ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τεχνολογία Blockchain και έξυπνα συμβόλαια

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεννάδη Ολυμπία

Επιβλέπων : Στεφανέας Πέτρος
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2020

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τεχνολογία Blockchain και έξυπνα συμβόλαια

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεννάδη Ολυμπία

Επιβλέπων : Στεφανέας Πέτρος
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 8η Ιουλίου 2020

……..	……..	……...
Στεφανέας Πέτρος	Καρώνη Χρυσηίς	Κουκουβίνος Χρήστος
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

……

Γεννάδη Ολυμπία

Διπλωματούχος Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών Ε.Μ.Π.

Περίληψη

Η παρούσα διπλωματική εργασία έχει ως στόχο την ανάδειξη καινοτόμων μεθόδων και συγκεκριμένα τη μελέτη της τεχνολογίας Blockchain, η οποία γίνεται όλο και περισσότερο δημοφιλής στο χώρο της κρυπτογραφίας και παράλληλα αναπτύσσεται και εφαρμόζεται σε διάφορους επιχειρηματικούς τομείς. Στην εποχή των παγκόσμιων ηλεκτρονικών επικοινωνιών, η έννοια της ασφάλειας αποκτά ζωτική σημασία. Για το λόγο αυτό, η ανάγκη για την εξέλιξη της επιστήμης της κρυπτογραφίας συνεχώς αυξάνεται.

Αρχικά παρουσιάζεται ο ορισμός του Blockchain, ενώ γίνεται μελέτη γύρω από την αρχιτεκτονική του και τα πλεονεκτήματα που προσφέρει. Οδηγός στην ανάλυση αυτή, αποτελεί το σύνολο των θεμελιωδών εννοιών της κρυπτογραφίας που αναπτύσσονται στο τρίτο κεφάλαιο. Οι παραλλαγές που μπορεί να λάβει ο μηχανισμός του Blockchain ως προς τη δομή του δικτύου και τα πρωτόκολλά του, καλύπτουν ένα ευρύ φάσμα και αρκετές από αυτές αναγράφονται στην παρούσα εργασία. Επιπλέον, αναφέρονται εφαρμογές της τεχνολογίας οι οποίες πλέον χρησιμοποιούνται σε μεγάλο βαθμό.

Κύριος σκοπός είναι η υπογράμμιση της σημασίας που έχει η εφαρμογή του συγκεκριμένου μηχανισμού στον κλάδο της υγείας και η παρουσίαση των οφειλών του. Είναι γνωστό πως οι ηλεκτρονικοί ιατρικοί φάκελοι και τα δεδομένα που εμπεριέχουν γίνονται αντικείμενο πόθου από κακόβουλους χρήστες υπολογιστών αλλά και από βιομηχανίες οι οποίες ψάχνουν τρόπους να προβούν στο ιδιοτελές κέρδος. Επομένως η προφύλαξή τους αποκτά ισχυρό νόημα. Ταυτόχρονα η αξιοποίηση της τεχνολογίας Blockchain και των έξυπνων συμβολαίων, ενδυναμώνει τον τρόπο λειτουργίας του συστήματος υγείας, δημιουργώντας έναν αποτελεσματικότερο τρόπο αντιμετώπισης των προβλημάτων που συναντάει η κοινωνία και η επιστημονική κοινότητα στον τομέα αυτό. Εν συνέχεια, αναλύεται ένα μοντέλο που συνδέει το Cloud Computing με το Blockchain χρησιμοποιώντας τα έξυπνα συμβόλαια. Το μοντέλο, θα μπορούσε να δώσει λύση στην ασφάλεια των ιατρικών ηλεκτρονικών φακέλων και την ανταλλαγή τους, αλλά και στον μεγάλο όγκο δεδομένων που συσσωρεύεται στα συστήματα.

Τέλος, πραγματοποιείται μία σύντομη ανασκόπηση στα συμπεράσματα της εργασίας και εξετάζονται οι μελλοντικές προοπτικές της τεχνολογίας Blockchain.

Λέξεις Κλειδιά

Κρυπτογραφία, Blockchain, Δομή, Λειτουργία, Εφαρμογές, Ιατρικά Δεδομένα, Διαμοιρασμός Δεδομένων, Cloud Computing, Έξυπνα Συμβόλαια, Μεγάλα Ιατρικά Δεδομένα

Abstract

The purpose of this diploma thesis is to highlight innovative methods and particularly Blockchain technology which is becoming increasingly popular in the field of cryptography and at the same time is being developed and applied in various business sectors. In the age of global digital communications, security is necessary for our personal data. For this reason, the need for the development of cryptography is constantly increasing.

Initially, the definition of Blockchain technology is presented while its structure and the advantages that offers are described. The fundamental concepts of cryptography which are described in the third chapter are important for the understanding of the analysis of Blockchain technology. The protocols and the network structures of Blockchain mechanism can cover a wide range and several of them are mentioned in this paper. Furthermore, technology applications of Blockchain technology that are now widely used are presented.

The main purpose is to emphasize the importance of the implementation of this mechanism in the health sector and the presentation of its benefits. It is well known that electronic health records and their data are being coveted by malicious computer users as well as by industries looking for ways to make a profit. Therefore, their protection is significant. At the same, the use of Blockchain technology enhances the health system and creates a more effective way to deal with the problems that society and scientific community are facing. Next, a model that combines Cloud Computing and Blockchain technology using Smart Contracts is described. This model could provide a solution to the security of medical electronic files and their exchange, but also to the large amount of data that accumulates in systems.

Finally, a review of the conclusions is carried out and the future prospects of Blockchain technology are examined.

Key Words

Cryptography, Blockchain, Structure, Function, Applications, Medical Data, Exchange of Data, Cloud Computing, Smart Contracts, Big Medical Data

Ευχαριστίες

Κλείνοντας τον κύκλο των προπτυχιακών μου σπουδών θα ήθελα να ευχαριστήσω όλους τους ανθρώπους του Εθνικού Μετσόβιου Πολυτεχνείου που συντέλεσαν στην αποκόμιση των γνώσεων μου. Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της συγκεκριμένης διπλωματικής εργασίας, τον κύριο Πέτρο Στεφανέα για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον αντικείμενο άλλα και για την πολύτιμη καθοδήγησή του κατά την εκπόνηση της εργασίας. Χωρίς την υποστήριξή του και την εμπιστοσύνη του το έργο μου θα ήταν δυσκολότερο.

Ακόμα, θα ήθελα να ευχαριστήσω τους κοντινούς μου ανθρώπους, τους φίλους μου και συμφοιτητές μου για τις εμπειρίες που μοιραστήκαμε όλο αυτό το διάστημα. Κυρίως όμως, χρωστάω ευγνωμοσύνη στη Δανάη, στη Ροδάνθη και στην Τίνα οι οποίες ήταν πάντα δίπλα μου από τα σχολικά χρόνια έως και σήμερα. Η στήριξή τους, η τρέλα τους, αλλά και η πίστη τους σε εμένα, μου έδιναν δύναμη να ανταπεξέλθω σε κάθε δυσκολία. Τις ευχαριστώ γιατί μαζί τους έχτισα τις πιο όμορφες στιγμές. Τέλος, ένα μεγάλο ευχαριστώ στην οικογένειά μου που παρά τις όσες διαφωνίες με έμαθε να στοχεύω ψηλά με τόλμη και θάρρος.

Περιεχόμενα

1

Εισαγωγή

Με τη ραγδαία εξέλιξη της κοινωνίας και της τεχνολογίας γεννιέται συνεχώς η ανάγκη για την εύρεση καινοτόμων ιδεών στο χώρο της κρυπτογραφίας. Μία από τις πιο επαναστατικές ιδέες στο χώρο αυτόν έρχεται να συναντήσει το χρηματοοικονομικό σύστημα και τον τομέα των οικονομικών συναλλαγών.

Η σημερινή ψηφιακή οικονομία βασίζεται στην εξάρτηση από μία τρίτη αξιόπιστη πηγή η οποία θα διασφαλίζει την ιδιωτικότητα και την ασφάλεια των ψηφιακών αρχείων. Όλες οι ηλεκτρονικές συναλλαγές ελέγχονται, όπως για παράδειγμα μία πιστοποιημένη αρχή που βεβαιώνει ότι ένα ψηφιακό πιστοποιητικό είναι αληθές ή μία υπηρεσία ηλεκτρονικού ταχυδρομείου που επαληθεύει ότι το mail έχει παραδοθεί. Με την εφεύρεση ενός νέου ψηφιακού τρόπου οργάνωσης αρχείων, καταρρίπτονται αυτοί οι δεσμοί εξάρτησης.

Το 2008 ο Satoshi Nakamoto δημιουργεί ένα νέο είδος ψηφιακού νομίσματος με το όνομα Bitcoin. Το Bitcoin είναι ένα peer-to-peer (P2P) σύστημα πληρωμών και ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα, για τη διαχείριση του οποίου χρησιμοποιούνται μέθοδοι κρυπτογραφίας. Με πιο απλά λόγια, είναι το πρώτο ψηφιακό νόμισμα το οποίο δεν υπάρχει σε φυσική μορφή χρημάτων. Οι τεχνικές μέθοδοι στις οποίες βασίζεται το Bitcoin, του προσδίδουν ένα μεγάλο πλεονέκτημα. Το γεγονός ότι δεν είναι αναγκαία η χρήση κάποιου διαμεσολαβητή για την ανταλλαγή του. Η παρέμβαση κάποιας κεντρικής τράπεζας όπως γίνεται στις "πραγματικές" χρηματαποστολές είναι πλέον περιττή με την εφεύρεση του. Επιπλέον, λόγω των κρυπτογραφικών αρχών που ακολουθεί, δεν ελέγχεται από καμία κυβέρνηση ή υπηρεσία. Η παραγωγή του εξαρτάται παρά μόνο από ένα δίκτυο ανθρώπων που το χρησιμοποιούν.

Όλες οι συναλλαγές στην οικονομία του Bitcoin παρακολουθούνται από ένα ηλεκτρονικό "λογιστικό βιβλίο" που ονομάζεται Blockchain. Πολλαπλά αντίγραφα αυτού του "βιβλίου" υπάρχουν και συγκρίνονται μεταξύ τους, έτσι ώστε να διασφαλιστεί ότι όλες οι συναλλαγές είναι νόμιμες και έχουν καταγραφεί σωστά [1].

Αν και τα κρυπτονομίσματα είναι ένα ενδιαφέρον και με πολλές προοπτικές εξέλιξης αντικείμενο, η τεχνολογία στην οποία στηρίζονται, το Blockchain, έχει μετατραπεί σε ένα από τα πιο πολυσυζητημένα τεχνολογικά επιτεύγματα, με επενδύσεις δισεκατομμυρίων και μία ολόκληρη βιομηχανία να χτίζεται πάνω της. Οι δυνατότητες και οι χρήσεις της συγκεκριμένης τεχνολογίας είναι πολλές και διευρύνονται πέρα από την αγορά του

συναλλάγματος, συμπεριλαμβάνοντας ένα τεράστιο χάσμα εφαρμογών και πεδίων, όπως είναι για παράδειγμα ο κλάδος της ιατρικής, της εκπαίδευσης ή της έρευνας.

Τα οφέλη από την υιοθέτηση αυτής της τεχνολογίας είναι αναρίθμητα χάρη στην αρχιτεκτονική της. Το Blockchain είναι μία καινοτομία της οποίας οι κατασκευαστικές ιδιότητες προσφέρουν όλο και περισσότερες ουσιαστικές βάσεις στον ψηφιακό κόσμο, όπου υπάρχει διάθεση για τον καθορισμό υψηλότερων επιπέδων αυτονομίας και ανάθεσης. Ο ασφαλής και αμετάβλητος χαρακτήρας του, έχει προκαλέσει το ενδιαφέρον του ιδιωτικού τομέα αλλά και των κυβερνητικών αρχών. Πειράματα διεξάγονται παγκοσμίως για το πώς θα μπορούσε να αξιοποιηθεί το Blockchain σε εθνικό επίπεδο. Οι εφαρμογές πλέον αγγίζουν όλους τους τομείς της οικονομίας και της κοινωνίας, από τη χρηματοδότηση στο ηλεκτρονικό εμπόριο, την ασφάλεια τροφίμων, τη διαχείριση αλυσίδας προϊόντων ακόμα και την ηλεκτρονική ψηφοφορία.

Δεν υπάρχει τεχνολογία που να πυροδότησε τόσο μεγάλο πάθος αλλά και τόσο μεγάλη διαμάχη μεταξύ των ειδικών από την εμφάνιση του Διαδικτύου. Με τη ζυγαριά να αμφιταλαντεύεται ανάμεσα στα οφέλη που μπορεί να προσφέρει αλλά και τους κινδύνους που μπορεί να κρύβει, ενισχύεται το αίσθημα της σύγχυσης. Αδιαμφισβήτητα, η εξερεύνηση του Blockchain είναι μία από τις μεγαλύτερες προκλήσεις που έχουν να αντιμετωπίσουν οι επιστήμονες και είναι ικανή να αλλάξει ολοκληρωτικά τα δεδομένα που μέχρι τώρα γνωρίζαμε.

2

Μια εισαγωγή στο Blockchain

2.1 Τι είναι το Blockchain

Η νέα τεχνολογία Blockchain είναι ένα αποκεντρωμένο δίκτυο ομότιμων κόμβων (peer-to-peer) μέσα στο οποίο καταγράφονται τα δεδομένα και οι συναλλαγές που έχουν πραγματοποιηθεί μεταξύ τους. Στο δίκτυο αυτό, τα δεδομένα καταχωρούνται και αποθηκεύονται σε πακέτα (Block), τα οποία συνδέονται μεταξύ τους δημιουργώντας έτσι μία αλυσίδα από μπλοκ. Σε αυτόν τον τρόπο λειτουργίας οφείλει η τεχνολογία το όνομά της (Blockchain).

