ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

D.I.MA
ΠΜΣ "Ψηφιακή Καινοτομία και Διοίκηση"
MSc in Digital Innovation and Management

Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων
Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας
Πανεπιστήμιο Πατρών

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η τεχνολογία Blockchain και οι εφαρμογές της με αξιοποίηση τεχνικών Ψηφιακού Μάρκετινγκ

Μαρτζάκλης Κωνσταντίνος

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής

Χαλκιόπουλος Κωνσταντίνος

Α΄ Συν-Επιβλέπων

κα. Ήρα Αντωνοπούλου

Β΄ Συν-Επιβλέπων

κ. Ιωάννης Σταματίου

Πάτρα 2022

Ευχαριστίες

Ευχαριστώ θερμά τον καθηγητή μου κ. Χαλκιόπουλο για την καθοδήγησή του και την οικογένειά μου που μου στάθηκαν όλη αυτή την περίοδο.

Περίληψη

Η τεχνολογία του Blockchain στοχεύει στην αλλαγή του διαδικτυακού κόσμου παγκοσμίως και παράλληλα την ανάπτυξη του.

Σε αυτή την εργασία θα αναλύσουμε την έννοια, τον ορισμό και τη σημαντικότητα της τεχνολογίας του Blockchain. Τονίζονται τα πλεονεκτήματά της, καθώς η ασφάλεια, το απόρρητο και η αρχιτεκτονική του Blockchain κάνει αυτή την τεχνολογία να ξεχωρίζει σε σύγκριση με άλλες.

Επίσης θα παρουσιαστεί μια σύντομη εξήγηση των βασικών τεχνικών εννοιών πίσω από το Blockchain, όπως είναι η κρυπτογραφία, η αρχιτεκτονική των δικτύων και οι γλώσσες σεναρίων. Ακόμα, θα δοθούν παραδείγματα εστιάζοντας σε συναλλαγές και σε αποκεντρωμένους οργανισμούς.

Στόχος είναι να γίνει κατανοητή η λειτουργία της τεχνολογίας του Blockchain και πως γίνονται οι συναλλαγές στον ψηφιακό κόσμο. Ακόμα, είναι αξιοσημείωτο να γίνουν αντιληπτά από τον αναγνώστη τα οφέλη που μπορούν να αποκτηθούν από την εφαρμογή του Blockchain στην πραγματικότητα. Όπως είναι η περίπτωση του Bitcoin.

Επιπρόσθετα, θα γίνει αναφορά στις εφαρμογές της τεχνολογίας του Blockchain στο ψηφιακό μάρκετινγκ και πώς αυτή μπορεί να βοηθήσει στην εξέλιξή του. Τέλος, θα δοθεί έμφαση στο Smart Contract το οποίο είναι σημαντικό και δυνατό εργαλείο του Blockchain που επιτρέπει πολλαπλές πηγές αξίας και κανόνων σε συναλλαγές.

Τέλος, θα παρουσιαστούν τα συμπεράσματα και η ανάγκη για περαιτέρω έρευνα και ανάλυση στο χώρο της τεχνολογίας του Blockchain.

Λέξεις κλειδιά: Blockchain, σενάρια, ψηφιακός κόσμος, έξυπνα συμβόλαια, εφαρμογές, κρυπτογραφία, έξυπνο δίκτυο, κυβερνο-φυσικό σύστημα, ευφυές σύστημα μεταφορών

Abstract

Blockchain technology aims to change the world of the internet and at the same time its development.

In this paper, we will analyze the meaning, the definition and the importance of Blockchain technology. Its advantages are emphasized, as the security, privacy and architecture of Blockchain make this technology stand out compared to others.

There will also be a brief explanation of the key technical concepts behind Blockchain, such as cryptography, network architecture, and scripting languages. Examples will also be given focusing on transactions and decentralized organizations.

Furthermore, the goal is to understand how Blockchain technology works and how transactions are made in the digital world. Still, it is remarkable for the reader to realize the benefits that can be gained from the application of Blockchain in reality. As is the case with Bitcoin.

In addition, reference will be made to the applications of Blockchain technology in digital marketing and how this can help in its development. Finally, emphasis will be placed on Smart Contract which is an important and powerful tool of Blockchain that allows multiple sources of value and rules in transactions.

Finally, the conclusions and the need for further research and analysis in the field of Blockchain technology will be presented.

Keywords: Blockchain, scripts, digital world, smart contracts, applications, cryptography, smart grid, Cyber-physical system, intelligent transportation systems

Πρόλογος

Η διπλωματική εργασία υλοποιήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών «Ψηφιακή Καινοτομία και Διοίκηση» του Πανεπιστημίου Πατρών το ακαδημαϊκό έτος 2021-2022 και υπό την επίβλεψη του καθηγητή κ. Κωνσταντίνου Χαλκιόπουλου.

Σε αυτή την εργασία θα δοθεί βάσει στην κατανόηση της έννοιας της τεχνολογίας του Blockchain. Βασικό κίνητρο της διεξαγωγής της μελέτης είναι να αναλυθεί το Blockchain ως μια βασική τεχνολογία η οποία ήδη δεν αποτελεί απλός μέρος του Bitcoin αλλά θεωρείται ως ένα «νέο Διαδίκτυο».

Επίσης, αυτή η μελέτη στοχεύει να βρει την τρέχουσα θέση του Blockchain στην παγκόσμια τεχνολογική σκηνή και να συζητήσει τις δυνατότητες εφαρμογής στο ψηφιακό μάρκετινγκ.

Πίνακας Περιεχομένων

Πίνακας εικόνων

Εισαγωγή

Εισαγωγικά Στοιχεία

Ιστορικά συμβαίνουν κάποιες τεχνολογικές ανακαλύψεις που ανοίγουν έναν εντελώς νέο κόσμο πολλών δυνατοτήτων. Παραδείγματος χάριν, η εφεύρεση του διαδικτύου ήταν μια τέτοια σημαντική ανακάλυψη που άλλαξε τον κόσμο σχεδόν από κάθε οπτική γωνία. Από την άλλη, η τεχνολογία του Blockchain είναι και αυτή μια από τις αναδυόμενες σημαντικές ανακαλύψεις που αναμένεται να φέρει επανάσταση στον τρόπο που εκτελούνται οι διαδικτυακές συναλλαγές, επηρεάζοντας έτσι μια τεράστια κατηγορία πιθανών τομέων εφαρμογής της. [22]

Προτού γίνει η επεξήγηση της έννοια του Blockchain, θα παρουσιάσουμε ένα παράδειγμα για να γίνει απλούστερα κατανοητή. Υποθέτουμε ότι υπάρχει μια κεντρική βιβλιοθήκη στην πόλη, η οποία διατηρεί μια βάση δεδομένων με όλα τα βιβλία της. Ως μέρος της κεντρικής βάσης δεδομένων της βιβλιοθήκης ,διατηρούνται προσωπικές πληροφορίες των μελών της οι οποίες περιλαμβάνουν ευαίσθητες λεπτομερείς όπως είναι η διεύθυνση κατοικίας, τα στοιχεία πληρωμής πιστωτικής και χρεωστικής κάρτας τους, η χρέωση των συνδρομών τους, οι χρεώσεις δανεισμού και τα πιθανά πρόστιμα εάν τα βιβλία δεν έχουν επιστραφεί ή έχυνα καθυστερήσει πέραν την ημερομηνίας λήξης δανεισμού. Επίσης, διατηρεί τα προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου (email), αριθμούς τηλεφώνων, τι είδος ανάγνωσης συνήθως επιλέγει το μέλος. Όλες αυτές οι πληροφορίες είναι ιδιωτικές και ευαίσθητες για κοινή χρήση με τρίτους.

Αυτή η ελεύθερη κοινή χρήση των προσωπικών στοιχείων γίνεται ρουτίνα για τις καθημερινές συναλλαγές. Όπου, μια τέτοια συνήθεια βασίζεται σε ένα προκαταρκτικό γεγονός ότι εμείς εμπιστευόμαστε αυτούς τους οργανισμούς και τις κεντρικές βάσεις δεδομένων. Στις οποίες βάσεις δεδομένων υποθέτουμε ότι διατηρούν τα αρχεία της ζωής μας και τις ιδιωτικές συναλλαγές μας με ακρίβεια και ασφάλεια. Ωστόσο, αν σκεφτούμε σε βάθος την έννοια της «εμπιστοσύνης», δεν υπάρχει καμία εγγύηση ότι ο οργανισμός-ίδρυμα θα κρατήσει αυτές τις πληροφορίες με ασφάλεια υπό οποιεσδήποτε συνθήκες. Για παράδειγμα, σε χώρες όπου υπάρχει έλλειψη εμπιστοσύνης σε εταιρίες και κυβερνήσεις , καθιστά τις συναλλαγές επικίνδυνες και δύσκολο να διασφαλιστούν. Για αυτόν τον λόγο, οι κεντρικές βάσεις δεδομένων και οι θεσμοί λειτουργούν ακριβώς όταν υπάρχει εμπιστοσύνη στο νόμο, τους

κανονισμούς, την κυβέρνηση και τους ανθρώπους. Γεγονός που μπορεί να εγγυηθεί σε όλες τις χώρες, με όλους τους κανονισμούς , από όλους τους εργαζομένους με ειλικρίνεια και εμπιστοσύνη.

Από το παραπάνω παράδειγμα της βιβλιοθήκης, στην πραγματικότητα εκτείνεται για πλησιάσει κάθε τομέα της ζωής μας. Συλλογιστείτε τις τράπεζες που διαθέτουν τα στοιχεία των πιστωτικών και χρεωστικών καρτών, τις προσωπικές πληροφορίες και όλες τις συναλλαγές πληρωμών. Επίσης, σκεφτείτε τις ασφαλιστικές εταιρίες, τις εταιρίες κοινής ωφέλειας, τους παρόχους δικτύων κινητής τηλεφωνίας, τα νοσοκομεία και τα κυβερνητικά ιδρύματα κοκ.. είναι εμφανές ότι ζούμε σε έναν κόσμο που εξαρτάται πλήρως από ένα κεντρικό σύστημα που βασίζεται στην εμπιστοσύνη.

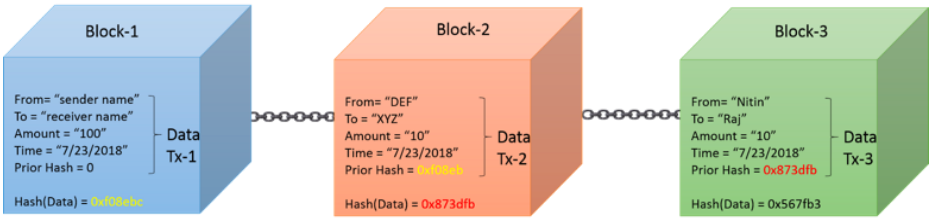
Ο βασικός στόχος της τεχνολογίας του Blockchain είναι να μην υπάρχει αυτό το κεντρικό σύστημα που βασίζεται στην εμπιστοσύνη να εμπλέκεται με τις συναλλαγές. Δηλαδή, η αναδυόμενη τεχνολογία, στοχεύει να μετακινηθεί από αυτά τα κεντρικά συστήματα που βασίζονται στην εμπιστοσύνη σε αποκεντρωμένα συστήματα χωρίς εμπιστοσύνη (trust). Με αυτόν τον τρόπο, παρέχει ένα σύστημα χωρίς εμπιστοσύνη μεταξύ οποιωνδήποτε εμπλεκόμενων ισοτιμιών χωρίς την ανάγκη μεσαζόντων που σχετίζονται με τις συναλλαγές. Επομένως, οι τεχνολογίες του Blockchain, μπορούν να χρησιμοποιηθούν για την άρση της ανάγκης για τα κεντρικά ιδρύματα και τις βάσεις δεδομένων όπου όλοι οι εμπλεκόμενοι στη συναλλαγή μπορούν να προβάλλουν και να επικυρώσουν άμεσα τη συναλλαγή τους. Αυτή η διαδικασία έχει ως αποτέλεσμα τη δημιουργία μιας πραγματικής διαφάνειας χωρίς εμπιστοσύνη.

Από την άλλη πλευρά, πολλοί άνθρωποι πιστεύουν ότι το Blockchain είναι μια τεχνολογία που απλώς τροφοδοτεί το Bitcoin (κρυπτονόμισμα). Αν και αυτός ήταν ο αρχικός του σκοπός, στη συνέχεια φάνηκε ότι είναι ικανό για περισσότερα. Η λέξη “Blockchain” δεν είναι απλώς μια ενιαία τεχνολογία, αλλά μια συντομογραφία μιας σειράς τεχνολογιών κατανεμημένων καθολικών που μπορούν να προγραμματιστούν για να καταγράφουν και να παρακολουθούν οτιδήποτε έχει αξία. Στο παράδειγμα με τη βιβλιοθήκη γίνεται αναφορά σε βιβλία, ωστόσο, αυτό μπορεί να χρησιμοποιηθεί για κάθε είδους ακίνητα, οικονομικές συναλλαγές, ιατρικά δεδομένα, επιχειρήσεις κοινής ωφέλειας κλπ.. Επομένως, είναι ένα αποκεντρωμένο σύστημα χωρίς εμπιστοσύνη (trust-free system) για οτιδήποτε έχει αξία. [23]

Αναλυτικά παρακάτω θα παρουσιαστούν οι λόγοι για τους οποίους η τεχνολογία του Blockchain πρόκειται να φέρει επανάσταση στον τρόπο με τον οποίο αλληλοεπιδρούμε μεταξύ μας.

A. <u>Ο τρόπος με τον οποίο παρακολουθεί και αποθηκεύει δεδομένα.</u>

Το Blockchain αποθηκεύει πληροφορίες σε παρτίδες που ονομάζονται μπλοκ (blocks) και είναι συνδεδεμένες μεταξύ τους με χρονολογικό τρόπο για να σχηματίζουν μια συνεχόμενη γραμμή. Μεταφορικά αυτή η γραμμή λέγεται «αλυσίδα από μπλοκ» (chain-of-blocks), όπως φαίνεται στο παρακάτω σχήμα. [4]



Εικόνα 1 Blockchain

Αν γίνει μια αλλαγή σε πληροφορίες που έχουν καταγραφεί σε συγκεκριμένο μπλοκ, τότε αυτές οι αλλαγές δεν μπορούν να ξαναγραφούν στο αρχικό μπλοκ. Αντίθετα , οι νέες πληροφορίες αποθηκεύονται σε ένα νέο μπλοκ που δείχνει αυτή την αλλαγή. Για παράδειγμα αν το Χ άλλαξε σε Υ σε συγκεκριμένα δεδομένα και χρόνο. Αυτή η μέθοδος για κάποιους είναι οικεία καθώς η ιδέα του Blockchain βασίζεται σε μια παλιότερη μέθοδο, αυτή του Γενικού Χρηματοοικονομικού Καθολικού (General Financial Ledger) [23]. Είναι ένας μη-καταστροφικός τρόπος αντιμετώπισης των αλλαγών των δεδομένων με την πάροδο του χρόνου.

Αυτό που κάνει τα πράγματα να διαφέρουν με το Blockchain σε σχέση με την παλαιά μέθοδο του Γενικού Χρηματοοικονομικού Καθολικού, αρχικά, είναι ένα βιβλίο και έπειτα τα αρχεία της βάσεις δεδομένων αποθηκεύονται σε ένα ενιαίο σύστημα. Από την άλλη, το "chain-of-blocks" έχει σχεδιαστεί για να είναι αποκεντρωμένο και κατανεμημένο σε μεγάλο αριθμό υπολογιστών. Αυτή η αποκέντρωση των πληροφοριών μειώνει την ικανότητα παραβίασης των δεδομένων και καθιστά το Blockchain μοναδικό.

B. Δημιουργία εμπιστοσύνης στα δεδομένα πριν προστεθεί ένα νέο μπλοκ στην αλυσίδα.

Ξεκινώντας, θα πρέπει να λυθεί ένα κρυπτογραφικό παζλ που δημιουργεί το μπλοκ. Στη συνέχεια ο υπολογιστής που λύνει το παζλ μοιράζεται τη λύση σε όλους τους άλλους υπολογιστές του δικτύου. Έπειτα, όλοι οι υπολογιστές του δικτύου θα επαληθεύσουν τη λύση και εάν είναι σωστή το μπλοκ μπορεί να προστεθεί στην αλυσίδα. Αυτό ονομάζεται απόδειξη εργασίας (proof-of-work). Ο συνδυασμός αυτών των μαθηματικών παζλ και η επαλήθευση από πολλούς υπολογιστές διασφαλίζει ότι μπορούμε να εμπιστευτούμε κάθε μπλοκ που βρίσκεται στην αλυσίδα. Λόγω ότι το δίκτυο κάνει την οικοδόμηση της εμπιστοσύνης για εμάς, έχουμε τη δυνατότητα να αλληλοεπιδράσουμε απευθείας με τα δεδομένα μας σε πραγματικό χρόνο. Έτσι το Blockchain με την τεχνολογία του αλλάζουν το παιχνίδι των συναλλαγών.

C. Δεν υπάρχουν μεσάζοντες.

Επί του παρόντος , όταν γίνονται συναλλαγές μεταξύ μας, δεν δείχνουμε σε άλλο άτομο το οικονομικό ή επιχειρηματικό μας ιστορικό. Αντιθέτως, απαντάμε σε ‘εμπίστους μεσάζοντες, όπως είναι οι τράπεζες ή οι δικηγόροι, για να προβάλουν τα αρχεία μας και να διατηρήσουν τα δεδομένα εμπιστευτικά ασφαλή. Αυτοί οι μεσάζοντες δημιουργούν εμπιστοσύνη μεταξύ των συμβαλλόμενων μερών και μπορούν να επαληθεύσουν τα αρχεία.

Αυτός ο τύπος εμπιστοσύνης μεταξύ της αλληλεπίδρασης “peer-to-peer”, με τα δεδομένα μας, μπορεί να φέρει επανάσταση με τον τρόπο συναλλαγής. Επιπλέον, το Blockchain είναι ένας τύπος τεχνολογίας που μπορεί να εφαρμοστεί με πολλούς διαφορετικούς τρόπους. Για παράδειγμα κάποια Blockchain μπορεί να είναι εντελώς δημόσια και προσβάσιμα. Άλλοι τύποι μπορεί να είναι κλειστά σε μια επιλεγμένη ομάδα εξουσιοδοτημένων χρηστών, όπως υπάλληλοι εταιρειών, τράπεζες ή κρατικοί φορείς. Ακόμα, υπάρχουν τα υβριδικά δημόσιο-ιδιωτικά (hybrid public-private) Blockchain. Σε αυτή την περίπτωση το επίπεδο πρόσβασης προσαρμόζεται μεταξύ ιδιωτικών και δημόσιων τύπων με βάση την εφαρμογή για την οποία χρησιμοποιείται. Ως παράδειγμα, μια κυβέρνηση μπορεί να χρησιμοποιήσει Υβριδικό Blockchain ποιοι κατέχουν ιδιοκτησίες γης. Πληροφορίες που είναι δημόσια δεδομένα αλλά παράλληλα είναι και τα ιδιωτικά προσωπικά δεδομένα.

Συνεπώς, ο συνδυασμός όλων αυτών των παραγόντων (αποκέντρωση των δεδομένων, οικοδόμηση της εμπιστοσύνης και άμεση αλληλεπίδραση χωρίς μεσάζοντες), δίνει στην τεχνολογία του Blockchain τη δυνατότητα να υποστηρίξει πολλούς τρόπους αλληλεπίδρασης και συναλλαγών μεταξύ μας. Ο κυριότερος στόχος του Blockchain είναι να επαναφέρει όλες

τις συναλλαγές αξίας σε όλον τον κόσμο. Για αυτό καθίσταται και ένα βασικός τομές έρευνας και μελέτης από πολλούς επιστήμονες ώστε να αξιοποιηθούν οι ευκαιρίες και οι προκλήσεις.

Δομή εργασίας

Παρακάτω θα αναλυθούν συνοπτικά τα κεφάλαια που θα ακολουθήσουν στην εργασία.

Εισαγωγή: Περιλαμβάνει μια εισαγωγή στον χώρο της τεχνολογίας του Blockchain.

Κεφάλαιο 1ο : Παρουσιάζει μια σύντομη εξήγηση των βασικών τεχνικών εννοιών πίσω από το Blockchain, όπως είναι η κρυπτογραφία, η αρχιτεκτονική των δικτύων και οι γλώσσες σεναρίων. Θα τεθούν τα θεμέλια της τεχνολογίας του Blockchain.

Κεφάλαιο 2ο : Παρουσιάζεται μια σύντομη ιστορία πίσω από την τεχνολογία του Blockchain. Επίσης θα γίνουν γνωστοί η έννοια, ο ορισμός και οι τύποι του Blockchain.

Κεφάλαιο 3ο : Αφού έχει γίνει κατανοητή η σημασία του Blockchain, στο κεφάλαιο αυτό θα παρουσιαστεί ο τρόπος λειτουργίας του Blockchain.

Κεφάλαιο 4ο : Στο κεφάλαιο αυτό θα παρουσιαστούν τα βασικά οφέλη που μπορούν να αποκτηθούν κατά την προσαρμογή και τη λειτουργία του Blockchain. Επίσης θα παρουσιαστούν προκλήσεις και τί μπορεί να δημιουργήσει αποτυχία στο Blockchain.

Κεφάλαιο 5ο : Περιλαμβάνει τη σχέση του Blockchain με το ψηφιακό μάρκετινγκ και κάποιες εφαρμογές του.

Κεφάλαιο 6ο : Θα δοθεί έμφαση στο Smart Contract , που θεωρείται ένα από τα πιθανά στοιχεία για περαιτέρω έρευνα στο μέλλον.

Κεφάλαιο 7ο : Blockchain στη βιομηχανία και προκλήσεις

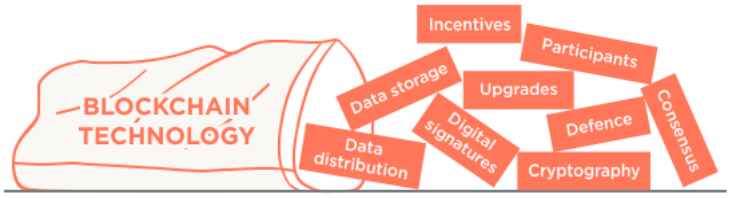
Κεφάλαιο 8ο : Blockchain Applications και μελέτες περίπτωσης

Συμπεράσματα: Περιλαμβάνει τα συμπεράσματα και τα πιο σημαντικά χαρακτηριστικά της μελέτης.

Κεφάλαιο 1ο Τεχνολογικό Υπόβαθρο

Η τεχνολογία του Blockchain μπορεί να θεωρηθεί ως ένα σακίδιο γεμάτο από τα απαραίτητα αντικείμενα όπως απεικονίζεται στην παρακάτω εικόνα. Τα Βασικά στοιχεία της είναι:

i. Κίνητρα,
ii. Αποθήκευση δεδομένων,
iii. Αναβάθμιση,
iv. Συμμετέχοντες,
v. Διανομή δεδομένων,
vi. Ψηφιακές υπογραφές,
vii. Προστασία-Άμυνα,
viii. Ομοφωνία και
ix. Κρυπτογράφηση.



Εικόνα 2 Απεικόνιση Τεχνολογίας Blockchain

Σε αυτό το κεφάλαιο θα δοθεί μια σύντομη εισαγωγή και επεξήγηση ορισμένων βασικών τεχνικών εννοιών που βρίσκονται πίσω από την Τεχνολογία Blockchain. Αυτές οι έννοιες είναι η Κρυπτογραφία (Cryptography), την αρχιτεκτονική των δικτύων (Network Architecture) και οι Σεναριακές Γλώσσες (Script Languages). Σε αυτό το κομμάτι της μελέτης θα γίνουν κατανοητά τα τεχνικά θεμέλια τη Τεχνολογίας του Blockchain. [40]

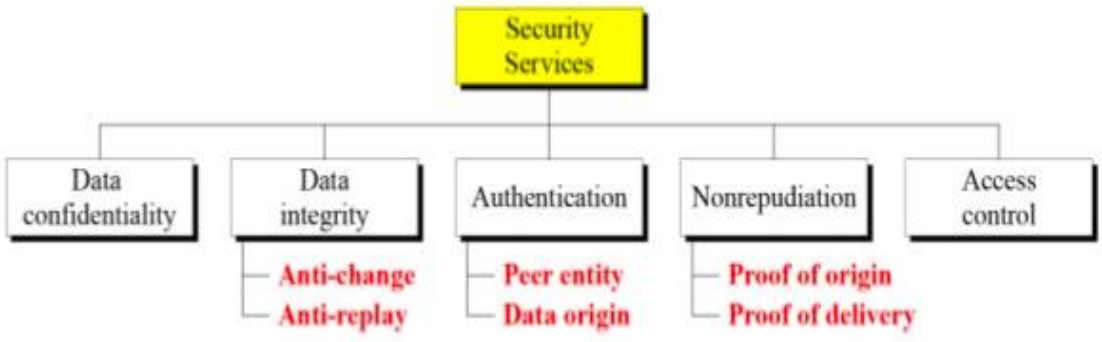
1.1 Κρυπτογραφία-Cryptography

Η Κρυπτογραφία είναι ένας κλάδος των μαθηματικών που χρησιμοποιείται ευρέως στην ασφάλεια των υπολογιστών. Στην Ελληνική γλώσσα, «Κρυπτογραφία» προέρχεται από τα συνθετικά «κρυπτός» και «γράφω» και σημαίνει *μυστική γραφή*. Ωστόσο, στην επιστήμη της της Κρυπτογραφίας είναι κάτι περισσότερο από μια μυστική μορφή γραφής. Δηλαδή, περιλαμβάνει περισσότερες μαθηματικές αποδείξεις.

Σε αυτή την ενότητα της εργασίας θα παρουσιαστούν μερικές βασικές κρυπτογραφίες που χρησιμοποιούνται στην Τεχνολογία του Blockchain [40].

Ξεκινώντας, η Κρυπτογραφία είναι η πρακτική και η μελέτη των τεχνικών για ασφαλή επικοινωνία με παρουσία τρίτων, που ονομάζονται αντίπαλοι (adversaries). Από τεχνική άποψη πρόκειται για την κατασκευή και την ανάλυση πρωτοκόλλων που εμποδίζουν τρίτα μέρη ή το κοινό να διαβάζουν προσωπικά μηνύματα. Επομένως, αυτή η τεχνική εγγυάται πολλές υπηρεσίες ασφάλειας των πληροφοριών όπως παρουσιάζεται στο σχήμα. Αυτές οι υπηρεσίες είναι:

i. Εμπιστευτικότητα των δεδομένων,
ii. Ακεραιότητα δεδομένων,
iii. Έλεγχος ταυτοποίησης,
iv. Μη-αποκήρυξη και
v. Έλεγχος πρόσβασης.



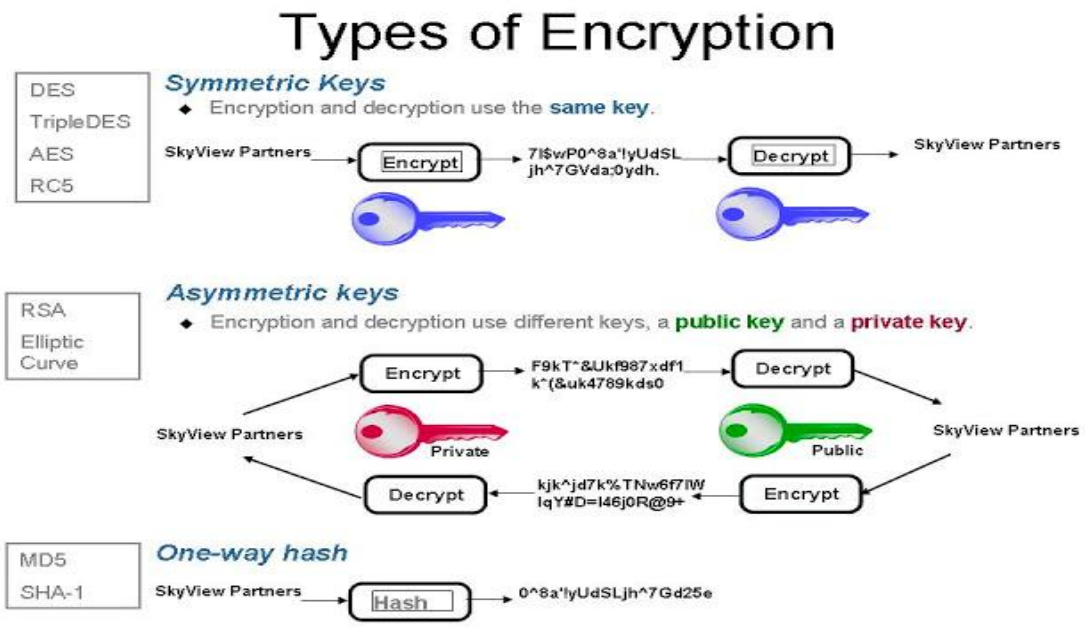
Εικόνα 3 Υπηρεσίες Ασφαλείας

Αυτές οι υπηρεσίες ασφαλείας επιτυγχάνονται με τη μετατροπή των δεδομένων, προκειμένου να τα καταστήσουν ανωφελή για ακούσιος αποδέκτες. Ως «Ανωφελή» σημαίνει τη ματαίωση δυο βασικών ενεργειών: την εξαγωγή πληροφοριών από τα δεδομένα και την εισαγωγή ψευδών δεδομένων ή τροποποίηση των δεδομένων αυτών. Αυτή η διαδικασία εγγυάται εξίσου τις υπηρεσίες εμπιστευτικότητας και ακεραιότητας. Επιπλέον, ως παράδειγμα μπορεί να παρουσιαστεί έναν αποστολέα να κρυπτογραφεί και να στέλνει ένα μήνυμα το οποίο αργότερα αρνείται ότι το έστειλε. Το να μην μπορεί ο αποστολέας να αρνηθεί την αποστολή συγκεκριμένων δεδομένων είναι ένας από τους βασικούς στόχους της Κρυπτογραφίας και ονομάζεται «Μη-αποκήρυξη» (Nonrepudiation). Στον πυρήνα της η Κρυπτογραφία είναι η θεωρία αλλά και σε μεγάλο βαθμό η πρακτική της πρόληψης και του εντοπισμού της εξαπάτησης καθώς και της απαγόρευσης πρόσβασης και χρήσης δεδομένων με τρίτους [40,41].

Επιπροσθέτως, η κρυπτογράφηση δεδομένων μπορεί να ταξινομηθεί σε τρεις κλάδους:

i. Χωρίς κλειδί (unkeyed),
ii. Με συμμετρικό κλειδί (symmetric-key) και
iii. Με ασύμμετρο κλειδί (asymmetric-key).

Τα πρωτόγονα «χωρίς κλειδί» είναι οι συναρτήσεις που δεν χρησιμοποιούν κάποιο κλειδί για την κρυπτογράφηση ενός μηνύματος πχ, κατακερματισμός αυθαίρετου (hash) και μεταθέσεων συνόλων (Permutation). Στην δεύτερη κατηγορία, τα πρωτόγονα συμμετρικού κλειδιού χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ενώ στην τρίτη περίπτωση του ασύμμετρου κλειδιού, η μέθοδος χρησιμοποιεί το σύστημα ενός δημόσιου κλειδιού και ενός ιδιωτικού (διαφορετικά και άνισα μεταξύ τους) που απαιτούνται και τα δύο για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.
Στο σχήμα παρακάτω απεικονίζονται και οι τρείς τύποι Κρυπτογραφίας. [40]



Εικόνα 4 Εικόνα Τύποι Κρυπτογραφίας

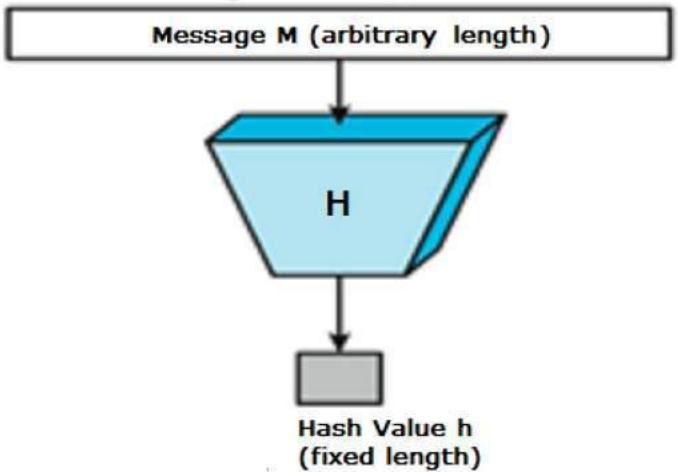
1.1.1 Βασική Τεχνολογία

Οι όροι κρυπτογραφία και κρυπτογράφηση χρησιμοποιούνται εναλλακτικά, και ουσιαστικά αναφέρονται στη διαδικασία μετατροπής συνηθισμένων πληροφοριών, που ονομάζεται «απλό κείμενο» (plaintext), σε ακατάληπτο κείμενο , το «κρυπτογραφημένο κείμενο» (ciphertext). Από την άλλη, αποκρυπτογράφηση είναι το αντίστροφο. Δηλαδή, είναι η μετάβαση από ακατάληπτο κρυπτογραφημένο κείμενο πίσω σε απλό κείμενο. Ως Cipher, είναι ένα ζεύγος αλγορίθμων που δημιουργούν την κρυπτογράφηση και την αποκρυπτογράφηση [40,41]

Η λεπτομερής λειτουργία ενός Cipher, ελέγχεται τόσο από τον αλγόριθμο όσο και σε κάθε περίπτωση από ένα «κλειδί». Το κλειδί είναι ένα μυστικό (ιδανικά είναι γνωστό μόνο σε όσους επικοινωνούν), και συνήθως είναι μια σύντομη σειρά χαρακτήρων που απαιτείται για την αποκρυπτογράφηση του κειμένου.

