα κινήτρων που υποστηρίζουν την ακεραιότητα στα συστήματα Blockchain. Τα Blockchain επιτρέπουν τη μεταφορά ψηφιακού νομίσματος μεταξύ των μερών, συχνά χωρίς αυτές τις μεταφορές να υποβάλλονται σε επεξεργασία ή καταγραφή από τράπεζες ή υπηρεσίες πληρωμών. Με τα έξυπνα συμβόλαια, τα Blockchain ενδέχεται να είναι σε θέση να υποστηρίξουν νέα είδη «προγραμματιζόμενου χρήματος», όπου οι πολιτικές που επιβάλλονται αυτόματα συνδέονται με συγκεκριμένα δέματα νομισμάτων. Μια από τις δημοφιλέστερες μορφές ψηφιακών συναλλαγμάτων αποτελεί το Bitcoin, το οποίο αναπτύχθηκε με βάση την τεχνολογία Blockchain. Ακόμη, όπως αναφέρεται και από την Lemieux (2016b), η τεχνολογία Blockchain θεωρείται ολόένα και περισσότερο ως μια λύση σε προβλήματα τήρησης αρχείων όπου υπάρχει ανάγκη για ένα αξιόπιστο δημόσιο καθολικό, όπως καθολικά χρηματοοικονομικών συναλλαγών (π.χ. Bitcoin), κτηματολόγιο, απογραφή πληθυσμού και άλλοι τύποι συστημάτων δημόσιας εγγραφής, ιδίως σε συνδυασμό με «έξυπνα συμβόλαια» που αυτοματοποιούν τους κανόνες που σχετίζονται με ορισμένους τύπους συμβατικών συναλλαγών (π.χ. αγορές ακινήτων). Πιο συγκεκριμένα, η τεχνολογία Blockchain του bitcoin δημιουργεί ένα κατακευματισμένο δημόσιο καθολικό που περιέχει το ιστορικό πληρωμών κάθε Bitcoin που κυκλοφορεί, παρέχοντας απόδειξη του ποιος κατέχει τι ανά πάσα στιγμή. Αυτό το κατακευματισμένο καθολικό αναπαράγεται σε χιλιάδες υπολογιστές – κόμβους του Bitcoin – σε όλο τον κόσμο και είναι δημόσια διαθέσιμο.

- Ανταποκριτική τραπεζική: Μια συμφωνία όπου αμοιβαίοι λογαριασμοί που τηρούνται μεταξύ δύο τραπεζών να αντικαθίστανται από ένα ενιαίο κοινό καθολικό (Staples et al., 2017).
- Εγγραφή, εκκαθάριση και διακανονισμός χρεόγραφων: Η από κοινού ανταλλαγή πληρωμών και οι διακρατήσεις τίτλων θεσπίζονται ως συναλλαγή σε ένα Blockchain (Staples et al., 2017).
- Αγορές: Τα έξυπνα συμβόλαια σε Blockchain μπορούν να παρέχουν μια πλατφόρμα υλοποίησης και αποδοχής προσφορών που σχετίζονται με εμπορία περιουσιακών στοιχείων ή υπηρεσιών. Το Blockchain καταγράφει την κατάσταση αυτών των προσφορών και ξεχωριστά έξυπνα συμβόλαια μπορούν να φέρουν από μόνα τους το ψηφιακό συνάλλαγμα που απαιτείται για την πληρωμή και εκπλήρωση αυτών των προσφορών. Συνεπώς λειτουργεί ως ένα είδος μεσεγγύησης, χωρίς να απαιτείται ένα τρίτο μέρος (π.χ. αξιόπιστος οργανισμός). Ωστόσο, τα Blockchain δεν ενδείκνυνται για συναλλαγές υψηλής συχνότητας στην αγορά (Staples et al., 2017).
- Χρηματοδότηση στο εμπόριο: Στην περίπτωση αυτή το Blockchain χρησιμοποιείται για την τεκμηρίωση εγγράφων που σχετίζονται με το εμπόριο, προκειμένου να μειωθεί ο κίνδυνος δανεισμού και να βελτιωθεί η πρόσβαση στη χρηματοδότηση για τη βιομηχανία. Εδώ τα έξυπνα συμβόλαια θα μπορούσαν να συμβάλλουν στον έλεγχο της εκτέλεσης διεργασιών μεταξύ των οργανισμών και να αυτοματοποιήσουν με διαφάνεια καθυστερημένες πληρωμές ή δόσεις (Staples et al., 2017).

Σύμφωνα με τους Staples et al. (2017), υπηρεσίες όπως οι διεθνείς πληρωμές έχουν ρυθμιστικές απαιτήσεις για τον προσδιορισμό της ταυτότητας των συμμετεχόντων, ως μέρος των πολιτικών για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Έτσι, η ταυτότητα στο Blockchain θεωρείται μερικές φορές ως βασικός παράγοντας για πολλές χρηματοοικονομικές υπηρεσίες στο Blockchain. Από καθαρά τεχνική άποψη, οι πραγματικές ταυτότητες δεν είναι απαραίτητες. Για παράδειγμα, στο Bitcoin, οι συναλλασσόμενοι πράκτορες, οι οποίοι δεν είναι απαραίτητως πρόσωπα, προσδιορίζονται με τη χρήση ψευδωνύμων, με ένα κρυπτογραφικό κλειδί. Επομένως, η διεθνής ανταλλαγή του ψηφιακού νομίσματος Bitcoin μπορεί να πραγματοποιηθεί χωρίς να τηρήσει την πραγματικής ταυτότητας ενός ατόμου.



Ωστόσο, οι ρυθμιστικές απαιτήσεις που αναφέρθηκαν παραπάνω δεν εξαλείφονται με τη χρήση ενός Blockchain συνεπώς το απόρρητο και η εμπιστευτικότητα μπορεί να αποτελέσουν μια πρόκληση κατά την ενσωμάτωση πληροφοριών που σχετίζονται με την ταυτότητα σε ένα σύστημα που βασίζεται σε Blockchain.

#### 2.4.2.2 Κυβερνητικές υπηρεσίες

Σύμφωνα με τους Staples et al. (2017), είναι πλέον ευρέως γνωστό ότι υπάρχουν πολλοί υποσχόμενοι τομείς εφαρμογής για την τεχνολογία Blockchain πέρα από τις χρηματοοικονομικές υπηρεσίες. Τα Blockchain γενικά μπορούν να στοχεύουν στη βελτιωμένη παροχή κρατικών υπηρεσιών ενώ τα ιδιωτικά Blockchain μπορούν να χρησιμοποιηθούν στη διευκόλυνση της ανταλλαγής πληροφοριών και του συντονισμού των διαδικασιών μεταξύ των φορέων εντός της κυβέρνησης. Οι τομείς εφαρμογής που διερευνώνται στις κυβερνήσεις παγκοσμίως περιλαμβάνουν:

- Μητρώα και ταυτότητα: Συμπεριλαμβανομένων περιπτώσεων όπως ταυτότητες και χαρακτηριστικά ατόμων, εταιρειών, συσκευών, αδειοδοτήσεις, προσόντα και πιστοποιήσεις. Η αποθήκευση των καταχωρήσεων ενός μητρώου ή η κρυπτογραφική πιστοποίηση των καταχωρήσεων σε ένα Blockchain μπορεί να διευκολύνει την πρόσβαση και την επικύρωση έναντι του μητρώου. Τα Blockchain θα μπορούσαν επίσης να χρησιμοποιηθούν για τον διαμοιρασμό πιστοποιημένων αναγνωριστικών για άτομα και εταιρείες και αυτά τα αναγνωριστικά θα μπορούσαν με τη σειρά τους να ενεργοποιήσουν άλλες εφαρμογές Blockchain. Ωστόσο, αυτό μπορεί να φέρει ενστάσεις σχετικά με το απόρρητο και την εμπιστευτικότητα (Staples et al., 2017).
- Επιχορηγήσεις και κοινωνική ασφάλιση: Τα έξυπνα συμβόλαια θα μπορούσαν να αυτοματοποιήσουν το συντονισμό των διαδικασιών υποβολής αίτησης, λήψης απόφασης και διανομής πληρωμών σχετικά με επιχορηγήσεις και την κοινωνική ασφάλιση. Με ένα εξελιγμένο περιβάλλον πληρωμών, ένα έξυπνο συμβόλαιο θα μπορούσε αυτόματα να περιορίσει τις πληρωμές σε εγκεκριμένους προμηθευτές ή κατηγορίες δαπανών (Staples et al., 2017).
- Διαχείριση ποσοστών: Οι ποσοστώσεις, οι κατανομές και τα δικαιώματα σε φυσικούς πόρους που χορηγούνται από την κυβέρνηση θα μπορούσαν να

κατανεμηθούν και να εντοπιστούν μέσω ειδικών νομισμάτων (token) που έχουν δημιουργηθεί σε ένα Blockchain. Ανάλογα την περίπτωση, το Blockchain θα μπορούσε να υποστηρίξει μια ανεξάρτητη δευτερεύουσα αγορά για αυτά τα δικαιώματα καθώς δημιουργεί ένα συνεχιζόμενο αμετάβλητο αρχείο καταγραφής ελέγχου αυτών των δικαιωμάτων και της χρήσης τους (Staples et al., 2017).

- Φορολογία: Λειτουργίες που κυμαίνονται από την αυτοματοποιημένη είσπραξη φόρων με τη χρήση έξυπνων συμβάσεων έως τη βελτιωμένη συμμόρφωση με την έγκυρη δημοσίευση εργαλείων φορολογικής ρύθμισης και υπολογισμού ως έξυπνες συμβάσεις στο Blockchain (Staples et al., 2017).

#### 2.4.2.3 Επιχειρήσεις και βιομηχανία

Σύμφωνα με τους Staples et al. (2017), οι πλήρεις προοπτικές της τεχνολογίας Blockchain είναι πιθανό να αξιοποιηθούν εκτός των χρηματοοικονομικών και κυβερνητικών υπηρεσιών. Τα Blockchain αποτελούν μια θεμελιώδη τεχνολογία οριζόντιας πλατφόρμας που μπορεί να χρησιμοποιηθεί σε οποιονδήποτε τομέα της βιομηχανίας, συμπεριλαμβανομένων της γεωργίας, των υπηρεσιών κοινής ωφέλειας, της εξόρυξης, της μεταποίησης, του λιανικού εμπορίου, των μεταφορών, του τουρισμού, της εκπαίδευσης, των μέσων ενημέρωσης, της υγειονομικής περίθαλψης και της οικονομίας διαμοιρασμού (peer-to-peer). Ορισμένες γενικές εφαρμογές στους παραπάνω τομείς παρουσιάζονται παρακάτω:

- Εφοδιαστική αλυσίδα: η παρακολούθηση φυσικών περιουσιακών στοιχείων μέσω αλλαγών στην ιδιοκτησία και τη διαχείριση μπορεί να καταγραφεί και να κοινοποιηθεί μέσω δεδομένων που είναι αποθηκευμένα σε ένα Blockchain. Αυτό παράλληλα δημιουργεί πληροφορίες προέλευσης για τα αγαθά και παρέχει βελτιωμένη ορατότητα της επιμελητείας και ποιότητα της αλυσίδας εφοδιασμού. Σημαντικά γεγονότα στην αλυσίδα εφοδιασμού θα μπορούσαν να συνδεθούν με αυτόματες πληρωμές με τη χρήση έξυπνων συμβολαίων (Staples et al., 2017).
- Αποθήκευση, υπολογισμός και διαχείριση στο Διαδίκτυο των πραγμάτων (IoT): συσκευές συνδεδεμένες στο Διαδίκτυο μπορούν να χρησιμοποιήσουν το Blockchain ως μια συνεχή και διαθέσιμη λύση αποθήκευσης, μπορούν να χρησιμοποιήσουν έξυπνες συμβάσεις για να παρέχουν μια παγκόσμια κατανεμημένη υπολογιστική ικανότητα και μπορούν να βασίζονται στο Blockchain ως ασφαλές κανάλι για τη λήψη

πληροφοριών σχετικά με ενημερώσεις λογισμικού και διαμόρφωσης και δυναμικά εκχωρημένο έλεγχο πρόσβασης (συμπεριλαμβανομένου του ελέγχου φυσικής πρόσβασης, για συσκευές κλειδώματος) (Staples et al., 2017).

- Μετρημένη πρόσβαση σε πόρους και υπηρεσίες: η παρακολούθηση και η πληρωμή για τη χρήση βοηθητικών προγραμμάτων ή υπηρεσιών μπορούν να παρέχονται από συσκευές IoT και σχετικές έξυπνες συμβάσεις (Staples et al., 2017).
- Ψηφιακά δικαιώματα και διαχείριση IP: ένα Blockchain μπορεί να παρέχει ένα αξιόπιστο μητρώο περιουσιακών στοιχείων μέσω ή άλλης πνευματικής ιδιοκτησίας και μπορεί να παρέχει τη δυνατότητα διαχείρισης, ανάθεσης ή μεταφοράς πληροφοριών πρόσβασης και δικαιωμάτων για αυτά τα περιουσιακά στοιχεία. Ωστόσο τα μέσα αυτά δεν αποθηκεύονται απαραίτητα στο ίδιο το Blockchain. Αντίθετα, κρυπτογραφικοί κατακερματισμοί, μεταδεδομένα και άλλα αναγνωριστικά που είναι αποθηκευμένα στο Blockchain ενδέχεται να ενσωματωθούν με μαζική αποθήκευση εκτός του Blockchain (Staples et al., 2017).
- Διαχείριση δεδομένων: ένα Blockchain μπορεί να δημιουργήσει ένα επίπεδο μεταδεδομένων για αποκεντρωμένη κοινή χρήση δεδομένων και ανάλυση. Αν και τα ίδια τα μεγάλα σύνολα δεδομένων είναι απίθανο να αποθηκευτούν εκεί, ένα Blockchain μπορεί να βοηθήσει στον εντοπισμό και την ενοποίηση αυτών των συνόλων δεδομένων και των υπηρεσιών ανάλυσης δεδομένων. Οι μηχανισμοί ελέγχου πρόσβασης που εφαρμόζονται σε ένα Blockchain μπορεί να επιτρέψουν την ευκολότερη ενοποίηση δημόσιων πηγών δεδομένων με ιδιωτικά σύνολα δεδομένων και υπηρεσίες ανάλυσης (Staples et al., 2017).
- Βεβαίωση και απόδειξη ύπαρξης: ένα Blockchain μπορεί να χρησιμοποιηθεί για την καταγραφή αποδεικτικών στοιχείων σχετικών με την ύπαρξη δεδομένων ή εγγράφων, δημιουργώντας μια εγγραφή με χρονική σήμανση ενός κρυπτογραφικού hash των περιεχομένων αυτών των εγγράφων. Αυτό μπορεί να συνδυαστεί με αρχεία βεβαίωσης ή μαρτυρίας αντίστοιχων φυσικών εγγράφων από αξιόπιστα τρίτα μέρη. Ωστόσο, μπορεί να είναι αρκετά δύσκολο να αποδειχθεί η μοναδικότητα ή η ανυπαρξία τέτοιων εγγραφών εγγράφων, εκτός εάν υπάρχει μια ευρέως αποδεκτή αυστηρή μορφολογία ως προς το περιεχόμενό τους (Staples et al., 2017).

- Διατμηματική λογιστική: πολυεθνικές εταιρείες ή μεγάλες επιχειρήσεις με ξεχωριστές επιχειρηματικές μονάδες, συχνά έχουν ανάγκες δικαιοδοσίας ή διακυβέρνησης όχι μόνο για να ελέγχουν τη δική τους εσωτερική λογιστική, αλλά και για να μοιράζονται λογιστικές πληροφορίες με άλλα τμήματα. Μια απλή εφαρμογή της τεχνολογίας Blockchain σε ένα κοινόχρηστο ιδιωτικό δίκτυο μπορεί να δημιουργήσει ένα κοινό κατανεμημένο καθολικό των λογαριασμών μεταξύ των τμημάτων, στις διεπαφές μεταξύ των τμημάτων. Εδώ ο ρόλος της μη απόρριψης είναι ο βελτιωμένος έλεγχος και η διαχείριση αλλαγών των λογιστικών πληροφοριών (Staples et al., 2017).
- Εταιρικές υποθέσεις (ψηφοφορία διοικητικών συμβουλίων και μετόχων και εγγραφές): οι αρχές ψηφοφορίας των μελών του διοικητικού συμβουλίου ή των μετόχων σε εταιρείες θα μπορούσαν να καταγραφούν και να εξουσιοδοτηθούν σε ένα Blockchain. Τα έξυπνα συμβόλαια σε Blockchain θα μπορούσαν να χρησιμοποιήσουν αυτό το αρχείο για να κρίνουν τις ψήφους που διεξάγονται στο Blockchain για συγκεκριμένες κινήσεις. Ούτως ή άλλως οι συναλλαγές Blockchain δεν είναι απαραίτητα κρυφές οπότε ενδέχεται να απαιτούνται κρυπτογραφικοί μηχανισμοί για την πρόληψη πιθανών ανεπιθύμητων στρατηγικών συμπεριφορών κατά την ψηφοφορία (Staples et al., 2017).

### 2.4.3 Περιπτώσεις χρήσης

Η τεχνολογία Blockchain είναι μια τεχνολογία που αναπτύσσεται διαρκώς και έχει ήδη εφαρμοστεί από διάφορους φορείς, υπηρεσίες και εταιρείες δημόσιου και ιδιωτικού τομέα. Σύμφωνα με τους Al Omar et al. (2018), η υπηρεσία του Υπουργείου Άμυνας του Ηνωμένου Βασιλείου εξετάζει το ενδεχόμενο χρήσης Blockchain για τη βελτίωση της αξιοπιστίας ενός δικτύου που χρησιμοποιεί αισθητήρες για την παρακολούθηση εθνικών ανησυχιών ενώ η Houston Kemp, μια εταιρεία τεχνολογίας με έδρα τη Σιγκαπούρη, εργάζεται στην Αυστραλία για να αναπτύξει ένα σύστημα βασισμένο σε Blockchain, το οποίο θα χρησιμοποιείται για τη διατήρηση αρχείων όλων των ερευνητικών πληροφοριών.

Η Franks (2020) παραθέτει ορισμένα παραδείγματα που αξιοποιήθηκε η τεχνολογία Blockchain σε Ευρώπη και Αμερική:

- Λουξεμβούργο: Το IDKeep , μια πλατφόρμα ταυτότητας που σχεδιάστηκε από την Cambridge Blockchain και τη LuxTrust , δημιουργεί ένα hash των εγγράφων ταυτότητας που υποβάλλονται από νέους πελάτες, σημειώνοντας αν το άτομο είναι αναγνωρισμένος πελάτης. Το hash, όχι τα προσωπικά δεδομένα, αποθηκεύονται σε ένα επιχειρηματικό Ethereum Blockchain. Αξίζει να σημειωθεί ότι η χρηματοοικονομική ρυθμιστική αρχή του Λουξεμβούργου έχει έναν κόμβο στο Blockchain, ώστε να μπορεί να εποπτεύει σε πραγματικό χρόνο.
- Πολωνία: Στην περίπτωση αυτή αναπτύχθηκε ένα πρόγραμμα διαχείρισης εγγράφων στον τραπεζικό τομέα. Η PKO BP, μια μεγάλη πολωνική τράπεζα, χρησιμοποιεί Blockchain για να καταγράφει κάθε έγγραφο ως μη αναστρέψιμο hash υπογεγραμμένο με το ιδιωτικό κλειδί της τράπεζας. Ένας πελάτης μπορεί να επαληθεύσει εξ αποστάσεως εάν τα αρχεία που ελήφθησαν είναι αληθή ή αν επιχειρήθηκε τροποποίηση του εγγράφου. Το Trudatum, μια λύση RegTech (ρυθμιστικής τεχνολογίας) που δημιουργήθηκε από την Coinfirm, μπορεί να επαληθεύσει την αυθεντικότητα οποιουδήποτε τύπου αρχείου, συμπεριλαμβανομένων εγγράφων και γραφικών. Με αυτό τον τρόπο, ένα έγγραφο αποστέλλεται στο Trudatum, υπογράφεται ψηφιακά και καταχωρείται στο δημόσιο Blockchain. Έπειτα ο ιδιοκτήτης του λαμβάνει επιβεβαίωση μέσω email. Χρησιμοποιώντας το hash, οποιοσδήποτε παραλήπτης του εγγράφου μπορεί να ελέγξει τα περιεχόμενα του σε σχέση με την εγγραφή που είναι αποθηκευμένη στο Blockchain.
- Ηνωμένο Βασίλειο: Η Medical Chain είναι η πρώτη περίπτωση στον ιατρικό κλάδο στο Ηνωμένο Βασίλειο που χρησιμοποιεί τεχνολογία Blockchain και δέχεται κρυπτονομίσματα (MedTokens) ως πληρωμή για υπηρεσίες υγείας. Η Medical Chain αποθηκεύει αρχεία σχετικά με την υγεία σε ένα Blockchain χρησιμοποιώντας μια δομή διπλής αλυσίδας: Hyperledger Fabric και ένα token ERC20 στο Ethereum. Οι ασθενείς έχουν πρόσβαση και έλεγχο των αρχείων τους ενώ γιατροί, νοσοκομεία, εργαστήρια, φαρμακοποιοί και ασφαλιστές υγείας μπορούν να ζητήσουν άδεια πρόσβασης στο αρχείο ενός ασθενούς για να εξυπηρετήσουν τον σκοπό τους και να καταγράψουν τις συναλλαγές στο κατακευματισμένο καθολικό.

- Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ): Το Υπουργείο Γεωργίας των ΗΠΑ (USDA) ελέγχει και πιστοποιεί ως πρόγραμμα επαληθευμένης διαδικασίας. Η BeefChain είναι η πρώτη εταιρεία Blockchain που έλαβε την παραπάνω πιστοποίηση καθώς το λογισμικό της (BeefChain) χρησιμοποιεί το Blockchain Ethereum για να δημιουργήσει ένα ψηφιακό ίχνος διαφανών, αδιάψευστων εγγραφών που αφορούν όλα τα στάδια της αλυσίδας εφοδιασμού (Franks, 2020).

#### **2.4.4 Περιεχόμενο και κίνδυνοι**

Σύμφωνα με την Franks (2020), η τεχνολογία Blockchain γενικά αποτελεί μια τεχνολογία τήρησης αρχείων που αντικαθιστά την εμπιστοσύνη σε έναν μεσάζοντα (π.χ. μια τράπεζα ή μια κυβερνητική υπηρεσία) με την εμπιστοσύνη στην τεχνολογία (π.χ. μηχανισμός συναίνεσης και δίκτυο peer-to-peer). Τα κατανεμημένα καθολικά είναι εγγραφές που μοιράζονται μεταξύ όλων των μελών του δικτύου (κόμβοι), δίνοντας τη δυνατότητα σε κάθε κόμβο να επαληθεύσει τα σύνολα δεδομένων. Τα παραποιημένα σύνολα δεδομένων εξαιρούνται, επιτρέποντας στο κατανεμημένο καθολικό να παρουσιάσει μια αμετάβλητη ενιαία πηγή αλήθειας. Αυτή η ανατρεπτική καινοτομία έχει τη δυνατότητα να μεταμορφώσει τόσο την προσωπική όσο και την επαγγελματική μας ζωή καθώς είναι κατάλληλη για αρχειακά έγγραφα, τη μακροπρόθεσμη διατήρηση άλλων αρχείων όπως αρχεία ζωτικής σημασίας (π.χ. πιστοποιητικά γέννησης), αρχεία υγειονομικής περίθαλψης, ασφαλιστήρια συμβόλαια ζωής και αρχεία ακινήτων. Ωστόσο, η τεχνολογία κατανεμημένου καθολικού γενικά και η τεχνολογία Blockchain ειδικά, παρουσιάζουν και κινδύνους, όπως τρωτά σημεία, κινδύνους από τη μεριά του προμηθευτή, προβλήματα επεκτασιμότητας, βιωσιμότητας, έλλειψη προτύπων και κανονισμών και μη ελεγμένο κώδικα. Όσο οι εσωτερικοί και εξωτερικοί παράγοντες που επηρεάζουν τις επιχειρηματικές δραστηριότητες οδηγούν σε αλλαγές στον τρόπο διαχείρισης των αρχείων, οι πολιτικές και πρακτικές διαχείρισης αρχείων και διακυβέρνησης πληροφοριών θα επηρεαστούν.

#### **2.4.5 Πλατφόρμες Blockchain**

Σύμφωνα με τη National Archives and Records Administration (NARA) (2019), το Blockchain αποτελείται από μια συλλογή υποκείμενων τεχνολογιών που μπορούν να συνδεθούν μεταξύ

τους με πολλούς τρόπους. Αυτό επιτρέπει στα Blockchain να διαμορφωθούν με πολλούς τρόπους για να εξυπηρετούν διαφορετικούς σκοπούς. Η ανασκόπησή μας σε διάφορες πλατφόρμες Blockchain εντόπισε τέσσερις διαφορετικές προσεγγίσεις που αντιπροσωπεύονται από τις επιλογές που περιγράφονται παρακάτω.

1. Bitcoin: Το Bitcoin είναι ένα κρυπτονόμισμα με μια σχετική πλατφόρμα ανοιχτού κώδικα. Το Blockchain του Bitcoin έχει σχεδιαστεί κυρίως για να υποστηρίξει την ανταλλαγή κρυπτονομισμάτων χωρίς ενδιάμεσο τρίτο μέρος, δεν προϋποθέτει καμία εμπιστοσύνη μεταξύ των μερών και απαιτεί πολλούς αποκεντρωμένους κόμβους για να διασφαλιστεί ότι το Blockchain δεν έχει φθαρεί από κακόβουλους παράγοντες
2. Ripple: Όπως και το Bitcoin, το Ripple βασίζεται σε ένα πρωτόκολλο ανοιχτού κώδικα που χρησιμοποιεί Blockchain για την ανταλλαγή αξίας. Διαθέτει μια καθιερωμένη βάση χρηστών από τοπικές και παγκόσμιες τράπεζες που χρειάζεται να πραγματοποιούν διεθνείς πληρωμές σε πραγματικό χρόνο ενώ επιτρέπει επίσης το εμπόριο αγαθών, περιουσιακών στοιχείων και αντικειμένων αξίας.
3. Ethereum: Ενώ οι δύο παραπάνω πλατφόρμες επικεντρώνονται κυρίως στο εμπόριο των δικών τους (κρυπτο)νομισμάτων, το Ethereum κυκλοφόρησε τον Ιούλιο του 2015 με στόχο την παροχή μιας πλήρως λειτουργικής γλώσσας προγραμματισμού που θα επιτρέπει στους χρήστες να δημιουργούν πλήρεις εφαρμογές με ενσωματωμένο Blockchain. Το Ethereum αποτελεί μια γλώσσα προγραμματισμού ανοιχτού κώδικα και χρηματοδοτούμενη από το κοινό του ενώ οι χρήστες του Ethereum μπορούν να προγραμματίσουν εκτελέσιμα έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές χρησιμοποιώντας το Blockchain.
4. Hyperledger: Το έργο Hyperledger εστιάζει στην ανάπτυξη μιας συλλογικής προσέγγισης ανοιχτής πηγής (open source) στα κατακευματωμένα καθολικά. Αναπτύσσοντας πρότυπα και ένα συνολικό πλαίσιο για τα Blockchain, το Hyperledger έχει κερδίσει την υποστήριξη οργανισμών όπως η Cisco, η American Express και η IBM. Ορισμένες σχολές βιβλιοθηκών και πληροφορικής ενσωματώνουν το Hyperledger στο πρόγραμμα σπουδών τους ενώ η Hyperledger έχει δηλώσει ότι δεν θα δημιουργήσει ποτέ κρυπτονόμισμα.

#### 2.4.5.1 Blockchain και βάσεις δεδομένων

Σύμφωνα με τους Al Omar et al. (2018), η κύρια λειτουργία της κυβέρνησης είναι να διατηρεί δεδομένα ατόμων. Η διαχείριση και η χρήση αυτών των δεδομένων μπορεί να αποδειχθεί δυσκίνητη, ακόμη και για προηγμένες κυβερνήσεις. Διαφορετικές κρατικές υπηρεσίες διαθέτουν αντίστοιχα ξεχωριστές βάσεις δεδομένων, γεγονός που αποτελεί εμπόδιο στην ομαλή ροή δεδομένων μεταξύ διαφορετικών κρατικών υπηρεσιών. Η ύπαρξη τέτοιων πολλαπλών βάσεων δεδομένων αυξάνει επίσης το κόστος της ασφάλειάς τους και έτσι η πιθανότητα παράνομων αλλαγών αυξάνεται σταδιακά. Με το αυξανόμενο μέγεθος των αρχείων, ένα καλό σύστημα τήρησης αρχείων και ανταλλαγής πληροφοριών έχει καταστεί απαραίτητο στο σημερινό παγκόσμιο περιβάλλον. Οι κρατικές υπηρεσίες πρέπει να επικοινωνούν μεταξύ τους αλλά και διεθνώς με αντίστοιχες υπηρεσίες άλλων χωρών οπότε η ύπαρξη αρχείων με ακρίβεια και χρονική σήμανση διευκολύνει σημαντικά το έργο τους.

Έτσι έρχονται στο προσκήνιο τα Blockchain. Το καθολικό του Blockchain διασφαλίζει ότι κανένα μέρος δεν μπορεί να ελέγξει το peer-to-peer δίκτυο, έτσι ο κίνδυνος παραβίασης δεδομένων μειώνεται. Επιπλέον, η αποκεντρωμένη φύση του καθολικού Blockchain καθιστά δύσκολη την παραβίαση του και επίσης ο κίνδυνος ανάμειξης πληροφοριών μειώνεται σημαντικά σε σύγκριση με τα τρέχοντα συστήματα που χρησιμοποιούν οι παραδοσιακές ψηφιακές βάσεις δεδομένων. Μια κεντρική βάση δεδομένων μπορεί να αποτελέσει στόχος πολλών ειδών ηλεκτρονικής παραβίασης (hack) που μπορεί να βλάψουν σοβαρά την ακεραιότητα και την εγκυρότητα των δεδομένων. Η ασφάλεια του συστήματος εξαρτάται από το ίδιο το σύστημα βάσης δεδομένων. Κυβερνοεπιθέσεις, όπως η SQL injection, όπου οι χάκερς προσπαθούν να αποκτήσουν πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε μια βάση δεδομένων, έχουν γίνει πιο συχνές τελευταία.

Η αποκεντρωμένη φύση του Blockchain ωστόσο εγγυάται ότι εγγενή προβλήματα του συστήματος, όπως δυσλειτουργίες υλικού και λογισμικού, δεν έχουν καμία επίδραση στην ακεραιότητα των δεδομένων, καθώς τα δεδομένα έχουν πολλαπλά αντίγραφα αποθηκευμένα σε κάθε κόμβο του δικτύου. Τα δεδομένα στο Blockchain είναι αμετάβλητα συνεπώς όλες οι αλλαγές είναι ορατές σε ολόκληρο το δίκτυο. Τα δεδομένα που ενημερώνονται από έναν κόμβο επαληθεύονται από πολλούς κόμβους οπότε τα παραποιημένα δεδομένα σπάνια μπορούν να βρουν το δρόμο τους στο Blockchain.



**Πίνακας 2: Σύγκριση Blockchain – παραδοσιακής βάσης δεδομένων (Al Omar et al., 2018).**

<b>Λειτουργία</b>	<b>Blockchain</b>	<b>Παραδοσιακή βάση δεδομένων</b>
Αποθήκευση	Αποκεντρωμένη	Συγκεντρωτική
Μεταβλητότητα	Αμετάβλητα	Μεταβλητά
Πλεονασμός	Πλεονάζων	Μη πλεονάζων
Κόστος	Μειώνεται όσο αυξάνεται ο όγκος των δεδομένων	Αυξάνεται όσο αυξάνεται ο όγκος των δεδομένων
Διαφάνεια	Όλοι οι κόμβοι πιστοποιούν την εγκυρότητα των δεδομένων	Η εγκυρότητα των δεδομένων μπορεί να ελεγχθεί μόνο από τον διαχειριστή της βάσης δεδομένων
Σημείο αποτυχίας	Αποτυγχάνει μόνο αν προκύψει βλάβη σε όλους τους κόμβους παράλληλα	Μπορεί να αποτύχει από οποιαδήποτε βλάβη υλικού ή λογισμικού του διακομιστή (server)
Διαλειτουργικότητα	Καλό επίπεδο διαλειτουργικότητας	Δύσκολο να επιτευχθεί διαλειτουργικότητα

Ο Πίνακας 2 δείχνει μια συνοπτική σύγκριση χαρακτηριστικών των Blockchain και των παραδοσιακών βάσεων δεδομένων. Η αποθήκευση αναφέρεται στον τρόπο με τον οποίο αποθηκεύονται τα δεδομένα, η μεταβλητότητα είναι η δυνατότητα αλλαγής των δεδομένων, ο πλεονασμός αναφέρεται στην ευκολία ανάκτησης των δεδομένων σε περίπτωση απώλειας, το κόστος αναφέρεται στο οικονομικό κόστος υλοποίησης και συντήρησης αυτών των συστημάτων, η διαφάνεια αναφέρεται στην ορατότητα της δραστηριότητας των δεδομένων εντός του συστήματος, το σημείο αποτυχίας υποδεικνύει το πιο αδύναμο χαρακτηριστικό του συστήματος που μπορεί να οδηγήσει στην αποσταθεροποίηση ή την καταστροφή του και τέλος η διαλειτουργικότητα αφορά την επικοινωνία μεταξύ πολλαπλών παρόμοιων συστημάτων.

#### 2.4.5.2 Blockchain και τεχνολογία κατακευμημένου καθολικού

Σύμφωνα με την Franks (2020), ως κατακευμημένο καθολικό μπορεί να θεωρηθεί μια βάση δεδομένων που υπάρχει σε πολλές τοποθεσίες ή μεταξύ πολλών συμμετεχόντων. Τα κατακευμημένα καθολικά μπορούν, αλλά όχι απαραίτητα, να εξαρτώνται από την τεχνολογία Blockchain καθώς το καθολικό αποθηκεύεται σε πολλούς διακομιστές, οι οποίοι με τη σειρά τους σχηματίζουν ένα δίκτυο peer-to-peer μέσω του οποίου οι διακομιστές επικοινωνούν για να διασφαλίσουν ότι διατηρούνται τα πιο ακριβή και ενημερωμένα αρχεία των συναλλαγών. Αυτό που κάνει το Blockchain να ξεχωρίζει από την τεχνολογία κατακευμημένου καθολικού είναι η κρυπτογραφική υπογραφή και σύνδεση ομάδων εγγραφών (μπλοκ) στο καθολικό για να σχηματιστεί μια αλυσίδα. Τα κατακευμημένα καθολικά Blockchain είναι εγγραφές (σύνολα δεδομένων) που μοιράζονται σε όλους τους κόμβους (υπολογιστές) στο δίκτυο, καθιστώντας δυνατή την επαλήθευση των συνόλων δεδομένων σε κάθε κόμβο. Τα παραποιημένα σύνολα δεδομένων εξαιρούνται, επιτρέποντας στο κατακευμημένο καθολικό να παρουσιάσει μια αμετάβλητη και αξιόπιστη ενιαία πηγή. Ανάλογα με τη συγκεκριμένη εφαρμογή του Blockchain, το κοινό (χρήστες) μπορεί να έχει την ευκαιρία να παράσχει πληροφορίες σχετικά με τον τρόπο δομής και λειτουργίας του.



Σχήμα 1: Σχέση μεταξύ Blockchain και DLT (Franks, 2020).

Όπως φαίνεται και στο σχήμα 1, η τεχνολογία κατακευμημένου καθολικού μπορεί να υπάρχει χωρίς Blockchain, αλλά το Blockchain αποτελεί μια μορφή τεχνολογίας κατακευμημένου καθολικού.

#### 2.4.6 Γενιές Blockchain

Σύμφωνα με την Franks (2020), η τεχνολογία Blockchain μπορεί να θεωρηθεί ότι έχει περάσει από δύο στάδια και βρίσκεται πλέον στην τρίτη φάση ανάπτυξης. Το Blockchain 1.0 εισήγαγε οικονομικές συναλλαγές και πληρωμές μέσω κρυπτονομισμάτων, αρχικά με τη χρήση Bitcoin. Έκτοτε έχουν αναπτυχθεί πάνω από 1.600 διαφορετικά κρυπτονομίσματα. Αυτές οι χρηματοοικονομικές συναλλαγές που πραγματοποιούνται στην πρώτη φάση (και συνεχίζονται σήμερα) περιλαμβάνουν κόμβους σε ένα κατακεντρωμένο δίκτυο που μπορεί να είναι «πλήρεις κόμβοι» (αποθήκευση μιας πλήρους λίστας για κάθε μεμονωμένη συναλλαγή) ή «ελαφροί κόμβοι» (αποθήκευση μερικής λίστας). Οι κόμβοι εξόρυξης συνήθως εκτελούν πλήρεις κόμβους (διατήρηση της πλήρους λίστας), αλλά δεν είναι όλοι οι κόμβοι εξορύκτες. Οι εξορύκτες (miners) ομαδοποιούν τις συναλλαγές σε μπλοκ και τις προτείνουν στο δίκτυο για επικύρωση. Τα επικυρωμένα μπλοκ προστίθενται στην αλυσίδα και οι εξορύκτες λαμβάνουν αποζημίωση για την εργασία τους. Απαιτείται ένα πορτοφόλι για την αποθήκευση της αξίας, αλλά σε αυτήν την περίπτωση το πορτοφόλι αποθηκεύει το ιδιωτικό κλειδί για πρόσβαση στο Bitcoin (ή σε άλλους τύπους κρυπτονομισμάτων) που είναι αποθηκευμένα στο Blockchain. Ένα πορτοφόλι μπορεί να έχει τη μορφή μιας εφαρμογής, ενός ιστότοπου ή μιας συσκευής που διαχειρίζεται το ιδιωτικό κλειδί. Οι διαχειριστές αρχείων πρέπει να είναι βέβαιοι ότι ο νέος τύπος εγγραφής που δημιουργείται από τη συναλλαγή στο Blockchain (το ιδιωτικό κλειδί) αποθηκεύεται, ασφαλίζεται και διαχειρίζεται. Το Blockchain 2.0 εμφανίστηκε όταν το Ethereum παρουσίασε κατακεντρωμένες εφαρμογές και έξυπνα συμβόλαια που μπορούν να λειτουργήσουν στα πλαίσια ενός Blockchain. Το Ethereum εισήγαγε επίσης τη γλώσσα προγραμματισμού Solidity, μια γλώσσα υψηλού επιπέδου που βασίζεται σε συμβόλαια και χρησιμοποιείται για την κωδικοποίηση των έξυπνων συμβολαίων. Η εισαγωγή των έξυπνων συμβολαίων καθιστά δυνατή τη δημιουργία συμβάσεων για ψηφοφορία, crowdfunding, τυφλές δημοπρασίες, πορτοφόλια πολλαπλών υπογραφών κ.α.. Τα έξυπνα συμβόλαια εκτελούν συναλλαγές (συμφωνίες) όταν ακολουθείται ένα συγκεκριμένο σύνολο κανόνων, όπως όταν και τα δύο μέρη υπογράφουν μια συμφωνία, ή μπορούν να ενεργοποιηθούν από εξωτερικά δεδομένα, όπως η παρέλευση μιας ημερομηνίας λήξης ή η επίτευξη ενός στόχου τιμής. Εάν οι πληροφορίες που είναι απαραίτητες για την ενεργοποίηση της σύμβασης βρίσκονται εκτός του δικτύου Blockchain (δηλαδή εκτός αλυσίδας), τότε πρέπει να γίνει εύρεση και επαλήθευση των πραγματικών

περιστατικών ώστε να γίνει η τροφοδοσία των δεδομένων στο δίκτυο Blockchain. Για το άμεσο μέλλον, δεν θα βρίσκονται όλα τα δεδομένα σε ένα Blockchain. Εάν η τεχνολογία κατανεμημένου καθολικού και τα Blockchain πρόκειται να ενσωματωθούν στις λειτουργίες των περισσότερων βιομηχανιών, η επεκτασιμότητα πέρα από το Blockchain είναι απαραίτητη. Οι διαχειριστές αρχείων και οι επαγγελματίες διαχείρισης πληροφοριών είναι υπεύθυνοι για όλα τα αρχεία, τόσο εντός όσο και εκτός αλυσίδας. Όσο αναπτύσσονται νέες τεχνολογίες, οι παραδοσιακές έννοιες, όπως ο ορισμός της «διαγραφής», μπορεί να χρειαστούν βελτίωση. Η διαγραφή σε ένα περιβάλλον Blockchain μπορεί κάποια στιγμή να οδηγήσει στην καταστροφή του ιδιωτικού κλειδιού αλλά όχι των δεδομένων στο μπλοκ. Το μεταβαλλόμενο νομικό τοπίο μπορεί επίσης να επηρεάσει τέτοιες πρακτικές καθώς, για παράδειγμα, ορισμένοι στην Ευρωπαϊκή Ένωση, προτείνουν εξαίρεση από την απαίτηση «δικαιώματος διαγραφής» του γενικού κανονισμού για την προστασία δεδομένων (GDPR) ως προς τα αρχεία που είναι αποθηκευμένα σε Blockchain.