Το δίκτυο του Blockchain είναι διανεμημένο ισότιμα. Αυτό σημαίνει πώς κανένα πρόσωπο μέσα στο δίκτυο δεν υπερέχει έναντι κάποιου άλλου και υπάρχει απουσία προτεραιότητας. Όλα τα πρόσωπα που συμμετέχουν στο δίκτυο, έχουν πρόσβαση σε αυτό κρατώντας ο καθένας ένα αντίγραφο του αρχείου καταχωρήσεων, κάτι που εξασφαλίζει την ασφάλεια και τη διαφάνεια των συναλλαγών [1]. Η διαδικασία δημιουργίας και διαφύλαξης του αρχείου καθορίζεται και ελέγχεται από ένα Σύνταγμα κανόνων που ονομάζεται πρωτόκολλο συναίνεσης και ρυθμίζεται από τους συμμετέχοντες. Για τη σύνταξη ενός συμπαγούς πρωτοκόλλου δεν είναι αναγκαία η απόδειξη τιμιότητας και εμπιστοσύνης μεταξύ των τελευταίων [2].

Κάθε συναλλαγή προτού καταχωρηθεί στην αλυσίδα, ελέγχεται από τα πρόσωπα του δικτύου με βάση τους κανόνες που έχουν συμφωνηθεί. Εφόσον εξακριβωθεί και εγκριθεί, τοποθετείται σύμφωνα με τη χρονολογική σειρά κατά την οποία έχει πραγματοποιηθεί.

Το αρχείο που δημιουργείται και μοιράζεται σε ένα μεγάλο αριθμό χρηστών, είναι κρυπτογραφημένο και δεν επιτρέπει την αλλαγή στις εγγραφές που έχουν ήδη περαστεί σε αυτό, ενώ η απουσία κεντρικού διαχειριστή αυξάνει την αξιοπιστία του συστήματος δίνοντας του τη δυνατότητα να μη μπορεί να χειραγωγηθεί εύκολα [3]. Στο τέλος λειτουργεί ως ένα αμετάβλητο αρχείο συναλλαγών που δεν απαιτεί να βασίζεται σε μία εξωτερική αρχή για την επικύρωση της αυθεντικότητας και της ακεραιότητας των δεδομένων. Οποιαδήποτε πληροφορία μπορεί να αποθηκευτεί στο μπλοκ, γεγονός που συμβάλλει στην εκτεταμένη χρήση του [4].

Το Blockchain, στην ουσία, μπορεί να περιγραφεί ως μία κατανεμημένη, κρυπτογραφημένη βάση δεδομένων ή μητρώο (ledger) μέσα στο οποίο αποθηκεύονται και

επαληθεύονται πληροφορίες αξίας οι οποίες εντάσσονται σε μπλοκ και δημιουργούν μία συνεχή αλυσίδα στην οποία μπορεί να έχει πρόσβαση ο κάθε κόμβος (node) που συμμετέχει στο δίκτυο, ενώ η τροποποίηση και η αντιστρεψιμότητα της πληροφορίας είναι σχεδόν απίθανη εφόσον αυτή έχει καταγραφεί στο μητρώο. Η πληροφορία μπορεί να αφορά κάποιο περιουσιακό στοιχείο ή πνευματική ιδιοκτησία, μέχρι και ένα σύστημα ψηφοφορίας ή νομικών εγγράφων [5]. Όπως χαρακτηρίστηκε από το περιοδικό "The Economist" (2015), το Blockchain είναι μία "μηχανή εμπιστοσύνης". Λόγω των κρυπτογραφικών τεχνικών και της αποκεντρωμένης και κατανεμημένης φύσης τους, οι αλυσίδες λέγεται ότι είναι εξαιρετικά ανθεκτικές.

2.2 Η ιστορία πίσω από τη δημιουργία του

Η αρχική ιδέα της τεχνολογίας Blockchain χρονολογείται το 1991, όταν οι ερευνητές Stuart Haber και W. Scott Stornetta εισήγαγαν μία υπολογιστικά πρακτική λύση για τον σχεδιασμό ψηφιακών εγγράφων τα οποία θα "σφραγίζονται" με χρονολογική σειρά, ώστε να μην μπορούν να επικαιροποιηθούν ή να αλλοιωθούν.

Το σύστημα χρησιμοποιούσε μία κρυπτογραφημένη αλυσίδα από μπλοκ για την αποθήκευση των χρονολογικά "σφραγισμένων" εγγράφων, ενώ το 1992 όταν ενσωματώθηκε στο σχεδιασμό η μέθοδος Merkle Trees, αυτό έγινε πιο αποτελεσματικό επιτρέποντας τη συλλογή πολλών εγγράφων σε ένα μπλοκ μόνο. Ωστόσο η τεχνολογία αυτή δεν χρησιμοποιήθηκε και το δίπλωμα ευρεσιτεχνίας τους έληξε το 2004, τέσσερα χρόνια πριν από την ίδρυση του Bitcoin [6].

Το 2008, κατά τη διάρκεια της Παγκόσμιας Οικονομικής Κρίσης, δημοσιεύτηκε το πρώτο επιστημονικό άρθρο σχετικά με το νέο μηχανισμό, με τίτλο "Bitcoin : A Peer to Peer Electronic Cash System". Ο εγκέφαλος πίσω από αυτή την έρευνα υπέγραψε με το ψευδώνυμο Satoshi Nakamoto, του οποίου η πραγματική ταυτότητα παραμένει άγνωστη μέχρι στιγμής. Υπάρχουν πολλές υποθέσεις ότι πίσω από αυτό το ψευδώνυμο κρύβεται μία ομάδα ειδικών στην κρυπτογραφία και στην επιστήμη υπολογιστών. Ανεπιτυχείς προσπάθειες πραγματοποιήθηκαν για την εύρεση της πραγματικής ταυτότητας, καθώς στη δημοσίευση χρησιμοποιήθηκε μία υπηρεσία ανώνυμης αλληλογραφίας (Vistomail) και ένας δωρεάν λογαριασμός ηλεκτρονικού ταχυδρομείου (gmx.com) από τον όποιο υπήρχε επικοινωνία όταν συνδεόταν μέσω Tor. Κάποιοι θεωρούν ότι η απόκρυψη των προσωπικών στοιχείων έγινε με σκοπό την προστασία του υπεύθυνου για την έρευνα προσώπου, αλλά και του ίδιου του δικτύου. Πιθανότατα χρησιμοποιήθηκε το όνομα Satoshi επειδή σημαίνει "σοφία" ή "λόγος" και το Nakamoto το οποίο έχει την έννοια της "Κεντρικής Πηγής" [7] [8].

Η Οικονομική Κρίση παρείχε εύφορο έδαφος για τη λειτουργία, την απορρόφηση και την επέκταση των κρυπτονομισμάτων, ειδικότερα του Bitcoin. Στο πλαίσιο έλλειψης εμπιστοσύνης ως προς το σύστημα διακυβέρνησης, το Bitcoin θεωρήθηκε από ορισμένους ως μία επιθυμητή εναλλακτική λύση. Στην επιστημονική δημοσίευση του Satoshi Nakamoto αναγράφονταν λεπτομέρειες για το πώς η τεχνολογία θα μπορούσε να ενισχύσει την εμπιστοσύνη στα ψηφιακά συστήματα μέσω μιας αποκεντρωμένης πηγής η οποία δε θα ελεγχόταν από κανέναν [9]. Ένα νέο μοντέλο απορρήτου περιγραφόταν, στο οποίο το τρίτο άτομο εμπιστοσύνης που εμπλέκεται στις συναλλαγές αντικαθίσταται από κρυπτογραφικές μεθόδους. Οι συναλλαγές επικυρώνονται μόνο από τους συμμετέχοντες, αποφεύγοντας σημεία αποτυχίας που υπάρχουν στο παραδοσιακό σύστημα ιδιωτικότητας (π.χ. τραπεζικά συστήματα). Μία από τις ιδιαιτερότητες του μοντέλου, ήταν η δυνατότητα επίλυσης του προβλήματος “double-spending” , δηλαδή το γεγονός ότι τα ψηφιακά νομίσματα μπορούν να δαπανηθούν πάνω από μία φορά επειδή μπορεί να γίνει αντιγραφή του ψηφιακού αρχείου. Επιπροσθέτως, το νέο σύστημα επέτρεπε στις συναλλαγές να είναι δημόσιες και την ίδια στιγμή τα εμπλεκόμενα πρόσωπα να παραμένουν ανώνυμα ενισχύοντας έτσι την διαφάνεια και διατηρώντας τη μυστικότητα. Τα ελκυστικά χαρακτηριστικά του Bitcoin, προσφέρουν προστασία κατά της απάτης, σε συγκυρίες όπου οι “δυνατότεροι παίκτες” του οικονομικού συστήματος πρωτοστατούν στην παραβίαση λογιστικών βιβλίων και μετρήσεων της αγοράς [10].

Στις 3 Ιανουαρίου του 2009, το πρώτο ψηφιακό νόμισμα Bitcoin δημιουργήθηκε μέσα από τη διαδικασία “εξόρυξης” (Mining) που ακολούθησε ο Satoshi Nakamoto. Ο Hal Finney ήταν ο πρώτος αγοραστής Bitcoin, καταγράφοντας την πρώτη Παγκόσμια συναλλαγή του ψηφιακού νομίσματος. Το 2009, η αξία του ήταν μικρότερη από το ένα δέκατο του ενός σεντ και το 2017 έφτασε να αξίζει περισσότερο από 20.000 δολάρια. Η αξία του αλλάζει σε ακαριαίο χρόνο και μπορεί από τη μία μέρα στην άλλη να πολλαπλασιαστεί ή να υποπολλαπλασιαστεί [11].

Ενώ το Bitcoin αποτελεί το έναυσμα για την πρώτη πρακτική εφαρμογή του Blockchain, στην πραγματικότητα είναι ένας συνδυασμός διαφόρων σημαντικών τεχνικών που αναπτύχθηκαν κατά τη διάρκεια των τελευταίων τεσσάρων δεκαετιών τουλάχιστον. Το 2013, η φήμη της τεχνολογίας Blockchain εκτοξεύθηκε ως αποτέλεσμα της χρήσης του και σε άλλα κρυπτονομίσματα, όπως το Ethereum, αλλά και στην ευρεία βιομηχανική εφαρμογή του. Η δημιουργία του Ethereum αποτέλεσε το δεύτερο ορόσημο στην ιστορία του Blockchain. Την ίδια χρονολογία, ο νεαρός προγραμματιστής Vitalik Buterin δημοσίευσε ένα πλάνο για την ανάπτυξη μιας νέας κατανεμημένης πλατφόρμας βασισμένη στην τεχνολογία Blockchain, με αφορμή την ανάγκη οικοδόμησης μιας κατάλληλης προγραμματιστικής γλώσσας για τις αποκεντρωμένες εφαρμογές [10].

2.3 Οι φάσεις στην εξέλιξή του

Το οικονομικό, πολιτικό, ανθρωπιστικό και νομικό σύστημα επωφελείται από τη δημιουργία του Bitcoin και της τεχνολογίας Blockchain, καθιστώντας ξεκάθαρη την τεράστια ισχύ των δυνατοτήτων τους, η οποία θα μπορούσε να αναδιαμορφώσει όλες τις πτυχές της κοινωνίας και των λειτουργιών της [12]. Σύμφωνα με τη Melanie Swan, όπως διατυπώνει στο βιβλίο της "Blockchain : Blueprint for a New Economy" , η εξέλιξη του Blockchain, μπορεί να ταξινομηθεί σε τρεις φάσεις.

- **Πρώτη φάση : Blockchain 1.0 – Ψηφιακό Νόμισμα**

Το Blockchain 1.0 είναι η ανάπτυξη του ψηφιακού νομίσματος και η εφαρμογή του στις ηλεκτρονικές συναλλαγές. Το Bitcoin είναι μία τυπική εφαρμογή σε αυτή την κατηγορία όπου η πράξη φαίνεται να είναι πιο μπροστά από τη θεωρία. Οι συναλλαγές μπορούν να πραγματοποιούνται με άμεσο τρόπο μεταξύ δύο συμμετεχόντων συνδυάζοντας ασφάλεια και μυστικότητα. Σε αντίθεση με τα παραδοσιακά νομίσματα, η τιμή του μεταβάλλεται συνεχώς. Η συγκεκριμένη φάση βρίσκεται σε ενεργό επίπεδο, αφού καθημερινά πραγματοποιούνται συναλλαγές του νομίσματος Bitcoin [13] [14].

- **Δεύτερη φάση : Blockchain 2.0 – Έξυπνα Συμβόλαια**

Το Blockchain 2.0 εξετάζει μία γενικότερη μορφή των οικονομικών, εμπορικών και χρηματοπιστωτικών εφαρμογών οι οποίες παίρνουν μεγαλύτερη έκταση από αυτή των απλών συναλλαγών του ψηφιακού νομίσματος. Τέτοιες εφαρμογές περιλαμβάνουν μετοχικά κεφάλαια, ομόλογα, δάνεια, νομικά μέσα όπως τίτλοι, συμβόλαια και άλλα περιουσιακά στοιχεία. Όλα αυτά τα αρχεία μπορούν να αποθηκευτούν και να μεταφερθούν σε μία πλατφόρμα Blockchain από όπου θα μπορεί να εκτελεστεί οποιαδήποτε ενέργεια. Φυσικά, θα μπορούν να κωδικοποιηθούν και να προστατευθούν με τη χρήση αυτής της τεχνολογίας.