1.1.2 Συναρτήσεις Κατακερματισμού

Μια συνάρτηση κατακερματισμού είναι απλώς μια συνάρτηση που λαμβάνει την τιμή εισόδου και μέσω αυτήν την είσοδο δημιουργεί μια τιμή εξόδου η οποία είναι προσδιοριστική της πρώτης. Για οποιαδήποτε τιμή εισόδου X, η έξοδος θα λαμβάνει πάντα την ίδια τιμή εξόδου Y, όποτε εκτελείτε η συνάρτηση κατακερματισμού. Με αυτόν τον τρόπο, κάθε είσοδος έχει μια καθορισμένη έξοδο όπως φαίνεται και στο σχήμα παρακάτω.



Εικόνα 5 Συνάρτηση Κατακερματισμού

Επομένως, μια συνάρτηση κατακερματισμού είναι κάτι που λαμβάνει μια είσοδο (μπορεί να είναι οποιαδήποτε δεδομένα όπως αριθμοί, αρχεία κ.λπ.) και εξάγει έναν κατακερματισμό (hash). Ένας κατακερματισμός εμφανίζεται συνήθως ως δεκαεξαδικός αριθμός.

Επιπλέον, υπάρχουν διαφορετικοί αλγόριθμοι κατακερματισμού και οι πιο γνωστοί είναι MD, SHA. Οι συναρτήσεις κατακερματισμού είναι γενικά μη αναστρέψιμες (one way), το οποίο σημαίνει ότι δεν μπορούν να καταλάβουν την είσοδο εάν δεν γνωρίζουν την έξοδο. Η μόνη εξαίρεση είναι μόνο αν δοκιμάσουν κάθε πιθανή είσοδο (γνωστή ως brute-force attack) [40].

Τέλος, υπάρχουν πολλές εφαρμογές για συναρτήσεις κατακερματισμού, αλλά ο έλεγχος της ακεραιότητας των δεδομένων είναι η πιο κοινή. Αυτή η εφαρμογή χρησιμοποιείται για τη

δημιουργία ελέγχων των αρχείων δεδομένων. Επίσης παρέχει διαβεβαίωση στον χρήστη σχετικά με την ορθότητα των δεδομένων.

1.1.3 Public Key Infrastructure (PKI)

Το Public Key Infrastructure (PKI) [40,41] είναι ένα σύνολο απαιτήσεων που επιτρέπουν (μεταξύ άλλων) τη δημιουργία ψηφιακών υπογραφών. Μέσω του PKI, κάθε συναλλαγή ψηφιακής υπογραφής περιλαμβάνει ένα ζεύγος κλειδιών: ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Αρχικά το ιδιωτικό κλειδί δεν είναι κοινόχρηστο και χρησιμοποιείται μόνο από τον υπογράφοντα για την ηλεκτρονική υπογραφή εγγράφων. Στην δεύτερη περίπτωση, το δημόσιο κλειδί είναι ανοιχτά διαθέσιμο και χρησιμοποιείται από όσους χρειάζεται να επικυρώσουν την ηλεκτρονική υπογραφή του υπογράφοντος. Το PKI επιβάλλει πρόσθετες απαιτήσεις, όπως η Αρχή Πιστοποιητικών (Certificate Authority-CA), ένα ψηφιακό πιστοποιητικό, το λογισμικό εγγραφής του τελικού χρήστη (end-user enrollment software) και τα εργαλεία για τη διαχείριση, την ανανέωση και την ανάκληση των κλειδιών και των πιστοποιητικών.

1.1.4 Ψηφιακές Υπογραφές

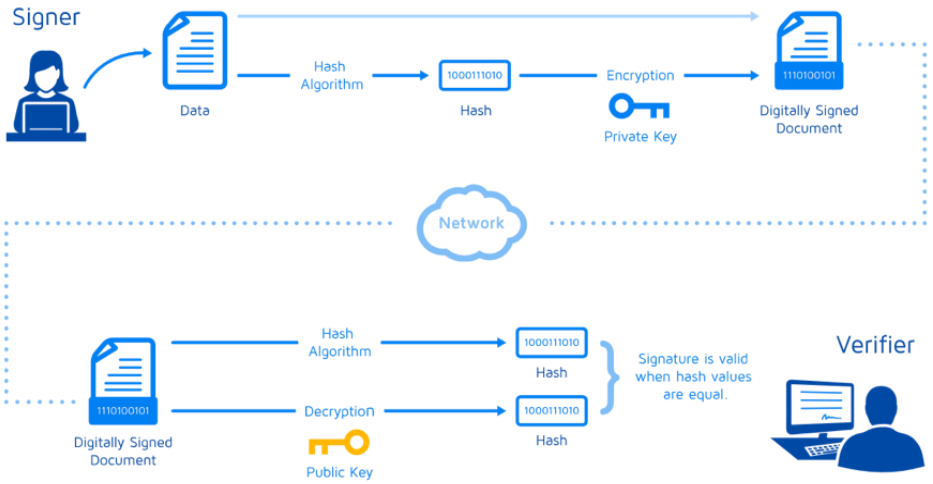
Η ψηφιακή υπογραφή είναι μια διαδικασία που εγγυάται ότι το περιεχόμενο ενός μηνύματος δεν έχει αλλοιωθεί κατά τη μεταφορά του. Όταν ο αποστολέας, ο διακομιστής (server), υπογράφει ψηφιακά ένα έγγραφο προσθέτει ένα one-way κατακερματισμό (κρυπτογράφηση) για το περιεχόμενο του μηνύματος χρησιμοποιώντας το ζεύγος δημοσίου και ιδιωτικού κλειδιού του. Ο πελάτης (client) μπορεί ακόμα να το διαβάσει, αλλά η διαδικασία δημιουργεί μια «υπογραφή» που μόνο το δημόσιο κλειδί του διακομιστή μπορεί να αποκρυπτογραφήσει. Έπειτα ο πελάτης χρησιμοποιώντας το δημόσιο κλειδί του διακομιστή, μπορεί να επικυρώσει τον αποστολέα καθώς και την ακεραιότητα του περιεχομένου του μηνύματος.

Στην περίπτωση που γίνει η μετάδοση του μηνύματος αλλά η ψηφιακή υπογραφή δεν ταιριάζει με το δημόσιο κλειδί στο ψηφιακό πιστοποιητικό, τότε ο πελάτης γνωρίζει ότι το μήνυμα που έλαβε έχει τροποποιηθεί [7].

Επομένως, η ψηφιακή υπογραφή είναι ένα μαθηματικό μοντέλο που παρουσιάζει την αυθεντικότητα των ψηφιακών μηνυμάτων ή εγγράφων. Επίσης, μια έγκυρη ψηφιακή υπογραφή προσφέρει στον παραλήπτη:

i. Λόγο να πιστεύει ότι το μήνυμα δημιουργήθηκε από κάποιον γνωστό αποστολέα (authentication),
ii. Να γνωρίζει ότι αποστολέας δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα (non-repudiation) και ότι
iii. Το μήνυμα δεν άλλαξε κατά την αποστολή του (integrity).

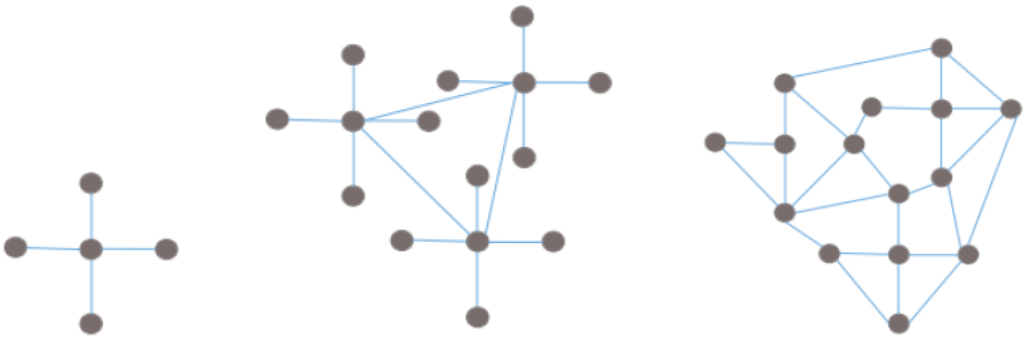
Επιπροσθέτως, όταν ο χρήστης υπογράφει ηλεκτρονικά ένα έγγραφο, η υπογραφή δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί του, το οποίο φυλάσσεται πάντα με ασφάλεια από τον υπογράφοντα. Ο μαθηματικός αλγόριθμος λειτουργεί σαν κρυπτογράφηση, δημιουργώντας δεδομένα που ταιριάζουν με το υπογεγραμμένο έγγραφο και ονομάζεται κατακερματισμός. Τα κρυπτογραφημένα δεδομένα που προκύπτουν είναι η ψηφιακή υπογραφή και σημειώνεται με την ώρα που έγινε. Ένα το έγγραφο αλλάξει μετά την υπογραφή, η ψηφιακή υπογραφή ακυρώνεται.
Ως παράδειγμα που απεικονίζεται παρακάτω, συνοψίζεται η διαδικασία της συνάρτησης κατακερματισμού, της κρυπτογράφησης ιδιωτικών και δημόσιων κλειδιών και της ψηφιακής υπογραφής [7].



Εικόνα 6 Διαδικασία της συνάρτησης κατακερματισμού, της κρυπτογράφησης ιδιωτικών και δημόσιων κλειδιών και της ψηφιακής υπογραφής.

1.2 Αρχιτεκτονική Δικτύων

Βασικό χαρακτηριστικό της τεχνολογίας του Blockchain έγκειται στην κατανεμημένη φύση του (distributed nature). Σε αντίθεση με τα κεντρικά και τα αποκεντρωμένα δίκτυα , στο παρακάτω σχήμα φαίνονται οι διαφορές ανάμεσα σε αυτές τις τρεις αρχιτεκτονικές δικτύων [24].



Εικόνα 7 Εικόνα Διαφορές ανάμεσα στις αρχιτεκτονικές δικτύων

Ένα σύστημα κατανεμημένου Δικτύου Υπολογιστών (Distributed Computing Network), είναι ένα σύστημα όπου τα δεδομένα και οι πόροι κατανέμονται σε διάφορους κόμβους υλικού. Είναι δομημένο ως αρχιτεκτονική δικτύου peer-to-peer πάνω στο Διαδίκτυο. Ο όρος peer-to-peer (P2P) σημαίνει ότι οι υπολογιστές που συμμετέχουν στο δίκτυο είναι ομότιμοι μεταξύ του, δηλαδή είναι όλοι ίσοι και ίδιοι. Ακόμα, όλοι οι κόμβοι του δικτύου μοιράζονται την προσπάθεια για παροχή υπηρεσιών ταυτόχρονα. Η κατανομή του ελέγχου στην τεχνολογία του Blockchain και η εφαρμογή στο Bitcoin είναι μια βασική αρχή σχεδιασμού που μπορεί να επιτευχθεί και διατηρηθεί μόνο από την αρχιτεκτονική δικτύου P2P [24].

Επιπλέον, στο σενάριο του Blockchain, κάθε κόμβος διατηρεί μια βάση δεδομένων (καθολικό) όλων των έγκυρων συναλλαγών, οι οποίες αποστέλλονται μεταξύ των κόμβων του δικτύου. Παρόλο που κάθε κόμβος έχει ένα αντίγραφο του καθολικού, μόνο οι χρήστες που έχουν την ψηφιακή υπογραφή για αυτό, μπορούν να έχουν πρόσβαση στις πληροφορίες. Αυτό συνεπάγεται ότι το κοινόχρηστο καθολικό μπορεί να θεωρηθεί ως δοχείο– container (blocks) που αποθηκεύονται τα δεδομένα. Ωστόσο, αυτά τα δοχεία είναι σφραγισμένα και το περιεχόμενό τους μπορούν να τα δουν μόνο όσοι έχουν την άδεια [43,44].

Οι κόμβοι αναγνωρίζουν ο ένας τον άλλον από τη διεύθυνση IP τους, ενώ οι χρήστες απευθύνονται ο ένας στον άλλον μέσω του δημόσιου κλειδιού τους. Επομένως, κάθε κόμβος μπορεί να στείλει μια συναλλαγή σε κάθε άλλο κόμβο του δικτύου εάν γνωρίζει το δημόσιο κλειδί του παραλήπτη. Και σε όλη αυτή τη διαδικασία δεν εμπλέκεται καμία κεντρική αρχή.

1.3 Σεναριακές Γλώσσες

Η γλώσσα που χρησιμοποιείται στις συναλλαγές στην Τεχνολογία του Blockchain ονομάζεται Script. Η Script είναι μια πολύ απλή γλώσσα προγραμματισμού που σχεδιάστηκε για περιορισμένο εύρος και εκτέλεση για μια σειρά υπολογιστών. Απαιτεί ελάχιστη επεξεργασία και δεν μπορεί να κάνει πολλές από τις προηγμένες εργασίες που μπορούν να κάνουν άλλες σύγχρονες γλώσσες προγραμματισμού. Αυτό σημαίνει ότι τα σενάρια έχουν περιορισμένη πολυπλοκότητα και προβλέψιμους χρόνους εκτέλεσής τους [24]. Ωστόσο, αυτός ο περιορισμός είναι ένα πλεονέκτημα καθώς διασφαλίζει ότι η γλώσσα δεν μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός άπειρου βρόχου (infinite loop) ή ΄άλλης μορφής λογικών επιθέσεων (logic attacks) .

Κάθε συναλλαγή επικυρώνεται από κάθε πλήρη κόμβο το δίκτυο, επομένως μια περιορισμένη γλώσσα αποτρέπει τη χρήση της επικύρωσης της συναλλαγής ως τρωτή.
Επιπλέον, η σεναριακή γλώσσα συναλλαγών είναι ανιθαγενής, καθώς δεν υπάρχει κατάσταση πριν από την εκτέλεση του σεναρίου, ή στάδιο που αποθηκεύεται μετά την εκτέλεση του.

Υπάρχουν δύο τύποι σεναρίων στα οποία βασίζεται το Blockchain για την επικύρωση των συναλλαγών. Αυτοί είναι:

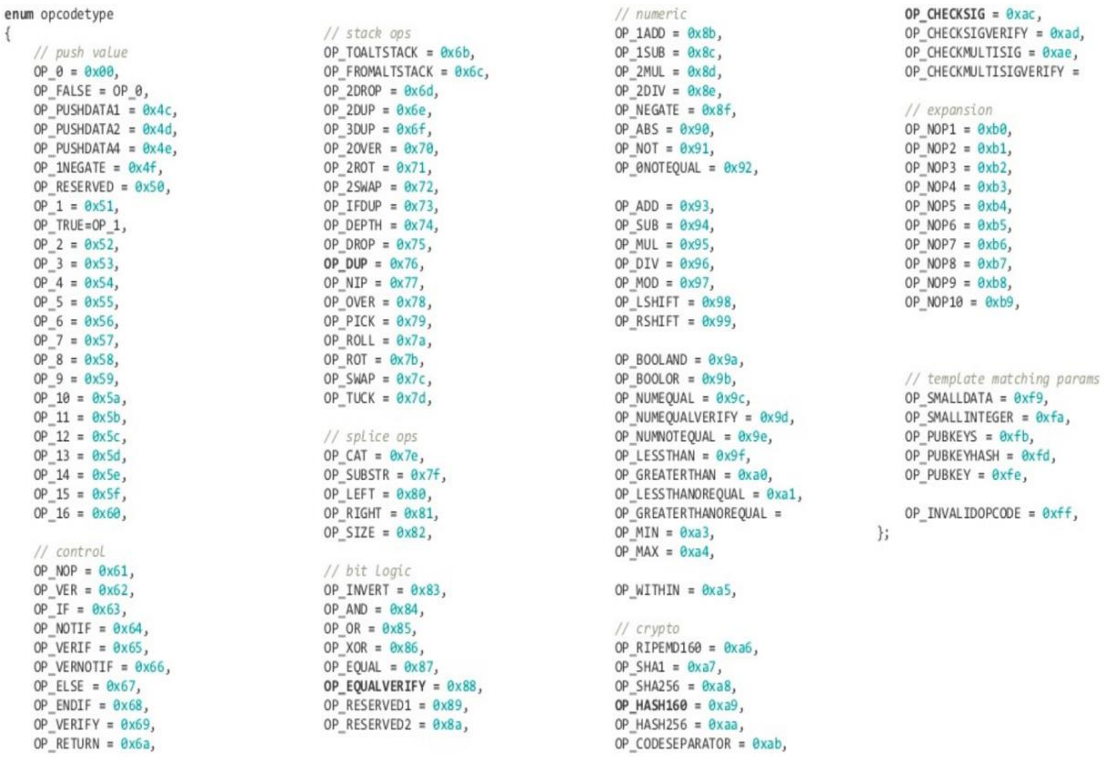
i. Ένα σενάριο κλειδώματος (locking script) : θεωρείται μια συνθήκη δαπανών που εκτελείται σε κάθε έξοδο. Καθορίζει τις προϋποθέσεις που πρέπει να πληρούνται για να δαπανηθεί η έξοδος στο μέλλον.
ii. Ένα σενάριο ξεκλειδώματος (unlocking script): είναι μια δέσμη ενεργειών που επιλύει τις συνθήκες που τίθενται σε μια έξοδο, κλειδώνοντάς τη δέσμη αυτή. Επιτρέπει να

δαπανηθεί η έξοδος. (πχ όταν η ‘έξοδος χρησιμοποιείται σαν είσοδος στην επόμενη συναλλαγή).

Επιπροσθέτως, η συναλλαγή θα επικυρωθεί εκτελώντας μαζί τα σενάρια κλειδώματος και ξεκλειδώματος. Το σενάριο κλειδώματος περιείχε συνήθως τον κατακερματισμό του δημοσίου κλειδιού και παλαιότερα ήταν γνωστό με τις ονομασίες: scriptPubKey, witness script και cryptographic puzzle. Ενώ το σενάριο ξεκλειδώματος περιέχει τις περισσότερες φορές την ψηφιακή υπογραφή που παράγεται από το ιδιωτικό κλειδί του χρήστη και είναι γνωστό αλλιώς ως scriptSig [24].

Το σενάριο (script) αποτελείται από δύο είδη:

i. Τα δεδομένα (data): τις υπογραφές και τα δημόσια κλειδιά
ii. OPCODES: είναι απλές λειτουργίες που διαχειρίζονται τα δεδομένα. Παρακάτω παρουσιάζεται η λίστα με όλους τους τύπους OPCODES που χρησιμοποιούνται σε σενάρια.



```
enum opcodetype
{
    // push value
    OP_0 = 0x00,
    OP_FALSE = OP_0,
    OP_PUSHDATA1 = 0x4c,
    OP_PUSHDATA2 = 0x4d,
    OP_PUSHDATA4 = 0x4e,
    OP_1NEGATE = 0x4f,
    OP_RESERVED = 0x50,
    OP_1 = 0x51,
    OP_TRUE=OP_1,
    OP_2 = 0x52,
    OP_3 = 0x53,
    OP_4 = 0x54,
    OP_5 = 0x55,
    OP_6 = 0x56,
    OP_7 = 0x57,
    OP_8 = 0x58,
    OP_9 = 0x59,
    OP_10 = 0x5a,
    OP_11 = 0x5b,
    OP_12 = 0x5c,
    OP_13 = 0x5d,
    OP_14 = 0x5e,
    OP_15 = 0x5f,
    OP_16 = 0x60,

    // control
    OP_NOP = 0x61,
    OP_VER = 0x62,
    OP_IF = 0x63,
    OP_NOTIF = 0x64,
    OP_VERIF = 0x65,
    OP_VERNOTIF = 0x66,
    OP_ELSE = 0x67,
    OP_ENDIF = 0x68,
    OP_VERIFY = 0x69,
    OP_RETURN = 0x6a,

    // stack ops
    OP_TOALTSTACK = 0x6b,
    OP_FROMALTSTACK = 0x6c,
    OP_2DROP = 0x6d,
    OP_2DUP = 0x6e,
    OP_3DUP = 0x6f,
    OP_2OVER = 0x70,
    OP_2ROT = 0x71,
    OP_2SWAP = 0x72,
    OP_IFDUP = 0x73,
    OP_DEPTH = 0x74,
    OP_DROP = 0x75,
    OP_DUP = 0x76,
    OP_NIP = 0x77,
    OP_OVER = 0x78,
    OP_PICK = 0x79,
    OP_ROLL = 0x7a,
    OP_ROT = 0x7b,
    OP_SWAP = 0x7c,
    OP_TUCK = 0x7d,

    // splice ops
    OP_CAT = 0x7e,
    OP_SUBSTR = 0x7f,
    OP_LEFT = 0x80,
    OP_RIGHT = 0x81,
    OP_SIZE = 0x82,

    // bit logic
    OP_INVERT = 0x83,
    OP_AND = 0x84,
    OP_OR = 0x85,
    OP_XOR = 0x86,
    OP_EQUAL = 0x87,
    OP_EQUALVERIFY = 0x88,
    OP_RESERVED1 = 0x89,
    OP_RESERVED2 = 0x8a,

    // numeric
    OP_1ADD = 0x8b,
    OP_1SUB = 0x8c,
    OP_2MUL = 0x8d,
    OP_2DIV = 0x8e,
    OP_NEGATE = 0x8f,
    OP_ABS = 0x90,
    OP_NOT = 0x91,
    OP_0NOTEQUAL = 0x92,

    OP_ADD = 0x93,
    OP_SUB = 0x94,
    OP_MUL = 0x95,
    OP_DIV = 0x96,
    OP_MOD = 0x97,
    OP_LSHIFT = 0x98,
    OP_RSHIFT = 0x99,

    OP_BOOLAND = 0x9a,
    OP_BOOLOR = 0x9b,
    OP_NUMEQUAL = 0x9c,
    OP_NUMEQUALVERIFY = 0x9d,
    OP_NUMNOTEQUAL = 0x9e,
    OP_LESSTHAN = 0x9f,
    OP_GREATERTHAN = 0xa0,
    OP_LESSTHANOREQUAL = 0xa1,
    OP_GREATERTHANOREQUAL =
    OP_MIN = 0xa3,
    OP_MAX = 0xa4,

    OP_WITHIN = 0xa5,

    // crypto
    OP_RIPEMD160 = 0xa6,
    OP_SHA1 = 0xa7,
    OP_SHA256 = 0xa8,
    OP_HASH160 = 0xa9,
    OP_HASH256 = 0xaa,
    OP_CODESEPARATOR = 0xab,

    OP_CHECKSIG = 0xac,
    OP_CHECKSIGVERIFY = 0xad,
    OP_CHECKMULTISIG = 0xae,
    OP_CHECKMULTISIGVERIFY =

    // expansion
    OP_NOP1 = 0xb0,
    OP_NOP2 = 0xb1,
    OP_NOP3 = 0xb2,
    OP_NOP4 = 0xb3,
    OP_NOP5 = 0xb4,
    OP_NOP6 = 0xb5,
    OP_NOP7 = 0xb6,
    OP_NOP8 = 0xb7,
    OP_NOP9 = 0xb8,
    OP_NOP10 = 0xb9,


    // template matching params
    OP_SMALLDATA = 0xf9,
    OP_SMALLINTEGER = 0xfa,
    OP_PUBKEYS = 0xfb,
    OP_PUBKEYHASH = 0xfd,
    OP_PUBKEY = 0xfe,

    OP_INVALIDOPCODE = 0xff,
};
```

Εικόνα 8 Εικόνα Λίστα με όλους τους τύπους OPCODES που χρησιμοποιούνται σε σενάρια

Ωστόσο πολλές εφαρμογές του Blockchain [24] βασίζονται στα βασικά τυποποιημένα σενάρια που είναι:

- Pay To Pubkey (P2PK).
- Pay To Pubkey Hash (P2PKH).
- Pay To Multisig (P2MS).
- Pay To Script Hash (P2SH).

Επίσης, η γλώσσα σεναρίων ονομάζεται ακόμα stack-based , δηλαδή που βασίζεται σε στοιβάδα επειδή χρησιμοποιεί μια δομή δεδομένων, τη στοίβα. Μια στοίβα είναι πολύ απλής μορφής και επιτρέπει δυο λειτουργίες, την push και pop.
Η λειτουργία PUSH προσθέτει ένα στοιχείο στην κορυφή της στοίβας ενώ η POP αφαιρεί το επάνω στοιχείο της.

Οι λειτουργίες που συμβαίνουν σε μια στοίβα ενεργούν μόνο στο ανώτατο στοιχείο της και μια δομή δεδομένων ονομάζεται επίσης LIFO σειρά (Last-In-First-Out queue).

Κεφάλαιο 2ο Τί είναι το Blockchain

Σε αυτό το κεφάλαιο θα γίνει μια σύντομη ιστορική αναδρομή πίσω από την τεχνολογία του Blockchain και θα παρουσιαστεί η ιδέα, η έννοια και οι τύποι του.

2.1 Μια σύντομη ιστορική αναδρομή στην Τεχνολογία Blockchain

Προκειμένου να γίνει πλήρως κατανοητή η έννοια του Blockchain, θα πρέπει να γίνει μια μικρή αναδρομή στο ιστορικό της ιδέας αυτής.

Ξεκινώντας, η αρχική ιδέα γεννήθηκε το 2008 όταν το Bitcoin εισήχθη στον τεχνολογικό κόσμο από ένα άγνωστο άτομο (ή ομάδα), με το όνομα Satoshi Nakamoto. Ο ίδιος παρουσίαση τη λευκή βίβλο του, μια εργασία με τίτλο “Bitcoin: A Peer-to-Peer Cash System” [23].

Σε αυτή την εργασία, περιέγραψε τις τεχνολογίες για την υποστήριξη συναλλαγών ψηφιακού νομίσματος ή ηλεκτρονικών πληρωμών απευθείας από το ένα μέρος στο άλλο χωρίς να περάσουν από κάποιο χρηματοπιστωτικό ίδρυμα. Από τότε το Bitcoin έχει γίνει πρωταγωνιστής καθώς το πρόγραμμα ανοιχτού κώδικα έγινε διαθέσιμο στο κοινό όπου ο καθένας μπορεί να το εγκαταστήσει και να εγγραφεί στο δίκτυο Bitcoin P2P.

Το όνομα “Blockchain” καθιερώθηκε από το 2014, μέχρι τότε στη «λευκή βίβλο» Nakamoto, οι λέξεις “block” και “chain” τις χρησιμοποιούσαν ξεχωριστά.

Επιπλέον, αυτό που διακρίνει την τεχνολογία του Blockchain από τις άλλες προηγμένες τεχνολογίες διαδικτυακών πληρωμών είναι ότι υποστηρίζει το Bitcoin. Αυτός ήταν και ένας σημαντικός παράγοντας επιτυχίας του οδήγησε στην επιτυχία του Bitcoin, καθώς υπήρχε άνοδος καινοτόμων ιδεών και υπηρεσιών που επεκτείνουν τις εφαρμογές του Blockchain [23].

2.2 Η ιδέα πίσω από την Τεχνολογία του Blockchain

Αρχικά η ιδέα του Blockchain γεννήθηκε πρώτη φορά με την εφαρμογή του Bitcoin ως ψηφιακό νόμισμα. Ωστόσο πολλοί επαγγελματίες και ειδικοί πιστεύουν ότι η έννοια της τεχνολογίας του Blockchain μπορεί να χρησιμοποιηθεί πέρα από το Bitcoin. Σε εφαρμογές

όπως έργα ως δημόσιο καθολικό για κάθε τύπων συναλλαγών και όχι σε ψηφιακό νόμισμα. Ένα ακόμα παράδειγμα είναι ότι πολλοί επιστήμονες πιστεύουν ότι η τεχνολογία έχει μεγάλο αντίκτυπο στον ενεργειακό τομέα, τις εφοδιαστικές αλυσίδες, τη μουσική βιομηχανία και τον υγειονομικό τομέα.

Παρακάτω θα παρουσιαστούν οι τρεις προτεινόμενες γενιές του Blockchain.

Type	Description	Examples
Blockchain 1.0	Currency	Cryptocurrencies like Bitcoin. Was first introduced in 2009.
Blockchain 2.0	Contracts	Financial services, crowdfunding, Bitcoin prediction markets, smart property, smart contracts. Was introduced through the release of NXT in 2013.
Blockchain 3.0	Justice, efficiency and coordination applications beyond currency, economics, and markets	Digital Identity, Intellectual Property Protection, Governance Services, Elections. Solutions within these areas of applications are starting to take form.

Εικόνα 9 οι Γενιές του Blockchain

Η πρώτη είναι το Blockchain 1.0 που αναφέρεται στο ψηφιακό νόμισμα. Η δεύτερη το Blockchain 2.0 που υποστηρίζει την ψηφιακή οικονομία και τέλος η Blockchain 3.0 που βασίζεται στην ψηφιακή κοινωνία.

Βασικός λόγος για τον οποίο δεν υπάρχει γενικά αποδεκτός ορισμός της έννοιας του Blockchain μεταξύ ερευνητών και επαγγελματιών είναι διότι η κάθε πλευρά χρησιμοποιεί την τεχνολογία σε διαφορετικούς τομείς και κλάδους. Ως δεύτερη αιτιολογία μπορεί να θεωρηθεί ότι το Blockchain είναι ένα αναδυόμενο πεδίο έρευνας που δεν έχει ενοποιημένη ορολογία και καθορισμένες έννοιες.

Ορισμός με βάση τον Drescher [45]

> *«Το Blockchain είναι ένα καθαρά κατανεμημένο Peer-to-Peer σύστημα λογιστικών βιβλίων που χρησιμοποιεί μια μονάδα λογισμικού που αποτελείται από ένα αλγόριθμο, ο οποίος διαπραγματεύεται αυτό το ενημερωτικό περιεχόμενο που σχετίζεται με τα συνδεδεμένα μπλοκ δεδομένων. Αυτό γίνεται μαζί με τις τεχνολογίες κρυπτογράφησης και ασφάλειας για την επίτευξη και τη διατήρηση της ακεραιότητας».*

Ορισμός με βάση τον Ølnes [46]

> *«Το Blockchain είναι μια ανοιχτή, κατανεμημένη και αξιόπιστη βάση δεδομένων στο Διαδίκτυο».*

Ορισμός με βάση των Seebacher και Schüritz [15]

> *«Το Blockchain είναι μια κατανεμημένη βάση δεδομένων, η οποία μοιράζεται και συμφωνείται σε ένα δίκτυο peer-to-peer. Αποτελείται από μια συνδεδεμένη ακολουθία μπλοκ, που περιέχει συναλλαγές με χρονική σήμανση που είναι ασφαλισμένες με κρυπτογραφία δημόσιου κλειδιού και επαληθεύεται από την κοινότητα του δικτύου. Μόλις ένα στοιχείο προσαρτηθεί στην αλυσίδα, δεν μπορεί να αλλάξει. Με αυτόν τον τρόπο ένα Blockchain μετατρέπεται σε ένα αμετάβλητο αρχείο παλαιότερης δραστηριότητας».*

Ορισμός με βάση του Bilonia [47]

> *«Το Blockchain είναι μια αποκεντρωμένη κατανεμημένη βάση δεδομένων με αμετάβλητα αρχεία, όπου οι συναλλαγές προστατεύονται από ισχυρούς κρυπτογραφικούς αλγόριθμους και η κατάσταση του Δικτύου διατηρείται από τον αλγόριθμο Consensus».*

Είναι σαφές ότι υπάρχει συναίνεση μεταξύ των ερευνητών ότι το Blockchain είναι μια συνδεδεμένη ομάδα κατακερματισμένων συναλλαγών που αναπαράγονται μεταξύ των συμμετεχόντων και δημιουργεί μια κατανεμημένη ανοιχτή βάση δεδομένων. Όπως δηλαδή είναι το Διαδίκτυο ανοιχτό για νέους συμμετέχοντες και νέες μεγάλες καινοτομίες. Επίσης είναι ουδέτερη καθώς οι συναλλαγές δρομολογούνται μεταξύ των συμμετεχόντων χωρίς να λαμβάνεται υπόψη το ίδιο το περιεχόμενο ή η πηγή αυτού. Ακόμα, η βάση δεδομένων είναι αποκεντρωμένη, διότι καμία κεντρική αρχή δεν ελέγχει τις συναλλαγές της και τα εμπλεκόμενα μέρη. Τέλος είναι αμετάβλητη, καθώς το περιεχόμενο του ιστού δεν μπορεί να διαγραφεί και οι συναλλαγές δεν μπορούν να είναι αδέσμευτες [23].