Το Blockchain 3.0 αναγνωρίζει την αναγκαιότητα διαλειτουργικότητας μεταξύ του δικτύου Blockchain και άλλων συστημάτων και υπηρεσιών. Αυτή η γενιά του Blockchain φέρνει στο προσκήνιο το λεγόμενο “Blockchain ως υπηρεσία (BaaS)”, όπου οι «προμηθευτές» αξιοποιούν τους πόρους τους για να παρέχουν υπηρεσίες στους «πελάτες». Οι πελάτες μπορούν να αξιοποιήσουν λύσεις που βασίζονται σε cloud υπηρεσίες για να δημιουργήσουν, να φιλοξενήσουν και να χρησιμοποιήσουν τις δικές τους εφαρμογές Blockchain, έξυπνες συμβάσεις και λειτουργίες στο Blockchain. Ο πάροχος υπηρεσιών που βασίζονται σε cloud διαχειρίζεται όλες τις απαραίτητες εργασίες και δραστηριότητες για να διατηρεί την υποδομή ευέλικτη και λειτουργική. Οι προμηθευτές προϊόντων που βασίζονται σε cloud έχουν επίσης αρχίσει να παρέχουν τις δικές τους λύσεις Blockchain. Οι διαχειριστές αρχείων και οι επαγγελματίες διαχείρισης πληροφοριών, έχοντας εμπειρία στην αξιολόγηση υπηρεσιών και προϊόντων τρίτων παρόχων για επιχειρήσεις και συστήματα που βασίζονται σε cloud, μπορούν να αξιοποιήσουν την τεχνογνωσία τους για να βοηθήσουν τον οργανισμό στην αξιολόγηση λύσεων Blockchain από τρίτους. Ωστόσο τα Blockchain δεν θα αντικαταστήσουν όλα τα παλαιού τύπου συστήματα οπότε οι επαγγελματίες διαχείρισης αρχείων θα είναι υπεύθυνοι για την ενσωμάτωση των αρχείων Blockchain στις υπάρχουσες πρακτικές διαχείρισης αρχείων τους. Επειδή η διατήρηση και η διάθεση αρχείων δεν συμπεριλήφθηκαν ως μέρος του αρχικού σχεδιασμού των λύσεων τεχνολογίας Blockchain, οι

επαγγελματίες διαχείρισης αρχείων έχουν την ευκαιρία και την υποχρέωση να πιέσουν για να συμπεριληφθούν αυτά τα χαρακτηριστικά στα ήδη υπάρχοντα συστήματα Blockchain.

#### 2.4.6.1 Blockchain ως υπηρεσία / Blockchain as a Service (BaaS)

Σύμφωνα με τους Bhatia et al. (2020), όπως συμβαίνει και με τις τεχνολογίες που βασίζονται σε cloud, όπως η υποδομή ως υπηρεσία ή το λογισμικό ως υπηρεσία, το Blockchain έχει πλέον εξελιχθεί σε σημείο που οι ιδιωτικές εταιρείες προσφέρουν πλέον το Blockchain ως υπηρεσία (BaaS). Αρχικά, οι πάροχοι ήταν μικρές εταιρείες που προσπαθούσαν να αξιοποιήσουν το Blockchain, τα token και τις πλατφόρμες ανοιχτού κώδικα. Με την τεχνολογία να έχει ωριμάσει, μεγάλες εταιρείες, όπως η Amazon και η Microsoft αναπτύσσουν και εμπλουτίζουν τις διαθέσιμες επιλογές. Το BaaS ελαχιστοποιεί την ανάγκη για επένδυση σε υλικό, ανάπτυξη πλατφορμών και πολύπλοκο προγραμματισμό, καθώς τέτοιοι μηχανισμοί είναι πλέον ενσωματωμένοι και οι πελάτες απλώς προσλαμβάνουν τον πάροχο υπηρεσιών της επιλογής τους για να διαμορφώσει ή να ενεργοποιήσει τις εφαρμογές που θέλουν, συμπεριλαμβανομένων των έξυπνων συμβολαίων. Οι πάροχοι υπηρεσιών παρέχουν επίσης στους οργανισμούς πρότυπα για την εφαρμογή μιας διακυβέρνησης καταμεμημένου καθολικού, η οποία διαφέρει από τα παραδοσιακά επιχειρηματικά μοντέλα καθώς οι οργανισμοί αξιοποίησαν τη δική τους εφευρετικότητα. Οι περισσότεροι πάροχοι χρησιμοποιούν πλατφόρμες ανοιχτού κώδικα και πιο ευρέως διαθέσιμες, όπως το Hyperledger και το Ethereum (π.χ. Amazon Web Services και Microsoft Azure). Οι προβληματισμοί σχετικά με τη διαχείριση αρχείων από τρίτα μέρη κατά την εφαρμογή του BaaS είναι οι ίδιες σε σύγκριση με άλλες τεχνολογίες διαχείρισης αρχείων. Πιο συγκεκριμένα, αυτό περιλαμβάνει οργανωτικά δεδομένα που είναι αποθηκευμένα σε ένα cloud που δεν ανήκει στον οργανισμό, αλλά παρόλα αυτά υπάρχει ανάγκη να διατηρηθεί η νόμιμη ιδιοκτησία ή τα δικαιώματα δεδομένων των πληροφοριών.

Κατά την υιοθέτηση τεχνολογιών Blockchain, οι οργανισμοί θα πρέπει να:

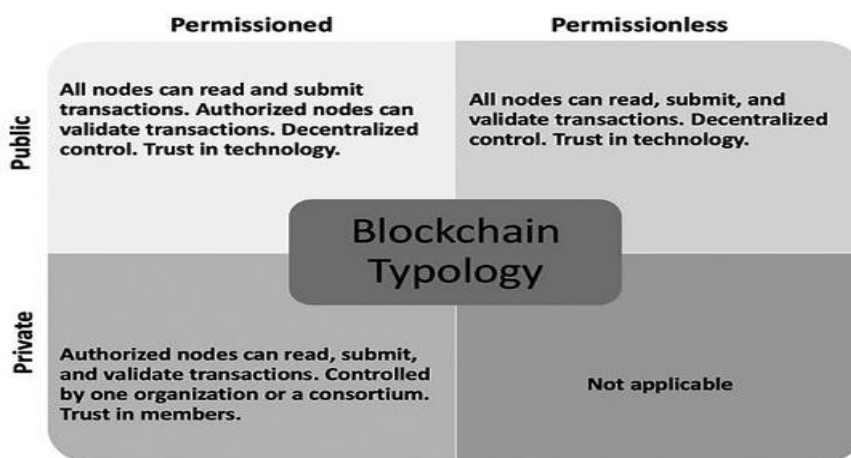
- αναπτύξουν πολιτικές για την αντιμετώπιση των επιπτώσεων της διαδικασίας διαχείρισης αρχείων στο πλαίσιο του Blockchain.
- εφαρμόσουν συστήματα που μπορούν να εκτελέσουν αρχειακές πολιτικές.

- διασφαλίσουν ότι τα αρχεία του Blockchain και τα δεδομένα των συναλλαγών είναι προσβάσιμα στην πάροδο του χρόνου.
- είναι σε θέση να απορρίψουν αρχεία Blockchain ή δεδομένα συναλλαγών.

#### **2.4.7 Τύποι Blockchain**

Σύμφωνα με τη Franks (2020), ένα Blockchain μπορεί να κατηγοριοποιηθεί ως δημόσιο ή ιδιωτικό. Το ιδιωτικό μπορεί να τμηματοποιηθεί περαιτέρω, ανάλογα με την ιδιοκτησία του (μεμονωμένος οργανισμός ή κοινοπραξία). Καθένας από αυτούς τους τύπους διαφέρει ως προς τον βαθμό κεντρικού ελέγχου που επιδεικνύεται, την άδεια που απαιτείται για τη συμμετοχή και την εμπιστοσύνη που υπάρχει στη διαδικασία. Ένα δημόσιο Blockchain συνήθως θεωρείται χωρίς άδεια και αναξιόπιστο (η εμπιστοσύνη δεν μπορεί να είναι ο καλύτερος όρος, καθώς υπάρχει εμπιστοσύνη – αλλά στο σύστημα). Οι συμμετέχοντες χρησιμοποιούν ψευδώνυμο. Είναι αποκεντρωμένο, απαιτεί 51% συμφωνία μεταξύ των συμμετεχόντων κόμβων για την επιβεβαίωση συναλλαγών και την προσθήκη μπλοκ στην αλυσίδα, είναι ανοιχτό σε όλους στο δίκτυο και παρέχει κίνητρα για εξορύκτες (υπολογιστές στο δίκτυο που προσπαθούν να επικυρώσουν νέες συναλλαγές και να τις καταγράψουν στο Blockchain λαμβάνοντας κρυπτονομίσματα ως αντάλλαγμα). Οι πιθανές εφαρμογές αφορούν συναλλαγές μεταξύ επιχειρήσεων (business-to-business/B2B) και συναλλαγές μεταξύ επιχείρησης και καταναλωτή (business-to-consumer/B2C). Τα ιδιωτικά Blockchain είναι αξιόπιστα καθώς οι συμμετέχοντες είναι γνωστοί και σε ένα βαθμό αξιόπιστοι, απαιτείται ψηφοφορία ή συναίνεση για την έγκριση συναλλαγών που θα εγγραφούν στο Blockchain και τα δικαιώματα ανάγνωσης μπορεί να είναι ελεύθερα ή περιορισμένα. Πιθανές εφαρμογές για ιδιωτικά Blockchain που ελέγχονται από έναν μόνο οργανισμό είναι εσωτερικές εφαρμογές όπως η διαχείριση βάσεων δεδομένων και ο έλεγχος. Ένα ιδιωτικό Blockchain που ελέγχεται από μια κοινοπραξία είναι επίσης εξουσιοδοτημένο και αξιόπιστο. Η διαφορά όμως είναι ότι πολλοί οργανισμοί χρησιμοποιούν το Blockchain για να επιδιώξουν συνεργατικές πρωτοβουλίες. Οι διαχειριστές αρχείων και οι επαγγελματίες της διακυβέρνησης πληροφοριών πρέπει να αντιληφθούν τους όρους και την τεχνολογία για να συμμετέχουν αξιόπιστα στις αποφάσεις για την εφαρμογή λύσεων και να αντιμετωπίζουν τους τρόπους με τους οποίους αυτές οι λύσεις επηρεάζουν τα προγράμματά τους. Στο

παρακάτω σχήμα απεικονίζεται συνοπτικά η τυπολογία ενός Blockchain και οι επιμέρους κατηγορίες που διακρίνεται.



Σχήμα 2: Τυπολογία Blockchain (Franks, 2020).

Σχετικά με τους τύπους των Blockchain έχει αναφερθεί αντίστοιχα και η National Archives and Records Administration (NARA) (2019), όπου τα κατηγοριοποιεί στα 3 παρακάτω είδη:

1. Δημόσιο: Τα ευρέως κατανεμημένα Blockchain είναι ανοιχτά σε οποιονδήποτε χρήστη ενώ παράλληλα είναι ανοιχτού κώδικα, με τον κώδικα να διατηρείται από μια ευρεία κοινότητα. Για παράδειγμα, το Bitcoin, ένα από τα πιο γνωστά δίκτυα Blockchain, είναι δημόσιο.
2. Με άδεια: Ευρέως κατανεμημένο δίκτυο Blockchain με καθιερωμένους ρόλους που μπορούν να αναλάβουν τα άτομα όταν χρησιμοποιούν το Blockchain. Για παράδειγμα, μια ομάδα τραπεζών μπορεί να μοιράζεται ευαίσθητες πληροφορίες αποθεματικών μετρητών μεταξύ τους μέσω του Blockchain.
3. Ιδιωτικό: Συχνά ένα μικρότερο Blockchain με αυστηρό έλεγχο, το οποίο δημιουργείται μεταξύ αξιόπιστων οντοτήτων που επιθυμούν να μοιραστούν ευαίσθητες πληροφορίες. Για παράδειγμα, ένας οργανισμός θα μπορούσε να χρησιμοποιήσει ένα εσωτερικό Blockchain με σκοπό την πιστοποίηση εγγράφων για δική του χρήση.

Φυσικά οι συμμετέχοντες στο δίκτυο Blockchain χρησιμοποιούν δημόσια και ιδιωτικά κλειδιά για την ψηφιακή υπογραφή και την πραγματοποίηση ασφαλών συναλλαγών εντός του συστήματος.

Υπάρχει επίσης και η προσέγγιση των Kikitamara et al. (2017), όπου αναφέρεται ότι οι τύποι Blockchain μπορούν να έχουν διπλή προσέγγιση: μια προσέγγιση πιο αφαιρετική ως προς τα τεχνολογικά χαρακτηριστικά και μια πιο επιχειρηματική προσέγγιση. Στην περίπτωση αυτή αναφέρονται τρεις γενικοί τύποι Blockchain, το ιδιωτικό Blockchain, το δημόσιο Blockchain και το Blockchain κοινοπραξίας. Στη συνέχεια οι παραπάνω τύποι ομαδοποιούνται με βάση την επιχειρηματική προοπτική για να προκύψουν δύο κατηγορίες: το ανοιχτό Blockchain για δημόσιο Blockchain και το κλειστό Blockchain για ιδιωτικό Blockchain ή Blockchain κοινοπραξίας. Το ιδιωτικό Blockchain ή το Blockchain κοινοπραξίας συνδέεται με ένα περιορισμένο περιβάλλον, (π.χ. εταιρεία, όμιλος εταιρειών ή μια συγκεκριμένη αλυσίδα αξίας), ενώ το δημόσιο Blockchain υποστηρίζει έναν τύπο Blockchain που δεν χρειάζεται άδεια.

#### 2.4.7.1 Τύποι Blockchain από τεχνολογικής άποψης

##### – Ιδιωτικό Blockchain

Όπως αναφέρεται και από τους Kikitamara et al. (2017), για ένα πλήρως ιδιωτικό Blockchain, τα δικαιώματα εγγραφής διατηρούνται κεντρικά σε έναν οργανισμό. Τα δικαιώματα ανάγνωσης μπορεί να είναι δημόσια ή περιορισμένα σε αυθαίρετο βαθμό. Πιθανές εφαρμογές περιλαμβάνουν τη διαχείριση βάσεων δεδομένων ή τον έλεγχο, εσωτερικά σε μια μεμονωμένη εταιρεία, και έτσι η δημόσια αναγνωσιμότητα μπορεί να μην είναι απαραίτητη σε πολλές περιπτώσεις, αν και σε άλλες περιπτώσεις είναι επιθυμητή η δημόσια δυνατότητα ελέγχου. Ενδεικτικά παραδείγματα αποτελούν το Hyperledger και το MultiChain.

Το Hyperledger είναι μια συλλογική προσπάθεια ανοιχτού κώδικα που δημιουργήθηκε για την προώθηση τεχνολογιών Blockchain μεταξύ διαφορετικών κλάδων. Πρόκειται για μια παγκόσμια συνεργασία, που φιλοξενείται από το Ίδρυμα Linux, συμπεριλαμβανομένων ηγετών στα χρηματοοικονομικά, την τραπεζική, το IoT, την αλυσίδα εφοδιασμού, την κατασκευή και την τεχνολογία. Ως προς το MultiChain, αυτό αποτελεί μια πλατφόρμα για τη δημιουργία και την ανάπτυξη ιδιωτικών Blockchain. Έχει τη δυνατότητα να επιλύει προβλήματα εξόρυξης, ιδιωτικότητας και διαφάνειας μέσω της ολοκληρωμένης διαχείρισης των αδειών του χρήστη. Είναι εύκολο στη ρύθμιση και μπορεί να λειτουργήσει με διαφορετικά Blockchain ταυτόχρονα. Το όφελος για τους ιδρυματικούς χρήστες είναι ότι επιτρέπει τη διαμόρφωση και την ανάπτυξη ιδιωτικών Blockchain από διαχειριστές



συστημάτων και όχι από εξειδικευμένους προγραμματιστές. Μια αναλογία είναι ο τρόπος με τον οποίο τα συστήματα διαχείρισης σχεσιακών βάσεων δεδομένων (π.χ. Oracle, SQL Server), επιτρέπουν τη δημιουργία και χρήση βάσεων δεδομένων με μερικές εντολές SQL. Ένα επιπλέον πλεονέκτημα της υποστήριξης πολλαπλών Blockchain είναι η ευκαιρία για έναν διακομιστή να δημιουργήσει συνδέσεις μεταξύ των δραστηριοτήτων σε διαφορετικές αλυσίδες. Για παράδειγμα, ένα ίδρυμα μπορεί να θέλει η άφιξη κεφαλαίων σε ένα Blockchain να ενεργοποιήσει μια αντίστοιχη μεταφορά κεφαλαίων σε κάποιο άλλο.

– Blockchain κοινοπραξίας

Σύμφωνα με τους Kikitamara et al. (2017), το Blockchain κοινοπραξίας είναι εν μέρει ιδιωτικό καθώς η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Για παράδειγμα, θα μπορούσε κανείς να φανταστεί μια κοινοπραξία 15 χρηματοπιστωτικών ιδρυμάτων, καθένα από τα οποία λειτουργεί έναν κόμβο, εκ των οποίων 10 πρέπει να υπογράψουν κάθε μπλοκ για να είναι έγκυρο το μπλοκ. Το Blockchain μπορεί να είναι δημοσίως αναγνώσιμο, ή περιορισμένο μόνο για τους συμμετέχοντες. Μια πλατφόρμα κοινοπραξίας παρέχει πολλά από τα ίδια οφέλη που σχετίζονται με το ιδιωτικό Blockchain (π.χ. αποτελεσματικότητα και απόρρητο συναλλαγών) χωρίς να εδραιώνει την ισχύ μιας μόνο εταιρείας. Οι πλατφόρμες Blockchain κοινοπραξίας έχουν πολλά κοινά πλεονεκτήματα με ένα ιδιωτικό Blockchain, αλλά λειτουργούν υπό την ηγεσία ενός ομίλου αντί μιας οντότητας. Παραδείγματα αυτού του τύπου είναι το Ethereum και το R3.

Το Ethereum είναι μια πλατφόρμα Blockchain που επιτρέπει σε οποιονδήποτε να δημιουργήσει και να χρησιμοποιήσει αποκεντρωμένες εφαρμογές που λειτουργούν με τεχνολογία Blockchain. Αυτή τη στιγμή αριθμεί περισσότερες από 86 συνεργαζόμενες εταιρείες ενώ προσπαθεί να αναπτύξει τεχνολογία η οποία μπορεί να υποστηρίξει λειτουργίες σχετικά με οικονομικές συναλλαγές κρατικών οργανισμών. Αυτό αναφέρεται στην τεχνική προοπτική του Bitcoin. Στο περιβάλλον του Ethereum, υπάρχουν αντικείμενα που ονομάζονται "λογαριασμοί", με κάθε λογαριασμό να έχει μια διεύθυνση αποτελούμενη από 20 byte και οι μεταβάσεις κατάστασης είναι άμεσες μεταφορές αξίας και πληροφοριών μεταξύ λογαριασμών που περιέχουν τα παρακάτω τέσσερα πεδία:

1. Το nonce, έναν μετρητή που χρησιμοποιείται για να διασφαλιστεί ότι κάθε συναλλαγή μπορεί να διεκπεραιωθεί μόνο μία φορά.
2. Το τρέχον υπόλοιπο σε ether.

3. Τον κωδικό σύμβασης, εάν υπάρχει.
4. Τον αποθηκευτικό χώρο (άδειος από προεπιλογή).

Το Ethereum μπορεί επίσης να θεωρηθεί ως μια διευρυμένη έκδοση του Bitcoin, καθώς χρησιμοποιεί μια παρόμοια υποκείμενη τεχνολογία Blockchain, διευρύνοντας παράλληλα το εύρος του τι μπορεί να κάνει.

Το R3 αποτελεί μια εταιρεία τεχνολογίας κατανεμημένων βάσεων δεδομένων που εδρεύει στη Νέα Υόρκη. Διατηρεί συνεργασίες με πολλά από τα μεγαλύτερα χρηματοπιστωτικά ιδρύματα του κόσμου και έχει ως αποστολή να εξερευνήσει τα οφέλη της τεχνολογίας κατανεμημένου καθολικού.

#### – Δημόσιο Blockchain

Αυτός ο τύπος Blockchain έχει σαν αρχή ότι οποιοσδήποτε στον κόσμο μπορεί να έχει πρόσβαση στα δεδομένα. Αυτό περιλαμβάνει τη διαδικασία συναίνεσης για την εγγραφή των δεδομένων στο δημόσιο Blockchain ή τον αποκλεισμό τους. Το δημόσιο Blockchain είναι ένα σύστημα ανοιχτού κώδικα, το οποίο προστατεύεται από την έννοια της κρυπτοοικονομίας, ενός συστήματος οικονομικών κινήτρων και κρυπτογραφικής επαλήθευσης που υποστηρίζεται από αλγόριθμους συναίνεσης όπως η απόδειξη εργασίας (proof-of-work / PoW) και η απόδειξη συμμετοχής (proof-of-stake / PoS). Η κρυπτοοικονομία επιτρέπει στους προγραμματιστές να δημιουργήσουν συστήματα που έχουν ορισμένες επιθυμητές ιδιότητες, όπως η διαθεσιμότητα, όπου υψηλότερες χρεώσεις οδηγούν σε ταχύτερες συναλλαγές, ή η σύγκλιση, όπου υπάρχει η δυνατότητα προσθήκης νέων μπλοκ στο Blockchain, τα οποία όμως δεν μπορούν να αντικατασταθούν ή να αφαιρεθούν. Ένα παράδειγμα δημόσιου Blockchain είναι το Bitcoin.

Το Bitcoin αποτελεί το πιο δημοφιλές παράδειγμα μιας ιδέας που συνδέεται εγγενώς με την τεχνολογία Blockchain. Το Bitcoin είναι ένα ψηφιακό νόμισμα και ένα ηλεκτρονικό σύστημα πληρωμών στο οποίο χρησιμοποιούνται τεχνικές κρυπτογράφησης για τη ρύθμιση της δημιουργίας μονάδων νομίσματος και την επαλήθευση της μεταφοράς κεφαλαίων, λειτουργώντας ανεξάρτητα από μια κεντρική τράπεζα. Η “αλυσίδα” του Bitcoin αποτελείται από πολλά διαφορετικά στοιχεία: προγραμματιστές λογισμικού, εξορύκτες, ανταλλακτήρια, υπηρεσίες επεξεργασίας εμπορών, εταιρείες ψηφιακών πορτοφολιών και χρήστες ή καταναλωτές. Από τη μεριά ενός μεμονωμένου χρήστη, σημαντικά στοιχεία στις συναλλαγές

Bitcoin αποτελούν η διεύθυνση, το ιδιωτικό κλειδί, το λογισμικό πορτοφολιού και το λογισμικό υπολογιστή για τη διαχείριση του Bitcoin. Τα πλεονεκτήματα των δημόσιων Blockchain γενικά εμπίπτουν σε δύο μεγάλες κατηγορίες:

1. Τα δημόσια Blockchain παρέχουν έναν τρόπο προστασίας των χρηστών μιας εφαρμογής από τους προγραμματιστές, αποδεικνύοντας ότι υπάρχουν ορισμένες λειτουργίες που ακόμη και οι προγραμματιστές μιας εφαρμογής δεν έχουν τη δυνατότητα να εκτελέσουν.
2. Τα δημόσια Blockchain είναι ανοιχτά και, ως εκ τούτου, είναι πιθανό να χρησιμοποιηθούν από πάρα πολλές οντότητες και να αξιοποιήσουν κάποια από τα χαρακτηριστικά του, όπως η μείωση του κόστους στους μεσάζοντες μέσω της χρήσης ενός έξυπνου συμβολαίου.

Ακόμη, υπάρχει ένας βελτιωμένος μηχανισμός για ένα δημόσιο καθολικό που αναπτύχθηκε από το IOTA1. Όσον αφορά την αναγκαιότητα της κρυπτοοικονομίας, δημιούργησαν ένα σύστημα όπου δεν υπάρχει διαχωρισμός μεταξύ του χρήστη και του εξορύκτη με σκοπό να εξαλειφθεί η ανάγκη για τους χρήστες να πληρώνουν εξορύκτες για την απόδειξη της εργασίας (PoW) αλλά να το κάνουν μόνοι τους.

**Πίνακας 3: Γενική σύγκριση δημόσιου και ιδιωτικού Blockchain (Kikitamara et al., 2017).**

Χαρακτηριστικά	Δημόσιο	Ιδιωτικό/κοινοπραξίας
Πρόσβαση	Ανοιχτή πρόσβαση στη βάση δεδομένων για ανάγνωση/εγγραφή	Χρειάζεται για ανάγνωση ή/και εγγραφή
Ταχύτητα	Αργό	Γρήγορο
Ασφάλεια	PoW/PoS	Πιστοποιημένοι συμμετέχοντες
Ταυτότητα	Ανώνυμα/με ψευδώνυμο	Επώνυμα

#### 2.4.7.2 Τύποι Blockchain από επαγγελματικής άποψης

##### – Κλειστό Blockchain

Σύμφωνα με τους Kikitamara et al. (2017), τα ιδιωτικά Blockchain ή τα Blockchain κοινοπραξιών κατηγοριοποιήθηκαν ως κλειστά Blockchain λόγω των παρόμοιων πλεονεκτημάτων που προσφέρουν και οι δύο σε μια επιχείρηση. Αυτή η επιλογή

χρησιμοποιεί Blockchain σε ένα σταθερό περιβάλλον και είναι εστιασμένη στην επιχείρηση. Χωρίς να επιτρέπονται αλλαγές στο περιβάλλον του, το μόνο ευεργετικό αποτέλεσμα του Blockchain προέρχεται από τη βελτιστοποίηση της διαδικασίας. Ο τύπος της καινοτομίας είναι σταδιακός, χρησιμοποιώντας τρέχοντα οικονομικά μοντέλα ή λύσεις από τους κυρίαρχους παίκτες της αγοράς. Συνήθως, αυτοί οι τύποι Blockchain αποτελούν πόλο έλξης για γνωστούς παίκτες του κλάδου, οι οποίοι αναδιοργανώνουν και χτίζουν ξανά την ήδη υπάρχουσα υποδομή με λίγες σημαντικές αλλαγές. Το IBM Hyperledger, για παράδειγμα, εστιάζει σε αυτόν τον τύπο. Συγκεντρώνει διαφορετικούς γνωστούς παίκτες σε μία λύση Blockchain. Αυτή η λύση δεν χρειάζεται μηχανισμό επικύρωσης (εμπιστοσύνης), όπως το PoW οπότε οι παίκτες γνωρίζονται ήδη και έτσι η εμπιστοσύνη δεν αποτελεί πρόβλημα. Η βελτιστοποίηση είναι δυνατή επειδή όλοι έχουν τα ίδια δεδομένα την ίδια στιγμή (έλλειψη σφαλμάτων ή καθυστέρησης δεδομένων ελαχιστοποιούν τις ευκαιρίες για τη μυστικοποίηση της αγοράς). Μπορούμε να δούμε τις βιομηχανίες ως ένα συνδεδεμένο σώμα. Τα αποτελέσματα της συνέργειας μεγιστοποιούνται εάν όλοι οι παίκτες στο οικοσύστημα λύσεων Blockchain συνεργαστούν για να δημιουργήσουν μια υγιή λύση και να ρυθμίσουν τον ανταγωνισμό με σταθερές και υγιείς διαδικασίες.

Οι λύσεις κλειστών Blockchain, ιδιαίτερα οι λύσεις κοινοπραξίας, συμβάλλουν στη δημιουργία διαφανών αγορών. Το όφελος για τους γνωστούς παράγοντες της αγοράς (ιδιοκτήτες της τρέχουσας υποδομής) από τη δημιουργία ενός κλειστού συστήματος Blockchain είναι ότι πρόκειται για ένα πολύ ελεγχόμενο σύστημα. Ένα φαινόμενο περιορισμού εμφανίζεται μόλις οι χρήστες είναι μέρος του κλειστού κυρίαρχου συστήματος. Οι κυρίαρχοι παίκτες μπορούν να αποφασίσουν από κοινού εάν μπορούν να εισέλθουν νέοι παράγοντες της αγοράς και εάν θα αναγκάσουν τους χρήστες να αγοράσουν πρόσθετες ενημερώσεις ή υλικό.

Μια κυρίαρχη λύση για την ταυτότητα αποτελεί το καλύτερο εμπόδιο εισόδου, γιατί κάθε συναλλαγή χρειάζεται μια ταυτότητα. Άλλες τυπικές λειτουργίες της ταυτότητας περιλαμβάνουν την ιδιοκτησία δεδομένων, στην οποία ο χρήστης ελέγχει τα δικά του δεδομένα, και η αναγνώριση ανά χαρακτηριστικό, στην οποία ο χρήστης δεν επαληθεύεται από το δικό του μοναδικό αναγνωριστικό, αλλά από ένα χαρακτηριστικό που έχει επαληθευτεί στο Blockchain.

#### – Ανοιχτό Blockchain

Ένα δημόσιο Blockchain μπορεί να επιφέρει ανατρεπτικές αλλαγές και έχει τη δυνατότητα να οδηγήσει σε μια προγραμματιζόμενη οικονομία. Σε ένα ανοιχτό Blockchain οποιοσδήποτε μπορεί να αναπτύξει λύσεις που μπορούν να χρησιμοποιηθούν από οποιονδήποτε άλλο. Αυτό μπορεί να δημιουργήσει νέα οικονομικά μοντέλα, όπως μια οικονομία μηδενικού περιθωρίου. Σε αυτό το οικονομικό μοντέλο, οι νέοι παράγοντες της αγοράς προτιμούν αυτοδιαχειριζόμενες μηχανές, ξεφεύγοντας από τα συνηθισμένα τρέχοντα μοντέλα της βιομηχανίας και της αγοράς. Επιτρέπει επίσης συναλλαγές από μηχανή σε μηχανή. Επιπλέον, οι κατανεμημένοι αυτόνομοι οργανισμοί (Distributed Autonomous Organizations / DAO) σε συνδυασμό με την τεχνητή νοημοσύνη αποτελούν ένα λογικό επόμενο βήμα στην εξέλιξη των ανοιχτών εφαρμογών Blockchain.

#### 2.4.8 Μέρη ενός Blockchain

Σύμφωνα με τη National Archives and Records Administration (NARA) (2019), τα Blockchain γενικά αποτελούνται από τρία βασικά μέρη:

- i. **Μπλοκ:** Μια λίστα καταγεγραμμένων συναλλαγών μέσα σε μια συγκεκριμένη χρονική περίοδο. Οι συναλλαγές μπορεί να αντιπροσωπεύουν οποιοδήποτε είδος δραστηριότητας, από την καταχώριση ενός τίτλου γης έως μια μεμονωμένη αγορά. Τυχόν κανόνες που σχετίζονται με το ίδιο το μπλοκ θεσπίζονται κατά την πρώτη δημιουργία του δικτύου. Για παράδειγμα, ο μέγιστος αριθμός συναλλαγών σε ένα μπλοκ ή το μέγεθος κάθε μπλοκ μπορεί να είναι περιορισμένο.
- ii. **Αλυσίδα:** Όταν το μπλοκ φτάσει στο μέγιστο μέγεθος των συναλλαγών του, συνδέεται με το προηγούμενο μπλοκ μέσω ενός hash. Η τιμή hash ενός μπλοκ εισάγεται στο επόμενο μπλοκ, δημιουργώντας μια σύνδεση μεταξύ του νέου και του προηγούμενου μπλοκ. Η επανάληψη μιας συνάρτησης hash σε ένα αμετάβλητο μπλοκ δεδομένων θα δημιουργεί πάντα την ίδια τιμή σταθερού μήκους. Εάν ένα μπλοκ δεδομένων τροποποιηθεί, το τελικό hash που θα προκύψει θα είναι διαφορετικό οπότε ο οποιοσδήποτε χρήστης θα μπορεί να δει ότι τα hash είναι διαφορετικά και θα αντιληφθεί ότι το αρχικό μπλοκ έχει τροποποιηθεί και μπορεί να μην είναι πλέον αξιόπιστο.

- iii. Δίκτυο: Το δίκτυο αποτελείται από κόμβους που ο καθένας περιέχει μια πλήρη καταγραφή όλων των συναλλαγών σε ένα Blockchain. Δεν υπάρχει επίσημο κεντρικό αντίγραφο και κανένας κόμβος δεν είναι περισσότερο "έμπιστος" από έναν άλλο. Η ακεραιότητα των δεδομένων διατηρείται από το Blockchain που αναπαράγεται σε όλους τους κόμβους.

#### 2.4.9 Βασικές αρχές της τεχνολογίας Blockchain

Σύμφωνα με τα Vermont State Archives (2019), οι βασικές αρχές της τεχνολογίας Blockchain δεν έχουν αλλάξει. Αν και κάθε υλοποίηση μπορεί να διαφέρει, μερικά βασικά στοιχεία είναι χαρακτηριστικά όλων των Blockchain:

- οι συναλλαγές γίνονται ηλεκτρονικά μεταξύ των μερών.
- τα δεδομένα σχετικά με τις συναλλαγές, συμπεριλαμβανομένης της ταυτότητας (ή της διεύθυνσης) κάθε μέρους, μιας χρονικής σφραγίδας και μιας αναφοράς σε προηγούμενο μπλοκ, κατακερματίζονται (συνοψίζονται μέσω ενός αλγορίθμου κρυπτογράφησης).
- αυτές οι συναλλαγές μεταδίδονται στη συνέχεια στο δίκτυο και μεμονωμένοι κόμβοι στο δίκτυο εκτελούν επικύρωση ή επαλήθευση αυτών των συναλλαγών.
- μόλις επιτευχθεί «συναίνεση», κάθε σύνολο συναλλαγών (μπλοκ) προστίθεται στη συνέχεια στο ηλεκτρονικό μητρώο ή καθολικό (την αλυσίδα).
- η διαδικασία επαναλαμβάνεται για κάθε επόμενη συναλλαγή, προσθέτοντας συνεχώς στην αλυσίδα.

Η τεχνολογία που έγινε γνωστή ως Blockchain, δημιουργήθηκε για να δώσει λύση σε ένα πολύ συγκεκριμένο πρόβλημα: χρειαζόταν μια μέθοδος για τις συναλλαγές μέσω Διαδικτύου για μέρη που:

- 1) δεν γνωρίζουν απαραίτητα ο ένας την ταυτότητα του άλλου.
- 2) δεν εμπιστεύονται ο ένας τον άλλον.
- 3) δεν επιθυμούν να βασίζονται σε τρίτο μέρος/μεσάζοντα.

Έτσι, το Blockchain δημιουργήθηκε με τη σύνθεση υπαρχουσών μεθόδων όπως η κρυπτογραφία δημόσιου κλειδιού και η δικτύωση peer-to-peer για να παρέχει μια λύση που θεωρητικά βασίζεται στην κρυπτογραφική απόδειξη και όχι στην εμπιστοσύνη σε

οργανισμούς ή άτομα. Η κρυπτογραφία δημόσιου κλειδιού παρέχει μια ασφαλή μέθοδο για την επίλυση της πρώτης πρόκλησης που παρουσιάστηκε παραπάνω. Κάθε χρήστης έχει δύο σκετ κλειδιών (ένα δημόσιο και ένα ιδιωτικό), τα οποία συνδέονται μαθηματικά μεταξύ τους. Το ιδιωτικό κλειδί του χρήστη χρησιμοποιείται για την υπογραφή (κρυπτογράφηση) μηνυμάτων και διατηρείται μυστικό, ενώ το δημόσιο κλειδί, το οποίο μεταδίδεται δημόσια, μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση αυτών των μηνυμάτων. Έτσι, η προέλευση ενός μηνύματος μπορεί να εξακριβωθεί, εφόσον τα μηνύματα είναι υπογεγραμμένα με το ιδιωτικό κλειδί του χρήστη.

Ένας από τους πρωταρχικούς στόχους, αν όχι ο πρωταρχικός στόχος, της τεχνολογίας Blockchain (αλλά και της πλατφόρμας του Bitcoin) είναι η άρση της ανάγκης για αυτό το αξιόπιστο τρίτο μέρος. Η απαίτηση ύπαρξης ενός διαμεσολαβητή και των υπηρεσιών του προσθέτει κόστος και χρόνο διεκπεραίωσης και εκθέτει τα μέρη στις συναλλαγές σε έναν νέο κίνδυνο: κακόβουλη ή επιθετική συμπεριφορά εκ μέρους αυτού του διαμεσολαβητή. Χρησιμοποιώντας την επαλήθευση συναλλαγών peer-to-peer, ο διαμεσολαβητής αντικαθίσταται από ένα δίκτυο όπου όσοι θέλουν να πραγματοποιήσουν συναλλαγές συμφωνούν να μοιραστούν το βάρος του να είναι εκείνοι οι ενδιαμέσοι. Δεδομένου ότι οι συναλλαγές είναι κρυπτογραφημένες, ο φυσικός ρόλος των μελών αυτού του δικτύου (γνωστοί ως κόμβοι) είναι να αποκρυπτογραφούν αυτές τις συναλλαγές επαληθεύοντάς τις (καθώς δεν θα γινόταν σωστά η αποκρυπτογράφηση σε σωστά διαμορφωμένες συναλλαγές εάν δημιουργήθηκαν εσφαλμένα). Αυτοί οι κόμβοι στο Blockchain του Bitcoin αποζημιώνονται για το έργο τους μέσω της «εξόρυξης» επιπλέον νομισμάτων. Έτσι, το δίκτυο, μέσω του πρωτοκόλλου Blockchain, αντικαθιστά τον ενδιάμεσο. Το τελευταίο κομμάτι αυτής της μεθόδου είναι το λεγόμενο «πρωτόκολλο συναίνεσης» το οποίο αναγκάζει το δίκτυο να συμφωνήσει ως προς την ορθότητα και την οργάνωση των συναλλαγών για να προχωρήσει.

Κάθε συναλλαγή αποτελείται γενικά από:

- 1) μια λίστα εισροών (αναφορές σε προηγούμενες συναλλαγές).
- 2) μια λίστα εκροών (αποτελέσματα των συναλλαγών).
- 3) Επαληθεύσεις.
- 4) χρονικές σημάνσεις.

Αυτά τα δεδομένα μαζί παρέχουν ένα συνοπτικό αρχείο συναλλαγών, ένα σύνολο εγγραφών που έχουν επαληθευτεί και έχουν επόμενες συναλλαγές, αφού μετατραπούν σε μπλοκ. Όλα τα μπλοκ μαζί αποτελούν ένα Blockchain. Αυτά τα μπλοκ αποθηκεύονται, φυλάσσονται και αναφέρονται από τους κόμβους κατά την προσθήκη νέων μπλοκ. Παράμετροι όπως το μέγεθος της συναλλαγής, ο αλγόριθμος κρυπτογράφησης, το μοντέλο συναίνεσης και η δομή των μπλοκ ποικίλλουν από Blockchain σε Blockchain. Μια αλλαγή σε ορισμένες από τις παραμέτρους αλλάζει θεμελιωδώς τη φύση του Blockchain. Λόγω της μεγάλης απόκλισης στα πιθανά μοντέλα σχεδίασης και εμπιστοσύνης των Blockchain, είναι επιτακτική ανάγκη να αξιολογηθεί η λειτουργικότητά τους σε ευρεία κλίμακα σε σχέση με τις βασικές απαιτήσεις για την τήρηση κρατικών αρχείων.

#### **2.4.10 Τεχνικά χαρακτηριστικά**

Σύμφωνα με τους Sadiku et al. (2018), η τεχνολογία Blockchain διαθέτει τα παρακάτω βασικά χαρακτηριστικά:

- Δίκτυο Peer-to-Peer (P2P): Η πρώτη απαίτηση του Blockchain είναι ένα δίκτυο, μια υποδομή που μοιράζονται πολλά μέρη και μπορεί να είναι μικρής κλίμακας (π.χ. LAN) ή μεγάλης κλίμακας (π.χ. Internet). Όλοι οι κόμβοι που συμμετέχουν σε ένα Blockchain συνδέονται σε ένα αποκεντρωμένο δίκτυο P2P. Οι συναλλαγές μεταδίδονται στο δίκτυο P2P ενώ, λόγω ορισμένων περιορισμών των δικτύων P2P, ορισμένοι προμηθευτές παρέχουν Blockchain που βασίζονται σε τεχνολογία cloud.
- Διαδοχική κρυπτογράφηση: Ένα Blockchain χρησιμοποιεί κρυπτογράφηση για την προστασία των δεδομένων που σχετίζονται με τις συναλλαγές. Τα μπλοκ κρυπτογραφούνται με διαδοχικό τρόπο, δηλαδή, το αποτέλεσμα κρυπτογράφησης του προηγούμενου μπλοκ χρησιμοποιείται για την κρυπτογράφηση του τρέχοντος μπλοκ. Το Blockchain είναι προστατευμένο με κρυπτογραφία δημόσιου κλειδιού, με κάθε peer να δημιουργεί τα δικά του ζεύγη δημόσιων/ιδιωτικών κλειδιών.
- Κατανεμημένη βάση δεδομένων: Ένα Blockchain κατανέμεται ψηφιακά σε έναν αριθμό υπολογιστών οπότε κάθε μέρος σε ένα Blockchain έχει πρόσβαση σε ολόκληρη τη βάση δεδομένων χωρίς όμως τη δυνατότητα ελέγχου των



δεδομένων ή των πληροφοριών που περιέχονται. Με δεδομένο ότι το Blockchain είναι αποκεντρωμένο, δεν υπάρχει ανάγκη για κεντρικές εξουσιοδοτήσεις (π.χ. τράπεζες).