Μία σημαντική αναδυόμενη περίπτωση που χρησιμοποιεί τη δομή Blockchain είναι τα έξυπνα συμβόλαια (Smart Contracts). Ένα έξυπνο συμβόλαιο είναι ένα πρόγραμμα που περιέχει όρους τους οποίους οι εμπλεκόμενοι έχουν συμφωνήσει να τηρήσουν στις μεταξύ τους αλληλεπιδράσεις. Όταν οι προϋποθέσεις που έχουν τεθεί ικανοποιηθούν, τότε το συμβόλαιο εκτελείται αυτόματα. Μία τέτοια χαρακτηριστική περίπτωση αποτελεί η μίσθωση αυτοκινήτου χωρίς να απαιτείται η συμπλήρωση των κατάλληλων εντύπων, αρχή που υιοθετήθηκε από τις εταιρείες Visa και DocuSign το 2015. Η πιο γνωστή πλατφόρμα που ασχολείται με έξυπνα συμβόλαια είναι η Ethereum. Ωστόσο, υπάρχουν ακόμα θέματα ασφάλειας και η πιθανότητα ένας αντίπαλος να εκμεταλλευτεί την εκτέλεση ενός έξυπνου

συμβολαίου και να αποκτήσει κέρδος μέσω αυτού δεν είναι μηδενική. Με τα κατάλληλα εργαλεία όμως, μπορεί να εξαλειφθεί [12] [14].

- **Τρίτη φάση : Blockchain 3.0 – Εφαρμογές**

Το Blockchain 3.0 αφορά την εξάπλωση του σε ένα εύρος εφαρμογών πέρα από το πεδίο οικονομίας, αναλαμβάνοντας δράση στην επιστήμη, στην τέχνη, στην εκπαίδευση, στην υγεία, στον κυβερνοχώρο. Η αυτοτέλεια γίνεται πιο έντονη στην τρίτη φάση, με το Blockchain 3.0 να αποτελεί τη θεμελιώδη βάση για ένα νέο πρότυπο οργάνωσης στην κοινωνία που θα επιφέρει μεγαλύτερη αποτελεσματικότητα και μικρότερη προστριβή. Μία καλύτερη συνεργασία μεταξύ των ανθρώπων και ο συντονισμός στις μεταξύ τους αλληλεπιδράσεις μπορούν να επιτευχθούν. Κάποιες από τις πιο ελπιδοφόρες μορφές του Blockchain 3.0 είναι οι έξυπνες πόλεις οι οποίες θα διευκολύνουν σημαντικά τη διαβίωση, την κινητικότητα, την οικονομία σε μία κοινωνία, η χρήση αποκεντρωμένων συστημάτων για τη διαχείριση ιατρικών αρχείων ή υψηλής προτεραιότητας φακέλων, η ελεγχόμενη παροχή κυβερνητικών υπηρεσιών χωρίς τις περιττές διαδικασίες [13] [14]. Οι πληροφορίες προβλέπονται να είναι ασφαλείς και εύκολα διαχειρίσιμες με την παγκόσμια και ευρεία χρήση αποκεντρωμένων συστημάτων Blockchain.

2.4 Τύποι του Blockchain

1. **<u>Δημόσια Δίκτυα Blockchain</u>**

Στο δημόσιο Blockchain (Public Blockchain) δεν είναι απαραίτητη η άδεια για να συμμετάσχει κάποιος χρήστης. Οποιοσδήποτε μπορεί να ενταχθεί στο δίκτυο και να δημιουργήσει ένα μπλοκ μέσω της διαδικασίας “απόδειξη εργασίας”, να υποβάλλει ή να διαβάσει συναλλαγές. Επιπλέον, τα δίκτυα Blockchain αυτού του τύπου είναι πλήρως αποκεντρωμένα, δηλαδή δεν υπάρχει κεντρική αρχή για να επεξεργαστεί τις πληροφορίες που περιλαμβάνονται αλλά και να πραγματοποιήσει οποιαδήποτε τροποποίηση στα πρωτόκολλα του δικτύου, με αποτέλεσμα το σύστημα να είναι ισχυρό έναντι επιθέσεων. Ακόμα, υποστηρίζουν την ανωνυμία η οποία με τη σειρά της παρέχει προστασία στην ιδιωτικότητα των χρηστών. Παράλληλα, το γεγονός ότι κάθε μέλος έχει τη δυνατότητα να διαβάσει κάθε συναλλαγή, προσδίδει στο σύστημα διαφάνεια [52].

Το καλύτερο ίσως χαρακτηριστικό αυτού του τύπου, είναι η κατανεμημένη φύση του, καθώς η πραγματοποίηση κάποιας συναλλαγής μπορεί να γίνει οποιαδήποτε στιγμή και από οποιοδήποτε μέρος χωρίς χρέωση και με μεγάλη ταχύτητα. Αυτό προσφέρει μεγάλη ελευθερία στους χρήστες που επιθυμούν να συμμετάσχουν στο δίκτυο. Δύο από τα μεγαλύτερα και διαδεδομένα δημόσια δίκτυα Blockchain είναι εκείνο του Bitcoin και του Ethereum [53].

2. Ιδιωτικά Δίκτυα Blockchain

Το ιδιωτικό δίκτυο Blockchain (Private Blockchain) δεν επιτρέπει σε κανέναν χρήστη να συμμετέχει ελεύθερα στο δίκτυο και να έχει πρόσβαση στον "κατάλογο" με τα δεδομένα. Ενέργειες εκτελούν μόνο εξουσιοδοτημένοι χρήστες αναλόγως με τα δικαιώματα που κατέχουν. Τέτοια δίκτυα υιοθετούνται κυρίως από οργανισμούς και επιχειρηματικές μονάδες που σκοπός τους είναι να καταγράψουν και να διαφυλάξουν σημαντικές πληροφορίες, έχοντας όμως τη δυνατότητα να τις ανταλλάσσουν μεταξύ τους. Ένα ιδιωτικό σύστημα Blockchain μπορεί να είναι μερικώς αποκεντρωμένο ή να κρατά τις εγγραφές του συγκεντρωτικά σε έναν οργανισμό. Οι χρήστες έχουν το δικαίωμα να διαπραγματευτούν και να επιτύχουν συναίνεση με τον επιθυμητό κόμβο [52].

Επιπροσθέτως, στα ιδιωτικά δίκτυα, η ταυτότητα των μελών είναι γνωστή, αλλά οι συναλλαγές είναι ορατές μόνο σε όσους έχουν την κατάλληλη άδεια. Δεδομένου ότι στη διαδικασία συναίνεσης δεν εμπλέκονται όλοι οι χρήστες, τα ιδιωτικά δίκτυα έχουν υψηλότερη απόδοση σε σχέση με τα δημόσια. Προσφέρουν μεγαλύτερη αποτελεσματικότητα και ταχύτερες συναλλαγές αλλά η ασφάλεια δεν είναι τόσο ισχυρή όσο είναι στα δημόσια [53].

3. Ομοσπονδιακά Δίκτυα Blockchain

Πρόκειται για ένα εξουσιοδοτημένο σύστημα το οποίο ελέγχεται από μία επιλεγμένη ομάδα κόμβων. Έχει τα ίδια οφέλη που έχει και ένα ιδιωτικό δίκτυο Blockchain και θα μπορούσε να θεωρηθεί υποκατηγορία τους. Τα ομοσπονδιακά δίκτυα Blockchain (Consortium Blockchain) χρησιμοποιούνται κυρίως στον τραπεζικό τομέα και επιτρέπουν μεγαλύτερο έλεγχο του δικτύου από συγκεκριμένους κόμβους. Οι επιδράσεις τους είναι κρίσιμης σημασίας καθώς μειώνουν το κόστος των συναλλαγών. Ωστόσο, δεν είναι ακόμα σαφές αν η τεχνολογία αυτή θα είναι αποδοτική και αν θα υιοθετηθεί.

3

Βασικές έννοιες στην Κρυπτογραφία

Είναι πλέον αδιαμφισβήτητο το γεγονός ότι η κρυπτογραφία και οι κάθε είδους εφαρμογές της έχουν κομβικό ρόλο στη σύγχρονη τεχνολογία και ειδικότερα σε τομείς όπως είναι η ασφαλής πρόσβαση σε συστήματα και υπηρεσίες, η ασφαλής επικοινωνία, η ανάκτηση και διαχείριση ευαίσθητων δεδομένων, οι ηλεκτρονικές συναλλαγές, οι ηλεκτρονικές ψηφοφορίες και οι στρατιωτικές εφαρμογές. Ιδιαίτερα, τις τελευταίες δεκαετίες η απότομη άνθηση των τηλεπικοινωνίων έχει καταστήσει την κρυπτογραφία αναπόσπαστο κομμάτι των τεχνολογικών εξελίξεων και αντικείμενο έντονης ερευνητικής δραστηριότητας, η οποία την έχει μετατρέψει από μορφή τέχνης σε επιστήμη, με αυστηρούς ορισμούς και αποδείξεις.

Η ιστορία της κρυπτογραφίας μπορεί να διαιρεθεί σε τρία στάδια. Στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης χρησιμοποιούσαν τον τρόπο της έντυπης απεικόνισης. Έλαβαν τη μορφή αντικατάστασης και μετάθεσης γραμμάτων. Χαρακτηριστικό παράδειγμα είναι ο αλγόριθμος του Καίσαρα ο οποίος επινοήθηκε με σκοπό να επικοινωνεί ο Ιούλιος Καίσαρας με τους επιτελείς του, χωρίς να έχουν δυνατότητα πρόσβασης στα μηνύματα οι εχθροί του. Σαν δεύτερο στάδιο αναφέρεται αυτό των κρυπτογραφικών μηχανών. Τελευταίο στάδιο θεωρείται το σύγχρονο κρυπτογραφικό σύστημα, απόρροια της αμοιβαίας αλληλεπίδρασης των μαθηματικών, τα οποία αποτελούν θεμελιώδη βάση για το σχεδιασμό των υπολογιστών, οι οποίοι επέτρεψαν τη χρήση πολυπλοκότερων αλγορίθμων με μεγαλύτερη ταχύτητα [42].

Από τη στιγμή που η κρυπτογραφία ξεκίνησε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για την απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν αγώνα ταχύτητας. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μία αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με στόχο τη διαφύλαξη εθνικών μυστικών και στρατηγικών. Στον 20ό αιώνα, τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά.

Ένα από τα γεγονότα που χαράχθηκαν στην ιστορία της κρυπτογραφίας είναι η χρήση της περίφημης μηχανής Αίνιγμα (Enigma) η οποία χρησιμοποιήθηκε από τη Γερμανία κατά τη διάρκεια του Β’ Παγκοσμίου Πολέμου για την κρυπτογράφηση ραδιοτηλεπικοινωνιών.

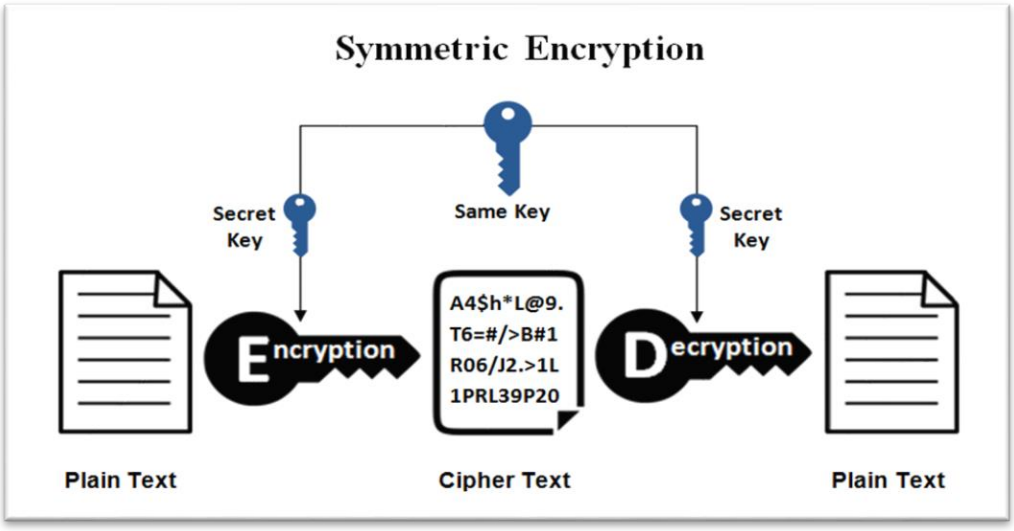
Στην πορεία οι Βρετανοί συγκέντρωσαν μία ομάδα κρυπταναλυτών με επικεφαλή τον Alan Turing, με σκοπό να αποκρυπτογραφήσουν τα μηνύματα του Γερμανικού επιτελείου. Ο Turing, θεωρώντας ότι μόνο μία αυτόματη και σχετικά γρήγορη μηχανή θα μπορούσε να δώσει λύση στις δοκιμές, οδηγήθηκε στην κατασκευή εξομοιωτή της μηχανής Αίνιγμα. Η αποκρυπτογράφηση των μηνυμάτων με τη συμβολή του εξομοιωτή αποτέλεσε ορόσημο στην έκβαση του Πολέμου ο οποίος τελικά κρίθηκε υπέρ των Συμμάχων.