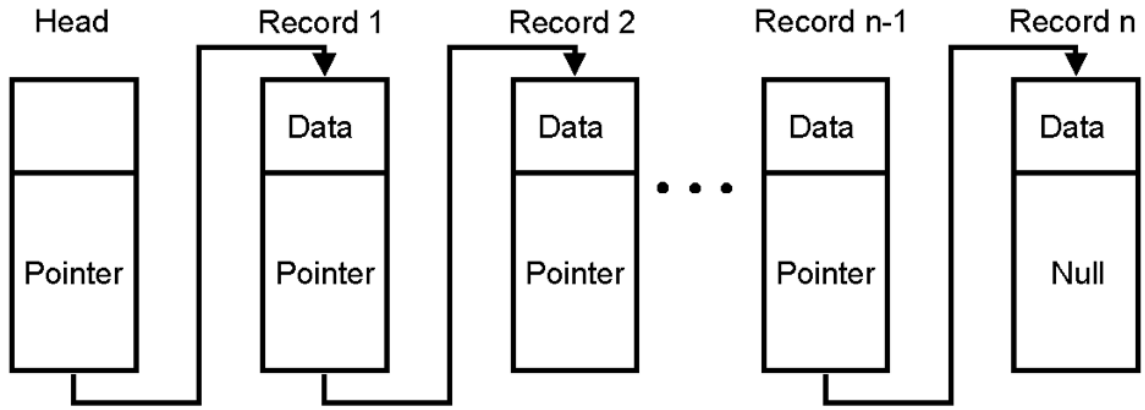
Συνοψίζοντας, το ενδιαφέρον μέρος του Blockchain είναι η ανοιχτή φύση του. Σημαίνει, δηλαδή, ότι το Blockchain από μόνο του ως τεχνολογία είναι απαραίτητο συστατικό αλλά δεν

είναι αρκετό για να δημιουργήσει την πραγματική μαγεία ως μια πλατφόρμα εμπιστοσύνης που δεν ελέγχεται από κανέναν και δεν μπορεί να διαγραφεί ή να αλλάξει μετά την καταγραφή των συναλλαγών.

Είναι προφανές ότι αυτά τα χαρακτηριστικά δεν αφορούν το Blockchain από μόνα τους. Στην πραγματικότητα, εάν το Blockchain εφαρμόζεται σε ένα περιβάλλον που είναι κλειστό θα ελέγχεται από ένα μέρος. Όπως αυτό το μέρος να αποφασίσει ποιες συναλλαγές θα καταγραφούν και ποιες δεν είναι καλές συναλλαγές που δεν θα καταγραφούν. Τότε, σίγουρα θα χάσει όλα τα ενδιαφέροντα χαρακτηριστικά του. Επομένως, ορισμένοι ειδικοί του Blockchain ,προτιμούν να χρησιμοποιούν τη λέξη OPEN μπροστά από το Blockchain. Όπου, αναφέρουν την έννοια του ΑΝΟΙΚΤΟ, ως ανοιχτή πρόσβαση, ανοιχτού κώδικα, ανοιχτό στις καινοτομίες χωρίς άδεια και κανέναν έλεγχο.

2.3 Γιατί ονομάζεται “Blockchain”

Όπως περιγράφεται στο παράδειγμα της βιβλιοθήκης στην εισαγωγή, κάθε φορά που προσφέρεται ή δανείζεται ένα βιβλίο μεταξύ των συμμετεχόντων στο δίκτυο της βιβλιοθήκης, δημιουργείται μια συναλλαγή [24]. Ταυτόχρονα μπορούν να γίνουν πολλές διαφορετικές συναλλαγές στο ίδιο δίκτυο. Αυτές οι νέες συναλλαγές που πραγματοποιήθηκαν θα ομαδοποιηθούν ως μπλοκ και θα προστεθεί πάνω από τα προηγούμενα μπλοκ της αλυσίδας (προηγούμενες συναλλαγές χρονικά) [23]. Στο παρακάτω σχήμα φαίνεται πως λειτουργεί μια τέτοια αλυσίδα.



Εικόνα 10 Μια αλυσίδα από μπλοκ (Chain of Blocks)

Καθώς κάθε συναλλαγή σε κάθε μπλοκ πραγματοποιείται σε μια συγκεκριμένη χρονική στιγμή, τότε κάθε μπλοκ συνδέεται με το προηγούμενο. Συνεπώς, συνδέοντας τα μπλοκ μεταξύ τους δημιουργείται μια αλυσίδα από μπλοκ (Chain of Blocks), εξ' ου και το όνομα της τεχνολογίας "Blockchain". Από το 2014 το Blockchain θεωρείται από κάποιους επιστήμονες ως νέες εφαρμογές της κατανεμημένης βάσης δεδομένων.

2.4 Blockchain vs Bitcoin

Όλοι οι ερευνητές συμφώνησαν ότι η πρώτη έμμεση αναφορά στον όρο Blockchain εισήχθη για πρώτη φορά από τον Satoshi Nakamoto [23] στην εργασία του με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System". Σε αυτή την εργασία αναφέρεται στα μπλοκ ως ένα από τα υποκείμενα στοιχεία που υποστηρίζουν το προτεινόμενο ηλεκτρονικό σύστημα μετρητών, που ονομάζεται Bitcoin. Πρέπει να σημειωθεί ότι πίσω από το Bitcoin κρύβονται και άλλες τεχνολογίες για αυτό τον λόγο δεν μπορούμε να την θεωρήσουμε ως τη τεχνολογία που υποστηρίζει την επιτυχία του Bitcoin.

Επιπλέον, είναι σημαντικό να σημειωθεί ότι δεν πρέπει να χρησιμοποιούνται οι όροι "Bitcoin" και "Blockchain" εναλλακτικά. Αυτός ο συσχετισμός γίνεται συχνά διότι το Bitcoin ήταν η πρώτη κυρίαρχη εφαρμογή του Blockchain και έτσι διαδόθηκε η τεχνολογία περαιτέρω [46].

Το Bitcoin είναι ένα ψηφιακό νόμισμα, που χρησιμοποιείται κυρίως ως μια νέα μέθοδος πληρωμής η οποία βασίζεται στην τεχνολογία του Blockchain στο κύριο μέρος της τεχνολογικής ραχοκοκαλιάς του. Ωστόσο, το Blockchain δεν μπορεί να θεωρηθεί μόνο ως η τεχνολογία που υποστηρίζει σε μεγάλο βαθμό το Bitcoin, διότι είναι περισσότερα από αυτό. Δηλαδή, μπορεί να χρησιμοποιηθεί για την καταγραφή και την ασφαλή εξοικονόμηση οποιασδήποτε συναλλαγής ανεξαρτήτου μορφής (οικονομικής ή μη). Πολλές εταιρίες και κυβερνήσεις αναπτύσσουν εφαρμογές και αναπτύσσονται πάνω στην Blockchain τεχνολογία.

2.5 Τύποι του Blockchain

Υπάρχουν διαφορετικές επιλογές για την σχεδίαση των μοντέλων ενός Blockchain, αυτές οι επιλογές ταξινομούνται με βάση ποιος πρέπει να του επιτρέπεται να συμμετέχει και να παρατηρεί τα δεδομένα στο δίκτυο Blockchain [48].

Βάσει του παραπάνω, υπάρχουν τρεις τύποι Blockchain.

i. Το ιδιωτικό (private Blockchain),
ii. το κοινοπρακτικό (consortium Blockchain) στο οποίο μια ομάδα οργανισμών μοιράζονται το ίδιο ενδιαφέρον ή ανησυχία , και
iii. το δημόσιο (public Blockchain)

Πολλοί θεωρούν το κοινοπρακτικό ως έναν τύπο ιδιωτικού Blockchain, αυτό έχει ευρύτερο πεδίο εφαρμογής καθώς ομαδοποιεί ορισμένους τομείς υπό το ίδιο δίκτυο Blockchain [23]. Παραδείγματος χάριν τέτοιοι τομείς μπορεί να είναι οι τράπεζες και άλλες χρηματοοικονομικές εταιρείες.

Οι παραπάνω τρεις τύποι μερικές φορές ομαδοποιούνται ξανά σε τρεις κατηγορίες με βάση την προοπτική *άδειας* που θα λάβουν. Αυτές οι κατηγορίες είναι οι εξής:

i. Ανοιχτό Blockchain για ανοιχτή πρόσβαση ,
ii. Κλειστό Blockchain για περιορισμένη πρόσβαση, και
iii. Υβριδικό Blockchain για προσαρμοσμένη πρόσβαση.

Επιπρόσθετα, ο πρώτος και κλασικός τύπος Blockchain είναι το δημόσιο (Permissionless), όπως είναι το Blockchain του Bitcoin. Αυτός ο τύπος ονομάζεται «δημόσιος» με την έννοια ότι τα δίκτυα είναι ανοιχτά στο ευρύ κοινό να ενταχθούν ως χρήστες ή να λειτουργούν ως κόμβοι. Επίσης τα δεδομένα της αλυσίδας είναι δημοσίως διαφανή. Ωστόσο, αυτός ο τύπος επιτρέπει περισσότερες δυνατότητας παραβίασης του Blockchain (hacking). Γεγονός που είχε παρατηρηθεί στο περιβόητο DAO-hack , όπου περίπου 50 εκατομμύρια δολάρια αποσπάστηκαν από ένα ETH Fund [1]. Ένα ακόμα χαρακτηριστικό του ανοιχτού τύπου, είναι ότι σπάει το απόρρητο των δεδομένων καθώς όλοι όσοι επιθυμούν να εγγραφούν στο δίκτυο μπορούν να τα δουν. Επομένως, ο «χωρίς άδεια» τύπος του Blockchain [48], δεν είναι γενικά αποδεκτός από τους υποστηρικτές της τεχνολογίας αυτής και από τα οφέλη που θέλουν να έχουν. Ως εκ τούτου , αναπτύχθηκαν οι “Permissioned” αλυσίδες. Η αρχή αυτών είναι ότι υπάρχει κανονισμός για το ποιος επιτρέπεται να ενταχθεί και να συμμετέχει στο δίκτυο.

Τα Blockchain μπορούν να γίνουν περισσότερο ή λιγότερο ευέλικτα ή και ακόμα πιο συγκεκριμένα ως προς τις ενέργειες που επιτρέπουν στο δίκτυό τους. Σε αυτή την κατηγορία

συναντάμε τον τρίτο τύπο Blockchain, την υβριδική αλυσίδα, καθώς υπάρχει συσχέτιση μεταξύ επιτρεπόμενων και χωρίς άδεια Blockchain.

Αν και δεν υπάρχει ακόμα κάποια επίσημη ταξινόμηση για πολλές από τις πτυχές των τύπων σχεδιασμού Blockchain , ορισμένοι συγγραφείς προσπάθησαν να καλύψουν αυτό το κενό προτείνοντας μια σύγκριση μεταξύ αυτών των τύπων. Στο σχήμα παρουσιάζεται αυτή η σύγκριση με Blockchain με ή χωρίς αδειοδότηση και αν είναι γενικευμένη ή εξειδικευμένη η αλυσίδα. συνοδεύεται με ένα παράδειγμα για το καθένα.

	Permissionless	Permissioned
General purpose	Ethereum	Monax's eris-db
Specialised	Bitcoin	Multichain

Πιο συγκεκριμένα,

- **Ethereum:** είναι μια πλατφόρμα ανοιχτού λογισμικού, γενικού σκοπού και χωρίς άδεια που βασίζεται στην τεχνολογία του Blockchain. Επιτρέπει στους προγραμματιστές να δημιουργούν και να αναπτύσσουν αποκεντρωμένες εφαρμογές που αυτές εκτελούν έξυπνες συμβάσεις (Smart Contracts) [1].

- **Bitcoin:** είναι μια εφαρμογή εξειδικευμένου σκοπού (τα Κρυπτονομίσματα), μια μορφή ηλεκτρονικών μετρητών επίσης, είναι αποκεντρωμένο ψηφιακό νόμισμα χωρίς κεντρική τράπεζα ή ενιαίο διαχειριστή (open/ανοιχτό για συμμετοχή και χρήση από το κοινό). Μπορεί να αποσταλεί από χρήστη σε χρήστη στο δίκτυο P2P του, χωρίς να χρειάζονται μεσάζοντες [23].

- **Multichain:** είναι μια πλατφόρμα για τη δημιουργία ιδιωτικών Blockchain. Επιλύει τα σχετικά προβλήματα εξόρυξης (mining), του απορρήτου (privacy) και της διαφάνειας (openness). Αυτό υλοποιείται μέσω της ολοκληρωμένης διαχείρισης αδειών του χρήστη [49].

- **Monax's eris-db:** παρείχε μια δωρεάν πλατφόρμα ανοικτού κώδικα για να βοηθήσει τους προγραμματιστές να δημιουργήσουν, να στείλουν και να εκτελέσουν διάφορες εφαρμογές Blockchain και Smart Contract για επιχειρηματικά συστήματα. Αυτή η

πλατφόρμα είναι γνωστή ως. “eris-db” και ήταν ο πρώτος πελάτης Blockchain με επιτρεπόμενο (permissioned) σχεδιασμό αλυσίδας.

Συνοψίζοντας, στο κεφάλαιο αυτό είδαμε ότι υπάρχουν *δύο κύριοι τύποι μοντέλων* σχεδιασμού ενός Blockchain. Μεταξύ αυτών των δύο τύπων είναι και η υβριδική επιλογή με την οποία μπορεί να δημιουργηθούν περισσότερο ή λιγότερο ευέλικτες (flexible) η συγκεκριμένες (specific) επιτρεπόμενες ενέργειες.

A. **Public/Open/Permissionless Model:** είναι ένα Blockchain στο οποίο δεν υπάρχουν περιορισμοί στην ανάγνωση των δεδομένων και στην υποβολή συναλλαγών μέσα στην αλυσίδα.
B. **Private/Closed/Permissioned Model:** είναι ένα Blockchain, στο οποίο η άμεση πρόσβαση σε δεδομένα του δικτύου και η υποβολή συναλλαγών περιορίζεται σε μια προκαθορισμένη λίστα οντοτήτων.

Κεφάλαιο 3ο Πώς λειτουργεί το Blockchain

Με βάση το προηγούμενο κεφάλαιο έγινε κατανοητό γιατί χρειάζεται και τι είναι το Blockchain. Σε αυτήν την ενότητα, θα παρουσιαστούν οι τεχνικές έννοιες και η λειτουργία της τεχνολογίας του Blockchain.

3.1 Συναλλαγές

Οι συναλλαγές αποτελούν το κύριο μέρος του καθολικού του Blockchain. Όλες οι τεχνολογίες Blockchain έχουν σχεδιαστεί για να διασφαλίζουν ότι οι συναλλαγές μπορούν να δημιουργηθούν, να διαδοθούν να δίκτυο, να επικυρωθούν και τελικά να προστεθούν στο κεντρικό καθολικό (global ledger).
Από τεχνική άποψη, ο πιο θεμελιώδης ορισμός μια συναλλαγής είναι ένα ατομικό συμβάν που επιτρέπεται από το υποκείμενο πρωτόκολλο.

Με πιο απλά λόγια, μια συναλλαγή είναι πολλά δεδομένα που περιγράφουν την κίνηση του νομίσματος, πχ Bitcoin, το οποίο είναι μόνο ένα από τα πολλά με τεχνολογία Blockchain. Με άλλα λόγια, δεν περιορίζουν όλα τα Blockchain την χρησιμότητά του στις συναλλαγές των πληρωμών. Η αλυσίδα του Ethereum είναι παρόμοια με του Bitcoin αλλά αποθηκεύει και επιπλέον διαφορετικά είδη πληροφοριών [24].
Για παράδειγμα, θα μπορούσαν να αποθηκεύσουν ένα πρόγραμμα στο Blockchain του Ethereum που παρακολουθεί ποιος κατέχει, ποιες πράξεις και σε ποιες κατοικίες. Το πρόγραμμα αυτό θα μπορούσε επίσης να είναι υπεύθυνο για την επαναφορά της ιδιοκτησίας εάν τα στεγαστικά δάνεια δεν πληρωθούν εγκαίρως.

Το θεμελιώδες δομικό στοιχείο μιας συναλλαγής Blockchain είναι μια έξοδος συναλλαγής (transaction output). Τα αποτελέσματα των συναλλαγών είναι αδιαίρετα κομμάτια χρησιμοποιημένου νομίσματος, που καταγράφονται στο Blockchain και αναγνωρίζονται ως έγκυρα από όλο το δίκτυο.

Επιπλέον, όλοι οι κόμβοι στο δίκτυο Blockchain παρακολουθούν όλα τα διαθέσιμα αποτελέσματα, τα οποία είναι γνωστά ως *έξοδος μη δαπανημένων συναλλαγών (unspent transaction output- UTXO)*. Κάθε συναλλαγή αντιπροσωπεύει μια αλλαγή (μετάβαση

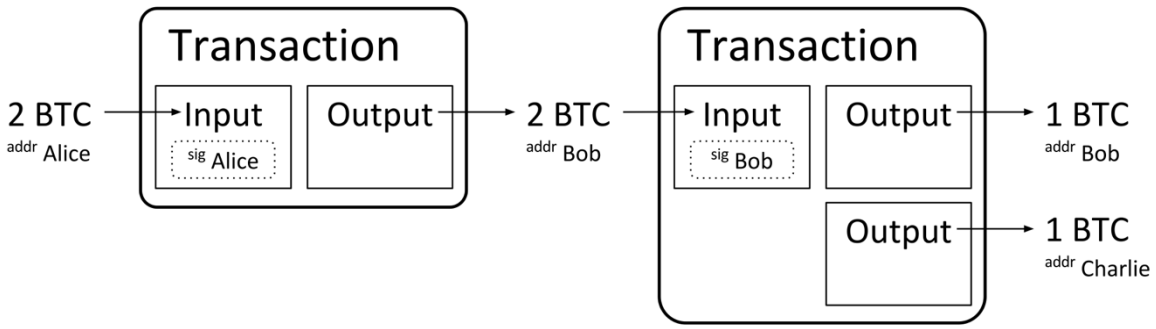
κατάστασης) στο σύνολο UTXO. Ακόμα, τα αποτελέσματα αυτά της συναλλαγής αποτελούνται από δύο μέρη:

i. Το ποσό αξίας (amount of value).
ii. Ένα κρυπτογραφικό παζλ που καθορίζει τη συνθήκη που απαιτείται για να δαπανηθεί έξοδος.

Η γλώσσα προγραμματισμού των συναλλαγών χρησιμοποιείται στο σενάριο κλειδώματος (το κρυπτογραφικό παζλ).

Επιπρόσθετα, η είσοδος της συναλλαγής προσδιορίζει ποιο UTXO θα καταναλωθεί και περιέχει απόδειξη ιδιοκτησίας μέσω του σεναρίου ξεκλειδώματος. όπως φαίνεται στο σχήμα στη συνέχεια, οι εισροές συναλλαγής βρίσκονται στον πίνακα (λίστα) που ονομάζεται VIN. Η είσοδος περιέχει:

i. το αναγνωριστικό- Transaction ID (αναφέρεται στην συναλλαγή που περιέχει το UTXO που δαπανάται),
ii. ένα ευρετήριο εξόδου VOUT (προσδιορίζει ποιο UTXO από τη συναλλαγή αναφέρεται) και
iii. ένα scriptSig, που ικανοποιεί τις προϋποθέσεις που τίθενται στο UTXO που χρησιμοποιείται στο ξεκλείδωμα για τις δαπάνες.



Εικόνα 11 transaction output

3.2 Κατανεμημένη συναίνεση- Distributed Consensus

Ξεκινώντας, η πλειονότητα των ατόμων στο δίκτυο πρέπει να συμφωνήσει ότι μια συναλλαγή είναι έγκυρη για να πραγματοποιηθεί και να προστεθεί στο Blockchain. Αυτή η έγκριση της πλειοψηφίας ονομάζεται κατανεμημένη συναίνεση (Distributed Consensus).

Με αυτή τη λογική, αντί μια οντότητα να εγκρίνει όλες τις συναλλαγές και να διατηρεί τη βάση δεδομένων με ακρίβεια, η ευθύνη στην αλυσίδα μοιράζεται μεταξύ όλων των συμμετεχόντων στο δίκτυο. Έτσι η κατανεμημένη φύση του Blockchain λειτουργεί για την έγκριση των συναλλαγών, όλα τα άτομα που είναι συνδεδεμένα στο δίκτυο μπορούν να αποφασίζουν για το εάν μια συναλλαγή πρέπει να γίνει αποδεκτή ή όχι,

Γενικώς, δεν θα ήταν βιώσιμο για όλους στο δίκτυο να συμφωνήσουν να εγκρίνουν μια ψεύτικη συναλλαγή ως έγκυρη καθώς έτσι κάποιος προσπαθεί να εξαπατήσει το σύστημα και την αλυσίδα. Όπως συμβαίνει με πολλά Blockchain , το όριο της συναίνεσης είναι πάνω από το 50%. Εάν δηλαδή περισσότερο από το 50% των μελών του δικτύου συμφωνεί πως μια συναλλαγή είναι έγκυρη τότε και μόνο τότε γίνεται αποδεκτή [24].

3.3 Εξόρυξη και απόδειξη εργασίας-Mining & Proof of Work (PoW)

Αρχικά, τα αιτήματα των συναλλαγών αποστέλλονται σε κάθε υπολογιστή του δικτύου για επικύρωση (έγκριση) και έπειτα προστίθενται στο Blockchain. Προκειμένου να επικυρωθεί μια συναλλαγή και να προστεθεί στην αλυσίδα, οι συμμετέχοντες πρέπει να ανταγωνιστούν για να λύσουν ένα «παζλ». (Το οποίο είναι υπολογιστικά δύσκολο). Το «παζλ» αυτό είναι συνδεδεμένο στο επόμενο μπλοκ, πριν αυτό προστεθεί στο Blockchain. Αυτή η διαδικασία επίλυσης του «παζλ» είναι γνωστή ως εξόρυξη (mining) [24]. Ακόμα, ο υπολογιστής που λύνει πρώτος το παζλ, λαμβάνει μια ανταμοιβή που συνήθως εξαργυρώνεται στο κρυπτονόμισμα ή το διακριτικό που χρησιμοποιείται σε αυτό το δίκτυο. Θεωρείται ως μια εξαργύρωση μικρών ποσοτήτων αξίας τους μπλοκ.

Το μέλος που κάνει την εξόρυξη (miner), και λύνει αυτό το παζλ φτάνοντας στο να προσθέτει στο δίκτυο ένα έγκυρο μπλοκ έχει ανταμοιβή για τη συνεισφορά του, η οποία είναι της μορφής

ισχύς, ηλεκτρικής ενέργειας και πόρους στο δίκτυο. Θεωρείται ότι είναι σημαντικό καθώς βοηθάει στη διατήρηση του δικτύου σε λειτουργία.

Επομένως, η εξόρυξη είναι η διαδικασία με την οποία οι συναλλαγές επαληθεύονται και προστίθενται στο δημόσιο καθολικό εκτελώντας μια υπολογιστική εργασία (το «παζλ») η οποία είναι δαπανηρή στην εκτέλεσή της αλλά εύκολη για άλλους να την επαληθεύσουν.

Από την άλλη , το Proof of Work (PoW) είναι η επικύρωση της εργασίας που έλαβε χώρα και η απόδειξη της ορθότητάς της [24].

3.4 Ψηφιακό Πορτοφόλι – Digital Wallet

Ξεκινώντας, ένα ψηφιακό πορτοφόλι (Digital Wallet) είναι απλώς η διεπαφή του χρήστη στο σύστημα του Blockchain. Μπορεί να θεωρηθεί όπως ένα πρόγραμμα περιήγησης ιστού (web browser) είναι η κοινή διεπαφή του χρήστη με το πρωτόκολλο HTTP για τη χρήση του διαδικτύου.
Τεχνικά, είναι ένα πρόγραμμα λογισμικού που αποθηκεύει ιδιωτικά και δημόσια κλειδιά αλληλοεπιδρώντας με διάφορα Blockchain [24]. Επίσης επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν ψηφιακές τιμές και να παρακολουθούν το υπόλοιπο στο λογαριασμό τους. Εάν κάποιος θέλει να χρησιμοποιήσει οποιοδήποτε κρυπτονόμισμα χρειάζεται να έχει ένα ψηφιακό πορτοφόλι.

Ο κ. Αντωνόπουλος κατηγοριοποιεί τους τύπους των πορτοφολιών ανάλογα με την πλατφόρμα. Αυτοί είναι:

i. Desktop,
ii. Mobile,
iii. Web,
iv. Hardware και
v. Paper.

Επίσης τα κατηγοριοποιεί με τον βαθμό αυτονομίας τους και τον τρόπο αλληλεπίδρασης με το δίκτυο σε τρεις κατηγορίες:

i. Full Node Client,
ii. Lightweight client και
iii. Third party API client.

Όλα τα ψηφιακά πορτοφόλια διαφέρουν ως προς την ποιότητα, την απόδοση, την ασφάλεια, το απόρρητο και την αξιοπιστία τους. Ορισμένα από αυτά είναι κατάλληλα για αρχάριους χρήστες ενώ άλλα είναι για προχωρημένους,

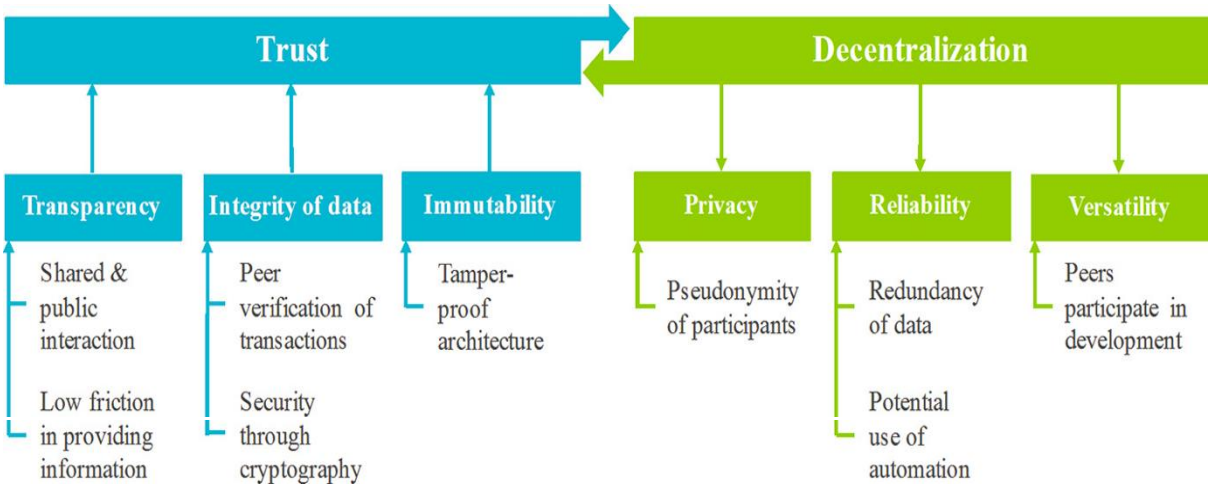
Επομένως η επιλογή ενός σωστού πορτοφολιού είναι αρκετά υποκειμενική και εξαρτάται από τον χρήστη και την τεχνογνωσία του.

Κεφάλαιο 4ο Τα πλεονεκτήματα του Blockchain και οι προκλήσεις του

Το κεφάλαιο που ακολουθεί περιέχει μια σύντομη επισκόπηση των χαρακτηριστικών και των πλεονεκτημάτων του Blockchain. Τα πλεονεκτήματα αυτά μπορούν να αποκτηθούν όταν προσαρμόζονται και λειτουργούν μακροπρόθεσμα οι Αρχές της τεχνολογίας αυτής. Επίσης, θα επισημανθούν ορισμένες προκλήσεις που θα μπορούσαν να προκαλέσουν την αποτυχία του Blockchain [22].

4.1 Τα πλεονεκτήματα του Blockchain

Ξεκινώντας, η τεχνολογία του Blockchain θεωρείται ως μια αναδυόμενη τεχνολογία, στην οποία υπάρχει χώρος για βελτίωση και περαιτέρω έρευνα. Ωστόσο, τα χαρακτηριστικά του μπορούν εύκολα να εντοπιστούν και να συζητηθούν με βάση τις ώριμες τεχνικές του έννοιες. Βάσει του Seebacher, εντοπίστηκαν και αναλύθηκαν τα βασικά χαρακτηριστικά του Blockchain [22] τα οποία φαίνονται στο παρακάτω σχήμα.



Εικόνα 12 Βασικά χαρακτηριστικά Blockchain

Η τεχνολογία του Blockchain παρείχε πολλά πλεονεκτήματα σε σχέση με τις υπάρχουσες τεχνολογίες. Τα δύο βασικά στοιχεία που τονίζονται είναι η εμπιστοσύνη (Trust) και η αποκέντρωση (Decentralization). Και τα δύο αυτά χαρακτηριστικά διευκολύνουν τη δημιουργία άλλων σημαντικών πλεονεκτημάτων που θα παρουσιαστούν στη συνέχεια [24].

4.1.1 Απόρρητο – Privacy

Στην τεχνολογία Blockchain το απόρρητο μπορεί να θεωρηθεί και σαν πλεονέκτημα και σαν πρόκληση ταυτόχρονα. Από τη θετική πλευρά, οι ταυτότητές των συμμετεχόντων διατηρούνται ανώνυμες, γεγονός που επέτρεψε να υπάρχει υψηλός βαθμός Ιδιωτικότητας. Επιπλέον όλες οι αλληλεπιδράσεις μεταξύ των κόμβων του δικτύου είναι ασφαλείς χρησιμοποιώντας την κρυπτογραφία του δημόσιου κλειδιού [24].
Σε αντίθεση με τα υπάρχοντα συστήματα συναλλαγών, οι ταυτότητες των συμμετεχόντων και τα στοιχεία της συναλλαγής τα κατέχουν και τα διαχειρίζονται τρίτα μέρη (Third parties).

4.1.2 Αξιοπιστία - Reliability

Οι μηχανισμοί του Blockchain διασφαλίζουν την αξιοπιστία μέσω του δικτύου. Δεν προστίθενται συναλλαγές στο καθολικό εκτός και εάν *εξορυχθούν, επικυρωθούν* και *επιβεβαιωθούν*, ώστε στη συνέχεια να αναπαραχθούν σε όλο το δίκτυο μέσω του μηχανισμού αποθήκευσης αποκέντρωσης. Με αυτόν τον τρόπο τα δεδομένα γίνονται ανθεκτικά τόσο σε διάρκεια και ποιότητα όσο και σε ισχύ.

4.1.3 Ευελιξία – Versatility

Ενώ η ιδέα του Blockchain γεννήθηκε για πρώτη φορά με την εφαρμογή του Bitcoin, η κύρια έννοια της τεχνολογίας αυτής χρησιμοποιήθηκε πολύ πέρα από το Bitcoin καθώς μπορεί να εφαρμοστεί ως δημόσιο καθολικό για κάθε τύπο συναλλαγών και όχι μόνο ως ψηφιακό νόμισμα.
Πολλοί επιστήμονες πιστεύουν ότι αυτή η τεχνολογία έχει μεγάλο αντίκτυπο στον ενεργειακό τομέα, τις αλυσίδες εφοδιασμού, τον υγειονομικό κλάδο καθώς και στην ίδια την αλυσίδα κλπ. Αυτό το χαρακτηριστικό είναι πολύ σημαντικό καθώς το καθιστά ευέλικτο στον χώρο [23,24].