- Διαφάνεια με ψευδωνυμία: Κάθε κόμβος ή συμμετέχων σε ένα Blockchain έχει μια μοναδική αλφαριθμητική διεύθυνση 30 και πλέον χαρακτήρων που τον προσδιορίζει. Οι χρήστες μπορούν να επιλέξουν να παραμείνουν ανώνυμοι ή να αποδείξουν την ταυτότητά τους σε άλλους.
- Μη αναστρεψιμότητα των αρχείων: Μόλις μια συναλλαγή εισαχθεί στη βάση δεδομένων και ενημερωθούν οι λογαριασμοί, τα αρχεία δεν μπορούν να τροποποιηθούν. Οι εγγραφές στη βάση δεδομένων είναι μόνιμες, με χρονολογική σειρά και διαθέσιμες σε όλους τους άλλους στο δίκτυο.

Παρόμοια εικόνα προκύπτει και από τη National Archives and Records Administration (NARA) (2019), όπου εκτός από τη λειτουργία με δίκτυα peer-to-peer, αναφέρονται ακόμη ως βασικά χαρακτηριστικά τα παρακάτω:

- αποκεντρωμένη τήρηση αρχείων των συναλλαγών
- διενέργεια συναλλαγών που βασίζονται στην εμπιστοσύνη και τη συναίνεση
- αντοχή των συστημάτων Blockchain σε παραβίαση.

Γενικά οποιαδήποτε διένεξη ή ανακρίβεια εντός του συστήματος (π.χ. για κάποια πληροφορία που αφορά μια συναλλαγή ή ακόμα και για την ίδια τη συναλλαγή) μπορεί να επιλυθεί αυτόματα με προκαθορισμένους κανόνες του καθολικού.

Παράλληλα, όπως τονίζεται και από τους Staples et al. (2017), η σωστή λειτουργία ενός συστήματος Blockchain εξαρτάται και από ορισμένα βασικά στοιχεία, συμπεριλαμβανομένων των παρακάτω:

- κατάλληλα κριτήρια ακεραιότητας που πρέπει να ελέγχονται για κάθε συναλλαγή (και μπλοκ)
- η ορθότητα του λογισμικού και των τεχνικών πρωτοκόλλων του συστήματος
- ισχυροί κρυπτογραφικοί μηχανισμοί για την αναγνώριση των 2 μερών και τον έλεγχο της εξουσίας τους ως προς την προσθήκη νέων συναλλαγών

- σειρά από μηχανισμούς κινήτρων για να παρακινήσουν τους κόμβους επεξεργασίας να συμμετέχουν στην κοινότητα και να συμπεριφέρονται με ειλικρίνεια, προς τα συμφέροντά της.

Σύμφωνα με τον Stancic (2018), στο πλαίσιο της διαχείρισης εγγράφων και αρχείων και λαμβάνοντας υπόψη όλα τα χαρακτηριστικά του Blockchain καθώς και τις ήδη υπάρχουσες τεχνολογίες και έννοιές του, θα μπορούσε να συναχθεί το συμπέρασμα ότι το Blockchain μπορεί να χρησιμοποιηθεί για:

- να επιβεβαιώσει την ακεραιότητα ενός αρχείου
- να επιβεβαιώσει την ύπαρξη ή τη δημιουργία ενός αρχείου σε μια συγκεκριμένη χρονική στιγμή (δηλαδή, όχι μετά τη χρονοσήμανση και την εγγραφή της στο Blockchain)
- να επιβεβαιώσει μια αλληλουχία αρχείων
- να υποστηρίξει/βελτιώσει την αποδοχή (ή μη απόρριψη) μιας εγγραφής και
- να βελτιώσει τις δυνατότητες επικύρωσης των ψηφιακά υπογεγραμμένων αρχείων κατά τη μακροχρόνια διατήρησή τους.

Συνοπτικά, τα συστήματα Blockchain, όπως αναφέρεται από τους Sunil Bakale & Sangamesh K (2019), διαθέτουν ορισμένα βασικά πλεονεκτήματα, τα οποία απεικονίζονται και στο σχήμα παρακάτω. Τα χαρακτηριστικά που αναφέρονται είναι τα εξής:

- Αποκεντρωμένη διαχείριση

Τα Blockchain είναι δίκτυα peer-to-peer που κάθε κόμβος εκτελείται ανεξάρτητα, ακολουθώντας παράλληλα τα πρωτόκολλα, επομένως είναι κατάλληλα για εφαρμογές όπου οι ενδιαφερόμενοι επιθυμούν να συνεργαστούν μεταξύ τους χωρίς να υπάρχει έλεγχος από έναν κεντρικό διαμεσολαβητή διαχείρισης.

- Αμετάβλητη διαδρομή ελέγχου

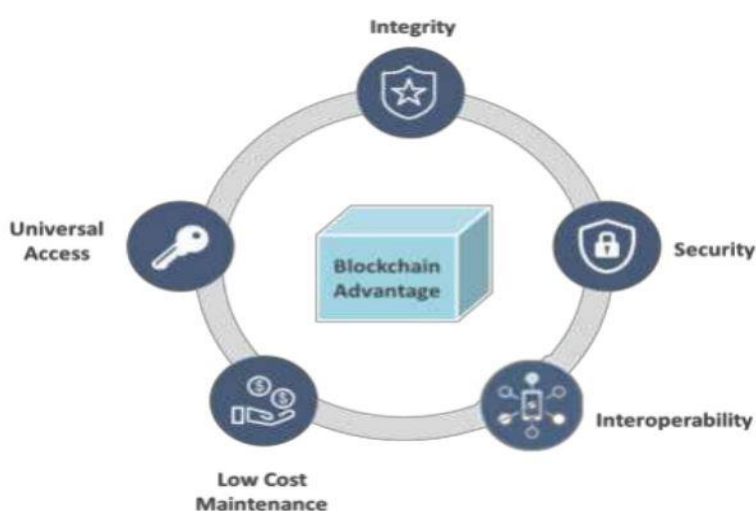
Τα Blockchain υποστηρίζουν τη δημιουργία και την ανάγνωση συναρτήσεων που είναι πολύ δύσκολο να αλλάξουν τα δεδομένα ή τα αρχεία. Έτσι, τα Blockchain είναι κατάλληλα ως μη χρεώσιμα καθολικά για την καταγραφή σημαντικών πληροφοριών (π.χ. αρχεία ασφαλιστικών απαιτήσεων).

- Προέλευση δεδομένων

Στα Blockchain, η ιδιοκτησία μπορεί να αλλάξει μόνο από τον κάτοχο, ακολουθώντας τα Κρυπτογραφικά πρωτόκολλα. Επίσης, η προέλευση των στοιχείων είναι ανιχνεύσιμη οπότε οι πηγές ή τα δεδομένα και τα αρχεία μπορούν να επιβεβαιωθούν, αυξάνοντας τη δυνατότητα επαναχρησιμοποίησης των επαληθευμένων δεδομένων (π.χ. ιατρικά αρχεία ασθενών).

- Στιβαρότητα και διαθεσιμότητα

Τα Blockchain βασίζονται σε κατακευματημένη τεχνολογία και επομένως ένα μοναδικό σημείο αποτυχίας δεν μπορεί να αποτελέσει πρόβλημα καθώς κάθε κόμβος διαθέτει αντίγραφο με το ιστορικό δεδομένων ολόκληρων εγγραφών συνεπώς ευνοείται η διατήρηση και η συνεχής διαθεσιμότητα αρχείων (π.χ. τα ηλεκτρονικά αρχεία ασθενών).



**Σχήμα 3: Πλεονεκτήματα Blockchain** (Sunil Bakale & Sangamesh K, 2019).

Σε συνέχεια των παραπάνω, αναφέρεται από τους Staples et al. (2017) ότι, όπως είναι φυσικό, τα συστήματα Blockchain μπορούν και να διαφέρουν μεταξύ τους με διάφορους τρόπους, όπως:

- Η αποδοχή κόμβων επεξεργασίας: Σε ένα δημόσιο σύστημα Blockchain, όπως το Bitcoin, οποιοσδήποτε μπορεί να γίνει κόμβος επεξεργασίας (ή εξορύκτης (miner)) ενώ σε ένα ιδιωτικό σύστημα Blockchain, η αποδοχή των κόμβων επεξεργασίας ελέγχεται από τα διοικητικά του όργανα.
- Ο μηχανισμός συναίνεσης: Τα περισσότερα δημόσια Blockchain χρησιμοποιούν το μηχανισμό Nakamoto, όπου οι κόμβοι επεξεργασίας κατά σύμβαση αντιμετωπίζουν

το μεγαλύτερο ιστορικά μπλοκ ως έγκυρο ιστορικό. Ο ρυθμός δημιουργίας των μπλοκ είναι περιορισμένος, συχνά με τη χρήση ενός μηχανισμού απόδειξης εργασίας, όπου ένας κόμβος επεξεργασίας μπορεί να προσθέσει μόνο ένα νέο μπλοκ αποδεικνύοντας ότι έχει ολοκληρωθεί μια δύσκολη εργασία. Η απόδειξη εργασίας χρησιμοποιείται ευρέως, αλλά η βοηθητική προσπάθεια που απαιτείται για την ολοκλήρωση μιας δύσκολης εργασίας μπορεί να αποδειχθεί αναποτελεσματική ως προς το οικονομικό σκέλος. Σε ένα σύστημα απόδειξης συμμετοχής (proof-of-stake/PoS), ο κόμβος επεξεργασίας που μπορεί να προσθέσει ένα νέο μπλοκ στον επόμενο γύρο καθορίζεται από το μέγεθος της συμμετοχής του στα Blockchain παγκοσμίως ή/και σε αυτόν τον γύρο. Η απόδειξη συμμετοχής μπορεί να είναι πιο αποτελεσματική, αλλά έχει αναπτυχθεί πιο πρόσφατα οπότε δεν έχει ακόμη υιοθετηθεί ευρέως. Όπως είναι φυσικό έχουν προταθεί και άλλοι μηχανισμοί συναίνεσης. Σε ιδιωτικά Blockchain, συμβατικοί αλγόριθμοι αναπαραγωγής, όπως η πρακτική ανοχής σφαλμάτων Byzantine, μπορούν να χρησιμοποιηθούν αντί της συναίνεσης Nakamoto. Αυτό ναί μεν μπορεί να παρέχει ισχυρότερες εγγυήσεις για την ολοκλήρωση των συναλλαγών και μπορεί να είναι πιο αποτελεσματικό, αλλά υποστηρίζει μικρότερο αριθμό αξιόπιστων κόμβων επεξεργασίας.

- Η αναπαράσταση συναλλαγών: Ένα κατανεμημένο καθολικό μπορεί να καταγράφει οικονομικές συναλλαγές, όπως στο Bitcoin. Ωστόσο, ένα κατανεμημένο καθολικό μπορεί να θεωρηθεί ως μια κοινόχρηστη βάση δεδομένων και μπορεί να επιτρέψει την καταγραφή οποιουδήποτε άλλου είδους δεδομένων. Πιο συγκεκριμένα, τα δεδομένα που καταγράφονται για μια συναλλαγή μπορεί να είναι το κείμενο ενός προγράμματος υπολογιστή και ο έλεγχος ακεραιότητας για αυτήν τη συναλλαγή μπορεί να περιλαμβάνει την εκτέλεση αυτού του προγράμματος, δίνοντας έτσι τη δυνατότητα στους συμμετέχοντες να δημιουργήσουν «έξυπνα συμβόλαια». Μια συναλλαγή Blockchain δεν είναι κατάλληλη για όλα τα δεδομένα καθώς αναπαράγεται παγκοσμίως, οπότε οι συναλλαγές δεν πρέπει να περιέχουν πολύ μεγάλο όγκο δεδομένων, ούτε δεδομένα απλού κειμένου καθώς αυτά πρέπει να παραμείνουν εμπιστευτικά. Έτσι, υπάρχει μια επιλογή σχετικά με το ποια δεδομένα θα πρέπει να αποθηκεύονται εντός των συναλλαγών («on chain») ή σε εξωτερικά συστήματα («off chain»). Ωστόσο, ακόμα κι αν τα στατικά δεδομένα αποθηκεύονται

εκτός αλυσίδας, το Blockchain μπορεί ακόμη να καταγράψει ένα κρυπτογραφικό hash αυτών των δεδομένων για να επιτρέψει τον έλεγχο της ακεραιότητάς τους.

#### 2.4.10.1 Hash

Σύμφωνα με τη National Archives and Records Administration (NARA) (2019), το hash είναι ένας αλγόριθμος που παίρνει μια μεταβλητή συμβολοσειρά δεδομένων και δημιουργεί μια τιμή σταθερού μήκους. Τα δεδομένα που σχετίζονται με τις συναλλαγές πρέπει να είναι μικρά έτσι ώστε η εγκυρότητα της συναλλαγής να μπορεί να υπολογιστεί γρήγορα και να διανεμηθεί σε άλλους κόμβους. Μεγάλοι όγκοι δεδομένων αποθηκεύονται συχνά «εκτός αλυσίδας» με δείκτες ή κατακερματισμούς των δεδομένων που είναι αποθηκευμένα μέσα στο Blockchain. Συνήθως τα καθολικά χρησιμοποιούνταν για την καταγραφή των συναλλαγών που αφορούσαν περιουσιακά στοιχεία ή αγαθά, όπου μόνο η συναλλαγή αποτυπωνόταν στο καθολικό ενώ η ακίνητη περιουσία διαχειριζόταν ξεχωριστά.

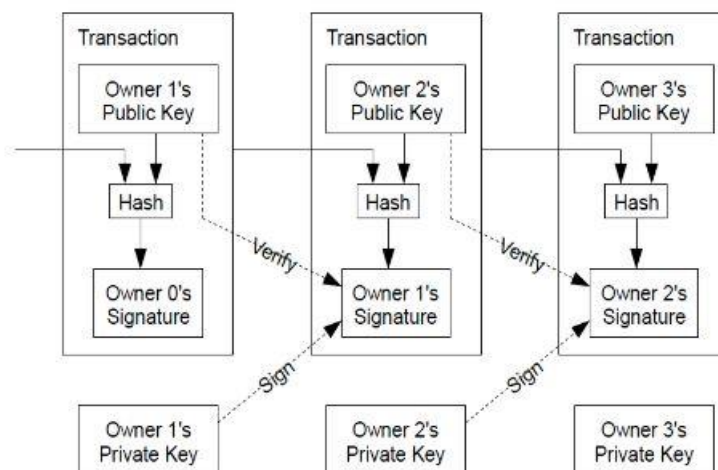
Για παράδειγμα, ένας ασφαλής αλγόριθμος κατακερματισμού που δημιουργεί μια υπογραφή 256-bit (SHA-256) παράγει διαφορετικές τιμές κατακερματισμού ακόμη και για μικρές παραλλαγές στην ορθογραφία των λέξεων "National Archives".

**Πίνακας 4: Παράδειγμα ενός Hash (National Archives and Records Administration (NARA), 2019).**

Τιμή εισαγωγής συμβολοσειράς μεταβλητού κειμένου	Τιμή Hash
National Archives	6429799b9af2d91cbf915cb0290f3a50281193a977b3457d63e454 1cc5788c5 b
National Archives (διπλό κενό ανάμεσα στις λέξεις)	d926fe7e72d09b249701dbcde2dad0ccb9b4bb653e053e461a67b bb951dcae 0b
Nati0nal Archives	5f2d570fc940d5f8de89310db43f789fdd99f51e89c021e1a50acb7a 6fe2cf83

Όπως αναφέρει και η Lemieux (2017), όταν το μπλοκ φτάσει στο μέγιστο μέγεθός του, συνδέεται με τα προηγούμενα μπλοκ. Αυτό επιτυγχάνεται κρυπτογραφικά με την προσθήκη των κατακερματισμών όλων των συναλλαγών στο νέο μπλοκ στον κατακερματισμό του

προηγούμενου μπλοκ, το οποίο με τη σειρά του παράγει ένα νέο κατακερματισμό μπλοκ. Αυτός ο κατακερματισμός προστίθεται στη συνέχεια σε όλους τους κατακερματισμούς συναλλαγών του επόμενου μπλοκ για την παραγωγή ενός άλλου νέου κατακερματισμού μπλοκ, όπως φαίνεται και στο σχήμα 4 παρακάτω. Η εγκυρότητα των εγγραφών των συναλλαγών επιτυγχάνεται μέσω του μηχανισμού συναίνεσης. Ο μηχανισμός συναίνεσης είναι ένας αλγόριθμος που έχει σχεδιαστεί για να διασφαλίζει ότι οι ενημερώσεις στο Blockchain έχουν συμφωνηθεί και κοινοποιηθεί σε ολόκληρο το δίκτυο με διαφανή τρόπο, ότι η σειρά με την οποία τα αρχεία των συναλλαγών εισήλθαν στο Blockchain είναι αδιαμφισβήτητη και ότι τυχόν αλλαγές σε αυτά που έχουν γραφτεί στο καθολικό θα είναι ανιχνεύσιμες. Μόλις εγγραφούν στο Blockchain, τα αρχεία των συναλλαγών προορίζονται να είναι αμετάβλητα.

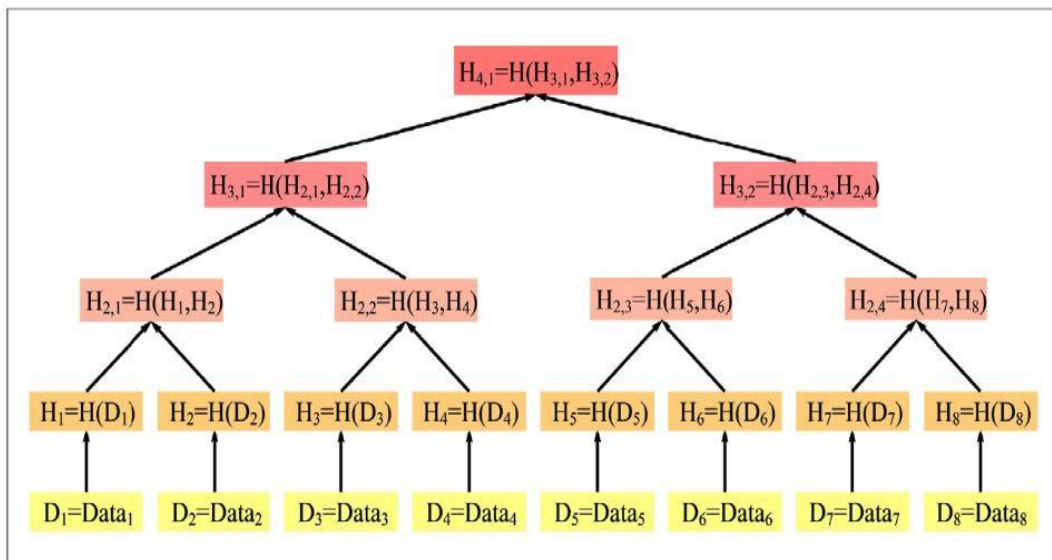


**Σχήμα 4: Ενδεικτική δομή ενός Blockchain (Lemieux, 2017).**

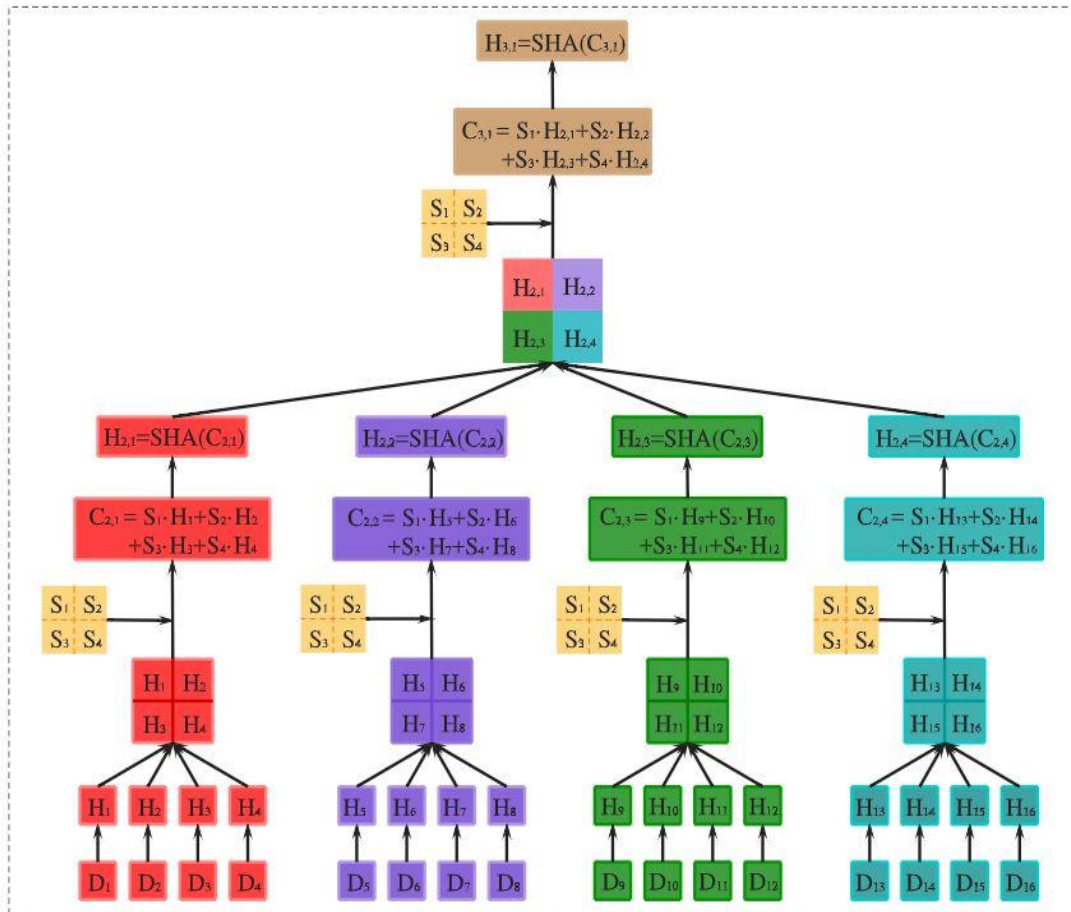
Πολλές φορές, για εξοικονόμηση χώρου, πολλές τιμές κατακερματισμού μπορούν να συγκεντρωθούν και να κατακερματιστούν ξανά, δημιουργώντας μια ενιαία τιμή κατακερματισμού ή μια ρίζα Merkle ("Merkle root") που αντιπροσωπεύει πολλούς κατακερματισμούς. Αυτή η τεχνολογία ονομάζεται δέντρο Merkle ("Merkle tree") και παρουσιάζεται παρακάτω.

### 2.4.10.2 Merkle Tree

Σύμφωνα με τη Lemieux (2017), σε ορισμένα Blockchain, όταν η αλυσίδα γίνεται αρκετά μεγάλη, συντομεύεται σε Merkle Tree, όπου η “ρίζα” (βάση) του δέντρου αποτελεί τον κατακερματισμό όλων των προηγούμενων συναλλαγών. Αυτό επιτρέπει την εξοικονόμηση χώρου αποθήκευσης χωρίς να επηρεαστεί η ακεραιότητα της αλυσίδας. Όταν η συνεχής αλυσίδα χωρίζεται στα δύο (π.χ. όταν υπάρχει μια αλλαγή στο πρωτόκολλο ή το λογισμικό του Blockchain), το Blockchain λέγεται ότι έχει διακλαδωθεί. Ο Stancic (2018) με τη σειρά του αναφέρει ότι οι τιμές κατακερματισμού μπορούν να ομαδοποιηθούν για να σχηματίσουν έναν νέο κατακερματισμό. Ας φέρουμε ως παράδειγμα μια εταιρεία, η οποία δημιουργεί έναν αριθμό εγγράφων ανά ώρα. Μια τιμή κατακερματισμού υπολογίζεται για κάθε έγγραφο. Κάθε ώρα, όλες οι τιμές κατακερματισμού από όλα τα έγγραφα ομαδοποιούνται και κατακερματίζονται μαζί για να ληφθεί μόνο ένας ωριαίος κατακερματισμός. Στο τέλος της οκτάωρης εργάσιμης ημέρας, για παράδειγμα τη Δευτέρα, και οι οκτώ «ωριαίες» τιμές κατακερματίζονται μαζί για να ληφθεί μία συνολική τιμή κατακερματισμού για τη Δευτέρα. Αυτό το hash ονομάζεται root hash ή top hash. Αυτή η προσέγγιση εισήχθη για πρώτη φορά το 1980 από τον Ralph C. Merkle και με δεδομένο ότι η δομή μοιάζει με δέντρο (ανάποδα), ονομάστηκε δέντρο Merkle (“Merkle tree”).



Σχήμα 5: Απλή μορφή ενός Merkle Tree (Zhu et al., 2021).



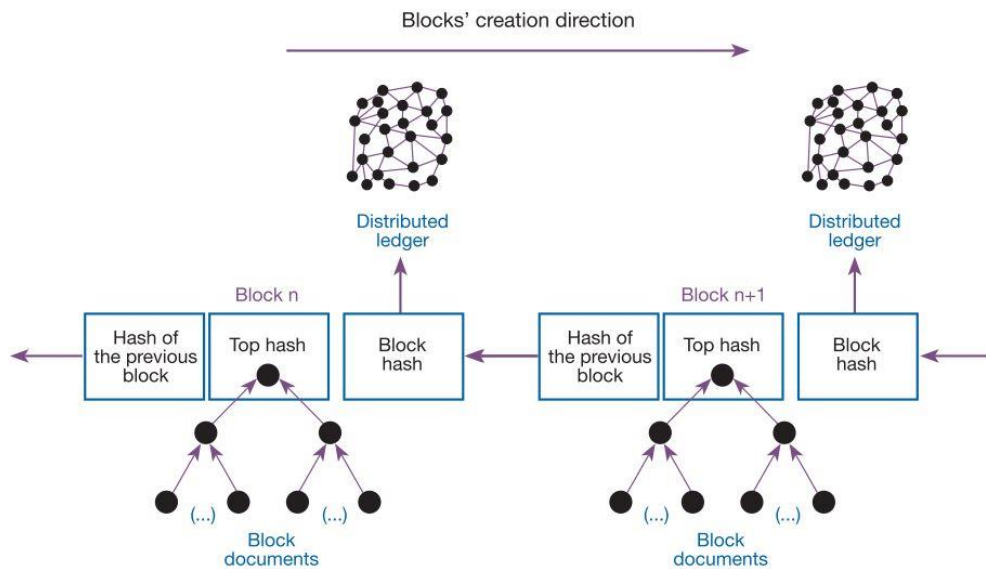
Σχήμα 6: Σύνθετη μορφή ενός Merkle Tree (Zhu et al., 2021).

#### 2.4.10.3 Πραγματοποίηση μιας συναλλαγής σε Blockchain περιβάλλον

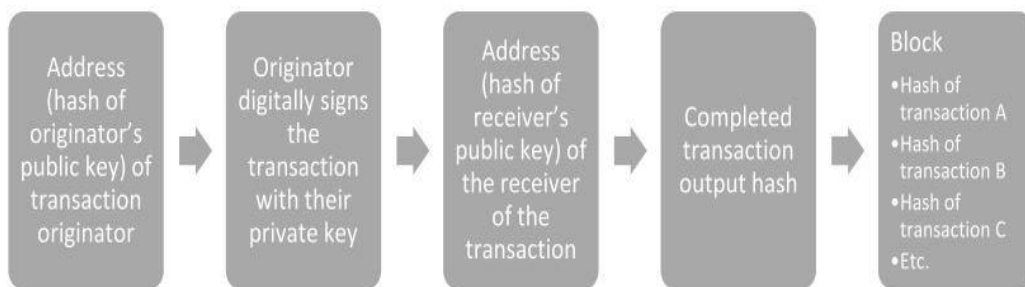
Σύμφωνα με τους Lemieux et al. (2019), όταν τα άτομα θέλουν να πραγματοποιήσουν μια συναλλαγή σε ένα δίκτυο Blockchain, όπως η μεταφορά μιας μονάδας κρυπτονομίσματος ή της ιδιοκτησίας ενός ακινήτου σε κάποιον άλλο, μεταφέρουν τον έλεγχο του περιουσιακού στοιχείου μεταφέροντας την αναπαράστασή του στο Blockchain (μερικές φορές ονομάζεται μάρκα ή token) χρησιμοποιώντας ασύμμετρη (ή PKI) κρυπτογραφία. Μια διεύθυνση υποδηλώνεται με τον κατακερματισμό ενός δημόσιου κλειδιού και ορισμένα πρόσθετα δεδομένα και λειτουργεί κάπως σαν ταχυδρομικός κώδικας που υποδεικνύει τον προορισμό μιας συγκεκριμένης μεταφοράς αξίας. Για κάθε δημόσιο κλειδί υπάρχει ένα αντίστοιχο ιδιωτικό κλειδί. Το άτομο χρησιμοποιεί το ιδιωτικό του κλειδί για να υπογράψει ψηφιακά τη συναλλαγή (βλ. Σχήμα 8) και να δώσει εξουσιοδότηση για να πραγματοποιηθεί η συναλλαγή. Η ψηφιακά υπογεγραμμένη συναλλαγή (που αποδίδεται ως κατακερματισμός εξόδου



συναλλαγής) στη συνέχεια ομαδοποιείται με άλλες ψηφιακά υπογεγραμμένες συναλλαγές και επικυρώνεται, επιβεβαιώνεται και καταχωρείται στο καθολικό, κάνοντας έτσι μια καταχώριση για να υποδείξει ότι η συναλλαγή πραγματοποιήθηκε στο αντίγραφο (replica) του καθολικού που συνήθως διατηρούν όλοι οι υπολογιστές που αποτελούν το δίκτυο Blockchain.



**Σχήμα 7: Δημιουργία ενός μπλοκ σε ένα Blockchain (Stancic, 2018).**



**Σχήμα 8: Η διαδικασία εκτέλεσης μιας συναλλαγής σε ένα Blockchain (Lemieux et al., 2019).**

#### 2.4.10.3.1 Υποδομή Δημοσίου Κλειδιού

Όπως αναφέρεται από τη National Archives and Records Administration (NARA) (2019), η Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure - PKI) συνδυάζει μαθηματικά δύο μεγάλους αριθμούς ή κλειδιά που δεν είναι πανομοιότυπα. Αυτό ονομάζεται ασύμμετρη κρυπτογραφία. Και τα δύο κλειδιά μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Ένα κλειδί μπορεί να κοινοποιηθεί δημόσια (δημόσιο κλειδί) και ένα διατηρείται ιδιωτικά (ιδιωτικό κλειδί). Για παράδειγμα, οποιοσδήποτε χρησιμοποιεί το δημόσιο κλειδί μπορεί να στείλει και να κρυπτογραφήσει ένα μήνυμα, αλλά μόνο το άτομο με το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει και να διαβάσει το μήνυμα. Στο πλαίσιο ενός Blockchain, ένας χρήστης μπορεί να υπογράψει μια συναλλαγή με το ιδιωτικό του κλειδί και οποιοσδήποτε μπορεί να επαληθεύσει τον υπογράφονα χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί.

#### 2.4.10.4 Έξυπνα συμβόλαια Blockchain

Σύμφωνα με τους Bhatia et al. (2020), ένα έξυπνο συμβόλαιο είναι ένα συμβόλαιο που έχει μεταφραστεί στη γλώσσα λογισμικού του Blockchain, είναι αποθηκευμένο στο Blockchain και μπορεί να εκτελεστεί αυτόνομα από ένα συμβάν ενεργοποίησης. Με άλλα λόγια, ένα έξυπνο συμβόλαιο είναι μια σειρά από δηλώσεις if/then που έχουν προγραμματιστεί και αποθηκευτεί στο Blockchain. Μόλις εκπληρωθούν οι απαιτήσεις του έξυπνου συμβολαίου, θα εκτελεστεί αυτόματα και η ενέργεια που προκύπτει θα αποθηκευτεί και θα κοινοποιηθεί σε ολόκληρο το Blockchain.

Κατά την ανάπτυξη πλατφορμών Blockchain, όπως αναφέρει η National Archives and Records Administration (NARA) (2019), οι προγραμματιστές συστημάτων έχουν τη δυνατότητα να προγραμματίζουν έξυπνα συμβόλαια που θα καθιστούν τα δεδομένα ή τις εγγραφές συναλλαγών κρυπτογραφικά απρόσιτα. Αυτό σημαίνει ότι οι εγγραφές δεν διαγράφονται από το Blockchain, αλλά συντάσσονται κρυπτογραφικά ώστε να μην είναι δυνατή η προβολή τους δημόσια.

Από την άποψη της διαχείρισης αρχείων, λειτουργίες όπως τα κρυπτογραφικά μη προσβάσιμα δεδομένα υποδεικνύουν ότι η διατήρηση και η διάθεση των αρχείων δεν αποτελούσαν μέρος της αρχικής πρόθεσης των προγραμματιστών Blockchain. Η χρήση αυτών των έξυπνων συμβολαίων θα μπορούσε δυνητικά να αντιμετωπίσει τις απαιτήσεις

πρόσβασης, διατήρησης, απόρριψης και επίλυσης δικαστικών διαφορών σε αρχεία, ανάλογα με τον τρόπο με τον οποίο αναπτύσσονται οι κανόνες, οι ρόλοι και οι δυνατότητες του Blockchain.

#### **2.4.11 Θεμελιώδη χαρακτηριστικά ενός συστήματος Blockchain**

##### **2.4.11.1 Αυθεντικότητα**

Σύμφωνα με τη Lemieux (2016a), για να διαπιστωθεί η αυθεντικότητα, οι αρχικά κατακερματισμένες εγγραφές πρέπει να αρχειοθετούνται χωριστά σε μορφή που να είναι αμετάβλητη και απαράβατη. Αυτό επιτρέπει την αναδιαμόρφωσή τους για μεταγενέστερη σύγκριση με τον κατακερματισμό που είναι ήδη αποθηκευμένος στο Blockchain, για σκοπούς επιβεβαίωσης της αυθεντικότητας. Εάν οι αρχικές εγγραφές δεν διατηρηθούν ακριβώς όπως δημιουργήθηκαν και κατακερματιστούν με τον ίδιο ακριβώς τρόπο, υπάρχει κίνδυνος να μην ταιριάζουν οι κατακερματισμοί και να αποτύχει ο μηχανισμός αυθεντικότητας. Αξίζει να σημειωθεί ότι η σύγκριση του κατακερματισμού των αρχικών εγγραφών συναλλαγών με τον κατακερματισμό που είναι καταχωρημένος στο Blockchain είναι μόνο η ελάχιστη απαίτηση για τον καθορισμό της αυθεντικότητας των εγγραφών. Το κατακερματισμένο περιεχόμενο δεν μπορεί επίσης να ανασυσταθεί από τον κατακερματισμό του για να μπορέσει να χρησιμεύσει ως αρχείο καθώς ο κατακερματισμός αποτελεί μια μονόδρομη συνάρτηση που δεν μπορεί να πραγματοποιηθεί αντίστροφα. Επομένως, οι ισχυρισμοί ότι ορισμένες εφαρμογές χρησιμεύουν ως μόνιμα αρχεία, σε αντίθεση με την απλή αποθήκευση κατακερματισμών περιεχομένου, μπορεί να προκαλέσει σύγχυση στους τελικούς χρήστες, οι οποίοι μπορεί να πιστεύουν ότι αγοράζουν ένα προϊόν που επιλύει προβλήματα σχετικά με την αρχειοθέτηση και όχι σχετικά με την αυθεντικότητα των αρχείων.

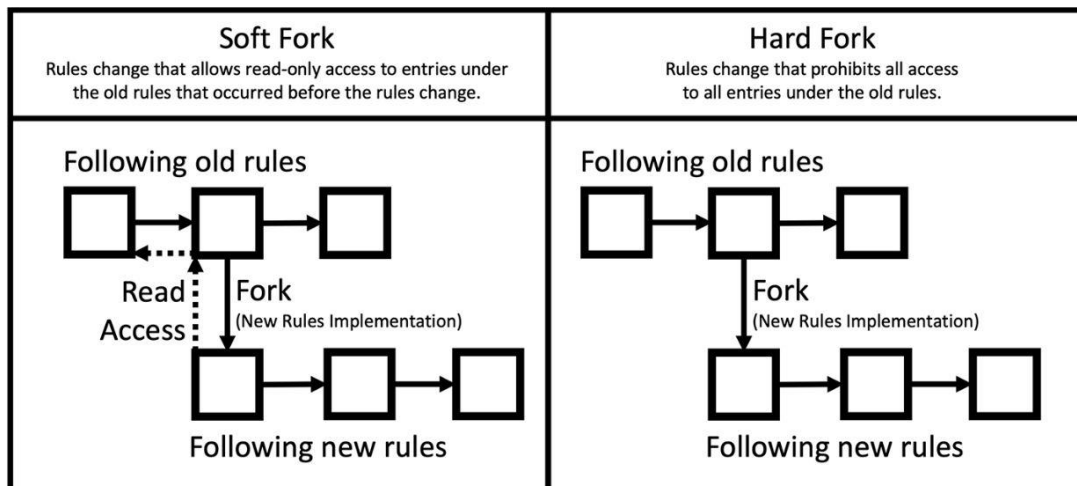
##### **2.4.11.2 Δυνατότητα ελέγχου**

Όπως αναφέρουν οι Siwan et al. (2017), μετά την ολοκλήρωση της συναλλαγής με token (μάρκα), ο πάροχος υπηρεσιών cloud δημιουργεί μια συναλλαγή απόδειξης για τον κάτοχο της εγγραφής, ο οποίος μπορεί να εντοπίσει το αρχείο καταγραφής πρόσβασης μέσω συνδεδεμένων συναλλαγών. Εξάλλου όλες οι συναλλαγές στο Blockchain περιλαμβάνουν μια χρονική σήμανση του χρήστη και μια διεύθυνση στο σύστημα οπότε υπάρχει δυνατότητα ο κάτοχος του αρχείου να λάβει ένα χρονοδιάγραμμα για έλεγχο. Επίσης, ο κάτοχος των

αρχείων μπορεί να αποκτήσει αυτά τα αρχεία καταγραφής χωρίς να χρειαστεί να επικοινωνήσει με τον πάροχο υπηρεσιών cloud.

### 2.4.11.3 Ασφάλεια και αμεταβλητότητα αρχείων

Σύμφωνα με τους Bhatia et al. (2020), πλατφόρμες ή συστήματα που υφίστανται παρείσφρηση από αναξιόπιστους κόμβους ενδέχεται να διαταράξουν την ισορροπία ή τον υπολογισμό της συναίνεσης. Αυτή η ανισορροπία μπορεί να υποβάλει το τελευταίο μπλοκ σε αναθεώρηση. Το fork είναι μια αλλαγή στο πρωτόκολλο ή τη δομή δεδομένων. Γενικά, έχει αναπτυχθεί όταν ένα καθολικό παραβιάζεται ή όταν ανακαλύπτεται ένα λάθος στην κωδικοποίηση ή ένα σφάλμα. Στο Σχήμα 9, παρουσιάζονται δύο τύποι, τα soft fork και τα hard fork. Ένα soft fork διαθέτει συμβατότητα προς τα πίσω. Ένας νέος κανόνας μπορεί να εφαρμοστεί και τα παλαιότερα μπλοκ θα παραμείνουν αμετάβλητα. Οποιαδήποτε νέα μπλοκ προστίθενται στο δίκτυο θα συμμορφώνονται με τον νέο κανόνα, αλλά εάν ένας κόμβος δεν υποστηρίζει την αλλαγή, η συναλλαγή θα εξακολουθεί να είναι έγκυρη. Σε αντίθεση με το soft fork, ένα hard fork δεν είναι συμβατό προς τα πίσω και όλοι οι κόμβοι θα πρέπει να συμμορφώνονται με τον νέο κανόνα.



Σχήμα 9: Διάγραμμα soft και hard fork (Bhatia et al., 2020).

Τα κλασικά χαρακτηριστικά ασφαλείας είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα (Staples et al., 2017).

#### 2.4.11.4 Εμπιστευτικότητα

Οι Staples et al. (2017) προσθέτουν ότι εμπιστευτικότητα σημαίνει ότι δεν πραγματοποιείται μη εξουσιοδοτημένη αποκάλυψη πληροφοριών. Αυτό είναι συνήθως πιο δύσκολο να γίνει σε συστήματα που βασίζονται σε Blockchain, επειδή από προεπιλογή οι πληροφορίες είναι ορατές για όλους στο δίκτυο. Οι πληροφορίες μπορούν να κρυπτογραφηθούν ασύμμετρα με το δημόσιο κλειδί ενός συγκεκριμένου μέρους, έτσι ώστε μόνο αυτό το μέρος να μπορεί να το αποκρυπτογραφήσει, ή συμμετρικά με ένα κοινό μυστικό κλειδί, έτσι ώστε η ομάδα των μερών με πρόσβαση στο μυστικό κλειδί να μπορεί να το αποκρυπτογραφήσει. Η τελευταία περίπτωση απαιτεί ένα ασφαλές μέσο για την ανταλλαγή του μυστικού κλειδιού εκτός αλυσίδας.

Ωστόσο, από τη στιγμή που οι πληροφορίες πρέπει να υποβληθούν σε επεξεργασία με μεθόδους έξυπνων συμβολαίων, τότε αυτές οι πληροφορίες πρέπει να αποκρυπτογραφηθούν. Αυτό συμβαίνει επειδή ο κώδικας έξυπνου συμβολαίου εκτελείται σε όλους τους κόμβους του δικτύου και επομένως οποιοσδήποτε από αυτούς πρέπει να μπορεί να επεξεργάζεται τα δεδομένα εισόδου. Αυτό απαιτείται για την επίτευξη συναίνεσης σχετικά με τα αποτελέσματα της εκτέλεσης έξυπνων συμβολαίων. Η ενσωμάτωση κλειδιών σε ένα έξυπνο συμβόλαιο θα οδηγούσε σε αποκάλυψη του κλειδιού σε όλους τους συμμετέχοντες.

