ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

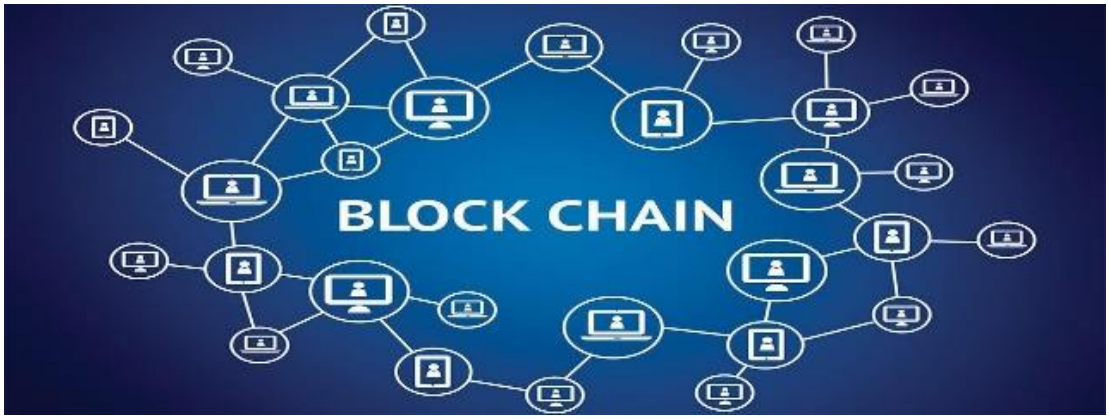
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΗΓΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Χρήση της τεχνολογίας Blockchain για την ψηφιακή ταυτοποίηση»

Ντεμίρης Βάιος
Α.Μ.: 22018



Επιβλέπων Καθηγητής: Δρ. Κόγιας Γ. Δημήτριος

Αθήνα, Ιούλιος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΗΓΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Χρήση της τεχνολογίας Blockchain για την ψηφιακή ταυτοποίηση»

Ντεμίρης Βάιος
Α.Μ.: 22018

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Επιβλέποντος

Η παρούσα μεταπτυχιακή διπλωματική εργασία εγκρίθηκε από την κάτωθι τριμελή επιτροπή αξιολόγησης:

Α' Μέλος	**Β' Μέλος**	**Γ' Μέλος**
Κόγιας Δημήτριος	Λελίγκου Ελένη Αικατερίνη	Καρκαζής Παναγιώτης
Επισκέπτης Καθηγητής	Καθηγήτρια	Αναπληρωτής Καθηγητής
Dimitrios Kogias Digitally signed by Dimitrios Kogias Date: 2024.09.02 19:22:37 +03'00'	ELENI AIKATERINI LELIGKOU Digitally signed by ELENI AIKATERINI LELIGKOU Date: 2024.09.03 10:58:41 +03'00'	PANAGIOTIS KARKAZIS Digitally signed by PANAGIOTIS KARKAZIS Date: 2024.09.03 12:10:50 +03'00'

Ημερομηνία Εξέτασης: 24/07/2024

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Ντεμίρης Βάιος** του **Νικολάου**, με αριθμό μητρώου **22018**, φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών **«Προηγμένες Τεχνολογίες Υπολογιστικών Συστημάτων», του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, της Σχολής Μηχανικών, 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

Ντεμίρης Βάιος

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά, θα ήθελα να εκφράσω τις ευχαριστίες μου ως προς τους Καθηγητές μου, οι οποίοι μου παρείχαν τη δυνατότητα να ασχοληθώ με ένα θέμα τόσο συναρπαστικό και πρωτοποριακό.

Επιπλέον, θα ήθελα να εκφράσω την ευγνωμοσύνη μου ως προς την οικογένειά μου και τους φίλους μου για τη στήριξη και τη συνεχή ενθάρρυνσή τους κατά τη διάρκεια των σπουδών μου, ιδίως ως προς τους γονείς μου και τη γυναίκα μου, οι οποίοι δεν έπαψαν να με υποστηρίζουν και να πιστεύουν σε μένα.

Τέλος, δεν μπορώ παρά να εκφράσω τις ευχαριστίες μου ως προς τον τεσσάρων χρονών υιό μου, τον Νικόλα, που παρά το γεγονός ότι για ένα αρκετά μεγάλο χρονικό διάστημα ήμουν απασχολημένος περισσότερο απ' όσο ήθελα και ήθελε, αυτός μου έδινε δύναμη και ενέργεια.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία διερευνά τις δυνατότητες της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση. Παρέχει μια ολοκληρωμένη ανάλυση του τρόπου με τον οποίο η τεχνολογία του Blockchain, που αρχικά σχεδιάστηκε για κρυπτονομίσματα, φέρνει επανάσταση στη διαχείριση και την ασφάλεια της ψηφιακής ταυτοποίησης. Η διπλωματική εργασία ξεκινά με μια εισαγωγή στη τεχνολογία του Blockchain και εν συνεχεία εμβαθύνει στις τεχνικές της λειτουργίες και αναλύει τα βασικά της χαρακτηριστικά, όπως η αποκέντρωση, η διαφάνεια και το αμετάβλητο των εγγραφών. Στη συνέχεια, παρουσιάζει τις τρέχουσες προκλήσεις στον τομέα της ψηφιακής ταυτοποίησης, όπως τα τρωτά σημεία ασφάλειας, οι ανησυχίες για το απόρρητο και η αναποτελεσματικότητα στα παραδοσιακά συστήματα. Τα επόμενα κεφάλαια διερευνούν τις πρακτικές εφαρμογές του Blockchain στην ψηφιακή ταυτοποίηση μέσω διαφόρων περιπτωσιολογικών μελετών, τονίζοντας πρωτοβουλίες τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Η διπλωματική εργασία εξετάζει, επίσης, κριτικά τις προκλήσεις και τους περιορισμούς της εφαρμογής της τεχνολογίας Blockchain, συμπεριλαμβανομένων των ζητημάτων επεκτασιμότητας, των ρυθμιστικών εμποδίων και των ηθικών προκλήσεων. Προσβλέποντας στο μέλλον, συζητά τις αναδυόμενες τάσεις και τις πιθανές μελλοντικές εξελίξεις σε εφαρμογές Blockchain για ψηφιακή ταυτοποίηση. Η διπλωματική εργασία ολοκληρώνεται με τη σύνθεση των γνώσεων που αποκτήθηκαν, αντανακλώντας τις ευρύτερες επιπτώσεις της τεχνολογίας Blockchain σε αυτόν τον τομέα και προσφέροντας συστάσεις για μελλοντική έρευνα και εφαρμογή.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Εφαρμογή της τεχνολογίας Blockchain

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Blockchain, Ψηφιακή Ταυτοποίηση, Αποκέντρωση, Ασφάλεια, Απόρρητο, eIDAS, Αποκεντρωμένα Αναγνωριστικά (DIDs), Επαληθεύσιμα Διαπιστευτήρια (VCs)

ABSTRACT

This thesis explores the possibilities of Blockchain technology in digital identification. It provides a comprehensive analysis of how Blockchain technology, originally designed for cryptocurrencies, is revolutionizing digital identity management and security. The thesis begins with an introduction to Blockchain technology and then delves into its technical operations and analyzes its key features such as decentralization, transparency and immutability of records. It then presents current challenges in the field of digital identification, such as security vulnerabilities, privacy concerns, and inefficiencies in traditional systems. The following chapters explore the practical applications of Blockchain in digital identification through various case studies, highlighting both public and private sector initiatives. The thesis also critically examines the challenges and limitations of implementing Blockchain technology, including scalability issues, regulatory hurdles and ethical challenges. Looking ahead, it discusses emerging trends and possible future developments in Blockchain applications for digital identification. The thesis concludes by synthesizing the knowledge gained, reflecting on the broader implications of Blockchain technology in this area and offering recommendations for future research and application.

SCIENTIFIC FIELD: Application of Blockchain technology

KEY WORDS: Blockchain, Digital Identification, Decentralization, Security, Privacy, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs)

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ 1

1.1. Εισαγωγή 1

1.2. Σκοπός & Στόχοι Διπλωματικής Εργασίας 2

1.3. Μεθοδολογία Εργασίας 4

1.4. Διάρθρωση Εργασίας 4

ΚΕΦΑΛΑΙΟ 2: ΚΑΤΑΝΟΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN 7

2.1. Εισαγωγή Κεφαλαίου 7

2.2. Σύντομη Ιστορία του Blockchain 8

2.3. Βασικά Χαρακτηριστικά της Τεχνολογίας Blockchain 9

2.4. Η Μηχανική του Blockchain 11

2.4.1. Τρόπος Λειτουργίας Blockchain 12

2.4.2. Χαρακτηριστικά Αποκέντρωσης & Ασφάλειας 13

2.5. Το Blockchain Πέρα από τα Κρυπτονομίσματα 14

2.5.1. Άλλες Εφαρμογές του Blockchain 15

2.5.2. Μελέτες Περίπτωσης Blockchain σε Διάφορους Τομείς 17

2.5.2.1. Εφοδιαστική Αλυσίδα: Ιχνηλασιμότητας Τροφίμων από τη Walmart 17

2.5.2.2. Υγειονομική Περίθαλψη: Ψηφιακά Αρχεία Υγείας στην Εσθονία 18

ΚΕΦΑΛΑΙΟ 3: ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ: ΠΡΟΚΛΗΣΕΙΣ & ΑΠΑΙΤΗΣΕΙΣ 21

3.1. Εισαγωγή Κεφαλαίου 21

3.2. Επισκόπηση της Ψηφιακής Ταυτοποίησης 22

3.3. Εξέλιξη των Μεθόδων Ταυτοποίησης 23

3.4. Τρέχουσες Προκλήσεις στην Ψηφιακή Ταυτοποίηση 25

3.4.1. Ανησυχίες για το Απόρρητο 25
3.4.2. Τρωτά Σημεία Ασφαλείας 27
3.5. Απαιτήσεις για Ένα Ιδανικό Ψηφιακό Σύστημα Ταυτοποίησης 29
3.5.1. Αξιοπιστία 29
3.5.2. Προσβασιμότητα 31
3.5.3. Έλεγχος Χρήστη & Απόρρητο 33
ΚΕΦΑΛΑΙΟ 4: ΤΟ BLOCKCHAIN ΩΣ ΛΥΣΗ ΨΗΦΙΑΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ 35
4.1. Εισαγωγή Κεφαλαίου 35
4.2. Η Καταλληλόλητα του Blockchain για Ψηφιακή Ταυτοποίηση 35
4.2.1. Αμετάβλητες Εγγραφές 36
4.2.2. Αποκεντρωμένος Έλεγχος 37
4.3. Μελέτη Περίπτωσης: Η Χρήση του Blockchain στα Εκλογικά Συστήματα Ψηφοφορίας 39
4.3.1. Γενικά 39
4.3.2. Χρήση του Blockchain στα Εκλογικά Συστήματα Ψηφοφορίας 41
4.3.3. Η Περίπτωση της Σιέρρα Λεόνε 43
4.3.4. Η Περίπτωση της Πόλης Zug της Ελβετίας 45
ΚΕΦΑΛΑΙΟ 5: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ BLOCKCHAIN ΣΤΗ ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ 48
5.1. Εισαγωγή Κεφαλαίου 48
5.2. Κοινωνικός Αντίκτυπος 48
5.2.1. Απόρρητο & Προσωπική Ασφάλεια 49
5.2.2. Διακυβέρνηση & Συμμετοχή των Πολιτών 51
5.3. Οικονομικές & Επιχειρηματικές Επιπτώσεις 52
5.3.1. Σχέση Κόστους-Αποτελεσματικότητας 53
5.3.2. Επιχειρηματικά Μοντέλα Συστημάτων Ταυτοποίησης που Βασίζονται σε Blockchain 54

ΚΕΦΑΛΑΙΟ 6: ΠΡΟΤΥΠΑ, ΚΑΝΟΝΙΣΤΙΚΗ ΣΥΜΜΟΡΦΩΣΗ & BLOCKCHAIN ΣΤΗΝ ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ 57
6.1. Εισαγωγή Κεφαλαίου 57
6.2. Το eIDAS & η Ψηφιακή Ταυτοποίηση 58
6.2.1. Επισκόπηση Κανονισμού eIDAS 58
6.2.2. eIDAS 1 έναντι eIDAS 2 59
6.2.3. Ο Ρόλος του Blockchain στο eIDAS 62
6.3. Αποκεντρωμένα Αναγνωριστικά (DIDs) & Επαληθεύσιμα Διαπιστευτήρια (VCs) 64
6.3.1. Επισκόπηση DIDs & VCs 64
6.3.2. Προκλήσεις & Εκτιμήσεις 66
ΚΕΦΑΛΑΙΟ 7: ΠΡΟΚΛΗΣΕΙΣ & ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ 69
7.1. Εισαγωγή Κεφαλαίου 69
7.2. Τεχνικές & Ηθικές Προκλήσεις 69
7.2.1. Ζητήματα Επεκτασιμότητας 70
7.2.2. Δεοντολογικά Ζητήματα & Διακυβέρνηση Δεδομένων 72
7.3. Το μέλλον του Blockchain στην Ψηφιακή Ταυτοποίηση 73
7.3.1. Αναδυόμενες Τάσεις 74
7.3.2. Πιθανές Εξελίξεις & Μελλοντικοί Τομείς Έρευνας 76
ΚΕΦΑΛΑΙΟ 8: ΣΥΜΠΕΡΑΣΜΑΤΑ & ΣΥΣΤΑΣΕΙΣ 79
8.1. Συμπεράσματα 79
8.2. Συστάσεις 81
ΒΙΒΛΙΟΓΡΑΦΙΑ 84

ΕΥΡΕΤΗΡΙΟ ΓΡΑΦΗΜΑΤΩΝ & ΠΙΝΑΚΩΝ

Γραφήματα

Γράφημα 1. Το Blockchain ως υπηρεσία ηλεκτρονικής ψηφοφορίας.....43

Πίνακες

Πίνακας 1. Συγκριτική ανάλυση eIDAS 1 και eIDAS 2 61

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1. Εισαγωγή

Στην ψηφιακή εποχή, η έννοια της ταυτότητας υπερβαίνει τις απλές φυσικές ιδιότητες και περιλαμβάνει μια πλειάδα ψηφιακών αλληλεπιδράσεων και συναλλαγών. Καθώς η ζωή γίνεται ολοένα και πιο συνυφασμένη με τον ψηφιακό κόσμο, η ανάγκη για ασφαλή, αξιόπιστα και αποτελεσματικά συστήματα ψηφιακής ταυτοποίησης δεν ήταν ποτέ πιο επιτακτική. Αυτή η εργασία εμβαθύνει στις δυνατότητες της τεχνολογίας Blockchain και στον επαναπροσδιορισμό της ψηφιακής ταυτοποίησης, προσφέροντας μια αλλαγή από τα παραδοσιακά κεντρικά συστήματα σε ένα πιο ασφαλές, αποκεντρωμένο πλαίσιο.

Η έλευση του διαδικτύου και των ψηφιακών τεχνολογιών έχει επιφέρει άνευ προηγουμένου ευκολία και συνδεσιμότητα. Ωστόσο, έχει επίσης εισαγάγει σημαντικές προκλήσεις στη διαχείριση ταυτότητας, συμπεριλαμβανομένων ζητημάτων ασφάλειας, ιδιωτικότητας και εμπιστοσύνης. Οι παραβιάσεις δεδομένων, η κλοπή ταυτότητας και η απάτη εντοπίζονται σε μεγάλο βαθμό, υπογραμμίζοντας τις ευπάθειες των υπαρχόντων συστημάτων ψηφιακής ταυτοποίησης. Σε αυτό το πλαίσιο, η τεχνολογία Blockchain δεν αναδύεται απλώς ως εναλλακτική επιλογή, αλλά ως απαραίτητη εξέλιξη για την επιδίωξη ενός πιο ασφαλούς ψηφιακού κόσμου.

Το Blockchain, στον πυρήνα του, είναι μια τεχνολογία κατανεμημένου καθολικού. Ωστόσο, οι εφαρμογές του εκτείνονται πολύ πέρα από τη σφαίρα των ψηφιακών νομισμάτων. Η τεχνολογία του Blockchain προσφέρει μια αποκεντρωμένη δομή, όπου οι πληροφορίες αποθηκεύονται σε ένα δίκτυο υπολογιστών, καθιστώντας τις σχεδόν αδιαπέραστες από μη εξουσιοδοτημένες αλλαγές. Αυτό το εγγενές χαρακτηριστικό ασφαλείας, σε συνδυασμό με τη διαφάνεια και την ιχνηλασιμότητα, καθιστά το Blockchain ιδανική επιλογή για τη διαχείριση ψηφιακών ταυτοτήτων.

Η σημασία του Blockchain στην ψηφιακή ταυτοποίηση έγκειται στην ικανότητά του να παρέχει ένα ενοποιημένο, αμετάβλητο και ασφαλές αρχείο

δεδομένων ταυτότητας που μπορεί να επαληθευτεί αποτελεσματικά, χωρίς να διακυβεύεται το απόρρητο. Αυτή η προσέγγιση όχι μόνο ενισχύει την ασφάλεια, αλλά δίνει, επίσης, τη δυνατότητα στα άτομα να έχουν μεγαλύτερο έλεγχο των προσωπικών τους πληροφοριών. Σε ένα σύστημα που βασίζεται σε Blockchain, οι χρήστες μπορούν να διαχειρίζονται ανεξάρτητα τις ψηφιακές τους ταυτότητες, αποφασίζοντας πώς, πότε και με ποιον θα μοιραστούν τα δεδομένα τους.

Ωστόσο, η ενσωμάτωση του Blockchain στην ψηφιακή ταυτοποίηση δεν γίνεται δίχως προκλήσεις. Ζητήματα, όπως η επεκτασιμότητα, η διαλειτουργικότητα και η κανονιστική συμμόρφωση αποτελούν σημαντικά εμπόδια. Επιπλέον, οι ηθικές συνέπειες μιας τόσο βαθιάς αλλαγής στον χειρισμό των προσωπικών δεδομένων απαιτούν μια πιο προσεκτική εξέταση. Η εξισορρόπηση των πλεονεκτημάτων του Blockchain με αυτές τις προκλήσεις απαιτεί μια λεπτή κατανόηση τόσο της τεχνολογίας όσο και του περίπλοκου τοπίου της ψηφιακής ταυτότητας.

1.2. Σκοπός & Στόχοι Διπλωματικής Εργασίας

Σκοπός της διπλωματικής εργασίας είναι να παρέχει μια διεξοδική και διορατική εξερεύνηση της εφαρμογής της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση. Αυτό περιλαμβάνει την κατανόηση της πολύπλευρης φύσης του Blockchain, την κατανόηση των δυνατοτήτων του να φέρει επανάσταση στον τρόπο με τον οποίο διαχειριζόμαστε τις ψηφιακές ταυτότητες και την κριτική ανάλυση των προκλήσεων και των ευκαιριών που παρουσιάζει. Η διπλωματική εργασία στοχεύει στην επίτευξη αρκετών στόχων και συγκεκριμένα στους κάτωθι:

- Εννοιολογική προσέγγιση της τεχνολογίας Blockchain: Αποσαφήνιση των θεμελιωδών αρχών της τεχνολογίας Blockchain, εξηγώντας πώς λειτουργεί, τα βασικά της χαρακτηριστικά και γιατί θεωρείται μια σημαντική ανακάλυψη στον τομέα της ψηφιακής ασφάλειας και ψηφιακής ταυτοποίησης.
- Αξιολόγηση του αντίκτυπου του Blockchain στην ψηφιακή ταυτοποίηση: Αξιολόγηση του πως η τεχνολογία Blockchain μπορεί να βελτιώσει την ασφάλεια, το απόρρητο και την αποτελεσματικότητα των συστημάτων

ψηφιακής ταυτοποίησης. Αυτό περιλαμβάνει μια σύγκριση με τις παραδοσιακές μεθόδους ταυτοποίησης, ώστε να επισημανθούν οι εξελίξεις που φέρνει το Blockchain.

- Προσδιορισμός προκλήσεων και περιορισμών: Κριτική ανάλυση των προκλήσεων που σχετίζονται με την εφαρμογή του Blockchain στην ψηφιακή ταυτοποίηση. Αυτό περιλαμβάνει τεχνικά εμπόδια, όπως η επεκτασιμότητα και η διαλειτουργικότητα, καθώς και τα ρυθμιστικά και ηθικά ζητήματα και ζητήματα απορρήτου.
- Διερεύνηση εφαρμογών στον πραγματικό κόσμο: Παροχή συγκεκριμένων παραδειγμάτων και περιπτωσιολογικών μελετών όπου η τεχνολογία Blockchain χρησιμοποιείται ήδη ή έχει τη δυνατότητα να χρησιμοποιηθεί στην ψηφιακή ταυτοποίηση. Αυτό βοηθά στην κατανόηση των πρακτικών επιπτώσεων και του αντίκτυπου της τεχνολογίας Blockchain στον πραγματικό κόσμο.
- Συζήτηση μελλοντικών προοπτικών και τάσεων: Διερεύνηση της μελλοντικής κατεύθυνσης του Blockchain στην ψηφιακή ταυτοποίηση, συμπεριλαμβανομένων των αναδυόμενων τάσεων, των πιθανών εξελίξεων και των περιοχών που είναι ώριμες για μελλοντική έρευνα. Αυτός ο στόχος εστιάζει να παρέχει μια προοπτική για το πώς το Blockchain θα μπορούσε να συνεχίσει να εξελίσσεται και να επηρεάζει τον τομέα της ψηφιακής ταυτοποίησης.

Μέσω αυτών των στόχων, η διπλωματική εργασία προσπαθεί να προσφέρει μια ολοκληρωμένη κατανόηση της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση. Επιδιώκει να συμβάλει ουσιαστικά στη συζήτηση για τη διαχείριση της ψηφιακής ταυτοποίησης στη σύγχρονη εποχή, παρέχοντας σαφήνεια και κατεύθυνση σε ένα ταχέως εξελισσόμενο τεχνολογικό τοπίο.

1.3. Μεθοδολογία Εργασίας

Η βάση αυτή της διπλωματικής εργασίας βασίζεται σε εκτεταμένη δευτερογενή έρευνα, αντλώντας από μια ποικιλία επιστημονικών μελετών, άρθρων, εκθέσεων του κλάδου, μελετών περιπτώσεων και θεωρητικών αναλύσεων. Αυτή η έρευνα συμβάλει καθοριστικά στην κατασκευή ενός ολοκληρωμένου θεωρητικού πλαισίου για την κατανόηση της εφαρμογής της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση.

Η δευτερογενής έρευνα που διεξήχθη για αυτή την εργασία παρέχει μια ισχυρή θεωρητική βάση, επιτρέποντας μια ολοκληρωμένη εξερεύνηση της τεχνολογίας Blockchain στο πλαίσιο της ψηφιακής ταυτοποίησης. Η παρούσα έρευνα όχι μόνο ενημερώνει την τρέχουσα κατάσταση της τεχνολογίας και των εφαρμογών της, αλλά προσφέρει, επίσης, πληροφορίες για τις προκλήσεις, τις ευκαιρίες και τις μελλοντικές κατευθύνσεις του Blockchain στη διαχείριση της ψηφιακής ταυτοποίησης.

1.4. Διάρθρωση Εργασίας

Ακολουθεί μια σύντομη επισκόπηση κάθε κεφαλαίου της διπλωματικής εργασίας σχετικά με την τεχνολογία Blockchain στην ψηφιακή ταυτοποίηση:

- Κεφάλαιο 1: Εισαγωγή

  Αυτό το κεφάλαιο θέτει τη βάση για τη διπλωματική εργασία, εισάγοντας το κύριο θέμα της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση. Σκιαγραφεί το τρέχον τοπίο της ψηφιακής ταυτοποίησης, τις προκλήσεις που αντιμετωπίζει και τις δυνατότητες του Blockchain ως λύσης. Στο κεφάλαιο παρουσιάζονται, επίσης, οι στόχοι, το εύρος και η μεθοδολογία της εργασίας.
- Κεφάλαιο 2: Κατανόηση της Τεχνολογίας Blockchain

  Αυτό το κεφάλαιο εμβαθύνει στις τεχνικές πτυχές της τεχνολογίας Blockchain. Εξηγεί τις βασικές αρχές, τον τρόπο λειτουργίας του Blockchain, τα βασικά του χαρακτηριστικά, όπως η αποκέντρωση, η αμετάβλητη φύση του και η

διαφάνεια, και γιατί αυτά τα χαρακτηριστικά είναι ωφέλιμα για την ψηφιακή ταυτοποίηση. Επίσης, παρουσιάζεται η χρήση του Blockchain πέρα από τα κρυπτονομίσματα και σε άλλους τομείς.

- Κεφάλαιο 3: Ψηφιακή Ταυτοποίηση: Προκλήσεις & Απαιτήσεις

  Αυτό το κεφάλαιο συζητά την έννοια της ψηφιακής ταυτοποίησης, τη σημασία της στον σύγχρονο κόσμο και τις προκλήσεις που αντιμετωπίζει αυτήν τη στιγμή, όπως ανησυχίες για την ασφάλεια, ζητήματα απορρήτου και την ανάγκη για αποτελεσματικές διαδικασίες επαλήθευσης.
- Κεφάλαιο 4: Το Blockchain ως Λύση Ψηφιακής Ταυτοποίησης

  Εστιάζοντας στην εφαρμογή του Blockchain στην ψηφιακή ταυτοποίηση, αυτό το κεφάλαιο διερευνά πώς το Blockchain μπορεί να αντιμετωπίσει τις προκλήσεις που περιεγράφηκαν στο προηγούμενο κεφάλαιο. Συζητά τα πλεονεκτήματα των συστημάτων που βασίζονται σε Blockchain έναντι των παραδοσιακών συστημάτων ψηφιακής ταυτοποίησης. Επίσης, παρουσιάζονται μελέτες περίπτωσης της χρήσης του Blockchain για ψηφιακή ταυτοποίηση και συγκεκριμένα, μέσω των περιπτώσεων χρήσης του στις εκλογικές ψηφοφορίες της Σιέρρα Λεόνε και της πόλης Zug στην Ελβετία.
- Κεφάλαιο 5: Οι Επιπτώσεις του Blockchain στη Ψηφιακή Ταυτοποίηση

  Σε αυτό το κεφάλαιο παρουσιάζονται οι επιπτώσεις του Blockchain στη ψηφιακή ταυτοποίηση και συγκεκριμένα, ο κοινωνικός αντίκτυπος και οι οικονομικές και επιχειρηματικές επιπτώσεις.
- Κεφάλαιο 6: Πρότυπα, Κανονιστική Συμμόρφωση & Blockchain στην Ψηφιακή Ταυτοποίηση

  Το κεφάλαιο αυτό εμβαθύνει στη σχέση μεταξύ Blockchain και ψηφιακής ταυτοποίησης, εξετάζοντας τον ρόλο των προτύπων, της κανονιστικής συμμόρφωσης και των αναδυόμενων τεχνολογιών. Το βασικό επίκεντρο αυτού του κεφαλαίου είναι ο Κανονισμός eIDAS, αλλά και η εξέταση των εννοιών των Αποκεντρωμένων Αναγνωριστικών (DIDs) και των Επαληθεύσιμων Διαπιστευτηρίων (VCs) στο πλαίσιο του Blockchain.
- Κεφάλαιο 7: Προκλήσεις & Μελλοντικές Προοπτικές

Ενώ το Blockchain προσφέρει πολλά πλεονεκτήματα, αυτό το κεφάλαιο εξετάζει τις προκλήσεις του και τις μελλοντικές του προοπτικές. Καλύπτει τεχνικές και ηθικές προκλήσεις, αλλά και το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση.

- Κεφάλαιο 8: Συμπεράσματα & Συστάσεις

  Το τελευταίο κεφάλαιο συνθέτει τα βασικά ευρήματα από την εργασία. Παρέχει μια περίληψη των κύριων σημείων που συζητήθηκαν, αντανακλά τις επιπτώσεις της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση και προσφέρει τελικές συστάσεις.

Κάθε κεφάλαιο της παρούσας διπλωματικής εργασίας συμβάλλει στην οικοδόμηση μιας ολοκληρωμένης κατανόησης της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση, από τα τεχνικά της θεμέλια έως τις πρακτικές εφαρμογές, τις προκλήσεις και τις μελλοντικές προοπτικές της.

ΚΕΦΑΛΑΙΟ 2: ΚΑΤΑΝΟΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

2.1. Εισαγωγή Κεφαλαίου

Το κεφάλαιο αυτό στοχεύει στην παροχή μιας ολοκληρωμένης κατανόησης της τεχνολογίας Blockchain, ξεκινώντας από την ιστορική της εξέλιξη και προχωρώντας σε μια εις βάθος ανάλυση των βασικών της χαρακτηριστικών και των μηχανισμών λειτουργίας της. Ξεκινώντας με μια σύντομη ιστορία του Blockchain, το κεφάλαιο εντοπίζει την προέλευσή του από τις πρώτες έννοιες της κρυπτογραφικής χρονοσήμανσης έως την τρέχουσα κατάστασή του ως μιας ευέλικτης τεχνολογίας με εφαρμογές που εκτείνονται πολύ πέρα από τα κρυπτονομίσματα.

Στη συνέχεια, το κεφάλαιο εμβαθύνει στα βασικά χαρακτηριστικά που καθορίζουν την τεχνολογία Blockchain, συμπεριλαμβανομένης της αποκέντρωσης, της αμετάβλητης φύσης των εγγραφών, της διαφάνειας, της ασφάλειας και της ικανότητάς της να εκτελεί έξυπνα συμβόλαια. Επιπλέον, το κεφάλαιο εξετάζει τις τεχνικές λειτουργίες του Blockchain, εξερευνώντας τον τρόπο με τον οποίο δημιουργούνται τα μπλοκ, συνδέονται και επικυρώνονται για να σχηματίσουν ένα ασφαλές και διαφανές καθολικό.

Για να καταδείξει την ευελιξία του Blockchain, το κεφάλαιο παρουσιάζει διάφορες εφαρμογές του πέρα από τον τομέα των κρυπτονομισμάτων. Αυτό περιλαμβάνει περιπτωσιολογικές μελέτες από τομείς, όπως η διαχείριση της εφοδιαστικής αλυσίδας και η υγειονομική περίθαλψη, όπου το Blockchain χρησιμοποιείται για την ενίσχυση της ιχνηλασιμότητας, της ασφάλειας και της αποδοτικότητας.