4.1.4 Διαφάνεια - Transparency

Η τεχνολογία του Blockchain παρέχει διαφάνεια σε όλα τα άτομα στο δίκτυό του καθώς οι συναλλαγές είναι ορατές σε όλους τους συνδεδεμένους υπολογιστές χωρίς να ελέγχονται από τρίτους. Ακόμα, όπως έχει σημειωθεί, η πλειονότητα των υπολογιστών αυτών πρέπει να εγκρίνει τις συναλλαγές ή οποιεσδήποτε αλλαγές στην αλυσίδα, αποτρέποντας την απόκρυψη ή την παραποίηση των συναλλαγών.
Με αυτόν τον τρόπο, το σύστημα που βασίζεται στο Blockchain προσφέρει τεράστιες βελτιώσεις στη διαφάνεια σε σύγκριση με τα υπάρχοντα λογιστικά βιβλία [22].

4.1.5 Ακεραιότητα των Δεδομένων - Integrity of Data

Η ακεραιότητα των δεδομένων είναι ένα από τα βασικά χαρακτηριστικά που διευκολύνουν και χτίζουν εμπιστοσύνη προς την τεχνολογία του Blockchain. Επιπλέον, αυτή η ακεραιότητα επιτυγχάνεται με μια έξυπνη ιδέα κρυπτογραφίας που συνθέτει τον μηχανισμό της συναίνεσης (Consensus mechanism). Για να επιτευχθεί η συναίνεση, το δίκτυο Blockchain χρησιμοποιεί έναν άλλον μηχανισμό που αναφέρθηκε σε προηγούμενο κεφάλαιο, τον Proof-of-Work (PoW). Αυτοί οι μηχανισμοί διασφαλίζουν ότι η αλλαγή οποιασδήποτε μονάδας πληροφοριών στην αλυσίδα θα σήμαινε τη χρήση τεράστιου όγκου υπολογιστικής ισχύος για να γίνει παράκαμψη ολόκληρου του δικτύου.

Επίσης, το Blockchain προσφέρει μια λύση που μπορεί να λύσει ένα από τα δυσκολότερα ανοιχτά προβλήματα που είναι γνωστό ως *διπλής δαπάνης (Double Spending Problem).* Αυτό το πρόβλημα θεωρείται ως την εμφανή ευπάθεια που παραβιάζει τη ακεραιότητα του συστήματος [45]. Σε αυτή την περίπτωση, το δίκτυο του Blockchain σφραγίζει την πρώτη συναλλαγή όπου ο ιδιοκτήτης ξοδεύει ένα συγκεκριμένο νόμισμα και απορρίπτει τις επόμενες δαπάνες του νομίσματος, εξαλείφοντας έτσι τη διπλή δαπάνη.

4.1.6 Αμετάβλητο – Immutability

Το Blockchain έχει σχεδιαστεί για να είναι αμετάβλητο. Δηλαδή, γράφονται δεδομένα μόλις εμφανιστούν και είναι διαθέσιμα σε όλους στο δίκτυο.

Τεχνικά αυτό φαίνεται να είναι η επιθυμητή ποιότητα , καθώς σημαίνει ότι κανένας δεν μπορεί να επιστρέψει στην αρχή και να ξαναγράψει την ιστορία. Έτσι όταν μια συναλλαγή προστεθεί σε ένα μπλοκ, το οποίο στη συνέχεια εγκρίνεται και προστίθεται στην αλυσίδα, αυτή η συναλλαγή δεν μπορεί να αλλάξει/μεταβληθεί. Αυτός ο βαθμός του αμετάβλητου αυξάνεται με τον όγκο της εργασίας που δεσμεύεται το μπλοκ [24].

4.2 Οι προκλήσεις του Blockchain

Σε αυτή την ενότητα θα παρουσιαστούν ορισμένα σημαντικά προβλήματα και προκλήσεις που χρειάζεται το Blockchain για να ξεπεραστούν. Πολλοί υποστηρίζουν ότι ο λόγος αποτροπής του Blockchain είναι αυτά τα προβλήματα.

Θα κατηγοριοποιήσουμε τις προκλήσεις ως τις τεχνικές στην μια πλευρά και από την άλλη θα ομαδοποιηθούν όλες οι υπόλοιπες κατηγορίες.

4.2.1 Τεχνικές προκλήσεις

1. Ασφάλεια-Security

   Η ασφάλεια είναι από τα κυριότερα ερευνητικά θέματα στην τεχνολογία του Blockchain. Παρακάτω θα παρουσιαστούν κάποια προβλήματα ασφαλείας [11,20].

   i. **Περιστατικά ασφάλειας**: με την αυξανόμενη χρήση των Κρυπτονομισμάτων ως τρόπο διεξαγωγής πληρωμών και μεταφορών, τα συμβάντα ασφαλείας έχουν αυξηθεί και έχουν ως συνέπεια τις οικονομικές απώλειες των χρηστών (πχ του Bitcoin). Οι πιο συχνές παραβιάσεις ασφαλείας ήταν οι επιθέσεις DDoS, παραβίαση ιδιωτικών λογαριασμών με χρήση διαφημιστικών ιών ή Trojan horses.

ii. **51% Attack**: όπως επισημάνθηκε στο κεφάλαιο 4 , οι μηχανισμοί του Blockchain σχεδιάστηκαν με την προϋπόθεση ότι οι «ειλικρινείς» κόμβοι (honest nodes) θα ελέγχουν το δίκτυο. Εάν οι κόμβοι εισβολείς (attacker nodes) ελέγχουν συλλογικά την υπολογιστική ισχύ τότε το δίκτυο είναι ευάλωτο. Αυτή η κατάσταση ονομάζεται *"51% Attack"*.

iii. **Προβλήματα ελατότητας δεδομένων:** η ακεραιότητα των δεδομένων είναι ένα ουσιαστικό ζήτημα στο περιβάλλον το Blockchain, καθώς τα δεδομένα πρέπει να αποστέλλονται σε όλα τα μέρη του δικτύου για επαλήθευση. Επομένως είναι σημαντικό να μην αλλοιώνονται ή παραβιάζονται. Σε μια επίθεση ελατότητας, ο εισβολέας παρεμποδίζει, τροποποιεί και αναμεταδίδει μια συναλλαγή, με αποτέλεσμα ο εκδότης της συναλλαγής να πιστεύει ότι η αρχική του συναλλαγή δεν επιβεβαιώθηκε.

iv. **Ζητήματα ταυτοποίησης και κρυπτογραφίας:** στο Blockchain , το ιδιωτικό κλειδί είναι το κύριο στοιχείο ελέγχου ταυτότητας. Ωστόσο είχε συμβεί περιστατικό όπου κλάπηκαν ιδιωτικά κλειδιά ενός πελάτη.

2. Σπατάλη πόρων -Wasted Resources

Η εξόρυξη, Mining Blockchain, απαιτεί υψηλή ποσότητα ενέργειας για τον υπολογισμό και την επαλήθευση των συναλλαγών με ασφάλεια. Για παράδειγμα η εξόρυξη Bitcoin σπαταλά περίπου 15 εκ. $/ημέρα. Η σπατάλη αυτή του Bitcoin προκαλείται από την προσπάθεια του Proof-of-Work. Το ζήτημα με της σπατάλη των πόρων πρέπει να έχει πιο καινοτόμες λύσεις ώστε να υπάρχει πιο αποτελεσματική εξόρυξη στο Blockchain [42].

3. Απόρρητο-Privacy

Το Blockchain βασίζεται σε ένα κατανεμημένο δίκτυο συναίνεσης χωρίς ένα κεντρικό αξιόπιστο μέρος, όπου όλες οι συναλλαγές είναι διαφανείς και ανακοινώνονται στα μέλη.

Επομένως, το απόρρητο στην αλυσίδα διατηρείται διαμοιράζοντας την ροή της πληροφορίας.

Η διακοπή της ροής αυτής σημαίνει ότι το κοινό μπορεί να δει όλες τις συναλλαγές χωρίς όμως τις πληροφορίες που συνδέουν τη συναλλαγή με τις ταυτότητες. Πολλές μελέτες προτείνουν ως λύση διάφορα μοντέλα για αύξηση της ανωνυμία στο Blockchain.

4. Έξυπνα Συμβόλαιο- Smart Contracts

Το έξυπνο συμβόλαιο έχει αναγνωριστεί ως μια από τις τεχνικές προκλήσεις του Blockchain. Είναι μια πολλά υποσχόμενη προσέγγιση και αξίζει να μελετηθεί και να αναπτυχθεί περαιτέρω. Για αυτόν τον λόγο στο κεφάλαιο 7 θα γίνει εστίαση πάνω σε αυτό.

Κεφάλαιο 5ο Ψηφιακό Μάρκετινγκ και Blockchain

5.1 Τι είναι το Ψηφιακό Μάρκετινγκ

Το ψηφιακό μάρκετινγκ, που ονομάζεται επίσης διαδικτυακό μάρκετινγκ, είναι η προώθηση επωνυμιών για σύνδεση με πιθανούς πελάτες χρησιμοποιώντας το διαδίκτυο και άλλες μορφές ψηφιακής επικοινωνίας. Αυτό περιλαμβάνει όχι μόνο το ηλεκτρονικό ταχυδρομείο, τα μέσα κοινωνικής δικτύωσης και τη διαφήμιση μέσω ιστού, αλλά και μηνύματα κειμένου και πολυμέσων ως κανάλι μάρκετινγκ.
Ουσιαστικά, αν μια καμπάνια μάρκετινγκ περιλαμβάνει ψηφιακή επικοινωνία, είναι ψηφιακό μάρκετινγκ.

5.1.1 Τύποι του Ψηφιακού Μάρκετινγκ

Υπάρχουν τόσες εξειδικεύσεις στο ψηφιακό μάρκετινγκ, όσοι και τρόποι αλληλεπίδρασης με τη χρήση ψηφιακών μέσων. Ακολουθούν μερικά βασικά παραδείγματα.

i. Βελτιστοποίηση μηχανών αναζήτησης- Search Engine Optimization (SEO)

Η βελτιστοποίηση μηχανών αναζήτησης, ή SEO, είναι τεχνικά ένα εργαλείο μάρκετινγκ και όχι μια μορφή μάρκετινγκ από μόνη της. Το Balance το ορίζει ως «την τέχνη και την επιστήμη να κάνεις τις ιστοσελίδες ελκυστικές για τις μηχανές αναζήτησης» [2,3].
Τα πιο σημαντικά στοιχεία που πρέπει να λαμβάνονται υπόψη κατά τη βελτιστοποίηση μιας ιστοσελίδας περιλαμβάνουν:

- Ποιότητα περιεχομένου
- Επίπεδο αφοσίωσης των χρηστών
- Φιλικότητα προς το κινητό
- Αριθμός και ποιότητα εισερχόμενων συνδέσμων
- Η στρατηγική χρήση αυτών των παραγόντων κάνει το SEO επιστήμη, αλλά το απρόβλεπτο που εμπλέκεται το καθιστά τέχνη.

ii. Μάρκετινγκ περιεχομένου- Content Marketing

Το SEO είναι ένας σημαντικός παράγοντας στο μάρκετινγκ περιεχομένου, μια στρατηγική που βασίζεται στη διανομή σχετικού και πολύτιμου περιεχομένου σε ένα κοινό-στόχο.
Όπως σε κάθε στρατηγική μάρκετινγκ, ο στόχος του μάρκετινγκ περιεχομένου είναι να προσελκύσει δυνητικούς πελάτες που τελικά μετατρέπονται σε πελάτες. Αλλά το κάνει διαφορετικά από την παραδοσιακή διαφήμιση. Αντί να δελεάζει προοπτικές με πιθανή αξία από ένα προϊόν ή μια υπηρεσία, προσφέρει αξία δωρεάν με τη μορφή γραπτού υλικού.
Όσο αποτελεσματικό και αν είναι το μάρκετινγκ περιεχομένου, μπορεί να είναι δύσκολο. Οι συγγραφείς μάρκετινγκ περιεχομένου πρέπει να μπορούν να κατατάσσονται σε υψηλά επίπεδα στα αποτελέσματα των μηχανών αναζήτησης, ενώ παράλληλα προσελκύουν άτομα που θα διαβάσουν το υλικό, θα το μοιραστούν και θα αλληλοεπιδράσουν περαιτέρω με την επωνυμία. Όταν το περιεχόμενο είναι σχετικό, μπορεί να δημιουργήσει ισχυρές σχέσεις σε όλη τη γραμμή [2,3].

iii. Μάρκετινγκ μέσων κοινωνικής δικτύωσης- Social Media Marketing

Το μάρκετινγκ μέσων κοινωνικής δικτύωσης σημαίνει αύξηση της επισκεψιμότητας και της αναγνωρισιμότητας της επωνυμίας, εμπλέκοντας τους ανθρώπους σε συζητήσεις στο διαδίκτυο. Οι πιο δημοφιλείς πλατφόρμες για το μάρκετινγκ μέσων κοινωνικής δικτύωσης είναι το Facebook, το Twitter, το Instagram, και το TikTok με το LinkedIn και το YouTube να μην είναι πολύ πίσω.

Επειδή το μάρκετινγκ μέσων κοινωνικής δικτύωσης περιλαμβάνει ενεργό συμμετοχή κοινού, έχει γίνει ένας δημοφιλής τρόπος για να τραβήξετε την προσοχή. Είναι το πιο δημοφιλές μέσο περιεχομένου για επαγγελματίες του μάρκετινγκ B2C με ποσοστό 96%, και κερδίζει έδαφος και στη σφαίρα B2B. Σύμφωνα με το Content Marketing Institute, το 61% των εμπόρων περιεχομένου B2B αύξησαν τη χρήση των μέσων κοινωνικής δικτύωσης.

iv. Μάρκετινγκ με πληρωμή ανά κλικ- Pay per click Marketing

Pay-per-click, ή PPC, είναι η ανάρτηση μιας διαφήμισης σε μια πλατφόρμα και η πληρωμή κάθε φορά που κάποιος κάνει κλικ σε αυτήν.

Ένας αλγόριθμος δίνει **προτεραιότητα** σε κάθε διαθέσιμη διαφήμιση με βάση διάφορους παράγοντες, όπως:

- Ποιότητα διαφήμισης
- Συνάφεια λέξης-κλειδιού
- Ποιότητα σελίδας προορισμού
- Ποσό προσφοράς

v. Affiliate marketing

Το μάρκετινγκ θυγατρικών επιτρέπει σε κάποιον να κερδίσει χρήματα προωθώντας την επιχείρηση άλλου ατόμου. Θα μπορούσατε να είστε είτε ο προωθητής είτε η επιχείρηση που συνεργάζεται με τον προωθητή, αλλά η διαδικασία είναι η ίδια και στις δύο περιπτώσεις.

5.2 Πως το Blockchain επηρεάζει το Ψηφιακό Μάρκετινγκ

A. Επηρεάζει τα δεδομένα και το απόρρητο των καταναλωτών

Όταν ένας καταναλωτής επισκέπτεται έναν ιστότοπο ή μια εφαρμογή, παρέχει ορισμένα δεδομένα. Χρησιμοποιώντας αυτά τα δεδομένα, μια εταιρεία δημιουργεί ένα προφίλ καταναλωτή σύμφωνα με τα προϊόντα που αγόρασε, τις αναζητήσεις και άλλα. Όταν ένας καταναλωτής μοιράζεται δεδομένα στο διαδίκτυο, υπάρχει πάντα η πιθανότητα διαρροής των δεδομένων. Αλλά με τη χρήση της τεχνολογίας Blockchain, μπορείτε να το αποτρέψετε. Τέλος, διασφαλίζει ότι τα δεδομένα παραμένουν μόνο στους πελάτες και ότι δεν υπάρχει διαρροή στο σύστημα πουθενά.

Επιπλέον, επιστρέφει τη δύναμη στον πελάτη που μπορεί να αποφασίσει ποια δεδομένα θα ήθελε να μοιραστεί με τους πελάτες ή όχι.

Β. Παρέχει διαφάνεια και αυθεντικότητα

Οι καταναλωτές αυτές τις μέρες ενδιαφέρονται πολύ όχι μόνο για το προϊόν, αλλά για το πού κατασκευάστηκε ή από ποιον; Παλαιότερα, όταν οι καταναλωτές αγόραζαν προϊόντα, δεν ήταν σίγουροι αν έπαιρναν βιολογικά και αυθεντικά προϊόντα ή όχι; Δεν ήξεραν καν πού σχεδιάστηκαν τα προϊόντα; Αλλά με την τεχνολογία Blockchain, όλα αυτά αλλάζουν.

Παρέχει την ευκαιρία στους πελάτες να έχουν πλήρη διαφάνεια και να γνωρίζουν κάθε λεπτομέρεια για την υπηρεσία ή τα προϊόντα. Ο κατασκευαστής γνωρίζει πλέον τις πληροφορίες που σχετίζονται με το σχεδιασμό, την αποθήκη, τους εργάτες και άλλα. Τους βοηθά να μεταδώσουν τις λεπτομέρειες στον πελάτη τους και έτσι ώστε να μπορούν να κάνουν μια τεκμηριωμένη επιλογή.

5.3 Πώς το Blockchain βελτιώνει το Ψηφιακό Μάρκετινγκ

Εφαρμογές του Blockchain στο Ψηφιακό Μάρκετινγκ

Το Blockchain πρόκειται επίσης να επηρεάσει τους τρόπους με τους οποίους οι επιχειρήσεις κάνουν ψηφιακό μάρκετινγκ και διαφήμιση. Το θετικό είναι ότι πολλές από αυτές τις αλλαγές ισοπεδώνουν τους όρους ανταγωνισμού και επιτρέπουν στις μικρές εταιρείες να έχουν την ίδια πρόσβαση στους καταναλωτές με τις μεγαλύτερες [2,3].

Ακολουθούν έξι τρόποι με τους οποίους το Blockchain θα βελτιώσει το ψηφιακό μάρκετινγκ και τη διαφήμιση.

1. Βελτίωση της ασφάλειας

Η ασφάλεια των δεδομένων είναι ένα τεράστιο ζήτημα για όλους όσους αγοράζουν και πωλούν στο διαδίκτυο. Υπάρχουν συχνές παραβιάσεις που κάνουν την είδηση και όλοι αναρωτιούνται εάν η ταυτότητα ή τα οικονομικά τους στοιχεία έχουν παραβιαστεί.

Με το Blockchain, κάθε συναλλαγή επαληθεύεται και είναι δημόσια ορατή, αλλά τα άτομα που εμπλέκονται είναι ανώνυμα. Ως αποτέλεσμα, θα υπάρχει καλύτερη ασφάλεια για όλες τις συναλλαγές και όλοι οι εμπλεκόμενοι παραμένουν εντελώς ανώνυμοι.

2. Διαφημίσεις χωρίς μεσάζοντες

Με το Blockchain, μπορούν να παραληφθούν εντελώς τα δίκτυα διαφημίσεων. Οι χρήστες θα επαληθεύονται αυτόματα, επομένως δεν θα χρειαστεί τρίτο μέρος όπως η Google για να δημιουργηθεί εμπιστοσύνη. Οι εταιρείες που τοποθετούν διαφημίσεις και ιστότοπους με διαθέσιμο χώρο μπορούν να συνεργαστούν απρόσκοπτα.

3. Οι εταιρείες μπορούν να λάβουν υψηλότερης ποιότητας πληροφορίες καταναλωτών

Οι άνθρωποι θέλουν να ελέγχουν τα προσωπικά της στοιχεία, δεν θέλουν να εγγράφονται στην Εταιρεία Α και να λαμβάνουν ξαφνικά διαφημίσεις από την Εταιρεία Β, την Εταιρεία Γ και την Εταιρεία Δ.

Το Blockchain θα δώσει τις καταναλωτές την ευκαιρία να χρεώσουν τα στοιχεία επικοινωνίας της και να διασφαλίσουν ότι μόνο οι εταιρείες που ενδιαφέρονται θα λαμβάνουν τα δεδομένα της. Αυτό μπορεί να ακούγεται αρνητικό για τις επιχειρήσεις, αλλά στην πραγματικότητα είναι θετικό– αντί να σπαταλούν οι εταιρείες χρήματα σε δεδομένα από άτομα που δεν τις ενδιαφέρουν, θα λαμβάνουν στοχευμένες, ακριβείς πληροφορίες από εκείνους που είναι πραγματικά περίεργοι για την εταιρεία της.

4. Θα είναι ευκολότερο για τις μικρές εταιρείες να οικοδομήσουν εμπιστοσύνη

Μια μικρή επιχείρηση, μπορεί να είναι δύσκολο να ξεχωρίσει, ειδικά αν υπάρχουν καθιερωμένοι παίκτες στον κλάδο της. Πολλοί καταναλωτές είναι ευνόητα επιφυλακτικοί με επιχειρήσεις για τις οποίες δεν έχουν ξανακούσει και τα προϊόντα κακής ποιότητας είναι μια επιδημία στο διαδίκτυο.

Με το Blockchain, οι αξιόπιστες επιχειρήσεις θα μπορούν να οικοδομήσουν γρήγορα εμπιστοσύνη όσο μικρές και αν είναι. Θα μπορούν να αποδείξουν από πού προέρχονται τα προϊόντα τους και να δείξουν στους ανθρώπους κάθε βήμα της αλυσίδας εφοδιασμού. Αυτό θα βοηθήσει τους πελάτες να γνωρίζουν τι παρέχουν και θα είναι πολύ πιο πρόθυμοι να αγοράσουν από αυτές σε σχέση με άλλους ανταγωνιστές [2,3].

5. Το Blockchain επιτρέπει εναλλακτικές πληρωμές

Αν και η αποδοχή του Bitcoin και άλλων κρυπτονομισμάτων δεν είναι ακόμη κυρίαρχη, θα μπορούσε να γίνει. Το Blockchain κάνει αυτόν τον τύπο πληρωμής διαφανή. Οι έμποροι λιανικής δεν θα χρειάζεται να ανησυχούν για πλαστές επιταγές, κακές πιστωτικές κάρτες ή άλλα ζητήματα αντίστροφης χρέωσης.
Με πιο ασφαλείς πληρωμές, θα μπορούσε μια επιχείρηση να εξοικονομήσει χιλιάδες κάθε χρόνο σε τραπεζικές προμήθειες που σχετίζονται με αντιστροφές χρεώσεων και απάτη.

6. Αποφυγή του Fake Factor

Φαίνεται ότι σχεδόν τα πάντα στο διαδίκτυο είτε είναι ψεύτικα είτε θα μπορούσαν να είναι. Ψεύτικοι ακόλουθοι, ψεύτικα likes, ακόμη και ψεύτικα προϊόντα, καθώς οι εγκληματίες προσπαθούν να εξαπατήσουν τους ανθρώπους από τα χρήματα που κέρδισαν με κόπο. Είναι ο λόγος που οι καταναλωτές δυσκολεύονται να εμπιστευτούν τις διαφημίσεις – και γιατί εταιρείες σαν τη δική σας δυσκολεύονται να επιτύχουν απόδοση επένδυσης (ROI) στο μάρκετινγκ.

Με το Blockchain, θα γνωρίζει μια επιχείρηση εάν τα χρήματα που ξοδεύει σε διαφημίσεις πηγαίνουν στο κοινό που στοχεύει. Επίσης, θα συναλλάσσει απευθείας με εκδότες και όχι με αμφισβητούμενα τρίτα μέρη. Το μάρκετινγκ θα είναι πιο αποτελεσματικό και οι πελάτες θα γνωρίζουν ότι μπορούν να εμπιστευτούν τις διαφημίσεις.

Κεφάλαιο 6ο Smart Contract

Σε αυτό το κεφάλαιο θα επικεντρωθούμε στο έξυπνο συμβόλαιο ως μια από τις πιθανές μελλοντικές ερευνητικές κατευθύνσεις της τεχνολογίας Blockchain. Θα μελετηθεί και θα γίνει κατανοητή η έννοια και η χρήση του.

6.1 Δίκαιο Συμβάσεων

Το δίκαιο των συμβάσεων είναι ένας από τους πιο δυναμικά ανεπτυγμένους τομείς του δικαίου. Εξελίσσεται συνεχώς, ανταποκρινόμενο στην εμφάνιση νέων επιχειρηματικών μοντέλων και τεχνολογιών. Ως εκ τούτου, υπάρχουν διαφορετικές μέθοδοι σύναψης συμβάσεων με βάση την επιχείρηση και την τεχνολογία που χρησιμοποιείται [26].

Το Blockchain θεωρείται ένα νέο επιχειρηματικό μοντέλο και μια νέα τεχνολογική πλατφόρμα. Επίσης, αποσκοπεί στην αφαίρεση του τρίτου μέρους μεταξύ των εμπλεκόμενων σε οποιαδήποτε συναλλαγή. Έτσι ο Savalyev θεώρησε ότι τα έξυπνα συμβόλαια ως καλό παράδειγμα ανάπτυξης των διαδικασιών και των μεθόδων σύναψης συμβάσεων ως προς το Blockchain [26].

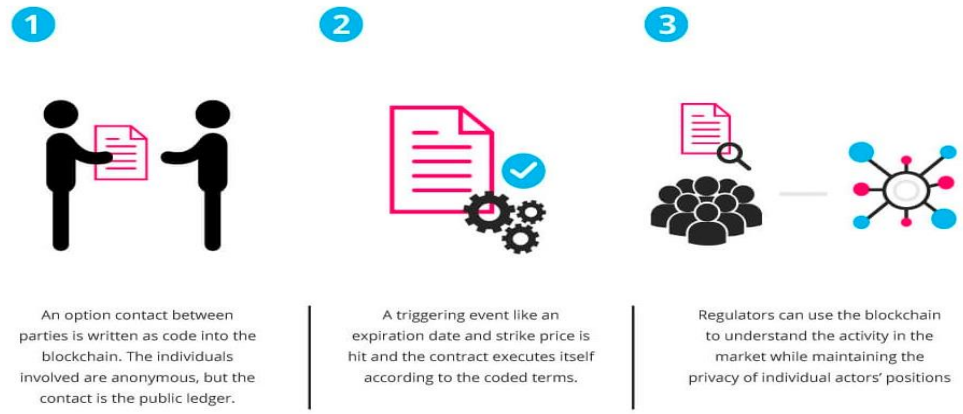
6.2 Το όραμα του Smart Contract

Το όραμα του Smart Contract περιγράφεται από τον Hingley [14] ως:

"What if a legal agreement could be monitored, executed and enforced without the need for human action or interference? Imagine a world in which a string of code could recognize the fulfillment of conditions, automatically transfer assets at the agreed times and register those transfers".

Αυτό το όραμα ταιριάζει ακριβώς με το όραμα του Blockchain, το οποίο είναι η υλοποίηση συναλλαγών χωρίς εμπιστοσύνη, προσαρμόζοντας μια αυτοεκτελούμενη και αυτοεπιβαλλόμενη σύμβαση με στόχο την αντικατάσταση των μερών που βασίζονται στην εμπιστοσύνη.

Έτσι, το έξυπνο συμβόλαιο και το Blockchain βρίσκονται ουσιαστικά στο ίδιο δρόμο και προς τον ίδιο στόχο.



Εικόνα 13 Πώς Λειτουργεί ένα Smart Contract

Επομένως, τα έξυπνα συμβόλαια προορίζονται να είναι ψηφιακά συμβόλαια που επιτρέπουν σε δύο ή περισσότερα χωριστά μέρη να συνάψουν μια συμφωνία, του οποίου οι όροι κωδικοποιούνται σε γλώσσα υπολογιστή αντί για νομική γλώσσα [12,8].

Το πλεονέκτημα ενός έξυπνου συμβολαίου είναι ότι δεν απαιτεί από τρίτους να ελέγχουν τις συναλλαγές. Αυτό έχει ένα προφανές πλεονέκτημα κόστους και ταχύτητας.

6.3 Ο ορισμός του Smart Contract

Ένας από τους πολλά υποσχόμενους τομείς εφαρμογής της τεχνολογίας Blockchain είναι η χρήση της για τη δημιουργία πλήρως αυτοματοποιημένων συμβάσεων, δηλαδή συμφωνιών που εκτελούνται χωρίς την ανθρώπινη συμμετοχή. Τέτοιες συμφωνίες στο τεχνολογικό περιβάλλον αναφέρονται συχνά ως έξυπνες συμβάσεις (Smart Contracts) [26].

Ειδικότερα, τα έξυπνα συμβόλαια είναι συνηθισμένα συμβόλαια, αλλά είναι γραμμένα σε κώδικα υπολογιστή για να εκτελεστούν σε περιβάλλον Blockchain. Το Blockchain θα επαληθεύσει, θα εκτελέσει και θα επιβάλει αυτόματα τους όρους της σύμβασης μεταξύ των

συμφωνηθέντων μερών. Αυτά τα συμβόλαια ονομάζονται έξυπνα επειδή μπορούν να είναι εν μέρει ή πλήρως αυτο-εκτελούμενα.

Σύμφωνα με τον απλούστερο ορισμό, ένα έξυπνο συμβόλαιο είναι μια συμφωνία της οποίας η απόδοση είναι αυτοματοποιημένη. Ωστόσο, επειδή μπορεί να είναι εν μέρει αυτο-εκτελούμενο/αυτοεπιβαλλόμενο (self-executing/self-enforcing) ο κ. Stark προτιμά να ονομάζεται αυτοματοποιήσιμο (automatable) παρά αυτοματοποιημένο (automated) [13,26]. Επίσης ,υποστηρίζει αυτή την αλλαγή επειδή στην πράξη μπορεί να υπάρχουν μέρη μιας νομικής συμφωνίας των οποίων η απόδοση απαιτεί ανθρώπινη παρέμβαση για τον έλεγχο, την εκτέλεση και επιβολή.

Ως εκ τούτου, είναι απαραίτητο να αναλυθεί εάν υπάρχει ή όχι κάτι νέο στα έξυπνα συμβόλαια σε σύγκριση με τις υπάρχουσες πρακτικές.

Ας εξετάσουμε διαφορετικές πρακτικές, όπως η αγορά ανταλλαγής, για να συγκρίνουμε και να βρούμε τον βαθμό καινοτομίας του έξυπνου συμβολαίου. Όπως τα Χρηματιστήρια, όπου χρησιμοποιούνται ευρέως τα λεγόμενα αυτοματοποιημένα συστήματα συναλλαγών. Για παράδειγμα, στις αγορές συναλλάγματος οι συναλλαγές εκτελούνται συχνά όχι από τον ίδιο τον έμπορο, αλλά από ένα σύστημα υπολογιστή που βασίζεται σε μια στρατηγική συναλλαγών που εφαρμόζεται.
Από το 2014, περισσότερο από το 75% των μετοχών που διαπραγματεύονται στα χρηματιστήρια των Ηνωμένων Πολιτειών προέρχονται από εντολές αυτοματοποιημένων συστημάτων συναλλαγών. Επομένως, οι αυτοματοποιημένες συμβάσεις δεν είναι κάτι καινούργιο, έχουν ήδη χρησιμοποιηθεί ευρέως σε πολλούς τομείς για μεγάλο χρονικό διάστημα.

Ορισμός του Smart Contract από τον Greenspan [50]:

«Ένα Smart Contract είναι κομμάτι του κώδικα που αποθηκεύεται σε ένα Blockchain, ενεργοποιείται από συναλλαγές και τέλος διαβάζει και γράφει τα δεδομένα στη βάση αυτού του Blockchain.

Τα 6 χαρακτηριστικά ενός Smart Contract βάσει του Savelyev [26]

1. Αποκλειστικά ηλεκτρονική φύση-solely electronic nature,
2. Εφαρμογή λογισμικού-software implementation,
3. Αυξημένη βεβαιότητα-increased certainty,
4. «υπό όρους» φύση-conditional nature,
5. Αυτοαπόδοση-self-performance,
6. Αυτάρκεια- self-sufficiency.

Συνοψίζοντας, όταν ένα έξυπνο συμβόλαιο εκτελείται στο Blockchain, λειτουργεί αυτόματα. Εάν πληρούνται οι όροι της σύμβασης, οι πληρωμές ή η αξία ανταλλάσσονται βάσει των όρων της σύμβασης. Ομοίως, εάν δεν πληρούνται οι όροι της σύμβασης, οι πληρωμές ενδέχεται να παρακρατηθούν εάν εγγραφούν στο έξυπνο συμβόλαιο.

Τα έξυπνα συμβόλαια εκτελούνται καθώς προγραμματίζονται σε ένα αποκεντρωμένο δίκτυο υπολογιστών στο Blockchain εξαλείφοντας τους κινδύνους γύρω από μη εξουσιοδοτημένες αλλαγές. Η σύμβαση εκτελείται αυτόματα, ανταλλάσσοντας αξία και πληρωμές μεταξύ ατόμων χωρίς να απαιτείται η επιβολή τους από δικηγόρους ή δικαστήρια.