#### 2.4.11.5 Ακεραιότητα

Όπως αναφέρεται από τη National Archives and Records Administration (NARA) (2019), ένα από τα θεμελιώδη ζητήματα για τη διαχείριση αρχείων είναι η διασφάλιση της αυθεντικότητας και της ακεραιότητας των αρχείων. Η τεχνολογία Blockchain παρουσιάζει στους διαχειριστές αρχείων έναν νέο τρόπο για να διασφαλίσουν ότι τα ηλεκτρονικά συστήματα προσφέρουν ακεραιότητα. Αντιπροσωπευτικό παράδειγμα αποτελούν οι ψηφιακές υπογραφές, μια κοινή μορφή δεδομένων συναλλαγών που μπορούν να αποθηκευτούν σε ένα Blockchain. Προς το παρόν, όταν υπογράφεται ψηφιακά ένα ηλεκτρονικό έγγραφο κειμένου (π.χ. PDF), η υπογραφή αποθηκεύεται στο ίδιο το έγγραφο. Οι υπογραφές πρέπει να εφαρμόζονται διαδοχικά και εάν λήξει το πιστοποιητικό, μπορεί να αμφισβητηθεί η εγκυρότητα του εγγράφου. Η αποθήκευση υπογραφών, μαζί με έναν κατακερματισμό του εγγράφου, καταργεί την απαίτηση για διαδοχική υπογραφή και

πιστοποιητικά. Αυτό θα μπορούσε να είναι ιδιαίτερα χρήσιμο για μακροπρόθεσμα αρχεία, όπως τίτλους γης και διαθήκες.

Αντίστοιχα, ένα Blockchain θα μπορούσε να χρησιμοποιηθεί για να εγγυάται την αυθεντικότητα μιας εγγραφής. Όταν ένας οργανισμός παρέχει ένα αρχείο στους χρήστες, συνήθως παρέχει πληροφορίες σχετικά με την προέλευση αλλά και πιστοποίηση ότι είναι αληθινό και ακριβές αντίγραφο. Σε κάθε περίπτωση, υπάρχει πάντα η δυνατότητα σύγκρισης με το πρωτότυπο. Εάν το πιστοποιητικό γνησιότητας διατηρείται σε ένα Blockchain, η εγγραφή μπορεί να κατακερματιστεί εκ νέου για να προσδιοριστεί εάν έχουν γίνει αλλαγές ή τροποποιήσεις. Οι φωτογραφίες μπορούν να αλλοιωθούν, να περικοπούν ή να τροποποιηθούν με άλλο τρόπο από έναν ερευνητή, γεγονός που μπορεί να αποδειχθεί συγκρίνοντας τα hash.

Αντίστοιχη εικόνα παρουσιάζεται και από τους Staples et al. (2017), όπου τονίζεται ότι η ακεραιότητα είναι η απουσία ακατάλληλων (μη έγκυρων ή μη εξουσιοδοτημένων) αλλαγών του συστήματος και αποτελεί βασικό χαρακτηριστικό για τα Blockchain. Όταν μια συναλλαγή συμπεριληφθεί σε ένα Blockchain και συμπληρώσει κάποιο χρονικό διάστημα, γίνεται μέρος του ουσιαστικά αμετάβλητου καθολικού και δεν μπορεί να τροποποιηθεί. Αυτό ισχύει εξίσου για τα έξυπνα συμβόλαια, καθώς ο κώδικας τους αναπτύσσεται σε μια συναλλαγή και επομένως υπόκειται στις ίδιες εγγυήσεις ακεραιότητας. Η τεχνολογία Blockchain αρχικά εμφανίστηκε για να υποστηρίξει ένα κρυπτονόμισμα επομένως δεν προκαλεί έκπληξη το γεγονός ότι η ακεραιότητα είναι ένα βασικό χαρακτηριστικό αξιοπιστίας. Ούτως ή άλλως η ακεραιότητα αποτελεί βασικό χαρακτηριστικό αξιοπιστίας για την εμπορική ασφάλεια των ηλεκτρονικών υπολογιστών.

Η υψηλή ακεραιότητα και η μη αποκήρυξη δεν είναι πάντα ιδανική. Για παράδειγμα, μερικές φορές τα ιστορικά δεδομένα μπορεί να χρειαστεί να διαγραφούν ή να μεταβληθούν. Εάν έχει δημιουργηθεί μια ακατάλληλη καταχώριση στο μητρώο, το δικαστήριο μπορεί να διατάξει τον γραμματέα να αλλάξει το μητρώο για να αφαιρέσει αυτήν την καταχώριση, σαν να μην είχε δημιουργηθεί ποτέ. Αυτό δεν είναι τεχνικά δυνατό σε πολλές πλατφόρμες Blockchain. Ακόμη, τα Blockchain μπορεί να “προσβληθούν” από παράνομο περιεχόμενο. Ορισμένα Blockchain έχουν προταθεί για την αντιμετώπιση αυτής της πρόκλησης, αλλά δεν υπάρχουν ακόμη ευρέως αποδεκτές και αποτελεσματικές λύσεις. Εναλλακτικά, εάν τα Blockchain αποθηκεύουν αποκλειστικά κατακερματισμούς δεδομένων που είναι αποθηκευμένα εκτός

αλυσίδας, τότε η παραδοσιακή διαχείριση δεδομένων μπορεί να αντιμετωπίσει τη διαγραφή δεδομένων με εντολή δικαστηρίου, αν απαιτείται, παρόλο που οι κατακερματισμοί ενδέχεται να μην μπορούν ποτέ να διαγραφούν.

#### 2.4.11.5.1 Θεωρία της εμπιστοσύνης / Μοντέλο εμπιστοσύνης 3 επιπέδων

Σύμφωνα με τους Lemieux et al. (2019), τα Blockchain, μέσα από έναν συνδυασμό κοινωνικού σχεδιασμού και μηχανικής, σχεδιασμού και μηχανικής τήρησης αρχείων, και τεχνικού σχεδιασμού και μηχανικής, (βλ. Σχήμα 10), λειτουργούν ως σύστημα εμπιστοσύνης. Έτσι, ο σχεδιασμός των Blockchain μπορεί να ειπωθεί ότι βασίζεται σε τρία αλληλεπιδρώντα «επίπεδα εμπιστοσύνης»:

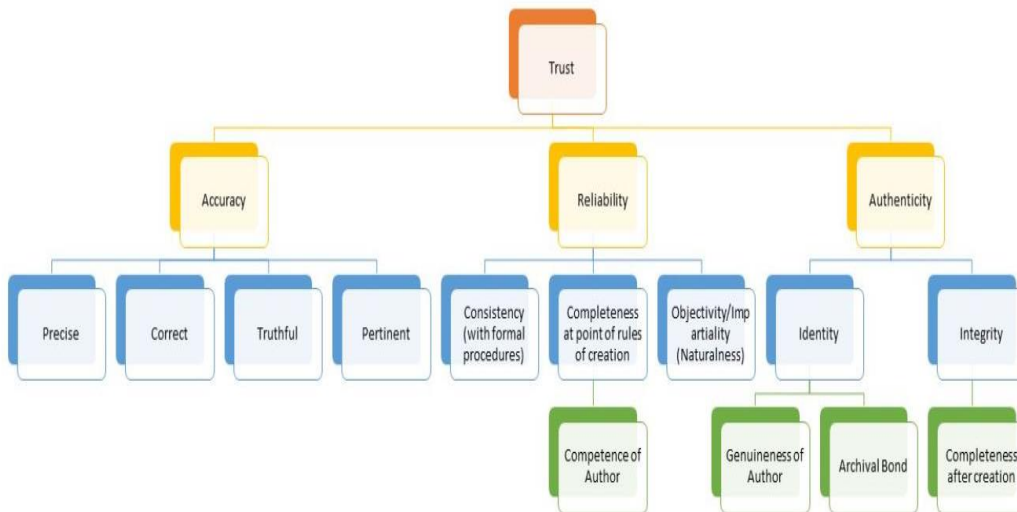
1. ένα κοινωνικό επίπεδο, όπου οι κοινωνικοί φορείς αλληλεπιδρούν μεταξύ τους και καθορίζουν πόσες πληροφορίες χρειάζονται και σε ποια μορφή προκειμένου να μπορούν να εμπιστευθούν και να δράσουν βάσει εμπιστοσύνης.
2. ένα επίπεδο αρχείων, όπου παρέχονται οι πληροφορίες που οι κοινωνικοί φορείς έχουν αποφασίσει ότι πρέπει να λάβουν από το σύστημα Blockchain για να δράσουν αποτελεσματικά
3. ένα τεχνικό επίπεδο, όπου περιλαμβάνει τα τεχνικά μέσα με τα οποία οι κοινωνικοί φορείς αλληλεπιδρούν και δημιουργούν, αποθηκεύουν και λαμβάνουν πληροφορίες σχετικά με αυτές τις αλληλεπιδράσεις ως ανθεκτική στην παραποίηση και μη απορριπτέα απόδειξη γεγονότων σχετικών με πράξεις.

Κάθε ένα από αυτά τα επίπεδα διαλειτουργεί με στόχο την επίτευξη αξιόπιστων συναλλαγών. Λόγω της ικανότητάς τους να αλλάζουν τις υπάρχουσες τεχνικές, αρχειακές και κοινωνικές σχέσεις εμπιστοσύνης, τα Blockchain έχουν τη δυνατότητα να επηρεάσουν μεγάλο αριθμό κοινωνικών, πολιτικών και οικονομικών τομέων.



**Σχήμα 10: Μοντέλο εμπιστοσύνης τριών επιπέδων της τεχνολογίας Blockchain (Lemieux et al., 2019).**

Πολλά έχουν γραφτεί ανά τους αιώνες σχετικά με τη βάση της εμπιστοσύνης στα τεκμηριωμένα στοιχεία, ιδιαίτερα από νομική και ιστορική σκοπιά. Εν προκειμένω, η μελέτη της αξιοπιστίας των αρχείων που βασίζονται σε Blockchain βασίζεται σε αρχειακή και διπλωματική θεωρία. Παράλληλα, η διπλωματική και η αρχειακή επιστήμη σχηματίζουν συμπληρωματικές προοπτικές που επιτρέπουν την κατανόηση της φύσης και της βάσης της εμπιστοσύνης στα αρχεία ως πηγές απόδειξης των γεγονότων και των πράξεων στις οποίες αναφέρονται. Γενικά, αυτή η προοπτική χαρακτηρίζεται από την απαίτηση ότι τα αρχεία διαθέτουν τρεις θεμελιώδεις ιδιότητες για να θεωρούνται αξιόπιστα: ακρίβεια, αξιοπιστία και αυθεντικότητα. Αυτά αποσυντίθενται σε διάφορα χαρακτηριστικά και απαιτήσεις όπως παρουσιάζονται παρακάτω στο σχήμα 11, την ταξινόμηση της εμπιστοσύνης.



**Σχήμα 11: Η ταξινόμηση της εμπιστοσύνης (Lemieux et al., 2019).**



#### 2.4.11.6 Διαθεσιμότητα / αξιοπιστία

Όπως αναφέρεται και από τους Staples et al. (2017), η διαθεσιμότητα αφορά την ετοιμότητα για σωστή εξυπηρέτηση ενώ η αξιοπιστία είναι η συνέχεια της σωστής εξυπηρέτησης. Ειδικότερα στο πλαίσιο λειτουργίας συστημάτων που βασίζονται σε τεχνολογία Blockchain, η διαθεσιμότητα σχετίζεται με την ικανότητα αξιοποίησης λειτουργιών του συστήματος ενώ η αξιοπιστία σχετίζεται με τη λήψη σταθερά σωστών αποτελεσμάτων από τις παραπάνω λειτουργίες.

Για τα συστήματα Blockchain, υπάρχουν περιπτώσεις στις οποίες η διάκριση μεταξύ αξιοπιστίας και διαθεσιμότητας μπορεί να είναι ασαφής, καθώς δεν υπάρχει καθολικά καθορισμένος χρόνος έως τον οποίο πρέπει να έχει ολοκληρωθεί μια συναλλαγή. Εάν ένα σύστημα Blockchain δεν συμπεριλάβει ποτέ μια συναλλαγή, αυτό θα είναι όχι μόνο αποτυχία διαθεσιμότητας αλλά και αξιοπιστίας του συστήματος Blockchain, από την οπτική γωνία μιας εφαρμογής πελάτη. Ακόμα και στην περίπτωση που μια συναλλαγή περιλαμβάνεται εξαρχής σε κάποιο μπλοκ, αυτό δεν εγγυάται ότι το μπλοκ θα αναγνωριστεί ως μέρος του Blockchain στο μέλλον.

Οι συναλλαγές που αξιοποιούν έξυπνα συμβόλαια ή επικαλούνται τις μεθόδους τους, προσθέτουν ένα επιπλέον επίπεδο πολυπλοκότητας. Αυτό συμβαίνει διότι υπόκεινται σε περισσότερες παραμέτρους που μπορεί να επηρεάσουν την επιτυχή συμπερίληψή τους αλλά και γιατί χρησιμοποιούν πιο σύνθετη λειτουργικότητα του δικτύου. Αυτό συνεπάγεται στο γεγονός ότι βασίζονται στο δίκτυο που μοιράζεται τους ίδιους αποδεκτούς κανόνες με το σύστημα, ως προς αυτή τη λειτουργικότητα.

#### 2.4.11.7 Συντηρησιμότητα

Σύμφωνα με τους Staples et al. (2017), η δυνατότητα συντήρησης αναφέρεται στην ικανότητα ενός συστήματος να υποστεί τροποποιήσεις και επισκευές. Σε συστήματα που βασίζονται σε Blockchain και χρησιμοποιούν έξυπνα συμβόλαια, αυτό είναι πιο δύσκολο να εφαρμοστεί για τα έξυπνα συμβόλαια παρά σε συνηθισμένα κατακεμημένα συστήματα. Αυτό συμβαίνει επειδή τα έξυπνα συμβόλαια περιλαμβάνουν κώδικα που ρυθμίζει τις αλληλεπιδράσεις μεταξύ αμοιβαία αναξιόπιστων μερών. Η εμπιστοσύνη προέρχεται από το γεγονός ότι ο κώδικας δεν μπορεί να αλλάξει εύκολα. Εν τέλει μπορούν να γίνουν αλλαγές σε ένα σύστημα

που βασίζεται σε Blockchain, όχι αλλάζοντας τα δεδομένα που είναι αποθηκευμένα στο Blockchain, αλλά αντ' αυτού αλλάζοντας την ερμηνεία των δεδομένων στο Blockchain.

Ένα χαρακτηριστικό πλεονέκτημα των συστημάτων που βασίζονται σε Blockchain αποτελεί το γεγονός ότι κανένα μέρος δεν διατηρεί τον έλεγχο του συστήματος. Ωστόσο, αυτό δημιουργεί προκλήσεις για τη διακυβέρνηση και τη διαχείριση της εξέλιξης συστημάτων που βασίζονται σε Blockchain. Ενδέχεται να χρειαστούν αλλαγές για τη διόρθωση ελαττωμάτων, την προσθήκη λειτουργιών ή τη μετεγκατάσταση σε νέα περιβάλλοντα πληροφορικής (IT). Ωστόσο, σε ένα σύστημα με πολλά μέρη αλλά χωρίς μεμονωμένο ιδιοκτήτη, η διαχείριση αυτών των αλλαγών μοιάζει περισσότερο με διπλωματία παρά με παραδοσιακή διαχείριση κινδύνων, με συμβατική διαχείριση τεχνικών αλλαγών ή με διαχείριση προϊόντων. Υπάρχει η δυνατότητα να βγουν συμπεράσματα από ένα λογισμικό ανοιχτού κώδικα, το οποίο αντιμετωπίζει παρόμοιες προκλήσεις ανάπτυξης. Ωστόσο, η διακυβέρνηση ενός Blockchain δεν είναι απλώς ένα πρόβλημα ανάπτυξης λογισμικού αλλά είναι και πρόβλημα ανάπτυξης και λειτουργίας. Τόσο για τα δημόσια όσο και για τα ιδιωτικά συστήματα Blockchain, τα βασικά ενδιαφερόμενα μέρη περιλαμβάνουν τους χρήστες του Blockchain, προγραμματιστές λογισμικού με ηθική ή συμβατική εξουσία στη βάση του κώδικα, εξορύκτες ή κόμβους επεξεργασίας εντός του συστήματος, και κυβερνητικές ρυθμιστικές αρχές σε σχετικούς κλάδους.

#### 2.4.11.8 Επιμέλεια & έλεγχος

Όπως αναφέρεται από τους Lemieux et al. (2019), κατά τη συζήτηση της ιδιοκτησίας μιας εγγραφής, είναι σημαντικό να αποσαφηνιστεί ο τρόπος που χρησιμοποιείται η επιμέλεια και ο έλεγχος για τη διάκριση ή τον προσδιορισμό της ιδιοκτησίας. Για αρχή παρουσιάζονται παρακάτω οι ορισμοί των όρων αυτών.

Επιμέλεια: Η επιμέλεια συνεπάγεται με τη φυσική κατοχή ενός αρχείου, ακόμη και αν ο δημόσιος φορέας (κάτοχος) δεν έχει απαραίτητα ευθύνη για τα αρχεία. Η φυσική κατοχή συνήθως περιλαμβάνει την ευθύνη για την πρόσβαση, τη διαχείριση, τη συντήρηση, τη διατήρηση, την απόρριψη και τη διασφάλιση. Όπου υπάρχουν περισσότερα από ένα αντίγραφα ενός αρχείου, μπορεί να υπάρχουν περισσότεροι από ένα άτομο/οργανισμό που έχουν την επιμέλεια του αρχείου.

Έλεγχος: Ο έλεγχος συνεπάγεται με τη δύναμη ή την εξουσία διαχείρισης ενός αρχείου καθ' όλη τη διάρκεια του κύκλου ζωής του, συμπεριλαμβανομένου του περιορισμού, της ρύθμισης και της διαχείρισης της χρήσης ή της αποκάλυψής του. Όταν οι πληροφορίες σε ένα αρχείο σχετίζονται άμεσα με περισσότερα από ένα άτομο/οργανισμό, τότε μπορεί αντίστοιχος αριθμός να έχει τον έλεγχο του αρχείου. Το άτομο/οργανισμός με το μεγαλύτερο ενδιαφέρον επεξεργάζεται το αίτημα για πληροφορίες.

Ακολουθούν ορισμένοι παράγοντες που υποδεικνύουν ότι ένας δημόσιος φορέας έχει τον έλεγχο ενός αρχείου:

- το αρχείο δημιουργήθηκε από ένα μέλος του προσωπικού, έναν αξιωματικό ή ένα μέλος του φορέα κατά την άσκηση των καθηκόντων του
- το αρχείο δημιουργήθηκε από εξωτερικό σύμβουλο του φορέα
- το αρχείο προσδιορίζεται σε μια σύμβαση ως υπό τον έλεγχο του φορέα
- το περιεχόμενο του αρχείου σχετίζεται με την εντολή και τα καθήκοντα του φορέα
- ο φορέας έχει την εξουσία να ρυθμίζει τη χρήση και την απόρριψη του αρχείου
- ο φορέας έχει βασιστεί στο αρχείο σε σημαντικό βαθμό
- το αρχείο είναι στενά ενσωματωμένο με άλλα αρχεία που κατέχει ο φορέας
- η σύμβαση επιτρέπει στο φορέα να επιθεωρήσει, να επανεξετάσει, να κατέχει ή να αντιγράψει αρχεία που παράγονται, παραλαμβάνονται ή αποκτήθηκαν από τον ανάδοχο ως αποτέλεσμα της σύμβασης.

Ουσιαστικά, οι κύριοι τρόποι για να προσδιορίσουμε τον τρόπο με τον οποίο παρουσιάζεται η ιδιοκτησία συνοψίζεται στο ότι η επιμέλεια αποτελεί τη φυσική κατοχή ενός αρχείου και ότι ο έλεγχος αποτελεί τη δύναμη ή τη νομική εξουσία για τη διαχείριση μιας εγγραφής καθ' όλη τη διάρκεια του κύκλου ζωής της. Επιμέλεια δεν σημαίνει απαραίτητα τον νόμιμο έλεγχο ή την εξουσία επί ενός αρχείου.

#### **2.4.12 Στρατηγική ανάπτυξης ενός συστήματος διαχείρισης αρχείων που βασίζεται στην τεχνολογία Blockchain**

Σύμφωνα με την Franks (2020), μεταξύ των τεσσάρων τύπων πρωτοβουλιών Blockchain που έχει εντοπίσει, ο διαχειριστής αρχείων αποτελεί έναν εξ αυτών. Οι πρωτοβουλίες διαχείρισης και διατήρησης αρχείων έχουν σχεδιαστεί για να επιτρέπουν σε έναν ή παραπάνω οργανισμούς να διασφαλίζουν ότι τα αρχεία δεν μπορούν να αλλοιωθούν και ότι μπορούν

να περάσουν από έλεγχο, κατόπιν αίτησης. Οι υπόλοιπες τρεις πρωτοβουλίες είναι ο διαταράκτης Blockchain με στόχο την επίτευξη αποκέντρωσης των επιχειρηματικών ή/και τεχνολογικών λειτουργιών, η εμπορία ψηφιακών περιουσιακών στοιχείων για τη διευκόλυνση της δημιουργίας (ή εκπροσώπησης) και ανταλλαγής νέων ψηφιακών περιουσιακών στοιχείων και το σχέδιο αποτελεσματικότητας με στόχο τη βελτίωση της αποτελεσματικότητας σε υπάρχουσες επιχειρηματικές διαδικασίες στο πλαίσιο μιας εταιρείας ή μιας βιομηχανίας. Ανεξάρτητα από την αρχική πρόθεση, καθένας από τους τέσσερις τύπους πρωτοβουλιών Blockchain χρησιμοποιεί καταναμημένα καθολικά που παρέχουν ένα αρχείο συναλλαγών που πρέπει να θεωρηθούν ως μέρος μιας στρατηγικής τεχνολογίας καταναμημένου καθολικού Blockchain. Για να αναπτυχθεί μια στρατηγική για την τεχνολογία Blockchain χρειάζεται να γίνουν αντιληπτά ποια από τα οφέλη της εφαρμογής της τεχνολογίας Blockchain αποτελούν τους βασικούς παράγοντες (π.χ. η αύξηση της αξιοπιστίας, η βελτίωση της αποτελεσματικότητας ή/και η ενίσχυση της ασφάλειας). Έτσι, απαιτούνται τα ακόλουθα βήματα:

1. Προσδιορισμός της τρέχουσας κατάστασης αποθήκευσης ψηφιακών δεδομένων/πληροφοριών:
  - εξέταση των πολιτικών και των πρακτικών του ιδρύματός/οργανισμού σχετικά με τα ψηφιακά δεδομένα, ιδίως των πολιτικών διαχείρισης αρχείων και πληροφοριών και το πρόγραμμα διατήρησης αρχείων
  - προσδιορισμός των δεδομένων/πληροφοριών που είναι κατάλληλα για αποθήκευση εντός αλλά και εκτός Blockchain
2. Έρευνα του εξωτερικού πλαισίου:
  - διερεύνηση νόμων και νομικών ζητημάτων, όπως απαιτήσεις δικαιοδοσίας, αναγνώριση έξυπνων συμβάσεων ως νομικών συμβάσεων και «δικαίωμα διαγραφής» στοιχείων της νομοθεσίας (π.χ., EU GDPR)
  - κατανόηση των κανονισμών που ενδέχεται να επηρεάσουν τον τρόπο αποθήκευσης των δεδομένων σε οποιοδήποτε τομέα
3. Κατανόηση των κριτηρίων που πρέπει να πληροί ο προγραμματιστής/πάροχος Blockchain:
  - επιλογή μιας δημόσιας ή ιδιωτικής λύσης Blockchain με άδεια ή χωρίς άδεια

- ανάπτυξη μιας στρατηγικής για τη συλλογή/μετακίνηση εγγραφών που έχουν καταγραφεί σε ένα Blockchain, εάν το Blockchain δεν είναι βιώσιμο (π.χ. εγκατάλειψη προμηθευτή, αποχώρηση της πλειοψηφίας των κόμβων από το δίκτυο)
4. Προσδιορισμός του αντίκτυπου στα ήδη υπάρχοντα συστήματα των επιχειρήσεων/οργανισμών:
- Μπορεί το Blockchain να ενσωματωθεί με τα υπάρχοντα συστήματα;
  - Είναι εφικτή μια σπονδυλωτή προσέγγιση για την εφαρμογή της τεχνολογίας Blockchain;

Οι λύσεις Blockchain είναι επιχειρηματικές αποφάσεις. Μόλις ληφθεί μια απόφαση, ο διαχειριστής αρχείων και ο επαγγελματίας διαχείρισης πληροφοριών πρέπει να διασφαλίσουν ότι τα αρχεία που δημιουργούνται από συναλλαγές σε ένα Blockchain ή αποθηκεύονται/καταχωρούνται στο Blockchain μπορούν να είναι αξιόπιστα.

#### **2.4.13 Blockchain & Record Management**

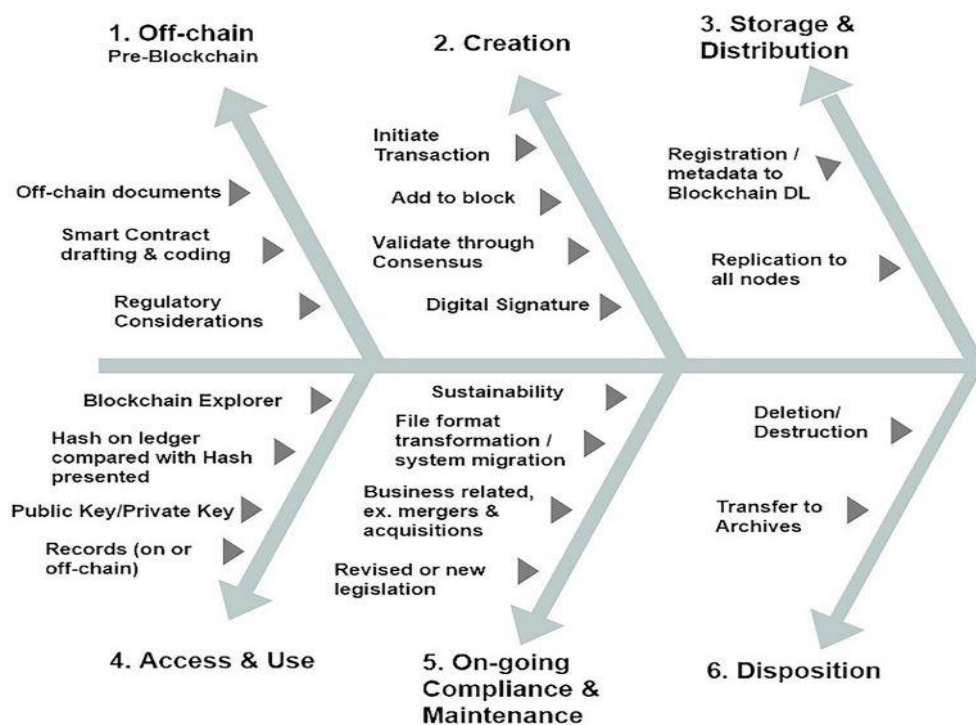
Όπως αναφέρεται από την Franks (2020), ο γενικός στόχος της διαχείρισης αρχείων Blockchain είναι να διασφαλίσει ότι η λύση κατανεμημένης τεχνολογίας Blockchain που εφαρμόζεται ανταποκρίνεται στις ανάγκες του οργανισμού, συμπεριλαμβανομένης της νομικής συμμόρφωσης, του απορρήτου και της εμπιστευτικότητας, της ακεραιότητας, και του ελέγχου των δεδομένων, των πολιτικών πρόσβασης και της διακυβέρνησης πληροφοριών.

Η τρέχουσα κατάσταση που παρουσιάζεται από τις εγγραφές τεχνολογίας κατανεμημένου καθολικού Blockchain, είτε είναι αποθηκευμένες ή εγγεγραμμένες σε Blockchain (η τήρηση αρχείων αποτελεί πρωταρχικό σκοπό) είτε δημιουργούνται μέσω συναλλαγών που πραγματοποιούνται σε Blockchain (η τήρηση αρχείων αποτελεί δευτερεύων σκοπό).

Για τη διαχείριση των αρχείων Blockchain διαχρονικά, οι δραστηριότητες που σχετίζονται με αρχεία (π.χ. δημιουργία, διάδοση) θα πρέπει να προσδιορίζονται σε έξι διαφορετικά στάδια. Αυτά τα στάδια και ορισμένες από τις δραστηριότητες που λαμβάνουν χώρα σε καθένα, όπως φαίνεται και στο Σχήμα 12, είναι τα εξής:

1. εκτός αλυσίδας: δραστηριότητες που πραγματοποιήθηκαν πριν από την έναρξη συναλλαγών στο Blockchain.

2. δημιουργία: δραστηριότητες που εμπλέκονται από την έναρξη της συναλλαγής έως την επικύρωση και την επαλήθευση.
3. αποθήκευση και διανομή: δραστηριότητες που σχετίζονται με τη διανομή των μπλοκ, συμπεριλαμβανομένων των μεταδεδομένων, στο κατακευματισμένο δίκτυο.
4. πρόσβαση και χρήση: δραστηριότητες που σχετίζονται με τη χρήση μιας διεπαφής για την προβολή συναλλαγών που έχουν καταγραφεί στο Blockchain.
5. συμμόρφωση και συντήρηση: δραστηριότητες που σχετίζονται με τη διασφάλιση της βιωσιμότητας και της συμμόρφωσης με την πάροδο του χρόνου
6. απόρριψη (συμπεριλαμβανομένης της μεταφοράς σε αρχείο): δραστηριότητες που πραγματοποιούνται για να διασφαλιστεί ότι τα αρχεία ή οι καταγεγραμμένες συναλλαγές απορρίπτονται ή μεταφέρονται σε μόνιμο αποθετήριο.



Σχήμα 12: 6 στάδια διαχείρισης αρχείων σε ένα Blockchain (Franks, 2020).

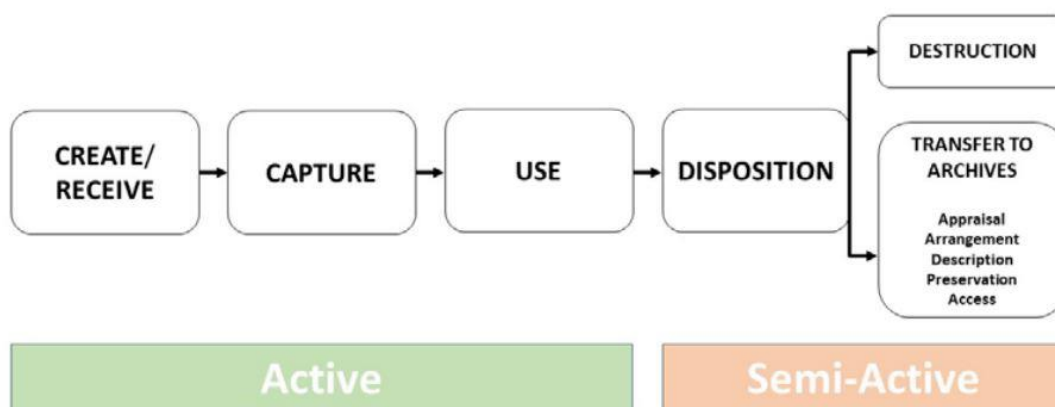
#### 2.4.13.1 Ο κύκλος ζωής μέσα σε ένα Blockchain

Σύμφωνα με τους Lemieux et al. (2019), ο όρος κύκλος ζωής χρησιμοποιείται για να περιγράψει τα στάδια της ύπαρξης ενός αρχείου από τη δημιουργία ή τη διανομή, τη χρήση και συντήρηση και τέλος την απόρριψη. Το παρακάτω μοντέλο (βλ. σχήμα 13) φέρει την ιδέα μιας γραμμικής διαδικασίας με καθορισμένη περίοδο και οριστικό τέλος που μπορεί να είναι καταστροφή ή μεταφορά σε αρχεία. Στην προσέγγιση του κύκλου ζωής, η δημιουργία των αρχείων δεν θεωρείται αρμοδιότητα του αρχειονόμου, αλλά είναι αποκλειστικά ευθύνη του δημιουργού των αρχείων. Το μοντέλο ορίζει ένα πλαίσιο στο οποίο οι εγγραφές έχουν διακριτές φάσεις ύπαρξης και οι ενέργειες που απαιτούνται από τον τηρητή αρχείων εξαρτώνται από τη φάση του κύκλου ζωής στην οποία βρίσκονται τα αρχεία.

Η προσέγγιση του κύκλου ζωής κάνει επίσης μια σαφή διάκριση μεταξύ των πρωταρχικών και δευτερευουσών αξιών που θεωρητικά διαθέτουν οι εγγραφές. Πρωταρχική αξία είναι η άμεση αξία που έχουν τα αρχεία για τον φορέα δημιουργίας σε σχέση με τις ανάγκες του, και ειδικότερα, η νομική, διοικητική και οικονομική συνάφεια. Η δευτερεύουσα αξία αποτελείται από πολιτιστικές και ιστορικές αξίες που μπορεί να έχουν τα αρχεία εκτός από την αρχική πρόθεση του δημιουργού. Είναι η αξία μιας εγγραφής ως αποδεικτικό στοιχείο και πληροφορία για άλλους χρήστες εκτός του δημιουργού και ενσωματώνεται σε όλα εκείνα τα αρχεία που περιλαμβάνουν τα αρχεία ως ιδρύματα μνήμης.

Με βάση τις ανάγκες των δημιουργών των αρχείων, η πρωταρχική αξία των αρχείων είναι παρούσα στο τρέχον στάδιο του κύκλου ζωής, ο οποίος χωρίζεται σε δύο φάσεις, την ενεργή και την ημιενεργή, βασισμένη σε μεγάλο βαθμό στην ανάγκη των δημιουργών να αναφέρονται στο αρχείο στο πλαίσιο της αρχικής επιχειρηματικής δραστηριότητας, στη συχνότητα ανάκτησης του αρχείου καθώς και στην ανάγκη των δημιουργών των αρχείων να διατηρούν το αρχείο για άλλους λόγους (π.χ. ως αποδεικτικά στοιχεία κάποιας ενέργειας). Η μετάβαση των αρχείων από την ενεργή στην ημιενεργή φάση αντιπροσωπεύεται συνήθως από τη μεταφορά τους από τον αποθηκευτικό χώρο στο γραφείο στην αποθήκευσή τους σε ένα κέντρο αρχείων που μπορεί να είναι στην ίδια ή σε άλλη τοποθεσία/εγκατάσταση. Το κέντρο αρχείων είναι ένας χώρος που δημιουργείται για τη μείωση του κόστους αποθήκευσης μεγάλων όγκων φυσικών αρχείων (π.χ. χάρτινων) που δεν αναφέρονται πλέον συχνά, αλλά που πρέπει να διατηρούνται για λόγους ελέγχου, νομικούς, ρυθμιστικούς, επιχειρηματικούς ή άλλους σκοπούς.

Αφού τα αρχεία μεταφερθούν σε ένα αρχειακό αποθετήριο, τότε υπόκεινται σε μια άλλη γραμμική ακολουθία διαδικασιών που ξεκινούν με την αξιολόγηση, που θεωρείται ευθύνη του αρχειονόμου, την επιλογή και την απόκτηση του περιεχομένου των αρχείων. Οι ακόλουθες διαδικασίες είναι η διευθέτηση, η περιγραφή και η φυσική διατήρηση, ακολουθούμενες από την παροχή πρόσβασης σε χρήστες των αρχείων (π.χ. ερευνητές).



Σχήμα 13: Μοντέλο κύκλου ζωής (Lemieux et al., 2019).

#### 2.4.13.2 Απόρριψη των αρχείων

Όπως αναφέρεται από τους Bhatia et al. (2020), Κατά την ανάπτυξη πλατφορμών Blockchain, οι προγραμματιστές συστημάτων έχουν τη δυνατότητα να αναπτύξουν έξυπνα συμβόλαια που θα καθιστούν τα δεδομένα συναλλαγών ή τις εγγραφές κρυπτογραφικά απρόσιτα (μη προσβάσιμα). Αυτό σημαίνει ότι οι εγγραφές δεν διαγράφονται από το Blockchain, αλλά αποκρύπτονται κρυπτογραφικά από τη γενική εικόνα. Δεν είναι ακόμη σαφές εάν τα κρυπτογραφικά μη προσβάσιμα δεδομένα σημαίνει ότι θα είναι μόνιμα απρόσιτα και επομένως θα μπορούσαν να θεωρηθούν ότι αφαιρέθηκαν ή απορρίφθηκαν.

Από την άποψη της διαχείρισης αρχείων, τα χαρακτηριστικά που καθιστούν τα δεδομένα κρυπτογραφικά απρόσιτα υποδεικνύουν ότι η διατήρηση και η απόρριψη των αρχείων δεν συμπεριλήφθηκαν ως μέρος της αρχικής πρόθεσης των προγραμματιστών του Blockchain. Η χρήση αυτών των έξυπνων συμβολαίων θα μπορούσε δυνητικά να αντιμετωπίσει τις απαιτήσεις πρόσβασης, διατήρησης, απόρριψης, ταξινόμησης και αποχαρακτηρισμού ασφαλείας και τυχόν δικαστικών/νομικών υποθέσεων, ανάλογα με τον τρόπο με τον οποίο αναπτύσσονται οι κανόνες, οι ρόλοι και τα χαρακτηριστικά του Blockchain.



### 2.4.13.3 Blockchain for Recordkeeping

Σύμφωνα με τα Vermont State Archives (2019), το Bitcoin αλλά και τα Blockchain γενικά, σχεδιάστηκαν ως συστήματα καταγραφής. Έχοντας κατά νου ότι υπάρχει μεγάλη ποικιλία σε προτεινόμενες λύσεις Blockchain, στο σημείο αυτό θα γίνει αναφορά σε ευρέως καθορισμένες κατηγορίες τεχνολογιών Blockchain. Επιπλέον, πρόκειται για έναν αμέτρητο αριθμό τεχνολογικών προϊόντων ή προτεινόμενων λύσεων που χαρακτηρίζουν τα Blockchain ως ένα μέρος των τεχνολογικών τους παροχών, σε συνδυασμό με παραδοσιακές πλατφόρμες διαχείρισης εγγράφων, βάσεις δεδομένων ή άλλο λογισμικό/υλικό. Θα ήταν αδύνατο να αξιολογηθούν ουσιαστικά όλοι οι πιθανοί τρόποι με τους οποίους τα Blockchain θα μπορούσαν να χρησιμοποιηθούν από κυβερνητικούς φορείς για σκοπούς τήρησης αρχείων. Αντίθετα, τα θεμελιώδη θα αξιολογηθούν με βάση την αξία τους σύμφωνα με τις νομικές απαιτήσεις και τις βέλτιστες πρακτικές του εκάστοτε κλάδου. Οι υλοποιήσεις Blockchain, όσον αφορά την τήρηση αρχείων, εμπίπτουν γενικά σε μία από τις τρεις κατηγορίες:

1. καταχώρηση των ίδιων των αρχείων σε Blockchain
2. καταχώρηση των αναγνωριστικών των αρχείων σε Blockchain
3. καταχώρηση «stand-ins» ή «tokens» σε Blockchain

Η διαφορά μεταξύ αυτών των τριών μεθόδων είναι το περιεχόμενο των δεδομένων εντός της συναλλαγής Blockchain καθώς τα Blockchain αποτελούν εργαλεία για τη μετάδοση, την αποκρυπτογράφηση και την καταγραφή των συναλλαγών οπότε μεμονωμένες υλοποιήσεις ορίζουν ρητά τη μορφή και το περιεχόμενο αυτών των συναλλαγών.

Η πρώτη κατηγορία είναι η πιο απλή, αλλά και η πιο αβέβαιη. Τις περισσότερες φορές αναφέρονται ως «έξυπνα συμβόλαια», όπως έχει αναφερθεί και παραπάνω αυτές οι εγγραφές είναι αυτοεκτελούμενος κώδικας που περιέχεται σε ένα Blockchain και ενεργοποιείται όταν πληρούνται ορισμένα κριτήρια ενώ τα αρχεία αυτών των συναλλαγών αποθηκεύονται επίσης στο Blockchain. Έτσι, σε αυτήν την περίπτωση ουσιαστικά οι ίδιες οι συναλλαγές και οι παράμετροι αυτών των συναλλαγών περιλαμβάνονται συνολικά στο Blockchain.

Η δεύτερη κατηγορία χρησιμοποιεί το Blockchain για μια αμετάβλητη καταχώρηση ενός ψηφιακού «δακτυλικού αποτυπώματος» (αναγνωριστικού) ενός αρχείου που διατηρείται εκτός της αλυσίδας σε άλλο σύστημα τήρησης αρχείων. Ο κρυπτογραφικός κατακερματισμός

των ηλεκτρονικών εγγραφών παρέχει έναν αξιόπιστο τρόπο παρακολούθησης της ακεραιότητας μιας εγγραφής. Όταν ένα ψηφιακό αρχείο κατακερματίζεται, η ακολουθία των bit του εκτελείται μέσω ενός μαθηματικού αλγόριθμου που παράγει ένα μοναδικό κατακερματισμό 256-bit (ή και άλλου μεγέθους). Είναι μαθηματικά απίθανο οποιαδήποτε άλλη ακολουθία bit να παράγει αυτόν τον κατακερματισμό ενώ ακόμη και η αλλαγή οποιουδήποτε μεμονωμένου bit στην αρχική εγγραφή θα προκαλούσε αλλαγή του κατακερματισμού. Σε αυτήν την περίπτωση, αυτοί οι κατακερματισμοί θα αποθηκευτούν στη συνέχεια στο Blockchain.