Συνολικά, το κεφάλαιο αυτό παρέχει μια ολοκληρωμένη βάση για την κατανόηση της τεχνολογίας Blockchain, θέτοντας τα θεμέλια για τα επόμενα κεφάλαια που διερευνούν την εφαρμογή της στην ψηφιακή ταυτοποίηση.

2.2. Σύντομη Ιστορία του Blockchain

Η ιδέα ενός πρωτοκόλλου τύπου Blockchain εμφανίστηκε για πρώτη φορά στις αρχές της δεκαετίας του 1990. Οι Haber και Stornetta (1991) εισήγαγαν μια υπολογιστικά πρακτική λύση για τη χρονοσήμανση ψηφιακών εγγράφων, έτσι ώστε να μην είναι δυνατή η αναδρομή ή η παραποίηση τους. Αυτή η ιδέα έθεσε τα θεμέλια για αυτό που αργότερα θα γινόταν η τεχνολογία Blockchain (Haber & Stornetta, 1991).

Η ανάπτυξη τεχνικών κρυπτογράφησης, όπως οι κρυπτογραφικές συναρτήσεις κατακερματισμού και οι ψηφιακές υπογραφές, ήταν ζωτικής σημασίας στην τότε εποχή πριν από το Blockchain. Αυτές οι τεχνολογίες παρείχαν τα απαραίτητα χαρακτηριστικά ασφαλείας που αργότερα θα αποτελούσαν αναπόσπαστο κομμάτι του Blockchain (Haber & Stornetta, 1991).

Ο όρος “Blockchain” κέρδισε το προσκήνιο με τη δημιουργία του Bitcoin το 2008, από ένα άτομο ή ομάδα, με το ψευδώνυμο Satoshi Nakamoto. Η λευκή βίβλος του Bitcoin, "Bitcoin: A Peer-to-Peer Electronic Cash System", εισήγαγε μια αποκεντρωμένη τεχνολογία λογιστικού η οποία στηρίζει όλα τα κρυπτονομίσματα (Nakamoto, 2008).

Η αρχική φάση της τεχνολογίας Blockchain, γνωστή ως Blockchain 1.0, χαρακτηρίστηκε από τη χρήση της σε συναλλαγές κρυπτονομισμάτων. Η επιτυχία του Bitcoin ενέπνευσε τη δημιουργία διαφόρων άλλων κρυπτονομισμάτων, το καθένα χρησιμοποιώντας Blockchain για την επίτευξη αποκέντρωσης και ασφάλειας (Swan, 2015).

Η δεύτερη φάση, το Blockchain 2.0, είδε την εφαρμογή της τεχνολογίας πέρα από τα νομίσματα. Η εισαγωγή του Ethereum το 2015 σηματοδότησε ένα σημαντικό ορόσημο. Η πλατφόρμα του Ethereum επέτρεψε τη δημιουργία έξυπνων συμβολαίων και αποκεντρωμένων εφαρμογών (DApps), επεκτείνοντας τη χρησιμότητα του Blockchain πέρα από απλές οικονομικές συναλλαγές (Buterin, 2014).

Επί του παρόντος, στην τρίτη της φάση, η τεχνολογία Blockchain υφίσταται διαφοροποίηση και ενσωμάτωση σε διάφορους τομείς. Αυτή η φάση χαρακτηρίζεται

από την εξερεύνηση εφαρμογών Blockchain σε τομείς, όπως η διαχείριση της εφοδιαστικής αλυσίδας, η υγειονομική περίθαλψη και η ψηφιακή ταυτοποίηση. Η εστίαση έχει μετατοπιστεί προς την επίλυση σύνθετων επιχειρηματικών προβλημάτων, την ενίσχυση της διαφάνειας και τη βελτίωση της ασφάλειας σε διάφορες ψηφιακές αλληλεπιδράσεις (Tapscott & Tapscott, 2016).

Παρά τις δυνατότητές του, το Blockchain αντιμετωπίζει διάφορες προκλήσεις, όπως η επεκτασιμότητα, η κατανάλωση ενέργειας και ρυθμιστικά ζητήματα. Ωστόσο, η συνεχιζόμενη έρευνα και ανάπτυξη αντιμετωπίζει αυτές τις προκλήσεις, ανοίγοντας το δρόμο για πιο ισχυρά και αποτελεσματικά συστήματα Blockchain (Yli-Huumo et al., 2016).

Αυτή η ιστορική επισκόπηση της τεχνολογίας Blockchain υπογραμμίζει την εξέλιξή της από μια εννοιολογική μέθοδο ψηφιακής χρονοσήμανσης σε μια επαναστατική τεχνολογία με ποικίλες εφαρμογές. Η κατανόηση αυτής της εξέλιξης είναι ζωτικής σημασίας για την κατανόηση των δυνατοτήτων του Blockchain στον μετασχηματισμό των συστημάτων ψηφιακής ταυτοποίησης. Οι παραπομπές που παρέχονται προσφέρουν ένα μείγμα τεχνικών γνώσεων και ιστορικού πλαισίου, απαραίτητες για μια ολοκληρωμένη κατανόηση της ανάπτυξης του Blockchain και της μελλοντικής του πορείας.

2.3. Βασικά Χαρακτηριστικά της Τεχνολογίας Blockchain

Στην παρούσα ενότητα παρουσιάζονται τα βασικά χαρακτηριστικά της τεχνολογίας Blockchain. Αυτά είναι τα εξής:

- Αποκέντρωση: Ένα από τα πιο καθοριστικά χαρακτηριστικά της τεχνολογίας Blockchain είναι η αποκεντρωμένη φύση της. Σε αντίθεση με τις παραδοσιακές βάσεις δεδομένων που διαχειρίζεται μια κεντρική αρχή, το Blockchain διανέμεται σε ένα δίκτυο υπολογιστών, ο καθένας από τους οποίους έχει ένα αντίγραφο του καθολικού. Αυτή η αποκέντρωση διασφαλίζει ότι καμία μεμονωμένη οντότητα δεν έχει έλεγχο σε ολόκληρο το δίκτυο,

ενισχύοντας την ασφάλεια και μειώνοντας τον κίνδυνο παραποίησης και απάτης (Nakamoto, 2008).

- Αμετάβλητο: Μόλις καταγραφούν δεδομένα στο Blockchain, είναι σχεδόν αδύνατο να αλλάξει. Αυτό το αμετάβλητο διασφαλίζεται μέσω κρυπτογραφικών συναρτήσεων κατακερματισμού, όπου κάθε μπλοκ περιέχει ένα μοναδικό κατακερματισμό του προηγούμενου μπλοκ, δημιουργώντας μια συνδεδεμένη αλυσίδα. Οποιαδήποτε προσπάθεια αλλαγής μιας μεμονωμένης εγγραφής θα απαιτούσε την εκ νέου εξόρυξη όλων των επόμενων μπλοκ, κάτι που δεν είναι υπολογιστικά πρακτικό, διασφαλίζοντας έτσι την ακεραιότητα των δεδομένων (Bayer et al., 1993).
- Διαφάνεια και ιχνηλασιμότητα: Η τεχνολογία Blockchain προσφέρει ένα άνευ προηγουμένου επίπεδο διαφάνειας. Όλες οι συναλλαγές στο Blockchain είναι ορατές σε οποιονδήποτε εντός του δικτύου, καθιστώντας το ένα εξαιρετικό εργαλείο για ιχνηλασιμότητα. Αυτό το χαρακτηριστικό είναι ιδιαίτερα επωφελές στη διαχείριση της εφοδιαστικής αλυσίδας και σε άλλους κλάδους όπου η διαφάνεια είναι ζωτικής σημασίας (Tapscott & Tapscott, 2016).
- Ασφάλεια: Ο συνδυασμός αποκέντρωσης, κρυπτογραφικού κατακερματισμού και μηχανισμών συναίνεσης καθιστά το Blockchain εξαιρετικά ασφαλές. Κάθε συναλλαγή επαληθεύεται από πολλούς κόμβους στο δίκτυο, καθιστώντας εξαιρετικά δύσκολο για τους κακόβουλους φορείς να χειριστούν τα δεδομένα. Αυτό το ισχυρό χαρακτηριστικό ασφαλείας είναι ιδιαίτερα ελκυστικό για οικονομικές συναλλαγές και διαχείριση ευαίσθητων δεδομένων (Yli-Huumo et al., 2016).
- Έξυπνα συμβόλαια: Τα έξυπνα συμβόλαια που εισήχθησαν κυρίως από το Ethereum, είναι αυτό-εκτελούμενες συμβάσεις με τους όρους της συμφωνίας απευθείας γραμμένους σε κώδικα. Εφαρμόζουν και εκτελούν αυτόματα τους όρους μιας σύμβασης όταν πληρούνται ορισμένες προϋποθέσεις, χωρίς να χρειάζονται μεσάζοντες. Αυτή η ικανότητα ανοίγει πολλές δυνατότητες σε διάφορους τομείς, συμπεριλαμβανομένων νομικών διαδικασιών, αυτοματοποιημένης διακυβέρνησης και πολλά άλλα (Buterin, 2014).

- Μηχανισμοί συναίνεσης: Το Blockchain λειτουργεί με μηχανισμούς συναίνεσης, όπως το Proof of Work (PoW) ή το Proof of Stake (PoS), τα οποία είναι πρωτόκολλα για να συμφωνηθεί η εγκυρότητα των συναλλαγών. Αυτοί οι μηχανισμοί διασφαλίζουν ότι όλοι οι συμμετέχοντες στο δίκτυο συμφωνούν για την τρέχουσα κατάσταση του Blockchain, καθιστώντας το πιο αξιόπιστο (Antonopoulos, 2014).
- Διαλειτουργικότητα και επεκτασιμότητα: Οι πρόσφατες εξελίξεις στην τεχνολογία Blockchain επικεντρώνονται στη βελτίωση της διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων Blockchain και στην ενίσχυση της επεκτασιμότητας για τη διαχείριση μεγαλύτερου αριθμού συναλλαγών (Mazières, 2016).

Αυτά τα βασικά χαρακτηριστικά δείχνουν γιατί η τεχνολογία Blockchain είναι επαναστατική και έχει τη δυνατότητα να μεταμορφώσει διάφορους κλάδους, συμπεριλαμβανομένης της ψηφιακής ταυτοποίησης. Η ικανότητά του να παρέχει ασφαλή, διαφανή και αμετάβλητα αρχεία το καθιστά ιδανική λύση για τη διαχείριση της ψηφιακής ταυτοποίησης με πιο ασφαλή και αποτελεσματικό τρόπο.

2.4. Η Μηχανική του Blockchain

Η παρούσα ενότητα της διπλωματικής εργασίας έχει ως στόχο να εμβαθύνει στις τεχνικές πτυχές της τεχνολογίας Blockchain. Εξετάζει τον τρόπο λειτουργίας του Blockchain, εξερευνώντας πώς δημιουργούνται, συνδέονται και επικυρώνονται τα μπλοκ για να σχηματίσουν ένα ασφαλές και διαφανές καθολικό. Επιπλέον, η ενότητα εξετάζει τα βασικά χαρακτηριστικά της αποκέντρωσης και της ασφάλειας που αποτελούν θεμελιώδη στοιχεία της τεχνολογίας Blockchain. Συνολικά, αυτή η ενότητα παρέχει μια πιο τεχνική κατανόηση του Blockchain, θέτοντας τα θεμέλια για την εξερεύνηση των εφαρμογών του πέρα από τα κρυπτονομίσματα σε τομείς, όπως η ψηφιακή ταυτοποίηση.

2.4.1. Τρόπος Λειτουργίας Blockchain

Στον πυρήνα του, το Blockchain είναι ένας τύπος κατανεμημένου καθολικού ή βάσης δεδομένων που μοιράζεται σε ένα δίκτυο υπολογιστών (κόμβων). Κάθε «μπλοκ» στο Blockchain περιέχει έναν αριθμό συναλλαγών και κάθε φορά που πραγματοποιείται μια νέα συναλλαγή στο Blockchain, μια εγγραφή αυτής της συναλλαγής προστίθεται στο καθολικό κάθε συμμετέχοντα. Αυτή η αποκεντρωμένη φύση είναι που διακρίνει το Blockchain από τις παραδοσιακές, κεντρικές βάσεις δεδομένων (Nakamoto, 2008).

Όταν ξεκινά μια συναλλαγή, επαληθεύεται πρώτα από τους κόμβους του δικτύου. Κάθε συναλλαγή στη συνέχεια μεταγλωττίζεται με άλλες σε ένα μπλοκ. Μια βασική πτυχή της τεχνολογίας Blockchain είναι η χρήση κρυπτογραφικών τεχνικών. Κάθε μπλοκ περιέχει ένα μοναδικό κρυπτογραφικό κατακερματισμό, μια χρονική σήμανση και δεδομένα συναλλαγών, καθώς και τον κατακερματισμό του προηγούμενου μπλοκ, που συνδέει τα μπλοκ μεταξύ τους σε μια χρονολογική και άθραυστη αλυσίδα (Bayer et al., 1993).

Για να προστεθεί ένα μπλοκ στο Blockchain, πρέπει να επικυρωθεί με συναινετικό μηχανισμό, όπως μέσω Απόδειξης Εργασίας (Proof of Work) ή Απόδειξη Συμμετοχής (Proof Of Stake). Στο Pow, το οποίο χρησιμοποιείται από το Bitcoin, οι κόμβοι («εξορύκτες») λύνουν σύνθετους μαθηματικούς γρίφους για να επικυρώσουν τις συναλλαγές και να δημιουργήσουν νέα μπλοκ. Το PoS, από την άλλη πλευρά, επιλέγει «επικυρωτές» αναλογικά με την ποσότητα μεριδίου τους στο κρυπτονόμισμα, απαιτώντας έτσι λιγότερη ενέργεια από το PoW (Antonopoulos, 2014).

Μόλις προστεθεί ένα μπλοκ στο Blockchain, είναι εξαιρετικά δύσκολο να αλλάξει. Εάν ένας εισβολέας ήθελε να αλλάξει μια συναλλαγή, θα έπρεπε να αλλάξει κάθε επόμενο μπλοκ στην αλυσίδα σε όλα τα αντίγραφα του καθολικού, κάτι που είναι πρακτικά αδύνατο, λόγω της αποκεντρωμένης και κρυπτογραφικής φύσης του δικτύου. Αυτό κάνει το Blockchain εξαιρετικά ασφαλές και ανθεκτικό σε παραβιάσεις (Swan, 2015).

Ενώ όλες οι συναλλαγές είναι ορατές και διαφανείς σε όλους στο δίκτυο, οι ταυτότητες των εμπλεκόμενων ατόμων κρυπτογραφούνται και αντιπροσωπεύονται μόνο από τα δημόσια κλειδιά τους. Αυτό παρέχει ένα επίπεδο ανωνυμίας διατηρώντας παράλληλα τη διαφάνεια των συναλλαγών (Tapscott & Tapscott, 2016).

2.4.2. Χαρακτηριστικά Αποκέντρωσης & Ασφάλειας

Η αποκέντρωση είναι χαρακτηριστικό της τεχνολογίας Blockchain. Σε αντίθεση με τα παραδοσιακά συστήματα που βασίζονται σε μια κεντρική αρχή, το Blockchain διανέμει το καθολικό του σε ένα δίκτυο κόμβων. Κάθε κόμβος έχει ένα αντίγραφο ολόκληρου του καθολικού και οι συναλλαγές καταγράφονται ταυτόχρονα σε αυτό το δίκτυο. Αυτή η δομή διασφαλίζει ότι δεν υπάρχει κανένα σημείο αποτυχίας ή ελέγχου, ενισχύοντας την ανθεκτικότητα του συστήματος και μειώνοντας τον κίνδυνο κεντρικής διαφθοράς ή χειραγώγησης (Nakamoto, 2008).

Η αποκεντρωμένη φύση του Blockchain ενισχύει εγγενώς την ασφάλειά του. Δεδομένου ότι το καθολικό δεν αποθηκεύεται σε μία μόνο τοποθεσία, αλλά σε ένα τεράστιο δίκτυο, καθίσταται εξαιρετικά δύσκολο για τους χάκερ να διακυβεύσουν την ακεραιότητα των δεδομένων. Αυτό το κατανεμημένο μοντέλο συναίνεσης σημαίνει, επίσης, ότι η εμπιστοσύνη δεν τοποθετείται σε μια ενιαία οντότητα, αλλά ενσωματώνεται στο ίδιο το σύστημα, μέσω του δικτύου συμμετεχόντων του (Swan, 2015).

Οι παραδοσιακές κεντρικές βάσεις δεδομένων είναι ευάλωτες από διακοπές λειτουργίας του διακομιστή ή στοχευμένες επιθέσεις στον κυβερνοχώρο. Αντίθετα, ένα δίκτυο Blockchain μπορεί να συνεχίσει να λειτουργεί ακόμα κι αν ορισμένοι κόμβοι αποτύχουν ή ενεργήσουν σε αυτόν κακόβουλα. Το σύστημα έχει σχεδιαστεί για να αντέχει ένα σημαντικό μέρος των κόμβων που αποτυγχάνουν χωρίς να χάσουν την ακεραιότητα ή τη συνέχεια των δεδομένων (Tapscott & Tapscott, 2016).

Κάθε μπλοκ στο Blockchain περιέχει ένα κρυπτογραφικό κατακερματισμό του προηγούμενου μπλοκ, δημιουργώντας μια ασφαλή και άθραυστη αλυσίδα. Αυτές οι συναρτήσεις κατακερματισμού είναι αλγόριθμοι μονής κατεύθυνσης που

μετατρέπουν μια είσοδο σε μια συμβολοσειρά byte σταθερού μεγέθους, η οποία εμφανίζεται τυχαία. Η αλλαγή ακόμη και ενός μόνο bit μιας συναλλαγής θα αλλάξει δραστικά τον κατακερματισμό, καθιστώντας εμφανή την παραβίαση (Bayer et al., 1993).

Το Blockchain χρησιμοποιεί έναν συνδυασμό δημόσιων και ιδιωτικών κλειδιών για την ασφάλεια των συναλλαγών. Το δημόσιο κλειδί ενός χρήστη είναι ορατό σε όλους και χρησιμοποιείται για τη λήψη συναλλαγών, ενώ το ιδιωτικό κλειδί διατηρείται μυστικό και χρησιμοποιείται για την υπογραφή των συναλλαγών. Αυτή η κρυπτογραφική μέθοδος διασφαλίζει ότι μόνο ο κάτοχος του ιδιωτικού κλειδιού μπορεί να εξουσιοδοτήσει συναλλαγές, παρέχοντας υψηλό επίπεδο ασφάλειας (Buterin, 2014).

Μόλις καταγραφούν δεδομένα στο Blockchain, δεν μπορούν να τροποποιηθούν αναδρομικά χωρίς να τροποποιηθούν όλα τα επόμενα μπλοκ και η συναίνεση του δικτύου. Αυτό το αμετάβλητο παρέχει ένα ασφαλές και προφανές αρχείο, καθιστώντας το Blockchain ιδανική τεχνολογία για εφαρμογές που απαιτούν μια αμετάβλητη διαδρομή ελέγχου (Yli-Huumo et al., 2016).

Ο συνδυασμός αποκέντρωσης και προηγμένων χαρακτηριστικών ασφαλείας καθιστά το Blockchain μια ισχυρή τεχνολογία με εφαρμογές πολύ πέρα από τα κρυπτονομίσματα. Η ικανότητά του να παρέχει ένα διαφανές και ασφαλές σύστημα είναι ιδιαίτερα ελκυστικό σε τομείς, όπως η ψηφιακή ταυτοποίηση, όπου η ακεραιότητα και η ασφάλεια των δεδομένων είναι πρωταρχικής σημασίας.

2.5. Το Blockchain Πέρα από τα Κρυπτονομίσματα

Η παρούσα ενότητα της διπλωματικής εργασίας διερευνά τις εφαρμογές της τεχνολογίας Blockchain πέρα από τον αρχικό της ρόλο στα κρυπτονομίσματα. Ενώ το Blockchain έγινε ευρέως γνωστό λόγω της σύνδεσής του με ψηφιακά νομίσματα, όπως το Bitcoin, οι δυνατότητές του εκτείνονται σε ένα ευρύ φάσμα τομέων. Αυτή η ενότητα εμβαθύνει σε αυτές τις ποικίλες εφαρμογές, παρέχοντας μελέτες περιπτώσεων από τομείς, όπως η διαχείριση εφοδιαστικής αλυσίδας και η

υγειονομική περίθαλψη, όπου το Blockchain χρησιμοποιείται για την ενίσχυση της ιχνηλασιμότητας, της ασφάλειας και της αποδοτικότητας. Συνολικά, αυτή η ενότητα αποκαλύπτει την ευελιξία του Blockchain και το δυναμικό του να φέρει επανάσταση σε διάφορους κλάδους πέρα από τον χρηματοπιστωτικό τομέα.

2.5.1. Άλλες Εφαρμογές του Blockchain

Σε αυτή την ενότητα παρουσιάζονται άλλες εφαρμογές του Blockchain, πέρα από τα κρυπτονομίσματα:

- Διαχείριση εφοδιαστικής αλυσίδας: Το Blockchain φέρνει επανάσταση στη διαχείριση της εφοδιαστικής αλυσίδας ενισχύοντας τη διαφάνεια, την ιχνηλασιμότητα και την αποτελεσματικότητα. Καταγράφοντας κάθε συναλλαγή σε ένα αποκεντρωμένο καθολικό, το Blockchain παρέχει μια αμετάβλητη και διαφανή καταγραφή της διαδρομής κάθε προϊόντος από τον κατασκευαστή στον καταναλωτή. Αυτή η ικανότητα είναι ιδιαίτερα πολύτιμη σε βιομηχανίες όπου η προέλευση και η αυθεντικότητα είναι ζωτικής σημασίας, όπως σε φαρμακευτικά προϊόντα και προϊόντα πολυτελείας (Kshetri, 2018).
- Υγειονομική περίθαλψη: Στην υγειονομική περίθαλψη, το Blockchain προσφέρει λύσεις για ασφαλή και αποτελεσματική διαχείριση των ιατρικών αρχείων, διασφαλίζοντας την ακεραιότητα των δεδομένων και το απόρρητο των ασθενών. Επιτρέποντας την αποθήκευση των δεδομένων με αποκεντρωμένο και αμετάβλητο τρόπο, το Blockchain μπορεί να διευκολύνει την καλύτερη ανταλλαγή δεδομένων μεταξύ των παρόχων υγειονομικής περίθαλψης, βελτιώνοντας τη φροντίδα των ασθενών και τις ερευνητικές ικανότητες (Mettler, 2016).
- Χρηματοοικονομικές υπηρεσίες: Πέρα από τα κρυπτονομίσματα, το Blockchain χρησιμοποιείται στον ευρύτερο χρηματοοικονομικό τομέα για τον εξορθολογισμό των διαδικασιών και τη μείωση της απάτης. Οι εφαρμογές περιλαμβάνουν διασυνοριακές πληρωμές, εκκαθάριση και διακανονισμό

συναλλαγών και επαλήθευση ταυτότητας, προσφέροντας ταχύτερες, φθηνότερες και πιο ασφαλείς χρηματοοικονομικές συναλλαγές (Guo & Liang, 2016).

- Ακίνητα: Το Blockchain απλοποιεί και διασφαλίζει τις συναλλαγές με ακίνητα. Το Blockchain αυξάνει τη ρευστότητα και μειώνει τους χρόνους και το κόστος των συναλλαγών. Τα έξυπνα συμβόλαια αυτοματοποιούν και επιβάλλουν συμφωνίες μίσθωσης, συμβάσεις πωλήσεων και καθήκοντα διαχείρισης ακινήτων (Turk & Mangan, 2018).
- Συστήματα ψηφοφορίας: Καταγράφοντας ψήφους σε Blockchain, η τεχνολογία μπορεί να μειώσει την εκλογική νοθεία και να αυξήσει την προσέλευση των ψηφοφόρων, καθιστώντας τη διαδικασία ψηφοφορίας πιο προσιτή και αξιόπιστη (Osgood, 2016).
- Πνευματική Ιδιοκτησία και δικαιώματα: Στον τομέα της πνευματικής ιδιοκτησίας, το Blockchain χρησιμοποιείται για τον έλεγχο ταυτότητας της προέλευσης του ψηφιακού περιεχομένου και τη διαχείριση των πνευματικών δικαιωμάτων. Παρέχει ένα διαφανές και ασφαλές σύστημα για την καταχώριση και την παρακολούθηση της πνευματικής ιδιοκτησίας, προσφέροντας έναν νέο τρόπο προστασίας των δικαιωμάτων των δημιουργών (De Filippi & Wright, 2018).
- Ενεργειακός τομέας: Το Blockchain πραγματοποιεί, επίσης, βήματα προόδου στον ενεργειακό τομέα, ιδιαίτερα στον τομέα των ανανεώσιμων πηγών ενέργειας. Επιτρέπει το peer-to-peer στο εμπόριο ενέργειας, επιτρέποντας στους καταναλωτές να αγοράζουν και να πουλούν πλεονάζουσα ενέργεια από ανανεώσιμες πηγές απευθείας μεταξύ τους, παρακάμπτοντας τις παραδοσιακές εταιρείες ενέργειας και προωθώντας τη χρήση ανανεώσιμων πηγών (Mengelkamp et al. (2018).

Αυτές οι ποικίλες εφαρμογές καταδεικνύουν το μετασχηματιστικό δυναμικό της τεχνολογίας Blockchain σε διάφορους κλάδους. Παρέχοντας λύσεις που είναι ασφαλείς, διαφανείς και αποτελεσματικές, το Blockchain δεν καινοτομεί μόνο τις υπάρχουσες διαδικασίες, αλλά παρέχει, επίσης, νέα επιχειρηματικά μοντέλα και ευκαιρίες.

2.5.2. Μελέτες Περίπτωσης Blockchain σε Διάφορους Τομείς

2.5.2.1. Εφοδιαστική Αλυσίδα: Ιχνηλασιμότητας Τροφίμων από τη Walmart

Πριν από την εφαρμογή του Blockchain, η Walmart, όπως και πολλοί μεγάλοι λιανοπωλητές, αντιμετώπιζε σημαντικές προκλήσεις στην παρακολούθηση της προέλευσης και της διαδρομής των προϊόντων διατροφής. Οι παραδοσιακές διαδικασίες της εφοδιαστικής αλυσίδας ήταν συχνά αργές και στερούνταν διαφάνειας, καθιστώντας δύσκολη την ταχεία ιχνηλάτηση των προϊόντων σε περίπτωση προβλήματος ασφάλειας των τροφίμων.

Η Walmart συνεργάστηκε με την IBM για να χρησιμοποιήσει την πλατφόρμα Blockchain τους, μέρος της πρωτοβουλίας IBM Food Trust. Αυτή η πλατφόρμα βασίζεται στο Hyperledger Fabric, μια υλοποίηση πλαισίου Blockchain που φιλοξενείται από το Linux Foundation. Η Walmart δοκίμασε για πρώτη φορά το σύστημα με δύο πιλοτικά έργα: την ανίχνευση του φρούτου μάνγκο στις Η.Π.Α. και του χοιρινού κρέατος στην Κίνα στην εφοδιαστική αλυσίδα. Αυτά τα προϊόντα επιλέχθηκαν λόγω της διαφορετικής πολυπλοκότητας της εφοδιαστικής αλυσίδας και της ανάγκης για αυστηρό ποιοτικό έλεγχο (Kamath, 2018).

Κάθε συμμετέχων στην εφοδιαστική αλυσίδα, από τον αγρότη μέχρι τον συσκευαστή και τον διανομέα, καταγράφει δεδομένα σχετικά με τα τρόφιμα στο Blockchain. Αυτά τα δεδομένα περιλαμβάνουν λεπτομέρειες, όπως ημερομηνία συγκομιδής, αριθμό παρτίδας, δεδομένα επεξεργασίας, ημερομηνίες λήξης και λεπτομέρειες αποστολής. Το σύστημα Blockchain επιτρέπει την πρόσβαση σε πραγματικό χρόνο σε αυτά τα δεδομένα από εξουσιοδοτημένους συμμετέχοντες. Αυτό σημαίνει ότι ανά πάσα στιγμή, η Walmart μπορεί να ελέγξει την προέλευση και τη διαδρομή οποιουδήποτε τρόφιμου στα καταστήματά της. (Kamath, 2018).

Με τη χρήση του Blockchain, ο χρόνος για τον εντοπισμό της προέλευσης των τροφίμων μειώθηκε δραστικά. Για παράδειγμα, η ανίχνευση της πηγής των μάνγκο μειώθηκε από 7 ημέρες σε μόλις 2,2 δευτερόλεπτα. Σε περίπτωση προβλήματος μόλυνσης τροφίμων, η Walmart μπορεί πλέον να εντοπίσει και να απομονώσει

γρήγορα την πηγή, μειώνοντας πιθανώς την εξάπλωση. Με τη χρήση αυτής της τεχνολογίας αυξάνεται η εμπιστοσύνη των καταναλωτών στα προϊόντα διατροφής της Walmart, καθώς οι πελάτες μπορούν να είναι σίγουροι για την ποιότητα και την ασφάλεια των αγορών τους (Kamath, 2018).

Η πρωτοβουλία αυτή της Walmart δείχνει πώς το Blockchain μπορεί να χρησιμοποιηθεί για να προσφέρει μεγαλύτερη διαφάνεια και αποτελεσματικότητα σε εφοδιαστικές αλυσίδες μεγάλης κλίμακας. Μετά την επιτυχία αυτών των πιλοτικών έργων, η Walmart κλιμακώνει την πρωτοβουλία και ενθαρρύνει τους προμηθευτές της να ενταχθούν στο δίκτυο Blockchain, υποδεικνύοντας μια κίνηση προς την ευρύτερη υιοθέτηση αυτής της τεχνολογίας στον τομέα του λιανικού εμπορίου (Kamath, 2018).

Αυτή η μελέτη περίπτωσης της πρωτοβουλίας Food Traceability Initiative της Walmart παρουσιάζει την πρακτική εφαρμογή της τεχνολογίας Blockchain για τη βελτίωση της διαφάνειας και της αποτελεσματικότητας της εφοδιαστικής αλυσίδας. Υπογραμμίζει πώς το Blockchain μπορεί να αντιμετωπίσει συγκεκριμένες προκλήσεις στην ασφάλεια και την ιχνηλασιμότητα των τροφίμων, προσφέροντας μαθήματα και γνώσεις που μπορούν να εφαρμοστούν σε διάφορους κλάδους που ασχολούνται με πολύπλοκες εφοδιαστικές αλυσίδες.