Ως παράδειγμα, οι κόμβοι και οι ενέργειές τους στο Blockchain έχουν χρονική σήμανση και δεν μπορούν να τροποποιηθούν. Αυτό δημιουργεί μια ιδανική πλατφόρμα για συμβόλαια, καθώς οποιεσδήποτε αλλαγές στα συμβόλαια έχουν χρονική σήμανση.

Τα συμβόλαια μπορούν να αποθηκευτούν (και να δημιουργήσουν νέες εκδόσεις) διατηρώντας παράλληλα τα προηγούμενα αντίγραφα (καθώς και ακριβείς χρονικές σημάνσεις σε όλες τις επεξεργασίες και αναθεωρήσεις). Όχι μόνο δίνει μια ακριβέστερη περιγραφή των διαδικασιών που πραγματοποιήθηκαν, αλλά επίσης κάνει όλα τα εμπλεκόμενα μέρη πιο ειλικρινή σχετικά με τις συναλλαγές που πραγματοποιούνται επειδή το καθολικό δεν μπορεί να τροποποιηθεί.

Όλα τα παραπάνω δείχνουν ότι το έξυπνο συμβόλαιο υπερβαίνει κατά πολύ τα υπάρχοντα μοντέλα διαδικασίας σύναψης συμβάσεων.

6.4 Πλατφόρμες του Smart Contract

Ξεκινώντας, υπάρχουν διαφορετικές πλατφόρμες έξυπνων συμβολαίων στις μέρες μας που ανταγωνίζονται στην αγορά.

Μεταξύ όλων αυτών των πλατφορμών, το Ethereum [1] θεωρείται ως η πιο επιτυχημένη εφαρμογή έξυπνων συμβάσεων σήμερα. Σχεδιάστηκε για να είναι ένα πιο γενικευμένο Blockchain όπου μπορούν να δημιουργηθούν και να εκτελεστούν πολύπλοκα έξυπνα συμβόλαια.

Το Ethereum δημιουργήθηκε ρητά για να επιτρέψει τη δημιουργία αποκεντρωμένων εφαρμογών (DApps) [17].

Το Σχήμα δίνει μια επισκόπηση όλων των διαφορετικών υπαρχουσών πλατφορμών έξυπνων συμβολαίων με βάση τη μελέτη σύγκρισης από το GitHub [17].

Platform name	Contract language	Live?	Origin	Inc. in	Est.	Pub. rel.
Bitcoin	Ivy-lang	Yes	USA	USA	2017.12	2017.12
BitShares	?	Yes				
Cardano	Plutus (Haskell inspired)	no	HK	Switzerland	2015	
Counterparty	?	Yes				
Corda						
DFINITY	Ethereum compatible (aka Solidity, Serpent, etc.)	No				
EOS	C/C++ (compiles to WASM)	no				
Ethereum	Solidity	Yes	CA	Switzerland	2014.04	2015.07
Ethereum Classic	Solidity	Yes	^^^	no	^^^	^^^
Exonum	Rust. Java bindings TBD	No	UA	Netherlands		2017.07
Hyperledger	Golang, JavaScript	?				
Lisk	Javascript					
Nem	?	?				
Neo	1st batch: dotNet; 2nd: Java,Kotlin; 3rd: C,C++,GO,Py,JS (TBD)	Yes	China	China	2014.06	2016.10
NXT	?	Yes				
Qtum	Solidity	Yes	Singapore	Singapore	2016	2017.09
quorum	?	?				
Radix	Scrypto (Based on JavaScript/TypeScript)	Yes	UK	UK	2018	
Rootstock	Solidity	no	Argentina	Argentina	2015.11	
Tezos	Michelson	no				
Ubiq	Solidity	Yes	CA	CA ?		2017.01
Urbit	Hoon	Yes				
Waves	*NA*	Yes	RU	?	2016	2016.11

Εικόνα 14 Εικόνα Επισκόπηση όλων των διαφορετικών υπαρχουσών πλατφορμών Smart Contract

Η ιδιαιτερότητα της πλατφόρμας έξυπνων συμβολαίων του Ethereum είναι ο βαθμός τυποποίησης και υποστήριξης που προσφέρει. Το Ethereum έχει δημοσιεύσει ένα σύνολο σαφώς καθορισμένων κανόνων που πρέπει να ακολουθούν οι προγραμματιστές, καθιστώντας την ανάπτυξη έξυπνων συμβολαίων ευκολότερη και λιγότερο επικίνδυνη. Το Ethereum έχει τη δική του γλώσσα προγραμματισμού έξυπνων συμβολαίων, τη Solidity, η οποία όχι μόνο βοηθά στην τυποποίηση αλλά και διευκολύνει πολύ τη δημιουργία συμβολαίων [17,18].

6.5 Χρήσεις του Smart Contract

Πολλές εταιρείες άρχισαν να αναπτύσσουν εφαρμογές που βασίζονται σε Blockchain τεχνολογία, χρησιμοποιώντας έξυπνα συμβόλαια [13,14]. Ως απλό παράδειγμα, το Ascribe για παράδειγμα επιτρέπει σε πολλούς διαφορετικούς καλλιτέχνες να διεκδικούν την κυριότητα του έργου τους και να εκδίδουν εκτυπώσεις περιορισμένης έκδοσης. Δηλαδή, το Ascribe χρησιμοποιεί το Blockchain για να εντοπίσει όλες τις αρχικές δημιουργίες και τις συναλλαγές μέσα στις δημιουργίες. Διαθέτει επίσης μια αγορά όπου οι καλλιτέχνες μπορούν να διαφημίζονται και οι άνθρωποι μπορούν να αγοράζουν και να πουλούν έργα τέχνης μέσω του ιστότοπού τους.

Παρακάτω ακολουθούν δύο πιθανές περιπτώσεις για εφαρμογή που είναι η Airbnb και η Uber [51] και πώς τα Smart Contract θα επηρεάσουν τις επιχειρήσεις.

6.5.1 Από το Airbnb στο bAirbnb

Η Airbnb έχει γίνει πλέον ο μεγαλύτερος προμηθευτής δωματίων στον κόσμο, όπως υπολογίζεται με βάση την αγοραία αξία και τα δωμάτια που κατέχουν [51]. Όμως, οι πάροχοι των δωματίων λαμβάνουν μόνο μέρος της αξίας που δημιουργούν. Οι διεθνείς πληρωμές πραγματοποιούνται μέσω ενδιάμεσων αρχών, οι οποίες λαμβάνουν προμήθειες για κάθε συναλλαγή και μεγάλα συναλλάγματα από την κορυφή και οι διακανονισμοί χρημάτων χρειάζονται πολύ χρόνο. Η Airbnb αποθηκεύει όλα τα δεδομένα, τόσο των ενοικιαστών όσο και των πελατών, γεγονός που εγείρει ανησυχίες σχετικά με το απόρρητο.

Ωστόσο, η ιδέα Blockchain ανοίγει την πόρτα για νέες επιχειρηματικές ευκαιρίες, όπως ο συνεταιρισμός ιδιοκτησίας που θα ελέγχεται μόνο από τα μέλη του.

Συγκεκριμένα, το bAirbnb [51] είναι μια κατανεμημένη εφαρμογή, ένα σύνολο έξυπνων συμβολαίων που αποθηκεύει δεδομένα σε ένα Blockchain με καταχωρίσεις στο σπίτι. Η εφαρμογή bAirbnb διαθέτει μια κομψή διεπαφή όπου οι ιδιοκτήτες μπορούν να ανεβάσουν πληροφορίες και φωτογραφίες της ιδιοκτησίας τους. Η πλατφόρμα διατηρεί βαθμολογίες φήμης τόσο των παρόχων όσο και των ενοικιαστών για να βελτιώσει τις αποφάσεις όλων.

Παραδείγματος χάριν, όταν θέλετε να νοικιάσετε, το λογισμικό bAirbnb σαρώνει και φιλτράρει το Blockchain για όλες τις καταχωρίσεις που πληρούν τα κριτήριά σας (π.χ. πέντε χιλιόμετρα από την Ακρόπολη, ένα υπνοδωμάτιο, 4+ αστέρια). Η εμπειρία χρήστη του bAirbnb είναι πανομοιότυπη με αυτή του Airbnb, εκτός από το ότι επικοινωνείτε peer to peer στο δίκτυο μέσω ασφαλών κρυπτογραφημένων και ασφαλών μηνυμάτων που δεν είναι αποθηκευμένα σε μια κεντρική βάση δεδομένων όπως το Airbnb. Εσείς και ο ιδιοκτήτης του δωματίου είστε οι μόνοι δύο που μπορείτε να διαβάσετε αυτά τα μηνύματα.

Η πρόσβαση στην ιδιοκτησία γίνεται χρησιμοποιώντας έξυπνες κλειδαριές (συσκευή IoT) που είναι συνδεδεμένη με το Blockchain. Όταν φτάσετε, το τηλέφωνό σας μπορεί να υπογράψει ένα μήνυμα με το δημόσιο κλειδί σας μια απόδειξη πληρωμής και η έξυπνη κλειδαριά θα ανοίξει για εσάς. Επομένως, οι ιδιοκτήτες δεν χρειάζεται να σας παραδώσουν το κλειδί ή να επισκεφθούν το ακίνητο. Εσείς και ο ιδιοκτήτης έχετε πλέον εξοικονομήσει τέλη Airbnb, δεν υπάρχουν χρεώσεις συναλλάγματος για διεθνή συμβόλαια και οι διακανονισμοί είναι εξασφαλισμένοι άμεσα. Τέλος, τα δεδομένα ιστορικού ενοικίασης είναι ασφαλή και ιδιωτικά μόνο μεταξύ των συμφωνηθέντων μερών. Αυτή είναι η πραγματική οικονομία επιμερισμού της αξίας. Τόσο οι πελάτες όσο και οι πάροχοι υπηρεσιών είναι οι νικητές.

6.5.2 Από το Uber στο GUber

Airbnb, Uber, Lyft, Taskrabbit, αυτές οι εταιρείες αποτελούν μέρος της λεγόμενης οικονομίας διαμοιρασμού. Δηλαδή, δεν έχουν καμία σχέση με την κοινή χρήση [51]. Η κοινή χρήση αφορά την ελεύθερη ανταλλαγή πληροφοριών και αξίας. Αυτό που κάνουν αυτές οι εταιρείες πολλών δισεκατομμυρίων δολαρίων είναι ότι είναι συγκεντρωτές υπηρεσιών. Πιο συγκεκριμένα, συγκεντρώνουν την πλεονάζουσα χωρητικότητα. Στο παράδειγμα της Uber, συγκεντρώνουν αυτοκίνητα και οδηγούς σε μια κεντρική πλατφόρμα και τα μεταπωλούν σε άτομα που αναζητούν μια βόλτα. Προσφέρουν πολύ καλή εξυπηρέτηση, αλλά έχει τους περιορισμούς του. Οι οδηγοί είναι γνωστό ότι είναι ασταθείς ή καταχρηστικοί. Όλοι υπόκεινται σε αυξημένες τιμές. Επίσης, οι οδηγοί δεν έχουν συλλογική διαπραγματευτική δύναμη. Η Uber συλλαμβάνει μια ασύμμετρη αξία αυτού που δημιουργείται καθώς λαμβάνει το 20%. Στη διαδικασία, καταγράφουν επίσης όλα αυτά τα δεδομένα για τους ανθρώπους που είναι δηλαδή, πού πηγαίνουν και αυτά είναι στοιχεία που μπορούν να υπονομεύσουν το απόρρητο σε μελλοντική εμπορική εκμετάλλευση.

Τώρα, ας έχουμε το σενάριο εάν η Uber είναι χτισμένη στο Blockchain. Μπορείτε να έχετε μια εφαρμογή που είναι χτισμένη στο Blockchain, ας την ονομάσουμε Great Uber ή GUber. Επομένως, όλοι μπορούν να αποκτήσουν ένα αντίγραφο του GUber όπως έχουν το Uber, συνδέονται στην εφαρμογή όπως ακριβώς κάνουν με το Uber.

Η GUber ξέρει τι είδους αυτοκίνητο θέλετε, πού πηγαίνετε, πόσο γρήγορα θέλετε να φτάσετε εκεί. Και σας ταιριάζει αυτόματα με ένα αυτοκίνητο που πληροί αυτά τα κριτήρια.
Επιπλέον, Η GUber έχει ενσωματωμένο ένα εγγενές σύστημα πληρωμών, όπως το Ethereum [1] και το Ether ή το bitcoin στο δίκτυο Bitcoin, επομένως δεν χρειάζεστε έναν κεντρικό μεσάζοντα για την επεξεργασία πληρωμών.

Επίσης, δεν χρειάζεστε έναν κεντρικό μεσάζοντα για να οργανώσετε τις δυνατότητες, επειδή η κατανεμημένη εφαρμογή μπορεί να το κάνει. Και ακόμη και πράγματα όπως η πληρωμή καυσίμων, η διαπραγμάτευση ευθυνών, η αγορά ασφάλισης και η αυτοματοποίηση είναι κάτι που τα αυτοκίνητα και οι οδηγοί μπορούν να κάνουν μόνοι τους. Στο όχι και τόσο μακρινό μέλλον, αυτά θα μπορούσαν απλώς να είναι αυτόνομα οχήματα που δεν ανήκουν σε κανέναν αλλά υπάρχουν σε μια κοινή εφαρμογή που εκτελεί αυτήν την υπηρεσία [51].

Συνεπώς, αυτός είναι ένας μεγάλος κίνδυνος για την Uber. Έχει πολλές θετικές κοινωνικές επιπτώσεις. Το προφανές είναι ότι οι οδηγοί κρατούν περισσότερο από την αξία, και ίσως αυτό μεταφράζεται σε χαμηλότερους ναύλους για μεμονωμένα άτομα. Σημαίνει επίσης ότι τα δεδομένα των ανθρώπων δεν αποθηκεύονται σε κεντρικά αποθετήρια όπως στο Uber, αλλά κρυπτογραφούνται και ελέγχονται από αυτούς. Αυτό αναδεικνύει ένα ενδιαφέρον σημείο. Ένα πραγματικά συναρπαστικό μέρος του Blockchain είναι ότι επαναφέρει τη δύναμη στα χέρια του χρήστη.

6.6 Το Smart Contract ως Ερευνητική κατεύθυνση

Παρόλο που ένα έξυπνο συμβόλαιο είναι μια λύση που χρησιμοποιεί την τεχνολογία Blockchain για τη δημιουργία συμβάσεων μεταξύ δύο ή περισσότερων συμμετεχόντων, πολλοί συγγραφείς και ερευνητές υποστηρίζουν ότι το Έξυπνο Συμβόλαιο μπορεί να είναι μια πολλά

υποσχόμενη ερευνητική προσέγγιση από μόνη της και αξίζει να μελετηθεί και να αναπτυχθεί περαιτέρω.
Επιπλέον, τα έξυπνα συμβόλαια μπορούν ενδεχομένως να χρησιμοποιηθούν σε διάφορα περιβάλλοντα και βιομηχανίες για διαφορετικούς σκοπούς , και όπως αναφέρθηκε προηγουμένως, οι περισσότερες από τις εφαρμογές που βασίζονται σε Blockchain θα διαχειρίζονται το έξυπνο συμβόλαιο.

Επομένως, υπάρχουν διαφορετικές κατευθύνσεις έρευνας για το έξυπνο συμβόλαιο που προσανατολίζονται στις ανάγκες του Blockchain. Αυτές οι πιθανές ερευνητικές κατευθύνσεις επισημαίνονται στις ακόλουθες υποενότητες. Ωστόσο, θα επεξεργαστούμε περισσότερα σε γλώσσες προγραμματισμού έξυπνων συμβολαίων.

6.6.1 Μια Μηχανική Λογισμικού προσανατολισμένη στο Blockchain

Μετά την καινοτομία της τεχνολογίας Blockchain, το Blockchain Oriented Software Engineering (BOSE) αναγνωρίστηκε και συμβουλεύτηκε από ερευνητές μηχανικής λογισμικού ως μία από τις αναδυόμενες ερευνητικές κατευθύνσεις που ακολούθησε το Blockchain . Αυτός είναι ένας νέος αναδυόμενος κλάδος μηχανικής λογισμικού που ονομάζεται (BOSE), προτείνεται με βάση την κατάσταση των πρακτικών των έργων της τεχνολογίας αυτής. Ο Porru και οι συνάδελφοί του διεξήγαγαν μια διερευνητική μελέτη σε ένα σώμα που περιλάμβανε 1184 αποθετήρια λογισμικού GitHub, τα οποία ταυτοποιήθηκαν με τη χρήση της Έκθεσης Blockchain της Moody's [29] .

Κατέληξαν στο συμπέρασμα ότι υπάρχει ανάγκη για νέες πρακτικές, μεθόδους και τεχνικές μηχανικής λογισμικού (BOSE) που να είναι κατάλληλες για νέες υλοποιήσεις Blockchain, στις οποίες το θεώρησαν ως σημαντικό έργο μηχανικής λογισμικού που θα συμβάλει στην υλοποίηση των δυνατοτήτων του Blockchain [29].

Επιπλέον, αυτή η πρόσκληση παρακινεί τους ερευνητές της μηχανικής λογισμικού να αναθεωρήσουν πρακτικές και τεχνικές μηχανικής λογισμικού και να τις βελτιώσουν ή να προτείνουν μια νέα. Αυτό είναι, φυσικά, ανοιχτό ευρύ πεδίο ερευνητικής κατεύθυνσης που πρέπει να ληφθεί υπόψη από τους ερευνητές για να ευθυγραμμιστούν οι τεχνικές και οι πρακτικές μηχανικής λογισμικού με τις ανάγκες της τεχνολογίας Blockchain.

6.6.2 Μια γλώσσα μοντελοποίησης που βασίζεται σε Blockchain Τεχνολογία

Τα συστήματα που προσανατολίζονται στο Blockchain ενδέχεται να απαιτούν εξειδικευμένα γραφικά μοντέλα για αναπαράσταση. Πιο συγκεκριμένα, τα υπάρχοντα μοντέλα θα μπορούσαν επίσης να προσαρμοστούν σε λογισμικό προσανατολισμένο στην αλυσίδα [29].

Για παράδειγμα, τα διαγράμματα UML μπορεί να τροποποιηθούν ή ακόμη και να δημιουργηθούν νέα για να λάβουν υπόψη τις ιδιαιτερότητες της μηχανικής λογισμικού που είναι προσανατολισμένες στο Blockchain. Διαγράμματα όπως το Διάγραμμα Περίπτωσης Χρήσης, Διάγραμμα Δραστηριότητας και Διάγραμμα Κατάστασης δεν θα μπορούσαν να αντιπροσωπεύουν αποτελεσματικά το περιβάλλον λογισμικού προσανατολισμένο στο Blockchain.

6.6.3 Smart Contract γλώσσες Προγραμματισμού

Αυτή η προσέγγιση στοχεύει στην εφαρμογή ενός Περιβάλλοντος Ανάπτυξης Έξυπνων Συμβάσεων (SCDE), που θα μπορούσαν να εξορθολογήσουν τη δημιουργία έξυπνων συμβολαίων μέσω εξειδικευμένων γλωσσών (για παράδειγμα, Solidity, μια γλώσσα σχεδιασμένη για τη σύνταξη έξυπνων συμβολαίων στο Ethereum [1]).

Αν και ο προγραμματισμός έξυπνων συμβολαίων μοιάζει από πολλές απόψεις με τον παραδοσιακό προγραμματισμό. Ωστόσο, εγείρει σημαντικές νέες προκλήσεις. Ο Delmolino [52] και οι συνεργάτες του υποστηρίζουν ότι ο προγραμματισμός έξυπνων συμβολαίων χρειάζεται διαφορετικό είδος σκέψης που μπορεί να μην έχουν αποκτήσει οι παραδοσιακοί προγραμματιστές. Τα συμβόλαια πρέπει να συντάσσονται για να διασφαλίζεται η δικαιοσύνη ακόμη και όταν οι αντισυμβαλλόμενοι ενδέχεται να επιχειρήσουν να εξαπατήσουν με οποιοδήποτε μέσο.

Ως εκ τούτου, ο Delmolino και άλλοι [52] , προτείνουν την ανάγκη για Γενικά Έξυπνα Συμβόλαια, βασισμένα σε διδάγματα και γνώσεις που αντλήθηκαν από ένα εργαστήριο κρυπτονομισμάτων. Καθώς οι τρέχουσες γλώσσες δέσμης ενεργειών που χρησιμοποιούνται

για την υλοποίηση έξυπνων συμβάσεων προσφέρουν ένα σύστημα δέσμης ενεργειών που δεν είναι ούτε εκφραστικό ούτε φιλικό προς τον χρήστη.

Λόγω αυτών των θεμελιωδών ορίων της εκφραστικότητας της γλώσσας σεναρίου, έχουν προταθεί διαφορετικές προσπάθειες τόσο στον ακαδημαϊκό χώρο όσο και στη βιομηχανία για να σχεδιαστούν διάφορα Περιβάλλοντα Ανάπτυξης Έξυπνων Συμβάσεων [27,28]. Ωστόσο, όλες αυτές οι προσπάθειες έγιναν με τρόπο που εκσυγχρονίζει την υπάρχουσα γλώσσα σεναρίου. Καθώς η εκ των υστέρων προσαρμογή της γλώσσας δεν είναι μόνο χρονοβόρα, αλλά μπορεί επίσης να οδηγήσει σε πιο δαπανηρές υλοποιήσεις όσον αφορά τον αριθμό των γύρων ή το κόστος στην αλυσίδα.

Συγκριτικά, πολλές από τις ίδιες εργασίες θα ήταν πιο εύκολο να προγραμματιστούν και θα ήταν πιο αποτελεσματικές, εάν είχαν κατασκευαστεί χρησιμοποιώντας μια γλώσσα έξυπνης σύμβασης γενικού σκοπού (της οποίας το Ethereum [1] είναι η πρώτη ενσάρκωση). Παρόλα αυτά, το Ethereum έχει τα δικά του συγκεκριμένα λάθη ή σφάλματα που πρέπει να αντιμετωπιστούν όπως αναφέρουν ο Delmolino και οι συνεργάτες του όπως: Call-Stack Bug, Blockhash Bug και Incentive Bugs.

Τώρα, ας πάρουμε αυτό το απλό παράδειγμα που δίνεται από την ομάδα του εργαστηρίου κρυπτονομισμάτων για να δείξουμε μερικές από τις τυπικές παγίδες για τον προγραμματισμό έξυπνων συμβολαίων [52].

Ένα απλό παράδειγμα «Πέτρα, Ψαλίδι, Χαρτί» για τη διάγνωση των σφαλμάτων. Σε αυτό το συμβόλαιο, δύο παίκτες θα παίξουν ένα απλό «Πέτρα, Ψαλίδι, Χαρτί» για χρήματα. Το πρόγραμμα της σύμβασης αποτελείται από δύο κύριες λειτουργίες:

- **Input του παίχτη**: Οι παίκτες εγγράφονται στο συμβόλαιο και καταθέτουν χρήματα για να παίξουν. Κάθε παίκτης παρέχει επίσης στοιχεία για το συμβόλαιο με τη μορφή βράχου, χαρτιού ή ψαλιδιού της επιλογής του.

- **οριστικοποίηση**: Η σύμβαση ορίζει έναν νικητή και στέλνει τα έσοδα στον νικητή.

Συνοψίζοντας, ακόμη και για ένα πολύ απλό έξυπνο συμβόλαιο, είναι δύσκολο να το δημιουργηθεί σωστά. Τι γίνεται με το πραγματικό πολύπλοκο έξυπνο συμβόλαιο; Ως εκ τούτου, πιστεύουμε ότι αυτή η προσέγγιση χρειάζεται περαιτέρω έρευνα εστίασης, η οποία μπορεί να είναι καίριας σημασίας για τη δημιουργία και την επιτυχία της υλοποίησης έξυπνων συμβάσεων.

Κεφάλαιο 7ο Blockchain στην Βιομηχανία 4.0

Λόγω της εξάπλωσης των Τεχνολογιών Πληροφορικής τις τελευταίες δεκαετίες, υπάρχει μια εκθετική αύξηση στη χρήση διαφόρων έξυπνων εφαρμογών όπως η έξυπνη γεωργία, η έξυπνη υγειονομική περίθαλψη, η εφοδιαστική αλυσίδα, οι επιχειρήσεις, ο τουρισμός, η φιλοξενία και η διαχείριση ενέργειας κ.λπ.

Για όλες τις προαναφερθείσες εφαρμογές, η ασφάλεια και το απόρρητο αποτελούν βασικές ανησυχίες, λαμβάνοντας υπόψη τη χρήση του ανοιχτού καναλιού, δηλαδή του Διαδικτύου για μεταφορά δεδομένων. Αν και πολλές λύσεις και πρότυπα ασφαλείας έχουν προταθεί όλα αυτά τα χρόνια για τη βελτίωση των επιπέδων ασφαλείας των προαναφερθέντων έξυπνων εφαρμογών, οι υπάρχουσες λύσεις είτε βασίζονται στην κεντρική αρχιτεκτονική (με ένα μόνο σημείο αστοχίας) είτε έχουν υψηλό κόστος υπολογισμού και επικοινωνίας [38].

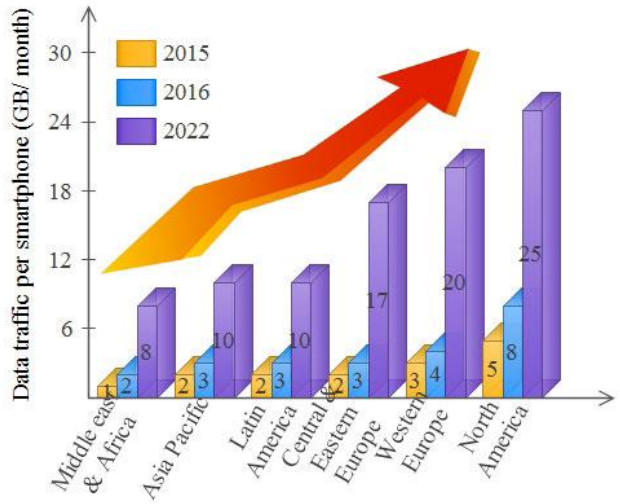
Επιπλέον, οι περισσότερες από τις υπάρχουσες λύσεις ασφάλειας έχουν επικεντρωθεί μόνο σε λίγες πτυχές και αποτυγχάνουν να αντιμετωπίσουν την επεκτασιμότητα, την ευρωστία, την αποθήκευση δεδομένων, την καθυστέρηση δικτύου, τη δυνατότητα ελέγχου, την αμετάβλητη και την ιχνηλασιμότητα. Για τον χειρισμό των προαναφερθέντων ζητημάτων, η τεχνολογία Blockchain μπορεί να είναι μία από τις λύσεις. Με κίνητρο από αυτά τα γεγονότα, σε αυτό το άρθρο, παρουσιάζουμε μια συστηματική ανασκόπηση των διαφόρων λύσεων που βασίζονται σε Blockchain και της δυνατότητας εφαρμογής τους σε διάφορες εφαρμογές που βασίζονται στο Industry 4.0.

Με τη μεγάλη δημοτικότητα του Διαδικτύου και των σχετικών τεχνολογιών, έχουν χρησιμοποιηθεί διάφορες εφαρμογές που βασίζονται στο Industry 4.0 σε όλο τον κόσμο, στις οποίες αισθητήρες και ενεργοποιητές ανιχνεύουν, υπολογίζουν και επικοινωνούν τα δεδομένα για τον αυτοματισμό της βιομηχανίας [53].

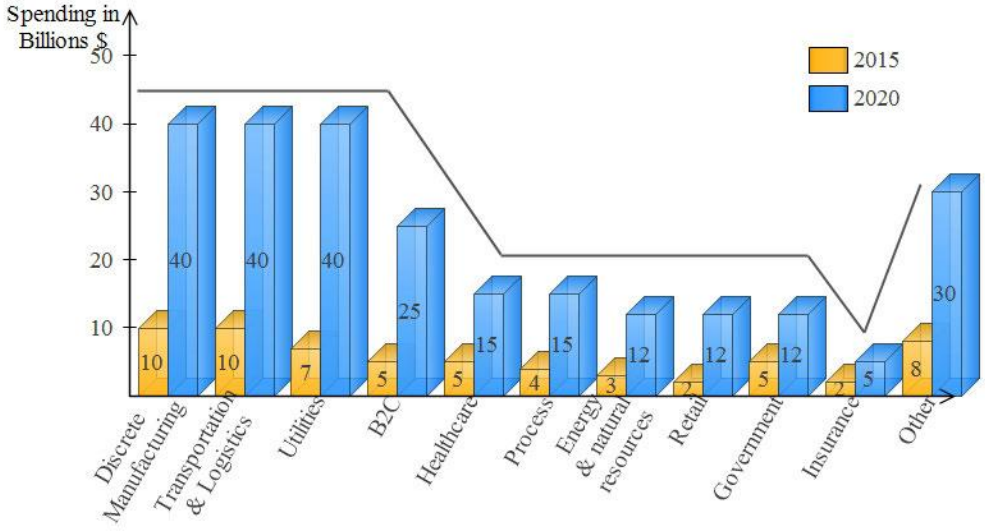
Όπως και στις εφαρμογές που βασίζονται στο Industry 4.0, τα δεδομένα μεταξύ διαφορετικών τοποθεσιών οφείλονται στη χρήση ενός ανοιχτού καναλιού, π.χ. Διαδικτύου, έτσι και οι απειλές για την ασφάλεια και το απόρρητο έχουν επίσης πολλαπλασιαστεί.

Επιπλέον, διαφορετικές εφαρμογές απαιτούν σύνολα δεδομένων από διαφορετικούς τομείς σε διαφορετικές μορφές. Απαιτείται επίσης η τυποποίηση της μορφής δεδομένων, ώστε να μπορούν να χρησιμοποιηθούν από διαφορετικές εφαρμογές που βασίζονται στο Industry 4.0.

Η χρήση έξυπνων τηλεφώνων και έξυπνων εφαρμογών για προσωπικές, επαγγελματικές και κοινωνικές δραστηριότητες αυξάνεται εκθετικά σε όλο τον κόσμο. Έχει ως αποτέλεσμα αύξηση τόσο της διακίνησης δεδομένων δικτύου (σε GB) όσο και της συνολικής δαπάνης (σε δισεκατομμύρια USD) όπως φαίνεται στο σχήμα παρακάτω.



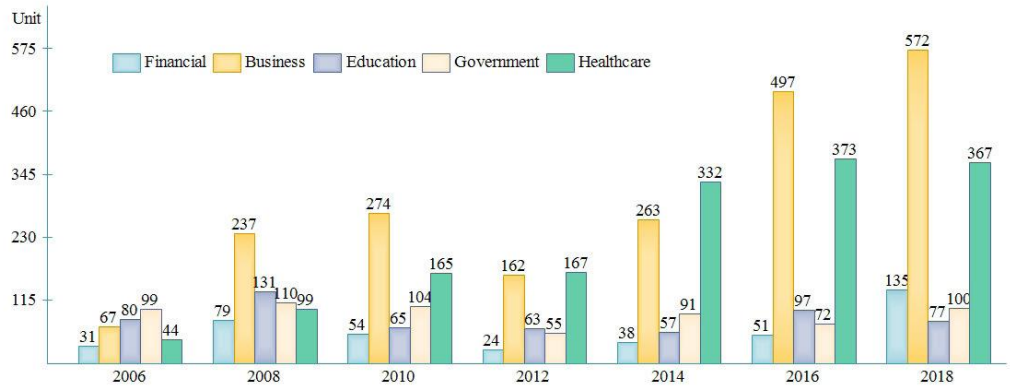
Εικόνα 15 Διακίνηση δεδομένων δικτύου (σε GB)



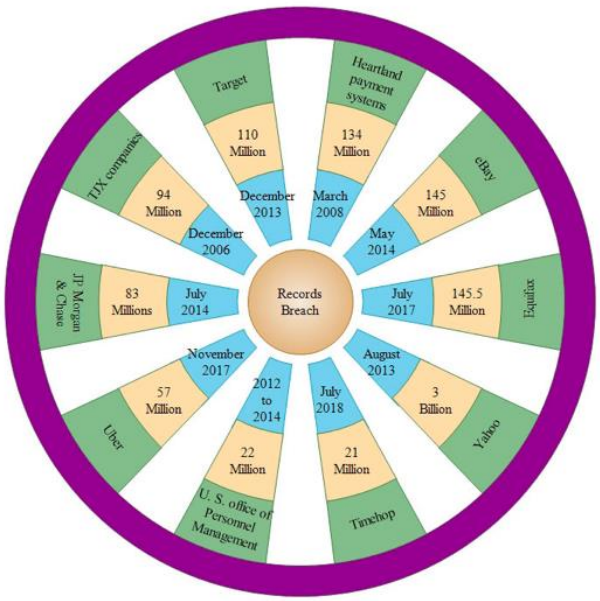
Εικόνα 16 Συνολική δαπάνη (σε δισεκατομμύρια USD)

Σύμφωνα με αυτήν την έκθεση, οι έξυπνες βιομηχανίες θα ξοδέψουν 40 δισεκατομμύρια δολάρια στο IoT έως το 2020 σε διάφορους τομείς, συμπεριλαμβανομένων των μεταφορών και της κατασκευής. Ωστόσο, λόγω του μεγάλου αριθμού ανταλλαγών δεδομένων μέσω του Διαδικτύου, η διατήρηση της εμπιστευτικότητας, του απορρήτου και της ακεραιότητας γίνεται μείζον ζήτημα στο Industry 4.0 . Επιπλέον, σύμφωνα με τις έρευνες που διεξήχθησαν από διαφορετικούς φορείς σχεδόν 60 εκατομμύρια άνθρωποι επηρεάζονται από κλοπή ταυτότητας και 12 δισεκατομμύρια αρχεία ανθρώπων έχουν κακοποιηθεί το 2018 και αναμένεται να αυξηθούν στα 33 δισεκατομμύρια έως το 2023, όπως φαίνεται στο σχήμα.