Αυτή η μέθοδος βασίζεται από κατασκευής και σχεδιασμό σε μεγάλο βαθμό σε άλλα συστήματα τήρησης αρχείων. Τα Blockchain εγγενώς δεν έχουν σχεδιαστεί για να έχουν τεράστια μεγέθη καθώς στην περίπτωση αυτή, λόγω του περιεχομένου τους, θα χρειαζόνταν πάρα πολύ μεγάλη υπολογιστική ισχύ για να γίνει το σύστημα πρακτικό. Παράλληλα απαιτείται ένας ισχυρός τρόπος που θα εξασφαλίζει για τη διατήρηση της προέλευσης και της συμφραζόμενης σύνδεσης μεταξύ του αντικειμένου και του «δακτυλικού του αποτυπώματος». Γενικά, ο διαχωρισμός των αρχείων από το πλαίσιο τους έρχεται σε αντίθεση με τις παραδοσιακές αρχειακές πρακτικές για καλό, καθώς η απώλεια του πλαισίου συνεπάγεται με απώλεια πληροφοριών, και τα Blockchain δεν έρχονται χωρίς εγγυήσεις.

Η τρίτη μέθοδος περιλαμβάνει τη δημιουργία αντικειμένων στο Blockchain, τα οποία είναι τα ίδια συναλλασσόμενα. Αυτό μπορεί να είναι γνωστό ως η προσέγγιση "token". Αυτές οι «μάρκες» συνδέονται με συγκεκριμένα αντικείμενα και τους τίτλους αυτών των αντικειμένων εκτός του Blockchain. Οι συναλλαγές στην αλυσίδα συνεπάγονται τη μεταφορά αυτών των μαρκών, και μαζί με αυτές, το ενδιαφέρον για οτιδήποτε αντιπροσωπεύουν.

Ανεξάρτητα από τα μεμονωμένα μοντέλα, οι παράμετροι για τον τρόπο με τον οποίο τα δίκτυα Blockchain αποσυνθέτουν τα μπλοκ, το ποσοστό των κόμβων που απαιτούνται για τη «συναίνεση», το μέγεθος των μπλοκ, τα μεταδεδομένα των μπλοκ, τον αλγόριθμο κρυπτογράφησης και άλλες λειτουργίες θα έχουν μεγάλη διακύμανση, ανάλογα με την εκάστοτε λύση Blockchain. Έτσι, η μέτρηση της αποτελεσματικότητας των Blockchain σε σχέση με την αυθεντικότητα, την ακεραιότητα, την αξιοπιστία και τη χρηστικότητα των εγγραφών θα παρέχει την πιο ξεκάθαρη αντίληψη.

Τα Blockchain είναι, από μόνα τους, αντίθετα με το θεμελιώδες μοντέλο της δημόσιας τήρησης αρχείων γενικά. Εάν η κυβέρνηση είναι τελικά υπόλογη στους πολίτες, μπορεί να

φαίνεται φυσικό ότι η καταγραφή δεδομένων σε προσβάσιμα από το κοινό Blockchain θα ήταν ένα όφελος. Ωστόσο, υπάρχει σημαντική διαφορά μεταξύ ενός μοντέλου φύλαξης που περιλαμβάνει διανεμημένα δεδομένα σε πολλά άτομα και της κρατικής επιμέλειας. Τα δίκτυα Blockchain δεν είναι υπόλογα σε κανέναν. Οι εταιρείες που παρέχουν λύσεις Blockchain ή τεχνολογίες που ενσωματώνουν Blockchain είναι υπόλογες ίσως στους μετόχους τους. Ακόμη και σήμερα, οι κυβερνήσεις σε όλο τον κόσμο εξετάζουν τον τρόπο με τον οποίο θα παρέχουν επίβλεψη και έλεγχο για τα Blockchain. Ακόμα κι αν τα Blockchain ήταν εντελώς αψευγάδιαστα, οι χρήστες τους πρέπει να βασίζονται στο δίκτυο, στο πρωτόκολλο, ή και στα δύο, ενώ είναι αμφίβολο εάν αυτές οι οντότητες μπορούν να είναι αξιόπιστες. Η αντικατάσταση της κυβέρνησης με ιδιώτες προμηθευτές ή απρόσωπα δίκτυα είναι καθαρή απώλεια για τη διαφάνεια, την ανάληψη ευθυνών και την εμπιστοσύνη.

#### 2.4.13.4 Αποθήκευση εγγραφών σε ένα Blockchain

Όπως αναφέρεται από τους Lemieux et al. (2019), τα συστήματα Blockchain αποτελούνται από μια πολύπλοκη «τεχνολογία stack» που συνδυάζει έναν αριθμό αλληλεπιδρώντων στοιχείων Blockchain και non-Blockchain. Δεδομένης της πολύπλοκης κατανεμημένης και αποκεντρωμένης αρχιτεκτονικής των συστημάτων Blockchain, οι εγγραφές μπορούν να διασκορπιστούν σε ένα ευρύ φάσμα συστημάτων και στοιχείων υποδομής. Παραδείγματα όπου μπορούν να αποθηκευτούν οι εγγραφές και σχόλια σχετικά με τα πλεονεκτήματα και τα μειονεκτήματά τους, παρουσιάζονται παρακάτω:

- Inter Planetary File System (IPFS): Το IPFS είναι μια τεχνολογία κατανεμημένου συστήματος αρχείων που βασίζεται σε κατανεμημένους πίνακες κατακερματισμού και το πρωτόκολλο BitTorrent. Αυτό αποτελεί ένα πρωτόκολλο peer-to-peer στο οποίο οι ομότιμοι συντονίζονται για τη διανομή των ζητούμενων αρχείων, όπως γίνεται συντονισμένα η διανομή των αιτούμενων αρχείων, όπως συντονίζονται οι κόμβοι Bitcoin για την καταγραφή συναλλαγών σε ένα κατανεμημένο καθολικό. Αυτό μπορεί να επιτευχθεί ανεξάρτητα από την τοποθεσία τους, έχοντας παράλληλα τη δυνατότητα να συνδυάζουν συστήματα αρχείων σε διαφορετικές συσκευές σε μία, χρησιμοποιώντας τη διεύθυνση περιεχομένου. Μεταξύ των πλεονεκτημάτων του είναι ότι κάθε κόμβος Blockchain αποθηκεύει μόνο εκείνα τα αρχεία που χρειάζεται, καθώς και τυχόν μεταδεδομένα σχετικά με τη θέση των αρχείων σε άλλες συσκευές.

Μεταξύ των μειονεκτημάτων του IPFS είναι ότι μετά τον διαμοιρασμό του αρχείου στο BitTorrent, η αποθήκευση δεδομένων από άλλες συσκευές δεν είναι εγγυημένη καθώς για να εγγυηθεί την παροχή ενός αρχείου σε άλλους ο αρχικός διαμοιραστής πρέπει να παραμείνει ενεργός και συνδεδεμένος. Τα αρχεία είναι επίσης στατικά (αμετάβλητα) ενώ η διαγραφή ενός αρχείου δεν υποστηρίζεται.

- Κατανεμημένες βάσεις δεδομένων: Σε βάσεις δεδομένων τέτοιου τύπου, όπως η MongoDB, η Cassandra ή η REthinkDB, ο πελάτης λειτουργεί με ένα από τα αντίγραφα και τα δεδομένα συγχρονίζονται αυτόματα με άλλους κόμβους. Υπάρχουν πολλά πλεονεκτήματα σε αυτούς τους τύπους βάσεων δεδομένων, συμπεριλαμβανομένου του ότι είναι γρήγορες, επεκτάσιμες και ανθεκτικές στη μη προσβασιμότητα μεμονωμένων αντιγράφων. Μεταξύ των μειονεκτημάτων, ωστόσο, είναι ότι είναι αδύνατο να δημιουργηθεί μια πλήρως κατανεμημένη βάση δεδομένων που να διασφαλίζει τη συνέπεια, τη διαθεσιμότητα και την ανοχή διαιρέσεων. Έτσι, αυτός ο τύπος βάσης δεδομένων μπορεί να φαίνεται ιδανικός για χρήση σε Blockchain. Ωστόσο, αν κάποιος σε ένα καλά εδραιωμένο σύμπλεγμα βάσεων δεδομένων τέτοιου τύπου προσθέσει ένα κακόβουλο αντίγραφο, το οποίο με τη σειρά του ενημερώσει τα άλλα αντίγραφα του συμπλέγματος ότι όλα τα δεδομένα πρέπει να διαγραφούν τότε όλα τα άλλα αντίγραφα διαγράφουν υπάκουα όλα τα δεδομένα και η βάση δεδομένων θα καταστραφεί ολοσχερώς. Συνεπώς, μια τέτοια συντονισμένη ενέργεια αντιγράφων είναι δυνατή τώρα μόνο σε ένα αξιόπιστο περιβάλλον. Εάν λοιπόν ένα αντίγραφο που λειτουργεί με κακόβουλο τρόπο τοποθετηθεί σε ένα σύμπλεγμα, μπορεί να προκαλέσει την καταστροφή όλων των δεδομένων του συμπλέγματος. Η χρήση ενός μηχανισμού συναίνεσης (π.χ. Practical Byzantine Fault Tolerance) που χρησιμοποιείται σε ορισμένα ιδιωτικά Blockchain, μεταξύ των κόμβων βοηθά στην προστασία έναντι του παραπάνω κινδύνου.
- BigChain DB ή IPDB (Inter Planetary Data Base): είναι μια συγκεκριμένη λύση με πολύ υψηλή ταχύτητα συναλλαγής σύμφωνα με τους δημιουργούς της (1.000.000/δευτερόλεπτο), καθώς και μεγάλη χωρητικότητα αποθήκευσης (λόγω κατανεμημένης αποθήκευσης με μερική αναπαραγωγή). Το BigChain DB λαμβάνει αυτά τα πλεονεκτήματα μέσω μιας απλοποιημένης συναίνεσης κατά τη δημιουργία μπλοκ και με την αποθήκευση όλων των μπλοκ και των συναλλαγών σε μια ήδη

υπάρχουσα εφαρμογή βάσης δεδομένων noSQL (π.χ. RethinkDB ή MongoDB). Ωστόσο, δεδομένου ότι κάθε κόμβος μπορεί να έχει πλήρη δικαιώματα εγγραφής στον κοινό χώρο αποθήκευσης δεδομένων, αυτό σημαίνει ότι το σύστημα BigChain DB δεν είναι ανεκτικό σε σφάλματα (όπως το Byzantine που αναφέρθηκε παραπάνω στην περίπτωση των κατανεμημένων βάσεων δεδομένων).

- Αποθήκευση στο σύννεφο («Cloud»): Το Cloud περιλαμβάνει ένα ευρύ φάσμα υποδομών και υπηρεσιών που διανέμονται σε ένα δίκτυο (συνήθως στο διαδίκτυο), είναι επεκτάσιμες, κατά παραγγελία, και έχουν σχεδιαστεί για να υποστηρίζουν τη διαχείριση μεγάλου όγκου ψηφιακών υλικών. Το κύριο πλεονέκτημα της αποθήκευσης σε cloud είναι ότι πλέον αποτελεί μια ώριμη τεχνολογία, οι κίνδυνοι της οποίας είναι γενικά αντιληπτοί. Το κύριο μειονέκτημα του είναι ότι συγκεντρώνει την αποθήκευση δεδομένων, γεγονός που εξαλείφει πολλά από τα πλεονεκτήματα της χρήσης της τεχνολογίας Blockchain εξαρχής. Ο Πίνακας 5 παρέχει ένα πλαίσιο για την κατανόηση των διαφορετικών τύπων εγγραφών που μπορούν να δημιουργηθούν και να αποθηκευτούν σε λύσεις Blockchain.

**Πίνακας 5: Είδη, παραδείγματα και τοποθεσία εγγραφών σε ένα σύστημα Blockchain (Lemieux et al., 2019).**

	<b>Υποστηρικτικά έγγραφα</b>	<b>Αρχεία συναλλαγών</b>	<b>Αρχεία καθολικού</b>
<i>Περιγραφή</i>	Πληροφορίες που παρέχουν υποστηρικτικές ή συμπληρωματικές πληροφορίες σχετικά με την εκτέλεση μιας συναλλαγής και που διατηρούν έναν αρχειακό δεσμό με το αρχείο της συναλλαγής.	Αναπαραστάσεις συναλλαγών με τη μορφή αρχείων, τα οποία αποτελούν «πληροφορία που έχει δημιουργηθεί, ληφθεί και διατηρηθεί ως αποδεικτικά και ως περιουσιακά στοιχεία από έναν οργανισμό ή άτομο, για την επιδίωξη νομικών υποχρεώσεων ή τη συναλλαγή επιχειρήσεων».	Hash που έχουν καταγραφεί και αποθηκευθεί σε ένα Blockchain, τα οποία μπορεί να αντιπροσωπεύουν και να αποτελούν αποδεικτικά εκτελεσμένων συναλλαγών, ύπαρξης ενός περιουσιακού στοιχείου ή μιας απαίτησης. Αυτά περιλαμβάνουν τις εγγραφές σε ένα κατανεμημένο καθολικό.

<i>Παράδειγμα</i>	Φωτογραφίες ενός ακινήτου προς πώληση.	Πωλητήριο συμβόλαιο που χρησιμοποιήθηκε για τη μεταβίβαση της ιδιοκτησίας ενός ακινήτου.	Το hash μιας συναλλαγής σε ένα Blockchain που αντιπροσωπεύει ένα ολοκληρωμένο/εκτελεσμένο πωλητήριο συμβόλαιο μεταβίβασης ακινήτου από τον πωλητή στον αγοραστή.
<i>Τοποθεσία</i>	Μπορεί να είναι αποθηκευμένα στη βάση δεδομένων ενός οργανισμού, σε cloud περιβάλλον ή σε μια κατανεμημένη αποθήκη δεδομένων (π.χ. IPFS).	Μπορεί να είναι αποθηκευμένα σε ένα Blockchain ως ένα έξυπνο συμβόλαιο, ένα έγγραφο ή ένα σύνδεσμο hash προς ένα έγγραφο ενσωματωμένο σε ένα αρχείο συναλλαγής καθολικού ως απλό ή κρυπτογραφημένο κείμενο, ή εκτός αλυσίδας με έναν παρόμοιο τρόπο με τα υποστηρικτικά έγγραφα.	Σε ένα Blockchain ή σε ένα κατανεμημένο καθολικό,

#### **2.4.14 Σχεδιασμός και διασφάλιση ενός συστήματος Blockchain**

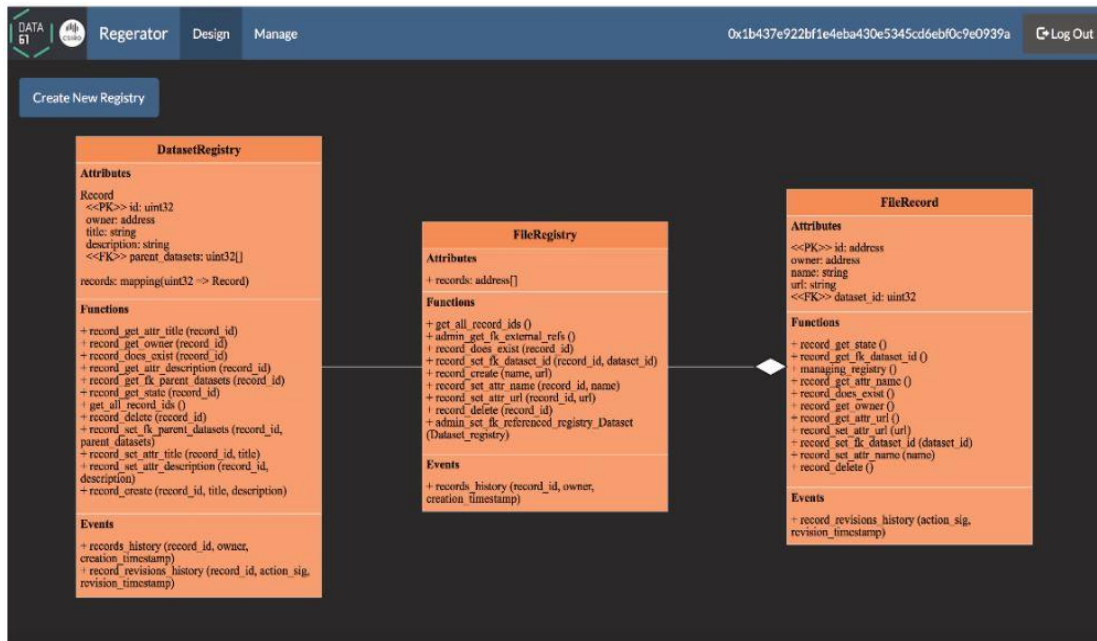
##### **2.4.14.1 Σχεδιασμός**

Σύμφωνα με τους Staples et al. (2017), ο σχεδιασμός ενός λογισμικού αποτελεί μια δημιουργική διαδικασία που προτείνει και αξιολογεί λύσεις σε πολύπλοκα προβλήματα με πολλούς αντικρουόμενους περιορισμούς. Ο τελικός σχεδιασμός ενός συστήματος λογισμικού είναι αποτέλεσμα πολλών σχεδιαστικών επιλογών σχετικά με την επιλογή, τη διαμόρφωση και την ενσωμάτωση των στοιχείων λογισμικού, υλικού και επικοινωνιών. Για συστήματα που βασίζονται σε Blockchain, οι επιλογές σχεδιασμού περιλαμβάνουν τη χρήση ενός Blockchain αντί μιας παραδοσιακής βάσης δεδομένων ή τη χρήση ενός ιδιωτικού Blockchain αντί ενός δημόσιου Blockchain. Συχνά σε ένα μοναδικό σύστημα που βασίζεται σε

Blockchain, ορισμένα δεδομένα μπορεί να αποθηκευτούν σε ένα Blockchain ενώ άλλα μέρη των δεδομένων αποθηκεύονται και κοινοποιούνται με τη χρήση συμβατικών υπολογιστικών συστημάτων, και αυτό αποτελεί άλλη μια επιλογή σχεδιασμού. Κατά τη χρήση ενός Blockchain, υπάρχουν πιο λεπτομερείς σχεδιαστικές επιλογές σχετικά με τον τύπο του Blockchain, το πρωτόκολλο συναίνεσης, το μέγεθος του μπλοκ και τη συχνότητα του μπλοκ. Όπως με κάθε σύστημα λογισμικού, υπάρχουν αντισταθμίσεις μεταξύ των NFP (Non Functional Properties / μη λειτουργικές ιδιότητες) στο σχεδιασμό συστημάτων που βασίζονται σε Blockchain. Οι αποφάσεις σχεδιασμού που βελτιώνουν την απόδοση ενός NFP για ένα σύστημα ενδέχεται να βλάψουν την απόδοση άλλων NFP. Μερικά απλά παραδείγματα αυτού περιλαμβάνουν:

- η κρυπτογράφηση δεδομένων πριν από την αποθήκευσή τους σε Blockchain μπορεί να αυξήσει την εμπιστευτικότητα, αλλά θα μειώσει την απόδοση και μπορεί να βλάψει τη διαφάνεια ή τη δυνατότητα ανεξάρτητου ελέγχου.
- η αποθήκευση μόνο ενός κατακερματισμού δεδομένων στην εντός του Blockchain και η διατήρηση των περιεχομένου εκτός του Blockchain θα βελτιώσει την εμπιστευτικότητα και μπορεί να βελτιώσει την απόδοση, αλλά εν μέρει υπονομεύει το χαρακτηριστικό πλεονέκτημα των Blockchain: την παροχή κατανεμημένης εμπιστοσύνης. Αυτό μπορεί να δημιουργήσει ένα μόνο σημείο αποτυχίας, μειώνοντας τη διαθεσιμότητα και την αξιοπιστία του συστήματος.
- η χρήση ενός ιδιωτικού Blockchain αντί για ένα δημόσιο Blockchain μπορεί να επιτρέψει μεγαλύτερο έλεγχο ως προς την αποδοχή επεξεργαζόμενων κόμβων και συναλλαγών στο σύστημα, αλλά θα δημιουργήσει και εμπόδια στην είσοδο και τη συμμετοχή οπότε θα μειώσει εν μέρει μερικά από τα οφέλη από της χρήσης ενός Blockchain.
- για Blockchain που χρησιμοποιούν μηχανισμό συναίνεσης Nakamoto (π.χ. Bitcoin ή Ethereum), η αναμονή για μεγάλο αριθμό μπλοκ επιβεβαίωσης μπορεί να αυξήσει την εμπιστοσύνη στην ακεραιότητα και την ανθεκτικότητα των συναλλαγών, αλλά θα προκαλέσει αδράνεια και ως εκ τούτου μπορεί να επηρεάσει τη διαθεσιμότητα της υπηρεσίας.

Η αρχιτεκτονική λογισμικού συχνά υποστηρίζεται από τη χρήση μοντέλων, τα οποία επικοινωνούν σχεδιαστικές αποφάσεις σε άλλους μηχανικούς λογισμικού, και τα οποία μπορούν να χρησιμοποιηθούν για την υποστήριξη ορισμένων ειδών ποσοτικής αξιολόγησης των NFP, χρησιμοποιώντας προσομοιώσεις ή αναλυτικές προσεγγίσεις. Ωστόσο, τα μοντέλα μπορούν επίσης να χρησιμοποιηθούν παραγωγικά, για να δημιουργήσουν αυτομάτως λειτουργικά συστήματα. Ένα στιγμιότυπο οθόνης μιας διεπαφής χρήστη σε ένα πρωτότυπο σύστημα για τη δημιουργία μητρώων σε Blockchain παρουσιάζεται στο Σχήμα 14.



**Σχήμα 14: Διεπαφή χρήστη κατά τη διάρκεια διαμόρφωσης μιας εγγραφής σε Blockchain περιβάλλον (Staples et al., 2017).**

#### 2.4.14.2 Διασφάλιση

Δεν έχει ακόμη αποσαφηνιστεί πλήρως ο τρόπος αντιμετώπισης των αποτυχιών που μπορεί να προκύψουν κατά τη χρήση συστημάτων που βασίζονται σε Blockchain. Οι περισσότερες δοκιμές ανάπτυξης συστημάτων που βασίζονται σε Blockchain μέχρι σήμερα έχουν παρουσιάσει μόνο αισιόδοξα σενάρια, όπου δεν παρουσιάζεται κανένα σφάλμα ή εξαίρεση. Ωστόσο, στα συστήματα Blockchain του πραγματικού κόσμου, μπορεί να προκύψουν προβλήματα όπως αμφισβητούμενες συναλλαγές, λανθασμένες διευθύνσεις, έκθεση ή απώλεια ιδιωτικών κλειδιών, σφάλματα εισαγωγής δεδομένων ή απροσδόκητες αλλαγές σε εγγραφές που έχουν καταχωρηθεί στο Blockchain. Το αμετάβλητο των καθολικών Blockchain



μπορεί να τα κάνει λιγότερο προσαρμόσιμα συγκριτικά με τις συμβατικές τεχνολογίες που ελέγχονται από αξιόπιστους οργανισμούς τρίτων. Ωστόσο, οι επιδείξεις συστημάτων που βασίζονται σε Blockchain δεν διερευνούν συνήθως την αιτία και την επίλυση των απαισιόδοξων σεναρίων. Ορισμένα προβλήματα μπορεί να είναι αναμενόμενα προβλήματα, με μηχανισμούς επίλυσης ενσωματωμένους σε έξυπνα συμβόλαια ή στην περιρρέουσα υποδομή. Άλλα προβλήματα μπορεί να είναι απρόβλεπτα, αλλά θα εξακολουθούν να απαιτούνται μηχανισμοί επίλυσης εκτός του Blockchain.

Οι ρυθμιστικές αρχές και οι επιχειρήσεις θα πρέπει να γνωρίζουν τους τυπικούς τεχνικούς κινδύνους και τους περιορισμούς των τεχνολογιών Blockchain και να δίνουν ιδιαίτερη προσοχή ώστε να διασφαλίζουν ότι οι υποστηρικτές νέων συστημάτων που βασίζονται σε Blockchain παρέχουν επαρκή στοιχεία ότι τα νέα συστήματα πληρούν τις απαιτήσεις που σχετίζονται με αυτούς τους κινδύνους και τους περιορισμούς (Staples et al., 2017).

#### **2.4.15 Blockchain & GDPR**

Όπως αναφέρεται από τους Hofman et al. (2019), ο GDPR (General Data Protection Regulation) αποτελεί μια απάντηση στην σχεδόν πανταχού παρούσα κατάσταση επιτήρησης που οι σύγχρονες τεχνολογίες πληροφοριών και επικοινωνιών, σε συνδυασμό με άλλες ρυθμιστικές δυνάμεις, συμπεριλαμβανομένων των οικονομικών, νομικών και κοινωνικών συστημάτων, επέτρεψαν να ανθίσουν. Ο GDPR καθιερώνει την προστασία δεδομένων ως θεμελιώδες δικαίωμα των πολιτών της ΕΕ και έχει αρκετά φιλόδοξους στόχους:

1. Οι αρχές και οι κανόνες για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους θα πρέπει, ανεξαρτήτως εθνικότητας ή τόπου κατοικίας, να σέβονται τα θεμελιώδη δικαιώματα και ελευθερίες τους, ιδίως το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.
2. Ο παρών κανονισμός προορίζεται να συμβάλει στην υλοποίηση ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης και μιας οικονομικής ένωσης, στην οικονομική και κοινωνική πρόοδο, στην ενίσχυση και τη σύγκλιση των οικονομιών στην εσωτερική αγορά και στην ευεξία των φυσικών προσώπων.

Προς υποστήριξη αυτών των στόχων, ο GDPR (συγκεκριμένα στο 1<sup>ο</sup> τμήμα του άρθρου 5) αναδεικνύει έξι «αρχές που σχετίζονται με την επεξεργασία δεδομένων προσωπικού

χαρακτήρα»: νομιμότητα, δικαιοσύνη και διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης, ακεραιότητα και εμπιστευτικότητα. Αυτές οι έξι αρχές συμπληρώνεται με μια έβδομη, πρωταρχική αρχή της λογοδοσίας από την πλευρά των υπευθύνων επεξεργασίας δεδομένων. Αυτές οι αρχές, σε γενικές γραμμές, θα φαίνονται οικείες στους επαγγελματίες της διαχείρισης αρχείων και πληροφοριών και της διακυβέρνησης των πληροφοριών. Αυτό οφείλεται στο γεγονός ότι ο GDPR θέτει την προσδοκία ορθής διακυβέρνησης πληροφοριών στους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων κατά τη χρήση των προσωπικών τους δεδομένων. Στον παρακάτω πίνακα παρουσιάζεται μια σύντομη αντιστοίχιση άρθρων του GARP (Generally Accepted Recordkeeping Principles/Γενικά αποδεκτές αρχές τήρησης αρχείων) της ARMA (Association of Records Managers & Administrators/Ένωση υπευθύνων και διαχειριστών αρχείων) [ΗΠΑ] σε ένα μέρος διατάξεων του GDPR [ΕΕ].

**Πίνακας 6: Αντιστοίχιση αρχών GARP με άρθρα του GDPR (Hofman et al., 2019)**

<b>Αρχή GARP</b>	<b>Περιγραφή</b>	<b>Αντιστοιχία με άρθρο του GDPR</b>
Αρχή της υπευθυνότητας	Ένα ανώτερο στέλεχος (ή ένα πρόσωπο ανάλογης εξουσίας) επιβλέπει το πρόγραμμα Διακυβέρνησης Πληροφοριών και θα αναθέτει την ευθύνη για τη διαχείριση πληροφοριών σε κατάλληλα άτομα.	-Άρθρο 37 GDPR (Υπεύθυνος Προστασίας Δεδομένων) -Άρθρο 24 GDPR (Ελεγκτής) -Άρθρο 27 GDPR (Εκπροσώπηση του ελεγκτή) -Άρθρο 28 GDPR (Επεξεργαστής)
Αρχή της διαφάνειας	Οι επιχειρηματικές διαδικασίες και δραστηριότητες ενός οργανισμού, συμπεριλαμβανομένου του προγράμματος Διακυβέρνησης Πληροφοριών, θα τεκμηριώνονται με ανοιχτό και επαληθεύσιμο τρόπο και η τεκμηρίωση αυτή θα είναι διαθέσιμη σε όλο το	-Άρθρο 5, Παράγραφος 2 GDPR (ευθύνη του ελεγκτή) -Άρθρο 12 GDPR (Διαφάνεια) -Άρθρο 13 GDPR (Πληροφορίες και πρόσβαση) -Άρθρο 14 GDPR (Πληροφορίες εάν δεν ελήφθησαν δεδομένα

	προσωπικό και στα κατάλληλα ενδιαφερόμενα μέρη.	από το υποκείμενο των δεδομένων) -Άρθρο 19 GDPR (Ειδοποίηση σχετικά με τη διαγραφή και τη διόρθωση) -Άρθρο 25 GDPR (προστασία δεδομένων από σχεδιασμό και από προεπιλογή) -Άρθρο 30 GDPR (Αρχεία Δραστηριοτήτων Επεξεργασίας) -Άρθρο 40 GDPR (Κώδικες Δεοντολογίας)
Αρχή της ακεραιότητας	Ένα πρόγραμμα Διακυβέρνησης Πληροφοριών θα κατασκευαστεί έτσι ώστε τα περιουσιακά στοιχεία πληροφοριών που παράγονται ή διαχειρίζονται για τον οργανισμό να έχουν μια εύλογη εγγύηση αυθεντικότητας και αξιοπιστίας.	-Άρθρο 5, Παράγραφος 1, στοιχείο β-ε GDPR (Αρχές) -Άρθρο 16 GDPR (Διόρθωση) -Άρθρο 17 GDPR (Διαγραφή)
Αρχή της προστασίας	Ένα πρόγραμμα Διακυβέρνησης Πληροφοριών θα κατασκευαστεί για να εξασφαλίσει ένα κατάλληλο επίπεδο προστασίας σε περιουσιακά στοιχεία πληροφοριών που είναι ιδιωτικά, εμπιστευτικά, προνομιακά, απόρρητα, διαβαθμισμένα, απαραίτητα για την επιχειρησιακή συνέχεια ή που απαιτούν άλλου είδους προστασία.	-Άρθρο 5 GDPR (Αρχές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα) -Άρθρο 24 GDPR (Μέτρα που πρέπει να εφαρμοστούν από τον ελεγκτή) -Άρθρο 32 GDPR (Ασφάλεια Επεξεργασίας) -Άρθρο 44 GDPR (Μεταφορές προσωπικών δεδομένων σε τρίτες χώρες και διεθνείς οργανισμούς)

Αρχή της συμμόρφωσης	Ένα πρόγραμμα Διακυβέρνησης Πληροφοριών θα κατασκευαστεί για να συμμορφώνεται με την ισχύουσα νομοθεσία, άλλες δεσμευτικές αρχές και τις πολιτικές του οργανισμού.	GDPR γενικά και ειδικότερα: -Άρθρο 6 GDPR (Νομιμότητα της επεξεργασίας) -Άρθρο 47 GDPR (Δεσμευτικοί εταιρικοί κανόνες)
Αρχή της διαθεσιμότητας	Ένας οργανισμός διατηρεί τα περιουσιακά στοιχεία πληροφοριών του με τρόπο που να διασφαλίζει την έγκαιρη, αποτελεσματική και ακριβή ανάκτησή τους.	-Άρθρο 15 GDPR (Δικαίωμα πρόσβασης από το αντικείμενο των δεδομένων) -Άρθρο 20 GDPR (Φορητότητα δεδομένων)
Αρχή της διατήρησης	Ένας οργανισμός διατηρεί τα στοιχεία του ενεργητικού του για κατάλληλο χρονικό διάστημα, λαμβάνοντας υπόψη τις νομικές, κανονιστικές, φορολογικές, λειτουργικές και ιστορικές απαιτήσεις του.	-Άρθρο 5, Παράγραφος 1, στοιχ. ε GDPR (διατήρηση) -Άρθρο 15 GDPR (Δικαίωμα πρόσβασης από το υποκείμενο των δεδομένων)
Αρχή της απόρριψης	Ένας οργανισμός πρέπει να παρέχει ασφαλή και κατάλληλη διάθεση για περιουσιακά στοιχεία πληροφοριών που δεν απαιτείται πλέον να διατηρούνται, σύμφωνα με την ισχύουσα νομοθεσία και τις πολιτικές του οργανισμού.	-Άρθρο 5 GDPR (Αρχές) -Άρθρο 17 GDPR (Διαγραφή) -Άρθρο 20 GDPR (Φορητότητα δεδομένων) -Άρθρο 30, Παράγραφος 1, στοιχ. στ GDPR

Το Blockchain γενικά αποτελεί μέρος μιας ευρύτερης τάσης «ψηφιοποιημένων οικοσυστημάτων», τα οποία είναι «πλατφόρμες που θέτουν τα θεμέλια για εντελώς νέα επιχειρηματικά μοντέλα που αποτελούν τη γέφυρα μεταξύ ανθρώπων και τεχνολογιών». Η διαχείριση αυτών των νέων μοντέλων, ωστόσο, θα απαιτήσει προσαρμογή –ή ακόμη και ανάπτυξη νέων– μοντέλων διακυβέρνησης πληροφοριών. Τα χρονοδιαγράμματα διατήρησης είναι τόσο μεταβλητά όσο και οι οργανισμοί που τα χρησιμοποιούν, αλλά όλα βασίζονται σε κάποια μορφή ταξινόμησης αρχείων ώστε να προσδιοριστεί η κατάλληλη περίοδος διατήρησης ανά περίπτωση. Η ταξινόμηση των εγγραφών Blockchain είναι εξαιρετικά δύσκολη, εν μέρει, επειδή ο αρχειακός δεσμός δεν έχει δημιουργηθεί εγγενώς στο

Blockchain περιβάλλον. Συνεπώς πρέπει να προστεθούν σημαντικά μεταδεδομένα στα Blockchain για να συσχετιστούν οι συναλλαγές με τις διαδικασίες στις οποίες συμμετέχουν. Χωρίς πληροφορίες σχετικά με την ταυτότητα ενός αρχείου, είναι δύσκολο, αν όχι αδύνατο, να καθοριστεί η κατάλληλη περίοδος διατήρησης.

Ένας σημαντικός αριθμός από τις βελτιώσεις που πρέπει να γίνουν στις λύσεις Blockchain έχουν να κάνουν με τη θεμελιώδη λειτουργία διαχείρισης αρχείων και πληροφοριών που εξυπηρετούν τα Blockchain. Για να ικανοποιηθούν τρέχουσες οργανωτικές ανάγκες σε περιπτώσεις όπου εφαρμόζονται λύσεις Blockchain, πρέπει να γίνουν κατανοητά πολύ περισσότερα σχετικά με τις εγγραφές Blockchain από την οπτική γωνία της διακυβέρνησης των πληροφοριών. Αυτή η κατανόηση θα απαιτήσει την εξέταση των πολύπλοκων, ενσωματωμένων, κοινωνικών, δεδομένων και τεχνικών επιπέδων των τεχνολογιών Blockchain.

Οι λύσεις Blockchain προσφέρουν μια σειρά από ελκυστικές πτυχές, από την άποψη της διακυβέρνησης των πληροφοριών:

- Προσφέρουν αποδιαμεσολάβηση, η οποία μπορεί να είναι ανεκτίμητη για κοινά αρχεία σε καταστάσεις χαμηλής εμπιστοσύνης (π.χ. μεταξύ χρηματοπιστωτικών ιδρυμάτων)
- Δημιουργούν και επικυρώνουν συναλλαγές αυτόματα, χωρίς ανθρώπινη παρέμβαση, γεγονός που μπορεί να μειώσει την εργασία που απαιτείται για τη δημιουργία αρχείων και να αυξήσει τη συμμόρφωση
- Προσφέρουν τεχνική διαφάνεια, δηλαδή τη δυνατότητα μιας τεχνικής λύσης να καθιστά διαθέσιμες και/ή προσβάσιμες πληροφορίες, πράγμα που μπορεί να υποστηρίξει τη διαφάνεια της διαδικασίας και ακόμη και την οργανωτική διαφάνεια
- Είναι ανθεκτικά σε παραποίηση και παραβιάσεις, γεγονός που μπορεί να αυξήσει την ασφάλεια και τη δυνατότητα ελέγχου των αρχείων.

Ωστόσο, η τεχνολογία Blockchain δεν σχεδιάστηκε αρχικά ως λύση τήρησης/διαχείρισης αρχείων (ή ακόμα και ως βάση δεδομένων) παρόλο που έχει τη δυνατότητα να λειτουργήσει ως ένα τέτοιο σύστημα, αλλά για να υποστηρίξει την ανταλλαγή του κρυπτονομίσματος Bitcoin. Εάν οι τεχνολογίες Blockchain πρόκειται να γίνουν κεντρικό μέρος της υποδομής των αρχείων μας, οι προκλήσεις σχετικά με τη διακυβέρνηση των πληροφοριών πρέπει επίσης να

αντιμετωπιστούν. Για παράδειγμα, σε περιπτώσεις όπου ένα Blockchain χρησιμοποιείται για τη διασφάλιση της ακεραιότητας των εγγραφών που δημιουργούνται εκτός του Blockchain, δεν υπάρχει κάποιο Blockchain που να εγγυάται ότι αυτές οι εγγραφές είναι ακριβείς ή αξιόπιστες. Όπως αναφέρθηκε παραπάνω, ο αρχειακός δεσμός δεν δημιουργείται εγγενώς στο Blockchain, καθιστώντας πρόκληση την αναγνώριση και ταξινόμηση των αρχείων. Η ανθεκτικότητα του Blockchain στην παραβίαση καθιστά δύσκολη, αν όχι αδύνατη, τη διόρθωση, την απόκρυψη και/ή την καταστροφή των αρχείων. Παράλληλα, η διεθνική, κατανεμημένη φύση του Blockchain μπορεί να δημιουργήσει σημαντικές προκλήσεις συμμόρφωσης όταν τα Blockchain χρησιμοποιούνται για τη διαχείριση των πληροφοριακών στοιχείων των οργανισμών. Επιπλέον, καθώς οι πάροχοι λύσεων Blockchain προσπάθησαν να καθιερώσουν τα Blockchain και ως συστήματα τήρησης/διαχείρισης αρχείων, έχουν τοποθετήσει συνεχώς αυξανόμενες ποσότητες δεδομένων, ορισμένα προσωπικά αναγνωρίσιμα, στο Blockchain. Σε πολλές περιπτώσεις, έχουν γράψει αυτές τις πληροφορίες σε καθαρό κείμενο, αντί για το κρυπτογραφημένο κείμενο ενός κατακερματισμού, με αποτέλεσμα τέτοιες πληροφορίες να καταγράφονται αμετάβλητα σε ένα ανοιχτό δημόσιο καθολικό. Τέτοιες ελλείψεις στον τεχνικό σχεδιασμό και τη χρήση του Blockchain από την οπτική γωνία της διακυβέρνησης πληροφοριών εγείρουν σοβαρά ερωτήματα σχετικά με το κατά πόσο η τεχνολογία αυτή μπορεί ποτέ να ανταποκριθεί στις απαιτήσεις του GDPR.

Άλλο ένα ζήτημα αποτελούν οι προκλήσεις του Blockchain έναντι του GDPR. Ο GDPR προέκυψε σε μεγάλο βαθμό στο πλαίσιο ενός Διαδικτύου που υποστηρίζεται από κεντρικές τεχνολογίες cloud. Το Blockchain, αντίθετα, βασίζεται σε μια κατανεμημένη αρχιτεκτονική. Αυτό δημιουργεί ένα ιδιαίτερο πρόβλημα όταν πρόκειται να καθοριστεί ποιος είναι υπεύθυνος ελέγχου ή επεξεργασίας δεδομένων εντός του πεδίου εφαρμογής του GDPR, όταν τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία σε ένα Blockchain περιβάλλον. Θεωρητικά, κάθε εξορύκτης σε ένα δημόσιο Blockchain χωρίς άδεια θα μπορούσε να είναι ελεγκτής κατά την έννοια του GDPR. Επιπλέον, το δικαίωμα στη λήθη, προσδιορίζεται επίσης ως ένα ιδιαίτερο πρόβλημα σε σχέση με μια τεχνολογία που μπορεί να αναφέρεται τα αμετάβλητα αρχεία ως ένα από τα κύρια πλεονεκτήματά της. Η αμεταβλητότητα των συναλλαγών δεδομένων που αποτυπώνονται μέσα σε Blockchain περιβάλλον αμέσως υποδηλώνει ότι μία από τις βασικές αρχές του GDPR (Άρθρο 17: δικαίωμα διαγραφής) δεν καλύπτεται από το Blockchain. Το δικαίωμα στη διαγραφή θα αποδειχθεί ένα ιδιαίτερα

ενδιαφέρον ζήτημα καθώς, αυτή τη στιγμή, το τι συνιστά διαγραφή δεν έχει αποσαφηνιστεί πλήρως και είναι ακόμα ανοιχτό προς συζήτηση. Άλλο ένα θέμα προς συζήτηση αποτελούν οι «στρατηγικές ανησυχίες» κατά τη δημιουργία και εφαρμογή λύσεων Blockchain. Ούτως ή άλλως ο GDPR αποτελεί άλλο ένα (πρόσφατο) παράδειγμα τρόπου ρύθμισης της συλλογής, χρήσης, αποθήκευσης και διακυβέρνησης των πληροφοριών. Την ίδια στιγμή όμως απαιτείται από τους οργανισμούς να κατανοούν και να διαχειρίζονται τα δεδομένα τους. Στην περίπτωση του GDPR, επίσης, δεν φαίνεται να υπάρχει πλήρης εμπιστοσύνη στους υπεύθυνους επεξεργασίας δεδομένων από τα υποκείμενα των δεδομένων οπότε δικαιούνται και περισσότερο έλεγχο σχετικά με τον τρόπο επεξεργασίας των δεδομένων τους. Τα Blockchain από την άλλη μπορούν να αποδειχθούν ισχυρά εργαλεία για την εφαρμογή του απορρήτου από την προεπιλογή και τον σχεδιασμό.