2.5.2.2. Υγειονομική Περίθαλψη: Ψηφιακά Αρχεία Υγείας στην Εσθονία

Η Εσθονία βρίσκεται στην πρώτη γραμμή της ψηφιακής καινοτομίας, με την πρωτοβουλία της “e-Estonia”, που στοχεύει στην ψηφιοποίηση των δημόσιων υπηρεσιών. Ο τομέας της υγειονομικής περίθαλψης ήταν βασικός στόχος, με τη δημιουργία ενός ασφαλούς, αποτελεσματικού και ενοποιημένου συστήματος ψηφιακών αρχείων υγείας. Δεδομένης της ευαισθησίας των ιατρικών δεδομένων, ένα σημαντικό μέλημα ήταν η διασφάλιση της ασφάλειας και του απορρήτου των αρχείων των ασθενών, επιτρέποντας ταυτόχρονα την απρόσκοπτη πρόσβαση σε εξουσιοδοτημένους παρόχους υγειονομικής περίθαλψης.

Η Εσθονία συνεργάστηκε με την Guardtime, μια εταιρεία τεχνολογίας Blockchain, για να εξασφαλίσει ότι τα αρχεία υγείας χρησιμοποιούν το KSI Blockchain (Keyless Signature Infrastructure). Αυτό το σύστημα ενσωματώθηκε στην υπάρχουσα υποδομή ψηφιακών μητρώων υγείας της Εσθονίας. Η λύση Blockchain χρησιμοποιήθηκε για τη διασφάλιση της ακεραιότητας και της ασφάλειας των αρχείων υγείας. Κάθε πρόσβαση στο αρχείο ενός ασθενούς καταγράφεται στο Blockchain, καθιστώντας αμέσως εμφανή οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση ή παραβίαση (Heston, 2020).

Κάθε φορά που πραγματοποιείται πρόσβαση ή τροποποίηση του αρχείου ενός ασθενούς, η συναλλαγή καταγράφεται στο Blockchain, δημιουργώντας μια αμετάβλητη διαδρομή ελέγχου. Αυτό διασφαλίζει ότι τυχόν αλλαγές στα αρχεία είναι ανιχνεύσιμες, διαφανείς και ασφαλείς. Οι ασθενείς έχουν πρόσβαση στα δικά τους αρχεία υγείας μέσω ασφαλούς ψηφιακής ταυτότητας και μπορούν να δουν ποιος έχει πρόσβαση στα αρχεία τους, ενισχύοντας τη διαφάνεια και την εμπιστοσύνη στο σύστημα (Heston, 2020).

Το σύστημα Blockchain αύξησε σημαντικά την ασφάλεια των ψηφιακών αρχείων υγείας, μειώνοντας τον κίνδυνο παραβίασης δεδομένων και μη εξουσιοδοτημένης πρόσβασης. Οι πάροχοι υγειονομικής περίθαλψης στην Εσθονία μπορούν να έχουν πρόσβαση σε ενημερωμένες πληροφορίες ασθενών πιο γρήγορα και αξιόπιστα, βελτιώνοντας την ποιότητα της περίθαλψης και μειώνοντας τον διοικητικό φόρτο. Οι ασθενείς απέκτησαν περισσότερο έλεγχο στα ιατρικά τους δεδομένα και μπορούν να παρακολουθούν την πρόσβαση στα αρχεία τους, οδηγώντας σε αυξημένη εμπιστοσύνη στο ψηφιακό σύστημα υγειονομικής περίθαλψης (Heston, 2020).

Η επιτυχημένη εφαρμογή του Blockchain στην υγειονομική περίθαλψη στην Εσθονία έχει χρησιμεύσει ως πρότυπο για άλλες χώρες που διερευνούν ψηφιακές λύσεις για τη διαχείριση ιατρικών δεδομένων. Αυτή η μελέτη περίπτωσης καταδεικνύει τις δυνατότητες της τεχνολογίας Blockchain στην αντιμετώπιση κρίσιμων προκλήσεων στον τομέα της υγειονομικής περίθαλψης, ιδιαίτερα στους τομείς της ασφάλειας δεδομένων και του απορρήτου των ασθενών (Heston, 2020).

Το σύστημα ψηφιακών αρχείων υγείας της Εσθονίας αποτελεί απόδειξη των δυνατοτήτων της τεχνολογίας Blockchain στον μετασχηματισμό της διαχείρισης δεδομένων υγειονομικής περίθαλψης. Παρέχοντας ένα ασφαλές, διαφανές και αποτελεσματικό σύστημα για το χειρισμό ευαίσθητων ιατρικών δεδομένων, η Εσθονία έχει θέσει ένα σημείο αναφοράς για την ψηφιακή καινοτομία στην υγειονομική περίθαλψη. Αυτή η μελέτη περίπτωσης προσφέρει πολύτιμες γνώσεις για την πρακτική εφαρμογή του Blockchain σε έναν κρίσιμο δημόσιο τομέα, υπογραμμίζοντας τόσο τα οφέλη του όσο και τις προκλήσεις της εφαρμογής μιας τέτοιας προηγμένης τεχνολογίας σε εθνική κλίμακα.

ΚΕΦΑΛΑΙΟ 3: ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ: ΠΡΟΚΛΗΣΕΙΣ & ΑΠΑΙΤΗΣΕΙΣ

3.1. Εισαγωγή Κεφαλαίου

Στον σημερινό ψηφιακό κόσμο, η ψηφιακή ταυτοποίηση έχει γίνει απαραίτητη. Επηρεάζει όλες τις πτυχές της ζωής μας, από τις διαδικτυακές συναλλαγές μέχρι την πρόσβαση σε βασικές υπηρεσίες. Η ψηφιακή ταυτότητα είναι ουσιαστικά μια ψηφιακή αναπαράσταση της ταυτότητας ενός ατόμου, που περιλαμβάνει προσωπικά στοιχεία που μπορούν να επαληθευτούν ηλεκτρονικά. Αυτό το κεφάλαιο εμβαθύνει στις πολυπλοκότητες της ψηφιακής ταυτοποίησης, εξετάζοντας την εξέλιξή της, τις τρέχουσες προκλήσεις και τις απαιτήσεις για ένα ιδανικό σύστημα ψηφιακής ταυτοποίησης.

Καθώς η τεχνολογία εξελίσσεται, το ίδιο συμβαίνει και με τις μεθόδους επαλήθευσης και πιστοποίησης της ταυτότητας. Αυτό το κεφάλαιο εξετάζει την εξέλιξη της ψηφιακής ταυτότητας, από τις πρώτες της μορφές έως τα τρέχοντα εξελιγμένα συστήματα. Συζητά την πρόοδο στα βιομετρικά στοιχεία, την άνοδο των ηλεκτρονικών ταυτοτήτων (eID) και τις προκλήσεις που θέτει το διαδίκτυο για την ασφαλή ψηφιακή ταυτοποίηση.

Παρά την πρόοδο, η ψηφιακή ταυτοποίηση αντιμετωπίζει σημαντικές προκλήσεις. Αυτό το κεφάλαιο ρίχνει φως σε αυτές τις προκλήσεις, συμπεριλαμβανομένων των ανησυχιών σχετικά με το απόρρητο, τα τρωτά σημεία ασφαλείας και την ανάγκη για ισχυρές διαδικασίες επαλήθευσης. Εξετάζει τους κινδύνους παραβίασης δεδομένων, τις δυνατότητες επιτήρησης και τις δυσκολίες στη διατήρηση της ακεραιότητας των δεδομένων σε ψηφιακά συστήματα ταυτοποίησης.

Τέλος, αυτό το κεφάλαιο ορίζει τις απαιτήσεις για ένα ιδανικό σύστημα ψηφιακής ταυτοποίησης. Διερευνά τις βασικές αρχές της αξιοπιστίας, της προσβασιμότητας και του ελέγχου και του απορρήτου του χρήστη. Συζητά πώς ένα αποτελεσματικό σύστημα ψηφιακής ταυτοποίησης θα πρέπει να είναι αξιόπιστο, προσβάσιμο σε όλους τους χρήστες και να δίνει τη δυνατότητα στα άτομα να

διαχειρίζονται τα δεδομένα τους. Αυτές οι απαιτήσεις χρησιμεύουν ως σημείο αναφοράς για την αξιολόγηση των υπαρχόντων συστημάτων και την καθοδήγηση της ανάπτυξης μελλοντικών λύσεων ψηφιακής ταυτοποίησης.

3.2. Επισκόπηση της Ψηφιακής Ταυτοποίησης

Η ψηφιακή ταυτοποίηση αντιπροσωπεύει την ταυτότητα ενός ατόμου σε ψηφιακή μορφή. Είναι μια κομβική πτυχή του όλο και πιο ψηφιακού κόσμου, που επηρεάζει τα πάντα, από τις ηλεκτρονικές συναλλαγές μέχρι την ασφάλεια των προσωπικών δεδομένων. Η έννοια της ταυτοποίησης έχει εξελιχθεί σημαντικά με την πάροδο του χρόνου. Οι παραδοσιακές μορφές ταυτοποίησης περιλαμβάνουν φυσικά έγγραφα, όπως ταυτότητες, διαβατήρια, άδειες οδήγησης, κ.α. ωστόσο, με την έλευση του διαδικτύου και των ψηφιακών τεχνολογιών, υπήρξε μια αλλαγή. Η ανάγκη για ένα ψηφιακό ισοδύναμο αυτών των φυσικών αναγνωριστικών έγινε εμφανής, οδηγώντας στην ανάπτυξη ψηφιακών αναγνωριστικών (Mayer-Schönberger & Cukier, 2013).

Μια ψηφιακή ταυτότητα συνήθως περιλαμβάνει αναγνωρίσιμες προσωπικές πληροφορίες, οι οποίες μπορεί να κυμαίνονται από βασικές λεπτομέρειες, όπως όνομα και ημερομηνία γέννησης έως πιο σύνθετα δεδομένα, όπως βιομετρικές πληροφορίες. Αυτή η ψηφιακή μορφή ταυτοποίησης χρησιμοποιείται σε διάφορες διαδικτυακές πλατφόρμες, δίνοντας τη δυνατότητα στα άτομα να αποδείξουν την ταυτότητά τους (Mayer-Schönberger & Cukier, 2013).

Η ανάπτυξη της ψηφιακής ταυτοποίησης έχει ενισχυθεί από την πρόοδο της τεχνολογίας. Οι καινοτομίες στα βιομετρικά στοιχεία, όπως η αναγνώριση δακτυλικών αποτυπωμάτων και προσώπου, έχουν ενισχύσει την ασφάλεια και την αξιοπιστία των ψηφιακών ταυτοτήτων. Αυτές οι τεχνολογίες διασφαλίζουν ότι οι ψηφιακές ταυτότητες είναι μοναδικές για ένα άτομο, μειώνοντας τον κίνδυνο κλοπής ταυτότητας και απάτης (Jain et al., 2016).

Η ψηφιακή ταυτοποίηση έχει γίνει αναπόσπαστη σε διάφορους τομείς, συμπεριλαμβανομένων των οικονομικών, της υγειονομικής περίθαλψης και των

κρατικών υπηρεσιών. Διευκολύνει μια σειρά από δραστηριότητες, από την ηλεκτρονική τραπεζική έως την πρόσβαση σε κρατικά οφέλη. Η σημασία της ψηφιακής ταυτοποίησης τονίστηκε περαιτέρω κατά τη διάρκεια της πανδημίας COVID-19, καθώς διαδραμάτισε κρίσιμο ρόλο στην ενεργοποίηση απομακρυσμένων υπηρεσιών και συναλλαγών (Jain et al., 2016).

Παρά τα πλεονεκτήματά της, η ψηφιακή ταυτοποίηση εγείρει σημαντικές ανησυχίες, ιδίως όσον αφορά το απόρρητο και την ασφάλεια των δεδομένων. Η συγκέντρωση προσωπικών δεδομένων σε ψηφιακές ταυτότητες μπορεί να τις καταστήσει στόχους κυβερνοεπιθέσεων. Επιπλέον, υπάρχουν ανησυχίες σχετικά με τον τρόπο με τον οποίο οι κυβερνήσεις και οι εταιρείες ενδέχεται να χρησιμοποιήσουν ή να κάνουν κατάχρηση αυτών των δεδομένων, εγείροντας ηθικά ερωτήματα σχετικά με την επιτήρηση και την προσωπική ελευθερία (Jain et al., 2016).

Επίσης, η υιοθέτηση και η εφαρμογή ψηφιακής ταυτοποίησης διαφέρει παγκοσμίως. Σε ορισμένες χώρες, τα εθνικά προγράμματα ψηφιακής ταυτοποίησης έχουν εφαρμοστεί με επιτυχία, ενώ σε άλλες, τα ζητήματα προσβασιμότητας και εμπιστοσύνης του κοινού παραμένουν σημαντικά εμπόδια (World Bank, 2018).

3.3. Εξέλιξη των Μεθόδων Ταυτοποίησης

Η ιστορία των μεθόδων ταυτοποίησης είναι ένα ταξίδι που αντικατοπτρίζει την εξέλιξη της ανθρώπινης κοινωνίας, της τεχνολογίας και της αυξανόμενης πολυπλοκότητας των αλληλεπιδράσεων και των συναλλαγών. Ιστορικά, η ταυτοποίηση βασιζόταν στην προσωπική αναγνώριση μέσα σε μικρές κοινότητες. Καθώς οι κοινωνίες μεγάλωναν, αυτή η μέθοδος έγινε μη πρακτική, οδηγώντας στην ανάπτυξη φυσικών εγγράφων ως απόδειξη της ταυτότητας. Οι αρχαίοι πολιτισμοί, όπως οι Ρωμαίοι, χρησιμοποιούσαν σφραγίδες ως μορφή προσωπικής ταυτοποίησης για συναλλαγές και νομικά έγγραφα (Martin & Taylor, 2020).

Η σύγχρονη έννοια των εγγράφων ταυτότητας προέκυψε με την άνοδο των εθνικών κρατών. Ο 15^{ος} αιώνας είδε την εισαγωγή των διαβατηρίων, αρχικά ως επιστολών ασφαλούς συμπεριφοράς για διεθνή ταξίδια. Με την πάροδο του χρόνου

εξελίχθηκαν σε τυποποιημένα έγγραφα που χρησιμοποιούνται για διασυνοριακή ταυτοποίηση (Lloyd, 2003).

Ο 19ος αιώνας εισήγαγε σημαντικές προόδους. Η φωτογραφία επέτρεψε τη συμπερίληψη της εικόνας ενός ατόμου σε έγγραφα ταυτοποίησης, ενισχύοντας την αξιοπιστία τους. Ταυτόχρονα, η συστηματική χρήση των δακτυλικών αποτυπωμάτων για αναγνώριση, που πρωτοστάτησε ο Sir Francis Galton και αργότερα αναπτύχθηκε από τον Sir Edward Henry, πρόσθεσε ένα μοναδικό βιομετρικό στοιχείο στις μεθόδους ταυτοποίησης (Cole, 2002).

Η ψηφιακή επανάσταση του τέλους του 20ου αιώνα άλλαξε τις μεθόδους ταυτοποίησης. Η εισαγωγή των ηλεκτρονικών ταυτοτήτων (eIDs), που αποθηκεύουν προσωπικά δεδομένα σε μαγνητικές λωρίδες ή τσιπ, σηματοδότησε μια σημαντική αλλαγή. Οι eID επέτρεψαν ταχύτερες διαδικασίες επαλήθευσης και αύξησαν τις εφαρμογές ταυτοποίησης, ειδικά σε ψηφιακές συναλλαγές (Martin & Taylor, 2020).

Επιπρόσθετα, η έλευση του διαδικτύου κατέστησε αναγκαία μια νέα μορφή ταυτοποίησης. Οι διαδικτυακοί λογαριασμοί, ασφαλισμένοι με ονόματα χρήστη και κωδικούς πρόσβασης, έγιναν πλέον ο κανόνας. Ωστόσο, οι περιορισμοί αυτής της μεθόδου, ιδιαίτερα στην ασφάλεια, οδήγησαν στην ανάπτυξη πιο εξελιγμένων συστημάτων ψηφιακής ταυτοποίησης, που ενσωματώνουν έλεγχο ταυτότητας πολλαπλών παραγόντων και βιομετρική επαλήθευση (Martin & Taylor, 2020).

Σήμερα, η πρόκληση έγκειται στην εξισορρόπηση της ασφάλειας, του απορρήτου και της ευκολίας στις μεθόδους ταυτοποίησης. Η άνοδος της τεχνολογίας Blockchain και η εφαρμογή της στην ψηφιακή ταυτοποίηση υπόσχεται μια αποκεντρωμένη, ασφαλή και ελεγχόμενη από τον χρήστη προσέγγιση, αντιμετωπίζοντας πολλές από τις αδυναμίες του τρέχοντος συστήματος (Pilkington, 2016).

Αυτή η ιστορική επισκόπηση παρέχει ένα ολοκληρωμένο υπόβαθρο για το πώς έχουν εξελιχθεί οι μέθοδοι ταυτοποίησης, θέτοντας το υπόβαθρο για μια βαθύτερη εξερεύνηση της ψηφιακής ταυτοποίησης και της τεχνολογίας Blockchain. Κάθε στάδιο της εξέλιξης έφερε το δικό του σύνολο προόδων και προκλήσεων, αντανακλώντας τα μεταβαλλόμενα κοινωνικά, τεχνολογικά και οικονομικά τοπία.

3.4. Τρέχουσες Προκλήσεις στην Ψηφιακή Ταυτοποίηση

Η ενότητα αυτή της παρούσας διπλωματικής εργασίας εμβαθύνει στις τρέχουσες προκλήσεις που αντιμετωπίζει η ψηφιακή ταυτοποίηση. Παρά την πρόοδο που έχει σημειωθεί σε αυτόν τον τομέα, υπάρχουν σημαντικά εμπόδια που πρέπει να ξεπεραστούν για να διασφαλιστεί η ασφάλεια, το απόρρητο και η αποτελεσματικότητα των ψηφιακών συστημάτων ταυτοποίησης. Η ενότητα διερευνά τις ανησυχίες σχετικά με το απόρρητο, τονίζοντας τους κινδύνους που σχετίζονται με την παραβίαση δεδομένων και την πιθανή επιτήρηση. Επιπλέον, η ενότητα ρίχνει φως στα τρωτά σημεία ασφαλείας, συμπεριλαμβανομένων των κυβερνοεπιθέσεων και της απάτης, που υπογραμμίζουν την ανάγκη για ισχυρές διαδικασίες επαλήθευσης. Συνολικά, η ενότητα παρέχει μια κριτική ανάλυση των προκλήσεων που πρέπει να αντιμετωπιστούν για την επίτευξη ενός αξιόπιστου και ασφαλούς συστήματος ψηφιακής ταυτοποίησης.

3.4.1. Ανησυχίες για το Απόρρητο

Τα συστήματα ψηφιακής ταυτοποίησης αποθηκεύουν και διαχειρίζονται εξαιρετικά ευαίσθητες προσωπικές πληροφορίες, συμπεριλαμβανομένων βιομετρικών δεδομένων, προσωπικών αριθμών αναγνώρισης και ιστορικού διευθύνσεων (Mayer-Schönberger & Cukier, 2013). Ο χειρισμός αυτών των δεδομένων εγείρει σημαντικές ανησυχίες σχετικά με το απόρρητο, όπως:

- Προκλήσεις απορρήτου:
  - ✓ <u>Παραβιάσεις δεδομένων:</u> Μία από τις κύριες ανησυχίες είναι ο κίνδυνος παραβιάσεων δεδομένων. Καθώς τα συστήματα ψηφιακής ταυτοποίησης συγκεντρώνουν μεγάλες ποσότητες προσωπικών δεδομένων, γίνονται ελκυστικοί στόχοι για επιθέσεις στον

κυβερνοχώρο, οδηγώντας δυνητικά στην έκθεση ευαίσθητων πληροφοριών (Roman et al., 2013).

- ✓ Παρακολούθηση: Ανησυχία για παρακολούθηση και κακή χρήση δεδομένων από κυβερνήσεις ή ιδιωτικούς φορείς. Η δυνατότητα παρακολούθησης των δραστηριοτήτων και των κινήσεων των ατόμων μέσω της ψηφιακής τους ταυτότητας μπορεί να οδηγήσει σε απώλεια της ανωνυμίας και της ιδιωτικής ζωής (Lyon, 2001).

- Blockchain και απόρρητο:
  - ✓ Διαφάνεια εναντίον απορρήτου: Αν και η διαφάνεια του Blockchain είναι ένα πλεονέκτημα, μπορεί να είναι ένα «δίκοπο μαχαίρι» όσον αφορά την προστασία της ιδιωτικής ζωής. Ο δημόσιος χαρακτήρας πολλών Blockchain σημαίνει ότι οι συναλλαγές, αφού καταγραφούν, είναι ορατές σε όλους τους συμμετέχοντες στο δίκτυο, οι οποίες θα μπορούσαν να περιλαμβάνουν προσωπικά δεδομένα (De Filippi & Wright, 2018).
  - ✓ Αμετάβλητα αρχεία: Η αμετάβλητη φύση του Blockchain είναι μια άλλη ανησυχία. Μόλις καταγραφούν προσωπικά δεδομένα σε ένα Blockchain, δεν μπορούν να τροποποιηθούν ή να διαγραφούν, γεγονός που έρχεται σε σύγκρουση με κανονισμούς απορρήτου, όπως το «δικαίωμα στη λήθη» του GDPR (Finck, 2018).
- Μετριασμός ανησυχιών περί απορρήτου:
  - ✓ Προηγμένη κρυπτογράφηση: Η χρήση προηγμένων μεθόδων κρυπτογράφησης μπορεί να βοηθήσει στην προστασία του απορρήτου των δεδομένων σε συστήματα ψηφιακής ταυτοποίησης. Τεχνικές, όπως οι αποδείξεις μηδενικής γνώσης (ZKP), επιτρέπουν την επαλήθευση των συναλλαγών χωρίς να αποκαλύπτονται τα υποκείμενα δεδομένα (Goldreich, 2009).
  - ✓ Ιδιωτικά Blockchain: Η εφαρμογή ιδιωτικών Blockchain, όπου η πρόσβαση είναι περιορισμένη, μπορεί να προσφέρει ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας. Αυτά τα συστήματα μπορούν να

σχεδιαστούν για να μοιράζονται μόνο συγκεκριμένα δεδομένα με εξουσιοδοτημένα μέρη (Vukolić, 2017).

- ✓ Κανονιστική συμμόρφωση: Η διασφάλιση ότι τα συστήματα ψηφιακής ταυτοποίησης συμμορφώνονται με τους νόμους και τους κανονισμούς περί προστασίας δεδομένων είναι ζωτικής σημασίας. Αυτό περιλαμβάνει μηχανισμούς για τη διόρθωση δεδομένων, τη διαγραφή και τη διαχείριση συναίνεσης (Koops, 2011).

Οι ανησυχίες για το απόρρητο στα συστήματα ψηφιακής ταυτοποίησης είναι πολύπλευρες και συνεπάγονται τον κίνδυνο παραβίασης δεδομένων, την πιθανή επιτήρηση και τις προκλήσεις που θέτει η ίδια η τεχνολογία Blockchain. Ενώ το Blockchain προσφέρει βελτιωμένη ασφάλεια και διαφάνεια, η εξισορρόπηση αυτών των χαρακτηριστικών με τις ανάγκες απορρήτου είναι ζωτικής σημασίας.

3.4.2. Τρωτά Σημεία Ασφαλείας

Τα συστήματα ψηφιακής ταυτοποίησης είναι επιρρεπή σε διάφορες μορφές κυβερνοεπιθέσεων, συμπεριλαμβανομένων του phishing, του κακόβουλου λογισμικού και της πειρατείας. Αυτές οι επιθέσεις μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα προσωπικά δεδομένα. Η διασφάλιση της ακεραιότητας των δεδομένων στα συστήματα ψηφιακής ταυτοποίησης είναι πρωταρχικής σημασίας. Οποιαδήποτε μη εξουσιοδοτημένη αλλαγή δεδομένων μπορεί να έχει σοβαρές συνέπειες, όπως κλοπή ταυτότητας ή ψευδή ταυτοποίηση (Juels & Oprea, 2013). Αναλυτικότερα:

- Τρωτά σημεία ασφαλείας ειδικά για το Blockchain:
  - ✓ Επιθέσεις 51%: Σε δίκτυα Blockchain, ιδιαίτερα σε αυτά που χρησιμοποιούν PoW, εάν μια μεμονωμένη οντότητα αποκτήσει έλεγχο πάνω από το 50% της υπολογιστικής ισχύος του δικτύου, μπορεί ενδεχομένως να χειραγωγήσει το Blockchain, γνωστό ως Επίθεση 51%. Αυτό αποτελεί μια σημαντική ανησυχία για τα μικρότερα δίκτυα Blockchain (Eyal & Sirer, 2018).

- ✓ Ευπάθειες έξυπνων συμβολαίων: Ενώ τα έξυπνα συμβόλαια αυτοματοποιούν και επιβάλλουν συμφωνίες στο Blockchain, είναι, επίσης, επιρρεπή σε ευπάθειες εάν δεν έχουν γραφτεί και ελεγχθεί σωστά (Atzei et al., 2017).

- Γενικές προκλήσεις ασφάλειας:
  - ✓ Επεκτασιμότητα και ασφάλεια: Καθώς τα συστήματα ψηφιακής ταυτοποίησης κλιμακώνονται, η διατήρηση της ασφάλειας χωρίς συμβιβασμούς στην απόδοση αποτελεί πρόκληση. Τα μεγαλύτερα συστήματα μπορεί να γίνουν πιο ευάλωτα σε επιθέσεις και να απαιτούν πιο σύνθετα πρωτόκολλα ασφαλείας (Croman et al., 2016).
  - ✓ Έλεγχος ταυτότητας χρήστη: Η διασφάλιση ότι το άτομο που έχει πρόσβαση στην ψηφιακή ταυτότητα είναι πράγματι ο νόμιμος κάτοχος αποτελεί μια κρίσιμη πρόκληση. Οι παραδοσιακοί μέθοδοι, όπως οι κωδικοί πρόσβασης, είναι συχνά αδύναμοι και ακόμη και τα βιομετρικά συστήματα μπορούν να εξαπατηθούν ή να παραβιαστούν (Jain et al., 2016).
- Μετριασμός τρωτών σημείων ασφαλείας:
  - ✓ Προηγμένες τεχνικές κρυπτογράφησης: Η εφαρμογή προηγμένων μεθόδων κρυπτογράφησης, συμπεριλαμβανομένων κβαντικών αλγορίθμων, μπορεί να ενισχύσει την ασφάλεια των συστημάτων ψηφιακής ταυτοποίησης έναντι των εξελισσόμενων απειλών στον κυβερνοχώρο (Bernstein & Lange, 2017).
  - ✓ Αποκέντρωση και πλεονασμός: Η αξιοποίηση της αποκεντρωμένης φύσης του Blockchain μπορεί να ενισχύσει την ασφάλεια. Η πλεονάζουσα αποθήκευση δεδομένων σε πολλούς κόμβους μειώνει τον κίνδυνο απώλειας δεδομένων ή παραβίασης (Zheng et al. (2017).
  - ✓ Τακτικοί έλεγχοι και ενημερώσεις: Η διεξαγωγή τακτικών ελέγχων ασφαλείας και η ενημέρωση του συστήματος για την επιδιόρθωση ευπαθειών είναι απαραίτητη. Αυτό περιλαμβάνει ενημέρωση των έξυπνων συμβολαίων και πρωτοκόλλων Blockchain για την

αντιμετώπιση προσδιορισμένων ζητημάτων ασφάλειας (Christidis & Devetsikiotis, 2016).

Τα τρωτά σημεία ασφαλείας στα συστήματα ψηφιακής ταυτοποίησης αποτελούν σημαντική ανησυχία, δεδομένης της ευαισθησίας των δεδομένων που εμπλέκονται. Ενώ η τεχνολογία Blockchain προσφέρει βελτιωμένα χαρακτηριστικά ασφαλείας, δεν είναι απρόσβλητη σε προκλήσεις, όπως οι Επιθέσεις 51% και οι ευπάθειες των έξυπνων συμβολαίων. Η αντιμετώπιση αυτών των ζητημάτων απαιτεί έναν συνδυασμό προηγμένης κρυπτογράφησης, προσεκτικού σχεδιασμού συστήματος, τακτικών ελέγχων και τήρησης βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας.

3.5. Απαιτήσεις για Ένα Ιδανικό Ψηφιακό Σύστημα Ταυτοποίησης

Η παρούσα ενότητα της παρούσας διπλωματικής εργασίας εξετάζει τις βασικές απαιτήσεις για ένα αποτελεσματικό σύστημα ψηφιακής ταυτοποίησης. Αναγνωρίζοντας τις προκλήσεις που συζητήθηκαν προηγουμένως, αυτή η ενότητα σκιαγραφεί τις βασικές αρχές που πρέπει να διέπουν ένα ιδανικό σύστημα ψηφιακής ταυτοποίησης. Αυτές οι αρχές περιλαμβάνουν την αξιοπιστία, η οποία διασφαλίζει ότι το σύστημα είναι αξιόπιστο και ασφαλές, την προσβασιμότητα, η οποία διασφαλίζει ότι το σύστημα είναι εύχρηστο και διαθέσιμο σε όλους τους χρήστες και τον έλεγχο και το απόρρητο του χρήστη, το οποίο δίνει τη δυνατότητα στα άτομα να διαχειρίζονται τα δεδομένα ταυτότητάς τους. Αυτή η ενότητα αποτελεί ένα πλαίσιο για την αξιολόγηση των υπαρχόντων συστημάτων και την καθοδήγηση της ανάπτυξης μελλοντικών λύσεων ψηφιακής ταυτοποίησης.

3.5.1. Αξιοπιστία

Η αξιοπιστία είναι ο ακρογωνιαίος λίθος κάθε ιδανικού συστήματος ψηφιακής ταυτοποίησης. Περιλαμβάνει όχι μόνο το χρόνο λειτουργίας και τη

διαθεσιμότητα του συστήματος, αλλά και την ακρίβεια και τη συνέπεια των δεδομένων που διατηρεί. Στο πλαίσιο της ψηφιακής ταυτοποίησης, η αξιοπιστία διασφαλίζει ότι το σύστημα είναι πάντα προσβάσιμο όταν χρειάζεται και ότι οι πληροφορίες που παρέχει είναι σωστές και ενημερωμένες. Αυτό είναι ιδιαίτερα σημαντικό σε τομείς, όπως η υγειονομική περίθαλψη, τα οικονομικά και οι νομικοί τομείς, όπου οι συνέπειες των αναξιόπιστων δεδομένων μπορεί να είναι σοβαρές (Wang & Strong, 1996).