Το Σχήμα δείχνει τα 10 πρόσφατα περιστατικά παραβιάσεων ασφαλείας που αναφέρθηκαν έως τον Ιούλιο του 2018, τα οποία αναμένεται να αυξηθούν τα επόμενα χρόνια [53-55].



Εικόνα 17 Παραβιάσεις ασφαλείας



Εικόνα 18 Παραβιάσεις ασφαλείας

Η ασφάλεια και η διατήρηση της ιδιωτικής ζωής αποτελούν σημαντικές ανησυχίες για τις εφαρμογές Industry 4.0. Ενδέχεται να υπάρχουν πιθανότητες μη εξουσιοδοτημένης παραβίασης δεδομένων ή διαρροής πληροφοριών που οδηγεί σε οικονομικές απώλειες σε εφαρμογές που βασίζονται στο Industry 4.0 [53,54]. Ελλείψει ισχυρής αρχιτεκτονικής ασφάλειας, το σύστημα μαζί με τα δεδομένα είναι επιρρεπές σε διάφορους τύπους επιθέσεων (όπως επιθέσεις DDoS, ARP spoo ng, αλλαγή ρυθμού δεδομένων, συμφόρηση δικτύου, χειραγώγηση, παρεμβολές θορύβου, phishing) και απειλές που μπορούν να βλάψουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων και μπορεί να επηρεάσει τη συνολική λειτουργία οποιουδήποτε συστήματος.

Για τέτοιους τύπους επιθέσεων, η πρόληψη είναι καλύτερη από οποιονδήποτε αντιδραστικό αμυντικό μηχανισμό για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της ιδιωτικής ζωής στο πλαίσιο των κανόνων νομικής συμμόρφωσης . Έχει βρεθεί στη βιβλιογραφία ότι με την αύξηση του ποσοστού αυτοματισμού στο Industry 4.0, αυξάνεται επίσης η πιθανότητα παραβίασης των κανόνων ασφαλείας και εξαπόλυσης νέου τύπου κυβερνοεπιθέσεων. Ο έλεγχος πρόσβασης, η εξουσιοδότηση, η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα είναι οι κύριες ανησυχίες στον κλάδο.

7.1 Blockchain 4.0

Αυτή η γενιά επικεντρώθηκε κυρίως σε υπηρεσίες όπως το δημόσιο καθολικό και τις κατανεμημένες βάσεις δεδομένων σε πραγματικό χρόνο. Αυτό το επίπεδο έχει απρόσκοπτη ενσωμάτωση εφαρμογών που βασίζονται στο Industry 4.0 [57].

Ακόμα, χρησιμοποιεί το έξυπνο συμβόλαιο που εξαλείφει την ανάγκη για συμβάσεις που βασίζονται σε χαρτί και ρυθμίζει εντός του δικτύου με τη συναίνεσή του.

Απαιτήσεις Blockchain 4.0:

- Έξυπνα συμβόλαια: Είναι ένα πρωτόκολλο που επιτρέπει την εκτέλεση συναλλαγών απουσία τρίτων που καθιστά τις συναλλαγές μη αναστρέψιμες και ανιχνεύσιμες.

- Tokenization: Είναι ένα από τα πιο σημαντικά πράγματα που πρέπει να συμπεριληφθεί στο Blockchain. Διευκολύνει την ψηφιακή αναπαράσταση των αγαθών, των υπηρεσιών και των δικαιωμάτων με τη βοήθεια διακριτικών. Επιτρέπει την ανταλλαγή αξιών και εμπιστοσύνης για διαφορετικούς χρήστες χωρίς να εμπλέκεται η κεντρική αρχή.

- Ασφάλεια δεδομένων: Η συμμόρφωση με την ασφάλεια είναι μια σημαντική και ουσιαστική απαίτηση της τεχνολογίας Blockchain από νομική άποψη.

- Αποκεντρωμένη αποθήκευση δεδομένων: Είναι βασική απαίτηση του κατανεμημένου συστήματος.

- Αμετάβλητο: Όλες οι εγγραφές στο δίκτυο δεν πρέπει να τροποποιούνται ή να παραβιάζονται στο κοινόχρηστο καθολικό. Αυτό επιτρέπει την ακεραιότητα των αποθηκευμένων δεδομένων.

- Συναίνεση: Οι συναλλαγές θα πρέπει να ενημερώνονται μόνο όταν όλοι οι επαληθευμένοι χρήστες του δικτύου συμφωνούν για το ίδιο.

- Δακτυλογραφημένα Μπλοκ: Απαιτείται για το έξυπνο συμβόλαιο και για πληρωμή υψηλής ταχύτητας σε επιχειρηματικές συναλλαγές. Έτσι, η μορφοποίηση δεδομένων των διαφορετικών τύπων μπλοκ περιλαμβάνει τον χρόνο τους, τον αλγόριθμο συναίνεσης, τον αριθμό των συναλλαγών ανά μπλοκ και τους τύπους δεδομένων περιεχομένου.

- Sharding: Απαιτείται για τον διαχωρισμό του περιεχομένου σε υποσύνολα κόμβων με τρόπο που να μην χρειάζεται όλοι οι κόμβοι να φέρουν όλο το φορτίο επεξεργασίας ή οποιοδήποτε βάρος.

- Διαχείριση δικαιωμάτων πρόσβασης: Απαιτείται κρυπτογράφηση ιδιωτικού και δημόσιου κλειδιού με βάση κρυπτογράφηση και κατανεμημένες βάσεις δεδομένων με ταυτοποίηση χρήστη για την εκχώρηση και διαχείριση δικαιωμάτων πρόσβασης.

- Πρότυπα που χρησιμοποιούνται για τη διαχείριση των επιτρεπόμενων αλυσίδων μπλοκ: Η αμεταβλητότητα του δικτύου Blockchain καθιστά την πρόσβαση στα δεδομένα με μια συγκεκριμένη σειρά. Τα δημόσια πιστοποιητικά είναι διαθέσιμα σε δημόσιο Blockchain, αλλά χωρίς να υπάρχει το ιδιωτικό κλειδί, δεν μπορεί να παρασχεθεί εξουσιοδότηση στους χρήστες. Επομένως, η διαχείριση όλων των δεδομένων θα πρέπει να γίνεται με σειρά στοιχείων δεδομένων, όπως η διεύθυνση πρωτοκόλλου διαδικτύου (IP), το όνομα, ο κώδικάς του και η επεκτάσιμη γλώσσα σήμανσης. Όλα αυτά δημοσιεύονται στην κοινοπραξία με τη διαδικασία επικοινωνίας.

- Τυπική μορφοποίηση δεδομένων: Στο σύστημα Blockchain, απαιτείται επίσης η τυποποίηση των μορφών δεδομένων σε σχέση με τις διεπαφές προγραμματισμού εφαρμογών (API). Κάθε οργανισμός στο δίκτυο Blockchain πρέπει να χρησιμοποιεί την ίδια μορφή δεδομένων ή API για να επικοινωνεί στο ίδιο δίκτυο.

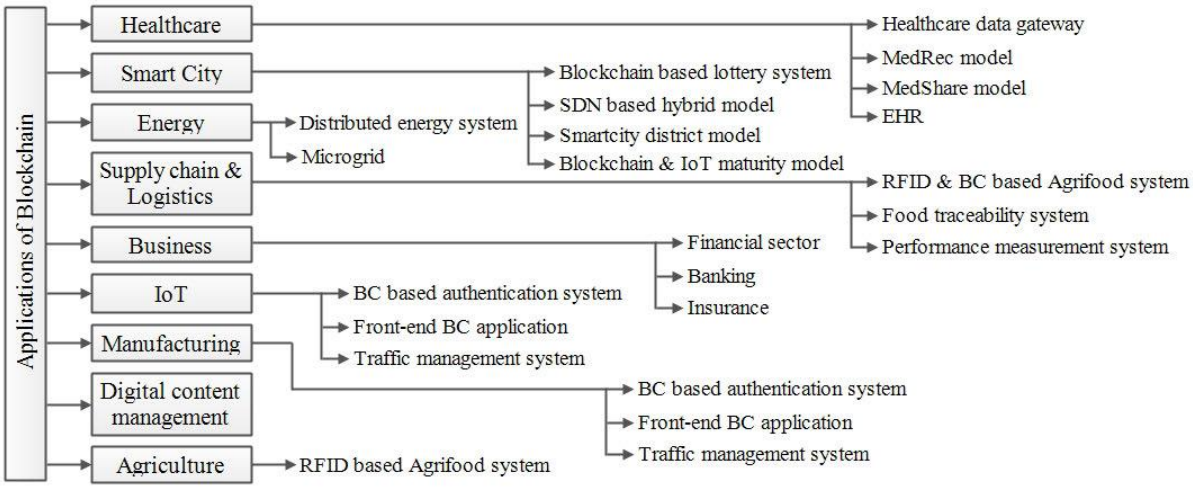
- Δυνατότητα ενημέρωσης: Η ανάγκη για ενημέρωση δεδομένων στο κατανεμημένο καθολικό είναι πιο σημαντική για τις εγγραφές. Σε ένα δίκτυο peer-to-peer, τα δεδομένα πρέπει να δομούνται και να ενημερώνονται συστηματικά για κάθε κόμβο που συναλλάσσεται εντός του δικτύου.

- Κρυπτογράφηση P2P μεταξύ κόμβων Blockchain: Απαιτείται κρυπτογράφηση για τη διασφάλιση των συναλλαγών μεταξύ των τελικών κόμβων που ενδέχεται να συνδέονται μεταξύ τους στο πρωτόκολλο Blockchain.

- UX: Ένας από τους σημαντικότερους παράγοντες σε ένα σύστημα είναι ο σχεδιασμός της διεπαφής χρήστη που παρέχει ένα εύκολο και βολικό περιβάλλον εφαρμογής στους χρήστες. Η κύρια διαφορά μεταξύ των συστημάτων που βασίζονται σε Blockchain και των συστημάτων που δεν βασίζονται σε Blockchain είναι ο τρόπος με τον οποίο το αντιλαμβάνεται ο χρήστης.
- Λειτουργία ανάπτυξης: Το κύριο βήμα στην παραγωγή του συστήματος είναι η επιλογή πλατφορμών που απαιτεί λιγότερο χρόνο και η πολυπλοκότητα της εγκατάστασης.

7.2 Εφαρμογή του Blockchain στην Βιομηχανία 4.0

Η λεπτομερής ταξινόμηση της ανάπτυξης Blockchain σε εφαρμογές πραγματικού χρόνου όπως η ενέργεια, η υγειονομική περίθαλψη, η κατασκευή, η γεωργία, οι επιχειρήσεις, η διανομή ψηφιακού περιεχομένου, το Smart City, το IoT [38], η εφοδιαστική αλυσίδα κλπ. φαίνονται στο παρακάτω σχήμα [58].



Εικόνα 19 Εφαρμογές με ανάπτυξη Blockchain

Α. ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ ΚΑΙ LOGISTICS

Οι γεωργικές εφαρμογές χρειάζονται κρίσιμες εισροές διαχείρισης, όπως η διαχείριση της εφοδιαστικής αλυσίδας (SCM) [59,60] που διαδραματίζει εξέχοντα ρόλο στις ανθρώπινες ζωές. Τα παραδοσιακά συστήματα logistics που χρησιμοποιούνται στην προμήθεια τροφίμων και τη γεωργία απλώς αποθηκεύουν τις παραγγελίες και τις παραδίδουν στον προορισμό. Αυτά τα συμβατικά συστήματα έχουν ένα κενό σε σχέση με διάφορα χαρακτηριστικά όπως η δυνατότητα ελέγχου, η ιχνηλασιμότητα και η διαφάνεια.

Ωστόσο, στη σύγχρονη ψηφιακή εποχή, αυτά τα χαρακτηριστικά μπορούν να βελτιώσουν την ασφάλεια και την ποιότητα των τροφίμων, και ως εκ τούτου, υπάρχει τεράστια ζήτηση καλής ποιότητας τροφίμων από τους καταναλωτές. Συνεπώς, οι περισσότεροι από τους οργανισμούς έρευνας και ανάπτυξης (E&A) υιοθετούν τεχνολογίες IoT [58], όπως ασύρματα δίκτυα

αισθητήρων (WSN) και ταυτοποιήσεις ραδιοσυχνοτήτων (RFIDs), που παρατηρούν εξ αποστάσεως την αλυσίδα εφοδιασμού τροφίμων.

Σύμφωνα με τους Caro [61] και συνεργάτες, οι περισσότερες από τις κεντρικές υποδομές cloud χρησιμοποιούνται ως τρέχουσες λύσεις IoT στο SCM. Αυτές οι υποδομές έχουν συνήθως ανοιχτά ζητήματα όπως η ακεραιότητα των δεδομένων, η έλλειψη διαφάνειας, η παραβίαση και το μεμονωμένο σημείο αστοχίας. Αυτά τα ζητήματα μπορούν να αντιμετωπιστούν με αποτελεσματικό τρόπο χρησιμοποιώντας Blockchains.

Τα αποκεντρωμένα αξιόπιστα συστήματα μπορούν να σχεδιαστούν για το ίδιο χρησιμοποιώντας το Blockchain. Μια αποκεντρωμένη, βασισμένη σε Blockchain λύση με το όνομα AgriBlockIoT, προτάθηκε στο για το Agri-Food SPM. Ενσωμάτωσε διάφορες συσκευές αισθητήρων IoT που παρήγαγαν και κατανάλωναν δεδομένα κατά μήκος της αλυσίδας. Μπορείτε να έχετε πρόσβαση στα αποθηκευμένα δεδομένα και θα μπορούσαν να υλοποιηθούν αυτόνομα εκτελέσιμα έξυπνα συμβόλαια μέσω του AgriblockIoT, με στόχο την επίτευξη διαφάνειας και μη ευελιξίας των εγγραφών σε ένα περιβάλλον που χρησιμοποιεί σύγχρονες συσκευές όπως Mini-PC και πύλες. Η απόδοση και η αποδοτικότητα του AgriblockIoT ποσοτικοποιούνται ως προς το φορτίο της CPU, την κυκλοφορία δικτύου και την καθυστέρηση. Η απόδοση μπορεί να βελτιωθεί δουλεύοντας στις περιορισμένες αρχιτεκτονικές υλικού. Ο Perboli [62] πρότεινε ότι το Blockchain βελτιώνει την αξιοπιστία, την αποτελεσματικότητα και τη διαφάνεια της εφοδιαστικής αλυσίδας και επιταχύνει τις εισερχόμενες διαδικασίες.

Αν και πολλές τεχνολογίες IoT χρησιμοποιούνται για την ασφάλεια των τροφίμων και το SCM, υπάρχουν ορισμένα ζητήματα που δεν αντιμετωπίζονται σωστά. Το κύριο θέμα είναι να αποφασίσουμε εάν οι πληροφορίες ή τα δεδομένα που μοιράζονται τα μέλη άλλης αλυσίδας εφοδιασμού είναι αξιόπιστα ή όχι. Για να ξεπεραστεί αυτό το ζήτημα, προτάθηκε ένα σύστημα που ονομάζεται Ανάλυση Κινδύνου και Κρίσιμα Σημεία Ελέγχου (HACCP), το οποίο παρείχε πληροφορίες εντοπισμού τροφίμων σε πραγματικό χρόνο σε όλα τα μέλη του SCM και διαθέτει χαρακτηριστικά όπως αξιοπιστία, διαφάνεια, ουδετερότητα, ασφάλεια και διαφάνεια.

Β. ΕΝΕΡΓΕΙΑΚΟΣ ΤΟΜΕΑΣ

Η ενέργεια είναι η πραγματική βάση της ύπαρξής μας. Είναι απαραίτητο για τη ζωή των ανθρώπων και όλων των άλλων ζωντανών οργανισμών στη γη.

Οι άνθρωποι και όλα τα ζωντανά πλάσματα στη γη δεν μπορούν να επιβιώσουν απουσία ενέργειας. Χρησιμοποιούμε ενέργεια για διάφορους σκοπούς όπως φαγητό, επικοινωνία, μεταφορά, θέρμανση/ψύξη και φωτισμός. Όλα τα συμβατικά μέσα μεταφοράς όπως τρένα, λεωφορεία, αυτοκίνητα και αεροπλάνα λειτουργούν με ενέργεια, η οποία προέρχεται από ηλεκτρική ενέργεια και ορυκτά καύσιμα. Τα τρόφιμα μας καλλιεργούνται με σημαντική ενεργειακή δαπάνη και η αποθήκευση και η μεταφορά τους καταναλώνουν επίσης ενέργεια. Οι τρόποι επικοινωνίας μας, όπως το διαδίκτυο και τα τηλέφωνα, λειτουργούν με ηλεκτρισμό. Ο ήλιος είναι η κύρια πηγή όλων των ενεργειών που είναι διαθέσιμες στη γη.

Επιπλέον, είναι πολύ σημαντικό να επιλέγετε προσεκτικά τον τύπο των ενεργειακών πόρων, γιατί μπορεί να οδηγήσει σε δυσμενείς επιπτώσεις στο περιβάλλον, όπως η υπερθέρμανση του πλανήτη και η ρύπανση. Οι ενεργειακοί πόροι ταξινομούνται σε δύο κατηγορίες:

- μη ανανεώσιμες πηγές και
- ανανεώσιμες πηγές ενέργειας.

Η εκθετική χρήση μη ανανεώσιμων πόρων μπορεί να οδηγήσει σε σπάνια ύπαρξη αυτών των πόρων. Άρα, είναι πολύ σημαντικό να τα διαχειρίζεσαι με εντατική φροντίδα και σωστή διαχείριση. Η σωστή χρήση των μη ανανεώσιμων πόρων έχει καταστεί υποχρεωτική λόγω της σπανιότητάς τους. Η χρήση ανανεώσιμων πηγών ενέργειας όπως η ηλιακή ενέργεια ή ο άνεμος μπορεί να αξιοποιήσει την ενεργειακή απόδοση για τη διατήρηση του οικοσυστήματος. Ως εκ τούτου, στις μέρες μας, οι περισσότερες χώρες ενθαρρύνουν τους ανθρώπους τους να χρησιμοποιούν ανανεώσιμες πηγές ενέργειας για την ανάπτυξη των βιομηχανιών, της γεωργίας και των μεταφορών τους [63].

C. ΔΙΑΝΟΜΗ ΨΗΦΙΑΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ

Από την εμπορευματοποίηση του Διαδικτύου το 1994, οι υπηρεσίες παράδοσης ψηφιακού περιεχομένου έχουν αυξηθεί εκθετικά [64].

Τα συστήματα παράδοσης είναι κυρίως δύο τύπων:

- μη προστατευμένα και
- προστατευμένα συστήματα παράδοσης.

Γενικά, το ψηφιακό περιεχόμενο προστατεύεται χρησιμοποιώντας τον συμβατικό μηχανισμό κρυπτογράφησης. Διαφορετικοί μηχανισμοί κρυπτογράφησης χρησιμοποιούν διαφορετικούς τρόπους για τη δημιουργία, τη διάδοση και τη διατήρηση των κλειδιών και την αποκρυπτογράφηση του κρυπτογραφημένου περιεχομένου με κλειδιά. Τα παραδοσιακά συστήματα όπως το Σύστημα Πρόσβασης υπό όρους και η Διαχείριση Ψηφιακών Δικαιωμάτων (DRM) είναι δημοφιλή για την προστασία ψηφιακού περιεχομένου, αλλά αντιμετωπίζουν ορισμένα σημαντικά ζητήματα όπως επιθέσεις δικτύου, κλοπή κλειδιών και πειρατικές επιθέσεις.

Για να ξεπεραστούν τα μειονεκτήματα του συμβατικού κεντρικού συστήματος, δημιουργήθηκε ένα αποκεντρωμένο σύστημα διανομής ψηφιακού περιεχομένου βασισμένο στην τεχνολογία Blockchain. Σε αυτό το σύστημα ψηφιακού περιεχομένου, ο κάτοχος του πραγματικού περιεχομένου θα μπορούσε να επιβλέπει και να ελέγχει την ασφάλεια καθώς και την απλότητα. Η χρήση των τεχνικών εξόρυξης εξασφάλισε ότι η προσθήκη κάθε τύπου συναλλαγής στο Blockchain [64]. Το PoW χρησιμοποιήθηκε ως ο μηχανισμός συναίνεσης για να εγγυηθεί την ασφάλεια και το απόρρητο των συναλλαγών που είναι αποθηκευμένες στο Blockchain. Λόγω ορισμένων ανοιχτών ζητημάτων όπως η επίθεση πειρατών, δεν ήταν δυνατός ο πλήρης έλεγχος αυτού του μηχανισμού.

D. ΤΟΥΡΙΣΜΟΣ ΚΑΙ ΦΙΛΟΞΕΝΙΚΗ ΒΙΟΜΗΧΑΝΙΑ

Ο τουρισμός είναι η διαδικασία του να περνάμε χρόνο σε εξωτερικό μέρος, δηλαδή μακριά από το σπίτι μας για σκοπούς όπως επαγγελματικούς , προσωπικούς , χαλάρωση και

ευχαρίστηση. Η εξυπηρέτηση των ταξιδιωτών είναι η κύρια λειτουργία της τουριστικής βιομηχανίας.

Σήμερα, οι περισσότεροι άνθρωποι αναζητούν και κάνουν κράτηση για τα ταξιδιωτικά τους εισιτήρια, τα τρόφιμα και τη διαμονή τους μέσω του Διαδικτύου. Ως εκ τούτου, η παγκόσμια χρήση του διαδικτύου, η βιομηχανία του τουρισμού και της φιλοξενίας έχει γνωρίσει ραγδαίες αλλαγές. Σε αυτόν τον ψηφιακό κόσμο, πολλές τουριστικές εταιρείες όπως η Expedia Group, η BCD Travel, η Uber, η Ola και η AirBnb έχουν αντικαταστήσει τα παραδοσιακά επιχειρηματικά τους μοντέλα με μοντέλα Consumer-to-Consumer (C2C) για να επιτύχουν διαφάνεια και ασφάλεια στις συναλλαγές.

Επιπρόσθετα, υπάρχει τεράστια ζήτηση για καινοτόμες πλατφόρμες στην τουριστική βιομηχανία, οι οποίες μπορούν να ενσωματώσουν τεχνολογία, χρήματα και γνώση. Η TUI και πολλές άλλες εταιρείες έχουν ήδη αρχίσει να χρησιμοποιούν το Blockchain για την υλοποίηση λειτουργιών όπως η κράτηση εισιτηρίων και η πραγματοποίηση πληρωμών. Πολλές εταιρείες όπως η Expedia, η CheapAir, η Webjet και τα One Shot Hotels χρησιμοποιούν Bitcoin για ταξιδιωτικούς σκοπούς, δηλαδή για κράτηση και κράτηση εισιτηρίων.

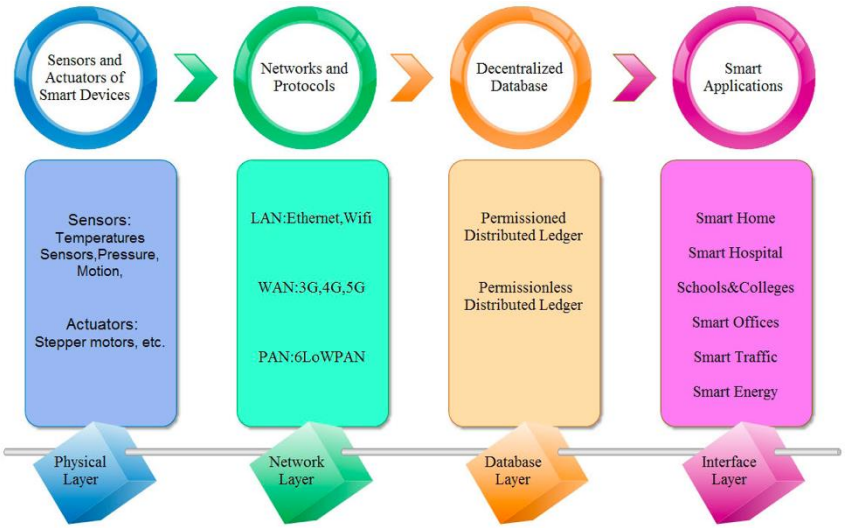
Συνεπώς, τα ψηφιακά νομίσματα απλώς ενσωματώνονται με έξυπνα συμβόλαια τα οποία έχουν αρκετή δυνατότητα να αναπτύξουν τεχνολογίες με μεγάλη αναστάτωση για την τουριστική βιομηχανία.

E. SMARTCITY

Σε εφαρμογές έξυπνων πόλεων, χρησιμοποιούνται ετερογενείς αισθητήρες από διάφορες έξυπνες συσκευές και χρήστες για τη συλλογή των απαιτούμενων δεδομένων. Αυτά τα δεδομένα υποβάλλονται σε επεξεργασία και χρησιμοποιούνται στη διαχείριση της κυκλοφορίας, τα συστήματα μεταφορών, τη διαχείριση απορριμμάτων, τα σχολεία, τις βιβλιοθήκες, τα δίκτυα ύδρευσης, τις κοινοτικές υπηρεσίες και τους σταθμούς παραγωγής ενέργειας για τη βελτίωση της απόδοσης.

Υπάρχει σταδιακή αύξηση του αριθμού των ανθρώπων που ζουν στις περιοχές της πόλης. Λόγω της αυξημένης χρήσης του Διαδικτύου, των μεγάλων δεδομένων και του IoT, η έννοια της έξυπνης πόλης έχει γίνει πολύ δημοφιλής [65].

Για να ενισχύσουμε την ανάπτυξη των έξυπνων πόλεων, χρειαζόμαστε αποτελεσματικούς μηχανισμούς για την επίλυση των υφιστάμενων προβλημάτων που σχετίζονται με την ενέργεια, τις μεταφορές, τη διακυβέρνηση και το περιβάλλον. Ορισμένα ανοιχτά ζητήματα όπως η ανεπαρκής ασφάλεια στο IoT [38], η δυσκολία στη συντήρηση και αναβάθμιση του εξοπλισμού, η διατήρηση της εμπιστοσύνης μεταξύ των χρηστών του Διαδικτύου, η βελτιστοποίηση του κόστους λειτουργίας κέντρων δεδομένων, η αντοχή σε ζημιές, το απόρρητο και η ασφάλεια πρέπει να αντιμετωπιστούν για την ανάπτυξη έξυπνων έργα της πόλης αποτελεσματικά και αποδοτικά.



Εικόνα 20 SMARTCITY

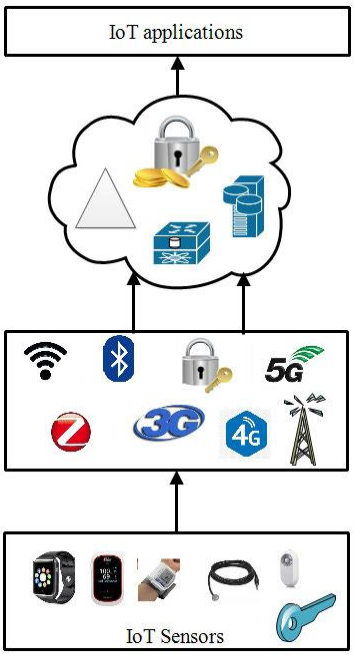
Επιπλέον, η τεχνολογία Blockchain είναι η δυνατότητα επίλυσης όλων αυτών των προβλημάτων και ως εκ τούτου, είναι η πλέον κατάλληλη για την ανάπτυξη λύσεων έξυπνων πόλεων [66].

Όπως γνωρίζουμε, η κατανάλωση ενέργειας αυξάνεται λόγω της αστικής ανάπτυξης. Σκοπός του Διαδικτύου είναι η ανάπτυξη ενός ευφυούς ενεργειακού συστήματος. Οι ερευνητές επικεντρώθηκαν κυρίως στο πώς το Blockchain θα μπορούσε να βοηθήσει στην επίλυση προβλημάτων στο διαδίκτυο, στα μεγάλα δεδομένα και στο IoT . Εξετάζοντας ζητήματα όπως η πιστοληπτική ικανότητα του χρήστη, η πιστοληπτική ικανότητα των δεδομένων στην κεντρική βάση δεδομένων, η προστασία του απορρήτου των δεδομένων και η προστασία της ιδιωτικής ζωής των δεδομένων [67].

F. INTERNET OF THINGS (IoT)

Στο Internet of Things (IoT), διάφορες συσκευές συνδέονται μέσω του Διαδικτύου για να μοιράζονται χρήσιμες πληροφορίες μέσω διακομιστών για την εκτέλεση συγκεκριμένων εργασιών ή ενεργειών στο εξωτερικό περιβάλλον, όπως η μέτρηση της θερμοκρασίας ή της υγρασίας και η μετακίνηση του άξονα. Η παράδοση των σωστών πληροφοριών στα σωστά άτομα τη σωστή στιγμή είναι δυνατή μέσω της χρήσης του IoT. Διάφοροι αισθητήρες ανιχνεύουν συνεχώς τα δεδομένα και αυτά τα δεδομένα που συλλέγονται μπορούν να χρησιμοποιηθούν για αποτελεσματική λήψη αποφάσεων. Τα πράγματα που είναι συνδεδεμένα στο διαδίκτυο αναμένεται να ξεπεράσουν τα 50 δισεκατομμύρια στο εγγύς μέλλον, κάτι που είναι βασικά μια προσέγγιση του τρόπου με τον οποίο αυτές οι διάφορες συσκευές θα πρέπει να σχεδιαστούν και να ενσωματωθούν μεταξύ τους, έτσι ώστε να παρέχεται ένα δίκτυο παροχής υπηρεσιών, το οποίο μπορεί να εξυπηρετήσει τις ανάγκες σε το μέλλον [68].

Η αρχιτεκτονική του IoT είναι βασικά η ραχοκοκαλιά οποιασδήποτε εφαρμογής και επομένως, θα πρέπει να δημιουργηθεί προσεκτικά λαμβάνοντας υπόψη τις ανάγκες της εξέλιξης της λειτουργικότητας, της επεκτασιμότητας, της διαθεσιμότητας και της δυνατότητας συντήρησης. Από αυτό το μοντέλο αρχιτεκτονικής IoT, είναι πολύ σαφές ότι η ασφάλεια είναι ένας ουσιαστικός παράγοντας σε όλα τα επίπεδα IoT όπως φαίνεται στην εικόνα [69].



Εικόνα 21 Εφαρμογές IoT

Σήμερα, οι περισσότερες συσκευές IoT δεν είναι πλήρως ασφαλείς και μπορούν εύκολα να παραβιαστούν. Αυτές οι συσκευές έχουν περιορισμένη χωρητικότητα δικτύου, περιορισμένη υπολογιστική ισχύ και μικρή χωρητικότητα αποθήκευσης. Λόγω αυτών των χαρακτηριστικών, τέτοιες συσκευές είναι ευάλωτες σε ποικίλες επιθέσεις σε σύγκριση με συστήματα υπολογιστών.