Στα περισσότερα κρυπτοσυστήματα είναι πλέον γνωστός ο τρόπος λειτουργίας τους και η ασφάλειά τους βασίζεται αποκλειστικά σε αριθμητικούς αλγόριθμους που επιτρέπουν την εκτέλεση πράξεων, ώστε η υπολογιστική δυσκολία των αντίστροφων πράξεων να είναι τεράστια. Η κρυπτογραφία είναι έτοιμη να προσφέρει ακόμη περισσότερο τις υπηρεσίες της στο σύνολο της ανθρωπότητας, προάγοντας τη δημοκρατία, το σεβασμό της ιδιωτικής ζωής και τελικά την ενεργό και ισότιμη συμμετοχή όλων στο οικονομικό, πολιτικό και κοινωνικό γίγνεσθαι.

3.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία (Symmetric Cryptography) βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση ενός μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.

Αυτό το είδος κρυπτογράφησης, γνωστό επίσης και ως συμβατική, αποτελούσε το μοναδικό τύπο κρυπτογράφησης, πριν εμφανιστεί εκείνη του δημοσίου κλειδιού το 1970. Παραμένει με διαφορά το πιο ευρέως διαδεδομένο είδος κρυπτογράφησης με αμέτρητες εφαρμογές, όπως η εξασφάλιση ασφαλούς σύνδεσης σε HTTPS ιστοσελίδες ή η κρυπτογράφηση του σκληρού δίσκου. Μετατρέπει το αρχικό μήνυμα (plaintext) σε κρυπτοκείμενο (ciphertext), κάνοντας χρήση ενός μυστικού κλειδιού και ενός αλγορίθμου κρυπτογράφησης E(K,X). Το αρχικό μήνυμα μπορεί να ανακτηθεί από το κρυπτοκείμενο χρησιμοποιώντας το ίδιο κλειδί και έναν αλγόριθμο αποκρυπτογράφησης D(K,Y). Γνωστοί συμμετρικοί αλγόριθμοι κρυπτογράφησης είναι ο AES, ο DES, ο 3DES [64].



Εικόνα 3.1 : Απεικόνιση Συμμετρικής Κρυπτογραφίας. Η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποιούνται με χρήση του ίδιου κλειδιού.

3.2 Κρυπτογράφηση Δημοσίου Κλειδιού

Η ανακάλυψη της κρυπτογραφίας δημοσίου κλειδιού (Public Key Cryptography) είναι η μεγαλύτερη και ίσως η μόνη πραγματική επανάσταση σε όλη την ιστορία της κρυπτογραφίας. Αποτελεί μία θεμελιώδη ευκαιρία για αλλαγή της όλης φιλοσοφίας των κρυπτογραφικών συστημάτων. Η κρυπτογράφηση δημοσίου κλειδιού ή διαφορετικά ασύμμετρη κρυπτογράφηση (Asymmetric Cryptography) στηρίζεται κυρίως σε μαθηματικές συναρτήσεις, σε αντίθεση με την συμμετρική κρυπτογραφία που εμπεριέχει κυρίως τις μεθόδους αντικατάστασης και αντιμετάθεσης. Κυρίως όμως αυτή η κατηγορία είναι ασύμμετρη, εμπεριέχοντας τη χρήση δύο ξεχωριστών κλειδιών για την κρυπτογράφηση και την αποκρυπτογράφηση. Η πρώτη πραγματοποιείται με ένα δημόσιο κλειδί, ενώ η δεύτερη με ένα ιδιωτικό. Η αξιοποίηση των δύο κλειδιών έχει επίδραση σε τομείς όπως η εμπιστευτικότητα, η διανομή κλειδιού και η αυθεντικοποίηση.

Η έννοια της κρυπτογραφίας δημοσίου κλειδιού αναπτύχθηκε σε μία προσπάθεια αντιμετώπισης δύο εκ των δυσκολότερων προβλημάτων που σχετίζονται με τη συμμετρική κρυπτογράφηση. Το πρώτο πρόβλημα αφορά τη διανομή του κλειδιού. Η διανομή του κλειδιού στη συμμετρική κρυπτογράφηση απαιτεί είτε οι δύο επικοινωνούντες να μοιράζονται εκ των προτέρων ένα κλειδί, το οποίο τους έχει διανεμηθεί με κάποιο τρόπο είτε τη χρήση ενός κέντρου διανομής κλειδιών. Ο Whitefield Diffie, ένας από εκείνους που ανακάλυψαν την κρυπτογράφηση δημοσίου κλειδιού (παράλληλα με τον Martin

Hellman), έκρινε ότι αυτή η δεύτερη απαίτηση καταργούσε τη βασική οντότητα της κρυπτογραφίας, δηλαδή την ικανότητα να διατηρείται καθολική μυστικότητα στην επικοινωνία. Το δεύτερο πρόβλημα, που μελέτησε εμπεριστατωμένα ο Diffie και που φαινομενικά δεν σχετιζόταν με το πρώτο, ήταν εκείνο των "ψηφιακών υπογραφών". Εάν επρόκειτο να εξαπλωθεί η χρήση της κρυπτογραφίας, όχι μόνο σε στρατιωτικές εφαρμογές αλλά και για εμπορικούς και ιδιωτικούς σκοπούς, τότε όλα τα ηλεκτρονικά μηνύματα και έγγραφα θα χρειάζονταν κάτι ισοδύναμο των υπογραφών που απαιτούνται στα γραπτά έγγραφα. Γεννήθηκε λοιπόν το ερώτημα αν θα μπορούσε να επινοηθεί μία μέθοδος που να εγγυάται πως κάθε συνδιαλεγόμενο μέλος θα είναι σίγουρο πως ένα ψηφιακό μήνυμα εστάλη από κάποιο συγκεκριμένο άτομο [64].

Οι Diffie και Hellman κατόρθωσαν να κάνουν μία εκπληκτική ανακάλυψη το 1976, επινοώντας μία μέθοδο, την κρυπτογράφηση δημοσίου κλειδιού, που αντιμετώπιζε και τα δύο προβλήματα και ήταν ριζικά διαφορετική από όλες τις προηγούμενες προσεγγίσεις στην κρυπτογραφία, οι οποίες είχαν ηλικία μεγαλύτερη των τεσσάρων χιλιετιών.

Οι ασύμμετροι αλγόριθμοι, όπως προαναφέρθηκε, χρησιμοποιούν ένα κλειδί για κρυπτογράφηση και ένα διαφορετικό για την αποκρυπτογράφηση, το οποίο όμως σχετίζεται με το πρώτο. Έχουν το πολύ σημαντικό χαρακτηριστικό ότι είναι υπολογιστικά ανέφικτο να καθοριστεί το κλειδί αποκρυπτογράφησης γνωρίζοντας μόνο τον κρυπτογραφικό αλγόριθμο και το κλειδί κρυπτογράφησης. Τα απαραίτητα βήματα για την εκτέλεση του αλγορίθμου είναι :

1. Κάθε χρήστης παράγει ένα ζεύγος κλειδιών που θα χρησιμοποιηθούν κατά την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων.

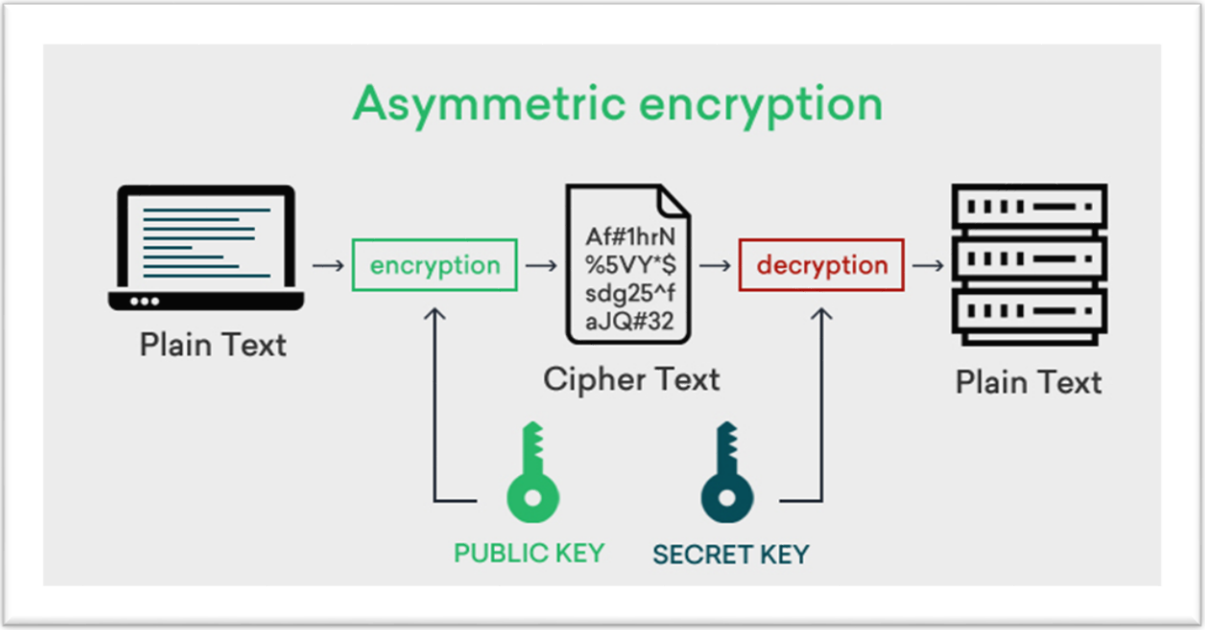
2. Κάθε χρήστης τοποθετεί το ένα από τα δύο κλειδιά σε ένα δημόσια προσπελάσιμο αρχείο. Αυτό είναι το δημόσιο κλειδί. Το άλλο κλειδί φυλάσσεται μυστικό.

3. Αν κάποιος από τους δύο συμμετέχοντες επιθυμεί να στείλει ένα εμπιστευτικό μήνυμα στον άλλον, τότε αυτός κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του δευτέρου.

4. Όταν ο τελευταίος λάβει το μήνυμα, το αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί. Κανένας άλλος παραλήπτης δε μπορεί να αποκρυπτογραφήσει το μήνυμα γιατί μόνο ο ίδιος γνωρίζει το ιδιωτικό κλειδί.

Με την προσέγγιση αυτή, όλοι οι μετέχοντες έχουν πρόσβαση στα δημόσια κλειδιά, αλλά τα ιδιωτικά κλειδιά παράγονται τοπικά από κάθε συμμετέχοντα και έτσι δε χρειάζεται να διανεμηθούν. Εφόσον το ιδιωτικό κλειδί του χρήστη παραμένει προστατευμένο και μυστικό, η εισερχόμενη επικοινωνία είναι ασφαλής. Οποιαδήποτε στιγμή, ένας χρήστης

μπορεί να αλλάξει το ιδιωτικό του κλειδί και να δημοσιεύσει το αντίστοιχο δημόσιο κλειδί, προκειμένου να αντικαταστήσει το παλιό.



Εικόνα 3.2 : Κρυπτογράφηση Δημοσίου Κλειδιού. Η κρυπτογράφηση πραγματοποιείται με δημόσιο κλειδί ενώ η αποκρυπτογράφηση με ιδιωτικό κλειδί.

3.3 Αυθεντικοποίηση Μηνύματος

Η αυθεντικοποίηση μηνύματος, καθώς και το συναφές θέμα των ψηφιακών υπογραφών, αποτελούν ίσως την πιο "θολή" περιοχή στην ασφάλεια δικτύων. Οι σχετικές επιγραφές, καθώς και τα μέτρα αντιμετώπισης αυτών, είναι τόσο συγκεχυμένα ώστε όσοι ασχολούνται με το χώρο αυτόν, αρχίζουν να θυμίζουν τους αστρονόμους από το παρελθόν, οι οποίοι τοποθετούσαν τη μία τροχιά πάνω στην άλλη σε μία προσπάθεια να εξηγήσουν κάθε φαινόμενο. Βέβαια, οι σημερινοί σχεδιαστές κρυπτογραφικών πρωτοκόλλων εργάζονται με ένα στερεό μοντέλο.

Η αυθεντικοποίηση μηνύματος είναι ένας μηχανισμός ή υπηρεσία που αποσκοπεί στην επιβεβαίωση της ακεραιότητας ενός μηνύματος. Είναι στην ουσία μία διαδικασία, που πιστοποιεί ότι τα λαμβανόμενα μηνύματα προέρχονται πράγματι από την πηγή που

ισχυρίζεται ότι τα στέλνει και δεν έχουν υποστεί μεταβολή. Η αυθεντικοποίηση μηνύματος μπορεί επίσης να επικυρώσει τη σωστή αλληλουχία των μηνυμάτων, αλλά και να προστατεύσει από επιθέσεις τροποποίησης χρονισμού. Η ψηφιακή υπογραφή είναι μία τεχνική αυθεντικοποίησης που μπορεί επιπλέον να αντιμετωπίσει τις επιθέσεις αποποίησης προέλευσης.

Οι δύο πιο κοινές κρυπτογραφικές τεχνικές που χρησιμοποιούνται για την αυθεντικοποίηση μηνύματος είναι ο Κώδικας Αυθεντικοποίησης Μηνύματος (Message Authentication Code – MAC) και μία ασφαλής Συνάρτηση Κατακερματισμού. Ο MAC είναι ένας αλγόριθμος που απαιτεί χρήση ενός μυστικού κλειδιού. Δέχεται σαν είσοδο ένα μήνυμα μεταβλητού μήκους και ένα μυστικό κλειδί και παράγει στην έξοδο έναν κώδικα αυθεντικοποίησης μηνύματος. Ένας παραλήπτης που έχει στην κατοχή του το μυστικό κλειδί μπορεί να δημιουργήσει τον κώδικα αυθεντικοποίησης μηνύματος για να πιστοποιήσει την ακεραιότητα του μηνύματος. Μία συνάρτηση κατακερματισμού αντιστοιχίζει ένα μήνυμα μεταβλητού μήκους σε μία τιμή κατακερματισμού σταθερού μήκους ή σύνοψη μηνύματος (Message digest). Για την αυθεντικοποίηση του μηνύματος, θα πρέπει μία ασφαλής συνάρτηση κατακερματισμού να συνδυαστεί, με κάποιον τρόπο, με ένα μυστικό κλειδί [64].