Γενικά υπάρχει μια πεποίθηση ότι η τεχνολογία Blockchain και το GDPR δεν μπορούν να συνυπάρξουν αρμονικά. Το μεγαλύτερο μέρος της αρχικής αντίδρασης σχετικά με το Blockchain είναι ότι αυτή η νέα τεχνολογία δεν είναι καθόλου συμβατή με τις νέες οδηγίες του GDPR, άποψη που αντικρούεται από τα δεδομένα που παρουσιάζονται παρακάτω.

Το Blockchain μπορεί να θεωρηθεί ως τεχνολογία που μπορεί όχι μόνο να βελτιώσει τη θεμελιώδη πτυχή του απορρήτου και της ασφάλειας δεδομένων, όπως ορίζεται και στο GDPR, αλλά μπορεί επίσης να μελετηθεί προσεκτικά, να σχεδιαστεί και να εφαρμοστεί σε πλήρη συμμόρφωση με τον GDPR ως προς το απόρρητο δεδομένων, χρησιμοποιώντας ορισμένες μοναδικές τεχνικές. Αυτές οι εναλλακτικές λύσεις δεν είναι απλές στην εφαρμογή τους και απαιτούν βαθιά κατανόηση του τρόπου λειτουργίας του Blockchain και του τρόπου αλληλεπίδρασης του τεχνολογικού οικοσυστήματος, για τη δημιουργία αρχιτεκτονικών συμβατών με το GDPR και το Blockchain.

Ορισμένα προβλήματα που εντοπίζονται, όπως το δικαίωμα διαγραφής, ο ορισμός ελεγκτών δεδομένων, η εύρεση και αναγνώριση προσωπικών δεδομένων σε Blockchain, αποτελούν αντικείμενο έρευνας για την επίλυση τους. Για παράδειγμα, η πιο συχνά προτεινόμενη λύση για τη «διαγραφή» δεδομένων από το Blockchain είναι η μη αναστρέψιμη κρυπτογράφηση, δηλαδή η ανάκληση των δικαιωμάτων πρόσβασης σε δεδομένα για να τα καταστήσει απρόσιτα, πράγμα που ενδέχεται να έρθει αντιμέτωπο με τη νομοθεσία σε ορισμένες περιπτώσεις. Μια άλλη προτεινόμενη λύση, που εφαρμόζεται πλέον συχνά, είναι απλώς η

αποθήκευση προσωπικών δεδομένων εκτός του Blockchain, με δείκτες που βρίσκονται εντός του Blockchain.

Έχουν αναπτυχθεί και προσφέρονται στην αγορά προϊόντα συμμόρφωσης με το GDPR που βασίζονται σε Blockchain, καθιστώντας έτσι σαφές ότι η τεχνολογία Blockchain μπορεί να βοηθήσει (και όχι να εμποδίζει) τη συμμόρφωση με τον GDPR. Ενδεικτικά, 3 από αυτά είναι τα εξής:

- **VOLTA:** είναι μια εφαρμογή που αναπτύχθηκε από την Guardtime για να παρέχει στους οργανισμούς μια λύση για τη συμμόρφωση με τον GDPR και έχει σχεδιαστεί για να υποστηρίζει διαδικασίες διακυβέρνησης και συμμόρφωσης για τη διαχείριση προσωπικών αναγνωρίσιμων πληροφοριών, που προσδιορίζονται από τον GDPR. Το VOLTA ενσωματώνει διαφορετικά συστήματα και ροές εργασίας (π.χ. εφαρμογές, διεργασίες και υπηρεσίες) για να παρακολουθεί τον τρόπο χρήσης των προσωπικά αναγνωρίσιμων πληροφοριών. Το VOLTA ολοκληρώνει την ενσωμάτωση υποστηρίζοντας ελαφριές διεπαφές (π.χ. CSV, REST) και «επιτρέποντας την εφαρμογή πολιτικών καθορισμένων από τον χρήστη σε όλες τις συναλλαγές που σχετίζονται με τη διαχείριση προσωπικών δεδομένων».
- **PikcioChain:** είναι μια εφαρμογή με προσέγγιση εστιασμένη περισσότερο στα δεδομένα. Το PikcioChain είναι μια κατανεμημένη πλατφόρμα που βασίζεται σε άδειες, αναπτύχθηκε από την Pikcio AG και εστιάζει στη συλλογή, πιστοποίηση, επαλήθευση και ανταλλαγή προσωπικών δεδομένων. Ακόμη, δίνει τη δυνατότητα στις επιχειρήσεις να εμπορεύονται και να ανταλλάσσουν προσωπικά δεδομένα, ενώ δίνει στα άτομα τον έλεγχο των προσωπικών τους δεδομένων και την ευκαιρία να αποζημιωθούν για τη χρήση τους.
- **GDPR Edge:** είναι μια λύση συμμόρφωσης με προσανατολισμό στις επιχειρήσεις, η οποία συνδυάζει ένα Blockchain με μια «λίμνη» δεδομένων.

Καθεμία από αυτές τις λύσεις στοχεύει ένα διαφορετικό τμήμα αναγκών στην εποχή μετά τον GDPR, δείχνοντας την πληθώρα επιλογών που μπορούν να προκύψουν από τη χρήση της Blockchain τεχνολογίας, με τρόπο που παράλληλα υποστηρίζει τη συμβατότητα με τον GDPR.



## Κεφάλαιο 3. Μεθοδολογία ή/και Σχέδιο εργασιών– Υλοποίηση – Εφαρμογή

### 3.1 Σχέδιο Εργασιών

Εφόσον δεν υπάρχουν διαθέσιμες πληροφορίες σχετικά με τον τρόπο λειτουργίας και τη ροή εργασιών της Υπηρεσίας, καθίσταται αναγκαία η επί τόπου επίσκεψη, παρατήρηση και καταγραφή επαρκών δεδομένων που θα συμβάλλουν στην ολοκλήρωση της ερευνητικής διαδικασίας, την ερμηνεία των αποτελεσμάτων και τη μετέπειτα συνεισφορά της σε μελλοντικά πρότζεκτ.

Σύμφωνα με την Μιχαήλ (2021), ο σχεδιασμός της έρευνας είναι απαραίτητος για λόγους:

- Ενδογενείς: σχετίζονται με την ανάγκη να:
  - Προετοιμάσει ο ερευνητής/η ερευνητική ομάδα αναγκαίες προκαταρκτικές ενέργειες
  - Να λάβει σημαντικές αποφάσεις
  - Να εντοπίσει κινδύνους που μπορούν να αναστείλουν ή να ματαιώσουν την έρευνα
  - Να αποκτήσει μια βάση για την παρακολούθηση της εξέλιξης της ερευνητικής διαδικασίας και των μεταβολών στους αρχικούς σχεδιασμούς.
- Εξωγενείς: σχετίζονται με την υποχρέωση του ερευνητή να παρουσιάσει με αναλυτικό τρόπο την ερευνητική του στρατηγική σε επιτροπές έγκρισης της πρότασης ή πιθανούς χρηματοδότες.

Όπως αναφέρουν οι Ίσαρη & Πουρκός (2016), Η σχέση μεταξύ της θεωρίας και της έρευνας είναι ανοικτή, αλληλεπιδραστική. Δεν υπάρχει μεταξύ τους διακριτός διαχωρισμός. Οι ερευνητικές υποθέσεις κατασκευάζονται καθώς προχωρά η έρευνα και η θεωρία αναδύεται από τα ερευνητικά δεδομένα. Αντίστοιχα ο ερευνητικός σχεδιασμός είναι μη δομημένος, ανοικτός και κατασκευάζεται κατά τη διάρκεια της έρευνας προσαρμοζόμενος συνεχώς στα νέα, απροσδόκητα δεδομένα. Έτσι, τα δεδομένα που προκύπτουν από συνεντεύξεις, αφηγήσεις και παρατηρήσεις των υποκειμένων (αφηγηματική προοπτική) παρουσιάζονται με διάφορους περιγραφικούς τρόπους.

## 3.2 Περιγραφή Υλοποίησης – Εφαρμογής

Η επιτόπου έρευνα στο χώρο της υπηρεσίας πραγματοποιήθηκε σε διάστημα 2 ημερών, έτσι ώστε να υπάρξει επαρκής χρόνος για ενασχόληση με όλα τα τμήματα της υπηρεσίας (βλ. συνημμένο έγγραφο στο παράρτημα). Στο διάστημα αυτό πραγματοποιήθηκε παρατήρηση και καταγραφή λεπτομερειών που αφορούν τον τρόπο λειτουργίας, τις συλλογές, το λογισμικό διαχείρισης εγγράφων, τον εξοπλισμό, τους χώρους, τις συνθήκες αποθήκευσης και τη διαδικασία ψηφιοποίησης. Έχοντας ήδη μια εμπειρία και έναν βαθμό εξοικείωσης με το προσωπικό και τη ροή εργασιών της υπηρεσίας λόγω της στρατιωτικής μου θητείας, δεν απαιτήθηκε τόσο μεγάλο χρονικό διάστημα για την εκπόνηση της έρευνας συγκριτικά με ένα άτομο που δεν είχε καμία προηγούμενη επαφή με τον συγκεκριμένο οργανισμό άμυνας.

## 3.3 Στόχος της Έρευνας και Μεθοδολογία

Όπως αναφέρθηκε παραπάνω, η έρευνα ανήκει στην κατηγορία των ποιοτικών ερευνών και συγκεκριμένα πραγματοποιήθηκε με τη μέθοδο της επιτόπιας παρατήρησης. Γενικά, όπως αναφέρεται και από την Μιχαήλ (2021), μια έρευνα που εντάσσεται στο πλαίσιο των ποιοτικών ερευνών μπορεί να έχει χαρακτηριστικά όπως τα παρακάτω:

- υιοθετεί ευέλικτα ερευνητικά σχέδια τα οποία μπορούν να επαναπροσδιοριστούν σε όλες τις πτυχές κατά τη διάρκεια της ερευνητικής διαδικασίας και βάσει ευρημάτων που προκύπτουν ήδη από τα αρχικά στάδια της έρευνας
- πραγματοποιείται στον «πραγματικό» κόσμο και όχι σε πειραματικά περιβάλλοντα
- αποσκοπεί στην ανακάλυψη νέων πτυχών του εξεταζόμενου φαινομένου μέσω της διατύπωσης υποθέσεων θεμελιωμένων στην ανάλυση των εμπειρικών δεδομένων
- χρησιμοποιεί ευέλικτες μεθόδους παραγωγής δεδομένων
- χρησιμοποιεί διαφορετικά είδη παρατήρησης και συλλογής δεδομένων: Επιτόπια συμμετοχική παρατήρηση (ανθρωπολογία), συνέντευξη, βιογραφικές αφηγήσεις, ομάδες εστίασης, συλλογή κι ανάλυση τεκμηρίων (φωτογραφιών, ημερολογίων, επιστολών, δημοσίων εγγράφων, φιλμ, δημοσιευμάτων στον τύπο, καταγραφών και διαλόγων σε ομάδες κοινωνικής δικτύωσης κλπ)
- αξιοποιεί μεθόδους και διαδικασίες που λαμβάνουν υπόψη την περιπλοκότητα, την λεπτομέρεια και το πλαίσιο παραγωγής δεδομένων

- αξιοποιεί μεθόδους που παρέχουν τη δυνατότητα σχηματισμού θεωρητικών κατηγοριών που θεμελιώνονται στα εμπειρικά δεδομένα, ενώ αποφεύγει την υπαγωγή των δεδομένων σε ένα προκαθορισμένο σύστημα ταξινομήσεων και εννοιών
- αναπτύσσει εξηγήσεις στο επίπεδο της κατανόησης του νοήματος και λιγότερο σε εκείνο της αποκάλυψης αιτιών.

Στη συγκεκριμένη περίπτωση, «συμμετέχων ως παρατηρητής» (the participant as observer), ο ερευνητής αποκαλύπτει την ιδιότητά του καθώς και τον σκοπό της έρευνας και συμμετέχει στις δραστηριότητες ή διεργασίες της υπό διερεύνηση ομάδας (Ίσαρη & Πουρκός, 2016). Η επιτόπια παρατήρηση αποτελεί μέθοδο που προέρχεται από την Ανθρωπολογία και ανήκει στις Εθνογραφικές μεθόδους. Συνίσταται στην παρατήρηση μιας συμπεριφοράς (η ενός φαινομένου) εντός του περιβάλλοντος στο οποίο εκδηλώνεται. Σε αυτή την περίπτωση τα υποκείμενα της έρευνας δεν ερωτώνται σε σχέση με τη συμπεριφορά τους αλλά παρατηρούνται από τον ερευνητή. Η επιτόπια παρατήρηση κυρίως ενδείκνυται για να διερευνηθούν στοιχεία που μπορεί να μην αξιολογούνται ως σημαντικά από τους ερευνώμενους και συνεπώς να μην αναφέρονται σε άλλη ερευνητική διαδικασία, όπως η συνέντευξη. Γενικά υπάρχουν διάφοροι τύποι παρατήρησης ανάλογα με τον βαθμό συμμετοχής του παρατηρητή και το βαθμό δόμησης της διαδικασίας παρατήρησης (κατηγορίες παρατήρησης).

Ακόμη, θα πρέπει να προηγηθεί μια προετοιμασία για την πρόσβαση στο πεδίο καθώς ο ερευνητής θα πρέπει ήδη από το στάδιο του σχεδιασμού να προβλέψει τις δυναμικές που μπορεί να ενεργοποιήσει η είσοδός του στο πεδίο αλλά και την ενδεχόμενη αναστάτωση που μπορεί να προκαλέσει και να σκεφτεί τους τρόπους με τους οποίους τα παραπάνω μπορεί να επηρεάσουν την έρευνά του. Αυτό επιβεβαιώνεται και από τους Ίσαρη & Πουρκός (2016), οι οποίοι αναφέρουν ότι η σχέση του ερευνητή με το αντικείμενο της έρευνας και το περιβάλλον είναι νατουραλιστική (το αντικείμενο μελετάται στο φυσικό του πλαίσιο), που σημαίνει ότι ο ερευνητής αποφεύγει κάθε μορφή χειρισμού, ερεθισμού, παρεμβολής ή διατάραξης του (π.χ. συμμετοχική παρατήρηση). Επιπρόσθετα, ο ερευνητής θεωρεί δεδομένη την υποκειμενική ανταπόκριση και τον αναστοχασμό των υποκειμένων και προσπαθεί να τα λάβει υπόψη ως αναπόσπαστο μέρος της ερευνητικής διαδικασίας. Σε κάθε περίπτωση απώτερος σκοπός είναι η κατανόηση των υποκειμένων, των επιμέρους τους

προοπτικών μαζί με το πλαίσιο που αυτές λειτουργούν, μέσα από την ανάλυση. Στην ανάλυση των προοπτικών αυτών το πολύ που μπορεί να κάνει ένας ερευνητής είναι να τις ταξινομήσει και να διακρίνει σε αυτές ιδεώδεις τύπους λαμβάνοντας υπόψη διάφορα κριτήρια ή διαστάσεις.

Πρακτικά κύριος στόχος της έρευνας είναι να αντλήσει και να παρουσιάσει ερευνητικά δεδομένα τα οποία:

- αρχικά θα παρουσιάζουν γενικές πληροφορίες σχετικά με τον τρόπο λειτουργίας της υπηρεσίας .
- εστιάζουν σε επιμέρους θεμελιώδεις κατηγορίες που αφορούν την υπηρεσία ξεκινώντας από το ανθρώπινο δυναμικό (δομή, προσωπικό), ενώ γίνεται αναφορά και σε πιο πρακτικά θέματα (εξοπλισμός και υποδομές), για να καταλήξει στα πιο τεχνικά ζητήματα (διαχείριση και αξιοποίηση αρχειακού υλικού, ψηφιοποίηση) .
- ειδική μνεία γίνεται στις ενέργειες που μπορούν να γίνουν εκ μέρους της ηγεσίας ως προς την κατάρτιση και «δια βίου μάθηση» του προσωπικού αλλά και της υπηρεσίας συνολικά ως προς τις νέες και συνεχώς μεταβαλλόμενες τεχνολογικές και νομοθετικές (ως προς τη διαχείριση αρχειακού υλικού και προσωπικών δεδομένων) εξελίξεις και μεταρρυθμίσεις.
- αναδεικνύουν τυχόν ελλείψεις/ανασταλτικούς παράγοντες που έχουν χρονικές και οικονομικές επιπτώσεις και εμποδίζουν την εύρυθμη λειτουργία της υπηρεσίας.
- στις προτάσεις δεν γίνεται αναφορά στην ενότητα διαχείρισης και αξιοποίησης αρχειακού υλικού καθώς οι αλλαγές στον τομέα αυτό είναι άμεσα συνδεδεμένες με την προτεινόμενη Blockchain τεχνολογία που θα ενσωματωθεί στο Document Management System.
- το κομμάτι της ψηφιοποίησης μένει επίσης εκτός της λίστας των προτάσεων καθώς αποτελεί μια διαδικασία που απαιτεί όχι μόνο χρόνο αλλά και εξειδικευμένο προσωπικό για να προχωρήσει ομαλά. Το σκέλος στο οποίο μπορεί να υπάρξει μεταβολή είναι ο τρόπος και το μέρος αποθήκευσης των ψηφιοποιημένων αρχείων, όπου η αποθήκευση δεν θα γίνεται τοπικά αλλά απευθείας στο νέο λογισμικό.
- οι προτάσεις που παρουσιάζονται παρακάτω, οι οποίες είναι επικεντρωμένες στην υπηρεσία, σε συνδυασμό με τα συμπεράσματα που προκύπτουν μέσα από τη

βιβλιογραφία, τα οποία είναι πιο γενικά, εφόσον συνδυαστούν μπορούν να αποτελέσουν αντικείμενο μελλοντικής έρευνας πάνω στο θέμα.

## **Κεφάλαιο 4. Αποτελέσματα – Ευρήματα / Επιτεύγματα**

### **4.1 Αναλυτική παρουσίαση αποτελεσμάτων**

Παρακάτω παρουσιάζονται αναλυτικά τα δεδομένα που προέκυψαν μέσα από την ερευνητική διαδικασία. Ορισμένες πληροφορίες από αυτές που παρατίθενται στη συνέχεια (π.χ. ονομασίες νομοθετικών διατάξεων, ημερομηνίες δημοσίευσης ΦΕΚ) προέκυψαν μέσα από αναζήτηση στον ιστό για να διασταυρωθούν και να επιτευχθεί όσο το δυνατόν μεγαλύτερη ακρίβεια.

#### **4.1.1 Δομή**

Η Υπηρεσία Στρατιωτικών Αρχείων υπάγεται στο Γενικό Επιτελείο Στρατού και αποτελείται από τα εξής τμήματα:

- Γραμματεία
- Τμήμα Ευρετηρίων και Κοινού
- 1<sup>ο</sup> Τμήμα: Έρευνας και Εκμετάλλευσης Αρχειακού Υλικού
- 2<sup>ο</sup> Τμήμα: Διακίνησης Αρχειακού Υλικού
- 3<sup>ο</sup> Τμήμα: Μικροφωτογράφισης
- 4<sup>ο</sup> Τμήμα: Υποστήριξης (το οποίο αποτελείται από το Τμήμα Διοικητικής Υποστήριξης και το Γραφείο Πληροφορικής)

#### **4.1.2 Υλικοτεχνικός εξοπλισμός και υποδομές**

- Υπάρχει επάρκεια τεχνολογικού εξοπλισμού, προσαρμοσμένος ανάλογα με τις ανάγκες και τις θέσεις εργασίας κάθε τμήματος.
- Ο εξοπλισμός διαμορφώνεται και συντηρείται τακτικά από το εξειδικευμένο προσωπικό του αρμόδιου τμήματος (γραφείο πληροφορικής).
- Στο κομμάτι της ψηφιοποίησης, η υπηρεσία διαθέτει τριών ειδών σαρωτές:
  - Επίπεδοι σαρωτές (flatbed), στους οποίους η κεφαλή κινείται κατά μήκος της σελίδας, σχεδίου ή φωτογραφίας

- Σαρωτές χειρός ή χειροκίνητοι (handheld), δηλαδή μικρές συσκευές, τις οποίες ο χρήστης μετακινεί με το χέρι με σταθερή ταχύτητα πάνω από το εκάστοτε τεκμήριο
  - Σαρωτές έλξης, που από ιδιαίτερη υποδοχή τραβούν τη σελίδα πάνω από τη σταθερή κεφαλή (sheet-fed).
- Παρά το αυξημένο κόστος και το γεγονός ότι πρόκειται για κρατικό φορέα με μειωμένη χρηματοδότηση, ο διαθέσιμος εξοπλισμός που διαθέτει η υπηρεσία για την υποστήριξη του έργου της είναι παραπάνω από επαρκής ποσοτικά αλλά και ποιοτικά, διευκολύνοντας έτσι το έργο του προσωπικού.
  - Ανάλογα την περίπτωση, υπάρχουν αντίστοιχες θέσεις εργασίας, προσαρμοσμένες στις ανάγκες του κάθε τμήματος, που θα καλύψουν τις απαιτήσεις για κάθε τμήμα και αίτημα.
  - Οι διαθέσιμες θέσεις εργασίας περιλαμβάνουν στην πλειονότητα των περιπτώσεων και σταθερό ηλεκτρονικό υπολογιστή. Αν κάποια θέση καλυφθεί από κάποιον οπλίτη θητείας, ο ηλεκτρονικός υπολογιστής αυτομάτως θα έχει περιορισμένες δυνατότητες για λόγους ασφαλείας.
  - Η επικοινωνία με την υπηρεσία μέσω διαδικτύου περιορίζεται μόνο στη χρήση ηλεκτρονικού ταχυδρομείου καθώς η ιστοσελίδα της υπηρεσίας βρίσκεται εκτός λειτουργίας (αρμοδιότητα του Κέντρου Πληροφορικής Υποστήριξης Ελληνικού Στρατού (ΚΕ.Π.Υ.Ε.Σ)).
  - Οι κτηριακοί χώροι της υπηρεσίας διατηρούνται σε καλή κατάσταση, έχοντας κατά νου την παλαιότητα τους. Φυσικά ιδιαίτερο βάρος δίνεται στις αποθήκες που βρίσκεται το αρχειακό υλικό.

#### **4.1.3 Προσωπικό**

- Απαρτίζεται κατά κύριο λόγο από μόνιμο στρατιωτικό και πολιτικό προσωπικό και από οπλίτες θητείας που έχουν υποστηρικτικό ρόλο στα κατά τόπους τμήματα.
- Ανεξάρτητα από τη θέση που κατέχει ο καθένας, η πλειοψηφία των εργαζομένων διαθέτει σχετική εμπειρία/προϋπηρεσία με το αντικείμενο της υπηρεσίας και τεχνογνωσία, έτσι ώστε να μπορούν να ανταποκριθούν στις ανάγκες της. Αυτό εξοικονομεί παράλληλα χρόνο και πόρους που θα απαιτούσε η διεξαγωγή

εκπαίδευσης σε βάθος με στόχο την εξοικείωση του κάθε εργαζόμενου με το αντικείμενο.

- Οι οπλίτες θητείας, με από την ολοκλήρωση της στρατιωτικής τους θητείας και εφόσον κρίνει η υπηρεσία ότι ανταποκρίθηκαν σωστά και επαρκώς στο ρόλο που τους ανατέθηκε, λαμβάνουν έγγραφο που πιστοποιεί την προϋπηρεσία τους σε έναν κρατικό φορέα και δη έναν οργανισμό άμυνας. Ένα έγγραφο σαν και αυτό αποτελεί σημαντικό εργαλείο για το βιογραφικό τους σημείωμα και τη μετέπειτα έυρεση εργασίας.
- Λόγω της ιδιότητας τους, κατά κύριο λόγο μέλη του μόνιμου στρατιωτικού προσωπικού, μετατίθεται σε άλλη υπηρεσία/μονάδα οπότε ανά τακτά χρονικά διαστήματα επέρχονται αλλαγές στη στελέχωση της υπηρεσίας και απαιτείται εκ νέου μια περίοδος προσαρμογής και εξοικείωσης με τη ροή εργασιών ανά περίπτωση.

#### **4.1.4 Document Management System – «Πάπυρος»**

Το λογισμικό Πάπυρος αποτελεί ένα σύστημα διαχείρισης εγγράφων, το οποίο αναπτύχθηκε από την εταιρεία Modus και είναι παραμετροποιημένο και προσαρμοσμένο στις ανάγκες της υπηρεσίας. Το μόνιμο προσωπικό της υπηρεσίας είναι και οι μοναδικοί εξουσιοδοτημένοι χρήστες της εφαρμογής, οι οποίοι έχουν μέσα από τη διεπαφή χρήστη δυνατότητες:

- οργάνωσης εγγράφων
- ταξινόμησης εγγράφων
- αρχειοθέτησης
- απλής και σύνθετης αναζήτησης
- αναζήτησης σε ειδικές κατηγορίες αρχείων (π.χ. παλιά έγγραφα, δέματα, microfis)
- πρόσβασης στο αρχειακό υλικό
- περιήγησης στον κατάλογο των διαθέσιμων συλλογών
- διεκπεραίωσης διαδικασιών και αιτημάτων, ανάλογα με τη φύση τους
- εντοπισμού και ανάκτησης ψηφιοποιημένων αρχείων
- προσθήκη νέων εγγραφών
- προσθήκη της ψηφιακής μορφής σε ήδη υπάρχουσες εγγραφές
- εντοπισμού της τρέχουσας τοποθεσίας μη ψηφιοποιημένων αρχείων



Ειδικότερα στο κομμάτι της αναζήτησης, που είναι και από τις πιο σημαντικές λειτουργίες του λογισμικού για την υπηρεσία, υπάρχει η δυνατότητα αξιοποίησης συγκεκριμένων πεδίων για ακόμη πιο εξειδικευμένη αναζήτηση. Ορισμένα από αυτά τα πεδία είναι τα εξής:

- μονάδα
- τίτλος
- έτος
- α/α ευρετηρίου
- πακέτο
- ντέξιον
- θέση
- είδος τεκμηρίου
- θυρίδα
- αριθμός φιλμ
- διαβάθμιση
- τύπος φυσικού εγγράφου

Το λογισμικό αυτό διαθέτει ενσωματωμένη λειτουργία προβολής της ψηφιοποιημένης μορφής ενός αρχείου που έχει καταχωρηθεί στο σύστημα, εφόσον διατίθεται, με τη χρήση του αντίστοιχου λογισμικού ανάλογα με το μορφότυπο του αρχείου.

Επιπλέον, η αναζήτηση, μέσα από το λογισμικό Πάπυρος, μπορεί φυσικά να πραγματοποιηθεί όχι μόνο στα φιλμ αλλά και στο φυσικό και ψηφιοποιημένο αρχείο.

#### **4.1.5 Διαχείριση και αξιοποίηση αρχειακού υλικού**

Η ΥΣΑ διατηρεί αρχεία σε φυσική μορφή και σε μικροφίλμ, τα οποία έχουν αποδεικτική ισχύ ίση με το πρωτότυπο, σύμφωνα με την κείμενη νομοθεσία (Άρθρο 15§2 του Νόμου 1599/1986 [«Σχέσεις κράτους-πολίτη, καθιέρωση νέου τύπου δελτίου ταυτότητας και άλλες διατάξεις»]). Επίσης, τηρεί μέρος του αρχείου σε ψηφιακή μορφή και είναι υπεύθυνη για τη διαδικασία ψηφιοποίησης του συνόλου του τηρούμενου αρχείου, δηλαδή τη μετατροπή του φυσικού αρχείου και του εγγεγραμμένου σε μικροφίλμ σε ψηφιακό, ώστε να είναι εύκολα προσβάσιμο και διαχειρίσιμο από την Υπηρεσία, και τους εκάστοτε αιτούντες Στρατιωτικούς και Δημόσιους Φορείς, όπως επίσης τους ερευνητές, ιστορικούς και λοιπούς ιδιώτες.

Η ΥΣΑ παρέχει αρχειακό υλικό κατά κύριο λόγο για υπηρεσιακή χρήση και η χορήγηση στοιχείων από τα αρχεία της ΥΣΑ σε ιδιώτες γίνεται ως εξής:

- Κατόπιν αιτήματος των ενδιαφερομένων, είτε δια ζώσης με φυσική παρουσία στο χώρο της υπηρεσίας, είτε απομακρυσμένα μέσω συμβατικού ή ηλεκτρονικού ταχυδρομείου
  - Από το μη διαβαθμισμένο αρχείο, μπορούν να δοθούν στοιχεία που δεν εμπίπτουν στις περιοριστικές διατάξεις της ισχύουσας νομοθεσίας για την προστασία των προσωπικών δεδομένων και συνεπώς καθίστανται διαθέσιμα για έρευνα στο κοινό, στο πλαίσιο των διατάξεων για την πρόσβαση στα δημόσια έγγραφα και στοιχεία.
  - Η αποδέσμευση διαβαθμισμένων στρατιωτικών αρχείων απαγορεύεται (Άρθρο 27 του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ), που έχει εκδοθεί σε εκτέλεση του Άρθρου 4§3 του ΝΔ 17/1974 «Περί πολιτικής σχεδιάσεως εκτάκτου ανάγκης»).
  - Αποχαρακτηρισμός της διαβάθμισης του αρχείου μπορεί να γίνει, μόνο για εξαιρετικά σημαντικό λόγο, από τον εκδότη του ή, σε περίπτωση που αυτός δεν υπάρχει πλέον, από τον καθ' ύλην αρμόδιο φορέα του οικείου Επιτελείου, ή με απόφαση επιτροπής.
  - Δεν επιτρέπεται ο υποβιβασμός του αρχείου ούτε μετά την παρέλευση συγκεκριμένου αριθμού ετών, παρόλο που μπορεί μέρος του αρχείου να έχει γίνει ήδη γνωστό από μελέτες ή άλλες εκδόσεις που έχουν δημοσιευθεί.

Τα στρατιωτικά αρχεία του Γενικού Επιτελείου Στρατού, Σχηματισμών, Συγκροτημάτων, Μονάδων, Υπομονάδων, Υπηρεσιών και λοιπών φορέων του Στρατού Ξηράς, όταν συμπληρώνουν τα προβλεπόμενα χρονικά όρια διατήρησής τους ως ενεργά αρχεία, για λόγους ιστορικούς και πληροφόρησης, ή σε έκτακτες περιπτώσεις όπως η διάλυση του φορέα έκδοσής τους, εκκαθαρίζονται και αποστέλλονται στην ΥΣΑ για αρχειοθέτηση, σύμφωνα και με την ισχύουσα νομοθεσία. Η ΥΣΑ παραλαμβάνει τα αρχεία σύμφωνα με τον προγραμματισμό που έχει γίνει και κατόπιν διαταγής του Γενικού Επιτελείου Στρατού (ΓΕΣ) και της Διεύθυνσης Γραμματειακής και Μεταφραστικής Υποστήριξης (ΔΓΜΥ). Στη συνέχεια, προβαίνει σε έλεγχο, διαλογή, ταξινόμηση, καταχώρηση, ευρετηρίαση και τοποθέτηση των

αρχείων σε προσωρινής θέσεις αποθήκευσης. Τα ατομικά έγγραφα του μόνιμου στρατιωτικού και πολιτικού προσωπικού τηρούνται ξεχωριστά.

Μετά την εγγραφή των αρχείων σε μικροφίλμ, τα αρχεία σε φυσική μορφή καταστρέφονται εντός του χώρου της υπηρεσίας (in-house) από το αρμόδιο τμήμα. Έπειτα συλλέγονται από το Τυπογραφείο του Ελληνικού Στρατού (ΤΥΕΣ) για πολτοποίηση.

Για περαιτέρω έρευνα, υλικό όπως νομοθετικές διατάξεις, προεδρικά διατάγματα, στρατιωτικά δελτία, ΦΕΚ και κυβερνητικές οδηγίες σχετικές με την υπηρεσία και τον τρόπο λειτουργίας της, κατά τα έτη λειτουργίας της, παρουσιάζονται παρακάτω:

- Εφημερίς της Κυβερνήσεως του Βασιλείου της Ελλάδος, Τεύχος 1, Φύλλο 109 (6/7/1972)
- Εφημερίς της Κυβερνήσεως του Βασιλείου της Ελλάδος, Τεύχος 1, Φύλλο 217 (8/12/1972)
- Υπουργείο Προγραμματισμού και Κυβερνητικής Πολιτικής, Γενική Διεύθυνση Δημόσιας Διοίκησης, Διεύθυνση Οργάνωσης και Μεθόδων. Θέμα: «Παροχή οδηγιών επί της δια μικροφωτογραφιών τήρησης των αρχείων των δημοσίων υπηρεσιών, ΝΠΔΔ, ΟΤΑ, και της αποδεικτικής αυτών ισχύος» (ΝΔ 1196/1972)
- Νόμος περί Κύρωσης του Κώδικα Διοικητικής Διαδικασίας (Ν.2690/1999)
- Στρατιωτικό δελτίο ΝΔΑ/6: Τρόπος τήρησης, ταξινόμησης, εκκαθάρισης, και μικροφωτογράφισης (εκδ. 30/11/2005)
- Νόμος περί Ψηφιακής Διακυβέρνησης (Ν.4727/2020)

#### **4.1.6 Ψηφιοποίηση**

- Η ψηφιοποίηση γίνεται με χρονολογική σειρά, ανάλογα με το έτος δημιουργίας του κάθε αρχείου, ξεκινώντας από το πιο παλιό και φτάνοντας στο πιο καινούριο, αλλά και ορισμένες φορές βάσει ενδιαφέροντος.
- Η υπάρχουσα διαδικασία προβλέπει σάρωση των αρχείων και εγγραφή των ψηφιοποιημένων αρχείων σε μικροφίλμ. Τα μικροφίλμ λόγω του μικρού όγκου τους μπορούν να χρησιμοποιηθούν για σκοπούς έρευνας καθώς έχουν μεγάλη αντοχή στο χρόνο.

- Μετά τη σάρωση ενός αρχείου γίνεται ποιοτικός έλεγχος στο ψηφιακό αρχείο και εφόσον δεν χρειάζεται κάποια διόρθωση πραγματοποιείται η εγγραφή του στο μικροφίλμ.
- Υπήρξε ένα πρότζεκτ ψηφιοποίησης το οποίο εκπονήθηκε με αξιοποίηση κοινωνικών κονδυλίων ΕΣΠΑ το διάστημα 2012-2014 και μέσα από το έργο αυτό ψηφιοποιήθηκε ένα μέρος του αρχείου που διατηρούσε η υπηρεσία. Ωστόσο, όπως είναι φυσικό από το 2014 μέχρι σήμερα έχει περιέλθει επιπλέον όγκος αρχείων στην κατοχή της υπηρεσίας.
- Λόγω του μεγάλου όγκου των αρχείων, της φύσης των αρχείων (ιστορικά, παλιά) αλλά και του περιεχομένου τους (διαβαθμισμένα), το έργο της ψηφιοποίησης δεν δύναται να ανατεθεί σε εξωτερικό παράγοντα (εταιρεία), Συνεπώς, η διαδικασία προχωράει εντός της υπηρεσίας (in-house) και έτσι είναι φυσικό να χρειαστεί ένα μεγάλο χρονικό διάστημα για να ολοκληρωθεί.
- Η υπηρεσία έχει επενδύσει στο κομμάτι του εξοπλισμού αλλά και στην επάρκεια θέσεων εργασίας και έτσι υπάρχει η δυνατότητα να προχωρήσει η ψηφιοποίηση κάθε είδους αρχείου, ανεξάρτητα από το μέγεθος, την παλαιότητα ή την κατάσταση του. Περισσότερες πληροφορίες σχετικά με τους διαθέσιμους σαρωτές δίνονται παραπάνω.
- Στη διαδικασία της ψηφιοποίησης του υπάρχοντος υλικού, συμμετέχει σε μόνιμη βάση το μόνιμο στρατιωτικό και πολιτικό προσωπικό του τμήματος ψηφιοποίησης.
- Σε περίπτωση που το τμήμα απασχολεί και οπλίτες θητείας, συμμετέχουν και εκείνοι στη διαδικασία από διάφορα πόστα, ανάλογα τις τρέχουσες ανάγκες, και αφού έχουν ολοκληρώσει ένα στάδιο εκπαίδευσης από το μόνιμο προσωπικό του τμήματος.
- Σε κάθε περίπτωση, οι αρμοδιότητες είναι μοιρασμένες οπότε υπάρχει σε μεγάλο βαθμό μια συνεχής ροή στη διαδικασία. Φυσικά όσο καλύτερα στελεχωμένα είναι τα τμήματα τόσο καλύτερο θα είναι και το παραγόμενο προϊόν σε ποσότητα και ποιότητα.
- Η ανάγκη για συνέχεια στη ροή εργασιών, ειδικά στο κομμάτι της ψηφιοποίησης, είναι επιτακτική για τη σταδιακή μετάβαση στην ψηφιακή εποχή. Αυτό βέβαια προϋποθέτει περαιτέρω εκσυγχρονισμό των διαδικασιών και εφάρμογή νέων τεχνολογιών που θα αναβαθμίσουν τις παρεχόμενες υπηρεσίες.

#### 4.1.7 Προτάσεις

##### Οργάνωση/διοίκηση

- Διεξάγηση αλλά και συμμετοχή σε εκπαιδευτικά προγράμματα και σεμινάρια, ανά τακτά χρονικά διαστήματα, εντός ή εκτός των χώρων της υπηρεσίας, με στόχο τη διαρκή επιμόρφωση και κατάρτιση του προσωπικού ως προς τις νέες εξελίξεις που αφορούν εν γένει τον κλάδο των αρχείων και της διαχείρισης τους. Σε αυτό θα βοηθούσε εξίσου η συμμετοχή του προσωπικού σε αντίστοιχες ημερίδες και συνέδρια στην Ελλάδα και το εξωτερικό.
- Παρακολούθηση νομοθετικών αλλαγών, σε τοπικό αλλά και Ευρωπαϊκό επίπεδο, που μπορεί να επηρεάσουν σε μικρό ή μεγάλο βαθμό τη ροή εργασιών της υπηρεσίας (π.χ. GDPR).
- Επιλογή ή θέσπιση ενός ολοκληρωμένου προτύπου διαχείρισης αρχειακού υλικού που θα αφορά όλο τον κύκλο ζωής του αρχείου από τη δημιουργία μέχρι την καταστροφή του (π.χ. US DoD Standard 5015.2) και θα εφαρμόζεται από το σύνολο των οργανισμών άμυνας.
- Απαραίτητη προϋπόθεση είναι η προθυμία για αλλαγή, εξέλιξη και εκσυγχρονισμό από τη μεριά της ηγεσίας αλλά και της πολιτείας και θα αφορά το δημόσιο τομέα στο σύνολο του.

##### Υλικοτεχνικός εξοπλισμός και υποδομές

- Διασφάλιση κατάλληλων συνθηκών αποθήκευσης αρχειακού υλικού σύμφωνα με διεθνή πρότυπα και οδηγίες.
- Ανάπτυξη νέας ιστοσελίδας σύμφωνα με τα σημερινά τεχνολογικά πρότυπα και διαμόρφωση της με γνώμονα τις τρέχουσες ανάγκες της υπηρεσίας.
- Ενσωμάτωση στη νέα ιστοσελίδα επιπλέον λειτουργιών όπως η φόρμα αιτημάτων, η οποία θα διαθέτει συγκεκριμένα και απαραίτητα πεδία που θα πρέπει να συμπληρώσει ο ενδιαφερόμενος ώστε να προχωρήσει στην αποστολή ενός αιτήματος. Η φόρμα αυτή θα διαθέτει και χώρο όπου ο χρήστης θα μπορεί να επισυνάπτει τα απαραίτητα δικαιολογητικά που χρειάζονται για την υποβολή του αιτήματος (π.χ. υπεύθυνη δήλωση με ψηφιακή υπογραφή) και θα μπορεί να

αποτελεί εν δυνάμει τον μοναδικό τρόπο απομακρυσμένης αποστολής αιτημάτων στην υπηρεσία.

#### Προσωπικό

- Αλλαγή της συχνότητας των μεταθέσεων για το στρατιωτικό προσωπικό που εργάζεται στην υπηρεσία. Εφόσον η μονιμοποίηση στελεχών είναι δύσκολο να πραγματοποιηθεί, τότε τα στελέχη μπορούν να παραμένουν για μεγαλύτερο χρονικό διάστημα στην υπηρεσία για να εξασφαλιστεί η μεταφορά της τεχνογνωσίας τους και η μεταλαμπάδευση των γνώσεων τους στους επόμενους. Αυτό το πλάνο θα διασφαλίσει τη συνέχεια της ροής εργασιών.
- Επιλογή στελεχών, πολιτικού προσωπικού αλλά και οπλιτών θητείας με σχετικό εκπαιδευτικό υπόβαθρο/προϋπηρεσία/εξειδίκευση, οι οποίοι θα στελεχώσουν την υπηρεσία και θα είναι σε θέση να υποστηρίξουν και να ανταποκριθούν στα καθήκοντα τους σε σύντομο χρονικό διάστημα, δίχως να χρειάζονται μεγάλη περίοδο προσαρμογής.