Μία από τις κύριες προκλήσεις για την αξιοπιστία είναι η επεκτασιμότητα. Καθώς περισσότεροι χρήστες συμμετέχουν και χρησιμοποιούν ένα ψηφιακό σύστημα ταυτοποίησης, η διατήρηση της απόδοσης και της αξιοπιστίας του γίνεται όλο και πιο περίπλοκη. Το σύστημα πρέπει να χειρίζεται έναν αυξανόμενο όγκο συναλλαγών και αλληλεπιδράσεων χωρίς να θέτει σε κίνδυνο την ταχύτητα ή την ακρίβεια. Η τεχνολογία Blockchain, με την αποκεντρωμένη αρχιτεκτονική της, μπορεί να διαδραματίσει σημαντικό ρόλο. Διανέμοντας δεδομένα σε ένα δίκτυο κόμβων, το Blockchain μειώνει τον κίνδυνο αστοχιών του συστήματος και απώλειας δεδομένων. Αυτή η αποκέντρωση όχι μόνο ενισχύει την ανθεκτικότητα του συστήματος σε φυσικές βλάβες, όπως διακοπές λειτουργίας του διακομιστή, αλλά και σε απειλές στον κυβερνοχώρο (Anderson & Moore, 2006).

Ωστόσο, το Blockchain δεν είναι πανάκεια για όλα τα ζητήματα αξιοπιστίας. Ενώ προσφέρει ένα ισχυρό πλαίσιο για την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, η ίδια η τεχνολογία πρέπει να εφαρμοστεί και να διατηρηθεί προσεκτικά. Ζητήματα, όπως η συμφόρηση δικτύου, όπως φαίνεται σε ορισμένες πλατφόρμες Blockchain, μπορεί να οδηγήσουν σε καθυστερήσεις και μειωμένη απόκριση του συστήματος. Επιπλέον, η αμετάβλητη φύση του Blockchain εγείρει προκλήσεις στη διόρθωση λανθασμένων καταχωρήσεων μόλις καταγραφούν (Anderson & Moore, 2006).

Επίσης, η κυβερνοασφάλεια αποτελεί μια άλλη κρίσιμη πτυχή της αξιοπιστίας. Τα συστήματα ψηφιακής ταυτοποίησης είναι ελκυστικοί στόχοι για κυβερνοεπιθέσεις, συμπεριλαμβανομένων των παραβιάσεων δεδομένων και των επιθέσεων άρνησης παροχής υπηρεσιών. Η διασφάλιση της ασφάλειας αυτών των συστημάτων είναι πρωταρχικής σημασίας, καθώς οι παραβιάσεις μπορούν να

οδηγήσουν σε κλοπή ταυτότητας και απάτη. Οι προηγμένες τεχνικές κρυπτογράφησης, οι τακτικοί έλεγχοι ασφαλείας και η τήρηση των βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας είναι απαραίτητες για την προστασία του συστήματος από τέτοιες απειλές (Wang & Strong, 1996).

Συμπερασματικά, η αξιοπιστία ενός συστήματος ψηφιακής ταυτοποίησης είναι πολύπλευρη, απαιτώντας ισορροπία μεταξύ τεχνολογικής ευρωστίας, επεκτασιμότητας και ασφάλειας. Το Blockchain προσφέρει σημαντικά πλεονεκτήματα από αυτή την άποψη, αλλά η εφαρμογή του πρέπει να συνοδεύεται από συνεχή μέτρα διαχείρισης και ασφάλειας για να διασφαλιστεί ότι το σύστημα παραμένει αξιόπιστο, καθώς κλιμακώνεται και εξελίσσεται.

3.5.2. Προσβασιμότητα

Η προσβασιμότητα αποτελεί μια κρίσιμη απαίτηση για ένα ιδανικό σύστημα ψηφιακής ταυτοποίησης. Διασφαλίζει ότι το σύστημα είναι εύκολα χρησιμοποιήσιμο από όλους τους προβλεπόμενους χρήστες, ανεξάρτητα από την τεχνική τους εμπειρία, τις φυσικές τους ικανότητες ή τη γεωγραφική τους θέση. Αυτή η πτυχή της ψηφιακής ταυτοποίησης δεν αφορά μόνο τη φιλικότητα προς τον χρήστη. Πρόκειται για τη συμπερίληψη και τη διασφάλιση ισότιμης πρόσβασης σε ζωτικές υπηρεσίες.

Στον τομέα της ψηφιακής ταυτοποίησης, η προσβασιμότητα μπορεί να ερμηνευθεί από πολλαπλές οπτικές γωνίες. Πρώτον, συνεπάγεται την ευκολία χρήσης του συστήματος. Η διεπαφή και ο σχεδιασμός της αλληλεπίδρασης πρέπει να είναι διαισθητική και να απευθύνεται σε ένα ευρύ φάσμα χρηστών, συμπεριλαμβανομένων εκείνων που δεν είναι γνώστες της τεχνολογίας. Αυτή η πτυχή τονίζεται στην εργασία του Nielsen (1993) στη μελέτη του με τίτλο "Usability Engineering", όπου τονίζεται η σημασία του σχεδιασμού με επίκεντρο τον χρήστη.

Μια άλλη κρίσιμη πτυχή της προσβασιμότητας είναι η φυσική προσβασιμότητα του συστήματος. Αυτό περιλαμβάνει ζητήματα για τα άτομα με αναπηρίες, διασφαλίζοντας ότι το σύστημα μπορεί να χρησιμοποιηθεί από άτομα με διάφορους τύπους αναπηριών. Η Κοινοπραξία του Παγκόσμιου Ιστού (W3C) παρέχει

οδηγίες για την προσβασιμότητα στον Ιστό, όπως περιγράφεται στις Οδηγίες Προσβασιμότητας Περιεχομένου του Ιστού (WCAG), οι οποίες είναι απαραίτητες για το σχεδιασμό ψηφιακών πλατφόρμων χωρίς αποκλεισμούς (WEC, 2024).

Η γεωγραφική προσβασιμότητα είναι, επίσης, πρωταρχικής σημασίας, ειδικά σε περιοχές με περιορισμένη σύνδεση στο διαδίκτυο ή σε αγροτικές περιοχές. Το ψηφιακό σύστημα ταυτοποίησης θα πρέπει να είναι προσβάσιμο σε διαφορετικά περιβάλλοντα, τα οποία ενδέχεται να απαιτούν λειτουργίες εκτός σύνδεσης ή εναλλακτικές μεθόδους πρόσβασης. Το Πρόγραμμα των Ηνωμένων Εθνών για την Ανάπτυξη (UNDP) συζητά αυτές τις προκλήσεις στις εκθέσεις του για την ψηφιακή ένταξη, τονίζοντας την ανάγκη για προσβάσιμες ψηφιακές λύσεις στις αναπτυσσόμενες περιοχές.

Επιπλέον, το σύστημα θα πρέπει να είναι γλωσσικά προσιτό, προσφέροντας πολύ-γλωσσική υποστήριξη για να εξυπηρετεί χρήστες από διαφορετικά γλωσσικά υπόβαθρα. Αυτό είναι ιδιαίτερα σημαντικό σε χώρες με πολλές επίσημες γλώσσες ή σε συστήματα που προορίζονται για παγκόσμια χρήση. Η σημασία της γλωσσικής προσβασιμότητας σε ψηφιακές πλατφόρμες συζητείται στην έρευνα των Rehm et al. (2016).

Όσον αφορά την τεχνολογία, το Blockchain μπορεί να διαδραματίσει καθοριστικό ρόλο στην ενίσχυση της προσβασιμότητας των συστημάτων ψηφιακής ταυτοποίησης. Ο αποκεντρωμένος χαρακτήρας του μπορεί να διευκολύνει την ευρύτερη πρόσβαση, καθώς δεν βασίζεται σε κεντρική υποδομή που μπορεί να αποτελέσει εμπόδιο σε ορισμένες περιοχές. Ωστόσο, η εφαρμογή του Blockchain πρέπει να λαμβάνει υπόψη τη φιλικότητα προς τον χρήστη και τις διαφορετικές ανάγκες των πιθανών χρηστών (Swan, 2015).

Η προσβασιμότητα στα συστήματα ψηφιακής ταυτοποίησης είναι πολύπλευρη, που περιλαμβάνει τη σχεδίαση διεπαφής χρήστη, τη φυσική και γεωγραφική προσβασιμότητα και τη γλωσσική ενσωμάτωση. Πρόκειται για τη διασφάλιση ότι όλοι, ανεξάρτητα από την τοποθεσία, τις ικανότητες ή το υπόβαθρό τους, μπορούν να έχουν πρόσβαση και να χρησιμοποιούν αποτελεσματικά το σύστημα. Αυτό δεν είναι απλώς μια τεχνική πρόκληση, αλλά και θέμα κοινωνικής ισότητας και κοινωνικής ένταξης.

3.5.3. Έλεγχος Χρήστη & Απόρρητο

Ο έλεγχος του χρήστη και το απόρρητο είναι βασικά στοιχεία στο σχεδιασμό ενός ιδανικού συστήματος ψηφιακής ταυτοποίησης. Αυτές οι πτυχές είναι βαθιά αλληλένδετες, καθώς ο αποτελεσματικός έλεγχος των προσωπικών δεδομένων από τους χρήστες αποτελεί θεμελιώδες στοιχείο του απορρήτου. Στο πλαίσιο της ψηφιακής ταυτοποίησης, ο έλεγχος του χρήστη αναφέρεται στην ικανότητα των ατόμων να διαχειρίζονται τις δικές τους πληροφορίες ταυτότητας, συμπεριλαμβανομένων των δεδομένων που κοινοποιούνται, με ποιον και υπό ποιες συνθήκες (Camenisch & Lysyanskaya, 2001).

Επίσης, το απόρρητο δεν αφορά μόνο τη διατήρηση μυστικών πληροφοριών, αλλά τη διασφάλιση ότι τα προσωπικά δεδομένα χρησιμοποιούνται με τρόπους που συνάδουν με τις προσδοκίες και τη συναίνεση του ατόμου. Αυτή η έννοια του απορρήτου είναι ευθυγραμμισμένη με τις αρχές που ορίζονται σε ορόσημα πλαίσια περί απορρήτου, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση, ο οποίος δίνει έμφαση στα δικαιώματα και τη συναίνεση του υποκειμένου των δεδομένων (Sullivan & Burger, 2017).

Η πρόκληση στα συστήματα ψηφιακής ταυτοποίησης είναι να εξισορροπηθεί ο έλεγχος των χρηστών με την ανάγκη για επαλήθευση και εμπιστοσύνη. Η τεχνολογία Blockchain, που συχνά προτείνεται ως λύση για την ψηφιακή ταυτοποίηση, προσφέρει μερικές ενδιαφέρουσες δυνατότητες από αυτή την άποψη. Ο αποκεντρωμένος χαρακτήρας του μπορεί να παρέχει στους χρήστες περισσότερο έλεγχο των δεδομένων τους, σε αντίθεση με τα παραδοσιακά κεντρικά μοντέλα όπου μια μεμονωμένη οντότητα διατηρεί και διαχειρίζεται προσωπικές πληροφορίες. Ωστόσο, το Blockchain εγείρει, επίσης, μοναδικές ανησυχίες για το απόρρητο, ιδιαίτερα σε δημόσια Blockchain, όπου τα δεδομένα των συναλλαγών είναι ορατά σε όλους τους συμμετέχοντες στο δίκτυο (Mühle et al., 2018).

Για να αντιμετωπιστούν αυτές οι ανησυχίες, υπάρχει ένα αυξανόμενο ενδιαφέρον για τεχνολογίες ενίσχυσης της ιδιωτικής ζωής στα οικοσυστήματα Blockchain, όπως οι αποδείξεις μηδενικής γνώσης. Αυτές οι τεχνολογίες επιτρέπουν την επαλήθευση των πληροφοριών χωρίς να αποκαλύπτονται τα υποκείμενα

δεδομένα, προσφέροντας έναν τρόπο διατήρησης του απορρήτου (Sullivan & Burger, 2017).

Επιπλέον, η έννοια της «αυτοκυριαρχίας ψηφιακής ταυτότητας (SSI)» έχει αναδειχθεί ως παράδειγμα στον χώρο της ψηφιακής ταυτοποίησης. Αυτό το μοντέλο υποστηρίζει ότι τα άτομα έχουν τον πλήρη έλεγχο της ψηφιακής τους ταυτότητας, συμπεριλαμβανομένης της ικανότητας να παρέχουν επαληθεύσιμα διαπιστευτήρια, χωρίς να βασίζονται σε μια κεντρική αρχή έκδοσης. Αυτή η προσέγγιση ευθυγραμμίζεται στενά με τις αρχές ελέγχου του χρήστη και του απορρήτου (Mühle et al., 2018).

Κατά την εφαρμογή αυτών των εννοιών, είναι σημαντικό να ληφθεί υπόψη η εμπειρία του χρήστη. Συστήματα που έχουν σχεδιαστεί με ισχυρά χαρακτηριστικά απορρήτου και ελέγχου, αλλά είναι δύσκολο να χρησιμοποιηθούν, μπορεί να οδηγήσουν σε κακή υιοθέτηση και αναποτελεσματική προστασία του απορρήτου. Ως εκ τούτου, ο σχεδιασμός των διεπαφών χρήστη και η συνολική διαδρομή του χρήστη στα συστήματα ψηφιακής ταυτοποίησης θα πρέπει να είναι διαισθητική και φιλική προς τον χρήστη, επιτρέποντας στα άτομα να κατανοούν και να διαχειρίζονται εύκολα τις ρυθμίσεις απορρήτου και τις προτιμήσεις κοινής χρήσης δεδομένων (Mühle et al., 2018).

Συνοπτικά, ο έλεγχος των χρηστών και το απόρρητο στα συστήματα ψηφιακής ταυτοποίησης αφορούν την ενδυνάμωση των ατόμων με τη διαχείριση των προσωπικών τους δεδομένων, διασφαλίζοντας ότι το απόρρητό τους γίνεται σεβαστό και διατηρείται. Αυτό απαιτεί προσεκτική ισορροπία τεχνολογίας, ρύθμισης και σχεδιασμού με επίκεντρο τον χρήστη, διασφαλίζοντας ότι τα συστήματα δεν είναι μόνο ασφαλή και συμβατά, αλλά και προσβάσιμα και εύχρηστα για τον τελικό χρήστη.

ΚΕΦΑΛΑΙΟ 4: ΤΟ BLOCKCHAIN ΩΣ ΛΥΣΗ ΨΗΦΙΑΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ

4.1. Εισαγωγή Κεφαλαίου

Έχοντας παρουσιάσει τις προκλήσεις και τις απαιτήσεις της ψηφιακής ταυτοποίησης, αυτό το κεφάλαιο εμβαθύνει στο Blockchain ως πιθανή λύση. Εξετάζει την καταλληλότητα του Blockchain για την αντιμετώπιση των προβλημάτων που ταλανίζουν τα παραδοσιακά συστήματα ψηφιακής ταυτοποίησης, αξιοποιώντας τα μοναδικά χαρακτηριστικά του, όπως οι αμετάβλητες εγγραφές και ο αποκεντρωμένος έλεγχος.

Το κεφάλαιο εξετάζει πώς το Blockchain μπορεί να προσφέρει μια πιο ασφαλή, διαφανή και αποτελεσματική μέθοδο για τη διαχείριση ψηφιακών ταυτοτήτων. Εμβαθύνει στις δυνατότητες του Blockchain να ενδυναμώνει τα άτομα, δίνοντάς τους περισσότερο έλεγχο στα προσωπικά τους δεδομένα και μειώνοντας την εξάρτηση από κεντρικές αρχές.

Επιπλέον, το κεφάλαιο αυτό παρουσιάζει μια μελέτη περίπτωσης για τη χρήση του Blockchain στα εκλογικά συστήματα ψηφοφορίας, εξετάζοντας συγκεκριμένα παραδείγματα από τη Σιέρα Λεόνε και την πόλη Zug της Ελβετίας. Αυτές οι περιπτώσεις χρησιμεύουν ως πρακτικές του τρόπου με τον οποίο το Blockchain μπορεί να εφαρμοστεί για τη βελτίωση της διαφάνειας, της ασφάλειας και της εμπιστοσύνης στις εκλογικές διαδικασίες.

4.2. Η Καταλληλόλητα του Blockchain για Ψηφιακή Ταυτοποίηση

Η παρούσα ενότητα διερευνά την καταλληλότητα της τεχνολογίας Blockchain για τα συστήματα ψηφιακής ταυτοποίησης, εξετάζοντας πώς τα μοναδικά χαρακτηριστικά της ευθυγραμμίζονται με τις απαιτήσεις της ασφαλούς και αποτελεσματικής ψηφιακής ταυτοποίησης. Η τεχνολογία Blockchain, που αρχικά σχεδιάστηκε για κρυπτονομίσματα, έχει εγγενείς ιδιότητες που την καθιστούν

κατάλληλη για την ταυτοποίηση ψηφιακών ταυτοτήτων. Αυτά τα χαρακτηριστικά περιλαμβάνουν αμετάβλητες εγγραφές, αποκεντρωμένο έλεγχο, κρυπτογραφική ασφάλεια και διαφάνεια. Στις επόμενες υπό-ενότητες του κεφαλαίου, αναλύεται κάθε ένα από αυτά τα χαρακτηριστικά, εξετάζοντας τα πλεονεκτήματα και τις προκλήσεις τους στο πλαίσιο της ψηφιακής ταυτοποίησης.

4.2.1. Αμετάβλητες Εγγραφές

Η έννοια των αμετάβλητων εγγραφών είναι κεντρική στη συζήτηση της καταλληλότητας του Blockchain για ψηφιακή ταυτοποίηση. Το αμετάβλητο στο πλαίσιο του Blockchain σημαίνει ότι μόλις εισαχθούν δεδομένα στο Blockchain, δεν μπορούν να τροποποιηθούν ή να διαγραφούν. Αυτό το χαρακτηριστικό έχει βαθιές επιπτώσεις στα συστήματα ψηφιακής ταυτοποίησης.

Η αμετάβλητη φύση του Blockchain διασφαλίζει την ακεραιότητα των δεδομένων που αποθηκεύονται σε αυτό. Στην ψηφιακή ταυτοποίηση, αυτό σημαίνει ότι τα αρχεία ταυτότητας, αφού επαληθευτούν και προστεθούν στο Blockchain, δεν μπορούν να παραβιαστούν. Αυτό ενισχύει την εμπιστοσύνη στο σύστημα, καθώς οι χρήστες και τα εξαρτημένα μέρη μπορούν να είναι βέβαιοι ότι οι πληροφορίες δεν έχουν τροποποιηθεί παράνομα. Το έργο των Crosby et al. (2016) με τίτλο “Blockchain technology: Beyond bitcoin” παρέχει πληροφορίες για το πώς η τεχνολογία Blockchain στηρίζει την εμπιστοσύνη στα ψηφιακά συστήματα.

Οι αμετάβλητες εγγραφές επιτρέπουν, επίσης, μια διαφανή και ελεγχόμενη διαδρομή των συναλλαγών. Στην ψηφιακή ταυτοποίηση, κάθε αλλαγή ή προσθήκη στο αρχείο ταυτότητας ενός ατόμου μπορεί να εντοπιστεί μέσω του Blockchain, παρέχοντας ένα σαφές ιστορικό αλληλεπιδράσεων. Αυτή η άποψη συζητείται λεπτομερώς από τους Yli-Huumo et al. (2016) στην εργασία τους με τίτλο “Where Is Current Research on Blockchain Technology? A Systematic Review”.

Η αμετάβλητη φύση του Blockchain θέτει όμως και προκλήσεις, ιδιαίτερα στο πλαίσιο της διόρθωσης δεδομένων και του δικαιώματος στη λήθη, όπως περιγράφεται στον GDPR. Από τη στιγμή που υπάρχουν πληροφορίες στο Blockchain,

η διόρθωση σφαλμάτων ή η αφαίρεση δεδομένων κατόπιν αιτήματος ενός ατόμου καθίσταται προβληματική (Finck, 2018).

Επιπρόσθετα, η αποθήκευση ευαίσθητων πληροφοριών, όπως βιομετρικών δεδομένων, σε ένα αμετάβλητο καθολικό εγείρει ανησυχίες σχετικά με το απόρρητο. Εάν αυτά τα δεδομένα παραβιάζονταν ποτέ, δεν θα μπορούσαν να αφαιρεθούν ή να τροποποιηθούν, οδηγώντας σε πιθανούς μακροπρόθεσμους κινδύνους για το απόρρητο. Αυτή η ανησυχία τονίζεται στην έρευνα του Pilkington (2016).

Για την αντιμετώπιση αυτών των προκλήσεων, ορισμένα συστήματα ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain εξερευνούν υβριδικές προσεγγίσεις. Χαρακτηριστικό παράδειγμα αποτελεί η αποθήκευση αναφορών ή κατακερματισμών δεδομένων ταυτότητας στο Blockchain, αντί για τα ίδια τα πραγματικά δεδομένα, όπως συζητήθηκε από τους Zyskind et al. (2015) στην εργασία τους με τίτλο "Decentralizing privacy: Using blockchain to protect personal data". Αυτή η προσέγγιση επιτρέπει τα οφέλη της αμετάβλητης φύσης, ενώ μετριάζει ορισμένες ανησυχίες σχετικά με το απόρρητο.

Επιπλέον, η έννοια της αποθήκευσης δεδομένων “εκτός Blockchain” κερδίζει έδαφος. Το Blockchain περιέχει δείκτες ή κρυπτογραφικές αποδείξεις για δεδομένα που είναι αποθηκευμένα αλλού. Αυτή η μέθοδος διατηρεί την ακεραιότητα και τη δυνατότητα ελέγχου του Blockchain, ενώ επιτρέπει την ενημέρωση ή την αφαίρεση των δεδομένων, όπως απαιτείται.

Το εξελισσόμενο τοπίο της τεχνολογίας Blockchain βλέπει καινοτομίες που στοχεύουν να εξισορροπήσουν τα οφέλη της αμετάβλητης φύσης με την ανάγκη για ευελιξία και προστασία της ιδιωτικής ζωής στα συστήματα ψηφιακής ταυτοποίησης.

4.2.2. Αποκεντρωμένος Έλεγχος

Ο αποκεντρωμένος έλεγχος είναι ένα καθοριστικό χαρακτηριστικό της τεχνολογίας Blockchain και διαδραματίζει κρίσιμο ρόλο στην καταλληλότητά της για ψηφιακά συστήματα ταυτοποίησης. Σε αντίθεση με τα παραδοσιακά κεντρικά συστήματα, όπου μια μεμονωμένη οντότητα έχει τον έλεγχο ολόκληρου του

συστήματος, το Blockchain κατανέμει τον έλεγχο σε ένα δίκτυο κόμβων. Αυτή η αποκέντρωση έχει πολλές επιπτώσεις για την ψηφιακή ταυτοποίηση.

Η αποκέντρωση στο Blockchain σημαίνει ότι δεν υπάρχει κανένα σημείο αποτυχίας. Αυτό ενισχύει την ασφάλεια και την ανθεκτικότητα του συστήματος έναντι επιθέσεων και τεχνικών αστοχιών. Σε ένα πλαίσιο ψηφιακής ταυτοποίησης, αυτό σημαίνει ότι το σύστημα είναι λιγότερο ευάλωτο σε επιθέσεις που στοχεύουν κεντρικούς αποθηκευτικούς χώρους δεδομένων. Η εργασία των Tapscott και Tapscott (2016) συζητά πώς η αποκέντρωση ενισχύει την ασφάλεια και την ευρωστία των συστημάτων που βασίζονται σε Blockchain.

Ο αποκεντρωμένος έλεγχος συνεπάγεται, επίσης, μειωμένη εξάρτηση από κεντρικές αρχές ή μεσάζοντες. Στην ψηφιακή ταυτοποίηση, αυτό μπορεί να ενδυναμώσει τα άτομα δίνοντάς τους περισσότερο έλεγχο στα δεδομένα ταυτότητάς τους. Οι χρήστες μπορούν να διαχειριστούν τις δικές τους ταυτότητες χωρίς να βασίζονται σε μια κεντρική εξουσία (Tapscott & Tapscott, 2016).

Μία από τις προκλήσεις με τα αποκεντρωμένα συστήματα είναι η καθιέρωση αποτελεσματικής διακυβέρνησης και τυποποίησης. Χωρίς κεντρική αρχή, ο συντονισμός των ενημερώσεων, των προτύπων και των πρωτοκόλλων μπορεί να είναι πολύπλοκος. Αυτό το ζήτημα επισημαίνεται στην έρευνα των De Filippi και Wright (2018) με τίτλο “Blockchain and the Law: The Rule of Code”.

Για την ψηφιακή ταυτοποίηση, η διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων Blockchain είναι, επίσης, ζωτικής σημασίας. Η αποκέντρωση μπορεί να οδηγήσει σε κατακερματισμό, όπου διαφορετικά συστήματα δεν μπορούν να επικοινωνήσουν αποτελεσματικά μεταξύ τους.

Για την αντιμετώπιση αυτών των προκλήσεων, υπάρχει μια αυξανόμενη εστίαση στην ανάπτυξη αποκεντρωμένων, αλλά διαλειτουργικών πλαισίων, για την ψηφιακή ταυτοποίηση. Αυτό περιλαμβάνει τη δημιουργία κοινών προτύπων και πρωτοκόλλων που επιτρέπουν σε διαφορετικά συστήματα Blockchain να αλληλοεπιδρούν απρόσκοπτα. Η Κοινοπραξία του Παγκόσμιου Ιστού (W3C) εργάζεται πάνω σε πρότυπα για αποκεντρωμένα αναγνωριστικά (DID), όπως περιγράφεται στα συνεχιζόμενα έργα και τις δημοσιεύσεις τους.

Επιπλέον, η έννοια των ομοσπονδιακών Blockchain αναδύεται ως λύση για την εξισορρόπηση της αποκέντρωσης με την ανάγκη για κάποιο επίπεδο συντονισμού και διακυβέρνησης. Σε αυτό το μοντέλο, πολλαπλά ανεξάρτητα Blockchain λειτουργούν με συντονισμένο τρόπο, διατηρώντας την αποκέντρωση, ενώ διασφαλίζουν τη διαλειτουργικότητα και τη διακυβέρνηση.

Συμπερασματικά, ο αποκεντρωμένος έλεγχος στο Blockchain προσφέρει σημαντικά πλεονεκτήματα για τα συστήματα ψηφιακής ταυτοποίησης, ιδιαίτερα όσον αφορά την ασφάλεια, την ανθεκτικότητα και την ενδυνάμωση των χρηστών. Ωστόσο, παρουσιάζει, επίσης, προκλήσεις στη διακυβέρνηση, την τυποποίηση και τη διαλειτουργικότητα. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί συνδυασμό τεχνολογικής καινοτομίας, συνεργατικής θέσπισης προτύπων και μοντέλων διακυβέρνησης. Η εξέλιξη της τεχνολογίας Blockchain προς αυτή την κατεύθυνση έχει τη δυνατότητα να φέρει επανάσταση στον τρόπο διαχείρισης και χρήσης των ψηφιακών ταυτοτήτων.

4.3. Μελέτη Περίπτωσης: Η Χρήση του Blockchain στα Εκλογικά Συστήματα Ψηφοφορίας

4.3.1. Γενικά

Η τεχνολογία Blockchain είναι μια τεχνολογία κατανεμημένου καθολικού που παρέχει έναν διαφανή και ασφαλή τρόπο καταγραφής και μεταφοράς δεδομένων. Η ψηφοφορία ως μέρος της εκλογικής διαδικασίας είναι ένα πολύ σημαντικό μέρος της δημοκρατίας επειδή παρέχει στους ανθρώπους την ευκαιρία να εκφράσουν τη γνώμη τους. Η ψηφοφορία με τη χρήση της τεχνολογίας Blockchain έχει ήδη χρησιμοποιηθεί σε οργανισμούς, συμπεριλαμβανομένων πολιτικών κομμάτων και επιχειρήσεων. Ορισμένοι αναφέρουν ότι το Blockchain θα μπορούσε να βοηθήσει τους ψηφοφόρους να αλληλοεπιδράσουν πιο βαθιά και να καταστήσει πιο κατανοητές τις σύνθετες διαδικασίες της εποχής μας (Harsha et al., 2018).

Μια διαδικασία όπου η τεχνολογία Blockchain χρησιμοποιείται στον πολιτικό κόσμο είναι το εκλογικό σύστημα. Μερικές χώρες παγκοσμίως έχουν χρησιμοποιήσει το Blockchain για να βελτιώσουν τα συστήματα ψηφοφορίας τους, δημιουργώντας ένα αποκεντρωμένο δίκτυο P2P με τη βοήθεια ενός δημόσιου καθολικού (Kazeem, 2018).

Η Σιέρα Λεόνε, μια χώρα στη Δυτική Αφρική, έγινε η πρώτη χώρα στον κόσμο που χρησιμοποίησε την τεχνολογία Blockchain για να επαληθεύσει την καταμέτρηση των ψήφων στις εκλογές τον Μάρτιο του 2018. Οι πολίτες ψήφισαν με στυλό και χαρτί και εν συνεχεία, τα ψηφοδέλτια συγκεντρώθηκαν από τους δημόσιους υπαλλήλους, τα οποία εισήγαγαν στο σύστημα χειροκίνητα. Η χρήση του Blockchain που διεξήχθη σε όλη τη διαδικασία ψηφοφορίας ήταν ιδιωτικό και όχι δημόσιο, γεγονός που σημαίνει ότι μόνο εξουσιοδοτημένο προσωπικό μπορούσε να κάνει καταχωρήσεις. Η κυβέρνηση της Σιέρα Λεόνε έχει τη φήμη της διεφθαρμένης και συχνά υπάρχει πολλή βία γύρω από τις εκλογές. Η ψηφοφορία με τη βοήθεια του Blockchain βοήθησε στη διασφάλιση ενός εύρυθμου αποτελέσματος, καθώς το κοινό είχε πρόσβαση στο Blockchain μόνο για ανάγνωση, επιβεβαιώνοντας ότι τα αποτελέσματα της ψηφοφορίας δεν είχαν παραβιαστεί (Kazeem, 2018).