Οι Samaniego και Deters παρατήρησαν ότι τα ζητήματα του λανθάνοντος χρόνου δικτύου προέκυψαν λόγω των συστημάτων IoT που επικεντρώνονται στο cloud. Για να ξεπεράσουν αυτά τα προβλήματα, ανέπτυξαν μια δομή διαχείρισης IoT που έχει σχεδιαστεί από λογισμικό, γνωστή ως Virtual Resources (VR). Οι απαραβίαστες, αποκεντρωμένες αλυσίδες μπλοκ έχουν τη δυνατότητα να λύσουν ζητήματα ασφάλειας σε οποιαδήποτε εφαρμογή IoT. Για να χρησιμοποιήσετε το Blockchain ως υπηρεσία για το IoT, το περιβάλλον φιλοξενίας είναι μία από τις προκλήσεις [69].

G. ΓΕΩΡΓΙΑ

Τον τελευταίο καιρό έχουν παρατηρηθεί διάφορα ζητήματα που σχετίζονται με την ασφάλεια των τροφίμων. Η υψηλότερη χρήση λιπασμάτων και φυτοφαρμάκων στα γεωργικά προϊόντα είναι το κύριο μέλημα για την ασφάλεια των τροφίμων. Τα υπολείμματα φυτοφαρμάκων και λιπασμάτων σε διάφορα γεωργικά προϊόντα έχουν προκαλέσει παγκόσμια ανησυχία.

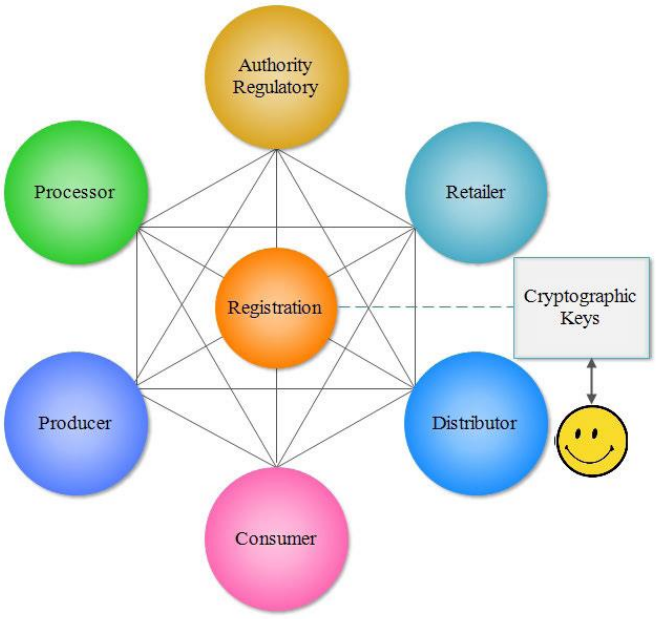
Εξαιτίας αυτού, υπάρχει τεράστια ζήτηση για ασφαλή αγροτικά προϊόντα στην αγορά. Για να καλύψουμε αυτή τη ζήτηση, χρειαζόμαστε ασφαλείς λύσεις για το χειρισμό της τέλειας ανίχνευσης και διαχείρισης της παραγωγής, της χονδρικής, της εφοδιαστικής στη λιανική, των προτύπων παραγωγής, των πιστοποιήσεων και της επιχειρηματικής φήμης .

Ο Hua [70] και οι συνεργάτες του, πρότεινε ένα σύστημα αγροτικής παρακολούθησης βασισμένο σε Blockchain, το οποίο ήταν βασικά ένα αποκεντρωμένο σύστημα προκειμένου να λυθεί η κρίση εμπιστοσύνης στον τομέα της εφοδιαστικής αλυσίδας. Αυτή η πλατφόρμα γεωργίας που βασίζεται σε Blockchain κατέγραψε τις πληροφορίες σχετικά με την παραγωγή, αποθήκευση, μεταφορά, επεξεργασία, διανομή και εφοδιαστική αλυσίδα γεωργικών προϊόντων για τρίτα μέρη, όπως κυβέρνηση, ασφαλιστικές εταιρείες, πελάτες και τράπεζες. Η πλατφόρμα τα κατέγραψε όλες τις πληροφορίες σχετικά με το γεωργικό προϊόν στο

Blockchain, τις δομές, καθώς θα μπορούσε να περιλαμβάνει διαφορετικούς χρήστες, όπως εταιρείες, φορείς, τράπεζες ή κυβέρνηση να συνεργαστούν.

Λαμβάνοντας υπόψη τις απαιτήσεις, αναπτύχθηκε ένα γεωργικό σύστημα ιχνηλασιμότητας για το ίδιο. Αυτό το σύστημα έλαβε υπόψη τα λιπάσματα, τα φυτοφάρμακα, τις εταιρείες, τους σπόρους, τις γεωργικές εργασίες, τον χρόνο και τις δοκιμές υπολειμμάτων. Σύμφωνα με τους συγγραφείς, ήταν ένα πολύ κουραστικό έργο να χτιστεί μια πλατφόρμα με ομοιόμορφη δομή, η οποία έλαβε υπόψη όλες τις σύνθετες πληροφορίες και εξαλείφει την πιθανότητα πλεονασμού σε δεδομένα.

Ως εκ τούτου, οι ερευνητές σχεδίασαν δύο σχετικές δομές ειδικά για τις βασικές πληροφορίες φύτευσης καθώς και για τα αρχεία προέλευσης. Οι πληροφορίες φύτευσης περιλάμβαναν τις πληροφορίες παραγωγής πηγής όσον αφορά την ταυτότητα, το όνομα του είδους, τον χρόνο φύτευσης, το όνομα της εταιρείας, τον αριθμό του θερμοκηπίου και τη γεωγραφική θέση. Τα αρχεία προέλευσης περιλαμβάνουν τις λεπτομέρειες σχετικά με τις γεωργικές δραστηριότητες όσον αφορά την ταυτότητα, την ημερομηνία και την ώρα, το πρόσωπο, την ψηφιακή υπογραφή, την τοποθεσία, τον τύπο λειτουργίας, τις εισροές και το σημείωμα και την εταιρεία. Η πλατφόρμα παρακολούθησης της γεωργίας αποτελούνταν από τρία στοιχεία - κόμβο δεδομένων, πελάτες και κέντρο εγγραφής.



Εικόνα 22 Σύστημα ιχνηλασιμότητας τροφίμων

Συνεπώς, τα ζητήματα στο γεωργικό σύστημα, όπως η πιστοληπτική ικανότητα των δεδομένων και η ενοποίηση των υποσυστημάτων, αντιμετωπίστηκαν εύκολα από αυτήν την ανοιχτή πλατφόρμα ανταλλαγής δεδομένων [71]. Εξαιτίας αυτού, οποιοσδήποτε συμμετέχων μπορούσε να δει τα δεδομένα που ανέβασαν οι συμμετέχουσες εταιρείες, κάτι που ήταν επίσης ένα από τα σημαντικότερα πλεονεκτήματα αυτής της πλατφόρμας.

7.3 Προκλήσεις στους τομείς της Βιομηχανίας 4.0

Οι τομείς που θα διερευνήσουμε για τις προκλήσεις στη Βιομηχανία 4.0 είναι οι εξής:

1) Τομέας Υγείας
2) Τομέας Internet of Things
3) Τομέας Επιχειρήσεων
4) Τομέας της Έξυπνης Πόλης
5) Τομέας γεωργίας
6) Τομέας Εφοδιαστικής Αλυσίδας

Πιο συγκεκριμένα θα αναλυθούν παρακάτω.

7.2.1 Προκλήσεις στον τομέα της υγείας

a) <u>Δείκτες ασθενών</u>

Κάθε χρόνο ο όγκος των δεδομένων που σχετίζονται με την υγειονομική περίθαλψη αυξάνεται και συχνά όταν ασχολούμαστε με τα δεδομένα υγειονομικής περίθαλψης, τα αρχεία αναντιστοιχίζονται ή αντιγράφονται. Επίσης, διαφορετικά συστήματα ηλεκτρονικών αρχείων υγείας έχουν τη δική τους μορφή δεδομένων και σύνολο δεδομένων για την εισαγωγή και την εκτέλεση των δεδομένων, γεγονός που δημιουργεί την ανάγκη ύπαρξης τυποποιημένης μορφής δεδομένων. Λόγω της χρήσης τεχνολογίας Blockchain, τα δεδομένα κατακερματίζονται κρυπτογραφικά στο καθολικό. Ο χρήστης θα μπορούσε να αναζητήσει τις καταγεγραμμένες συναλλαγές που μπορεί να έχουν πολλαπλές εγγραφές ή τα κλειδιά, αλλά με τη χρήση της τεχνολογίας Blockchain, όλες οι πληροφορίες συνδέονται με αναγνωριστικά ενός ασθενούς [72].

b) Διαχείριση Δεδομένων ασθενών

Ο νόμος της φορητότητας και της λογοδοσίας ασφάλισης υγείας είναι γνωστός ως (HIPAA-Health Insurance Portability and Accountability Act) ελέγχει το απόρρητο των δεδομένων των ασθενών και καθιστά ασφαλή τα δεδομένα PHI, αλλά οι ασθενείς πρέπει να δώσουν τα ιατρικά τους δεδομένα σε τρίτους, όπως φαρμακοποιούς, επιβάλλοντας την ανάγκη προστασίας των δεδομένων . Με τη χρήση του Blockchain, δημιουργείται ένας κατακερματισμός για τις πληροφορίες υγείας κάθε ασθενούς σε μπλοκ που περιέχουν τα αναγνωριστικά ασθενών. Χρησιμοποιώντας το API δικτύου ενός Blockchain, τα δεδομένα που σχετίζονται με την ασθένεια μπορούν να προβληθούν σε σχέση με τον πάσχοντα ασθενή χωρίς αποκαλύπτοντας τα προσωπικά στοιχεία του ασθενούς. Με τον ίδιο τρόπο, ένας ασθενής μπορεί να έχει το προνόμιο να αποφασίσει ποιος μπορεί να δει ή να έχει πρόσβαση στα δεδομένα του με ένα συγκεκριμένο τρίτο μέρος [72].

c) Ακεραιότητα Δεδομένων

Οι πληροφορίες υγείας των ασθενών, τα ηλεκτρονικά αρχεία υγείας, τα δεδομένα που συλλέγονται από το IoT και τα συστήματα παρακολούθησης διατηρούνται από τις ιατρικές εγκαταστάσεις. Εδώ, ο κύριος στόχος είναι η διασφάλιση των πληροφοριών και των τεχνικών κοινής χρήσης τους, η εξουσιοδότηση των εγκαταστάσεων υγειονομικής περίθαλψης και των φορέων τους να επιβεβαιώνουν τις σωστές πληροφορίες και να διασφαλίζουν τις κατάλληλες υπηρεσίες. Το Blockchain είναι πιο χρήσιμο σε τέτοια σενάρια λόγω της ικανότητάς του να παρέχει ακεραιότητα δεδομένων. Επιπλέον, η προσέγγιση του Blockchain είναι να μοιράζεται και να διανέμει δεδομένα δημόσια με τις ασφαλείς συναλλαγές. Η τεχνική που χρησιμοποιείται από αυτή την τεχνολογία είναι PoW με χρονική σήμανση.

d) Κλινικές δοκιμές

Οι ερευνητές που εργάζονται σε διάφορους τομείς θέλουν πάντα οι εμπιστευτικές τους πληροφορίες να αποθηκεύονται ιδιωτικά και με ασφάλεια, έτσι ώστε κανένα μη εξουσιοδοτημένο άτομο να μην μπορεί να παραβιάσει ή να τροποποιήσει ή να κλέψει τα δεδομένα τους. Στην τεχνολογία Blockchain, η τροποποίηση δεδομένων είναι αδύνατη με τον αλγόριθμο SHA256 που δημιουργεί τις μοναδικές τιμές κατακερματισμού που συνδέονται

μεταξύ τους σε μια αλυσίδα. Ο κλάδος της υγειονομικής περίθαλψης πρέπει να διατηρεί και να μοιράζεται με ασφάλεια τις πληροφορίες που σχετίζονται με κλινικές δοκιμές, οι οποίες μπορούν να κοινοποιηθούν μόνο σε εξουσιοδοτημένα μέρη, όπως χορηγούς έρευνας ή ρυθμιστικές επιτροπές. Με το Blockchain, τα δεδομένα μπορούν να διαχειρίζονται ή να ανιχνεύονται με συναίνεση σε πολλούς ιστότοπους, πρωτόκολλα και συστήματα. Οι ασθενείς που έχουν κατάλληλα προνόμια πρόσβασης μπορούν επίσης να έχουν πρόσβαση σε αυτές τις πληροφορίες σχετικά με θέματα υγείας τους και σχετική έρευνα [72].

e) Ιχνευσιμότητα Φαρμάκων

Επί του παρόντος, το κύριο εμπόδιο στη φαρμακολογία είναι η παραχάραξη φαρμάκων. Από την έρευνα των ερευνητών υγείας, έχει παρατηρηθεί ότι περίπου το 10 με 30 τοις εκατό των φαρμάκων στις αναπτυσσόμενες χώρες είναι διπλά. Το αρνητικό αποτέλεσμα αυτού είναι η απώλεια της επιχείρησης και η ακατάλληλη χρήση πλαστών φαρμάκων που μπορεί να οδηγήσει σε σοβαρές βλάβες στην υγεία ενός ατόμου. Η χρήση του δικτύου Blockchain στις εγκαταστάσεις ναρκωτικών μπορεί να εντοπίσει απάτες από τον έμπορο ναρκωτικών. Όλες οι λειτουργίες από τους κατασκευαστές έως τους προμηθευτές περιέχονται στο δίκτυο Blockchain που επιτρέπει την ανίχνευση ολόκληρης της διαδρομής των φαρμάκων.

f) Εμπλουτισμός των δεδομένων

Η αποθήκευση των μη δομημένων δεδομένων μπορεί να οδηγήσει σε μεταβλητότητα, κατανάλωση χρόνου στη διαδικασία αναζήτησης, έλλειψη αξιοπιστίας. Ο εμπλουτισμός δεδομένων είναι μια λειτουργία για την προσθήκη αξιών για την αύξηση της ποιότητας. Τα αρχεία υγείας πρέπει να είναι δομημένα, ασφαλή, ακριβή, με χρονική σήμανση και ευανάγνωστα. Απαιτείται να εκτελεστούν τα ακόλουθα βήματα για την οργάνωση των δεδομένων πριν από την προσθήκη τους στο Blockchain: Αντικατάσταση της ταυτότητας του ασθενούς με το δημόσιο κλειδί κατακερματισμού, προετοιμασία του για συμμόρφωση, προσθήκη μετα-πληροφοριών και δόμησή του για υπολογισμό. Τα οργανωμένα δεδομένα επιτρέπουν σε όλους τους παρόχους υγειονομικής περίθαλψης να έχουν πρόσβαση στα δεδομένα αποτελεσματικά [72].

7.2.3 Προκλήσεις στον τομέα του Internet of Things

a) Αρχιτεκτονική του IoT

Τα οικοσυστήματα IoT [38] εξαρτώνται από το κεντρικό δίκτυο στο οποίο όλες οι συσκευές είναι συνδεδεμένες σε ένα μοντέλο πελάτη-διακομιστή μέσω της επικοινωνίας μέσω διαμεσολάβησης. Χρησιμοποιεί τον διακομιστή cloud για τον έλεγχο ταυτότητας και την αναγνώριση συσκευών. Χρειάζεται υψηλότερο χρόνο επεξεργασίας, υπολογιστική ισχύ και εύρος ζώνης. Η αποκεντρωμένη αρχιτεκτονική Blockchain δημιουργεί ένα δίκτυο P2P μέσω του οποίου η ανταλλαγή μηνυμάτων, η κοινή χρήση και ο συντονισμός συσκευών γίνονται ευκολότερες.

b) Κεντρικές Βάσεις Δεδομένων

Μια κεντρική βάση δεδομένων έχει περιορισμένη υπολογιστική ισχύ και χωρητικότητα αποθήκευσης. Υπάρχει πάντα ένας μεγάλος αριθμός κόμβων για σύνδεση στον διακομιστή, κάτι που είναι μια χρονοβόρα εργασία. Είναι επίσης δύσκολο να υπάρχουν ελαττωματικοί κόμβοι σε αυτή τη δομή. Οι περισσότερες συσκευές IoT [38] συνδέονται με την κεντρική βάση δεδομένων και το δίκτυο cloud, γεγονός που αυξάνει το κόστος και τις υπολογιστικές απαιτήσεις. Στην τεχνολογία κατανεμημένης αλυσίδας μπλοκ, οι κόμβοι έχουν ελάχιστη συνδεσιμότητα και, ωστόσο, το δίκτυο παραμένει αξιόπιστο και ασφαλές. Με τους κατανεμημένους υπολογιστές, η χρήση της διαθέσιμης υπολογιστικής ισχύος αυξάνεται για δισεκατομμύρια συναλλαγές, ανεξάρτητα από την τοποθεσία των συσκευών. Αυτό καθιστά το IoT πιο αξιόπιστο και οικονομικό.

c) Θέματα Απορρήτου και ασφάλειας

Εάν τα δεδομένα των χρηστών αποθηκεύονται σε μια κεντρική βάση δεδομένων, το απόρρητο και η ασφάλεια γίνονται το κύριο μέλημα. Σήμερα, για να κερδίσουν πλεονεκτήματα, διάφορες εταιρείες αποθηκεύουν, χρησιμοποιούν και πωλούν τα δεδομένα των χρηστών σε τρίτους χωρίς τη συγκατάθεση των χρηστών. Τέτοιες ενέργειες θέτουν σε κίνδυνο το απόρρητο των δεδομένων των χρηστών. Η τεχνολογία Blockchain χρησιμοποιεί μια κατανεμημένη δομή

βάσης δεδομένων που αποθηκεύει δεδομένα σε κρυπτογραφημένη μορφή και έτσι μειώνει τον κίνδυνο κλοπής δεδομένων και παραβίασης του απορρήτου.

d) Νομική αναγνώριση συσκευών

Στην τρέχουσα εποχή, οι συσκευές αισθητήρων που χρησιμοποιούνται στις εφαρμογές IoT είναι μικρού μεγέθους και έχουν περιορισμένη χωρητικότητα υπολογιστών και αποθήκευσης. Ως εκ τούτου, τέτοιες συσκευές είναι ευάλωτες σε φυσικές επιθέσεις όπως πλαστοπροσωπία ή υποκλοπή. Η τεχνολογία Blockchain χρησιμοποιεί έξυπνα συμβόλαια και μηχανισμό συναίνεσης που ενισχύουν τη σωστή επαλήθευση ταυτότητας των κόμβων IoT, και εξαλείφει τη μη εξουσιοδοτημένη πρόσβαση στις ενεργές συσκευές από άγνωστους χρήστες.

7.2.3 Προκλήσεις στον τομέα των Επιχειρήσεων

a) Απόρρητο Δεδομένων

Το απόρρητο δεδομένων είναι μία από τις βασικές προκλήσεις στον επιχειρηματικό τομέα, όπου πολλά συστήματα αντιμετωπίζουν παραβιάσεις δεδομένων, διαρροή προσωπικών πληροφοριών, μη εξουσιοδοτημένη παρακολούθηση και υποκλοπή, παραβίαση δικαιωμάτων ελέγχου πρόσβασης, κλοπή και διαρροή δεδομένων. Με την κατανεμημένη τεχνολογία Blockchain, τα δεδομένα αποθηκεύονται με αμετάβλητο τρόπο έχοντας εξασφαλίσει χρονική σήμανση, δημόσιο έλεγχο και συναίνεση, καθιστώντας το σύστημα ανθεκτικό έναντι ζητημάτων απορρήτου.

b) Αποκατάσταση καταστροφής

Η αποθήκευση και η δημιουργία αντιγράφων ασφαλείας δεδομένων είναι πολύ σημαντικά σε κάθε επιχειρηματική εφαρμογή. Για την αποθήκευση και τη διατήρηση μεγάλου όγκου δεδομένων, απαιτείται περισσότερη υπολογιστική ισχύς που έχει ως αποτέλεσμα την αύξηση του συνολικού κόστους. Επιπλέον, εάν τα δεδομένα διατηρούνται σε ένα κεντρικό σύστημα, αυξάνεται επίσης ο κίνδυνος ενός μόνο σημείου αστοχίας. Ο μηχανισμός Blockchain χρησιμοποιεί αποκεντρωμένα συστήματα για τον κατανεμημένο χειρισμό δεδομένων.

Χρησιμοποιείται μια ιεραρχία συμπλέγματος για αποθήκευση και δημιουργία αντιγράφων ασφαλείας δεδομένων που εξαλείφει την πιθανότητα απώλειας των δεδομένων.

c) Smart Contracts

Η διαδικασία σύναψης συμβάσεων περιλαμβάνει υποβολή προσφορών, επικύρωση και έγκριση για την ενεργοποίηση των επόμενων βημάτων. Η εκτέλεση μιας παραδοσιακής σύμβασης μπορεί να απαιτεί ανθρώπινη παρέμβαση που καθιστά τη συμμετοχή τρίτου ως υπηρεσία. Το ίδιο απαιτείται ακόμη και κατά τη διάρκεια διαφωνιών και οδηγεί σε μεγαλύτερο χρόνο για την κατανάλωση πόρων και το υψηλό κόστος της σύμβασης. Με τη χρήση Blockchain δημιουργείται έξυπνος αυτοματισμός χωρίς ανθρώπινη παρέμβαση, ο οποίος εξαλείφει την εμπλοκή συναλλαγών τρίτων και τις περιττές χρονικές καθυστερήσεις.

d) Επιστολή πιστωτικής Πληρωμής (LETTER OF CREDIT- LC)

Μια διεθνής πληρωμή πίστωσης απαιτεί έναν αγοραστή και έναν αντιπρόσωπο και χρησιμοποιούν πιστώσεις που βασίζονται σε χαρτί για να πραγματοποιήσουν συναλλαγές. Σε αυτό το σενάριο, κάθε συμβαλλόμενο μέρος πρέπει να στείλει τα απαραίτητα έγγραφα μέσω ταχυδρομείου ή υπηρεσιών ταχυμεταφοράς. Λόγω της απαίτησης, ο χρόνος και το κόστος της διαδικασίας είναι πολύ υψηλότερο και δεν είναι βολικό για τους εξαγωγείς. Εάν χρησιμοποιηθεί σε αυτόν τον τομέα, η τεχνολογία Blockchain έχει τη δυνατότητα να εξαλείψει τη χρονική καθυστέρηση παρέχοντας οικονομικά αποδοτική ταχύτερες υπηρεσίες. Το Blockchain κάνει τις συναλλαγές διαφανείς και ενσωματωμένες με τον ηλεκτρονικό λογαριασμό του καθολικού.

7.2.4 Προκλήσεις στον τομέα της Έξυπνης Πόλης

a) Ψηφιακή Ταυτότητα

Στις διαδικτυακές υπηρεσίες χρειάζονται οι χρήστες ή οι πελάτες να παρέχουν προσωπικά στοιχεία ταυτοποίησης πριν κάνουν χρήση των υπηρεσιών. Όλα αυτά τα δεδομένα αποθηκεύονται εν αγνοία των ιδιοκτητών και είναι προσβάσιμα από τρίτους. Όταν η

αποκεντρωμένη τεχνολογία Blockchain χρησιμοποιείται για την υλοποίηση διαδικτυακών υπηρεσιών, δημιουργούνται ψηφιακά αναγνωριστικά για όλους τους χρήστες.
Αυτά τα αναγνωριστικά μαζί με τεχνικές ψηφιακής υδατογράφησης χρησιμοποιούνται κατά την εκτέλεση συναλλαγών χρήστη. Αυτός είναι ο τρόπος με τον οποίο τα δεδομένα των χρηστών μπορούν να αποθηκευτούν, να διατηρηθούν και να ελέγχονται στο εξουσιοδοτημένο δίκτυο με δικαιώματα πρόσβασης μόνο με τους μεμονωμένους χρήστες.

b) Διαχείρηση Μεταφορών

Η μεταφορική επιχείρηση είναι πολύ δημοφιλής αυτές τις μέρες για την παροχή καθημερινών υπηρεσιών σε μεγάλο αριθμό πελατών. Η παροχή των απαραίτητων υπηρεσιών στους πελάτες είναι αρκετά δαπανηρή. Η εμπλοκή τρίτων στην παροχή υπηρεσιών μπορεί να οδηγήσει σε παραβίαση του απορρήτου των προσωπικών δεδομένων των χρηστών καθώς και σε αύξηση του κόστους χρήσης των υπηρεσιών. Ένα αποκεντρωμένο δίκτυο Blockchain μπορεί να χειριστεί όλα αυτά τα ζητήματα αποτελεσματικά και αποδοτικά, ενεργοποιώντας μια πλατφόρμα P2P για υπηρεσίες μεταφοράς.

c) Εκπαίδευση

Πλέον, τα εκπαιδευτικά ιδρύματα είτε ιδιωτικά είτε δημόσια δεν παρέχουν τα ακριβή αρχεία στην κυβέρνηση. Αυτός είναι ο λόγος για τον οποίο η κυβέρνηση δεν μπορεί να ελέγξει ή να βοηθήσει για στόχους αλφαβητισμού. Με τη συμπερίληψη της τεχνολογίας Blockchain, τα εκπαιδευτικά αρχεία μπορούν να διατεθούν μέσω ενός αυτοματοποιημένου μηχανισμού συναίνεσης. Αυτή η λύση καθιστά τις πληροφορίες περιττές και τις ίδιες μπορεί να ενσωματώσει στο δημόσιο μητρώο πληθυσμού, ώστε να μπορεί να χειριστεί όλους τους στόχους αλφαβητισμού στον πληθυσμό της χώρας.

d) Χρήση Ιδιοκτησίας/Γης

Η παραδοσιακή εγγραφή γης ή ιδιοκτησίας είναι μια πολύ χρονοβόρα και δαπανηρή διαδικασία. Η τεχνολογία Blockchain μπορεί να εξαλείψει τα εμπόδια που σχετίζονται με αυτήν τη συμβατική διαδικασία, δημιουργώντας μια ψηφιακή διαδικασία αυτοματοποιημένης εγγραφής ιδιοκτησίας. Αυτή η λύση αυξάνει τη διαφάνεια και την εμπιστοσύνη εντός του συστήματος και βελτιώνει την οικονομία. Η νεότερη ανάπτυξη των έξυπνων πόλεων

συνδυάζει την τεχνολογία που βασίζεται σε Blockchain για μια σειρά διαδικασιών, όπως το κτηματολόγιο και το κτηματολόγιο, τη λήψη εγκρίσεων, τη δημιουργία αναφορών επιθεώρησης και την καταγραφή των πιστοποιητικών.

7.2.5 Προκλήσεις στον τομέα της Γεωργίας

a) Διατήρηση Αρχείων

Στη γεωργία, όλες οι πληροφορίες σχετικά με τα τρόφιμα, τους αγρότες, τις πληροφορίες πωλητών-αγοραστών είναι πολύ ξεπερασμένες και δεν είναι διαθέσιμες σε όλους τους χρήστες. Επομένως, είναι πολύ δύσκολο να επεξεργαστούμε τα δεδομένα και να κάνουμε ανάλυση αγοράς. Με τη χρήση του δικτύου Blockchain όλοι οι συμμετέχοντες έχουν πρόσβαση σε όλα τα αρχεία και τις συναλλαγές με αξιόπιστο και ασφαλή τρόπο.

b) Ιχνηλασιμότητα/Διαφάνεια

Η δεύτερη ανοιχτή πρόκληση στη γεωργία είναι η ιχνηλασιμότητα, η οποία εστιάζεται στην προέλευση των τροφίμων και την ποιότητά τους. Όμως, είναι πολύ δύσκολο να βρεις αυθεντικά και γνήσια προϊόντα ή τρόφιμα στην αλυσίδα εφοδιασμού. Το σύστημα παρακολούθησης αισθητήρων που βασίζεται σε Blockchain είναι μια βιώσιμη πιθανή λύση για την εξάλειψη του προαναφερθέντος ζητήματος.

c) Κόστος Συναλλαγής και πρόσβαση στην αγορά

Μερικές φορές οι αγρότες μικρής κλίμακας δεν έχουν πρόσβαση στο σύνολο της αγοράς στη γεωργία. Έτσι, οι αγρότες συμβιβάστηκαν με υψηλότερο κόστος με περιορισμένη πρόσβαση στην αγορά. Με τη βοήθεια της τεχνολογίας κατανεμημένου καθολικού δικτύου Blockchain, όλα τα δεδομένα είναι διαθέσιμα και έχουν εύκολη πρόσβαση σε κάθε αγορά του δικτύου, κάτι που βοηθά όλους τους αγρότες να συνδεθούν με την αγορά και επίσης να χτίσουν εμπιστοσύνη.

7.2.6 Προκλήσεις στον τομέα της Εφοδιαστικής Αλυσίδας

a) Πλαστογραφία

Στην σημερινή εποχή, κάθε βιομηχανία έχει ζητήματα παραποίησης προϊόντων και φαρμάκων. Αυτό δημιουργεί ζητήματα όπως η κακή ικανοποίηση των πελατών με την ποιότητα, τα μη επαληθεύσιμα προϊόντα ή τα πλαστά προϊόντα. Όλα αυτά κάνουν τη συνολική εμπιστοσύνη και τη φήμη των εταιρειών ή των κατασκευαστών να πέφτει. Η τεχνολογία Blockchain μειώνει την απόσταση μεταξύ πελατών και εταιρειών και κάνει τις διαδικασίες πιο διαφανείς. Αποθηκεύει το ιστορικό παρακολούθησης από παραβιάσεις των προϊόντων, γεγονός που καθιστά δύσκολη την παραποίηση των προϊόντων.

b) Αυθεντικότητα

Στον σημερινό κόσμο, οι χρήστες βασίζονται στα έγγραφα για να ελέγξουν την εγκυρότητα και την πρωτοτυπία των προϊόντων ή των υπηρεσιών. Αλλά τέτοια έγγραφα μπορούν εύκολα να μετριαστούν. Η τεχνολογία Blockchain παρέχει έναν ασφαλή τρόπο διατήρησης των πληροφοριών σχετικά με την αλυσίδα εφοδιασμού για την αποφυγή κάθε είδους τροποποίησης ή παραβίασης δεδομένων. Αυτή η τεχνολογία δίνει τη δυνατότητα στους πελάτες και τους προμηθευτές να εντοπίσουν την προέλευση καθώς και τις κινήσεις των προϊόντων. Με τη χρήση ετικετών RFID που είναι προσαρτημένες στα οχήματα, καθίσταται δυνατός ο εντοπισμός των προϊόντων μαζί με τις χρονικές σημάνσεις.

c) Παρακολούθηση προέλευσης

Κάθε κλάδος και εταιρεία έχει εξαρτήσεις από τις εφοδιαστικές αλυσίδες. Είναι πολύ δύσκολο να παρακολουθείτε κάθε ρεκόρ σε διαμετακόμιση ακόμη και σε πολυεθνικές εταιρείες. Η ανάγκη για διαφάνεια οδηγεί σε αυξημένο κόστος και ζητήματα σχέσεων με τους πελάτες που μπορεί να αποδυναμώσουν την αξία της επωνυμίας ή της εταιρείας. Μια αλυσίδα εφοδιασμού που βασίζεται σε Blockchain μπορεί να διατηρεί εύκολα όλα τα απαραίτητα αρχεία και τις λεπτομέρειες παρακολούθησης με τη βοήθεια των ενσωματωμένων αισθητήρων. Αυτό το είδος ακριβούς παρακολούθησης μπορεί να βοηθήσει στον εντοπισμό οποιασδήποτε απάτης που συμβαίνει οπουδήποτε στην αλυσίδα εφοδιασμού.

d) Αποτελεσματικότητα

Αν και οι σύγχρονες αλυσίδες εφοδιασμού μπορούν να χειριστούν την πολυπλοκότητα των διαδικασιών παραγωγής, εξακολουθούν να είναι εξαιρετικά αργές, ακριβές και αναποτελεσματικές. Όταν κάθε προμηθευτής και κατασκευαστής έχει τη δική του υποδομή, η παρακολούθηση των προϊόντων σε πραγματικό χρόνο είναι δύσκολη σε ένα κατακερματισμένο σύστημα. Οι καθυστερήσεις παράδοσης προϊόντων προκαλούνται συνήθως από την έλλειψη πρόσβασης σε ενημερωμένα δεδομένα. Αυτό μπορεί να μετριαστεί χρησιμοποιώντας την τεχνολογία Blockchain, η οποία αυξάνει την αποτελεσματικότητα της εφοδιαστικής αλυσίδας ενώ επιταχύνει τον χρόνο για την αγορά.

Κεφάλαιο 8ο Blockchain Applications

Σε προηγούμενα κεφάλαια, εξερευνήσαμε τι είναι το Blockchain, πώς λειτουργεί και γιατί είναι σημαντικό. Σε αυτό το κεφάλαιο θα καταλάβουμε πώς η βιομηχανία προσαρμόζει γρήγορα την τεχνολογία Blockchain, όπως διερευνήθηκε νωρίτερα ότι η τεχνολογία Blockchain είναι πολύ μεγαλύτερη από έναν απλό τομέα πληρωμών και χρηματοδότησης.