#### Document Management System

- Δημιουργία νέου συστήματος διαχείρισης εγγράφων βασισμένο στην τεχνολογία Blockchain, το οποίο θα αξιοποιεί όλα τα οφέλη της τεχνολογίας Blockchain που αναφέρονται στο θεωρητικό μέρος της εργασίας, θα είναι παραμετροποιημένο σύμφωνα με τις ανάγκες και τη ροή εργασιών της υπηρεσίας, θα ενσωματώνει όλο το περιεχόμενο που είναι αποθηκευμένο στο τρέχον σύστημα και θα αποτελεί ουσιαστικά μια αποκεντρωμένη λύση η οποία θα αντικαταστήσει το υπάρχον λογισμικό.
- Φυσικά θα χρειαστεί να προηγηθεί εκπαίδευση και επιμόρφωση του στρατιωτικού και πολιτικού προσωπικού της υπηρεσίας για την ομαλή μετάβαση από το ένα σύστημα στο άλλο. Πρόκειται για μια σύγχρονη λύση διαχείρισης εγγράφων, η οποία θα εισάγει λειτουργίες όπως η αποθήκευση σε cloud περιβάλλον, η ψηφιακή υπογραφή, και η ενσωμάτωση λειτουργίας οπτικής αναγνώρισης χαρακτήρων (OCR) που θα αναπτυχθεί με τη συμβολή των προγραμματιστών του λογισμικού και γλωσσολόγων και θα επιτρέπει την αναζήτηση μέσα στα ψηφιοποιημένα αρχεία.

- Σε μια τέτοια περίπτωση, η υπηρεσία θα φτάσει σε σημείο να διαθέτει ελάχιστο όγκο φυσικού αρχείου, το παραγόμενο αρχείο θα είναι αποκλειστικά πρωτογενώς ψηφιακό και κρυπτογραφημένο.
- Μια λύση σαν και αυτή μπορεί να αποτελέσει σημαντικό εργαλείο για το προσωπικό της υπηρεσίας και με τα διαθέσιμα εργαλεία του να εκσυγχρονίσει τις διαδικασίες και τη ροή εργασιών της υπηρεσίας στο σύνολο της και να αλλάξει ολοκληρωτικά τον τρόπο που αλληλεπιδρά η υπηρεσία όχι μόνο με το κοινό της αλλά και με άλλες υπηρεσίες (π.χ. data.gov.gr) και οργανισμούς (διαλειτουργικότητα).
- Από τη μεριά του χρήστη η πρόσβαση στο σύστημα θα πραγματοποιείται μόνο αν έχει υποβάλλει τα απαραίτητα δικαιολογητικά και έχει λάβει τα κατάλληλα διαπιστευτήρια που θα του δώσουν πρόσβαση στο υλικό που αναζητά.

## Κεφάλαιο 5. Συζήτηση – Συμπεράσματα – Μελλοντικές επεκτάσεις

Παρακάτω παρουσιάζονται συμπεράσματα, προβληματισμοί και προκλήσεις που προέκυψαν μέσα από τη βιβλιογραφική ανασκόπηση και το θεωρητικό μέρος της εργασίας.

### 5.1 Συμπεράσματα

- Σύμφωνα με τους Koch & Pieters (2017), ενώ τα Blockchain έχουν τη δυνατότητα να φέρουν επανάσταση στις συναλλαγές, η κατανόηση των περιορισμών τους είναι ζωτικής σημασίας για τους υπεύθυνους χάραξης πολιτικής και τους χρήστες. Οποιοδήποτε άτομο ή εταιρεία που χρησιμοποιεί μια τεχνολογία Blockchain πρέπει να κατανοήσει πώς κατανέμεται ο τελικός έλεγχος των κόμβων και ποιος θα αποφασίσει την ακρίβεια του καθολικού. Από πολλές απόψεις, οι καινοτόμοι της τεχνολογίας προορίζονται για την αποκέντρωση και τον εκδημοκρατισμό των συναλλαγών, φέρνοντας έτσι επανάσταση στον τρόπο με τον οποίο πραγματοποιούνται οι πληρωμές, ανταλλάσσονται τα περιουσιακά στοιχεία και καταγράφονται οι συμβάσεις.

Η Lemieux (2016a) καταλήγει στα παρακάτω:

- Η τεχνολογία Blockchain, που συχνά περιγράφεται ως παροχή ενός κατανεμημένου και συνεχώς αυξανόμενου αμετάβλητου καθολικού συναλλαγών, είναι μια τεχνολογία τήρησης αρχείων, με την έννοια της αρχειακής επιστήμης του όρου, όσο και μια τεχνολογία μεταφοράς αξίας.
- Πολλές τρέχουσες και προτεινόμενες εφαρμογές της τεχνολογίας Blockchain στοχεύουν στην αντιμετώπιση των προκλήσεων τήρησης αρχείων καθώς προσφέρουν μια νέα μορφή χρήσης, αποθήκευσης ή/και ελέγχου των αρχείων παραγωγής. Για παράδειγμα, το Blockchain στοχεύει να αλλάξει τον τρόπο με τον οποίο διαπιστώνεται η αυθεντικότητα των εγγραφών αλλάζοντας την εξάρτηση από ένα αξιόπιστο τρίτο μέρος σε έναν τρόπο διαπίστωσης αυθεντικότητας που βασίζεται στο σύστημα.



- Οι αξιώσεις που σχετίζονται με τη χρήση της τεχνολογίας Blockchain για τήρηση αρχείων έχουν, σε ορισμένες περιπτώσεις, διαφημιστεί υπερβολικά. Για παράδειγμα, οι λύσεις Blockchain που ισχυρίζονται ότι παρέχουν «αρχειακές» λύσεις όχι μόνο δεν διατηρούν αλλά μπορεί να μην παρέχουν ούτε μακροπρόθεσμη προσβασιμότητα στα αρχεία.
- Φαίνεται να υπάρχει ελάχιστη επίγνωση στην Blockchain κοινότητα σχετικά με τη θεωρία της αρχειακής επιστήμης, αρχές και πρακτικές ή για τις απαιτήσεις και τα πρότυπα τήρησης αρχείων που προκύπτουν από αυτές. Περισσότερη αλληλεπίδραση μεταξύ των κοινοτήτων διαχείρισης αρχείων και Blockchain θα προωθούσε μεγαλύτερη επίγνωση επί του θέματος.
- Παρά το γεγονός ότι η τεχνολογία Blockchain μπορεί να αποτελέσει μια τεχνολογία τήρησης αρχείων και υπάρχουν πολλές νέες νεοφυείς επιχειρήσεις που επικεντρώνονται στη χρήση της τεχνολογίας σε εφαρμογές τήρησης αρχείων, δεν υπάρχει πληθώρα ερευνητικών δεδομένων που να επικεντρώνονται στις επιπτώσεις αυτής της τεχνολογίας στο κομμάτι της τήρησης αρχείων. Οι συνεργασίες μεταξύ ακαδημαϊκής κοινότητας και βιομηχανίας στην εφαρμογή της τεχνολογίας Blockchain στην τήρηση αρχείων, ως επί το πλείστον, απουσιάζουν.
- Καθώς πρόκειται για τεχνολογία τήρησης αρχείων, η μελλοντική ανάπτυξη του Blockchain θα ωφεληθεί από τη θεωρητική και πρακτική γνώση της αρχειακής επιστήμης.
- Η τεχνολογία Blockchain δημιουργεί νέες μορφές αρχείων που πρέπει να αντιμετωπίζονται ως νομικά αποδεικτικά στοιχεία, μαζί με άλλα αρχεία, προκειμένου να ανταποκρίνονται σε επιχειρηματικούς και κοινωνικούς σκοπούς. Αυτό περιλαμβάνει τον καθορισμό του τρόπου με τον οποίο θα αντιμετωπίζονται τα αρχεία Blockchain σύμφωνα με την εκάστοτε νομοθεσία ως προς τα αποδεικτικά στοιχεία, καθώς και τον καλύτερο τρόπο διατήρησης της μακροπρόθεσμης αυθεντικότητας και της προσβασιμότητάς τους ως αποδεικτικών στοιχείων.

- Οι εκτιμήσεις για τον αντίκτυπο της τεχνολογίας Blockchain στη χρηματοπιστωτική σταθερότητα θα πρέπει να διερευνηθούν εάν η ευρεία χρήση της για τήρηση αρχείων θα μπορούσε να αποτελέσει κανάλι μετάδοσης.
- Υπάρχει αυξανόμενη υποστήριξη για την εισαγωγή τεχνικών προτύπων που σχετίζονται με την τεχνολογία Blockchain. Τα πρότυπα που επικεντρώνονται στη χρήση του Blockchain για τήρηση αρχείων μπορεί να βοηθήσουν να διασφαλιστεί ότι οι τεχνολογίες Blockchain ενσωματώνουν υπάρχουσες λύσεις και απαιτήσεις τήρησης αρχείων.

Όπως προκύπτει από τους Staples et al. (2017):

- Οι ρυθμιστικές αρχές και οι επιχειρήσεις θα πρέπει να είναι τεχνολογικά ουδέτερες όσον αφορά τον καθορισμό των κριτηρίων αποδοχής ενός συστήματος στον τομέα τους. Δηλαδή, δεν θα πρέπει να υπάρχει καμία ρύθμιση ή απαγόρευση ειδικά για την τεχνολογία Blockchain, ακόμη και για τα δημόσια Blockchain. Ομοίως, δεν θα πρέπει να υπάρχει απαίτηση για τη χρήση μιας συγκεκριμένης τεχνολογίας που δεν είναι Blockchain.
- Ακόμη και σε μεγάλο μέγεθος βιομηχανίες, τα δημόσια συστήματα Blockchain μπορεί να είναι κατάλληλα για χρήση για ορισμένους περιορισμένους σκοπούς, όπως δημόσιες ανακοινώσεις, κατάλογοι προϊόντων, έλεγχος ενημέρωσης λογισμικού ή πλήρως δημόσια κρατικά μητρώα.
- Οι ρυθμιστικές αρχές και οι επιχειρήσεις θα πρέπει να γνωρίζουν τους τυπικούς τεχνικούς κινδύνους και τους περιορισμούς των τεχνολογιών Blockchain και να δίνουν ιδιαίτερη προσοχή ώστε να διασφαλίζουν ότι οι υποστηρικτές νέων συστημάτων που βασίζονται σε Blockchain παρέχουν επαρκή στοιχεία ότι τα νέα συστήματα πληρούν τις απαιτήσεις που σχετίζονται με αυτούς τους κινδύνους και περιορισμούς.
- Οι ρυθμιστικές αρχές θα πρέπει να παρέχουν ενδεικτική καθοδήγηση σχετικά με τον τρόπο με τον οποίο θα αξιολογήσουν τι συνιστά επαρκή απόδειξη ότι ένα νέο σύστημα πληροί τις κανονιστικές απαιτήσεις.
- Είναι μια πρόκληση και επί του παρόντος είναι άγνωστο το πως θα επιτευχθεί η καλύτερη διακυβέρνηση για Blockchain και συστήματα που βασίζονται σε

Blockchain. Υπάρχει και το ενδεχόμενο να μην υπάρχει κεντρικός ιδιοκτήτης και η πλατφόρμα Blockchain να μπορεί να εξυπηρετεί πολλούς σκοπούς για διαφορετικές ομάδες ενδιαφερομένων οπότε αντίστοιχα αλλάζει και ο τρόπος με τον οποίο οι σχετικοί ενδιαφερόμενοι θα επηρεάσουν και θα διαχειριστούν τις αλλαγές στο λογισμικό και τη λειτουργική υποδομή για τα Blockchain και τα συστήματα που βασίζονται σε Blockchain.

- Οι επιτόπιες δοκιμές συστημάτων που βασίζονται σε Blockchain δεν θα πρέπει απλώς να καταδεικνύουν τη σκοπιμότητα των αισιόδοξων σεναρίων κατά την συνήθη επιτυχημένη χρήση αυτών των συστημάτων, αλλά θα πρέπει επίσης να καταδεικνύουν απαντήσεις στα απαισιόδοξα σενάρια που προκύπτουν τόσο από αναμενόμενα όσο και από απρόβλεπτα προβλήματα στο χρήση αυτών των συστημάτων.
- Τα Blockchain συνήθως συνδυάζονται με άλλα εξαρτήματα σε ένα ευρύτερο σύστημα. Λειτουργικότητα όπως οι διεπαφές χρήστη, η διαχείριση κρυπτογραφικού κλειδιού, η ενσωμάτωση του IoT (Internet of Things), και οι επικοινωνίες με άλλα εξωτερικά συστήματα είναι όλα εγγενώς εκτός αλυσίδας. Πολλές βάσεις δεδομένων είναι καλύτερο να αποθηκεύονται εκτός αλυσίδας, για λόγους επεκτασιμότητας (μεγάλα δεδομένα), λόγους εμπιστευτικότητας (ιδιωτικά δεδομένα) ή για λόγους διαχείρισης βάσεων δεδομένων παλαιού τύπου/τεχνολογίας.
- Τα Blockchain έχουν διαφορετικό μοντέλο κόστους από τις συμβατικές τεχνολογίες. Για τη μεταφορά ψηφιακού νομίσματος, τα Blockchain μπορεί να είναι φθηνότερα από τη συμβατική μεταφορά συναλλάγματος παραστατικού χρήματος. Τα Blockchain έχουν χαμηλή εφάπαξ χρέωση για μόνιμη αποθήκευση μικρών τμημάτων δεδομένων συναλλαγών και συμβάντων. Ωστόσο, τα Blockchain έχουν πολύ υψηλότερο κόστος για την εκτέλεση προγραμμάτων (έξυπνα συμβόλαια) απ' ό,τι μια συμβατική υποδομή (cloud ή εσωτερική).
- Πολλά ιδιωτικά Blockchain μοιράζονται πληροφορίες μεταξύ όλων των συμμετεχόντων κόμβων. Αυτό μπορεί να λειτουργήσει για μια πλήρως ενσωματωμένη λύση, αλλά εάν οι ανταγωνιστές είναι παρόντες στο ίδιο Blockchain, μπορεί να είναι σε θέση να ανακαλύψουν πληροφορίες που

κανονικά διατηρούνται ως εμπορικά εμπιστευτικές. Ορισμένα εναλλακτικά ιδιωτικά Blockchain περιορίζουν την ανταλλαγή πληροφοριών μόνο σε ενδιαφερόμενα μέρη, αλλά αυτά τα Blockchain συνήθως επαναφέρουν μεμονωμένα αξιόπιστα τρίτα μέρη στη λειτουργία του Blockchain.

- Δεν είναι δυνατή η αλλαγή του ιστορικού συναλλαγών στα περισσότερα Blockchain. Αυτό είναι συνήθως καλό, αλλά μπορεί να προκαλέσει προβλήματα εάν το Blockchain περιέχει παράνομο περιεχόμενο ή εάν ένα δικαστήριο διατάξει την αφαίρεση περιεχομένου από το Blockchain.

## 5.2 Προβλήματα

Η Lemieux (2016b) παρουσιάζει τα εξής ζητήματα:

- Έλεγχος του Bitcoin Blockchain: Ένα από τα βασικά ερωτήματα που πρέπει να απαντηθούν σχετικά με το Bitcoin Blockchain σχετίζεται με το ποιος ελέγχει τους κόμβους που είναι συλλογικά σημαντικοί για τη λειτουργία αυτής της τεχνολογίας ως κατανεμημένο δημόσιο καθολικό. Πρόσφατες αναφορές αναφέρουν την ύπαρξη μυστικών μονάδων παραγωγής («ορυχείων») Bitcoin που λειτουργούν στην Κίνα με μια μόνο μονάδα να παράγει 1,5 εκατομμύρια Bitcoin ανά μήνα. Δεδομένου αυτού, είναι σημαντικό να αναρωτηθούμε πόσο πραγματικά αποκεντρωμένο είναι το δημόσιο μητρώο Bitcoin και εάν η συγκέντρωση των κόμβων Bitcoin με τη συνδυασμένη υπολογιστική τους ισχύ θα μπορούσε να επιτρέψει τη συμπαιγνία μεταξύ των κόμβων και να διαβρώσει τη βάση της εμπιστοσύνης πάνω στην οποία βασίζεται το Bitcoin. Επιπλέον, για χώρες που βασίζονται στην αποθήκευση στοιχείων των δημόσιων αρχείων τους σε Bitcoin Blockchain ή οποιοδήποτε Blockchain που δεν λειτουργεί εντός της κυρίαρχης δικαιοδοσίας του, προκύπτουν ερωτήματα σχετικά με το πού βρίσκονται πραγματικά τα δημόσια αρχεία της χώρας, ποιος έχει πρόσβαση σε αυτά τα δεδομένα, και πώς γίνεται η διανομή των δεδομένων της χώρας, καθώς αυτά μπορούν να επηρεάσουν την ικανότητά της να εμπιστεύεται τα δημόσια αρχεία της.

- “Επιθέσεις Man-in-the-Middle”: Κάθε φορά που ένα σύστημα μεταβιβάζει πληροφορίες σε ένα άλλο σύστημα, υπάρχει πιθανότητα για επίθεση Man-in-the-Middle (MitMA). Το MitMA εμφανίζεται όταν ένας εισβολέας παρεμποδίζει κρυφά και πιθανώς αλλάζει την επικοινωνία μεταξύ δύο μερών που πιστεύουν ότι επικοινωνούν απευθείας μεταξύ τους.
- “Επιθέσεις SYN Flood”: Μια επίθεση SYN Flood είναι μια μορφή επίθεσης Denial-of-Service, κατά την οποία ένας εισβολέας στέλνει επαναλαμβανόμενες, γρήγορες αιτήσεις SYN στο σύστημα ενός στόχου σε μια προσπάθεια να καταναλώσει αρκετούς πόρους του διακομιστή ώστε το σύστημα να μην ανταποκρίνεται στη νόμιμη κίνηση. Ένα αίτημα SYN γίνεται όταν ένας διακομιστής ζητά σύνδεση για να επικοινωνήσει με άλλο διακομιστή στέλνοντας ένα μήνυμα SYN (synchronize/συγχρονισμού) στον διακομιστή. Αυτό ακολουθείται από μια διαδικασία αναγνώρισης μεταξύ των δύο διακομιστών. Σε μια επίθεση SYN Flood, ο διακομιστής που λαμβάνει το αίτημα δεν μπορεί να ολοκληρώσει τη διαδικασία αναγνώρισης πριν εμφανιστεί ένα νέο αίτημα, το οποίο τελικά «πλημμυρίζει» τους πόρους του διακομιστή με αιτήματα και τον κάνει να μην ανταποκρίνεται. Αν και το Bitcoin Blockchain έχει εφαρμόσει πολλά μέτρα για την πρόληψη επιθέσεων άρνησης υπηρεσίας (π.χ. επιθέσεις SYN Flood), εξακολουθεί να είναι δύσκολο να αποκλειστούν τέτοιες επιθέσεις, ειδικά σε μια τεχνολογική λύση που βασίζεται σε μεγάλο βαθμό στη μετάδοση των επικοινωνιών μέσω ενός δημόσιου δικτύου.
- “Επίθεση Sybil”. Μια επίθεση Sybil συμβαίνει όταν ένας εισβολέας γεμίζει ένα δίκτυο Blockchain με κόμβους που ελέγχονται από αυτόν, γεγονός που αυξάνει την πιθανότητα σύνδεσης μόνο με κόμβους εισβολέα. Αυτός ο τύπος επίθεσης μπορεί να επιτρέψει σε έναν εισβολέα να αρνηθεί να αναμεταδώσει μπλοκ και συναλλαγές, ακόμη και να αποσυνδέσει μια επικοινωνία εγγραφής εισόδου από το δίκτυο. Μπορεί επίσης να επιτρέψει σε έναν εισβολέα να αναμεταδώσει μόνο μπλοκ που εκείνος δημιουργεί. Η πιθανότητα αυτού του τύπου επίθεσης πιθανότατα αυξάνεται με την αυξανόμενη συγκέντρωση των εξορυκτών Bitcoin.
- Σφάλματα χρονισμού και επιθέσεις: Στο Bitcoin Blockchain, κάθε μεμονωμένο μπλοκ περιέχει μια λίστα συναλλαγών και μια χρονική σήμανση που αντιπροσωπεύει τον κατά προσέγγιση χρόνο δημιουργίας του μπλοκ, μεταξύ άλλων πρόσθετων

πληροφοριών. Οι χρονικές σημάνσεις στο μπλοκ επιτρέπουν στο σύστημα να ρυθμίζει την παραγωγή Bitcoin και να παράγει απόδειξη της χρονολογικής σειράς των συναλλαγών ως προστασία έναντι του προβλήματος της διπλής δαπάνης. Γενικά η χρονοσήμανση διευκολύνει τη διάκριση μιας αυθεντικής εγγραφής έναντι μιας μη αυθεντικής εγγραφής. Οι κόμβοι συνήθως υπολογίζουν τη χρονική σήμανση με βάση τον διάμεσο χρόνο των ομοτίμων ενός κόμβου, ο οποίος αποστέλλεται στο μήνυμα έκδοσης καθώς συνδέονται οι κόμβοι. Δεδομένης της εξάρτησης της τεχνολογίας Blockchain από τις χρονικές σημάνσεις, είναι εξαιρετικά σημαντικό οι μετρητές όλων των κόμβων που παρακολουθούν την ώρα του δικτύου να λειτουργούν σωστά για να αποφευχθούν σφάλματα στη χρονική σφραγίδα. Επιπλέον, ακόμη και όταν οι μετρητές λειτουργούν σωστά, είναι δυνατό για έναν εισβολέα να επιβραδύνει ή να επιταχύνει τον μετρητή χρόνου δικτύου ενός κόμβου πραγματοποιώντας σύνδεση ως πολλαπλοί ομοτίμοι κόμβοι και αναφέροντας ανακριβείς χρονικές σημάνσεις. Παρόμοια με τις επιθέσεις Sybil, η αυξανόμενη συγκέντρωση των εξορύξεων Bitcoin αυξάνει αντίστοιχα την πιθανότητα αυτού του τύπου επίθεσης.

- Διαχείριση κλειδιών: Η διαχείριση κλειδιών είναι απαραίτητη σε ένα σύστημα που βασίζεται στην κρυπτογραφία, όπως το Blockchain. Αυτό περιλαμβάνει τη δημιουργία, την ανταλλαγή, την αποθήκευση, τη χρήση και την αντικατάσταση κλειδιών, κάτι που είναι δύσκολο να επιτευχθεί στην πράξη, επειδή οι χρήστες πρέπει να διασφαλίζουν ότι δυνητικά εκατομμύρια κλειδιά είναι ταυτόχρονα προσβάσιμα, ανθεκτικά στην ψηφιακή κλοπή και στην απώλεια. Τα χαρακτηριστικά της αποτελεσματικής διαχείρισης κλειδιών, συμπεριλαμβανομένης της πολιτικής του συστήματος, της εκπαίδευσης των χρηστών, των οργανωτικών και τμηματικών αλληλεπιδράσεων και του συντονισμού μεταξύ όλων αυτών των στοιχείων, παραμένουν ένα άλυτο πρόβλημα. Η πολυπλοκότητα της διαχείρισης κλειδιών καθιστά τα ιδιωτικά κλειδιά, όπως αυτά που δημιουργήθηκαν για την υποστήριξη της λειτουργίας των συστημάτων Blockchain σαν το Factom και το Bitcoin, ευάλωτα σε απώλεια ή κλοπή. Για παράδειγμα, το λογισμικό Bitcoin διαχειρίζεται πολλά ιδιωτικά κλειδιά αποθηκευοντάς τα στον τοπικό αποθηκευτικό χώρο του κόμβου μέσα σε ένα αρχείο ή σε μια βάση δεδομένων εντός μιας προρυθμισμένης διαδρομής συστήματος αρχείων. Ένα αρχείο που περιέχει ιδιωτικά κλειδιά μπορεί να διαβαστεί

από οποιαδήποτε εφαρμογή που έχει πρόσβαση στον φάκελο εφαρμογών του χρήστη. Οι «εισβολείς» μπορούν να το εκμεταλλευτούν για να αποκτήσουν άμεση πρόσβαση στα αρχεία συναλλαγών οπότε οι χρήστες πρέπει να είναι προσεκτικοί ώστε να μην μοιράζονται ακούσια τον φάκελο της εφαρμογής Bitcoin (π.χ. μέσω δικτύων κοινής χρήσης αρχείων peer-to-peer, αντιγράφων ασφαλείας εκτός τοποθεσίας ή σε κοινόχρηστη μονάδα δίσκου) και πρέπει επίσης να είναι προσεκτικοί για να αποφύγουν την πιθανότητα φυσικής κλοπής κατά τη χρήση φορητών υπολογιστών ή κινητών τηλεφώνων. Μια άλλη απειλή είναι η απώλεια κλειδιών ως αποτέλεσμα γενικής αστοχίας εξοπλισμού εξαιτίας φυσικών καταστροφών, ηλεκτρικών βλαβών, πολεμικών ενεργειών ή εσφαλμένης διαγραφής (π.χ. μορφοποίηση λάθος μονάδας δίσκου ή διαγραφή λάθος φακέλου).

- Μακροχρόνια ψηφιακή διατήρηση:

- Διατήρηση και διαθεσιμότητα αρχικών αρχείων: Δεδομένου ότι η ψηφιακά υπογεγραμμένη έκδοση στο Bitcoin Blockchain δεν μπορεί να αντιστραφεί για να δημιουργήσει ένα αντίγραφο της αρχικής εγγραφής, τα πρωτότυπα πρέπει πάντα να διατηρούνται έτσι ώστε να μπορούν να κατακερματιστούν εκ νέου και να υπογραφούν ψηφιακά για λόγους σύγκρισης. Γενικά το επίπεδο οργάνωσης και επένδυσης που απαιτείται για τη διατήρηση των πρωτοτύπων δεν είναι αμελητέο, που περιλαμβάνει, σύμφωνα με το ISO 14721, τη δημιουργία ενός αξιόπιστου ψηφιακού αποθετηρίου και πρόσθετων στοιχείων όπως η τεχνική, η πολιτική και η θεσμική ικανότητα για απορρόφηση αρχείων, αποθήκευση αρχείων, διαχείριση δεδομένων, πρόσβαση, διάδοση και μετάβαση σε νέα μέσα και φόρμες.
- Ψηφιακές υπογραφές: Τόσο η λύση Factom όσο και η τεχνολογία Blockchain γενικά αλλά και η περίπτωση του Bitcoin Blockchain ειδικά, βασίζονται στη χρήση ψηφιακών υπογραφών, οι οποίες συνδυάζουν μια σύνοψη μηνύματος κατακερματισμού με κρυπτογράφηση. Καθώς η κρυπτογράφηση βασίζεται στη διαχείριση κλειδιών, η αποθήκευση ιδιωτικών κλειδιών για μεγάλο χρονικό διάστημα, όπως απαιτείται από το Factom και το Bitcoin Blockchain, απαιτεί από τους χρήστες να διατηρούν επίσης μια προδιαγραφή της μορφής αρχείου για να διασφαλίσουν ότι τα κλειδιά μπορούν να συνεχίσουν

να είναι αναγνώσιμα. Μια πρόσθετη πρόκληση αποτελεί το ότι, με την πάροδο του χρόνου, η αρχικά μικρή πιθανότητα για δύο διαφορετικές εγγραφές να παράγουν την ίδια σύνοψη μηνυμάτων (το φαινόμενο αυτό ονομάζεται σύγκρουση) αυξάνεται φυσικά. Εν τέλει, είναι σημαντικό το ότι ώθηση πίσω από τη χρήση της τεχνολογίας Blockchain αποτελεί η πρόληψη της απάτης, όπου με την πάροδο του χρόνου οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται για τη δημιουργία των συνοπτικών μηνυμάτων που χρησιμοποιούνται στις ψηφιακές υπογραφές μπορούν βέβαια να γίνουν ευάλωτοι. Στο παρελθόν, έχουν υπάρξει περιπτώσεις παραβίασης ευρέως χρησιμοποιούμενων αλγορίθμων ενώ και η ξεπερασμένη τεχνολογία της κρυπτογραφίας που βασίζεται στις ψηφιακές υπογραφές είναι επίσης ένα ζήτημα. Παράλληλα, ένα σύστημα ψηφιακής διατήρησης που πραγματοποιεί ελέγχους σε σχέση με προηγούμενες αναλύσεις μηνυμάτων πρέπει προληπτικά να αντικαταστήσει τον αλγόριθμο σύνοψής του με έναν νέο προτού ο τρέχων αλγόριθμος ξεπεραστεί ή σταματήσει να λειτουργεί λόγω σφάλματος. Για να γίνει αυτό, θα πρέπει να πραγματοποιήσει έλεγχο σε σχέση με την τρέχουσα σύνοψη για να επιβεβαιώσει ότι το στοιχείο είναι ακόμα λειτουργικό και στη συνέχεια να υπολογίσει μια σύνοψη χρησιμοποιώντας τον αλγόριθμο αντικατάστασης. Αυτό θα μπορούσε να προσαρτηθεί στην αποθηκευμένη λίστα αναλύσεων για το συγκεκριμένο αντικείμενο. Ωστόσο, εάν πρόκειται να ακολουθηθεί αυτή η διαδικασία, θα απαιτούσε ένα έμπιστο τρίτο μέρος για να την πραγματοποιήσει (πράγμα που ακυρώνει τον σκοπό της χρήσης μιας λύσης Blockchain) και, επιπλέον, αυξάνει την πιθανότητα αμφισβήτησης ως προς την αυθεντικότητα και την ακεραιότητα της νέας σύνοψης ως βάση για την επικύρωση των αρχικών εγγραφών. Αυτό το τελευταίο ζήτημα θα έπρεπε πιθανότατα να επιλυθεί σε δικαστήριο, το οποίο, με τη σειρά του, απαιτεί ένα νομικό σύστημα ικανό να λαμβάνει τέτοιους προσδιορισμούς.



Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά τα ζητήματα που έθιξε η Lemieux (2016b):

**Πίνακας 7: Σύνοψη περιορισμών και ρίσκων ενός Blockchain συστήματος (Lemieux, 2016b)**

<b>Απειλή/Ευπάθεια</b>	<b>Επίπτωση</b>	<b>Πιθανότητα</b>	<b>Κίνδυνος</b>
Έλεγχος του Blockchain	Απώλεια ελέγχου των κόμβων που επικυρώνουν τις συναλλαγές, οδηγώντας στην αποθήκευση μη αυθεντικών αρχείων στο Blockchain	Χαμηλή-μέτρια, αλλά θα αυξηθεί με τη συγκέντρωση του ελέγχου	Αυθεντικότητα
Έλεγχος δημιουργίας αρχείων εκτός του Blockchain περιβάλλοντος	Μπορεί να αποθηκευτούν αναξιόπιστα αρχεία στο Blockchain	Μέτρια-υψηλή	Αξιοπιστία
Επίθεση Man-in-the-Middle	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Υψηλή	Αυθεντικότητα
Επίθεση SYN Flood	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Μέτρια	Αυθεντικότητα
Επίθεση Sybil	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Μέτρια	Αυθεντικότητα
Λάθη χρονισμού	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Μέτρια	Αυθεντικότητα
Διαχείριση κλειδιών	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Μέτρια-υψηλή	Αυθεντικότητα

Επίθεση διακομιστή ελέγχου (Factom-specific)	Μπορεί να αποθηκευτούν μη αυθεντικά αρχεία στο Blockchain	Μέτρια	Αυθεντικότητα
Διατήρηση αρχικών αρχείων (απαιτείται για την επικύρωση όλων των συναλλαγών)	Αδυναμία επικύρωσης συναλλαγών λόγω αδυναμίας σύγκρισης του αρχικού hash με το hash στο Blockchain	Υψηλή	Αυθεντικότητα
Bit rot	Αδυναμία σύγκρισης του αρχικού hash με το hash στο Blockchain	Υψηλή	Αυθεντικότητα
Αλλαγή στον αλγόριθμο κρυπτογράφησης ή στον τρόπο με τον οποίο δημιουργείται το hash	Αδυναμία σύγκρισης του αρχικού hash με το hash στο Blockchain	Υψηλή	Αυθεντικότητα
Σύγκρουση μεταξύ hash	Αδυναμία επικύρωσης της συναλλαγής με βάση τη μοναδική ταυτότητα του πρωτοτύπου	Χαμηλή-μέτρια	Αυθεντικότητα
Παραβίαση κωδικού κρυπτογράφησης	Αδυναμία διασφάλισης της ακεραιότητας του Blockchain	Χαμηλή-μέτρια	Αυθεντικότητα

Περαιτέρω στοιχεία αναφέρονται από την (Lemieux, 2016a) ως προς τα εξής ζητήματα:

- Κενά γνώσης: Λίγοι επαγγελματίες διαχείρισης αρχείων γνωρίζουν πολλά για την τεχνολογία Blockchain και τους πιθανούς τομείς εφαρμογής και χρήσης της. Χρειάζεται να γίνει προσπάθεια ώστε να ενημερωθούν αυτοί οι επαγγελματίες πάνω σε μια τεχνολογία που έχει τη δυνατότητα να αλλάξει ριζικά τον τύπο των αρχείων που διαχειρίζονται και διατηρούν και τα συστήματα και τις διαδικασίες που

χρησιμοποιούν για να υποστηρίξουν την εργασία τους. Δημιουργικές και καινοτόμες, όπως είναι οι πολλές προτεινόμενες χρήσεις του Blockchain για τήρηση αρχείων, παρατηρήθηκε επίσης ένα σημαντικό κενό στη γνώση εντός της κοινότητας του Blockchain σχετικά με τις αρχειακές θεωρίες, αρχές, πρακτικές και πρότυπα που σχετίζονται με τη δημιουργία, τη διαχείριση και τη διατήρηση αυθεντικών αρχείων. Δεδομένου ότι η τήρηση αρχείων που βασίζεται σε Blockchain δημιουργεί νέα είδη αρχείων και νέες προκλήσεις για τη διαχείριση τέτοιων αρχείων καθ' όλη τη διάρκεια του κύκλου ζωής τους, η αποτυχία αντιμετώπισης αυτού του κενού γνώσης θα μπορούσε να οδηγήσει, στην καλύτερη περίπτωση, σε μια ανακεφαλαίωση των ήδη γνωστών και, στη χειρότερη περίπτωση, σε ακούσιες συνέπειες που με τη σειρά τους θα δημιουργήσουν νέους κινδύνους. Η τεχνολογία Blockchain θα μπορούσε να οδηγήσει σε πολλές αλλαγές στην τήρηση αρχείων, συμπεριλαμβανομένης της «χρηματοοικονομικής» της τήρησης αρχείων, πράγμα που μπορεί να οδηγήσει στην απαίτηση πληρωμής εξορυκτών Blockchain για να εργαστούν πάνω στην επικύρωση συναλλαγών, σε υψηλότερα επίπεδα αποκέντρωσης στη δημιουργία και τήρηση αρχείων συγκριτικά με παλιότερα, (π.χ. τα αρχεία και η τήρηση αρχείων κατανέμονται σε πολλά διαφορετικά συστήματα και τοποθεσίες), σε έναν κατακεκομμένο συναινετικό τρόπο δημιουργίας εμπιστοσύνης που διαφέρει από την παραδοσιακή προσέγγιση της στήριξης σε αξιόπιστα τρίτα μέρη και σε ορισμένα πλαίσια, σε διαχωρισμό της ψηφιακής υπογραφής από τα αρχικά αρχεία (ή πιθανόν και τα συστήματα τήρησης αρχείων), ως προς τα αρχεία που αποθηκεύονται εκτός αλυσίδας. Υπάρχουν αναμφίβολα και άλλες διαφορές, αλλά δεδομένης της τρέχουσας κατάστασης στο κομμάτι των γνώσεων, δεν έχουν ακόμη προσδιοριστεί πλήρως.

Έπειτα, από τα Vermont State Archives (2019) προβάλλονται τα παρακάτω θέματα:

- Μοντέλο ιδιοκτησίας δεδομένων σε Blockchain: Δεδομένου ότι τα περισσότερα Blockchain είναι εγγενώς αναξιόπιστα, δηλαδή δεν υπάρχει υπεύθυνο μέρος που θα είναι υπεύθυνο για τη διατήρηση των αρχείων Blockchain. Αν και μπορεί να είναι δύσκολο να δημιουργηθεί ένα αρχείο Blockchain, υπάρχει πιθανότητα να χαθούν τα αρχεία των παλαιών μπλοκ και θα ήταν πιθανότατα εξαιρετικά δύσκολο να γίνει επαναφορά των χαμένων μπλοκ (ένα μπλοκ που είναι εύκολο να ξαναχτιστεί είναι

πιθανώς εύκολο να πλαστογραφηθεί), οπότε υπάρχει πιθανότητα να χαθούν εντελώς. Πολλοί τεχνικοί πάνω στα Blockchain ισχυρίζονται ότι οι μεγαλύτερες αλυσίδες αντιγράφονται σε αρκετά σημεία ώστε αυτό να είναι απίθανο, αλλά ο πολλαπλασιασμός δεν υποκαθιστά τη διατήρηση. Όλα τα ψηφιακά δεδομένα υποβαθμίζονται με την πάροδο του χρόνου επομένως η μακροπρόθεσμη διατήρηση δεδομένων απαιτεί αφοσίωση, δέσμευση καθώς και τεχνική εμπειρογνομosύνη. Η λογοδοσία, ή αλλιώς ανάληψη ευθυνών, είναι ένας βασικός παράγοντας στη διακυβέρνηση των πληροφοριών, και χωρίς κανένα υπεύθυνο μέρος υπάρχει μεγάλος κίνδυνος ως προς τη μακροπρόθεσμη βιωσιμότητα.

- Υποβολή συναλλαγών ανώνυμα: Η δυνατότητα ανώνυμης υποβολής συναλλαγών σε Blockchain θα μπορούσε να αποτελέσει σημαντική πρόκληση για τη διασφάλιση της αυθεντικότητας των αρχείων. Μία από τις βασικές πτυχές για την αξιολόγηση της αυθεντικότητας ενός αρχείου είναι η αναγνώριση και η επιβεβαίωση των εκπροσώπων (συνήθως άτομα ή οργανισμοί) που εμπλέκονται στη δημιουργία του. Με δεδομένο ότι πολλά Blockchain επιτρέπουν την ανώνυμη υποβολή, θα ήταν απαραίτητες πρόσθετες δικλείδες προστασίας για να διασφαλιστεί ότι οι δημόσιοι υπάλληλοι ενεργούσαν υπό την επίσημη ιδιότητά τους κατά την υποβολή αρχείων στο δίκτυο που θα επαληθευθούν και θα καταγραφούν στο Blockchain. Και αν υποβάλλονταν μη αυθεντικά αρχεία αλλά ήταν καλά διαμορφωμένα, πιθανότατα θα ήταν πολύ δαπανηρό να αναστραφούν ή να αφαιρεθούν λανθασμένες συναλλαγές που δεν ανακαλύφθηκαν αμέσως.
- Επαλήθευση συναλλαγών: Δεν είναι σαφές τι μέρος του Blockchain θα πρέπει να διατηρηθεί για να ικανοποιηθεί μια νομική βάση εγκυρότητας. Τα Merkle Tree παρέχουν στους χρήστες τη δυνατότητα να επαληθεύουν τις συναλλαγές μέσα σε μπλοκ ή τμήματα μπλοκ χωρίς να χρειάζεται ολόκληρη η αλυσίδα, αλλά δεν υπάρχει σαφές πρότυπο για τον καθορισμό της εγκυρότητας ή της αξιοπιστίας ενός Blockchain στο σύνολό του. Σε μια τυπική νομική διαδικασία, μπορεί να ζητηθεί η επικύρωση ενός αρχείου που παρουσιάζεται και έτσι η μαρτυρία ενός υπαλλήλου μπορεί να βοηθήσει στον καθορισμό της γνησιότητας ενός αρχείου. Ενώ τα Blockchain μπορεί να είναι εσωτερικά συνεπή, θα πρέπει ακόμα να υπάρχει ένας εκπρόσωπος που να δημιουργεί τη σχέση μεταξύ της εγγραφής και του Blockchain.