Η αδυναμία διαφοροποίησης ή διαγραφής πληροφοριών από το Blockchain το καθιστά την καλύτερη τεχνολογία για συστήματα ψηφοφορίας. Η τεχνολογία του Blockchain υποστηρίζεται από ένα κατανεμημένο δίκτυο που αποτελείται από πολλούς διασυνδεδεμένους κόμβους, χωρίς να υπάρχει κάποια ενιαία αρχή που να ελέγχει το δίκτυο. Η αποδοχή μιας συναλλαγής εξαρτάται από την επιλογή των περισσότερων κόμβων εντός του Blockchain. Κάθε ένας από αυτούς τους κόμβους έχει το αντίγραφο του κατανεμημένου καθολικού που περιέχει το συνολικό ιστορικό όλων των προηγούμενων και των παρόντων συναλλαγών που έχει επεξεργαστεί το δίκτυο (Harsha et al., 2018).

Στις παραδοσιακές εκλογές, συνήθως έχουμε μια κεντρική αρχή που καταγράφει, μετράει και ελέγχει όλες τις ψήφους, ενώ με το Blockchain η στρατηγική γίνεται τοπική. Έτσι, ο καθένας μπορεί να προσθέσει ένα αντίγραφο του συνολικού αρχείου ψηφοφορίας στις δικές του συσκευές και οι πληροφορίες είναι κρυπτογραφημένες για την προστασία της ταυτότητας μεμονωμένων ψηφοφόρων.

Οι παράνομες ψήφοι δεν μπορούν να προστεθούν και, επίσης, ο λογαριασμός δεν μπορεί να αλλάξει επειδή όλοι έχουν ένα αντίγραφο.

4.3.2. Χρήση του Blockchain στα Εκλογικά Συστήματα Ψηφοφορίας

Τα κύρια στοιχεία ενός σύστημα ηλεκτρονικής ψηφοφορίας με τη χρήση Blockchain είναι τα εξής (Pawar et al., 2019):

- Ψηφοφόρος: Ο ψηφοφόρος διαδραματίζει ρόλο στο σύστημα. Ο ψηφοφόρος εγγράφεται στο σύστημα Blockchain παρέχοντας τα διαπιστευτήριά του, όπως τον αριθμό επιβεβαίωσης ψηφοφορίας, τη διεύθυνση, τον τηλεφωνικό αριθμό επικοινωνίας, κλπ.
- Διαχειριστής εκλογών: Ελέγχει και διαχειρίζεται όλα τα δεδομένα που εισάγει ο ψηφοφόρος αν είναι σωστά ή όχι και παράγει ιδιωτικά και δημόσια κλειδιά για τους ψηφοφόρους.
- Εκλογική διαδικασία: Σε αυτή τη διαδικασία, οι ψηφοφόροι επιλέγουν και ψηφίζουν τον υποψήφιο που προτιμούν.

Κατά τη στιγμή της εγγραφής, η υπηρεσία χρησιμοποιεί έναν μοναδικό αριθμό επιβεβαίωσης ψήφου που παρέχεται από τον ψηφοφόρο. Αυτός ο μοναδικός αριθμός επιβεβαίωσης ψηφοφορίας χρησιμοποιείται για τη δημιουργία ενός μοναδικού δημόσιου και ιδιωτικού κλειδιού για κάθε ψηφοφόρο. Αφού λάβει όλες τις απαραίτητες πληροφορίες από τον ψηφοφόρο, το σύστημα θα ελέγξει εάν ο ψηφοφόρος έχει δικαίωμα ψήφου ή όχι και στη συνέχεια αποδέχεται την εγγραφή του ψηφοφόρου (Harsha et al., 2018).

Κατά τη διάρκεια της εκλογικής διαδικασίας, απαιτείται το ιδιωτικό και το δημόσιο κλειδί για λόγους σύνδεσης και ψήφου για τον προτιμώμενο υποψήφιο. Λειτουργεί ως αναγνωριστικό σύνδεσης και ως κωδικός πρόσβασης κατά τη διαδικασία της ψηφοφορίας. Χρησιμοποιείται, επίσης, για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Αυτά τα δύο κλειδιά έχουν τη μορφή κώδικα, καθιστώντας τα μη αναγνώσιμα για τον χρήστη. Μετά την ολοκλήρωση της διαδικασίας εγγραφής, αυτά τα κλειδιά αποστέλλονται στο καταχωρημένο

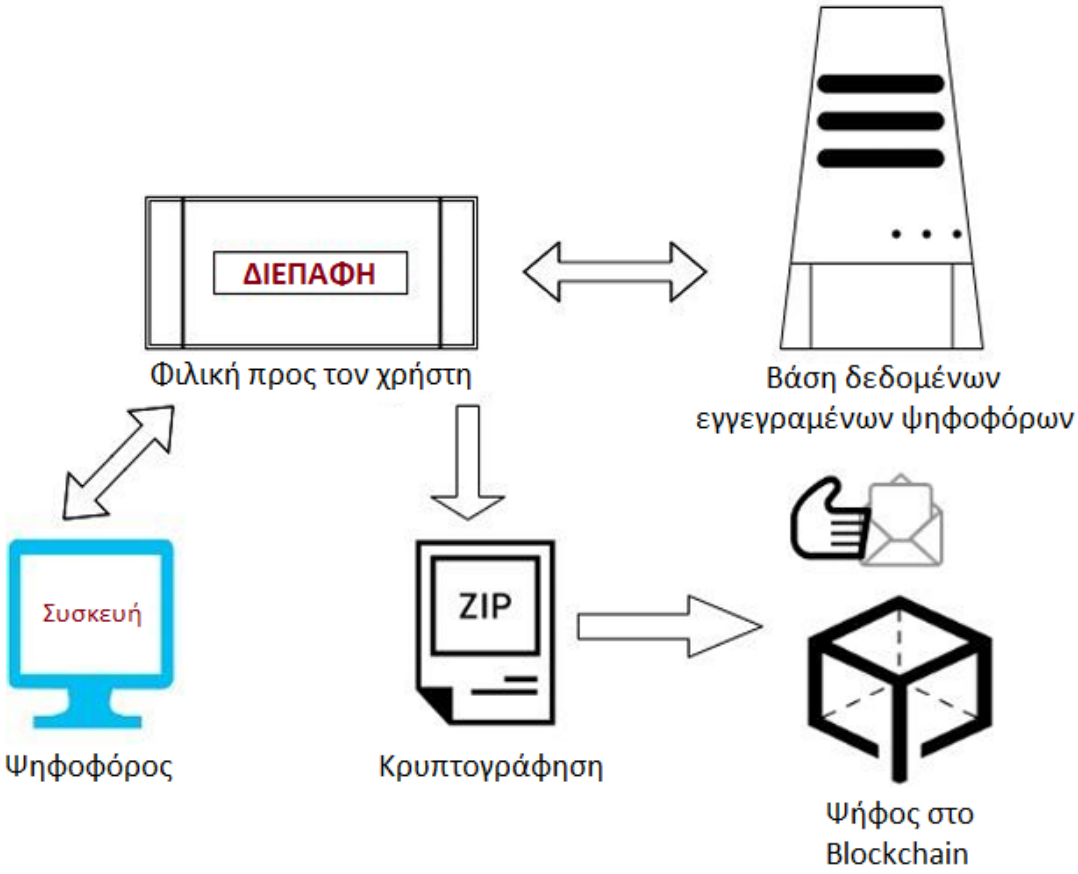
αναγνωριστικό email ή τον αριθμό κινητού τηλεφώνου που παρέχεται από τον ψηφοφόρο (Pawar et al., 2019).

Μετά τον επιτυχή έλεγχο ταυτότητας και την παραγωγή του ιδιωτικού και του δημόσιου κλειδιού, ο ψηφοφόρος συνδέεται στο σύστημα χρησιμοποιώντας αυτά τα κλειδιά. Με την είσοδο στο σύστημα, ο ψηφοφόρος μπορεί να επιλέξει και να δώσει την ψήφο του στον προτιμώμενο υποψήφιο. Αυτό γίνεται μέσω μιας φιλικής προς τον χρήστη διεπαφής. Αφού ο ψηφοφόρος ψηφίσει, το σύστημα δημιουργεί μια είσοδο που περιέχει τον μοναδικό αριθμό αναγνώρισης ψηφοφόρου, ο οποίος δόθηκε αρχικά, ακολουθούμενο από το όνομα της ψήφου με την τιμή κατακερματισμού της προηγούμενης ψήφου. Με αυτόν τον τρόπο κάθε είσοδος, καθώς και κρυπτογραφημένη έξοδος, είναι μοναδικές (Harsha et al., 2018).

Σε κάθε ψηφοφορία, το Blockchain καταγράφει τις κρυπτογραφημένες πληροφορίες. Στη συνέχεια, η ψηφοφορία μετατρέπεται σε ένα μπλοκ που προστίθεται στο σύστημα Blockchain και μεταδίδεται σε κάθε σύστημα του δικτύου. Με αυτόν τον τρόπο, όλοι οι ψηφοφόροι ακολουθούν την ίδια διαδικασία και κάθε μπλοκ προστίθεται στο σύστημα όπου υπολογίζεται η τιμή κατακερματισμού κάθε μπλοκ (Pawar et al., 2019).

Κάθε μπλοκ που υπάρχει στο σύστημα Blockchain περιέχει τα δεδομένα, τον κατακερματισμό του μπλοκ και την τιμή κατακερματισμού του προηγούμενου μπλοκ. Αφού δημιουργηθεί ένα μπλοκ και ανάλογα με τον επιλεγμένο υποψήφιο, οι πληροφορίες καταγράφονται στο αντίστοιχο μπλοκ του Blockchain. Κάθε μπλοκ συνδέεται, επίσης, με την προηγούμενη ψήφο. Καθώς το Blockchain είναι ένα αποκεντρωμένο σύστημα, οι ψήφοι δεν παραβιάζονται και οι χάκερ δεν μπορούν να εισβάλουν εύκολα στο σύστημα Blockchain για να χειραγωγήσουν τις ψήφους. Αφού ολοκληρωθεί όλη η εκλογική διαδικασία, υπολογίζονται οι ψήφοι και ανακοινώνονται τα αποτελέσματα. Η όλη ανωτέρω διαδικασία παρουσιάζεται στο παρακάτω Γράφημα 1.

Γράφημα 1. Το Blockchain ως υπηρεσία ηλεκτρονικής ψηφοφορίας



Πηγή: Harsha et al. (2018)

4.3.3. Η Περίπτωση της Σιέρρα Λεόνε

Τον Μάρτιο του 2018, η Σιέρα Λεόνε έγινε «πρωτοσέλιδο» φιλοξενώντας αυτές που αναφέρθηκαν ως οι πρώτες στον κόσμο εκλογές που βασίζονται στη τεχνολογία Blockchain. Αυτό το πρωτοποριακό γεγονός αντιπροσώπευε μια συγχώνευση παραδοσιακών δημοκρατικών διαδικασιών και τεχνολογίας αιχμής, θέτοντας ενδεχομένως προηγούμενο για μελλοντικές εκλογές παγκοσμίως (Kazeem, 2018).

Η Σιέρα Λεόνε, με ιστορία εκλογικών προκλήσεων, προσπάθησε να ενισχύσει τη διαφάνεια και την αξιοπιστία της εκλογικής της διαδικασίας. Η λύση ήταν η εφαρμογή της τεχνολογίας Blockchain, που είναι κυρίως γνωστή για την υποστήριξη κρυπτονομισμάτων, όπως το Bitcoin. Σε αντίθεση με τις τυπικές βάσεις δεδομένων, το Blockchain προσφέρει έναν αποκεντρωμένο και εξαιρετικά ασφαλή τρόπο καταγραφής πληροφοριών, καθιστώντας σχεδόν αδύνατη την αλλαγή των καταγεγραμμένων δεδομένων χωρίς εντοπισμό (Kazeem, 2018).

Για αυτό το εγχείρημα, η Σιέρα Λεόνε συνεργάστηκε με το Agora, ένα ελβετικό ίδρυμα που ειδικεύεται στις λύσεις ψηφιακής ψηφοφορίας. Το έργο εφαρμόστηκε πιλοτικά στη Δυτική Περιφέρεια, την πολυπληθέστερη περιοχή της Σιέρα Λεόνε. Η διαδικασία ήταν απλή, αλλά καινοτόμος. Οι πολίτες ψήφισαν χρησιμοποιώντας παραδοσιακές χάρτινες κάλπες, οι οποίες στη συνέχεια καταμετρήθηκαν χειροκίνητα. Καθώς καταγράφηκε κάθε ψήφος, τα δεδομένα καταγράφονταν ταυτόχρονα σε Blockchain. Αναλυτικότερα, η διαδικασία ψηφοφορίας είχε ως ακολούθως (Kazeem, 2018):

- Ψηφοφορία: Οι πολίτες ψήφισαν χρησιμοποιώντας παραδοσιακά χάρτινα ψηφοδέλτια.
- Καταμέτρηση: Αφού έκλεισαν οι κάλπες, οι ψήφοι καταμετρήθηκαν χειροκίνητα.
- Καταγραφή στο Blockchain: Καθώς καταμετρήθηκαν οι ψήφοι, τα αποτελέσματα καταγράφηκαν ταυτόχρονα σε ένα Blockchain. Στη διαδικασία αυτή συμμετείχαν εκπρόσωποι από διάφορα κόμματα και παρατηρητές, διασφαλίζοντας τη διαφάνεια.
- Ασφάλεια δεδομένων: Το Blockchain παρείχε ένα ασφαλές και αμετάβλητο αρχείο κάθε ψήφου, αποτρέποντας την παραβίαση ή την αλλαγή.
- Επαλήθευση αποτελεσμάτων: Τα αποτελέσματα που βασίζονταν σε Blockchain ήταν στη συνέχεια διαθέσιμα για επαλήθευση σε πραγματικό χρόνο, διασφαλίζοντας ότι ο επίσημος απολογισμός ταιριάζει με τις μετρήσεις στο Blockchain.

Αυτή η μέθοδος καταγραφής ψήφων σε Blockchain προσέφερε πολλά πλεονεκτήματα, όπως (Kazeem, 2018):

- Πρώτον, έφερε απαράμιλλη διαφάνεια, όπου κάθε καταγεγραμμένη ψήφος μπορούσε να δει και να επαληθευτεί από οποιοδήποτε μέρος, εξαλείφοντας τις αμφιβολίες για παραποίηση ή εσφαλμένη καταμέτρηση ψήφων.
- Δεύτερον, ενίσχυσε την ασφάλεια, αξιοποιώντας την ευρωστία του Blockchain έναντι της παραβίασης δεδομένων. Επιπλέον, το σύστημα υποσχέθηκε αποτελεσματικότητα, επιταχύνοντας τη διαδικασία καταμέτρησης ψήφων και μειώνοντας τα ανθρώπινα λάθη.

Ωστόσο, η πρωτοβουλία δεν ήταν χωρίς προκλήσεις. Σε μια χώρα που παλεύει με τεχνολογικές ανισότητες, η εφαρμογή τέτοιων λύσεων υψηλής τεχνολογίας έθεσε ερωτήματα σχετικά με την προσβασιμότητα και το ψηφιακό χάσμα. Υπήρχε, επίσης, το ζήτημα της εμπιστοσύνης του κοινού και των ενδιαφερομένων. Οι άνθρωποι έπρεπε να κατανοήσουν και να πιστέψουν στην τεχνολογία για να είναι πραγματικά αποτελεσματική. Επιπλέον, το κόστος και η υποδομή που απαιτούνταν για τη δημιουργία και τη συντήρηση ενός τέτοιου συστήματος ήταν σημαντικά (Kazeem, 2018).

Η εκλογική διαδικασία με τη χρήση Blockchain της Σιέρα Λεόνε ήταν κάτι περισσότερο από ένα απλό τεχνολογικό πείραμα. Ήταν ένα σημαντικό βήμα προς την επανεξέταση του τρόπου με τον οποίο η τεχνολογία μπορεί να υπηρετήσει τη δημοκρατία. Αν και δεν αντικατέστησε πλήρως το συμβατικό σύστημα ψηφοφορίας, προσέφερε μια συναρπαστική απόδειξη της ιδέας. Ο κόσμος παρακολούθησε τη Σιέρα Λεόνε να κάνει αυτά τα πρωτοποριακά βήματα, θέτοντας τις βάσεις για ένα μέλλον όπου οι εκλογές θα μπορούσαν να είναι πιο ασφαλείς, διαφανείς και αξιόπιστες, χάρη στη δύναμη της τεχνολογίας Blockchain.

4.3.4. Η Περίπτωση της Πόλης Zug της Ελβετίας

Το 2018, η μικρή ελβετική πόλη Zug, που συχνά αποκαλείται “Crypto Valley” για τη φιλόξενη στάση της απέναντι στις εταιρείες Blockchain και κρυπτονομισμάτων, ξεκίνησε ένα συναρπαστικό πείραμα. Διεξήγαγε μία από τις πρώτες δημοτικές εκλογές που βασίζονται σε Blockchain, ένα έργο που ήταν τόσο μια εισβολή στο

μέλλον της δημοκρατίας όσο και μια απόδειξη του πρωτοποριακού πνεύματος της πόλης στην ψηφιακή καινοτομία (Zug Stadt, 2018).

Το πείραμα της Zug δεν αφορούσε απλώς τη δοκιμή μιας νέας μεθόδου ψηφοφορίας, αλλά τον επανασχεδιασμό ολόκληρης της δημοκρατικής διαδικασίας στην ψηφιακή εποχή. Οι κάτοικοι της Zug προσκλήθηκαν να συμμετάσχουν σε αυτή τη δοκιμή κάνοντας πρώτα εγγραφή για δημιουργία ψηφιακής ταυτότητας. Αυτό το αναγνωριστικό ήταν ασφαλισμένο στο Blockchain του Ethereum, διασφαλίζοντας υψηλό επίπεδο ασφάλειας και γνησιότητας. Η βασική ιδέα ήταν να χρησιμοποιηθεί η τεχνολογία Blockchain για τη δημιουργία ενός συστήματος ψηφοφορίας που δεν ήταν μόνο ασφαλές και αδιάψευστο, αλλά και διαφανές και εύκολο να επαληθευτεί (Zug Stadt, 2018).

Η ίδια η διαδικασία ψηφοφορίας διεξήχθη μέσω μιας ειδικά σχεδιασμένης εφαρμογής για κινητά. Αυτή η προσέγγιση αντικατόπτριζε την κατανόηση της κινητικότητας και της συνδεσιμότητας του σύγχρονου κόσμου, με στόχο να κάνει την ψηφοφορία τόσο προσιτή όσο ο έλεγχος ενός email ή η αποστολή μηνύματος κειμένου. Μετά τη ρίψη των ψήφων, αυτοί κρυπτογραφήθηκαν και καταγράφηκαν στο Blockchain. Αυτή η μέθοδος εξασφάλιζε το απόρρητο και την ακεραιότητα της ψηφοφορίας, ενώ παράλληλα επέτρεπε τη διαφανή και ανεξάρτητη επαλήθευση των εκλογικών αποτελεσμάτων. Αναλυτικότερα, η διαδικασία ψηφοφορίας είχε ως ακολούθως (Zug Stadt, 2018):

- Εγγραφή για έκδοση ψηφιακής ταυτότητας: Οι κάτοικοι έπρεπε να εγγραφούν για ένα ψηφιακό αναγνωριστικό, που δημιουργήθηκε στο Blockchain του Ethereum, το οποίο ήταν συνδεδεμένο με την ταυτότητά τους.
- Πλατφόρμα ψηφοφορίας: Το σύστημα ψηφοφορίας βασίστηκε σε Blockchain και ήταν προσβάσιμο μέσω μιας εφαρμογής για κινητά, όπου οι εγγεγραμμένοι ψηφοφόροι μπορούσαν να ψηφίσουν με ασφάλεια.
- Κρυπτογράφηση και ανωνυμία: Οι ψήφοι κρυπτογραφήθηκαν για να διασφαλιστεί το απόρρητο και να αποφευχθεί η παραβίαση. Το Blockchain παρείχε ένα διαφανές, αλλά ανώνυμο αρχείο κάθε ψήφου.

- Επαλήθευση και αποτελέσματα: Μετά την περίοδο της ψηφοφορίας, τα αποτελέσματα επαληθεύτηκαν και δημοσιεύθηκαν, με το Blockchain να επιτρέπει την ανεξάρτητη επαλήθευση της ακεραιότητας κάθε ψήφου.

Η δοκιμή στη πόλη Zug εξέτασε πολλά βασικά πλεονεκτήματα του Blockchain στην ψηφοφορία. Η ασφάλεια, που αποτελεί πρωταρχικό μέλημα στις εκλογές, ενισχύθηκε από την αποκεντρωμένη φύση του Blockchain, καθιστώντας εξαιρετικά δύσκολο για οποιοδήποτε μεμονωμένο κόμμα να χειραγωγήσει τα αποτελέσματα. Η διαφάνεια ήταν ένα άλλο σημαντικό πλεονέκτημα. Κάθε συναλλαγή στο Blockchain καταγράφηκε και επαληθεύτηκε, αλλά το απόρρητο των ψηφοφόρων εξακολουθούσε να διατηρείται (Zug Stadt, 2018).

Ωστόσο, το πείραμα δεν ήταν χωρίς προκλήσεις. Η κλιμάκωση ενός τέτοιου συστήματος για μεγαλύτερες εκλογές, η διασφάλιση της προσβασιμότητας και της ευκολίας χρήσης του για όλους τους ψηφοφόρους και το πιο σημαντικό, η οικοδόμηση εμπιστοσύνης σε μια νέα τεχνολογία για κάτι τόσο κρίσιμο, όπως η ψηφοφορία, ήταν όλα εμπόδια που έπρεπε να αντιμετωπιστούν. Παρά τις προκλήσεις, η περίπτωση της Zug ήταν ένα κρίσιμο βήμα προς τα εμπρός. Παρουσίασε πώς η τεχνολογία, ιδιαίτερα το Blockchain, θα μπορούσε να χρησιμοποιηθεί για την ενίσχυση της δημοκρατικής διαδικασίας. Ενώ ήταν ένα πείραμα μικρής κλίμακας, η επιτυχία του έθεσε τις βάσεις για μελλοντική εξερεύνηση σχετικά με το πώς μπορεί να χρησιμοποιηθεί η τεχνολογία Blockchain στη διακυβέρνηση, όχι μόνο στην Ελβετία, αλλά και σε όλο τον κόσμο (Zug Stadt, 2018).

Αυτή η πρωτοποριακή πρωτοβουλία στη πόλη Zug λειτούργησε ως πρότυπο για πόλεις και χώρες που εξετάζουν τη χρήση του Blockchain στις εκλογικές τους διαδικασίες. Έδειξε ότι με προσεκτικό σχεδιασμό, ισχυρή τεχνολογία και δέσμευση στις δημοκρατικές αξίες, η ψηφιοποίηση της ψηφοφορίας θα μπορούσε να είναι μια βιώσιμη πορεία προς τα εμπρός. Το πείραμα στη Zug ήταν κάτι περισσότερο από μια απλή δοκιμή τεχνολογίας. ήταν μια ματιά στο μέλλον της δημοκρατίας στην ψηφιακή εποχή.

ΚΕΦΑΛΑΙΟ 5: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ BLOCKCHAIN ΣΤΗ ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ

5.1. Εισαγωγή Κεφαλαίου

Έχοντας διερευνήσει την εφαρμογή του Blockchain στην ψηφιακή ταυτοποίηση, το κεφάλαιο αυτό εμβαθύνει στις ευρείες επιπτώσεις αυτής της τεχνολογικής ενσωμάτωσης. Εξετάζει τόσο τις κοινωνικές όσο και τις οικονομικές και επιχειρηματικές επιπτώσεις, παρέχοντας μια ολιστική άποψη του πώς το Blockchain μπορεί να αναδιαμορφώσει την ψηφιακή ταυτοποίηση σε διάφορες πτυχές.

Στο κοινωνικό μέτωπο, το κεφάλαιο εξετάζει πώς το Blockchain επηρεάζει το απόρρητο και την προσωπική ασφάλεια. Διερευνά πώς η αποκέντρωση και η κρυπτογράφηση του Blockchain μπορούν να ενισχύσουν την προστασία της ιδιωτικής ζωής και να μειώσουν τους κινδύνους παραβίασης δεδομένων. Εξετάζει, επίσης, την έννοια της αυτό-κυρίαρχης ταυτότητας και τον πιθανό ρόλο της στην ενδυνάμωση των ατόμων μέσω του ελέγχου των ψηφιακών τους ταυτοτήτων.

Από οικονομική και επιχειρηματική σκοπιά, το κεφάλαιο αναλύει τη σχέση κόστους-αποτελεσματικότητας των συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain. Εξετάζει τη δυνατότητα μείωσης του λειτουργικού κόστους, βελτίωσης της αποτελεσματικότητας και δημιουργίας νέων επιχειρηματικών μοντέλων. Συζητά, επίσης, τις προκλήσεις που σχετίζονται με το κόστος εφαρμογής και συντήρησης, καθώς και την ανάγκη για προσεκτική εξέταση των οικονομικών επιπτώσεων.

5.2. Κοινωνικός Αντίκτυπος

Η παρούσα ενότητα εξετάζει τον κοινωνικό αντίκτυπο των συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain, εστιάζοντας σε δύο βασικούς τομείς: το απόρρητο και την προσωπική ασφάλεια, καθώς και τη διακυβέρνηση και

τη συμμετοχή των πολιτών. Αυτές οι πτυχές είναι ζωτικής σημασίας για την κατανόηση του ευρύτερου αντίκτυπου της τεχνολογίας Blockchain στην κοινωνία και τον τρόπο με τον οποίο διαμορφώνει την αλληλεπίδραση των ατόμων με τις κυβερνήσεις, τα ιδρύματα και τα προσωπικά τους δεδομένα.

5.2.1. Απόρρητο & Προσωπική Ασφάλεια

Η ενσωμάτωση της τεχνολογίας Blockchain σε συστήματα ψηφιακής ταυτοποίησης έχει βαθιές επιπτώσεις στο απόρρητο και την προσωπική ασφάλεια, που αποτελούν κρίσιμα στοιχεία του κοινωνικού αντίκτυπου τέτοιων τεχνολογιών. Αυτή η ενότητα διερευνά πώς το Blockchain επηρεάζει αυτές τις πτυχές, λαμβάνοντας υπόψη τόσο τα πιθανά οφέλη όσο και τις προκλήσεις.

Τα εγγενή χαρακτηριστικά του Blockchain, όπως η αποκέντρωση και η κρυπτογράφηση, προσφέρουν νέους τρόπους για τη βελτίωση του απορρήτου στα ψηφιακά συστήματα ταυτοποίησης. Με την αποκέντρωση της αποθήκευσης προσωπικών δεδομένων, το Blockchain μειώνει τον κίνδυνο παραβιάσεων δεδομένων μεγάλης κλίμακας που είναι πιο συνηθισμένες σε κεντρικές βάσεις δεδομένων. Αυτή η πτυχή τονίζεται στο έργο των Crosby et al. (2016) με τίτλο "Blockchain technology: Beyond bitcoin", το οποίο συζητά πώς η αρχιτεκτονική του Blockchain μπορεί να ενισχύσει την ασφάλεια των δεδομένων.

Επιπλέον, το Blockchain μπορεί να ενδυναμώσει τα άτομα με μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα. Η έννοια της αυτό-κυρίαρχης ταυτότητας, βασίζεται στην αρχή ότι τα άτομα πρέπει να κατέχουν και να ελέγχουν την ψηφιακή τους ταυτότητα χωρίς να βασίζονται σε εξωτερικές αρχές. Αυτή η προσέγγιση ευθυγραμμίζεται με τις αρχές σχεδιασμού του απορρήτου και μπορεί να βελτιώσει σημαντικά το προσωπικό απόρρητο στα ψηφιακά οικοσυστήματα (Finck, 2018).

Ωστόσο, η εφαρμογή του Blockchain στην ψηφιακή ταυτοποίηση παρουσιάζει, επίσης, μοναδικές προκλήσεις για το απόρρητο. Μία από τις κύριες ανησυχίες είναι η πιθανή μονιμότητα των προσωπικών δεδομένων στο Blockchain. Δεδομένου ότι τα δεδομένα Blockchain είναι αμετάβλητα, μόλις καταγραφούν

προσωπικές πληροφορίες, δεν μπορούν να τροποποιηθούν ή να διαγραφούν, εγείροντας ανησυχίες σχετικά με το δικαίωμα στη λήθη, μια βασική πτυχή των κανονισμών περί απορρήτου, όπως ο GDPR (Finck, 2018).

Επιπλέον, η δυνατότητα διαφάνειας του Blockchain, αν και είναι ευεργετική για έλεγχο και εμπιστοσύνη, μπορεί να είναι ένα δίκοπο μαχαίρι για την προστασία της ιδιωτικής ζωής. Στα δημόσια Blockchain, τα δεδομένα των συναλλαγών είναι ορατά σε όλους τους συμμετέχοντες, τα οποία θα μπορούσαν ενδεχομένως να οδηγήσουν σε παραβιάσεις του απορρήτου εάν δεν διαχειρίζονται σωστά. Αυτή η ανησυχία αντιμετωπίζεται στην έρευνα του Pilkington (2016).

Όσον αφορά την προσωπική ασφάλεια, τα συστήματα ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain μπορούν να προσφέρουν βελτιωμένα χαρακτηριστικά ασφαλείας έναντι κλοπής ταυτότητας και απάτης. Η κρυπτογραφική φύση του Blockchain, όπως περιγράφεται λεπτομερώς από τον Goldreich (2009), παρέχει ένα ισχυρό πλαίσιο για την ασφάλεια των προσωπικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

Ωστόσο, η ασφάλεια των συστημάτων Blockchain δεν είναι αλάνθαστη. Ζητήματα, όπως η διαχείριση κλειδιών και ο κίνδυνος ευπάθειας των έξυπνων συμβολαίων, πρέπει να αντιμετωπίζονται προσεκτικά. Η ασφάλεια των προσωπικών δεδομένων σε συστήματα Blockchain εξαρτάται από την ισχύ των κρυπτογραφικών πρακτικών και την ανθεκτικότητα της υποκείμενης υποδομής (Pilkington, 2016).