Ως εκ τούτου, αυτό το κεφάλαιο θα καλύψει τις πιθανές χρήσεις του Blockchain με παραδείγματα για την κατασκευή συστημάτων που βασίζονται σε Blockchain, για να δείξει πώς έχει τις δυνατότητες να αγγίξει σχεδόν κάθε κλάδο στον κόσμο.

8.1 Μελέτη περίπτωσης: Αγορά μιας κούπας καφέ

Ας ξεκινήσουμε με ένα απλό παράδειγμα του πώς η πρώτη εφαρμογή Blockchain που είναι το Bitcoin θα προσαρμοστεί ως επιλογή σε ένα σύστημα σημείων πώλησης. Ο Κ θα κάνει την πρώτη του λιανική συναλλαγή, αγοράζοντας ένα φλιτζάνι καφέ στο συνοικιακό μαγαζί Χ.

Το συγκεκριμένο καφέ άρχισε πρόσφατα να δέχεται το Bitcoin ως νέα μέθοδο πληρωμής προσθέτοντας μια επιλογή Bitcoin στο σύστημα σημείων πώλησης. Οι τιμές στο Cafe αναγράφονται σε ευρώ, αλλά οι πελάτες έχουν πλέον τη δυνατότητα να πληρώσουν είτε σε ευρώ είτε σε Bitcoin. Ο Κ δίνει την παραγγελία του για ένα φλιτζάνι καφέ και στο ταμείο, το σύστημα σημείων πώλησης μετατρέπει αυτόματα τη συνολική τιμή από ευρώ σε Bitcoin με τη σημερινή ισοτιμία της αγοράς και εμφανίζει την τιμή και στα δύο νομίσματα:

Πχ:
1.80€ καφές > 0,000065 BTC

Η διαδικασία που ακολουθείται είναι η εξής. Αρχικά, αν ο Κ ζητά να αγοράσει τον καφέ με Bitcoin, αυτομάτως η συναλλαγή αποκτά ένα εξατομικευμένο QR Code το οποίο το σκανάρει με το κινητό του.

Στο QR κωδικό βρίσκονται η διεύθυνση του Bitcoin, το ποσό (0,000065 BTC), το όνομα της καφετέριας και ο λόγος πληρωμής.

Στη συνέχεια ο Κ χρησιμοποιεί την εφαρμογή του Bitcoin Wallet που είναι εγκατεστημένη στο smartphone του για να σαρώσει τον γραμμικό κώδικα που εμφανίζεται. Θα εμφανιστεί μια πληρωμή 0,000065 BTC στο Καφέ Χ και επιλέγει ΑΠΟΣΤΟΛΗ για να εξουσιοδοτήσει την πληρωμή μέσα σε λίγα δευτερόλεπτα, ο ταμίας βλέπει τη συναλλαγή στο σύστημα και ολοκληρώνει την πληρωμή.

Αυτή η συναλλαγή είναι μια πληρωμή peer-to-peer που πηγαίνει απευθείας από τον λογαριασμό του Κ στο λογαριασμό της καφετέριας χωρίς να πηγαίνει σε τρίτους όπως τράπεζες. Αυτό το απλό παράδειγμα δείχνει πώς η πρώτη εφαρμογή Blockchain (Bitcoin) θα επηρεάσει τον χρηματοοικονομικό τομέα επιτρέποντας τέτοιες άμεσες πληρωμή χωρίς τραπεζικά συστήματα [16].

8.2 Μελέτη Περίπτωσης: Διαχείριση Δημόσιας Ταυτότητας

Η διαχείριση δημόσιας ταυτότητας είναι μία από τις πιθανές εφαρμογές που χρησιμοποιεί την τεχνολογία Blockchain [73]. Αυτή η βασική καινοτομία θα μπορούσε να ανοίξει το δρόμο για την επίλυση των προβλημάτων ασφάλειας της ταυτότητας και να γίνει η βάση άλλων βιομηχανιών. Φανταστείτε αν όλοι μπορούν να εμπιστεύονται τον καθένα για αυτό που ισχυρίζονται ότι είναι, τότε μπορούν να συνδεθούν μεταξύ τους για μια σειρά από άλλες εφαρμογές.

Η τεχνολογία Blockchain λύνει πολλά υπάρχοντα προβλήματα με τις ψηφιακές ταυτότητες. Επί του παρόντος, είναι σχετικά πιο εύκολο να δημιουργήσετε πλαστές ταυτότητες ή να κλέψετε την ταυτότητα κάποιου άλλου στο διαδίκτυο. Όπου, οι κωδικοί πρόσβασης δεν είναι ασφαλείς και οι κεντρικές βάσεις δεδομένων είναι ευάλωτες σε επιθέσεις. Όταν μια κεντρική βάση δεδομένων δέχεται επίθεση, μπορεί να παρέχει πρόσβαση σε όλα τα δεδομένα πελατών που είναι αποθηκευμένα στο σύστημα.

Επιπρόσθετα, τα συστήματα αναγνώρισης που βασίζονται σε Blockchain τεχνολογία παρέχουν ψηφιακές υπογραφές χρησιμοποιώντας κρυπτογραφία. Είναι μοναδικά, αδιαμφισβήτητα,

ασφαλή και σχεδόν αδύνατο να αντιγραφούν ή να προσπελαστούν χωρίς εξουσιοδότηση. Η ταυτοποίηση με βάση το Blockchain είναι πραγματική δυνατότητα στο μέλλον με τις κυβερνήσεις ήδη να κατασκευάζουν συστήματα ταυτότητας πάνω στο Blockchain.

Στο μέλλον, αυτό θα μπορούσε να χρησιμοποιηθεί για ψηφιακές ταυτότητες, διαβατήρια, άδειες οδήγησης, άδειες διαμονής, πιστοποιητικά γέννησης, πιστοποιητικά γάμου και άλλες μορφές ταυτοποίησης.

8.3 Μελέτη Περίπτωσης: Ακαδημαϊκό Πιστοποιητικό

«Το Blockchain είναι το μέλλον της πιστοποίησης και πιστεύουμε ότι τα επόμενα χρόνια, περισσότερα σχολεία θα χρησιμοποιήσουν το δημόσιο Blockchain για να εξασφαλίσουν τα πιστοποιητικά και τα πτυχία τους. Είναι αποτελεσματικότερο, ασφαλέστερο και απλούστερο από αυτό που μπορείτε να βρείτε σήμερα στον κλάδο».
Sylvain Kalache, Holberton School Co-Founder

Σήμερα, μέσω της τεχνολογίας Blockchain, είναι δυνατή η αποθήκευση των ακαδημαϊκών πιστοποιητικών και άλλων σημαντικών εγγράφων ως ψηφιακά πιστοποιητικά που είναι υπογεγραμμένα κρυπτογραφικά.
Η κοινή χρήση τους με τους εργοδότες ή άλλες αρχές σε περίπτωση πρόσληψης ή άλλων διαδικασιών αποδοχής γίνεται διαφανής και εύκολη. Αυτό το αμετάβλητο τεχνολογικό θαύμα απαιτεί από τις εκδίδουσες αρχές να δημοσιεύουν τα ψηφιακά πιστοποιητικά των μαθητών σε ένα δίκτυο Blockchain. Αποθηκεύονται ως μονόδρομη κωδικοποίηση κατακερματισμού. Κάθε φορά που ένας οργανισμός ή ένας εργοδότης ζητά αντίγραφο από τον υποψήφιο υπάλληλο, τα εκπαιδευτικά ιδρύματα ή το Πανεπιστήμιο στέλνουν τα ακαδημαϊκά διαπιστευτήρια ή έγγραφα μέσω Blockchain στον φοιτητή και σε αυτήν την περίπτωση, ο φοιτητής πρέπει να στείλει το δημόσιο κλειδί στον αντίστοιχο ακαδημαϊκό του ιδρύματα από τα οποία είχαν ολοκληρώσει τις σπουδές τους. Ο φοιτητής που υποβάλλει αίτηση για εργασία σε έναν οργανισμό μοιράζεται το ψηφιακό αντίγραφο των ακαδημαϊκών του διαπιστευτηρίων με τον υποψήφιο εργοδότη .

Επιπλέον, προς αυτή την κατεύθυνση, το Πανεπιστήμιο της Λευκωσίας ανακοίνωσε επίσημα ότι έχει εκδώσει τα πρώτα ακαδημαϊκά πιστοποιητικά των οποίων η αυθεντικότητα μπορεί να επαληθευτεί μέσω του Bitcoin Blockchain. Εν τω μεταξύ, το Πανεπιστήμιο του MIT

ανακοίνωσε το Έργο Ψηφιακών Πιστοποιητικών [21.1]. Το οποίο είναι ένα έργο επώασης από το Media Lab Learning Initiative and Learning Machine που δημιουργεί ένα οικοσύστημα για τη δημιουργία, την κοινή χρήση και την επαλήθευση εκπαιδευτικών πιστοποιητικών που βασίζονται σε Blockchain. Τα ψηφιακά πιστοποιητικά καταχωρούνται στο Blockchain του Bitcoin, υπογράφονται κρυπτογραφικά και προστατεύονται από παραβιάσεις.

Η παραποίηση ακαδημαϊκών μετεγγραφών και πιστοποιητικών είναι μια κοινή πρακτική με τους μαθητές που ισχυρίζονται ότι δεν απέκτησαν προσόντα. Το Blockchain θα δημιουργήσει διαφάνεια σχετικά με τα ακαδημαϊκά αρχεία και τα προσόντα των μαθητών. Επιτρέποντάς τους να επαληθεύονται εύκολα, εξαλείφοντας την απάτη εξοικονομώντας χρόνο και χρήμα για τον χειροκίνητο έλεγχο ή την απόδειξη των προσόντων.

8.4 Μελέτη Περίπτωσης: Εκλογικό Σύστημα

«Σε μια εποχή όπου τα όργανα διαχείρισης των εκλογών αγωνίζονται να προωθήσουν τη συμμετοχή των πολιτών με ένα ολοένα και πιο ευέλικτο και διασκορπισμένο εκλογικό σώμα, είναι σημαντικό να δοθούν στους ψηφοφόρους ασφαλείς και προσβάσιμες εναλλακτικές λύσεις για να συμμετάσχουν στη δημοκρατία».
Mike Summers, Διευθυντής της Smartmatic-Cybernetica
Κέντρο Αριστείας για Ψηφοφορία στο Διαδίκτυο (SCCEIV) [21.2]

Όπως εξηγείται σε προηγούμενο κεφάλαιο, η οικοδόμηση τεχνολογίας που επιτρέπει ψηφιακές ταυτότητες και ψηφιακές υπογραφές, θα διευκολύνει τη διαδικασία πιστοποίησης της ταυτότητας κάποιου για μια σειρά άλλων συναλλαγών και ενεργειών στο διαδίκτυο.

Συγκεκριμένα, η ψηφιακή ψηφοφορία είναι μια τεχνολογία που απέτυχε να εφαρμοστεί με επιτυχία σε όλες τις χώρες, λόγω κινδύνων ασφαλείας και ανησυχιών σχετικά με το απόρρητο. Η Εσθονία [21.3], η Δανία και η Νορβηγία έχουν πειραματιστεί με την ψηφιακή ψηφοφορία [21.2]. Ωστόσο, η Εσθονία έχει εφαρμόσει με επιτυχία ένα ψηφιακό σύστημα ψηφοφορίας μεγάλης κλίμακας. Η Δανία έχει χρησιμοποιήσει τεχνολογία Blockchain για ψηφοφορία μικρής κλίμακας με το Liberal Alliance, ένα πολιτικό κόμμα στη Δανία, χρησιμοποιώντας ένα σύστημα ψηφοφορίας Blockchain το 2014 [21.4]. Ενώ, στη Νορβηγία, η συμμετοχή στη

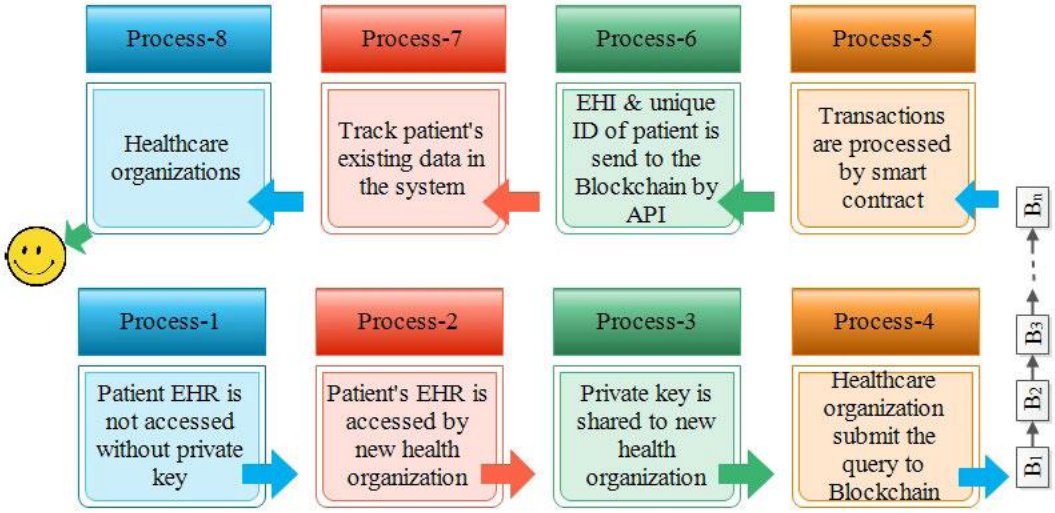
διαδικτυακή ψηφοφορία έφτασε το εντυπωσιακό 85,5 από τις 100 ψήφους κατά τη διάρκεια περιφερειακού δημοψηφίσματος που διεξήχθη στη Νορβηγία τον Μάιο του 2018.
Έτσι, χρησιμοποιώντας ένα σύστημα ψηφοφορίας βασισμένο σε Blockchain, ένας ψηφοφόρος μπορούσε να ελέγξει ότι η ψήφος του στάλθηκε με επιτυχία, ενώ εξακολουθούν να διατηρούν την ιδιωτικότητά τους και να κρύβουν την ταυτότητά τους. Θα έκανε επίσης την ψηφοφορία πιο προσιτή σε πολλά άτομα, αυξάνοντας ενδεχομένως τη συμμετοχή στις εκλογές.

8.5 Μελέτη Περίπτωσης: Ιατρικό Ιστορικό

Ένα από τα σημαντικά χαρακτηριστικά του Blockchain είναι ότι παρέχει ένα κατανεμημένο καθολικό, έτσι ώστε, όταν γίνονται αλλαγές σε ένα καθολικό, όλα τα άλλα αντίγραφα ενημερώνονται ταυτόχρονα. Αυτό διασφαλίζει ότι όλοι έχουν τα πιο πρόσφατα έγκυρα δεδομένα που ταιριάζουν με όλα τα αντίγραφα στο δίκτυο. Δίνει πολλές δυνατότητες να εφαρμοστεί στον κλάδο της υγείας. Εάν έχετε πάει ποτέ σε περισσότερους από έναν γιατρούς ή νοσοκομείο, θα γνωρίζετε ότι κάθε φορά που επισκέπτεστε έναν νέο γιατρό ή νοσοκομείο, περιλαμβάνει πολλή γραφειοκρατία σχετικά με το ιατρικό ιστορικό, τις αλλεργίες και άλλες ιατρικές ερωτήσεις που μπορεί να έχετε συμπληρώσει αρκετές φορές στο παρελθόν σε άλλες τοποθεσίες.

Πιο συγκεκριμένα, η αποθήκευση αυτών των πληροφοριών σε μια κοινή βάση δεδομένων με αρχεία υγείας σημαίνει ότι οι γιατροί, τα νοσοκομεία, οι χειρουργοί, οι νοσηλευτές και οι επαγγελματίες υγείας θα έχουν πρόσβαση σε κοινά δεδομένα σχετικά με έναν ασθενή. Θα είχαν τις πλήρεις λεπτομέρειες των ιατρικών αρχείων, εξοικονομώντας χρόνο και βοηθώντας τους να λαμβάνουν πιο ολοκληρωμένες αποφάσεις κατά τη θεραπεία ενός ασθενούς. Αυτό θα μπορούσε να σώσει τη ζωή σε περίπτωση που ένας ασθενής μεταφερθεί εσπευσμένα σε καταστάσεις έκτακτης ανάγκης. Τα αρχεία για τυχόν υποκείμενα ζητήματα υγείας, ομάδα αίματος, αλλεργίες σε ορισμένα φάρμακα, επαφές έκτακτης ανάγκης, τρέχοντα φάρμακα που μπορεί να λαμβάνουν ή άλλες λεπτομέρειες θα είναι άμεσα προσβάσιμα, όταν απαιτείται. Οι λεπτομέρειες του προηγούμενου ιστορικού ασθένειας ενός ασθενούς θα βοηθούσαν επίσης να συμπληρωθεί το παζλ του τι μπορεί να προκαλεί προβλήματα υγείας σε έναν ασθενή. Μια επίσκεψη σε γιατρό για μια πάθηση μπορεί να μην προκαλεί συναγερμό, αλλά όταν συνδυάζεται με μια επίσκεψη σε άλλο γιατρό ή επαγγελματία υγείας για μια φαινομενικά άσχετη πάθηση μπορεί να σηματοδοτήσει τα συμπτώματα ενός ακόμη αδιάγνωστου

προβλήματος. Κάθε επαγγελματίας υγείας μπορεί να έχει ακούσει μόνο ένα από τα συμπτώματα, παρέχοντάς του έτσι μόνο ένα μέρος της εικόνας. Αλλά με τις πρόσθετες πληροφορίες, μπορούν να διαγνώσουν καλύτερα τον ασθενή [21.5].



Εικόνα 23 Διαδικασίες μελέτης ιατρικού ιστορικού

Τέλος, οι εταιρείες ασφάλισης υγείας θα μπορούσαν να εξοικονομήσουν σημαντικά χρηματικά ποσά και χρόνο έχοντας επίσης πρόσβαση σε αυτή τη βάση δεδομένων. Εάν κάνετε αίτηση για ασφάλιση υγείας, προς το παρόν αυτό απαιτεί πολλές ερωτήσεις και ιατρικές εξετάσεις που μπορεί να είναι αρκετά επεμβατικές, χρονοβόρες και άβολες. Παρέχοντας πρόσβαση στα αρχεία υγείας σας σε έναν ασφαλιστή, θα έχει μια πλήρη εικόνα του ιστορικού της υγείας σας και θα είναι σε θέση να κάνει ασφαλιστικές αποφάσεις που βασίζονται σε αυτές τις πληροφορίες χωρίς να χρειάζονται εκτενείς δοκιμές και ερωτήσεις. Απλώς, το Blockchain [73] θα προσφέρει μια θεραπεία για τα κατακερματισμένα ιατρικά αρχεία των ασθενών.

Τα παραπάνω παραδείγματα εφαρμογών σε αυτό το κεφάλαιο δείχνουν ότι η τεχνολογία Blockchain [26] μπορεί να είναι η επόμενη μεγάλη καινοτομία σε μια σειρά βιομηχανιών. Αυτά τα παραδείγματα είναι ακριβώς όπως η κορυφή ενός παγόβουνου όσον αφορά το τι είναι ικανό το Blockchain [73]. Ωστόσο, η βασική εφαρμογή μεταξύ όλων των πιθανών εφαρμογών είναι το "Smart Contract" [12,13], καθώς οι περισσότερες από τις εφαρμογές που βασίζονται σε Blockchain θα διαχειρίζονται με έξυπνο συμβόλαιο.

Συμπεράσματα

Το Blockchain είναι μια αναδυόμενη τεχνολογία. Κατά τη γνώμη μου, είναι σε παρόμοιο επίπεδο ωριμότητας όπως ήταν το Διαδίκτυο στην πρώτη του ηλικία. Τότε, ήταν σαφές ότι το Διαδίκτυο είχε τη δυνατότητα να αλλάξει σχεδόν κάθε πτυχή της ανθρώπινης ζωής και των επιχειρήσεων σε όλο τον κόσμο, αλλά χρειάστηκε χρόνος για να ωριμάσει η τεχνολογία και να επιτύχει ευρεία υιοθέτηση και αντίκτυπο.

Σε αυτή τη εργασία πραγματοποιήθηκε μια έρευνα βασισμένη σε βιβλιογραφική ανασκόπηση του Blockchain, η οποία περιλαμβάνει αναλύσεις των αρχών, των πλεονεκτημάτων, των προκλήσεων και του τρόπου λειτουργίας της τεχνολογίας. Επίσης, σε αυτή την εργασία ορίστηκε και συζητήθηκε το ιστορικό υπόβαθρο του Blockchain, καθώς αυτή η ιστορική έρευνα θα επιτρέψει την κατανόηση του θέματος με σαφήνεια και θα προσφέρει μια σταθερή βάση για καλύτερη κατανόηση και περαιτέρω έρευνα. Ακόμα μελετήθηκε η σχέση του Ψηφιακού Μάρκετινγκ με την τεχνολογία Blockchain και πως εφαρμόζεται στην πράξη. Τέλος, η έννοια του έξυπνου συμβολαίου αναλύθηκε λεπτομερώς ως μία από τις πιθανές μελλοντικές κατευθύνσεις για την τεχνολογία Blockchain.

Σύμφωνα με τα ευρήματα, το Blockchain μπορεί να χρησιμοποιηθεί για κάτι περισσότερο από χρηματοοικονομικές υπηρεσίες και να παρέχει λύσεις σε διάφορα ζητήματα, ιδιαίτερα σε εμπόδια και προκλήσεις που σχετίζονται με την εμπιστοσύνη και την ασφάλεια. Η τεχνολογία έχει τεράστιες δυνατότητες ανάπτυξης και εφαρμογής ανάλογα με την περιοχή εφαρμογής της. Μακροπρόθεσμα, πιστεύουμε για την ευρεία υιοθέτηση και χρήση αυτής της τεχνολογίας. Ωστόσο, το πεδίο χρειάζεται περαιτέρω έρευνα για την αξιοποίηση του πλήρους δυναμικού τέτοιων προηγμένων τεχνολογιών όπως το Blockchain και τα έξυπνα συμβόλαια.

Βιβλιογραφία

Ιστοσελίδες

1. EthereumTeam, (2018) Ethereum Blockchain App Platform
   https:// https://ethereum.org/en//

2. Kashyap Sahil, (2020) How Blockchain affects digital marketing?
   https://yourstory.com/mystory/Blockchain-affect-digital-marketing/amp

3. Mailchimp, Digital Marketing
   https://mailchimp.com/marketing-glossary/digital-marketing/

4. IntelegainTeam, (2018) Bitcoin and Blockchain Technology: How do they Work?
   https://www.intelegain.com/bitcoin-and-Blockchain-technology/

5. R. Kastelein. ODI's Dr. James Smith, (2016) 'Undefined Radically Distributed Storage Technology'.
   https://www.the-Blockchain.com/2016/01/12/james-smith-data-infrastructure-technology-are-Blockchains-theanswer/

6. A. Lewis, (2015) Thoughts on Blockchain technology.
   https://bitsonblocks.net/2015/09/09/a- gentle- introduction- to- Blockchaintechnology/

7. DocuSignTeam, (2018) what are digital signatures?
   https://www.docusign.com uk / how - it - works / electronic - signature / digital - signature / digitalsignature-faq.

8. BlockgeeksTeam, (2016) Cryptocurrency Wallet Guide: A Step-By-Step Tutorial.
   https://blockgeeks.com/guides/cryptocurrency-wallet-guide/

9. Sphereofficial-Team, (2017) How The Blockchain Works - Infographic.
   https://steemkr.com/Blockchain/@sphereofficial/how-he-Blockchain-works-infographic

10. S. Mathieson, (2017) Blockchain starts to prove its value outside of finance.
    https://www.computerweekly.com/feature/Blockchain-starts-to-prove-itsvalue-outside-of-finance

11. T. Macaulay, (2016) Blockchain limitations: Is the distributed ledger technology overhyped?
    https://www.techworld.com/startups/what-are-limitations-ofBlockchain-experts-from-odi-explain-3648881/

12. RSK-Team, (2018) What is Smart Contract?
    https://faq.rsk.co/en/main/.

13. J. Stark, (2016) Making Sense of Blockchain Smart Contracts
    https://vimeo.com/168844103

14. T. Hingley, (2016) A smart new world: Blockchain and smart contracts. https://www.freshfields.com/en- gb/our- thinking/campaigns/digital/fintech/Blockchain-and-smart-contracts

15. BlockgeeksTeam, (2016) Smart Contracts: The Blockchain Technology That Will Replace Lawyers. https://blockgeeks.com/guides/smart-contracts/

16. StateOfTheDApps, (2018) DApp Statistics https://www.stateofthedapps.com/stats.

17. Orlovsky a, (2017) Awesome Smart Contracts https://github.com/Overtorment/awesome-smart-contracts

18. Mulders, (2018) Comparison of Smart Contract Platforms. https://hackernoon.com

19. SMathieson (2017) Blockchain starts to prove its value outside of finance. https://www.computerweekly.com/feature/Blockchain-starts-to-prove-itsvalue-outside-of-finance

20. Macaulay, (2016) Blockchain limitations: Is the distributed ledger technology overhyped? https://www.techworld.com/startups/what-are-limitations-ofBlockchain-experts-from-odi-explain-3648881/

21. Ehrsam, (2018) Blockchain Quotes. https://www.brainyquote.com/quotes/fred_ehrsam_850313

21.1. MITUniversityTeam, (2018) Digital Certificates Project http://certificates.media.mit.edu/home

21.2. SmartMaticTeam, (2018) online-voting-participation-reaches-85-during-referendum-in-norway http : / / www . smartmatic . com / news / article / online - voting -participation-reaches-85-during-referendum-in-norway/.

21.3. G. Estonian, (2018) Estonian Government Offical Website i-voting. https://eestonia.com/solutions/e-governance/i-voting/.

21.4. Tech4PartiesTeam, (2018) *Denmark Liberal Alliance - Blockchain Secure Online Voting* https://tech4parties.org/case- studies/denmark- liberal- allianceblockchain-secure-online-voting/.

21.5. A. Green, (2018) Blockchain offers cure for patients' fragmented medical records https://www.ft.com/content/6f138722-47d4-11e8-8c77-ff51caedcde6.

Βιβλιογραφία- Άρθρα

22. S. Seebacher and R. Schüritz. (2017), “Blockchain technology as an enabler of service systems: A structured literature review”. In: International Conference on Exploring Services Science. Springer

23. S. Nakamoto (2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”

24. M. Antonopoulos.(2017), Mastering Bitcoin: Programming the Open Blockchain. O’Reilly Media, Inc

25. L. Lamport, R. Shostak, and M. Peas (1982).e. “The Byzantine generals problem”. ACM Transactions on Programming Languages and Systems (TOPLAS)

26. Savelyev (2017), “Contract law 2.0:‘Smart’contracts as the beginning of the end of classic contract law”. Information & Communications Technology Law 26.2

27. M. Andrychowicz (2014), “Secure multiparty computations on bitcoin”. In: Security and Privacy (SP), 2014 IEEE Symposium on. IEEE.

28. H. Bentov and R. Kumaresan. (2014), “How to use bitcoin to design fair protocols”. In: International Cryptology Conference. Springer

29. CaresN (2016), “Robust, costeffective applications key to unlocking Blockchain’s potential credit benefits”. Moody’s Investor Service

30. Porru (2016) , “Blockchain-oriented software engineering: challenges and new directions”. In: Proceedings of the 39th International Conference on Software Engineering Companion. IEEE Press

31. Bigi (2016), “Validation of decentralised smart contracts through game theory and formal methods”. In: Programming Languages with Applications to Biology and Security. USA,Springer

32. Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, (2017) ``Introducing Blockchains for healthcare," in Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)

33. H. Johng, D. Kim, T. Hill, and L. Chung,(2017) ``Using Blockchain to enhance the trustworthiness of business processes: A goal-oriented approach,:, Proc. IEEE Int. Conf. Services Comput

34. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, (2019)``A survey on privacy protection in Blockchain system," J. Netw. Comput.

35. G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, (2019)``Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," Comput.

36. V. J. Morkunas, J. Paschen, and E. Boon, (2019)``How Blockchain technologies impact your business model," Bus. Horizons,

37. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, (2018)``Blockchain for business applications: A systematic literature review," in Business Information Systems. BIS (Lecture Notes in Business Information Processing), vol. 320, W. Abramowicz and A. Paschke, Eds. Cham, Switzerland: Springer

38. N. Mohamed and J. Al-Jaroodi, (2019)``Applying Blockchain in industry 4.0 applications," in Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)

39. Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustisek, (2019)``Towards decentralized IoT security enhancement: A Blockchain approach," Comput. Electr. Eng.

40. J. Katz , (1996) et al. Handbook of applied cryptography. CRC press

41. J. Katz (1996) et al. Handbook of applied cryptography. CRC press

42. M. Swan (2015) Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

43. V. Morabito. (2017) "Business Innovation Through Blockchain". Cham: SpringerInternational Publishing

44. M. Francisconi. "An explorative study on blockchain technology in application to port logistics". MA thesis. 2017

45. D. Drescher (2017), Blockchain basics. Springer

46. S. Ølnes, J. Ubacht, and M. Janssen. (2017). "Blockchain in government: Benefits and impli-cations of distributed ledger technology for information sharing."

47. S. Bilonia. (2017) How does Bitcoin Blockchain work and what are the rules behind it?

48. J. Bergquist. (2017) "Blockchain Technology and Smart Contracts: Privacy-preserving Tools". MA thesis

49. S. Kikitamara, M. van Eekelen, and D. I. J.-P. Doomernik. (2017) "Digital Identity Management on Blockchain for Open Model Energy System". MA thesis.

50. G. Greenspan. (2016) "Beware of the Impossible Smart Contract"

51. D. Tapscott and A. Tapscott. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

52. K. Delmolino (2016) et al. “Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab”. In: International Conference on Financial Cryptography and Data Security. Springer.

53. G. Gambhire, T. Gujar, and S. Pathak, (2018) ``Business potential and impact of industry 4.0 in manufacturing organizations," in Proc. 4th Int. Conf. Comput.Commun. Control Autom. (ICCUBEA)

54. P. Fraga-Lamas and T. M. Fernandez-Caramess, ``A review on Blockchain technologies for an advanced and cyber-resilient automotive industry, "IEEE Access

55. I. Makhdoom, M. Abolhasan, H. Abbas, andW. Ni, ``Blockchain's adoption in IoT: The challenges, and a way forward,"

56. U. Bodkhe, J. Chaklasiya, P. Shah, S. Tanwar, and M. Vora, ``Markov model for password attack prevention," in Proc. 1st Int. Conf. Comput., Commun., Cyber-Secur.

57. M. Holland, J. Stjepandic, and C. Nigischer, (2018) ``Intellectual property protection of 3D print supply chain with blockchain technology," in Proc. IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC)

58. U. Bodkhe and S. Tanwar, ``Secure data dissemination techniques for IoT applications: Research challenges and opportunities,"

59. M. M. Queiroz and S. F. Wamba, ``Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India andthe USA,"

60. F. Tian, ``A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things,"

61. M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, ``Blockchain based traceability in agri-food supply chain management: A practical implementation,"

62. G. Perboli, S. Musso, and M. Rosano, ``Blockchain in logistics and supply chain: A lean approach for designing real-world use cases,"

63. N. M. Kumar, ``Blockchain: Enabling wide range of services in distributed energy system,"

64. J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, ``The blockchain-based digital content distribution system,"

65. A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. Maasberg, andK.-K.-R. Choo, ``Multimedia big data computing and Internet of Things applications: A taxonomy and process model,"

66. S. Li, ``Application of blockchain technology in smart city infrastructure," in Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT),

67. S. Tanwar, S. Tanwar, L. M. Goya, M. Mittal, and B. Agarwal, Energy Conservation for IoT Devices: Concepts, Paradigms

68. M. Samaniego and R. Deters, ``Hosting virtual IoT resources on edgehosts with blockchain,"

69. M. A. Khan and K. Salah, ``IoT security: Review, blockchain solutions, and open challenges,"

70. J. Hua, X. Wang, M. Kang, H. Wang, and F.-Y. Wang, ``Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping,"

71. Y. M. Qin, D. L. Kong, and S. Li, ``China cold-chain logistics development report,"

72. P. Boucer, ``How blockchain technology could change our lives,"

73. M. Gates. Blockchain (2017), Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. CreateSpace Independent Publishing Platform