- Μετατροπή εγγραφών Blockchain: Παρόλο που ορισμένες δημόσιες εγγραφές σε ηλεκτρονική μορφή μπορούν να μετατραπούν σε αναλογική μορφή, μέσω εκτύπωσης ή αναπαραγωγής, δεν είναι εύκολα κατανοητός ο τρόπος με τον οποίο οι εγγραφές Blockchain μπορούν να μετατραπούν σε διαφορετικές μορφές. Η απλή εκτύπωση των δεδομένων από ένα Blockchain είναι κάπως παρόμοια με την εκτύπωση μιας ηλεκτρονικής υπογραφής. Αυτό που έχει μικρότερη σημασία είναι το περιεχόμενο της εγγραφής (καθώς είναι ως επί το πλείστον κρυπτογραφικά hashes και άλλα μεταδεδομένα μη αναγνώσιμα από τον άνθρωπο) παρά η δυνατότητα εντοπισμού της εγκυρότητας της εγγραφής. Αυτό θα πρέπει να πραγματοποιηθεί πλήρως σε ηλεκτρονικό περιβάλλον, και για να γίνει δεκτό ένα αντίγραφο μιας εγγραφής ως αποδεικτικό στοιχείο, ακόμη και η παραμικρή αλλαγή (με τυχαία ή σκόπιμα μέσα) θα δημιουργούσε πρόβλημα.
- Εξάρτηση από δίκτυα και πρωτόκολλα: Συμβαίνει ακόμα και σε μεγάλες εταιρείες το φαινόμενο των «εχθρικών εξαγορών», με την απόκτηση μεγάλου πακέτου μετοχών. Όσο η τεχνολογία συνεχίζει να βελτιώνεται, είναι αδύνατο να αποκλειστεί εντελώς ένα αντίστοιχο γεγονός σε ένα δίκτυο Blockchain, ειδικά όσο αναπτύσσονται περαιτέρω τεχνολογίες όπως οι κβαντικοί υπολογιστές και η μηχανική μάθηση. Τα Blockchain εξαρτώνται εγγενώς από τα δίκτυα και τα πρωτόκολλα που ορίζουν τις παραμέτρους της λειτουργίας τους. Εάν αυτά τα πρωτόκολλα και τα δίκτυα μπορούν να ελεγχθούν, η ακεραιότητα του ίδιου του Blockchain θα μπορούσε να τεθεί υπό αμφισβήτηση.
- Αναγνωσιμότητα από τον άνθρωπο: Τελικά, οι πληροφορίες που περιέχονται σε Blockchain δεν είναι εγγενώς αναγνώσιμες από τον άνθρωπο. Φυσικά, αυτό ισχύει για τις περισσότερες ηλεκτρονικές πληροφορίες, αλλά επειδή τα μπλοκ και οι συναλλαγές είναι εγγενώς κρυπτογραφημένα, υπάρχει ένα επιπλέον επίπεδο αφαιρετικότητας. Οι κατακερματισμοί είναι αναπαραστάσεις άλλων εγγραφών που έχουν εκτελεστεί μέσω ενός μαθηματικού αλγόριθμου, δηλαδή απλή αναπαράσταση πληροφοριών που είναι αποθηκευμένες κάπου αλλού. Από την άποψη της τήρησης αρχείων, η αποθήκευση δύο εγγενώς συνδεδεμένων τμημάτων πληροφοριών (αυτή είναι η αρχική εγγραφή και ο κατακερματισμός της) σε διαφορετικά συστήματα μπορεί να είναι ευεργετική, αλλά συχνά διασπά το πλαίσιο της αρχικής εγγραφής,

βλάπτοντας την αυθεντικότητά της. Ένα από τα οφέλη των Blockchain είναι η αμεταβλητότητα(σταθερότητα) τους καθώς ένα καταμεμημένο καθολικό που τηρείται σε δεκάδες μέρη είναι απίθανο να παραβιαστεί, επομένως οποιοδήποτε έγγραφο μπορεί να κατακερματιστεί και να συγκριθεί με μια εγγραφή εντός του Blockchain για να επαληθευτεί η εγκυρότητα του. Αν όμως αυτό το αρχικό έγγραφο χαθεί ή ο σύνδεσμος λείπει, θα ήταν δυνητικά πολύ δύσκολο να ξαναδημιουργηθεί αυτό το πλαίσιο.

- Βιωσιμότητα: Η μακροπρόθεσμη βιωσιμότητα των τρεχόντων μοντέλων Blockchain είναι στην καλύτερη περίπτωση αμφισβητήσιμη. Δεν υπάρχει ακόμη καμία μακροπρόθεσμη μελέτη βιωσιμότητας της τεχνολογίας ή της υποδομής του Blockchain. Το τρέχον μοντέλο του μεγαλύτερου Blockchain στον κόσμο, του Bitcoin, διατηρείται μέσω της εθελοντικής συμμετοχής. Δηλαδή, κάθε κόμβος στο δίκτυο συμβάλλει οικειοθελώς στην επαλήθευση συναλλαγών και αποζημιώνεται για αυτή τη συμμετοχή μέσω της ανακάλυψης νέων νομισμάτων. Δεδομένου ότι τα νομίσματα έχουν αξία, αυτό είναι μέρος του δίκαιου εμπορίου καθώς το κόστος του εξοπλισμού και της ισχύος που απαιτούνται για τους απαραίτητους υπολογισμούς είναι μικρότερα από την ανταμοιβή για αυτήν τη διεργασία, οπότε μπορεί να επιτευχθεί κέρδος και η εθελοντική συμμετοχή είναι αποτελεσματική.
- Πιθανότητα αποτυχίας: Η πλήρης αποτυχία του δικτύου φαίνεται απίστευτα απίθανη, αλλά η μείωση του αριθμού των φορέων αποτελεί επίσης μια απειλή. Με δεδομένο ότι τα πρωτόκολλα συναίνεσης υπαγορεύουν τη δημιουργία νέων μπλοκ, η σύλληψη ενός σημαντικού τμήματος του δικτύου θα μπορούσε να επιτρέψει την ανάληψη του ελέγχου αυτής της συναίνεσης, η οποία πιθανότατα θα έχει ως αποτέλεσμα τον κατακερματισμό των Blockchain μέσω διακλάδωσης, ή χειρότερα, μέσω της απώλειας εμπιστοσύνης στην ίδια την αλυσίδα. Ομοίως, η αποτυχία της υποδομής του δικτύου όχι μόνο θα επηρέαζε την ικανότητα της αλυσίδας να συνεχίσει να αναπτύσσεται μέσω της προσθήκης νέων συναλλαγών, αλλά θα έθετε επίσης υπό αμφισβήτηση τη διατήρηση των προηγούμενων μπλοκ. Λόγω των δυνατοτήτων που παρέχονται από τις Merkle Roots, η ακεραιότητα μεμονωμένων μπλοκ ή ακόμα και ομάδων μπλοκ μπορεί να διατηρηθεί μεμονωμένα, αλλά η πραγματική ψηφιακή διατήρηση και αποθήκευση τέτοιων μπλοκ θα τεθεί υπό

αμφισβήτηση. Για να διασφαλιστεί η μακροπρόθεσμη βιωσιμότητα των αρχείων που περιέχουν δεδομένα δακτυλικών αποτυπωμάτων ή είναι αποθηκευμένα σε ένα Blockchain, ένας σημαντικός αριθμός φορέων εντός του δικτύου πιθανότατα θα χρειαστεί να δεσμευτεί για την αποθήκευση μπλοκ, για όσο χρονικό διάστημα χρειάζεται. Σε ένα δημόσιο Blockchain όπως το Bitcoin, τέτοιες εγγυήσεις φαίνονται απίθανες αλλά όχι αδύνατες. Ίσως σε ιδιωτικά Blockchain, των οποίων τα δίκτυα αποτελούνται αποκλειστικά από φορείς που μπορούν να εμπιστευτούν οι ίδιοι και που μπορούν να συνάψουν συμφωνίες συνεργασίας (π.χ. δίκτυα κρατικών αρχείων ή βιβλιοθηκών), θα μπορούσαν να εξεταστούν για επ' αόριστον διατήρηση. Ίσως ομάδες κυβερνήσεων, όπως τα κράτη ή οι δήμοι, θα μπορούσαν να συμπράξουν και να συνεισφέρουν συνεργατικά πόρους σε ένα πραγματικά δημόσια ελεγχόμενο Blockchain που ανταποκρίνεται στις απαιτήσεις λογοδοσίας και τήρησης αρχείων ώστε να ικανοποιήσει τις δημόσιες ανάγκες.

Η National Archives and Records Administration (NARA) (2019) αναφέρει με τη σειρά της ορισμένους προβληματισμούς σχετικά με τη μεταφορά των εγγραφών προς κρατικές αρχειακές υπηρεσίες. Η μεταφορά αρχείων Blockchain στα Εθνικά Αρχεία είναι μια εντελώς θεωρητική συζήτηση, σε αυτό το σημείο. Καμία εγγραφή Blockchain δεν έχει προγραμματιστεί ακόμη ως μόνιμη εγγραφή. Πρέπει όμως να διερευνηθούν παράγοντες όπως:

- τι είδους πόροι, ειδικοί ή όχι, απαιτούνται για την αρχειοθέτηση εγγραφών Blockchain, όπως δεξιότητες διαχείρισης κόμβων/δικτύων
- κατά πόσο και σε τι βαθμό έχει πρόσβαση η αρχειακή υπηρεσία σε διάφορα μορφότυπα εγγραφών σε Blockchain περιβάλλον, εφόσον υπάρχει ποικιλομορφία ως προς τον τύπο των εγγραφών εντός των μπλοκ, οι οποίες συσσωρεύονται από πολλαπλές συναλλαγές
- ο τρόπος διαχείρισης, συντήρησης και παροχής πρόσβασης, από τη μεριά της αρχειακής υπηρεσίας, σε Blockchain που περιέχουν κρυπτογραφικά μη προσβάσιμα μέρη. Τα μπλοκ δεν ήταν δυνατό να αφαιρεθούν επειδή αυτό θα ακύρωνε το βασικό σκοπό του Blockchain, αλλά είναι πιθανό να μην είναι προσβάσιμα λόγω του τρόπου με τον οποίο θεσπίστηκαν οι κανόνες του Blockchain.

- σε περίπτωση που υπάρχουν πολλές υπηρεσίες εντός του δικτύου Blockchain, η καθεμία με τον δικό της κόμβο, θα πρέπει να καθοριστεί αν θα υπάρχει κάποιος μοναδικός υπεύθυνος (άτομο/υπηρεσία ή ο εκάστοτε ιδιοκτήτης) για τη μεταφορά των εγγραφών ή των δεδομένων συναλλαγών. Το Blockchain είναι κυριολεκτικά ακριβώς το ίδιο για κάθε οργανισμό.
- αν η ίδια η αρχειακή υπηρεσία γίνει η ίδια κόμβος, τότε η φυσική μεταφορά των εγγραφών Blockchain δεν αποκτήσει δευτερεύουσα σημασία και ίσως να μην χρειαστεί καν η νόμιμη μεταφορά των αρχείων Blockchain, εφόσον η αρχειακή υπηρεσία αποτελεί ήδη μέρος του Blockchain.

### 5.3 Προκλήσεις

Στη διεθνή βιβλιογραφία αναφέρονται επίσης ένας αριθμός προκλήσεων που προκύπτουν μέσα από την αξιοποίηση της τεχνολογίας Blockchain, ορισμένες εκ των οποίων παρουσιάζονται παρακάτω:

- Αποκέντρωση: Σύμφωνα με τη National Archives and Records Administration (NARA) (2019), τα τρέχοντα μοντέλα διαχείρισης αρχείων βασίζονται σε μια κεντρική συλλογή ηλεκτρονικών αρχείων που δημιουργούνται και διατηρούνται μέσα στις δομές και τα συστήματα ενός οργανισμού. Το Blockchain μεταθέτει την ευθύνη και την εμπιστοσύνη για τη διατήρηση ηλεκτρονικών αρχείων από τις δομές και τα συστήματα του οργανισμού σε ένα κατακεκομμένο δίκτυο. Αυτό αντιπροσωπεύει μια αλλαγή στο ρόλο των κεντρικών συστημάτων και εργαλείων διαχείρισης αρχείων, μια στροφή στο ίδιο το Blockchain που διασφαλίζει εκείνο την εγκυρότητα και την εμπιστοσύνη, αντί για τα συστήματα διαχείρισης αρχείων. Γενικότερα, αυτή η μετάβαση από ένα κεντρικό μοντέλο εμπιστοσύνης σε ένα μοντέλο που βασίζεται σε δίκτυο εφαρμόζεται ευρέως σε διάφορους τεχνολογικούς τομείς. Αυτή η μετατόπιση μπορεί να επηρεάσει τον τρόπο με τον οποίο οργανώνονται, κατατάσσονται και διατηρούνται τα αρχεία με την πάροδο του χρόνου, κάτι που με τη σειρά του θα επηρεάσει τον τρόπο συλλογής αρχείων, την εφαρμογή ελέγχων ως προς την



πρόσβαση και την πνευματική ιδιοκτησία και την εκτέλεση κανόνων απόρριψης, από τη μεριά των διαχειριστών αρχείων.

- Συνεχίζοντας πάνω στο ζήτημα της αποκέντρωσης, οι Bhatia et al. (2020) προσθέτουν ότι ορισμένοι οργανισμοί χρησιμοποιούν συστήματα διαχείρισης περιεχομένου για τον εντοπισμό, την προσθήκη ετικετών και τη διαχείριση συλλογών φωτογραφιών. Άλλοι οργανισμοί ενδέχεται να χρησιμοποιούν το Microsoft Office 365 για την άμεση διαχείριση ηλεκτρονικών αρχείων που δημιουργούνται με τη χρήση εφαρμογών σε υπολογιστικό περιβάλλον. Σε κάθε περίπτωση, είτε πρόκειται για τεχνολογία (π.χ. διαδίκτυο), είτε για τον τρόπο επικοινωνίας μας (π.χ. εφαρμογές κοινωνικής δικτύωσης), τα δίκτυα γίνονται πλέον πρωταρχική αρχή οργάνωσης.

Οι Kikitamara et al. (2017) με τη σειρά τους αναδεικνύουν τις εξής προκλήσεις:

- Απόδοση: Όταν μια συναλλαγή υποβάλλεται σε επεξεργασία, ένα Blockchain πρέπει να εκτελεί τις ίδιες εργασίες που κάνει μια κανονική βάση δεδομένων, με 3 επιπλέον λειτουργίες:
  1. Επαλήθευση υπογραφής: Κάθε συναλλαγή Blockchain πρέπει να υπογράφεται ψηφιακά με τη χρήση ενός δημόσιου/ιδιωτικού σχήματος κρυπτογράφησης. Η δημιουργία και η επαλήθευση αυτών των υπογραφών είναι υπολογιστικά περίπλοκη. Αντίθετα, στις κεντρικές βάσεις δεδομένων, αφού δημιουργηθεί μια σύνδεση, μετά δεν χρειάζεται η μεμονωμένη επαλήθευση κάθε εισερχόμενου αιτήματος.
  2. Μηχανισμοί συναίνεσης: Σε μια κατανεμημένη βάση δεδομένων, όπως ένα Blockchain, πρέπει να καταβληθεί προσπάθεια για να διασφαλιστεί ότι θα επιτευχθεί συναίνεση από τους κόμβους του δικτύου. Ανάλογα με τον μηχανισμό συναίνεσης, αυτό μπορεί να περιλαμβάνει επικοινωνία μεταξύ των 2 πλευρών ή/και αντιμετώπιση των forks και των επακόλουθων ανατροπών τους. Παρόλο που αποτελεί αρμοδιότητα των κεντρικών βάσεων δεδομένων να αντιμετωπίζουν αντικρουόμενες και ματαιωμένες συναλλαγές, αυτές είναι πολύ λιγότερο πιθανές όταν οι συναλλαγές βρίσκονται στην ουρά και υποβάλλονται σε επεξεργασία σε μία μόνο τοποθεσία.

3. Πλεονασμός: Δεν πρόκειται για την απόδοση ενός μεμονωμένου κόμβου, αλλά για το συνολικό ποσό υπολογισμού που απαιτεί ένα Blockchain. Ενώ οι κεντρικές βάσεις δεδομένων επεξεργάζονται συναλλαγές 1-2 φορές, σε ένα Blockchain οι συναλλαγές πρέπει να επεξεργάζονται ανεξάρτητα από κάθε κόμβο του δικτύου, πράγμα που σημαίνει ότι γίνεται πολύ περισσότερη δουλειά για να επιτευχθεί το ίδιο τελικό αποτέλεσμα.
- Επεκτασιμότητα: Σε δημόσια Blockchain, η επεκτασιμότητα είναι ένα σημαντικό ζήτημα που οι προγραμματιστές καλούνται να λύσουν ή να ελαχιστοποιήσουν. Αυτό το ζήτημα τίθεται συχνά σε τεχνικές συζητήσεις για το πρωτόκολλο bitcoin. Δεδομένου ότι το bitcoin είναι ένα αυτορυθμιζόμενο σύστημα που λειτουργεί ανακαλύπτοντας μπλοκ σε κατά προσέγγιση διαστήματα, η υψηλότερη απόδοση συναλλαγών του περιορίζεται ουσιαστικά στο μέγιστο μέγεθος μπλοκ διαιρεμένο με το διάστημα μπλοκ. Ωστόσο, το κύριο εμπόδιο για την επεκτασιμότητα του Blockchain είναι η τάση προς συγκέντρωση με μια αναπτυσσόμενη αλυσίδα μπλοκ: όσο μεγαλώνει το Blockchain, τόσο μεγαλύτερες γίνονται οι απαιτήσεις για αποθήκευση, εύρος ζώνης και υπολογιστική ισχύ που πρέπει να αξιοποιηθούν από τους πλήρεις κόμβους στο δίκτυο. Αυτό όμως εγκυμονεί τον κίνδυνο υψηλότερης συγκέντρωσης, σε περίπτωση που το Blockchain γίνει τόσο μεγάλο που μόνο λίγοι κόμβοι είναι σε θέση να επεξεργαστούν ένα μπλοκ.
  - Απόρρητο: Το Blockchain μπορεί να διατηρήσει ένα συγκεκριμένο επίπεδο ιδιωτικότητας μέσω του δημόσιου κλειδιού (μια διεύθυνση για κάθε οντότητα). Ωστόσο, αποδεικνύεται ότι το Blockchain δεν μπορεί να εγγυηθεί το απόρρητο των συναλλαγών, καθώς οι τιμές όλων των συναλλαγών και τα υπόλοιπα για κάθε (ψευδώνυμο) δημόσιο κλειδί είναι δημόσια ορατά. Έτσι, η δημόσια φύση του Blockchain σημαίνει ότι τα ιδιωτικά δεδομένα θα ρέουν μέσω κάθε πλήρους κόμβου που είναι πλήρως εκτεθειμένος. Το «HD Wallet» έχει ήδη αντιμετωπίσει αυτό το πρόβλημα μέσω της χρήσης ενός εκτεταμένου δημόσιου κλειδιού ως το μοναδικό ευρετήριο για τη συσχέτιση συναλλαγών Blockchain, δίνοντας στους χρήστες τη δυνατότητα να δημιουργούν όσα δημόσια κλειδιά θέλουν. Στη συνέχεια, οι χρήστες μπορούν να επιλέξουν να προστατεύσουν το απόρρητό τους στέλνοντας τις

πληρωμές τους σε πολλαπλές συναλλαγές χωρίς να απαιτείται ρητός συντονισμός μεταξύ του αποστολέα και του παραλήπτη.

- Κατανάλωση ενέργειας: Η δημιουργία μπλοκ PoW σε ένα δημόσιο Blockchain καταναλώνει μεγάλη ποσότητα υπολογιστικής ισχύος και μαζί με αυτήν μεγάλη ποσότητα ηλεκτρικής ενέργειας. Η υπολογιστική ισχύς χρησιμοποιείται μόνο για αυτή τη διαδικασία και τα αποτελέσματα δεν έχουν κανένα άλλο όφελος παρά μόνο για χάρη του Blockchain.
- Θέματα ασφαλείας: Τα Vermont State Archives (2019) αναφέρουν ότι τα Blockchain έχουν αναπτυχθεί με βασικά θεμέλια υγιή τεχνολογία και αρχές. Η κρυπτογραφία δημόσιου κλειδιού είναι μια μαθηματικά αποδεδειγμένη μέθοδος κρυπτογράφησης δεδομένων και εφαρμόζεται ευρέως σε όλο τον Ιστό. Ωστόσο, εκατοντάδες περιστατικά ασφαλείας ετησίως οφείλονται σε ψευδή πιστοποιητικά, κακή κρυπτογράφηση ή κακή εφαρμογή αυτής της τεχνολογίας. Ομοίως, η ύπαρξη περιττών αντιγράφων αρχείων παρέχει μεν βελτιωμένη προστασία για αρχεία ζωτικής σημασίας για αρχεία και άλλα ιδρύματα σε όλο τον κόσμο, αλλά η απώλεια δεδομένων και τα ασυμβίβαστα σφάλματα παραμένουν πιθανά. Η χρονική σήμανση και ο συντονισμός των συναλλαγών δημιουργούν εσωτερική συνέπεια, αλλά ακόμη και οι απαιτήσεις συναίνεσης μπορούν να «νικηθούν» με αρκετούς πόρους. Κανένα σύστημα δεν είναι τέλει και τα Blockchain δεν διαφέρουν. Για να είναι χρήσιμα τα Blockchain στη δημόσια τήρηση αρχείων, οι δημόσιοι φορείς πρέπει να είναι σε θέση να εγγυώνται τη μακροπρόθεσμη διατήρηση και τη συνεχή πρόσβαση στα δημόσια αρχεία που καταγράφονται στο περιβάλλον τους. Ακόμη και για αρχεία με βραχυπρόθεσμη αξία, η ανάγκη διατήρησης ψηφιακών αρχείων σε Blockchain είναι απαραίτητη. Ο φόβος της μακροπρόθεσμης βιωσιμότητας δεν εμπόδισε την κυβέρνηση να χρησιμοποιήσει τεράστια καθολικά για δικαστικά έγγραφα ή πολύπλοκα κεντρικά ιδιόκτητα συστήματα/μονάδες επεξεργασίας για την ανάλυση των δεδομένων. Μάλλον, αυτή η δέσμευση και υπευθυνότητα για τη συνέχιση της διαχείρισης των πληροφοριών για ολόκληρο τον κύκλο ζωής τους είναι το βασικό στοιχείο για τη δημόσια τήρηση αρχείων. Οι τεχνολογίες έρχονται και παρέρχονται αλλά σε κάθε περίπτωση τα δημόσια αρχεία, και ειδικά τα αρχειακά τεκμήρια, πρέπει να αντέξουν.

- Επιρροή σε κρατικές λειτουργίες: Όπως αναφέρεται από τη National Archives and Records Administration (NARA) (2019), το Blockchain μπορεί τελικά να αλλάξει βασικές κυβερνητικές λειτουργίες, όπως η πιστοποίηση πληροφοριών, οι οικονομικές συναλλαγές και η ταυτοποίηση των πολιτών. Οι αλλαγές σε αυτούς τους τομείς έχουν τη δυνατότητα να επηρεάσουν θεμελιωδώς τον ρόλο της κυβέρνησης ως αξιόπιστου αποθετηρίου πληροφοριών ή κατόχου αρχείων. Αρχειακές και άλλες υπηρεσίες και οι διαχειριστές αρχείων θα πρέπει να παρακολουθούν τον τρόπο με τον οποίο η τεχνολογία Blockchain ωριμάζει και εφαρμόζεται με την πάροδο του χρόνου για να διασφαλιστεί ότι εντοπίζονται και αντιμετωπίζονται ζητήματα διαχείρισης αρχείων.

Η Lemieux (2016a) εστιάζει στα παρακάτω ζητήματα:

- Σχέσεις μεταξύ των κοινοτήτων Blockchain και αρχειονομίας: Υπάρχει πραγματική ανάγκη τόσο για έρευνα όσο και για κινητοποίηση γνώσης για την ενίσχυση της σχέσης μεταξύ της κοινότητας του Blockchain, δηλαδή των καινοτόμων που θα δημιουργήσουν το μελλοντικό πλαίσιο ως προς την τήρησης αρχείων σε Blockchain περιβάλλον, και της κοινότητας της αρχειονομίας, δηλαδή των ειδικών στο κομμάτι της διαχείρισης αρχείων που θα ζήσουν στο μέλλον του Blockchain και διαθέτουν θεωρητική και πρακτική γνώση ως προς την τήρηση αρχείων από το παρελθόν και το παρόν. Συγκεκριμένα, η αρχειονομία έχει αναπτύξει θεωρία και μεθόδους για την αξιολόγηση της ακρίβειας, της αξιοπιστίας και της γνησιότητας των αρχείων, καθώς και αρχές, πρότυπα και τεχνικές για τη διασφάλιση μακροπρόθεσμης αυθεντικότητας και διαθεσιμότητας αρχείων που θα μπορούσαν να βοηθήσουν τους προγραμματιστές λύσεων Blockchain να ενσωματώσουν αυτά τα χαρακτηριστικά στα συστήματά τους. Οι αρχειακές έννοιες και τεχνικές για την αναπαράσταση και τον εντοπισμό της προέλευσης και τον «αρχειακό δεσμό» μεταξύ των κατανεμημένων στοιχείων των αρχείων μπορούν επίσης να είναι χρήσιμες όταν εφαρμόζονται στην τήρηση αρχείων σε Blockchain περιβάλλον.
- Εμπιστοσύνη: Η τεχνολογία Blockchain θα μπορούσε να αλλάξει το παράδειγμά μας για την εμπιστοσύνη στα αρχεία. Αντί να απευθυνθούμε σε αξιόπιστα τρίτα μέρη, όπως κρατικά μητρώα, για αποδεικτικά στοιχεία, θα μπορούσαμε να στραφούμε σε

ένα Blockchain. Αλλά θα μπορούσε επίσης να διασπάσει τα στοιχεία που απαιτούνται για τη διαπίστωση της αυθεντικότητας (π.χ. μεταδεδομένα και ψηφιακές υπογραφές) από τα ίδια τα αρχεία, να προκαλέσει οικονομική αστάθεια μέσω της χρηματιστικοποίησης της τήρησης αρχείων και να υπονομεύσει το προσωπικό απόρρητο τόσο όσο το προστατεύει. Δύσκολα θα υπάρξει άθραυστη και εντελώς ασφαλής τεχνολογία. Ήδη αναζητούνται και βρίσκονται τρόποι παράνομης εισόδου (hack) σε Blockchain ή χρήσης τους για απάτη. Αυτό δεν καθιστά την τεχνολογία εγγενώς «κακή» ή άχρηστη. Ο μεγαλύτερος κίνδυνος στην πραγματικότητα δεν προέρχεται από τα τρωτά σημεία, αλλά από την τυφλή εμπιστοσύνη που φαίνεται να υπάρχει ως τώρα στο Blockchain από τους προγραμματιστές Blockchain, τους νομοθέτες, τις αρχές επιβολής του νόμου και το ευρύ κοινό σε αυτήν την τεχνολογία. Οι πιθανοί κίνδυνοι από την υιοθέτηση της τεχνολογίας Blockchain για τήρηση αρχείων έχουν συζητηθεί ελάχιστα και έχουν ερευνηθεί ελάχιστα, εν μέρει λόγω του φόβου της καταστολής της καινοτομίας και εν μέρει λόγω της έλλειψης συμβολής από ερευνητές στον κλάδο της αρχειονομίας και άλλων ειδικών. Με την έρευνα των κινδύνων, καθώς και των πλεονεκτημάτων, της τεχνολογίας Blockchain, θα είναι δυνατό να αξιοποιηθούν τα οφέλη, ενώ θα μετριαστούν οι κίνδυνοι που συνεπάγεται αυτή η νέα τεχνολογία τήρησης αρχείων. Για να πετύχουν, είναι επίσης πιθανό οι καινοτομίες Blockchain να πρέπει να ενσωματωθούν στα υπάρχοντα ή ελαφρώς τροποποιημένα οικονομικά και νομικά συστήματα. Η αρχειονομία θα μπορούσε να συμβάλλει σε αυτή την ενσωμάτωση. Το εναλλακτικό σενάριο του επανασχεδιασμού αυτών των συστημάτων για την προσαρμογή του Blockchain φαίνεται λιγότερο πιθανό να πετύχει.

Εκτός από τον εμπλουτισμό της τήρησης αρχείων σε Blockchain, με την τεχνογνωσία και την εμπειρία των ειδικών του κλάδου της αρχειονομίας, η ευρύτερη συνεργασία και ανταλλαγή ιδεών μεταξύ των δύο κοινοτήτων θα τοποθετήσει τους αρχειονόμους και άλλους επαγγελματίες στο κομμάτι των αρχείων να καταγράφουν, να διαχειρίζονται και να διατηρούν αρχεία Blockchain. Η διεπιστημονική έρευνα στο Blockchain, που φέρνει νομικούς, οικονομικούς, αρχειακούς, διπλωματικούς, εγκληματολογικούς και ερευνητές υπολογιστών και πληροφοριών σε συνδυασμό με

καινοτόμους στον τομέα των Blockchain, είναι ένα κρίσιμο επόμενο βήμα στην τήρηση αρχείων Blockchain.

- Διαχείριση προσωπικών δεδομένων: Όπως επισημαίνουν οι Hofman et al. (2019), η διαχείριση προσωπικών δεδομένων θα συνεχίσει να είναι ένα από τα πιο δύσκολα, έντονα προβλήματα για την ανάπτυξη της διακυβέρνησης των πληροφοριών. Με δεδομένο το αρκετά ευρύ πεδίο εφαρμογής του GDPR, πολλοί οργανισμοί, συμπεριλαμβανομένων εκείνων εκτός της Ευρωπαϊκής Ένωσης, θα πρέπει να διαχειρίζονται προσωπικά δεδομένα σύμφωνα με τον GDPR. Η τεχνολογία Blockchain θα μπορούσε να διαδραματίσει σημαντικό ρόλο στο να διασφαλιστεί ότι οι οργανισμοί έχουν εύκολα ελεγχόμενα, ανθεκτικά σε παραβίαση και παραποίηση αρχεία, ώστε να καλύπτουν ευρύτερες οργανωτικές ανάγκες και να συμμορφώνονται με τον GDPR. Τελικά, το Blockchain και το GDPR είναι και οι δύο «τεχνολογίες εμπιστοσύνης», αν και οι επιπτώσεις τους στην διακυβέρνηση των πληροφοριών μέχρι στιγμής ήταν ουσιαστικά διαφορετικές. Το GDPR φαίνεται να έχει αφυπνίσει πολλούς οργανισμούς στη σημασία της διακυβέρνησης των πληροφοριών. Οι συζητήσεις για το Blockchain επικεντρώνονται συνήθως στα τεχνικά χαρακτηριστικά σε τέτοιο βαθμό που οι επιπτώσεις της διαχείρισης αρχείων και της διακυβέρνησης πληροφοριών της τεχνολογίας ξεχνιούνται. Οι επαγγελματίες της διακυβέρνησης πληροφοριών πρέπει να γεφυρώσουν το χάσμα, βοηθώντας τους οργανισμούς τους να χρησιμοποιούν τα τεχνικά εργαλεία – όπως το Blockchain – για να πετύχουν τους στόχους τους, συμπεριλαμβανομένης της συμμόρφωσης.

## 5.4 Επίλογος

Σύμφωνα με τον Stancic (2018), η τεχνολογία Blockchain έχει προσελκύσει την προσοχή ως βάση κρυπτονομισμάτων όπως το Bitcoin, αλλά οι δυνατότητές της εκτείνονται πολύ πέρα από αυτό, επιτρέποντας σε υπάρχουσες τεχνολογικές εφαρμογές να βελτιωθούν σημαντικά και να αναπτυχθούν νέες εφαρμογές που δεν ήταν ποτέ πρακτικές. Γνωστό και ως τεχνολογία κατανεμημένου καθολικού, το Blockchain αναμένεται να φέρει επανάσταση στη βιομηχανία και το εμπόριο και να οδηγήσει στην οικονομική αλλαγή σε παγκόσμια κλίμακα, επειδή είναι αμετάβλητο, διαφανές και επαναπροσδιορίζει την εμπιστοσύνη, επιτρέποντας ασφαλείς, γρήγορες, αξιόπιστες και διαφανείς λύσεις που μπορεί να είναι δημόσιες ή ιδιωτικές. Θα μπορούσε να ενδυναμώσει τους ανθρώπους στις αναπτυσσόμενες χώρες με αναγνωρισμένη ταυτότητα, ιδιοκτησία περιουσιακών στοιχείων και οικονομική ένταξη. Υπάρχουν πολλές εφαρμογές Blockchain που θα μπορούσαν να μεταμορφώσουν την κοινωνία. Μεταξύ αυτών είναι χρηματοοικονομικές υπηρεσίες που βασίζονται σε Blockchain, έξυπνες εφαρμογές ιδιοκτησίας (π.χ. καταχώριση τίτλου περιουσιακών στοιχείων), έξυπνες συμβάσεις, εφαρμογές στον τομέα της υγειονομικής περίθαλψης ή της μουσικής, συμβολαιογραφική επικύρωση, παρακολούθηση προέλευσης καθώς και εφαρμογές ηλεκτρονικής διακυβέρνησης όπως η δημόσια ψηφοφορία, η διαχείριση ταυτότητας κ.λπ. Επίσης, το Blockchain θα μπορούσε να βρει τη χρήση του στην καθιέρωση της διαφάνειας της κυβέρνησης και της επικοινωνίας της με τους πολίτες.

Οι Sunil Bakale & Sangamesh K (2019) συμπληρώνουν ότι το Blockchain δεν αρκεί για την ανάπτυξη επιχειρήσεων μεγάλης κλίμακας. Πολλά εμπόδια πρέπει να ξεπεραστούν προτού το Blockchain να μπορεί να υιοθετηθεί πλήρως ως κύρια τεχνολογία ροής για επιχειρηματικές λύσεις στον πραγματικό κόσμο. Για την ανάπτυξη διεπαφών ανοιχτού συστήματος και την ύπαρξη μεσάζοντων που προς το παρόν επωφελούνται από τον έλεγχο των δεδομένων για τη διασύνδεση με το σύστημα Blockchain. Για την τροφοδοσία εφαρμογών Blockchain, όπου πρέπει να βελτιώνονται συνεχώς πρωτόκολλα Blockchain χαμηλού επιπέδου, ισοδύναμα με τη ραχοκοκαλιά των τρεχουσών υπηρεσιών Διαδικτύου, όπως το TCP/IP και το HTTP. Πρέπει να βελτιωθεί η εμπιστοσύνη και η διαδικασία λήψης αποφάσεων στο Blockchain, ώστε το σύστημα να είναι πιο επεκτάσιμο με υψηλότερες συναλλαγές χωρίς να θυσιάζεται η

ασφάλεια. Για παράδειγμα, ένας τρόπος είναι να εκχωρήσει το δίκτυο Blockchain περισσότερο βάρος σε αξιόπιστους κόμβους για να επιταχύνει τον υπολογισμό του μπλοκ.



## Βιβλιογραφικές Αναφορές

- Al Omar, A., Rahman, S., Tasnim, M. A., Rahman, M. S., Zakirul, M., & Bhuiyan, A. (2018). Crab: Blockchain based criminal record management system. *Springer, 11342 LNCS*, 294–303. [https://doi.org/10.1007/978-3-030-05345-1\\_25](https://doi.org/10.1007/978-3-030-05345-1_25)
- Bhatia, S., Douglas, E. K., & Most, M. (2020). Blockchain and records management: disruptive force or new approach? *Records Management Journal, 30*(3), 277–286. <https://doi.org/10.1108/RMJ-08-2019-0040/FULL/HTML>
- Department of the Army. (2008). *Guide to Recordkeeping in the Army* (Pamphlet 2).
- Franks, P. C. (2020). Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal, 30*(3), 287–299. <https://doi.org/10.1108/RMJ-08-2019-0047/FULL/HTML>
- Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). “The margin between the edge of the world and infinite possibility”: Blockchain, GDPR and information governance. *Records Management Journal, 29*(1–2), 240–257. <https://doi.org/10.1108/RMJ-12-2018-0045/FULL/HTML>
- Kikitamara, S., Eekelen, M. van, Thesis, D. D.-U. M., & 2017, U. (2017). Digital identity management on blockchain for open model energy system. *Ru.Nl*. [http://www.ru.nl/publish/pages/769526/digital\\_identity\\_management\\_on\\_blockchain\\_final.pdf](http://www.ru.nl/publish/pages/769526/digital_identity_management_on_blockchain_final.pdf)
- Koch, C., & Pieters, G. C. (2017). Blockchain technology disrupting traditional records systems. *Papers.Ssrn.Com, 6*(2). [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2997588](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997588)
- Lemieux, V. L. (2016a). Help or Hype? In *researchgate.net*. [https://www.researchgate.net/profile/Victoria\\_Lemieux/project/Blockchain-technology-for-record-keeping-Help-or-Hype/attachment/5870953b08aedc0fc0c10236/AS:447791592939521@1483773243345/download/Final+Report\\_Volume1.pdf?context=ProjectUpdatesLog](https://www.researchgate.net/profile/Victoria_Lemieux/project/Blockchain-technology-for-record-keeping-Help-or-Hype/attachment/5870953b08aedc0fc0c10236/AS:447791592939521@1483773243345/download/Final+Report_Volume1.pdf?context=ProjectUpdatesLog)
- Lemieux, V. L. (2016b). Trusting records: is Blockchain technology the answer? *Records Management Journal, 26*(2), 110–139. <https://doi.org/10.1108/RMJ-12-2015->

- Lemieux, V. L. (2017). A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. *leeexplore.lee.org*.  
<https://doi.org/10.1109/BigData.2017.8258180>
- Lemieux, V. L., Hofman, D., Batista, D. A., & Joo, A. (2019). Blockchain Technology & Recordkeeping. *ARMA International Educational Foundation*.  
[www.armaedfoundation.org](http://www.armaedfoundation.org)
- Ministry Of Defence. (2014). *Defence Records Management Policy and Procedures* (MOD Departmental Record Officer (ed.); 4.3).
- National Archives and Records Administration (NARA). (2019). *Blockchain White Paper*.  
<https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf>
- Sadiku, M. N. O., Eze, K. G., & Musa, S. M. (2018). Blockchain Technology in Healthcare. *International Journal of Advances in Scientific Research and Engineering*, 4(5), 154–159.  
<https://doi.org/10.31695/ijasre.2018.32723>
- Siwan, N., Noh, S.-W., Park, Y., Sur, C., Shin, S.-U., & Rhee, K.-H. (2017). Blockchain-based user-centric records management system. *Researchgate.Net*, 10(11), 133–144.  
<https://doi.org/10.14257/ijca.2017.10.11.12>
- Stancic, H. (2018). New technologies applicable to document and records management: blockchain. *Arxiv.org*.  
<https://arxiv.org/abs/1810.01313>
- Staples, M., Chen, S., Falamaki, S., & Ponomarev, A. (2017). Risks and opportunities for systems using blockchain and smart contracts. Data61. *Agcenter.Com*.  
[https://www.agcenter.com/Documents links and slide shows/Blockchains and Smart Contracts.pdf](https://www.agcenter.com/Documents%20links%20and%20slide%20shows/Blockchains%20and%20Smart%20Contracts.pdf)
- Sunil Bakale, & Sangamesh K. (2019). Blockchain Technology for Securing Healthcare Records. *International Research Journal of Engineering and Technology (IRJET)*, 6(4), 1804–1806.  
[https://www.academia.edu/39650357/IRJET\\_Blockchain\\_Technology\\_for\\_Securing\\_Healthcare\\_Records](https://www.academia.edu/39650357/IRJET_Blockchain_Technology_for_Securing_Healthcare_Records)
- Vermont State Archives. (2019). *Blockchains for Public Recordkeeping and for Recording Land Records*.

[https://sos.vermont.gov/media/r3jh24ig/vsara\\_blockchains\\_for\\_public\\_recordkeeping\\_white\\_paper\\_v1.pdf](https://sos.vermont.gov/media/r3jh24ig/vsara_blockchains_for_public_recordkeeping_white_paper_v1.pdf)

Zhu, H., Guo, Y., & Zhang, L. (2021). An improved convolution Merkle tree-based blockchain electronic medical record secure storage scheme. *Journal of Information Security and Applications*, 61, 102952. <https://doi.org/10.1016/J.JISA.2021.102952>

Γενικά Αρχεία του Κράτους. (2018). *Υπηρεσία Στρατιωτικών Αρχείων*. <https://greekarchivesinventory.gak.gr/index.php/xsne-bb2γ-p2g5>

Γενικό Επιτελείο Στρατού (ΓΕΣ). (2021). *Αφιέρωμα στα 80 χρόνια από την ίδρυση της Υπηρεσίας Στρατιωτικών Αρχείων*.

Ίσαρη, Φ., & Πουρκός, Μ. (2016). *Ποιοτική μεθοδολογία έρευνας*. <https://repository-web.kallipos.gr/handle/11419/5826>

Μιχαήλ, Δ. (2021). *Μεθοδολογία Ποιοτικής Έρευνας*. Πανεπιστήμιο Δυτικής Μακεδονίας.

Υπουργείο Εθνικής Άμυνας. (2016). *ΥΠΗΡΕΣΙΑ ΣΤΡΑΤΙΩΤΙΚΩΝ ΑΡΧΕΙΩΝ*. <https://www.dideap.mil.gr/ypiresia-stratotikon-archeion/>

# Παράρτημα

ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΣΤΡΑΤΟΥ  
ΥΠΗΡΕΣΙΑ ΣΤΡ/ΚΩΝ ΑΡΧΕΙΩΝ  
ΓΡΑΜΜΑΤΕΙΑ  
Αθήνα, 19 Σεπ 22

## ΒΕΒΑΙΩΣΗ ΥΠΗΡΕΣΙΑΣ

Ο υπογεγραμμένος ΑΧΙΑΣ (ΠΖ) ΜΗΤΣΙΚΑΣ ΜΕΞΑΝΔΡΟΣ (ΑΜ:15491) Δντης  
Γραμματείας του ΓΕΣ/ΥΣΑ

### Βεβαιώνω

ότι, από την 19/09/2022 έως και 20/9/2022 ο Αναστάσιος Καρνεζης του  
Κων/νου ΑΔΤ ΑΚ220709 προσήλθε στην Υπηρεσία μας για σκοπούς έρευνας.

Η παρούσα βεβαίωση, χορηγείται κατόπιν αιτήσεως του ενδιαφερόμενου για  
κάθε νόμιμη χρήση.

ΘΕΩΡΗΘΗΚΕ  
Ο-  
ΔΙΕΥΘΥΝΤΗΣ



ΜΗΤΣΙΚΑΣ ΑΛΕΞΑΝΔΡΟΣ  
ΣΥΧΗΣ (ΤΘ.ΥΓΡ)