Συνοπτικά, ο κοινωνικός αντίκτυπος του Blockchain στην ψηφιακή ταυτοποίηση, ιδιαίτερα όσον αφορά το απόρρητο και την προσωπική ασφάλεια, είναι πολύπλευρος. Ενώ το Blockchain προσφέρει καινοτόμες προσεγγίσεις για τη βελτίωση της ιδιωτικότητας και της ασφάλειας, εισάγει, επίσης, νέες προκλήσεις που πρέπει να αντιμετωπιστούν. Η εξισορρόπηση των πλεονεκτημάτων των χαρακτηριστικών του Blockchain με την προστασία των ατομικών δικαιωμάτων απορρήτου και η διασφάλιση ισχυρής προσωπικής ασφάλειας είναι ζωτικής σημασίας για την υπεύθυνη και αποτελεσματική εφαρμογή συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain. Καθώς αυτή η τεχνολογία συνεχίζει να εξελίσσεται, η συνεχής έρευνα και η προσεκτική εξέταση αυτών των θεμάτων θα είναι ουσιαστικής σημασίας για τη διαμόρφωση του ρόλου της στην κοινωνία.

5.2.2. Διακυβέρνηση & Συμμετοχή των Πολιτών

Η ενσωμάτωση της τεχνολογίας Blockchain σε συστήματα ψηφιακής ταυτοποίησης έχει σημαντικές επιπτώσεις στη διακυβέρνηση και τη συμμετοχή των πολιτών, αναδιαμορφώνοντας τον τρόπο με τον οποίο τα άτομα αλληλοεπιδρούν με τις κυβερνητικές υπηρεσίες και συμμετέχουν σε δραστηριότητες του πολίτη. Αυτή η ενότητα διερευνά τις πιθανές επιπτώσεις και τις προκλήσεις του Blockchain σε αυτούς τους τομείς.

Το Blockchain μπορεί να εξορθολογήσει διάφορες κυβερνητικές διαδικασίες, καθιστώντας τις πιο αποτελεσματικές και διαφανείς. Παρέχοντας ένα ασφαλές και αμετάβλητο καθολικό, το Blockchain μπορεί να βελτιώσει τη διαχείριση των μητρώων του πολίτη, συμπεριλαμβανομένης της ψήφου, της ιδιοκτησίας και της νομικής τεκμηρίωσης (Tapscott & Tapscott, 2016).

Στο πλαίσιο της ψηφιακής ταυτοποίησης, το Blockchain μπορεί να διευκολύνει πιο ασφαλείς και αποτελεσματικές διαδικασίες επαλήθευσης ταυτότητας, μειώνοντας τη γραφειοκρατία και βελτιώνοντας την πρόσβαση στις κρατικές υπηρεσίες. Αυτή η πτυχή είναι ζωτικής σημασίας για την ενίσχυση των αλληλεπιδράσεων πολιτών-κυβέρνησης, όπως υπογραμμίζεται από τους Tapscott και Tapscott (2016).

Το Blockchain μπορεί, επίσης, να διαδραματίσει έναν μετασχηματιστικό ρόλο στη συμμετοχή των πολιτών, ιδιαίτερα στα συστήματα ψηφοφορίας. Με τη χρήση του Blockchain, οι διαδικασίες ψηφοφορίας μπορούν να γίνουν πιο διαφανείς, ασφαλείς και προσβάσιμες, αυξάνοντας ενδεχομένως τη συμμετοχή των ψηφοφόρων και την εμπιστοσύνη στα εκλογικά συστήματα (Finck, 2018). Αυτή η εφαρμογή διερευνάται στη μελέτη περίπτωσης του συστήματος ψηφοφορίας που βασίζεται σε Blockchain της Σιέρα Λεόνε.

Επιπλέον, η ψηφιακή ταυτοποίηση που βασίζεται σε Blockchain μπορεί να δώσει τη δυνατότητα στους πολίτες να έχουν μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα, ενισχύοντας τη δέσμευσή τους και τη συμμετοχή τους στις διαδικασίες του πολίτη. Αυτή η ενδυνάμωση ευθυγραμμίζεται με τις αρχές της δημοκρατικής διακυβέρνησης και της ενεργού συμμετοχής στα κοινά.

Ωστόσο, η εφαρμογή του Blockchain στη διακυβέρνηση και τη συμμετοχή των πολιτών δεν έρχεται χωρίς προκλήσεις. Μια σημαντική ανησυχία είναι το ψηφιακό χάσμα. Η διασφάλιση της ισότιμης πρόσβασης σε συστήματα που βασίζονται σε Blockchain είναι ζωτικής σημασίας. Μια άλλη πρόκληση είναι η ανάγκη για τυποποίηση και διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων Blockchain που χρησιμοποιούνται από διάφορες κυβερνητικές οντότητες. Αυτό είναι απαραίτητο για τη διασφάλιση της απρόσκοπτης αλληλεπίδρασης μεταξύ διαφορετικών υπηρεσιών και τμημάτων (Swan, 2015).

Οι δυνατότητές της τεχνολογίας Blockchain να εξορθολογήσει τις κυβερνητικές διαδικασίες, να αυξήσει τη διαφάνεια και να ενδυναμώσει τους πολίτες είναι σημαντικές. Ωστόσο, η συνειδητοποίηση αυτών των πλεονεκτημάτων απαιτεί την αντιμετώπιση προκλήσεων, όπως το ψηφιακό χάσμα, η τυποποίηση και η διασφάλιση της ασφάλειας και του απορρήτου των συστημάτων Blockchain. Καθώς οι κυβερνήσεις και οι θεσμοί συνεχίζουν να εξερευνούν τις εφαρμογές του Blockchain, η εστίαση σε αυτούς τους τομείς θα είναι ζωτικής σημασίας για τη μεγιστοποίηση του θετικού του αντίκτυπου στη διακυβέρνηση και τη συμμετοχή των πολιτών.

5.3. Οικονομικές & Επιχειρηματικές Επιπτώσεις

Η παρούσα ενότητα εμβαθύνει στις οικονομικές και επιχειρηματικές επιπτώσεις της ενσωμάτωσης της τεχνολογίας Blockchain στα συστήματα ψηφιακής ταυτοποίησης. Εξετάζει την πιθανή σχέση κόστους-αποτελεσματικότητας που προσφέρει το Blockchain, συμπεριλαμβανομένης της μείωσης του λειτουργικού κόστους και της αύξησης της αποτελεσματικότητας, καθώς και τις προκλήσεις κόστους που σχετίζονται με την εφαρμογή και τη συντήρηση του. Επιπλέον, διερευνά τα νέα επιχειρηματικά μοντέλα που μπορούν να προκύψουν από συστήματα ταυτοποίησης που βασίζονται σε Blockchain, όπως οι αποκεντρωμένες υπηρεσίες επαλήθευσης ταυτότητας και οι εφαρμογές διατομεακής ταυτότητας.

5.3.1. Σχέση Κόστους-Αποτελεσματικότητας

Η σχέση κόστους-αποτελεσματικότητας της τεχνολογίας Blockchain σε συστήματα ψηφιακής ταυτοποίησης είναι μια κρίσιμη πτυχή των οικονομικών και επιχειρηματικών συνεπειών της. Αυτή η ενότητα διερευνά τον τρόπο με τον οποίο το Blockchain μπορεί να προσφέρει δυνητικά εξοικονόμηση κόστους και κέρδη αποτελεσματικότητας, ενώ λαμβάνει, επίσης, υπόψη το σχετικό κόστος και τις προκλήσεις.

Ένα από τα κύρια οικονομικά οφέλη του Blockchain στην ψηφιακή ταυτοποίηση είναι η πιθανή μείωση του λειτουργικού κόστους. Τα παραδοσιακά συστήματα ταυτοποίησης περιλαμβάνουν συχνά πολλαπλούς μεσάζοντες και πολύπλοκες υποδομές, με αποτέλεσμα υψηλότερο κόστος. Το Blockchain μπορεί να εξορθολογήσει αυτές τις διαδικασίες παρέχοντας μια αποκεντρωμένη και ασφαλή πλατφόρμα για επαλήθευση ταυτότητας, μειώνοντας πιθανώς την ανάγκη για μεσάζοντες και το σχετικό κόστος (Tapscott & Tapscott, 2016).

Το Blockchain μπορεί, επίσης, να αυξήσει την αποτελεσματικότητα στις διαδικασίες διαχείρισης της ταυτότητας. Η αυτοματοποίηση των διαδικασιών επαλήθευσης μέσω έξυπνων συμβολαίων και η εξάλειψη των περιττών ελέγχων ταυτότητας μπορεί να επιταχύνει σημαντικά τις συναλλαγές και να μειώσει τον διοικητικό φόρτο (Yli-Huumo et al., 2016).

Ενώ το Blockchain μπορεί να προσφέρει μακροπρόθεσμη εξοικονόμηση κόστους, το αρχικό κόστος εφαρμογής του μπορεί να είναι σημαντικό. Η ανάπτυξη μιας υποδομής Blockchain, η διασφάλιση της συμμόρφωσης με τους κανονισμούς και η ενσωμάτωση της τεχνολογίας με τα υπάρχοντα συστήματα απαιτούν σημαντικές επενδύσεις. Επίσης, η συνεχής συντήρηση και η ανάγκη κλιμάκωσης του συστήματος Blockchain, καθώς αυξάνεται η χρήση είναι πρόσθετοι παράγοντες κόστους. Οι προκλήσεις επεκτασιμότητας του Blockchain, ιδιαίτερα για τα δημόσια Blockchain, μπορούν να οδηγήσουν σε αυξημένο κόστος όσον αφορά την υποδομή και την κατανάλωση ενέργειας (Croman et al., 2016).

Η σχέση κόστους-αποτελεσματικότητας του Blockchain εξαρτάται, επίσης ,από τη συγκεκριμένη περίπτωση χρήσης και την εφαρμογή. Οι εξατομικευμένες λύσεις που είναι προσαρμοσμένες στις συγκεκριμένες ανάγκες ενός οργανισμού ή κλάδου μπορούν να μεγιστοποιήσουν την εξοικονόμηση κόστους και τα κέρδη αποτελεσματικότητας (Swan, 2015).

Η τεχνολογία Blockchain έχει τη δυνατότητα να είναι οικονομικά αποδοτική σε συστήματα ψηφιακής ταυτοποίησης μειώνοντας το λειτουργικό κόστος και αυξάνοντας την αποτελεσματικότητα. Ωστόσο, οι οικονομικές και επιχειρηματικές επιπτώσεις είναι πολύπλοκες και περιλαμβάνουν σημαντικές αρχικές επενδύσεις και συνεχές κόστος συντήρησης. Η πραγματική σχέση κόστους-αποτελεσματικότητας του Blockchain θα εξαρτηθεί από διάφορους παράγοντες, συμπεριλαμβανομένης της κλίμακας εφαρμογής, της συγκεκριμένης περίπτωσης χρήσης και της ικανότητας εξισορρόπησης του αρχικού κόστους με τα μακροπρόθεσμα οφέλη. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, η λεπτή κατανόηση αυτών των οικονομικών πτυχών θα είναι ζωτικής σημασίας για οργανισμούς και κυβερνήσεις που εξετάζουν λύσεις ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain.

5.3.2. Επιχειρηματικά Μοντέλα Συστημάτων Ταυτοποίησης που Βασίζονται σε Blockchain

Τα συστήματα ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain έχουν τη δυνατότητα να ενεργοποιήσουν νέα και καινοτόμα επιχειρηματικά μοντέλα σε διάφορους τομείς. Αυτά τα μοντέλα μπορούν να αξιοποιήσουν τα μοναδικά χαρακτηριστικά της τεχνολογίας Blockchain, όπως η αποκέντρωση, η αμετάβλητη φύση του και η διαφάνεια, για να δημιουργήσουν αξία με τρόπους που δεν ήταν δυνατοί με τα παραδοσιακά συστήματα ταυτοποίησης.

Ακολούθως, παρουσιάζονται ορισμένα νέα επιχειρηματικά μοντέλα που ενεργοποιούνται από συστήματα ταυτοποίησης που βασίζονται σε Blockchain (Croman et al., 2016; Swan, 2015):

- Αποκεντρωμένες υπηρεσίες επαλήθευσης ταυτότητας: Το Blockchain επιτρέπει τη δημιουργία αποκεντρωμένων υπηρεσιών επαλήθευσης ταυτότητας, όπου οι χρήστες μπορούν να ελέγχουν και να μοιράζονται τις πληροφορίες ταυτότητάς τους με ασφάλεια. Αυτό το μοντέλο μπορεί να μειώσει την εξάρτηση από κεντρικούς παρόχους ταυτότητας και να δημιουργήσει ευκαιρίες για νέους παίκτες στην αγορά επαλήθευσης ταυτότητας.
- Βελτιωμένη ασφάλεια δεδομένων και υπηρεσίες απορρήτου: Με αυξανόμενες ανησυχίες σχετικά με το απόρρητο και την ασφάλεια των δεδομένων, τα συστήματα ταυτοποίησης που βασίζονται σε Blockchain μπορούν να προσφέρουν βελτιωμένες υπηρεσίες ασφάλειας. Οι επιχειρήσεις μπορούν να αναπτύξουν λύσεις που παρέχουν ασφαλή αποθήκευση ταυτότητας, κρυπτογραφημένη διαχείριση δεδομένων και συναλλαγές ταυτότητας που διατηρούν το απόρρητο.
- Εφαρμογές διατομεακής ταυτότητας: Τα συστήματα ταυτοποίησης που βασίζονται σε Blockchain μπορούν να διευκολύνουν διατομεακές εφαρμογές, όπου μια ενιαία ψηφιακή ταυτότητα μπορεί να χρησιμοποιηθεί σε διάφορους κλάδους, όπως η χρηματοδότηση, η υγειονομική περίθαλψη και οι κρατικές υπηρεσίες. Αυτή η διαλειτουργικότητα μπορεί να οδηγήσει στην ανάπτυξη μιας ολοκληρωμένης πλατφόρμας υπηρεσιών.
- Πλατφόρμες μικρό-διαπίστευσης και επαλήθευσης δεξιοτήτων: Στον εκπαιδευτικό και επαγγελματικό τομέα, το Blockchain μπορεί να ενεργοποιήσει συστήματα μικρό-διαπίστευσης, όπου οι δεξιότητες και τα επιτεύγματα των ατόμων καταγράφονται και επαληθεύονται με ασφάλεια. Αυτό το μοντέλο μπορεί να μεταμορφώσει τις πρακτικές πρόσληψης και επαγγελματικής ανάπτυξης.

Ενώ αυτά τα επιχειρηματικά μοντέλα προσφέρουν ευκαιρίες, παρουσιάζουν, επίσης, και προκλήσεις. Η συμμόρφωση με τους κανονισμούς, ιδιαίτερα στο πλαίσιο των νόμων περί απορρήτου, όπως ο GDPR, αποτελεί σημαντική ανησυχία. Επιπλέον, η υιοθέτηση αυτών των μοντέλων εξαρτάται από την εμπιστοσύνη των χρηστών και την ευρεία αποδοχή της τεχνολογίας Blockchain.

Τα συστήματα ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain ανοίγουν μια σειρά από καινοτόμα επιχειρηματικά μοντέλα που μπορούν να μεταμορφώσουν τον τρόπο διαχείρισης και χρήσης της προσωπικής ταυτότητας σε διαφορετικούς τομείς. Αυτά τα μοντέλα προσφέρουν βελτιωμένη ασφάλεια, απόρρητο και αποτελεσματικότητα, αλλά η επιτυχία τους θα εξαρτηθεί από την πλοήγηση σε ρυθμιστικά τοπία, την οικοδόμηση εμπιστοσύνης των χρηστών και τη διασφάλιση της διαλειτουργικότητας σε διάφορες πλατφόρμες και κλάδους.

ΚΕΦΑΛΑΙΟ 6: ΠΡΟΤΥΠΑ, ΚΑΝΟΝΙΣΤΙΚΗ ΣΥΜΜΟΡΦΩΣΗ & BLOCKCHAIN ΣΤΗΝ ΨΗΦΙΑΚΗ ΤΑΥΤΟΠΟΙΗΣΗ

6.1. Εισαγωγή Κεφαλαίου

Η ενσωμάτωση της τεχνολογίας Blockchain στα συστήματα ψηφιακής ταυτοποίησης παρουσιάζει μια σημαντική ευκαιρία για την ενίσχυση της ασφάλειας, της αποδοτικότητας και της εμπιστοσύνης των χρηστών. Ωστόσο, για να αξιοποιηθεί πλήρως το δυναμικό του Blockchain σε αυτόν τον τομέα, είναι σημαντικό να ληφθούν υπόψη τα υπάρχοντα πρότυπα και κανονιστικά πλαίσια που διέπουν την ψηφιακή ταυτοποίηση. Το κεφάλαιο αυτό εμβαθύνει στη σχέση μεταξύ Blockchain και ψηφιακής ταυτοποίησης, εξετάζοντας τον ρόλο των προτύπων, της κανονιστικής συμμόρφωσης και των αναδυόμενων τεχνολογιών.

Το βασικό επίκεντρο αυτού του κεφαλαίου είναι ο Κανονισμός eIDAS. Ο Κανονισμός eIDAS, που θεσπίστηκε από την Ευρωπαϊκή Ένωση, παρέχει ένα πλαίσιο για την ασφαλή και αξιόπιστη ηλεκτρονική ταυτοποίηση και υπηρεσίες εμπιστοσύνης στις ηλεκτρονικές συναλλαγές. Θα διερευνήσουμε πώς το Blockchain μπορεί να συμβάλει στην επίτευξη των στόχων του eIDAS, όπως η διασφάλιση της διαλειτουργικότητας και η ενίσχυση της ασφάλειας στις διασυνοριακές συναλλαγές.

Επιπλέον, το κεφάλαιο θα εξετάσει τις έννοιες των Αποκεντρωμένων Αναγνωριστικών (DIDs) και των Επαληθεύσιμων Διαπιστευτηρίων (VCs) στο πλαίσιο του Blockchain. Τα DIDs και τα VCs προσφέρουν έναν νέο τρόπο διαχείρισης και επαλήθευσης ψηφιακών ταυτοτήτων, δίνοντας τη δυνατότητα στα άτομα να έχουν μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων. Θα αναλυθούν τα πλεονεκτήματα και οι προκλήσεις που σχετίζονται με την εφαρμογή αυτών των τεχνολογιών, εξετάζοντας τις τεχνικές, κανονιστικές και ηθικές τους επιπτώσεις.

Συνολικά, αυτό το κεφάλαιο στοχεύει να παρέχει μια ολοκληρωμένη κατανόηση του τοπίου των προτύπων, της κανονιστικής συμμόρφωσης και του ρόλου του Blockchain στην ψηφιακή ταυτοποίηση. Εξετάζοντας τις τρέχουσες εξελίξεις και τις μελλοντικές κατευθύνσεις, επιδιώκουμε να ρίξουμε φως στο πώς το Blockchain

μπορεί να συμβάλλει σε ένα πιο ασφαλές, αποδοτικό και φιλικό προς το χρήστη μέλλον για την ψηφιακή ταυτοποίηση.

6.2. Το eIDAS & η Ψηφιακή Ταυτοποίηση

6.2.1. Επισκόπηση Κανονισμού eIDAS

Ο eIDAS είναι ένας Κανονισμός που θεσπίστηκε από την Ευρωπαϊκή Ένωση (Ε.Ε.) για τη δημιουργία ενός πλαισίου για την ασφαλή και αξιόπιστη ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στον ενιαίο ευρωπαϊκό χώρο (European Union, 2014). Ο κανονισμός αυτός έχει ως στόχο να ενισχύσει την εμπιστοσύνη στις διασυνοριακές συναλλαγές, να μειώσει τη γραφειοκρατία και να προωθήσει την ψηφιακή ενιαία αγορά στην Ε.Ε.

Ο Κανονισμός eIDAS καλύπτει ένα ευρύ φάσμα υπηρεσιών, συμπεριλαμβανομένης της ηλεκτρονικής υπογραφής, της ηλεκτρονικής σφραγίδας, της ηλεκτρονικής χρονοσήμανσης, της ηλεκτρονικής υπηρεσίας εγγεγραμμένης παράδοσης και της αυθεντικοποίησης ιστότοπων. Ο Κανονισμός θεσπίζει κοινά πρότυπα και απαιτήσεις για αυτές τις υπηρεσίες, διασφαλίζοντας ότι είναι νομικά αναγνωρισμένες και αποδεκτές σε όλα τα κράτη μέλη της Ε.Ε. (European Union, 2014).

Ένας από τους βασικούς στόχους του eIDAS είναι να διευκολύνει τη διασυνοριακή αναγνώριση των ηλεκτρονικών ταυτοτήτων. Αυτό σημαίνει ότι ένα ηλεκτρονικό αναγνωριστικό που εκδίδεται σε ένα κράτος μέλος θα πρέπει να αναγνωρίζεται και να γίνεται αποδεκτό σε άλλα κράτη μέλη (European Union, 2014). Αυτή η πτυχή είναι ιδιαίτερα σημαντική για την προώθηση των διασυνοριακών υπηρεσιών και τη μείωση των διοικητικών φραγμών για τους πολίτες και τις επιχειρήσεις στην Ε.Ε.

Ο eIDAS διαδραματίζει κρίσιμο ρόλο στην ενίσχυση της εμπιστοσύνης και της ασφάλειας στις ηλεκτρονικές συναλλαγές. Θεσπίζοντας κοινά πρότυπα και απαιτήσεις, ο κανονισμός συμβάλλει στη δημιουργία ενός πιο ασφαλούς και

αξιόπιστου ψηφιακού περιβάλλοντος. Αυτό είναι ιδιαίτερα σημαντικό σε τομείς, όπως η ηλεκτρονική διακυβέρνηση, οι χρηματοπιστωτικές υπηρεσίες και η υγειονομική περίθαλψη, όπου είναι απαραίτητη η ασφαλής και αξιόπιστη ηλεκτρονική ταυτοποίηση (European Union, 2014).

6.2.2. eIDAS 1 έναντι eIDAS 2

Σε αυτή την ενότητα ακολουθεί μια πλήρης ανάλυση του eIDAS 1 έναντι του eIDAS 2. Ο Κανονισμός eIDAS τέθηκε σε ισχύ το 2014, εναρμονίζοντας τα πρότυπα για ηλεκτρονική ταυτοποίηση, ηλεκτρονικές υπογραφές και ηλεκτρονικές σφραγίδες σε ολόκληρη την Ευρωπαϊκή Ένωση (Ε.Ε.). Ο eIDAS 1 εισήγαγε την έννοια των «επιπέδων διασφάλισης» (LoA), διασφαλίζοντας ένα ελάχιστο επίπεδο ασφάλειας για τις ηλεκτρονικές συναλλαγές. Επιπλέον, εισήγαγε την αρχή της αμοιβαίας αναγνώρισης, απαιτώντας από τα κράτη μέλη να αναγνωρίζουν τις ηλεκτρονικές ταυτότητες που εκδίδονται σε άλλα κράτη μέλη. Τα βασικά στοιχεία του eIDAS 1 είναι τα ακόλουθα (European Commission, 2014):

- Εναρμόνιση των προτύπων: Ο eIDAS 1 εναρμόνισε τα πρότυπα για ηλεκτρονική ταυτοποίηση, ηλεκτρονικές υπογραφές και ηλεκτρονικές σφραγίδες σε ολόκληρη την Ευρωπαϊκή Ένωση, διασφαλίζοντας ένα συνεπές πλαίσιο για τις ψηφιακές συναλλαγές.
- Επίπεδα διασφάλισης (LoA): Ο κανονισμός εισήγαγε την έννοια των επιπέδων διασφάλισης (LoA), τα οποία καθορίζουν διαφορετικά επίπεδα ασφάλειας για τις ηλεκτρονικές συναλλαγές. Αυτά τα επίπεδα κυμαίνονται από χαμηλό (LoA 1) έως υψηλό (LoA 4), επιτρέποντας στις επιχειρήσεις και τους χρήστες να επιλέξουν το κατάλληλο επίπεδο ασφάλειας για τις συγκεκριμένες ανάγκες τους.
- Αμοιβαία αναγνώριση ηλεκτρονικών ταυτοτήτων: Ο eIDAS 1 καθιέρωσε την αρχή της αμοιβαίας αναγνώρισης, απαιτώντας από τα κράτη μέλη να αναγνωρίζουν τις ηλεκτρονικές ταυτότητες που εκδίδονται σε άλλα κράτη μέλη. Αυτή η αρχή είναι ζωτικής σημασίας για τη διευκόλυνση των

διασυνοριακών υπηρεσιών και τη μείωση των διοικητικών φραγμών για τους πολίτες και τις επιχειρήσεις στην Ευρωπαϊκή Ένωση.

- Δημιουργία ενός πλαισίου για ηλεκτρονικές υπηρεσίες εμπιστοσύνης (eIDAS trust services): Ο κανονισμός δημιούργησε ένα πλαίσιο για ηλεκτρονικές υπηρεσίες εμπιστοσύνης, όπως ηλεκτρονικές υπογραφές, ηλεκτρονικές σφραγίδες, ηλεκτρονική χρονοσήμανση, ηλεκτρονική συστημένη επιστολή και έλεγχος ταυτότητας ιστότοπου. Αυτές οι υπηρεσίες διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της ασφάλειας και της εγκυρότητας των ηλεκτρονικών συναλλαγών.

Ο eIDAS 2, που προτάθηκε το 2021, επιδιώκει να εκσυγχρονίσει το υφιστάμενο πλαίσιο για να αντιμετωπίσει τις εξελισσόμενες ψηφιακές προκλήσεις. Εισάγει την έννοια του «Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας» (European Digital Identity Wallet), επιτρέποντας στους πολίτες να αποθηκεύουν και να χρησιμοποιούν την ψηφιακή τους ταυτότητα σε διάφορες διαδικτυακές και εκτός σύνδεσης υπηρεσίες. Ο eIDAS 2 στοχεύει, επίσης, στην ενίσχυση της ασφάλειας και της διαλειτουργικότητας των ηλεκτρονικών ταυτοτήτων, καθώς και στην επέκταση του πεδίου εφαρμογής του eIDAS για να καλύψει νέες τεχνολογίες και υπηρεσίες. Τα βασικά στοιχεία του eIDAS 2 είναι τα ακόλουθα (European Commission, 2021):

- Εισαγωγή του Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας: Ο eIDAS 2 εισάγει το Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας, το οποίο θα επιτρέπει στους πολίτες της ΕΕ να έχουν έναν ασφαλή και βολικό τρόπο για να αποθηκεύουν, να διαχειρίζονται και να χρησιμοποιούν τις ψηφιακές τους ταυτότητες σε διάφορες διαδικτυακές και εκτός σύνδεσης υπηρεσίες.
- Ενίσχυση της ασφάλειας και της διαλειτουργικότητας των ηλεκτρονικών ταυτοτήτων: Ο eIDAS 2 στοχεύει στην ενίσχυση της ασφάλειας και της διαλειτουργικότητας των ηλεκτρονικών ταυτοτήτων μέσω της χρήσης προηγμένων τεχνολογιών, όπως η κρυπτογραφία και το Blockchain. Αυτό θα διασφαλίσει ότι οι ψηφιακές ταυτότητες είναι ασφαλείς, αξιόπιστες και μπορούν να χρησιμοποιηθούν σε διαφορετικές πλατφόρμες και συστήματα

- Επέκταση του πεδίου εφαρμογής του eIDAS: Ο eIDAS 2 επεκτείνει το πεδίο εφαρμογής του αρχικού κανονισμού για να καλύψει νέες τεχνολογίες και υπηρεσίες, όπως η τεχνητή νοημοσύνη (AI) και το Διαδίκτυο των πραγμάτων (IoT). Αυτή η επέκταση θα διασφαλίσει ότι ο κανονισμός παραμένει επίκαιρος και σχετικός με τις εξελισσόμενες ψηφιακές τεχνολογίες.
- Ενίσχυση της εμπιστοσύνης και της ασφάλειας: Ο eIDAS 2 επιδιώκει να ενισχύσει περαιτέρω την εμπιστοσύνη και την ασφάλεια στις διασυνοριακές ψηφιακές συναλλαγές μέσω αυστηρότερων απαιτήσεων ασφάλειας, βελτιωμένων μηχανισμών εποπτείας και αυξημένης διαφάνειας.

Ακολούθως, παρουσιάζεται ο Πίνακας 1, όπου πραγματοποιείται μια συγκριτική ανάλυση των eIDAS 1 και eIDAS 2.

Πίνακας 1. Συγκριτική ανάλυση eIDAS 1 και eIDAS 2

Χαρακτηριστικό	eIDAS 1	eIDAS 2
Έναρξη Ισχύος	2014	(Αναμένεται) 2024
Εστίαση	Εναρμόνιση προτύπων, αμοιβαία αναγνώριση	Εκσυγχρονισμός, επέκταση πεδίου εφαρμογής
Βασικά Στοιχεία	Επίπεδα διασφάλισης, ηλεκτρονικές υπηρεσίες εμπιστοσύνης	Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας, ενισχυμένη ασφάλεια
Στόχοι	Ελάχιστα πρότυπα ασφάλειας, διασυνοριακή αναγνώριση	Βελτιωμένη εμπιστοσύνη, ασφαλείς ψηφιακές συναλλαγές

Πηγή: European Commission (2014,2021)

6.2.3. Ο Ρόλος του Blockchain στο eIDAS

Η τεχνολογία Blockchain, με την αποκεντρωμένη και κρυπτογραφημένη φύση της, έχει τη δυνατότητα να ενισχύσει σημαντικά την ασφάλεια και την εμπιστοσύνη στο πλαίσιο του eIDAS. Το Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός αξιόπιστου και διαφανούς μητρώου των ηλεκτρονικών ταυτοτήτων, καθιστώντας πιο δύσκολη την παραποίηση ή την κλοπή των δεδομένων ταυτότητας (Nakamoto, 2008). Αναλυτικότερα:

- Ασφάλεια και αμεταβλητότητα: Το Blockchain προσφέρει ένα υψηλό επίπεδο ασφάλειας και αμεταβλητότητας, καθιστώντας εξαιρετικά δύσκολη την αλλοίωση των αποθηκευμένων δεδομένων. Αυτό είναι ιδιαίτερα σημαντικό για ευαίσθητα δεδομένα, όπως οι ηλεκτρονικές ταυτότητες (Buterin, 2014). Η αμετάβλητη φύση του Blockchain διασφαλίζει ότι μόλις καταγραφούν τα δεδομένα στο καθολικό, δεν μπορούν να αλλάξουν, εξασφαλίζοντας έτσι την ακεραιότητα των ψηφιακών ταυτοτήτων.
- Αποκέντρωση και διαφάνεια: Η αποκεντρωμένη φύση του Blockchain διασφαλίζει ότι κανένας κεντρικός φορέας δεν ελέγχει τα δεδομένα, μειώνοντας τον κίνδυνο κατάχρησης ή παραβίασης. Επιπλέον, η διαφάνεια του Blockchain επιτρέπει τον έλεγχο και την επαλήθευση των δεδομένων από όλα τα εμπλεκόμενα μέρη (Swan, 2015). Αυτή η αποκέντρωση μπορεί να ενισχύσει την εμπιστοσύνη στο σύστημα, καθώς κανένας μεμονωμένος φορέας δεν έχει απόλυτο έλεγχο στα δεδομένα ταυτότητας.
- Κρυπτογραφική Ασφάλεια: Το Blockchain χρησιμοποιεί ισχυρή κρυπτογραφία για την προστασία των δεδομένων, καθιστώντας εξαιρετικά δύσκολη την αποκρυπτογράφηση ή την παραβίαση των πληροφοριών ταυτότητας. Αυτό το επίπεδο ασφάλειας είναι ζωτικής σημασίας για την προστασία των ευαίσθητων προσωπικών δεδομένων που σχετίζονται με τις ψηφιακές ταυτότητες.
- Μείωση Κόστους και Αποδοτικότητα: Η τεχνολογία Blockchain μπορεί να βοηθήσει στη μείωση του κόστους που σχετίζεται με τη διαχείριση και την

επαλήθευση των ψηφιακών ταυτοτήτων. Αυτοματοποιώντας τις διαδικασίες επαλήθευσης και εξαλείφοντας την ανάγκη για μεσάζοντες, το Blockchain μπορεί να εξορθολογήσει τις διαδικασίες και να τις κάνει πιο αποτελεσματικές.