Κάθε μηχανισμός αυθεντικοποίησης ή ψηφιακής υπογραφής διαθέτει δύο λειτουργικά επίπεδα. Στο χαμηλότερο, πρέπει να υπάρχει κάποιου είδους συνάρτηση που να παράγει έναν αυθεντικοποιητή, δηλαδή μία τιμή που θα χρησιμοποιηθεί για την αυθεντικοποίηση του μηνύματος. Αυτή η συνάρτηση χαμηλότερου επιπέδου χρησιμοποιείται στη συνέχεια ως πρωταρχικό πρωτόκολλο αυθεντικοποίησης σε ένα υψηλότερο επίπεδο, ώστε τελικά να επιτρέψει σε ένα χρήστη να πιστοποιεί την αυθεντικότητα του μηνύματος. Οι δύο σημαντικότεροι τύποι συναρτήσεων που μπορούν να χρησιμοποιηθούν για να παράγουν έναν αυθεντικοποιητή, όπως αναφέρθηκε προηγουμένως, είναι ο Κώδικας Αυθεντικοποίησης Μηνύματος (MAC) και η Συνάρτηση Κατακερματισμού (Hash Function).

3.3.1 Συναρτήσεις Κατακερματισμού

Οι συναρτήσεις κατακερματισμού αποτελούν πολύτιμο εργαλείο στη σχεδίαση τεχνικών για την αυθεντικοποίηση της πληροφορίας. Χρησιμοποιούνται για την παραγωγή "ψηφιακών δακτυλικών αποτυπωμάτων" και είναι συστατικό πολλών κρυπτοσυστημάτων. Μία συνάρτηση κατακερματισμού δέχεται ως είσοδο ένα μήνυμα μεταβλητού μήκους και παράγει μία έξοδο σταθερού μήκους, γνωστή και ως κώδικα κατακερματισμού. Μία

σημαντική διάκριση μεταξύ των συναρτήσεων κατακερματισμού και άλλων κρυπταλγορίθμων, όπως στον MAC, είναι ότι οι πρώτες δεν απαιτούν την ύπαρξη κλειδιού για την εφαρμογή τους. Αυτό σημαίνει ότι, δεδομένου ενός μηνύματος εισόδου, οποιοσδήποτε επιθυμεί, έχει τη δυνατότητα να υπολογίσει την κατακερματισμένη τιμή του μηνύματος. Υπάρχει ένα πλήθος συναρτήσεων κατακερματισμού που έχουν καθοριστεί σε πρότυπα που είναι διαθέσιμα στο κοινό. Για παράδειγμα, το πρότυπο Secure Hash Standard (SHS), προσδιορίζει πέντε κρυπτογραφικές συναρτήσεις κατακερματισμού, τις SHA-1, SHA-224, SHA-256, SHA-384 και SHA-512. Συνδυάζοντας ένα μήνυμα εισόδου με μία συνάρτηση κατακερματισμού, είναι εύκολο να μετατραπεί σε ένα μήνυμα εξόδου. Ωστόσο, οι συναρτήσεις αυτές, ικανοποιούν μαθηματικές ιδιότητες οι οποίες κάνουν το αρχικό κείμενο δύσκολα ανιχνεύσιμο. Δηλαδή, δεδομένου μίας εξόδου, είναι σχεδόν αδύνατο να υπολογιστεί η αρχική είσοδος. Επομένως, έχουν μία σημαντική ασυμμετρία· είναι εύκολο να εκτιμηθούν, αλλά δύσκολο να αντιστραφούν [15] [16] [64].

Μία τιμή κατακερματισμού *h*, παράγεται από μία συνάρτηση *H* της μορφής *h = H(M),* όπου *M* ένα μήνυμα μεταβλητού μήκους και *H(M)* η κατακερματισμένη τιμή σταθερού μήκους. Ο αποστολέας προσαρτά την τιμή κατακερματισμού στο μήνυμα, όταν αυτό είναι έτοιμο προς αποστολή. Ο δέκτης αυθεντικοποιεί το συγκεκριμένο μήνυμα υπολογίζοντας εκ νέου από το μήνυμα που έλαβε, την τιμή κατακερματισμού. Στην ουσία, είναι μαθηματικές συναρτήσεις που δέχονται ως είσοδο κάποιο δεδομένο, τυχαίου μεγέθους και επιστρέφουν μία αναπαράσταση σταθερού μεγέθους. Λόγω του ότι η συνάρτηση κατακερματισμού δε θεωρείται μυστική, απαιτούνται κάποια μέτρα προστασίας της τιμής αυτής [64].

Σκοπός μίας συνάρτησης κατακερματισμού είναι να δημιουργήσει ένα "αποτύπωμα" ενός αρχείου, μηνύματος ή άλλου τμήματος δεδομένων. Προκειμένου να μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση μηνύματος, μία συνάρτηση κατακερματισμού πρέπει να ικανοποιεί κάποιες προϋποθέσεις. Οι συναρτήσεις κατακερματισμού μπορούν να χωριστούν σε δύο κατηγορίες με βάση τις απαιτήσεις και τις ιδιότητες που θα ακολουθούν, τις μονόδρομες συναρτήσεις κατακερματισμού (One-way Hash Functions – OWFH) και τις συναρτήσεις αντίστασης σε συγκρούσεις (Collision Resistant Hash Functions – CRHF). Οι ιδιότητες αυτές φαίνονται παρακάτω [15].

1. Εφαρμόζονται σε τμήματα δεδομένων οποιουδήποτε μεγέθους και παράγει σταθερή έξοδο.

2. Δοθείσης ενός *x*, η κατακερματισμένη τιμή *H(x)* υπολογίζεται εύκολα, καθιστώντας πρακτική την υλοποίηση σε υλικό και σε λογισμικό. Διαφορετικά, η συνάρτηση κατακερματισμού δε θα είναι αποτελεσματική.

3. Για οποιαδήποτε τιμή *h*, είναι υπολογιστικά μη εφικτό να υπολογιστεί *x*, τέτοιο ώστε *H(x) = h*. Αυτή είναι η ιδιότητα του μονόδρομου (one-way property). Η ιδιότητα αυτή δηλώνει ότι είναι απλό να παραχθεί ένας κώδικας με δεδομένο ένα μήνυμα, αλλά και ουσιαστικά αδύνατο να ανακτηθεί το μήνυμα δοθέντος του κώδικα. Είναι σημαντική εάν στην τεχνική αυθεντικοποίησης συμπεριλαμβάνεται η χρήση μίας μυστικής τιμής.

4. Έχοντας ως είσοδο οποιοδήποτε *x*, να είναι υπολογιστικά μη εφικτό να βρεθεί $y \neq x$ τέτοιο ώστε *H(x) = H(y)*. Αυτό αναφέρεται ως ασθενής αντίσταση σε συγκρούσεις (weak collision resistance). Η ιδιότητα αυτή παρέχει την εγγύηση ότι δε μπορεί να βρεθεί εναλλακτικό μήνυμα που να κατακερματίζεται στην ίδια τιμή με ένα δεδομένο μήνυμα. Αυτό παρεμποδίζει την πλαστογραφία όταν χρησιμοποιείται κρυπτογραφημένος κώδικας κατακερματισμού.

5. Είναι υπολογιστικά αδύνατο να βρεθεί ζεύγος *(x, y)* τέτοιο ώστε *H(x) = H(y).* Αυτή ιδιότητα είναι γνωστή ως ισχυρή αντίσταση σε συγκρούσεις (strong collision resistance). Η ιδιότητα αυτή σχετίζεται με το πόσο ανθεκτική είναι η συνάρτηση κατακερματισμού απέναντι σε έναν τύπο επίθεσης, γνωστός και ως επίθεση γενεθλίων.

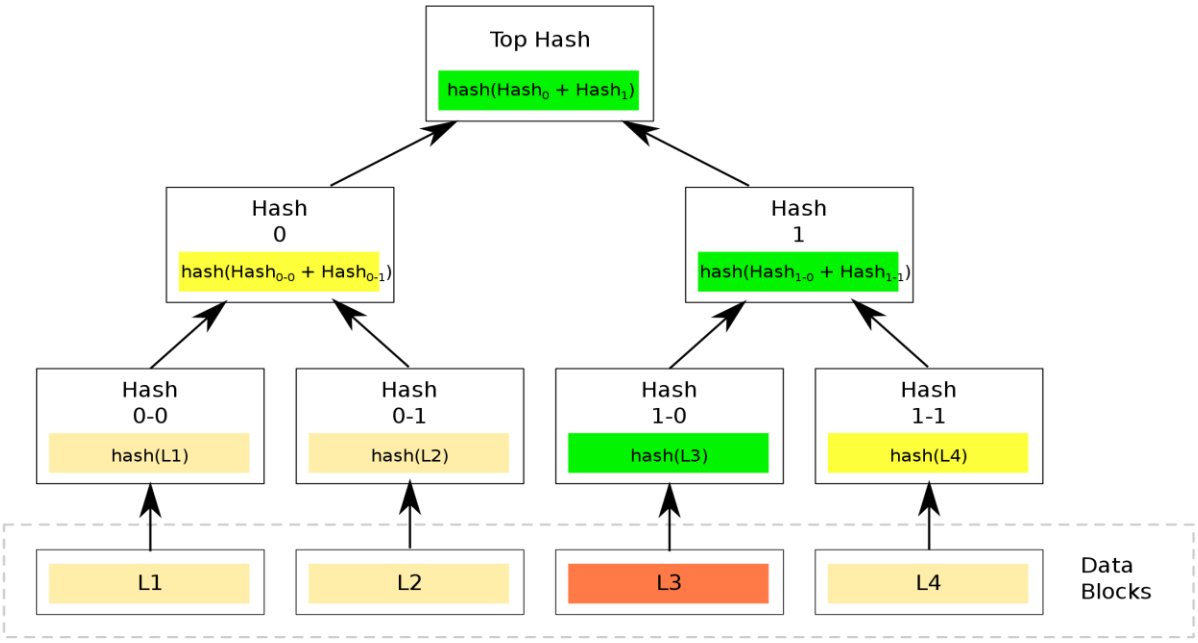
Εικόνα 3.3.1 : Έχουμε ως είσοδο τρία μηνύματα – κλειδιά τυχαίου μεγέθους. Καθένα από αυτά εφαρμόζεται σε μία συνάρτηση κατακερματισμού η οποία μετατρέπει το μήνυμα σε μία αναπαράσταση σταθερού μήκους. Παρατηρείται ότι όσο μεγάλο κι αν είναι το μέγεθος της εισόδου, στο τέλος θα προκύψει ένα σταθερό μέγεθος, γεγονός το οποίο κάνει τις συναρτήσεις κατακερματισμού τόσο αποδοτικές.

3.3.2 Μέθοδος Merkle Trees

Η ιστορία των Merkle Trees ξεκινάει το 1979 όταν ο ειδικός υπολογιστών Ralph Merkle δημοσίευσε ένα επιστημονικό άρθρο με το όνομα "A Certified Digital Signature" στο οποίο περιέγραφε μία νέα αποτελεσματική μέθοδο για τη διαδικασία επαλήθευσης των δεδομένων. Η ιδέα αυτή, έφερε την επανάσταση στον χώρο της κρυπτογραφίας και κατ' επέκταση στον τρόπο λειτουργίας των κρυπτογραφημένων πρωτοκόλλων. Τα Merkle Trees χρησιμοποιούνται εκτεταμένα στο Bitcoin που εισήγαγε ο Satoshi Nakamoto στον κόσμο, και επομένως στον μηχανισμό Blockchain.

Κάθε συναλλαγή που καταγράφεται σε κάποιο μπλοκ της αλυσίδας έχει τη μοναδική της αναγνωριστική ταυτότητα-τιμή (ID). Για τους περισσότερους μηχανισμούς Blockchain, η τιμή αυτή είναι ένας κωδικός 64 χαρακτήρων που καταλαμβάνει μνήμη 256 bits (32 bytes). Από τη στιγμή που μία αλυσίδα Blockchain αποτελείται από χιλιάδες μπλοκ και καθένα από αυτά περιλαμβάνει τεράστιο πλήθος συναλλαγών, ο χώρος μνήμης γίνεται γρήγορα πρόβλημα. Για το λόγο αυτό, η βελτιστοποίηση στο κομμάτι αυτό είναι απαραίτητη. Η χρήση όσο το δυνατόν λιγότερων δεδομένων κατά την επεξεργασία και την επαλήθευση των συναλλαγών, ελαχιστοποιεί το χρόνο επεξεργασίας της ενώ παράλληλα εξασφαλίζει υψηλότερο επίπεδο ασφάλειας. Η δομή των Merkle Trees έρχεται να δώσει τη λύση σε αυτό. Στην ουσία, τα Merkle Trees λαμβάνουν έναν τεράστιο αριθμό αναγνωριστικών τιμών οι οποίες είναι σχετικές με τις συναλλαγές και μέσα από μία μαθηματική διαδικασία καταλήγουν σε ένα μόνο κωδικό 64 χαρακτήρων. Ο κωδικός αυτός είναι εξαιρετικά σημαντικός, αφού επιτρέπει σε οποιονδήποτε υπολογιστή να επαληθεύει γρήγορα και αποτελεσματικά ότι μία συγκεκριμένη συναλλαγή πραγματοποιήθηκε σε ένα συγκεκριμένο μπλοκ μέσω μόνο μίας τιμής που ονομάζεται Merkle Root [35].