Η τεχνολογία Blockchain μπορεί να εφαρμοστεί σε διάφορες πτυχές του eIDAS και συγκεκριμένα:

- Διαχείριση ηλεκτρονικών ταυτοτήτων: Το Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός ασφαλούς και διαφανούς συστήματος διαχείρισης ηλεκτρονικών ταυτοτήτων, όπου οι χρήστες έχουν τον έλεγχο των δεδομένων τους και μπορούν να επιλέξουν με ποιον θα τα μοιραστούν (European Commission, 2021). Αυτό ενισχύει την ιδιωτικότητα των χρηστών και δίνει τη δυνατότητα μεγαλύτερου ελέγχου των προσωπικών τους πληροφοριών.
- Ηλεκτρονικές υπογραφές και σφραγίδες: Το Blockchain μπορεί να χρησιμοποιηθεί για την επικύρωση και την καταγραφή ηλεκτρονικών υπογραφών και σφραγίδων, διασφαλίζοντας την αυθεντικότητα και την ακεραιότητά τους (Zyskind et al., 2015). Αυτό μπορεί να βοηθήσει στην πρόληψη της απάτης και να διασφαλίσει τη νομική εγκυρότητα των ηλεκτρονικών εγγράφων.
- Ηλεκτρονικές υπηρεσίες εμπιστοσύνης: Το Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός αποκεντρωμένου συστήματος ηλεκτρονικών υπηρεσιών εμπιστοσύνης, όπως η χρονοσήμανση και η επικύρωση ψηφιακών πιστοποιητικών (Christidis & Devetsikiotis, 2016). Αυτό μπορεί να αυξήσει την ασφάλεια και την αξιοπιστία αυτών των υπηρεσιών.

Παρά το σημαντικό δυναμικό του, η ενσωμάτωση του Blockchain στο eIDAS αντιμετωπίζει προκλήσεις, όπως η επεκτασιμότητα, η διαλειτουργικότητα και η κανονιστική συμμόρφωση. Ωστόσο, η συνεχής έρευνα και ανάπτυξη στον τομέα του Blockchain αναμένεται να ξεπεράσει αυτές τις προκλήσεις και να ανοίξει το δρόμο για ένα πιο ασφαλές και αξιόπιστο ψηφιακό μέλλον (European Union Agency for Cybersecurity, 2020).

6.3. Αποκεντρωμένα Αναγνωριστικά (DIDs) & Επαληθεύσιμα Διαπιστευτήρια (VCs)

6.3.1. Επισκόπηση DIDs & VCs

Τα Αποκεντρωμένα Αναγνωριστικά (DIDs) και τα Επαληθεύσιμα Διαπιστευτήρια (VCs) είναι θεμελιώδεις έννοιες στο πλαίσιο της ψηφιακής ταυτοποίησης που βασίζεται σε blockchain. Προσφέρουν έναν νέο τρόπο διαχείρισης και επαλήθευσης ψηφιακών ταυτοτήτων, δίνοντας τη δυνατότητα στα άτομα να έχουν μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων.

Τα DIDs είναι ένα νέο είδος αναγνωριστικού που επιτρέπει σε άτομα, οργανισμούς ή ακόμα και αντικείμενα να έχουν μια μοναδική, επαληθεύσιμη και αποκεντρωμένη ψηφιακή ταυτότητα. Σε αντίθεση με τα παραδοσιακά αναγνωριστικά, όπως τα ονόματα χρηστών ή οι αριθμοί κοινωνικής ασφάλισης, τα DIDs δεν ελέγχονται από κάποια Κεντρική Αρχή, αλλά αποθηκεύονται σε ένα αποκεντρωμένο σύστημα, όπως το Blockchain (W3C, 2022). Κάθε DID είναι μια μοναδική συμβολοσειρά χαρακτήρων που συνδέεται με ένα σύνολο κρυπτογραφικών κλειδιών. Αυτά τα κλειδιά επιτρέπουν στον κάτοχο του DID να αποδείξει τον έλεγχο της ψηφιακής του ταυτότητας και να υπογράψει και να επαληθεύσει ψηφιακά διαπιστευτήρια.

Τα DIDs διαθέτουν τα ακόλουθα χαρακτηριστικά/πλεονεκτήματα:

- Αυτοκυριαρχία: Τα DIDs δίνουν στους χρήστες τον πλήρη έλεγχο της ψηφιακής τους ταυτότητας. Οι χρήστες μπορούν να αποφασίσουν ποια δεδομένα θα μοιραστούν, με ποιον και πότε. Αυτό ενισχύει την προστασία της ιδιωτικής ζωής και δίνει τη δυνατότητα στους χρήστες να διαχειρίζονται τα προσωπικά τους δεδομένα (Allen, 2016).
- Ασφάλεια και ιδιωτικότητα: Τα DIDs χρησιμοποιούν κρυπτογραφία για να προστατεύσουν τα δεδομένα των χρηστών και να διασφαλίσουν την ιδιωτικότητά τους. Αυτό μειώνει τον κίνδυνο κλοπής ταυτότητας και απάτης,

καθώς τα δεδομένα είναι κρυπτογραφημένα και προσβάσιμα μόνο από εξουσιοδοτημένα μέρη (Hardman & Pentland, 2019).

- Διαλειτουργικότητα: Τα DIDs είναι σχεδιασμένα να είναι διαλειτουργικά, επιτρέποντας τη χρήση τους σε διαφορετικές πλατφόρμες και εφαρμογές (Sporny et al., 2019). Αυτό σημαίνει ότι οι χρήστες μπορούν να χρησιμοποιούν την ψηφιακή τους ταυτότητα σε διάφορους τομείς και υπηρεσίες χωρίς να χρειάζεται να δημιουργούν και να διαχειρίζονται πολλαπλές ταυτότητες.

Τα VCs είναι ψηφιακά έγγραφα που περιέχουν πληροφορίες σχετικά με ένα άτομο, οργανισμό ή αντικείμενο. Αυτές οι πληροφορίες μπορούν να είναι οτιδήποτε, από προσωπικά δεδομένα και επαγγελματικά προσόντα έως εκπαιδευτικά πιστοποιητικά ή άδειες. Στην ουσία, είναι ψηφιακές εκδόσεις φυσικών διαπιστευτηρίων, όπως πτυχία πανεπιστημίου ή άδειες οδήγησης. Τα VCs είναι κρυπτογραφικά υπογεγραμμένα και συνδέονται με ένα DID, διασφαλίζοντας την αυθεντικότητα και την ακεραιότητά τους (W3C, 2022).

Τα VCs διαθέτουν τα ακόλουθα χαρακτηριστικά/πλεονεκτήματα:

- Επαληθευσιμότητα: Τα VCs μπορούν να επαληθευτούν από οποιονδήποτε, χωρίς να χρειάζεται επικοινωνία με τον εκδότη του διαπιστευτηρίου (Camenisch & Lysyanskaya, 2004). Αυτό καθιστά τη διαδικασία επαλήθευσης ταχύτερη και πιο αποτελεσματική, καθώς οι επαληθευτές μπορούν να επιβεβαιώσουν την αυθεντικότητα ενός VC χρησιμοποιώντας κρυπτογραφικές αποδείξεις.
- Φορητότητα: Οι χρήστες μπορούν να αποθηκεύουν τα VCs τους σε ένα ψηφιακό πορτοφόλι και να τα μοιράζονται με άλλους όταν χρειάζεται (Preukschat & Reed, 2017). Αυτό παρέχει ευκολία και ευελιξία στη διαχείριση και κοινή χρήση ψηφιακών διαπιστευτηρίων, καθώς οι χρήστες μπορούν να έχουν πρόσβαση και να παρουσιάζουν τα διαπιστευτήριά τους από οποιαδήποτε συσκευή με σύνδεση στο διαδίκτυο.
- Επιλεκτική αποκάλυψη: Οι χρήστες μπορούν να επιλέξουν ποια μέρη ενός VC θα αποκαλύψουν, προστατεύοντας την ιδιωτικότητα τους (Paquin & Zaverucha, 2019). Αυτό επιτρέπει στους χρήστες να μοιράζονται μόνο τις

απαραίτητες πληροφορίες για μια συγκεκριμένη συναλλαγή ή αλληλεπίδραση, ελαχιστοποιώντας τον κίνδυνο υπερβολικής κοινοποίησης δεδομένων.

Ο συνδυασμός των DIDs και των VCs δημιουργεί ένα ισχυρό εργαλείο για την ψηφιακή εποχή. Επιτρέπει στους χρήστες να έχουν τον έλεγχο της ψηφιακής τους ταυτότητας, να προστατεύουν την ιδιωτικότητα τους και να μοιράζονται πληροφορίες με ασφάλεια και εμπιστοσύνη. Αυτή η τεχνολογία έχει τη δυνατότητα να μεταμορφώσει τον τρόπο που αλληλοεπιδρούμε στο διαδίκτυο, δημιουργώντας ένα πιο αξιόπιστο και χωρίς αποκλεισμούς ψηφιακό περιβάλλον.

6.3.2. Προκλήσεις & Εκτιμήσεις

Η υιοθέτηση και η εφαρμογή των DIDs και VCs, παρά τα πλεονεκτήματά τους, δεν είναι χωρίς προκλήσεις. Αυτές οι προκλήσεις εκτείνονται σε τεχνολογικές, κοινωνικές και νομικές πτυχές και απαιτούν προσεκτική εξέταση για την επιτυχή ενσωμάτωσή τους στα συστήματα ψηφιακής ταυτοποίησης.

Όσον αφορά τις τεχνολογικές προκλήσεις των DIDs και των VCs, αυτές είναι οι ακόλουθες:

- Επεκτασιμότητα και απόδοση: Η τεχνολογία Blockchain, που συχνά χρησιμοποιείται για την αποθήκευση και επαλήθευση DIDs και VCs, αντιμετωπίζει προκλήσεις επεκτασιμότητας και απόδοσης. Η επεκτασιμότητα αναφέρεται στην ικανότητα του δικτύου να χειρίζεται έναν αυξανόμενο αριθμό συναλλαγών και χρηστών. Για την ευρεία υιοθέτηση των DIDs και VCs, είναι απαραίτητο να αναπτυχθούν λύσεις που μπορούν να διαχειριστούν μεγάλο όγκο συναλλαγών και δεδομένων με αποδοτικό τρόπο. Αυτό περιλαμβάνει τη βελτιστοποίηση των αλγορίθμων συναίνεσης, την εξερεύνηση λύσεων εκτός αλυσίδας και την εφαρμογή τεχνικών διαμοιρασμού για τη διανομή του υπολογιστικού φόρτου (Croman et al., 2016).

- Διαλειτουργικότητα: Η διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων DIDs και VCs είναι ζωτικής σημασίας για την επιτυχία τους. Τα DIDs και τα VCs πρέπει να λειτουργούν απρόσκοπτα σε διάφορες πλατφόρμες, εφαρμογές και τομείς. Η ανάπτυξη κοινών προτύπων και πρωτοκόλλων είναι απαραίτητη για να διασφαλιστεί ότι τα DIDs και τα VCs μπορούν να ανταλλάσσονται και να επαληθεύονται εύκολα σε διαφορετικά συστήματα (Sporny et al., 2019).
- Ασφάλεια: Η ασφάλεια των DIDs και των VCs είναι πρωταρχικής σημασίας, καθώς περιέχουν ευαίσθητα προσωπικά δεδομένα. Η προστασία αυτών των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, παραβίαση και κλοπή ταυτότητας απαιτεί ισχυρούς μηχανισμούς ασφαλείας. Αυτό περιλαμβάνει την εφαρμογή προηγμένων κρυπτογραφικών τεχνικών, ασφαλών πρακτικών αποθήκευσης και συνεχείς ελέγχους ασφαλείας για την αντιμετώπιση πιθανών ευπαθειών (Hardman & Pentland, 2019).

Όσον αφορά τις κοινωνικές και νομικές προκλήσεις των DIDs και των VCs, αυτές είναι οι ακόλουθες:

- Εμπιστοσύνη και υιοθέτηση: Η οικοδόμηση εμπιστοσύνης στα DIDs και VCs είναι απαραίτητη για την ευρεία υιοθέτησή τους. Οι χρήστες πρέπει να είναι σίγουροι ότι τα δεδομένα τους είναι ασφαλή, ότι τα VCs που λαμβάνουν είναι γνήσια και ότι το σύστημα στο οποίο βασίζονται είναι αξιόπιστο. Αυτό απαιτεί διαφάνεια, εκπαίδευση των χρηστών και συνεργασία μεταξύ των ενδιαφερομένων για την προώθηση της κατανόησης και της αποδοχής αυτών των νέων τεχνολογιών.
- Νομικό πλαίσιο: Η ανάπτυξη ενός σαφούς και συνεπούς νομικού πλαισίου για τα DIDs και τα VCs είναι απαραίτητη για την αντιμετώπιση ζητημάτων όπως η ευθύνη, η προστασία των καταναλωτών και η διασυνοριακή αναγνώριση. Οι νομικοί και οι υπεύθυνοι χάραξης πολιτικής πρέπει να συνεργαστούν για να δημιουργήσουν ένα ρυθμιστικό περιβάλλον που να προωθεί την καινοτομία, διασφαλίζοντας παράλληλα την προστασία των δικαιωμάτων και των συμφερόντων των χρηστών.

- Ψηφιακός αποκλεισμός: Είναι σημαντικό να διασφαλιστεί ότι τα DIDs και τα VCs είναι προσβάσιμα σε όλους, ανεξάρτητα από την τεχνολογική τους ικανότητα ή το κοινωνικοοικονομικό τους υπόβαθρο. Αυτό απαιτεί την ανάπτυξη φιλικών προς τον χρήστη διεπαφών, την παροχή υποστήριξης και εκπαίδευσης και τη διασφάλιση ότι η τεχνολογία είναι προσιτή σε άτομα με αναπηρίες ή περιορισμένη πρόσβαση σε τεχνολογικούς πόρους.

Τα DIDs και VCs έχουν τη δυνατότητα να μεταμορφώσουν τον τρόπο που διαχειριζόμαστε την ψηφιακή μας ταυτότητα, προσφέροντας μεγαλύτερη ασφάλεια, ιδιωτικότητα και έλεγχο στους χρήστες. Εάν δεν αντιμετωπιστούν οι προκλήσεις που αναφέρθηκαν παραπάνω, τα DIDs και VCs θα μπορούσαν να οδηγήσουν σε αυξημένο κίνδυνο παραβίασης της ιδιωτικής ζωής, αποκλεισμού και απάτης.

ΚΕΦΑΛΑΙΟ 7: ΠΡΟΚΛΗΣΕΙΣ & ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

7.1. Εισαγωγή Κεφαλαίου

Ενώ η τεχνολογία Blockchain υπόσχεται να φέρει επανάσταση στην ψηφιακή ταυτοποίηση, η εφαρμογή της δεν έρχεται χωρίς προκλήσεις. Το κεφάλαιο αυτό εμβαθύνει σε αυτές τις προκλήσεις, εξετάζοντας τόσο τις τεχνικές όσο και τις ηθικές πτυχές. Επιπλέον, το κεφάλαιο διερευνά τις μελλοντικές προοπτικές του Blockchain στην ψηφιακή ταυτοποίηση, ρίχνοντας φως στις αναδυόμενες τάσεις και στους πιθανούς τομείς έρευνας.

Στο τεχνικό μέτωπο, το κεφάλαιο εξετάζει ζητήματα επεκτασιμότητας που σχετίζονται με την ικανότητα του Blockchain να χειρίζεται μεγάλο όγκο συναλλαγών. Συζητά, επίσης, ηθικά ζητήματα που σχετίζονται με τη διακυβέρνηση δεδομένων και την ανάγκη εξισορρόπησης της διαφάνειας με το απόρρητο.

Κοιτάζοντας το μέλλον, το κεφάλαιο εξετάζει τις αναδυόμενες τάσεις στην τεχνολογία Blockchain, όπως η ενσωμάτωσή της με την Τεχνητή Νοημοσύνη και το Διαδίκτυο των Πραγμάτων (IoT). Επιπλέον, συζητά τους πιθανούς τομείς έρευνας, συμπεριλαμβανομένης της ανάπτυξης πιο ενεργειακά αποδοτικών συστημάτων Blockchain και της διερεύνησης του ρόλου του Blockchain στην προώθηση της κοινωνικής και οικονομικής ένταξης.

7.2. Τεχνικές & Ηθικές Προκλήσεις

Ενώ η τεχνολογία Blockchain υπόσχεται πολλά για την ψηφιακή ταυτοποίηση, η εφαρμογή της συνοδεύεται από ένα σύνολο προκλήσεων που πρέπει να αντιμετωπιστούν προσεκτικά. Αυτή η ενότητα εμβαθύνει σε αυτές τις προκλήσεις, εξετάζοντας τόσο τις τεχνικές όσο και τις ηθικές πτυχές που απαιτούν προσεκτική εξέταση.

Από τεχνικής πλευράς, ένα από τα κύρια εμπόδια είναι η επεκτασιμότητα, η ικανότητα δηλαδή των συστημάτων Blockchain να χειρίζονται μεγάλο αριθμό συναλλαγών αποτελεσματικά. Αυτός ο περιορισμός μπορεί να εμποδίσει την ευρεία υιοθέτηση του Blockchain στην ψηφιακή ταυτοποίηση, ειδικά σε περιπτώσεις που απαιτούνται συναλλαγές υψηλής ταχύτητας. Η ενότητα διερευνά τις επιπτώσεις της επεκτασιμότητας και τις πιθανές λύσεις που μπορούν να μετριάσουν αυτό το ζήτημα.

Από ηθικής πλευράς, προκύπτουν σημαντικά ερωτήματα σχετικά με τη διακυβέρνηση των δεδομένων και το απόρρητο. Η διαφάνεια του Blockchain, αν και πλεονεκτική από πολλές απόψεις, εγείρει ανησυχίες σχετικά με το απόρρητο των ευαίσθητων προσωπικών πληροφοριών. Επιπλέον, η αποκεντρωμένη φύση του Blockchain εγείρει ερωτήματα σχετικά με τη διακυβέρνηση και τη λήψη αποφάσεων σε ένα σύστημα χωρίς Κεντρική Αρχή. Αυτή η ενότητα εξετάζει αυτές τις ηθικές πολυπλοκότητες και τις πιθανές προσεγγίσεις για την αντιμετώπισή τους.

7.2.1. Ζητήματα Επεκτασιμότητας

Τα ζητήματα επεκτασιμότητας αντιπροσωπεύουν μια σημαντική τεχνική πρόκληση στην ανάπτυξη της τεχνολογίας Blockchain, ιδιαίτερα στο πλαίσιο των συστημάτων ψηφιακής ταυτοποίησης. Η επεκτασιμότητα, σε αυτό το πλαίσιο, αναφέρεται στην ικανότητα του δικτύου Blockchain να χειρίζεται αποτελεσματικά έναν μεγάλο αριθμό συναλλαγών και χρηστών. Αυτή η πρόκληση είναι πολύπλευρη και περιλαμβάνει πτυχές, όπως η ταχύτητα συναλλαγής, η αποθήκευση δεδομένων και η συνολική απόδοση του δικτύου.

Ένα από τα κύρια ζητήματα επεκτασιμότητας στο Blockchain είναι η περιορισμένη απόδοση των συναλλαγών. Τα πρώτα δίκτυα Blockchain, όπως το Bitcoin, μπορούν να επεξεργαστούν μόνο έναν περιορισμένο αριθμό συναλλαγών ανά δευτερόλεπτο (TPS). Αυτός ο περιορισμός οφείλεται σε διάφορους παράγοντες, συμπεριλαμβανομένου του χρόνου που απαιτείται για την επικύρωση των συναλλαγών μέσω μηχανισμών συναίνεσης, όπως η απόδειξη εργασίας (PoW), και το μέγεθος των μπλοκ, το οποίο περιορίζει τον αριθμό των συναλλαγών που μπορούν

να συμπεριληφθούν σε κάθε μπλοκ. Για παράδειγμα, το δίκτυο Bitcoin έχει θεωρητικό μέγιστο περίπου 7 TPS, το οποίο είναι πολύ χαμηλότερο από αυτό που απαιτείται για εφαρμογές μεγάλης κλίμακας, όπως τα εθνικά συστήματα ψηφιακής ταυτοποίησης. Αυτός ο περιορισμός επισημαίνεται στη μελέτη των Croman et al. (2016).

Καθώς αυξάνεται ο αριθμός των συναλλαγών, το μέγεθος του Blockchain αυξάνεται αναλογικά, οδηγώντας σε προκλήσεις αποθήκευσης δεδομένων. Αυτό μπορεί να γίνει ιδιαίτερα προβληματικό για κόμβους με περιορισμένους πόρους ή για συσκευές με περιορισμένη χωρητικότητα αποθήκευσης, όπως κινητές συσκευές. Η αποθήκευση ολόκληρου του ιστορικού συναλλαγών μπορεί να γίνει δυσκίνητη και δαπανηρή, εμποδίζοντας την προσβασιμότητα και την αποδοτικότητα του συστήματος.

Για την αντιμετώπιση αυτών των ζητημάτων επεκτασιμότητας, οι ερευνητές και οι προγραμματιστές εξερευνούν διάφορες λύσεις. Μία προσέγγιση είναι η χρήση λύσεων δεύτερου επιπέδου (Layer 2), όπως το Lightning Network για το Bitcoin. Αυτές οι λύσεις δημιουργούν ένα δεύτερο επίπεδο πάνω από το κύριο δίκτυο Blockchain, όπου μπορούν να πραγματοποιηθούν συναλλαγές εκτός αλυσίδας. Αυτή η προσέγγιση μπορεί να αυξήσει σημαντικά την ταχύτητα συναλλαγών και να μειώσει το κόστος, καθώς οι συναλλαγές δεν χρειάζεται να επικυρωθούν από ολόκληρο το δίκτυο Blockchain.

Το Sharding είναι μια άλλη προσέγγιση όπου το Blockchain χωρίζεται σε μικρότερα και πιο διαχειρίσιμα “θραύσματα” (shards). Κάθε θραύσμα περιέχει ένα τμήμα του ιστορικού συναλλαγών του Blockchain, επιτρέποντας την παράλληλη επεξεργασία. Αυτή η τεχνική μπορεί να βελτιώσει σημαντικά την επεκτασιμότητα και τη συνολική απόδοση του συστήματος. Επιπλέον, η μετάβαση από τον μηχανισμό συναίνεσης Proof of Work (PoW) σε πιο ενεργειακά αποδοτικές εναλλακτικές, όπως η Proof of Stake (PoS), μπορεί να αντιμετωπίσει προβλήματα επεκτασιμότητας. Οι μηχανισμοί PoS καταναλώνουν σημαντικά λιγότερη ενέργεια από τους μηχανισμούς PoW, καθιστώντας τους πιο βιώσιμους για εφαρμογές μεγάλης κλίμακας (Croman et al., 2016).

Τα ζητήματα επεκτασιμότητας έχουν, επίσης, ηθικές επιπτώσεις. Εάν τα συστήματα ψηφιακής ταυτότητας που βασίζονται σε Blockchain δεν μπορούν να κλιμακωθούν αποτελεσματικά, κινδυνεύουν να αποκλείσουν μεγάλα τμήματα του πληθυσμού, ιδιαίτερα σε περιοχές υψηλής πυκνότητας ή σε αναπτυσσόμενες χώρες με λιγότερη τεχνολογική υποδομή (Swan, 2015).

Επίσης, ο περιβαλλοντικός αντίκτυπος του Blockchain, ειδικά των συστημάτων που βασίζονται σε PoW, αποτελεί μια σημαντική ηθική ανησυχία. Η υψηλή κατανάλωση ενέργειας για τις εργασίες εξόρυξης και τη συντήρηση του δικτύου έχει εγείρει ερωτήματα σχετικά με τη βιωσιμότητα της τεχνολογίας Blockchain.

7.2.2. Δεοντολογικά Ζητήματα & Διακυβέρνηση Δεδομένων

Οι ηθικοί προβληματισμοί και η διακυβέρνηση δεδομένων είναι κρίσιμες πτυχές των τεχνικών και ηθικών προκλήσεων που αντιμετωπίζει η τεχνολογία Blockchain, ειδικά στο πλαίσιο των συστημάτων ψηφιακής ταυτοποίησης. Αυτές οι προκλήσεις περιστρέφονται γύρω από την ηθική χρήση των δεδομένων, τα ζητήματα απορρήτου και τη διακυβέρνηση αποκεντρωμένων συστημάτων.

Ένα από τα κύρια ηθικά ζητήματα είναι η ισορροπία μεταξύ διαφάνειας και ιδιωτικότητας. Η εγγενής διαφάνεια και το αμετάβλητο του Blockchain μπορεί να έρχονται σε σύγκρουση με τα δικαιώματα απορρήτου και τους νόμους περί προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση (Finck, 2018).

Η ηθική χρήση του Blockchain στη ψηφιακή ταυτοποίηση περιλαμβάνει, επίσης, τη διασφάλιση ότι τα άτομα έχουν τον έλεγχο των δεδομένων τους και μπορούν να παρέχουν ενημερωμένη συγκατάθεση για τη χρήση του. Αυτό είναι ιδιαίτερα σημαντικό στο πλαίσιο των αυτό-κυριαρχικών ταυτοτήτων, όπου οι χρήστες θα πρέπει να έχουν την αυτονομία να διαχειρίζονται τα δικά τους δεδομένα. Η αποκεντρωμένη φύση του Blockchain θέτει μοναδικές προκλήσεις για τη

διακυβέρνηση των δεδομένων. Οι διαδικασίες λήψης αποφάσεων σε αποκεντρωμένα συστήματα μπορεί να είναι πολύπλοκες και η διασφάλιση της λογοδοσίας και της διαφάνειας είναι ζωτικής σημασίας (De Filippi & Wright, 2018).

Υπάρχει μια λεπτή ισορροπία μεταξύ της προώθησης της καινοτομίας στην τεχνολογία Blockchain και της διασφάλισης ηθικών πρακτικών στη διακυβέρνηση δεδομένων. Η υπερβολική ρύθμιση μπορεί να καταπνίξει την καινοτομία, ενώ η έλλειψη ρύθμισης μπορεί να οδηγήσει σε ηθικές παραβιάσεις. Αυτή η ισορροπία συζητείται από τον Swan (2015).

Για να είναι επιτυχημένα τα συστήματα ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain, πρέπει να κερδίσουν την εμπιστοσύνη και την αποδοχή του κοινού. Η αντιμετώπιση ηθικών κριτηρίων και η διασφάλιση ισχυρής διακυβέρνησης δεδομένων είναι το κλειδί για την οικοδόμηση αυτής της εμπιστοσύνης.

Οι ηθικοί προβληματισμοί και η διακυβέρνηση δεδομένων είναι αναπόσπαστα στοιχεία για την επιτυχή εφαρμογή συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain. Η εξισορρόπηση του απορρήτου, του ελέγχου των χρηστών, της τυποποίησης και της αποκεντρωμένης διακυβέρνησης με την ανάγκη ενίσχυσης της καινοτομίας και της εμπιστοσύνης του κοινού είναι ζωτικής σημασίας. Καθώς η τεχνολογία Blockchain συνεχίζει να εξελίσσεται, ο συνεχής διάλογος και η έρευνα σε αυτά τα ζητήματα ηθικής και διακυβέρνησης θα είναι ουσιαστικής σημασίας για τη διαμόρφωση της μελλοντικής ανάπτυξης και εφαρμογής της.

7.3. Το μέλλον του Blockchain στην Ψηφιακή Ταυτοποίηση

Καθώς η τεχνολογία Blockchain συνεχίζει να ωριμάζει και να εξελίσσεται, το δυναμικό της να αναδιαμορφώσει την ψηφιακή ταυτοποίηση γίνεται όλο και πιο εμφανές. Η ενότητα αυτή εμβαθύνει στις μελλοντικές προοπτικές του Blockchain σε αυτόν τον τομέα, εξετάζοντας τις αναδυόμενες τάσεις και τους πιθανούς τομείς έρευνας που θα διαμορφώσουν το μέλλον της ψηφιακής ταυτοποίησης.

Η ενότητα ξεκινά με την εξέταση των αναδυόμενων τάσεων στην τεχνολογία Blockchain και πώς αυτές οι τάσεις μπορούν να επηρεάσουν τα συστήματα ψηφιακής ταυτοποίησης. Αυτό περιλαμβάνει την ενσωμάτωση του Blockchain με άλλες τεχνολογίες αιχμής, όπως η Τεχνητή Νοημοσύνη (AI), η Μηχανική Μάθηση (ML) και το Διαδίκτυο των Πραγμάτων (IoT). Η ενότητα εξετάζει, επίσης, τις εξελίξεις στη βασική τεχνολογία Blockchain, όπως οι βελτιώσεις στην επεκτασιμότητα και τη διαλειτουργικότητα, οι οποίες είναι ζωτικής σημασίας για την ευρεία υιοθέτηση του Blockchain στην ψηφιακή ταυτοποίηση.