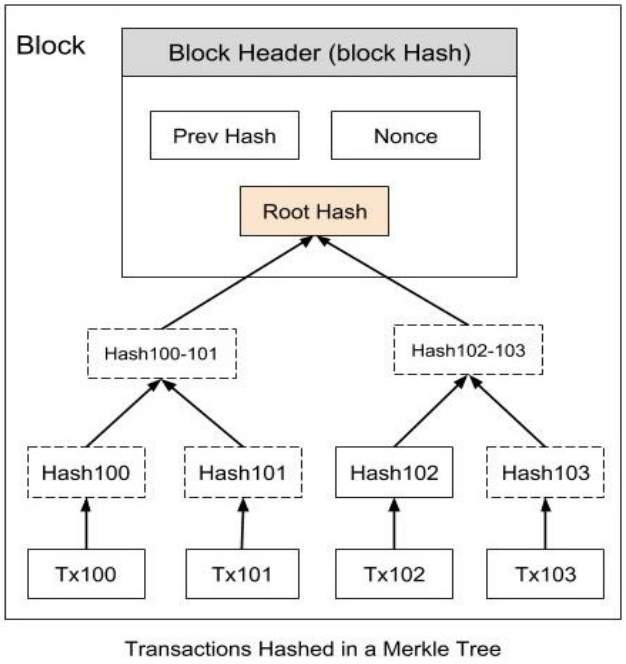
Ένα Merkle Tree είναι ένα δυαδικό δέντρο του οποίου κάθε κόμβος αναγράφει μία κατακερματισμένη τιμή. Το δέντρο αποτελείται από τους κόμβους – φύλλα, τους κόμβους – γονείς και τη ρίζα. Οι κόμβοι – φύλλα φέρουν μία ετικέτα με την τιμή κάθε συναλλαγής που πραγματοποιείται στο μπλοκ. Οι τιμές εισόδου ομαδοποιούνται σε ζεύγη και κάθε κόμβος του δέντρου που δεν είναι φύλλο και έχει δύο παιδιά, περιλαμβάνει τις τιμές των παιδιών του. Ο συνδυασμός των δύο τιμών θα περάσει από μία συνάρτηση κατακερματισμού ώστε να προκύψει μία νέα τιμή η οποία θα αναγράφεται πλέον στον κόμβο – γονέα. Στη συνέχεια, η διαδικασία θα επαναληφθεί με τις νέες τιμές να ομαδοποιούνται εκ νέου σε ζεύγη και μέσα από την μαθηματική συνάρτηση να προκύπτουν οι τιμές των επόμενων κόμβων – γονέων. Τελικά, μέσα από όλη αυτή την πορεία, δημιουργείται μία μοναδική τιμή, η ρίζα του Merkle Tree, που είναι αυτή που θα καθορίσει κιόλας το σύνολο των συναλλαγών στο μπλοκ και θα επιτρέψει την αποτελεσματική επαλήθευση της πληροφορίας. Στην περίπτωση που υπάρχει περιττός αριθμός εισόδων, δηλαδή συναλλαγών, τότε η τελευταία από αυτές αντιγράφεται και στη συνέχεια ζευγαρώνεται με τον εαυτό της [36].



Εικόνα 3.3.2.α : Αναπαράσταση ενός Merkle Tree με τους κόμβους – φύλλα και τις τιμές τους να φαίνονται στο τελευταίο επίπεδο και την Merkle Root στο πρώτο επίπεδο (Top Hash).

Παρά το γεγονός ότι το Bitcoin ήταν η πρώτη εφαρμογή των Merkle Trees, υπάρχουν πολλές άλλες διαφοροποιήσεις και πολύπλοκες εκδόσεις αυτών οι οποίες έχουν προταθεί κατά καιρούς. Για παράδειγμα, το Ethereum, που είναι το πιο αναγνωρίσιμο κρυπτονόμισμα, είναι ένα εξαιρετικό παράδειγμα διαφορετικής υλοποίησης των Merkle Trees.

Με την χρήση των Merkle Trees, μειώνεται σημαντικά ο χρόνος που απαιτείται για να διαπιστωθεί αν μία συναλλαγή βρίσκεται σε κάποιο συγκεκριμένο μπλοκ. Η διαδικασία αναζήτησης μίας πληροφορίας σε ολόκληρη τη βάση δεδομένων μέσω της ρίζας, γίνεται πολύ πιο ανώδυνα. Επιπλέον, ένα από τα σημαντικότερα οφέλη είναι η δυνατότητα διανομής μεγάλου όγκου δεδομένων σε μικρότερα διαχειρίσιμα τμήματα, ενώ το εμπόδιο επαλήθευσης της ακεραιότητας του περιεχομένου εξαλείφεται παρά το μέγεθος του όγκου. Τα Merkle Trees αποτελούν αναπόσπαστο κομμάτι του μηχανισμού Blockchain και των δικτύων ομότιμων κόμβων (Peer – to – Peer) με καθοριστικό ρόλο στον έλεγχο της αυθεντικότητας των δεδομένων. Η κατανόηση του τρόπου λειτουργίας τους και της τεχνολογίας τους είναι ζωτικής σημασίας και αποτελεί σκαλοπάτι για την ολοένα καλύτερη αντίληψη στον τομέα των κρυπτονομισμάτων, καθώς αυτά συνεχίζουν να εξελίσσονται σε μεγαλύτερα και πιο σύνθετα συστήματα.



Εικόνα 3.3.2.β : Η δομή ενός Merkle Tree στο μπλοκ της αλυσίδας Blockchain.

3.3.3 Ψηφιακές Υπογραφές

Η ανάπτυξη του ψηφιακού κόσμου, έφερε την ανάγκη για τη δόμηση καναλιών διανομής τα οποία θα είναι ασφαλή με την ύπαρξη ταυτοποίησης από τα αρμόδια πρόσωπα η οποία θα είναι ισοδύναμη με αυτή της γραπτής υπογραφής. Τελικά η εξέλιξη στην επιστήμη υπολογιστών υπόσχεται πολλές δυνατότητες στη θεωρία των κρυπτοσυστημάτων, μεταβάλλοντας την απαρχαιωμένη αυτή τέχνη, σε σύγχρονη επιστήμη.

Το 1976, ο Whitfield Diffie και ο Martin Hellman στο δημοσίευμά τους “New Directions in Cryptography”, παρουσίασαν για πρώτη φορά την ιδέα των ψηφιακών υπογραφών. Αργότερα, οι Ronald Rivest, Adi Shamir και Len Adleman εφηύραν τον αλγόριθμο RSA στον οποίο χρησιμοποιήθηκαν οι ψηφιακές υπογραφές. Η τεχνική αυτή όμως, αποδείχτηκε ότι δεν ήταν ασφαλής. Το πιο ευρέως γνωστό λογισμικό που χρησιμοποίησε ψηφιακές υπογραφές ήταν το Lotus Notes 1.0, που κυκλοφόρησε το 1989 [17] [18].

Μία ψηφιακή υπογραφή είναι μία μαθηματική τεχνική που χρησιμοποιείται για την επικύρωση της γνησιότητας και της ακεραιότητας ενός μηνύματος, λογισμικού ή

ψηφιακού έγγραφου. Είναι ένα "ηλεκτρονικό δακτυλικό αποτύπωμα" το οποίο πιστοποιεί το έγγραφο από τον αποστολέα και διασφαλίζει ότι θα παραμείνει αναλλοίωτο κατά την άφιξή του στον παραλήπτη. Λειτουργώντας ως ένα ψηφιακό ισοδύναμο χειρόγραφης υπογραφής ή σφραγίδας, η ψηφιακή υπογραφή προσφέρει πιο εγγενή ασφάλεια και προορίζεται να λύσει το πρόβλημα της παραβίασης και της πλαστοπροσωπίας στις ψηφιακές επικοινωνίες. Αποτελεί μία εξαιρετικά σημαντική εξέλιξη στην ιστορία της κρυπτογραφίας δημοσίου κλειδιού και παρέχει ένα σύνολο χαρακτηριστικών ασφαλείας που θα ήταν δύσκολο να υλοποιηθούν διαφορετικά. Η ψηφιακή υπογραφή διαθέτει συγκεκριμένες ιδιότητες, όπως ακριβώς γίνεται και στη χειρόγραφη υπογραφή :

- Πιστοποιεί τον υπογράφοντα αλλά και την ημερομηνία και ώρα της υπογραφής.
- Αυθεντικοποιεί τα δεδομένα κατά τη στιγμή της υπογραφής.
- Είναι επαληθεύσιμη από τρίτους, προκειμένου να μην υπάρχουν αμφισβητήσεις.

Αυτές επιτρέπουν την επίτευξη εμπιστοσύνης μεταξύ του αποστολέα και του παραλήπτη εξασφαλίζοντας την ασφάλεια και ακεραιότητα των ηλεκτρονικών δεδομένων. [19] [64]

Σχετικά με τον τρόπο λειτουργίας τους, οι ψηφιακές υπογραφές βασίζονται στην κρυπτογραφία δημοσίου κλειδιού, γνωστή και ως ασύμμετρη κρυπτογραφία. Χρησιμοποιώντας έναν αλγόριθμο δημοσίου κλειδιού, δημιουργούνται δύο κλειδιά τα οποία είναι μαθηματικά συνδεδεμένα, ένα δημόσιο και ένα ιδιωτικό. Τα δύο κρυπτογραφικά κλειδιά ελέγχουν την προέλευση της υπογραφής. Το άτομο που δημιουργεί την ψηφιακή υπογραφή χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την κρυπτογράφηση των σχετικών με την υπογραφή δεδομένων. Ο μόνος τρόπος αποκρυπτογράφησης των δεδομένων είναι με το δημόσιο κλειδί. Έτσι και επαληθεύονται. Η επιτυχία του μηχανισμού, βασίζεται στο γεγονός ότι η γνώση του δημοσίου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης. Η υπογραφή σημειώνεται, επίσης, με την ώρα υπογραφής του εγγράφου. Αν το έγγραφο αλλάξει μετά την υπογραφή, τότε εκείνη ακυρώνεται [20] [21].

Υπάρχουν τρεις βασικές λειτουργίες στις οποίες βασίζεται ο συγκεκριμένος μηχανισμός. Αρχικά, ο αλγόριθμος δημοσίου κλειδιού ο οποίος κατασκευάζει ένα ιδιωτικό και ένα δημόσιο κλειδί. Με το ιδιωτικό κλειδί δημιουργείται η ψηφιακή υπογραφή, ενώ με το δημόσιο ελέγχεται. Ακόμα, ο αλγόριθμος για την προσθήκη της υπογραφής σε κάποιο έγγραφο, αξιοποιώντας το ιδιωτικό κλειδί το οποίο ανήκει μόνο στον υπογράφοντα. Τέλος, ο αλγόριθμος για τον έλεγχο της υπογραφής, στον οποίο χρησιμοποιείται το δημόσιο κλειδί και ελέγχεται η αυθεντικότητα και η ακεραιότητα του εγγράφου. Επιπλέον, αξιοσημείωτο ρόλο έχει και η συνάρτηση κατακερματισμού, συγκεκριμένα μονόδρομη συνάρτηση κατακερματισμού, που θα συμπεριληφθεί σε ολόκληρη τη διαδικασία [21].

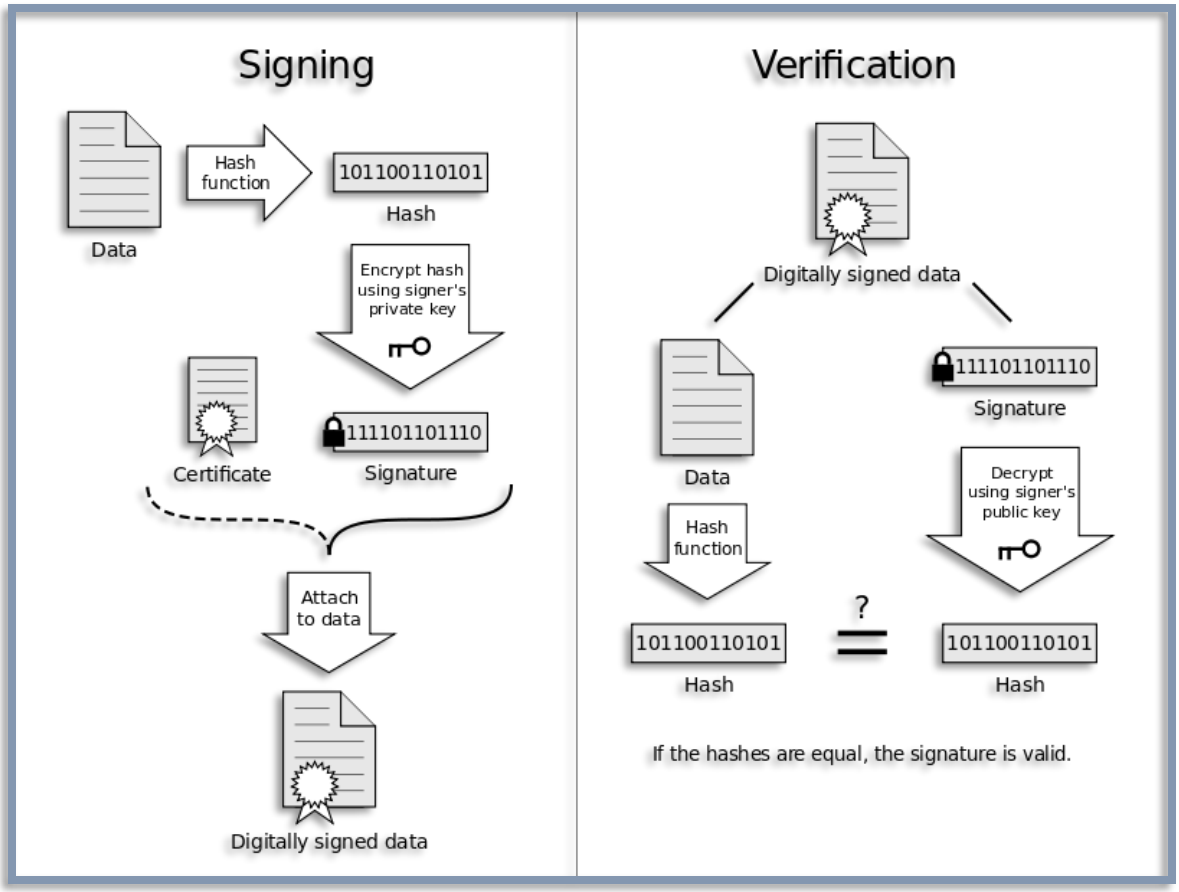
Αναλυτικότερα, τα άτομα που θα συμμετάσχουν στην μεταξύ τους επικοινωνία, επιλέγουν τα ίδια τον αλγόριθμο ασύμμετρης κρυπτογράφησης αλλά και την συνάρτηση κατακερματισμού που θα χρησιμοποιηθούν.