Επιπλέον, η ενότητα εξετάζει πιθανούς τομείς μελλοντικής έρευνας στο Blockchain και την ψηφιακή ταυτοποίηση. Αυτό περιλαμβάνει την εξερεύνηση του πώς το Blockchain μπορεί να συμβάλει στην κοινωνική και οικονομική ένταξη παρέχοντας ψηφιακή ταυτότητα σε περιθωριοποιημένους πληθυσμούς. Επιπλέον, η ενότητα τονίζει την ανάγκη για έρευνα σχετικά με τον περιβαλλοντικό αντίκτυπο των τεχνολογιών Blockchain και την ανάπτυξη πιο βιώσιμων λύσεων.

7.3.1. Αναδυόμενες Τάσεις

Το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση διαμορφώνεται από διάφορες αναδυόμενες τάσεις που αντικατοπτρίζουν το εξελισσόμενο τοπίο της τεχνολογίας, τα ρυθμιστικά περιβάλλοντα και τις προσδοκίες των χρηστών. Αυτές οι τάσεις υποδεικνύουν τις κατευθύνσεις προς τις οποίες είναι πιθανό να αναπτυχθεί η τεχνολογία Blockchain και πώς θα μπορούσε να μεταμορφώσει τα συστήματα ψηφιακής ταυτοποίησης. Αναλυτικότερα:

- Ενοποίηση με αναδυόμενες τεχνολογίες:
  - ✓ Τεχνητή Νοημοσύνη (AI) και Μηχανική Μάθηση (ML): Η ενσωμάτωση του Blockchain με τεχνολογίες AI και ML είναι μια σημαντική τάση. Αυτή η σύγκλιση μπορεί να ενισχύσει τις δυνατότητες των συστημάτων ψηφιακής ταυτοποίησης σε τομείς, όπως ο εντοπισμός απάτης, η επαλήθευση ταυτότητας και οι αυτοματοποιημένοι έλεγχοι συμμόρφωσης.

- ✓ Διαδίκτυο των Πραγμάτων (IoT): Το Blockchain ενσωματώνεται όλο και περισσότερο με συσκευές IoT. Στην ψηφιακή ταυτοποίηση, αυτή η ενοποίηση μπορεί να οδηγήσει σε πιο ασφαλή και αποτελεσματική διαχείριση των ταυτοτήτων από συσκευές IoT, ενισχύοντας την ασφάλεια και την ακεραιότητα των δεδομένων στα δίκτυα IoT.
- ✓ Κβαντο-ανθεκτικό Blockchain: Με την έλευση του κβαντικού υπολογισμού, υπάρχει μια αυξανόμενη ανάγκη για τεχνολογίες Blockchain που είναι ανθεκτικές σε επιθέσεις κβαντικών υπολογιστών. Η ανάπτυξη κβαντο-ανθεκτικών Blockchain περιλαμβάνει τη δημιουργία κρυπτογραφικών πρωτοκόλλων που μπορούν να αντέξουν την υπολογιστική ισχύ των κβαντικών υπολογιστών. Αυτή η μελλοντική προστασία είναι ζωτικής σημασίας για τη μακροπρόθεσμη βιωσιμότητα των συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain.
- ✓ Προηγμένες κρυπτογραφικές τεχνικές: Η εφαρμογή πιο προηγμένων τεχνικών κρυπτογράφησης, όπως αποδείξεις μηδενικής γνώσης, μπορεί να ενισχύσει το απόρρητο και την ασφάλεια στα συστήματα Blockchain. Αυτές οι τεχνικές επιτρέπουν την επαλήθευση συναλλαγών ή ταυτοτήτων χωρίς να αποκαλύπτονται υποκείμενες ευαίσθητες πληροφορίες, μια έννοια που κερδίζει έδαφος στην κοινότητα του Blockchain.

- Πρόοδος στην τεχνολογία Blockchain:
  - ✓ Λύσεις επεκτασιμότητας: Η αντιμετώπιση ζητημάτων επεκτασιμότητας είναι ένας βασικός τομέας εστίασης. Καινοτομίες όπως ο διαμοιρασμός, τα πρωτόκολλα Επιπέδου 2 και οι πιο αποτελεσματικοί μηχανισμοί συναίνεσης αναπτύσσονται για να ενισχύσουν τη χωρητικότητα συναλλαγών και την ταχύτητα των δικτύων Blockchain.
  - ✓ Διαλειτουργικότητα μεταξύ Blockchain: Η ανάπτυξη προτύπων και πρωτοκόλλων για τη διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων Blockchain είναι μια αυξανόμενη τάση. Αυτό είναι

ζωτικής σημασίας για τη δημιουργία ενός απρόσκοπτου και ολοκληρωμένου οικοσυστήματος ψηφιακής ταυτοποίησης σε διάφορες πλατφόρμες και βιομηχανίες.

- Ρυθμιστικές και ηθικές εξελίξεις:
  - ✓ Εναρμόνιση κανονισμών: Καθώς η τεχνολογία Blockchain ωριμάζει, υπάρχει μια τάση προς την εναρμόνιση των ρυθμιστικών πλαισίων μεταξύ των δικαιοδοσιών. Αυτό είναι ιδιαίτερα σημαντικό για συστήματα ψηφιακής ταυτοποίησης που λειτουργούν διασυνοριακά.
  - ✓ Εστίαση στα ηθικά πρότυπα: Δίνεται αυξανόμενη έμφαση στα ηθικά πρότυπα στην ανάπτυξη του Blockchain, ειδικά όσον αφορά το απόρρητο των δεδομένων και τη συναίνεση των χρηστών. Η ανάπτυξη δεοντολογικών κατευθυντήριων γραμμών και βέλτιστων πρακτικών είναι ζωτικής σημασίας για την οικοδόμηση εμπιστοσύνης και τη διασφάλιση της υπεύθυνης χρήσης του Blockchain στην ψηφιακή ταυτοποίηση.

Το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση χαρακτηρίζεται από τεχνολογικές εξελίξεις, ρυθμιστικές εξελίξεις και μια στροφή προς μοντέλα με επίκεντρο τον χρήστη. Η ενοποίηση με AI, ML και IoT, οι εξελίξεις στην επεκτασιμότητα και τη διαλειτουργικότητα, η εναρμόνιση των κανονισμών και η εστίαση στα ηθικά πρότυπα είναι βασικές τάσεις που διαμορφώνουν αυτό το μέλλον. Καθώς αυτές οι τάσεις εξελίσσονται, πιθανότατα θα οδηγήσουν σε σημαντικές αλλαγές στον τρόπο διαχείρισης και χρήσης της ψηφιακής ταυτοποίησης, προσφέροντας νέες ευκαιρίες και προκλήσεις στο ψηφιακό τοπίο.

7.3.2. Πιθανές Εξελίξεις & Μελλοντικοί Τομείς Έρευνας

Το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση είναι έτοιμο για σημαντικές εξελίξεις, με πολυάριθμους πιθανούς ερευνητικούς τομείς που αναδύονται, καθώς εξελίσσεται η τεχνολογία. Αυτές οι εξελίξεις οφείλονται στην

ανάγκη αντιμετώπισης των σημερινών περιορισμών και αξιοποίησης του πλήρους δυναμικού του Blockchain σε διάφορες εφαρμογές.

- Πιθανές εξελίξεις στο Blockchain για ψηφιακή ταυτοποίηση
  - ✓ Ενισχυμένη διαλειτουργικότητα: Μία από τις βασικές μελλοντικές εξελίξεις είναι η ενίσχυση της διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων Blockchain και παραδοσιακών συστημάτων ψηφιακής ταυτοποίησης. Η έρευνα σε αυτόν τον τομέα θα μπορούσε να επικεντρωθεί στην ανάπτυξη τυποποιημένων πρωτοκόλλων και πλαισίων για τη διαλειτουργικότητα.
  - ✓ Βελτιωμένες λύσεις επεκτασιμότητας: Η αντιμετώπιση των προκλήσεων επεκτασιμότητας του Blockchain είναι απαραίτητη για την ευρεία υιοθέτησή του στην ψηφιακή ταυτοποίηση. Οι μελλοντικές εξελίξεις θα μπορούσαν να περιλαμβάνουν πιο αποτελεσματικούς αλγόριθμους συναίνεσης, λύσεις εκτός Blockchain και τεχνικές διαμοιρασμού.
  - ✓ Ανθεκτικά Blockchain σε κβαντικές τεχνολογίες: Με την έλευση των κβαντικών υπολογιστών, η ανάπτυξη τεχνολογιών Blockchain ανθεκτικών στην κβαντική τεχνολογία γίνεται όλο και πιο σημαντική. Η έρευνα σε αυτόν τον τομέα θα επικεντρωθεί σε κρυπτογραφικές μεθόδους που μπορούν να αντέξουν την υπολογιστική ισχύ των κβαντικών υπολογιστών, διασφαλίζοντας τη μακροπρόθεσμη ασφάλεια των συστημάτων Blockchain.
- Τομείς μελλοντικής έρευνας στο Blockchain και την ψηφιακή ταυτοποίηση
  - ✓ Ενσωμάτωση με αναδυόμενες τεχνολογίες: Η έρευνα για την ενσωμάτωση του Blockchain με άλλες αναδυόμενες τεχνολογίες, όπως το AI, το ML και το IoT θα μπορούσε να οδηγήσει σε πιο προηγμένα και αποτελεσματικά συστήματα ψηφιακής ταυτότητας. Αυτό περιλαμβάνει τη χρήση AI για προγνωστικά αναλυτικά στοιχεία στη διαχείριση ταυτότητας και τη χρησιμοποίηση του IoT για επαλήθευση ταυτότητας σε πραγματικό χρόνο.

- ✓ Ηθική και κανονιστική συμμόρφωση: Καθώς η τεχνολογία Blockchain ωριμάζει, η έρευνα σχετικά με ηθικούς λόγους και τη συμμόρφωση με τους κανονισμούς θα γίνεται όλο και πιο σημαντική. Αυτό περιλαμβάνει μελέτες για το απόρρητο δεδομένων, τη συναίνεση των χρηστών και την ευθυγράμμιση με τους παγκόσμιους κανονισμούς όπως ο GDPR.
- ✓ Blockchain για κοινωνική και οικονομική ένταξη: Η έρευνα σχετικά με το πώς η ψηφιακή ταυτοποίηση που βασίζεται σε Blockchain μπορεί να συμβάλει στην κοινωνική και οικονομική ένταξη, ειδικά στις αναπτυσσόμενες χώρες, είναι ένας πολλά υποσχόμενος τομέας.
- ✓ Περιβαλλοντικός αντίκτυπος των τεχνολογιών Blockchain: Καθώς η βιωσιμότητα γίνεται παγκόσμια προτεραιότητα, η έρευνα για τον περιβαλλοντικό αντίκτυπο της τεχνολογίας του Blockchain είναι ζωτικής σημασίας. Αυτό περιλαμβάνει την ανάπτυξη πιο ενεργειακά αποδοτικών συστημάτων Blockchain και τη διερεύνηση του ρόλου του Blockchain στην προώθηση βιώσιμων πρακτικών.

Το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση είναι πλούσιο με πιθανές εξελίξεις και τομείς έρευνας. Από τις τεχνολογικές εξελίξεις, όπως η βελτιωμένη διαλειτουργικότητα και οι λύσεις επεκτασιμότητας έως τα ευρύτερα ζητήματα ηθικής συμμόρφωσης, κοινωνικής ένταξης και περιβαλλοντικής βιωσιμότητας, το πεδίο έρευνας και ανάπτυξης σε αυτόν τον τομέα είναι τεράστιο και πολυδιάστατο. Καθώς η τεχνολογία Blockchain συνεχίζει να εξελίσσεται, αυτοί οι ερευνητικοί τομείς θα διαδραματίσουν κρίσιμο ρόλο στη διαμόρφωση της εφαρμογής και του αντικτύπου της τεχνολογίας στον τομέα της ψηφιακής ταυτοποίησης και πέρα από αυτήν.

ΚΕΦΑΛΑΙΟ 8: ΣΥΜΠΕΡΑΣΜΑΤΑ & ΣΥΣΤΑΣΕΙΣ

Το κεφάλαιο αυτό χρησιμεύει ως επιστέγασμα της διπλωματικής εργασίας, συνοψίζοντας τα βασικά ευρήματα της εξερεύνησης της τεχνολογίας Blockchain στην ψηφιακή ταυτοποίηση. Επιπλέον, το κεφάλαιο προχωρά πέρα από τη σύνοψη, παρέχοντας συστάσεις που προκύπτουν από την ανάλυση και τις συζητήσεις που παρουσιάζονται σε όλη την εργασία.

Στην ενότητα των συμπερασμάτων, το κεφάλαιο ανακεφαλαιώνει τα βασικά σημεία που συζητήθηκαν σε όλη τη διπλωματική εργασία, εστιάζοντας στα πλεονεκτήματα και τις προκλήσεις της εφαρμογής του Blockchain στην ψηφιακή ταυτοποίηση. Αναδεικνύει τα πιθανά οφέλη, όπως η αυξημένη ασφάλεια, η αποκέντρωση και η ενδυνάμωση των χρηστών, ενώ αναγνωρίζει εμπόδια, όπως η επεκτασιμότητα, οι κανονιστικές ανησυχίες και οι ηθικές εκτιμήσεις.

Στην ενότητα των συστάσεων, το κεφάλαιο αξιοποιεί τα ευρήματα της διπλωματικής για να προτείνει κατευθύνσεις για μελλοντική έρευνα και ανάπτυξη. Οι συστάσεις αυτές θα μπορούσαν να περιλαμβάνουν τεχνικές βελτιώσεις, όπως η αντιμετώπιση των ζητημάτων επεκτασιμότητας ή η εξερεύνηση νέων κρυπτογραφικών τεχνικών. Επιπλέον, οι συστάσεις θα μπορούσαν να επεκταθούν σε κανονιστικές και ηθικές πτυχές, όπως η ανάγκη για σαφή νομικά πλαίσια και ηθικές κατευθυντήριες γραμμές για την ανάπτυξη και χρήση συστημάτων ψηφιακής ταυτοποίησης που βασίζονται σε Blockchain.

8.1. Συμπεράσματα

Η ενσωμάτωση της τεχνολογίας Blockchain σε συστήματα ψηφιακής ταυτοποίησης σηματοδοτεί ένα σημαντικό βήμα προς τα εμπρός στον τρόπο διαχείρισης των προσωπικών δεδομένων. Η αποκεντρωμένη φύση του, σε συνδυασμό με ισχυρά χαρακτηριστικά ασφάλειας και απορρήτου, τοποθετεί το Blockchain ως ισχυρό εργαλείο για την καταπολέμηση των παραβιάσεων δεδομένων

και της κλοπής ταυτότητας. Η δυνατότητα της τεχνολογίας να φέρει επανάσταση στη ψηφιακή ταυτοποίηση είναι καλά διατυπωμένη σε έργα, όπως αυτό των Tapscott και Tapscott (2016), τα οποία αναδεικνύουν τις μεταμορφωτικές της ικανότητες.

Ωστόσο, αυτή η μετάβαση δεν έρχεται χωρίς εμπόδια. Η επεκτασιμότητα παραμένει μια τρομερή πρόκληση, με την τρέχουσα ικανότητα των συναλλαγών του Blockchain να υπολείπεται των απαιτήσεων των ευρέως διαδεδομένων εφαρμογών ψηφιακής ταυτοποίησης. Αυτός ο περιορισμός είναι κάτι περισσότερο από ένα τεχνικό ζήτημα. Είναι ένα θεμελιώδες εμπόδιο για την υιοθέτηση και την επεκτασιμότητα συστημάτων που βασίζονται σε Blockchain.

Το ρυθμιστικό και ηθικό τοπίο που περιβάλλει το Blockchain είναι ένα άλλο πολύπλοκο σημείο. Η εξισορρόπηση της ανάγκης για απόρρητο, διακυβέρνηση δεδομένων και συμμόρφωση με τους κανονισμούς είναι ένα ιδιαίτερο έργο. Η εξελισσόμενη φύση αυτών των κανονισμών υπογραμμίζει την ανάγκη για εναρμόνιση και ηθική εξέταση στην ανάπτυξη τεχνολογιών Blockchain.

Το μέλλον του Blockchain στην ψηφιακή ταυτοποίηση διαμορφώνεται από τις αναδυόμενες τάσεις και τις τεχνολογικές εξελίξεις. Η σύγκλιση του Blockchain με την AI, το IoT και την ανάπτυξη κβαντικών αλγορίθμων ανοίγει νέους δρόμους για την αντιμετώπιση των σημερινών περιορισμών και την ενίσχυση των δυνατοτήτων των συστημάτων ψηφιακής ταυτοποίησης.

Επιπλέον, ο ρόλος του Blockchain στην προώθηση της κοινωνικής και οικονομικής ένταξης δεν μπορεί να υπερεκτιμηθεί. Η δυνατότητά του να παρέχει ασφαλή ψηφιακή ταυτοποίηση σε περιθωριοποιημένους πληθυσμούς είναι ένας φάρος ελπίδας για την αντιμετώπιση των παγκόσμιων ανισοτήτων.

Τέλος, η περιβαλλοντική βιωσιμότητα αναδεικνύεται, επίσης, ως κρίσιμος τομέας εστίασης. Η ενεργοβόρα φύση ορισμένων εφαρμογών Blockchain, ιδιαίτερα εκείνων που βασίζονται στο PoW, απαιτεί επανεκτίμηση των περιβαλλοντικών επιπτώσεων της τεχνολογίας. Η ανάπτυξη βιώσιμων λύσεων Blockchain δεν είναι απλώς μια τεχνική πρόκληση, αλλά μια ηθική επιταγή για το μέλλον αυτής της τεχνολογίας.

Η τεχνολογία Blockchain στην ψηφιακή ταυτοποίηση βρίσκεται σε ένα σταυροδρόμι ευκαιριών και ευθύνης. Η ικανότητά της να προσφέρει ασφαλή,

αποτελεσματική και ιδιωτική διαχείριση ταυτότητας αντισταθμίζεται από προκλήσεις στην επεκτασιμότητα, τη ρύθμιση και την ηθική εφαρμογή. Καθώς πλοηγούμαστε σε αυτό το τοπίο, η εστίαση πρέπει να παραμείνει στην αξιοποίηση των δυνατοτήτων του Blockchain με υπευθυνότητα, διασφαλίζοντας ότι η ανάπτυξή του σε συστήματα ψηφιακής ταυτοποίησης είναι τόσο ωφέλιμη όσο και καινοτόμος.

8.2. Συστάσεις

Γίνεται σαφές ότι αυτή η καινοτόμος τεχνολογία βρίσκεται στην πρώτη γραμμή μιας σημαντικής αλλαγής στον τρόπο διαχείρισης και προστασίας των ψηφιακών ταυτοτήτων. Το ταξίδι μέσα από διάφορες πτυχές του Blockchain, από τους θεμελιώδεις μηχανισμούς του έως την εφαρμογή του σε συστήματα ψηφιακής ταυτοποίησης, αποκαλύπτει ένα τοπίο πλούσιο σε δυνατότητες, αλλά και γεμάτο προκλήσεις.

Με βάση τα ευρήματα αυτής της διπλωματικής εργασίας, προτείνονται αρκετές συστάσεις για μελλοντική έρευνα και ανάπτυξη στον τομέα του Blockchain και της ψηφιακής ταυτοποίησης:

- Επένδυση σε Έρευνα και Ανάπτυξη: Οι κυβερνήσεις, οι ακαδημαϊκοί και οι παράγοντες του κλάδου θα πρέπει να συνεχίσουν να επενδύουν στην έρευνα και την ανάπτυξη τεχνολογιών Blockchain. Αυτό περιλαμβάνει την εξερεύνηση λύσεων επεκτασιμότητας, τη βελτίωση της διαλειτουργικότητας και την ανάπτυξη προτύπων για την ψηφιακή ταυτοποίηση που βασίζεται σε Blockchain.
- Ανάπτυξη σαφών νομικών πλαισίων: Καθώς η τεχνολογία Blockchain συνεχίζει να εξελίσσεται, είναι ζωτικής σημασίας η ανάπτυξη σαφών νομικών και κανονιστικών πλαισίων που να διέπουν τη χρήση της στην ψηφιακή ταυτοποίηση. Αυτά τα πλαίσια θα πρέπει να αντιμετωπίζουν ζητήματα απορρήτου, ασφάλειας δεδομένων και διασυνοριακής αναγνώρισης ψηφιακών ταυτοτήτων.

- Προώθηση της συνεργασίας και της τυποποίησης: Η συνεργασία μεταξύ των ενδιαφερομένων, συμπεριλαμβανομένων των κυβερνήσεων, των επιχειρήσεων και των οργανισμών τυποποίησης, είναι απαραίτητη για την καθιέρωση κοινών προτύπων και πρωτοκόλλων για την ψηφιακή ταυτοποίηση που βασίζεται σε Blockchain. Αυτό θα διασφαλίσει τη διαλειτουργικότητα και θα διευκολύνει την ευρεία υιοθέτηση της τεχνολογίας.
- Εστίαση στην εκπαίδευση και την ευαισθητοποίηση των χρηστών: Η εκπαίδευση των χρηστών σχετικά με τα οφέλη και τους κινδύνους της ψηφιακής ταυτοποίησης που βασίζεται σε Blockchain είναι ζωτικής σημασίας. Αυτό περιλαμβάνει την ευαισθητοποίηση σχετικά με την αυτοκυριαρχούμενη ταυτότητα, τη σημασία της ασφάλειας των κλειδιών και τον τρόπο προστασίας των προσωπικών δεδομένων.
- Διερεύνηση του Blockchain για κοινωνικό αντίκτυπο: Οι μελλοντικές έρευνες θα πρέπει να διερευνήσουν τον πιθανό ρόλο του Blockchain στην προώθηση της κοινωνικής και οικονομικής ένταξης. Αυτό περιλαμβάνει τη διερεύνηση του πώς το Blockchain μπορεί να παρέχει ψηφιακή ταυτότητα σε περιθωριοποιημένους πληθυσμούς και να διευκολύνει την πρόσβασή τους σε βασικές υπηρεσίες.
- Αντιμετώπιση περιβαλλοντικών ανησυχιών: Η έρευνα θα πρέπει να επικεντρωθεί στην ανάπτυξη πιο ενεργειακά αποδοτικών αλγορίθμων και μηχανισμών συναίνεσης για την τεχνολογία Blockchain. Αυτό είναι απαραίτητο για τον μετριασμό του περιβαλλοντικού αντίκτυπου του Blockchain και τη διασφάλιση της μακροπρόθεσμης βιωσιμότητάς του.

Η τεχνολογία Blockchain έχει τη δυνατότητα να φέρει επανάσταση στην ψηφιακή ταυτοποίηση, αλλά η υπεύθυνη και αποτελεσματική εφαρμογή της απαιτεί μια ολοκληρωμένη προσέγγιση που να λαμβάνει υπόψη τις τεχνικές, κανονιστικές και ηθικές πτυχές. Με συνεχή έρευνα, ανάπτυξη και συνεργασία μεταξύ των

ενδιαφερομένων, το Blockchain μπορεί να ανοίξει το δρόμο για ένα πιο ασφαλές, διαφανές και δίκαιο μέλλον για την ψηφιακή ταυτοποίηση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Allen, C. (2016). *The path to self-sovereign identity*. Blockchain & Decentralized Identity Architect — Internet Cryptography Pioneer — Co-author TLS Security Standard — Collaborative Tools & Patterns.
2. Anderson, R., & Moore, T. (2006). *The economics of information security*. New Series, Vol. 314, No. 5799.
3. Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.
4. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A *survey of attacks on Ethereum smart contracts*. International Conference on Principles of Security and Trust.
5. Bayer, D., Haber, S., & Stornetta, W. S. (1993). *Improving the Efficiency and Reliability of Digital Time-Stamping*. Barnard College Columbia University.
6. Bernstein, D. J., & Lange, T. (2017). *Post-Quantum Cryptography*. Nature. Volume 549.
7. Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. https://ethereum.org/ethereum.html [Πρόσβαση 20/12/2023].
8. Camenisch, J., & Lysyanskaya, A. (2001). *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*. IBM Research Zurich Research Laboratory.
9. Christidis, K., and Devetsikiotis, M. (2016). *Blockchains and Smart Contracts for the Internet of Things*. IEEE.
10. Cole, S. A. (2002). *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press.
11. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song, D. and Wattenhofer, R. (2016). *On Scaling Decentralized Blockchains*. International Conference on Financial Cryptography and Data Security.

12. Crosby, M., Nachiappan, Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). *Blockchain technology: Beyond bitcoin*. Berkeley. Sutarjsa Center.
13. De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.
14. European Union Agency for Cybersecurity (2020). *Blockchain and cybersecurity: Opportunities and challenges*. ENISA Report.
15. European Union (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Official Journal of the European Union, L 257/73.
16. European Commission (2021). *Proposal For A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On A Framework For A European Digital Identity*. COM (2021) 281 final.
17. Eyal, I., & Sirer, E. G. (2018). *Majority is not Enough: Bitcoin Mining is Vulnerable*. Communications of the ACM. Volume 61. Issue 7.
18. Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Max-Planck-Institut für Innovation und Wettbewerb, Munich.
19. Greenleaf, G., & Kemp, K. (2020). *Privacy, Identity and Security*.
20. Goldreich, O. (2009). *Foundations of Cryptography*. Cambridge University Press.
21. Guo, Y., & Liang, C. (2016). *Blockchain application and outlook in the banking industry*. Financial Innovation volume 2.
22. Haber, S., & Stornetta, W. S. (1991). *How to time-stamp a digital document. Journal of Cryptology*. International Association for Cryptologic Research.
23. Hardman, D., & Pentland, A. (2019). *Self-sovereign identity: A guide to the future of digital identity*.
24. Heston, T. F. (2020). *A Case Study in Blockchain Healthcare Innovation*. Department of Medical Education and Clinical Sciences, Washington State University, Spokane, Washington USA.
25. Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to Biometrics*. Springer.
26. Juels, A., & Oprea, A. (2013). *New approaches to security and availability for cloud data*. Communications of the ACM 56(2).

27. Kamath, R. (2018). *Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM*. The JBBA.
28. Kazeem, Y. (2018). *The world's first blockchain-powered elections have just happened in Sierra Leone*. Quartz.
29. Koops, B. J. (2011). *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice*. SCRIPTed 229.
30. Kshetri, N. (2018). *1 Blockchain's roles in meeting key supply chain management objectives*. International Journal of Information Management. Volume 39.
31. Lloyd, M. (2003). *The Passport: The History of Man's Most Travelled Document (2nd ed.).* Canterbury: Queen Anne's Fan.
32. Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.
33. Martin, A. and Taylor, T. (2020). *Exclusion and inclusion in identification: regulation, displacement and data justice*. Information Technology for Development. Volume 27. Issue 1.
34. Mazières, D. (2016). *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*. Stellar Development Foundation.
35. Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, work, and think.* Houghton Mifflin Harcourt.
36. Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D. and Weinhardt, C. (2018). *A blockchain-based smart grid: towards sustainable local energy markets*. Computer Science. Research and Development.
37. Mettler, M. (2016). *Blockchain technology in healthcare: The revolution starts here*. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services.
38. Harsha, V., Patil, Kanchan, G., Rathi, Malati, V. and Tribhuwan (2018). *A Study on Decentralized E-Voting System Using Blockchain Technology*. IJERT.
39. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). *A Survey on Essential Components of a Self-Sovereign Identity*. Hasso Plattner Institute. Potsdam, Germany.
40. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

www.bitcoin.org [Πρόσβαση 20/01/2024].

41. Nielsen, J. (1993). *Usability Engineering*. Morgan Kaufmann Publishers Inc.
42. Osgood, R. (2016). *The Future of Democracy: Blockchain Voting*. COMP116: Information Security.
43. Paquin, C., & Zaverucha, G. (2019). *Verifiable presentations.*
44. Pawar, D., Sarode, P., Santpure, S., Thore, P. and Nimbalkar, P. (2019). *Secure Voting System using Blockchain.* IJERT.
45. Pilkington, M. (2016). *Blockchain Technology: Principles and Applications*. eSearch Handbook on Digital Transformations.
46. Preukschat, A., & Reed, D. (2017). *Self-issued openid provider (SIOP*).
47. Rehm, G., Stein, D., Sasaki, F. and Witt, A. (2016). *Language technologies for a multilingual Europe*. Berlin: Language Science Press.
48. Roman, R., Zhou, J., & Lopez, J. (2013). *On the features and challenges of security and privacy in distributed internet of things*. Computer Networks. Volume 57, Issue 10.
49. Sporny, M., Longley, D., & Reed, D. (2019). *Decentralized identifiers (DIDs).*
50. Sullivan, C., & Burger, E. (2017). *E-residency and Blockchain*. Law Center, Georgetown University, Washington DC, USA.
51. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. 1st Edition. O' Reilly.
52. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Wikinomics.
53. Turk, V., & Mangan, D. (2018). *How Blockchain technology is transforming real estate market? Blockchain in Real Estate*.
54. Vukolić, M. (2017). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. IBM Research- Zurich.
55. Wang, R.Y. and Strong, D.M. (1996). *Beyond Accuracy: What Data Quality Means to Data Consumers*. J. Manag. Inf. Syst.
56. W3C (2022). *Decentralized Identifiers (DIDs) v1.0*. https://www.w3.org/TR/did-core [Πρόσβαση 17/06/2024].
57. W3C. (2022). *Verifiable Credentials Data Model v1.1.* https://www.w3.org/TR/vc-data-model/ [Πρόσβαση 17/06/2024].

58. WEC (2024). *WCAG 2 Overview*. https://www.w3.org/WAI/standards-guidelines/wcag/ [Πρόσβαση 18/12/2023].
59. World Bank (2018). *The global identification challenge: Who are the 1 billion people without proof of identity?* https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity [Πρόσβαση 20/12/2023].
60. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). *Where Is Current Research on Blockchain Technology? A Systematic Review*. PLoS ONE 11 (10).
61. Zheng, Z., Xie, S., Dai, H.N. and Chen, X. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. Conference: 6th IEEE International Congress on Big Data.
62. Zug Stadt (2018). *Evaluation of the Blockchain vote in the city of Zug*. Lucerne University of Applied Sciences and Arts.
63. Zyskind, G., Nathan, O. and Pentland, A.S. (2015). *Decentralizing privacy: Using Blockchain to protect personal data*. IEEE CS Security and Privacy Workshops.