- **Αλγόριθμος Προσθήκης Υπογραφής**

Ο αποστολέας που επιθυμεί να επισυνάψει τα υπογεγραμμένα έγγραφα, αρχικά εφαρμόζει τη συνάρτηση κατακερματισμού επάνω στα έγγραφα αυτά, ώστε να μπορέσει να παράγει την τιμή κατακερματισμού ως αποτέλεσμα. Στη συνέχεια, η τιμή αυτή κρυπτογραφείται με βάση το ιδιωτικό κλειδί που έχει στην κατοχή του ο υπογράφοντας. Η κρυπτογραφημένη σύνοψη σε συνδυασμό με επιπρόσθετες πληροφορίες, αποτελούν τη ψηφιακή υπογραφή η οποία επισυνάπτεται με τα απαραίτητα δεδομένα και τελικά αποστέλλονται στον χρήστη που θα κάνει την επαλήθευση. Ο λόγος για τον οποίο γίνεται κρυπτογράφηση στην παραγόμενη κατακερματισμένη τιμή και όχι σε ολόκληρο το μήνυμα, είναι η ευελιξία που διαθέτει ο αλγόριθμος κατακερματισμού να μπορεί να μετατρέψει μία αυθαίρετη είσοδο σε μία τιμή σταθερού μήκους, η οποία είναι συνήθως αρκετά μικρότερη. Το χαρακτηριστικό αυτό, εξοικονομεί χρόνο καθώς αντί να υπογράφεται ένα μεγάλου μεγέθους μήνυμα, χρειάζεται να υπογραφεί μόνο μία σταθερού και μικρού μήκους τιμή.

- **Αλγόριθμος Ελέγχου Υπογραφής**

Ο χρήστης ο οποίος λαμβάνει τα δεδομένα με την ψηφιακή υπογραφή, θα πραγματοποιήσει έλεγχο αυτής. Χρησιμοποιώντας το δημόσιο κλειδί, θα αποκρυπτογραφήσει τη σύνοψη -κατακερματισμένη τιμή- του εγγράφου. Κατόπιν, θα περάσει το μήνυμα που παρέλαβε μαζί με την υπογραφή από τον αλγόριθμο κατακερματισμού, δημιουργώντας έτσι μία επιπλέον έξοδο. Συγκρίνοντας την έξοδο με την τιμή που δημιουργήθηκε από την αποκρυπτογράφηση, ελέγχεται η αυθεντικότητα της υπογραφής. Αν οι δύο τιμές εξόδου είναι ίδιες, τότε η υπογραφή επικυρώνεται και πιστοποιεί ότι το αρχικό έγγραφο δεν έχει αλλοιωθεί. Εάν δεν υπάρχει αντιστοιχία μεταξύ τους, τότε το μήνυμα έχει παραποιηθεί ή η υπογραφή δημιουργήθηκε από ένα ιδιωτικό κλειδί που δεν αντιστοιχεί στο δημόσιο κλειδί που παρουσιάστηκε από τον υπογράφοντα.



Εικόνα 3.3.3 : Διάγραμμα μηχανισμού της ψηφιακής υπογραφής. Περιλαμβάνει τη σχεδίαση της υπογραφής και την επαλήθευσή της.

Η τεχνολογία ψηφιακών υπογραφών απαιτεί από όλα τα συμβαλλόμενα μέρη να εμπιστεύονται ότι το άτομο που δημιουργεί την υπογραφή έχει κατορθώσει να κρατήσει μυστικό το ιδιωτικό κλειδί. Διαφορετικά οποιαδήποτε άλλη πρόσβαση στο κλειδί, αυξάνει την πιθανότητα δημιουργίας ψευδών υπογραφών. Για την προστασία της ακεραιότητας της ψηφιακής υπογραφής, απαιτείται η δημιουργία των κλειδιών να γίνεται με έναν ασφαλή τρόπο. Η ύπαρξη του Πάροχου Υπηρεσιών Πιστοποίησης (Certificate Authority) δίνει τη λύση σε αυτό το πρόβλημα. Η συγκεκριμένη υπηρεσία είναι ένας οργανισμός, ο οποίος πιστοποιεί τη σχέση ενός χρήστη με το δημόσιο κλειδί του και θα πρέπει να εμπνέει εμπιστοσύνη. Πολλές φορές, μαζί με τα έγγραφα και την ψηφιακή υπογραφή, επισυνάπτεται και ένα ψηφιακό πιστοποιητικό του δημόσιου κλειδιού.

Οι βιομηχανίες χρησιμοποιούν την τεχνολογία αυτή για τη βελτιστοποίηση των διαδικασιών και την βελτίωση της ακεραιότητας των εγγράφων. Σε αυτές ανήκουν ο

κυβερνοχώρος, ο ιατρικός τομέας, ο κατασκευαστικός τομέας αλλά και ο χρηματοοικονομικός κλάδος. Οι εφαρμογές επεκτείνονται με τα περισσότερα σύγχρονα προγράμματα ηλεκτρονικού ταχυδρομείου να υποστηρίζουν τη χρήση ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών, καθιστώντας εύκολη την υπογραφή εξερχόμενων μηνυμάτων και την επικύρωση ψηφιακά υπογεγραμμένων εισερχόμενων μηνυμάτων. Οι ψηφιακές υπογραφές χρησιμοποιούνται, επίσης, εκτεταμένα για να αποδείξουν την αυθεντικότητα και την ακεραιότητα δεδομένων σχετικών με τις επικοινωνίες και τις συναλλαγές που εκτελούνται μέσω του διαδικτύου.

4

Αρχιτεκτονική του μηχανισμού Blockchain

Η τεχνολογία Blockchain, όπως προαναφέρθηκε, είναι μία αλληλουχία από μπλοκ, τα οποία συνδέονται μεταξύ τους και καταγράφουν μία σειρά από δεδομένα. Η αρχιτεκτονική της βασίζεται σε συγκεκριμένα χαρακτηριστικά. Αποτελείται από τα μπλοκ τα οποία έχουν μία συγκεκριμένη δομή και βασίζεται σε λειτουργίες, όπως είναι για παράδειγμα η δημιουργία των μπλοκ και το πρωτόκολλο συναίνεσης, οι οποίες διασφαλίζουν την αυθεντικότητα της πληροφορίας.

Εικόνα 4 : Παράδειγμα μιας αλυσίδας Blockchain με τα μπλοκ να συνδέονται μεταξύ τους με χρονολογική σειρά

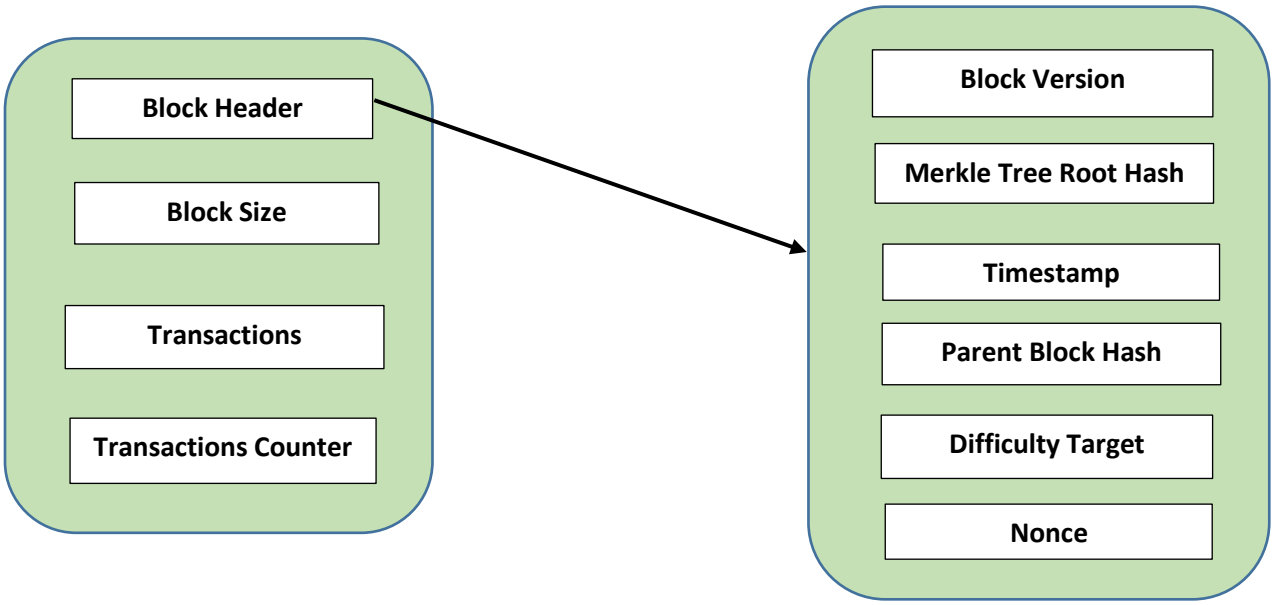
4.1 Η Δομή του Μπλοκ

Τα μπλοκ είναι δομές δεδομένων τα οποία έχουν σκοπό να καταγράψουν σύνολα συναλλαγών και να διανείμουν τις πληροφορίες σε όλους τους κόμβους του δικτύου Blockchain. Οι δομές αυτές είναι μεταξύ τους συνδεδεμένες, καθιστώντας σχεδόν αδύνατη οποιαδήποτε μεταβολή στα εσωτερικά τους δεδομένα. Η εσωτερική δομή ενός μπλοκ

αποτελείται από την επικεφαλίδα του (block header) και το σώμα του (block body). Πιο αναλυτικά η επικεφαλίδα του μπλοκ περιλαμβάνει τα παρακάτω μέρη:

1. Block Version
Περιλαμβάνει την έκδοση του μπλοκ και υποδεικνύει ποιοι κανόνες πρέπει να ακολουθούνται για την επικύρωση ενός μπλοκ.
2. Merkle Tree Root Hash
Είναι η κρυπτογραφημένη τιμή που προκύπτει από την εφαρμογή της συνάρτησης κατακερματισμού σε όλες τις συναλλαγές που περιέχονται στο μπλοκ.
3. Timestamp
Περιλαμβάνει το χρόνο, σε παγκόσμια μονάδα δευτερολέπτου, κατά τον οποίο δημιουργήθηκε το μπλοκ.
4. Parent Block Hash
Αποτελεί την κατακερματισμένη τιμή, δηλαδή τη Hash τιμή, του προηγούμενου μπλοκ.
5. Difficulty Target
Η δυσκολία που απαιτείται για να επικυρωθεί το συγκεκριμένο μπλοκ.
6. Nonce
Ένας ακέραιος τυχαίος αριθμός ο οποίος χρησιμοποιείται από τον αλγόριθμο “Proof-Of-Work” και μεταβάλλεται κατά τη διαδικασία της “εξόρυξης”.

Το σώμα του μπλοκ αποτελείται από τον **μετρητή των συναλλαγών** (Transaction Counter) και τις **συναλλαγές** (Transactions). Ο μετρητής συναλλαγών είναι ο συνολικός αριθμός των καταχωρήσεων που πραγματοποιούνται μέσα στο μπλοκ. Ο μέγιστος αριθμός συναλλαγών εξαρτάται από το **μέγεθος του μπλοκ** (block size) και το μέγεθος της κάθε συναλλαγής. Το μέγεθος κάθε μπλοκ εξαρτάται από το είδος της εφαρμογής που χρησιμοποιείται [23].



Εικόνα 4.1 : Η εσωτερική δομή του μπλοκ

4.2 Η σύνδεση των μπλοκ μεταξύ τους

Όλα τα μπλοκ στην αλυσίδα περιλαμβάνουν δεδομένα τα οποία κατοχυρώνονται με χρονολογική σειρά. Κάθε φορά που κατασκευάζεται ένα μπλοκ με συναλλαγές, υπολογίζεται η κατακερματισμένη τιμή τους μέσω των Merkle Trees. Η δομή δεδομένων αυτή, χρησιμοποιείται με σκοπό να παράγει μία μοναδική αναπαράσταση όλων των δεδομένων που είναι και η ρίζα του (Merkle Tree Root Hash), αποτελώντας μία αποτελεσματική διαδικασία για τον έλεγχο και την επαλήθευση των στοιχείων του μπλοκ. Στο πλαίσιο των κρυπτονομισμάτων και της τεχνολογίας Blockchain, ο αλγόριθμος κατακερματισμού που χρησιμοποιείται για τον υπολογισμό της τιμής Merkle Tree Root Hash, είναι ο Secure Hashing Algorithm 256 (SHA-256), ο οποίος παράγει μία αναπαράσταση μεγέθους 256-bits των συναλλαγών του αντίστοιχου μπλοκ. Οποιοδήποτε κι αν είναι το μέγεθος των δεδομένων, η έξοδος θα έχει πάντοτε μέγεθος 256-bits, γεγονός που παίζει σημαντικό ρόλο στην αποθήκευση μεγάλου όγκου δεδομένων και συναλλαγών.

Χωρίς να είναι απαραίτητη η απομνημόνευση άπειρων συναλλαγών, η σταθερού μεγέθους κατακερματισμένη τιμή τις αντικαθιστά, με αποτέλεσμα να "διαβάζονται" οι συναλλαγές μόνο μέσω αυτής. Είναι ένα μοναδικό ψηφιακό αποτύπωμα που προκύπτει σε κάθε μπλοκ που λόγω των ιδιοτήτων του, η πιθανότητα αποκρυπτογράφησης είναι μηδαμινή [25].

Κάθε μπλοκ, πέρα από τα χαρακτηριστικά που το καθορίζουν και τη δική του σύνοψη, περιλαμβάνει στην επικεφαλίδα του και την κατακερματισμένη τιμή του προηγούμενου μπλοκ. Με αυτόν τον τρόπο, συνδέονται τα μπλοκ μεταξύ τους δημιουργώντας την αναμενόμενη αλυσίδα. Στην περίπτωση που αλλάξει οποιοδήποτε δεδομένο, τότε θα πρέπει να αλλάξει και το μοναδικό αποτύπωμα που καθορίζει το μπλοκ. Όμως, άμα η κατακερματισμένη τιμή μεταβληθεί, τότε θα πρέπει αυτόματα να επαναπροσδιοριστεί και το πεδίο του επόμενου μπλοκ που περιέχει την τιμή του προηγούμενου μπλοκ. Τότε, το μπλοκ θα λάβει νέα τιμή, αλλάζοντας το πεδίο "Parent Block Hash" και του επόμενου μπλοκ, καταλήγοντας σε ένα ντόμινο που θα μεταβάλλει και θα αλλοιώσει ολόκληρη την αλυσίδα. Η ιδιότητα αυτή, συμβάλλει στη διατήρηση των πληροφοριών που υπάρχουν μέσα σε ένα μπλοκ. Αν και ισχυρή ιδιότητα, λόγω της εξελιγμένης σύγχρονης τεχνολογίας, από μόνη της δε δύναται να εξασφαλίσει την ασφάλεια της αλυσίδας και κατ' επέκταση των δεδομένων και των συναλλαγών. Για το λόγο αυτό, ο μηχανισμός του Blockchain, παρέχει και άλλα χαρακτηριστικά που εγγυώνται την ασφάλεια και την ακεραιότητα του περιεχομένου του και θα συζητηθούν παρακάτω [24] [25].

4.3 Δίκτυο Ομότιμων Κόμβων

Τα κυρίαρχα μοντέλα δικτυακών εφαρμογών είναι δύο :

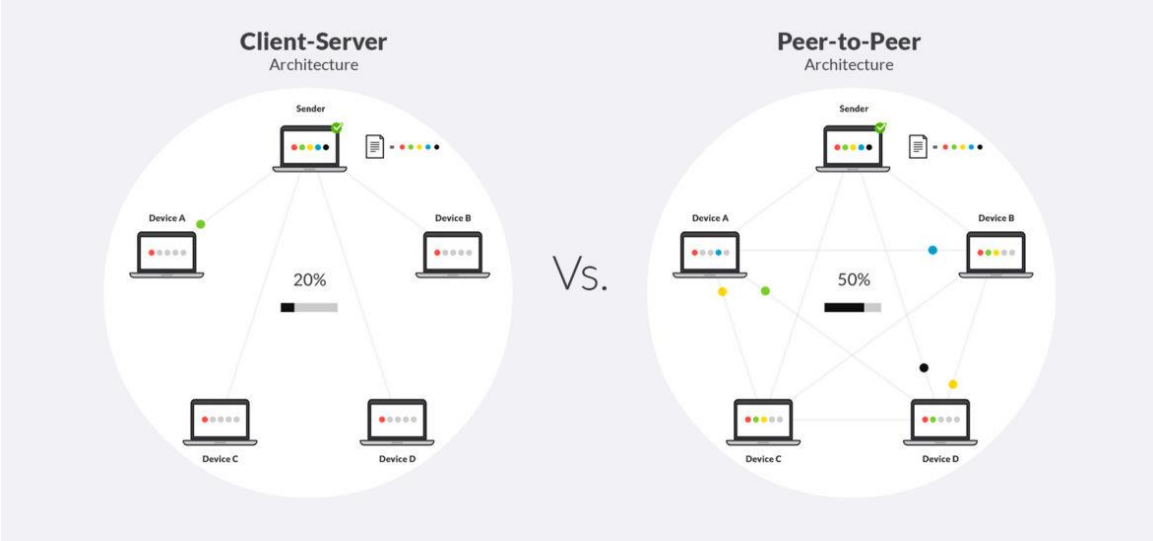
1. Η αρχιτεκτονική πελάτη – εξυπηρετητή (Client Server)
2. Η αρχιτεκτονική ομότιμων κόμβων (Peer – to – Peer / P2P)

Μέχρι σήμερα, το πιο συνηθισμένο μοντέλο πάνω στο οποίο εργάζονται τα δίκτυα υπολογιστών είναι αυτό του πελάτη–εξυπηρετητή ή διαφορετικά το κεντρικό μοντέλο. Στην αρχιτεκτονική αυτή, υπάρχουν κόμβοι-πελάτες οι οποίοι βασίζονται στον εξυπηρετητή για να τους προσφέρει συγκεκριμένες υπηρεσίες και εκείνος ανταποκρίνεται αναλόγως. Ο ρόλος του εξυπηρετητή, επομένως, είναι καθοριστικός για τη λειτουργία τέτοιου είδους δικτύων. Έχει όμως το αρνητικό ότι αν ο εξυπηρετητής αφαιρεθεί, τότε το δίκτυο καταρρέει.

Αντιθέτως, στο δίκτυο των ομότιμων κόμβων (P2P), οι συμμετέχοντες αποθηκεύουν και μοιράζονται συλλογικά τα αρχεία. Στην ουσία, ένα σύστημα P2P διατηρείται από ένα κατανεμημένο δίκτυο χρηστών όπου δεν υπάρχει κεντρικός διαχειριστής και όλοι οι κόμβοι έχουν την ίδια ισχύ και τα ίδια δικαιώματα να ενεργήσουν μέσα σε αυτό. Κάθε κόμβος κατέχει ένα αντίγραφο όλων των αρχείων, έχοντας τη δυνατότητα να πάρει τόσο το ρόλο του εξυπηρετητή όσο και το ρόλο του πελάτη, εξαλείφοντας την ανάγκη ύπαρξης διακομιστή. Όταν ένας κόμβος ενεργεί ως πελάτης, τότε μπορεί να έχει πρόσβαση σε πληροφορίες και σε αρχεία ενός άλλου συνδεδεμένου κόμβου. Όταν εργάζεται ως εξυπηρετητής, είναι η πηγή από την οποία οι υπόλοιποι κόμβοι λαμβάνουν δεδομένα. Στην πράξη, ωστόσο, και οι δύο λειτουργίες μπορούν να εκτελεστούν ταυτόχρονα. Μέσα στο σύστημα κυριαρχούν η ισοτιμία και η αυτονομία με τον κάθε κόμβο να έχει ενεργητικό ρόλο στη λήψη αποφάσεων. Η επικοινωνία και η συνεργασία μεταξύ τους βασίζεται σε αυστηρά καθορισμένους κανόνες οι οποίοι έχουν διαμορφωθεί από το πρωτόκολλο του συνεταιριστικού συστήματος. Οι κόμβοι μπορεί να διαφέρουν στην τοπική διαμόρφωση, στην ταχύτητα επεξεργασίας, στο εύρος ζώνης δικτύου και στην ποσότητα αποθήκευσης [27] [26].

Η αρχιτεκτονική P2P μπορεί να είναι το κατάλληλο μοντέλο για διάφορες περιπτώσεις χρήσεων, αλλά έγινε ιδιαίτερα δημοφιλής στη δεκαετία του 1990 όταν δημιουργήθηκαν τα πρώτα προγράμματα κοινής χρήσης αρχείων. Σήμερα, τα δίκτυα P2P βρίσκονται στον πυρήνα των περισσότερων κρυπτονομισμάτων, συνιστώντας ένα μεγάλο μέρος της βιομηχανίας Blockchain. Παρόλα αυτά, χρησιμοποιούνται επίσης σε άλλες κατανεμημένες εφαρμογές πληροφορικής συμπεριλαμβάνοντας τις μηχανές αναζήτησης σε ιστότοπους, ηλεκτρονικές αγορές και πρωτόκολλα. Περαιτέρω παραδείγματα εφαρμογών που βασίζονται στην αρχιτεκτονική P2P είναι η διανομή αρχείων (π.χ. BitTorrent), η τηλεφωνία διαδικτύου (π.χ. Skype), η υπηρεσία streaming μουσικής (π.χ. Napster).

Δεδομένου ότι κάθε κόμβος αποθηκεύει, μεταδίδει και λαμβάνει αρχεία, τα δίκτυα P2P τείνουν να είναι ταχύτερα και πιο αποδοτικά καθώς η βάση χρηστών τους μεγαλώνει. Επίσης, η κατανεμημένη αρχιτεκτονική τους καθιστά τα συστήματα πολύ ανθεκτικά στις επιθέσεις. Η τεχνολογία Blockchain που μελετάται βασίζεται στην αρχιτεκτονική ομότιμων κόμβων, έχοντας ως κύριο χαρακτηριστικό την απουσία κεντρικού διαχειριστή μέσα στο σύστημα. Δεν υπάρχει μεσάζοντας για την επεξεργασία και τη καταγραφή συναλλαγών μέσα στην αλυσίδα και έτσι το Blockchain λειτουργεί ως ένας ψηφιακός δίσκος που καταγράφει όλη τη δραστηριότητα. Μέσα στο πλαίσιο αυτό, οι συμμετέχοντες μπορούν να αναλάβουν διάφορους ρόλους. Οι πλήρεις κόμβοι διατηρούν ένα ενημερωμένο αντίγραφο του Blockchain και είναι αυτοί που παρέχουν ασφάλεια στο δίκτυο, ελέγχοντας τις συναλλαγές με τους κανόνες συναίνεσης του συστήματος.



Εικόνα 4.3 : Στην πρώτη εικόνα απεικονίζεται το μοντέλο πελάτη – εξυπηρετητή. Όλοι οι κόμβοι δίνουν εντολή στον κεντρικό διαχειριστή του συστήματος για να εξυπηρετηθούν. Αντιθέτως, στη δεύτερη εικόνα απεικονίζεται το μοντέλο ομότιμων κόμβων στο οποία όλοι οι κόμβοι έχουν το δικαίωμα και την αυτονομία να πράττουν αυτοβούλως.

Τα δίκτυα ομότιμων κόμβων μπορούν να κατηγοριοποιηθούν, με βάση την αρχιτεκτονική τους. Οι τρεις κύριοι τύποι στους οποίους διακρίνονται είναι τα μη δομημένα (unstructured), τα δομημένα (structured) και τα υβριδικά δίκτυα (hybrid).

4.3.1 Μη δομημένα δίκτυα ομότιμων κόμβων

Τα μη δομημένα δίκτυα δε παρουσιάζουν καμία συγκεκριμένη οργάνωση των κόμβων. Σχηματίζονται από κόμβους που τυχαία δημιουργούν συνδέσεις μεταξύ τους. Τα συστήματα αυτά θεωρούνται ισχυρά και ανθεκτικά έναντι υψηλής δραστηριότητας καταιγισμού, δηλαδή όταν αρκετοί κόμβοι συχνά εισέρχονται και εξέρχονται από το δίκτυο. Παραδείγματα που χρησιμοποιούν μη δομημένο δίκτυο ομότιμων κόμβων είναι η εφαρμογή Gnutella, Kazaa και το πρωτόκολλο Gossip. Σημαντικό πλεονέκτημα των δικτύων αυτών είναι η ευελιξία και ευκολία που έχουν να δομηθούν και να επιτρέψουν τοπικές βελτιστοποιήσεις σε διαφορετικές περιοχές της επικάλυψης. Παρά το πλεονέκτημα αυτό, η έλλειψη συγκεκριμένης δομής προκαλεί κάποιους περιορισμούς. Τα μη δομημένα δίκτυα ομότιμων κόμβων ενδέχεται να απαιτούν υψηλότερη χρήση μνήμης, καθώς τα ερωτήματα αναζήτησης δεδομένων αποστέλλονται στον μεγαλύτερο αριθμό κόμβων. Αυτό σημαίνει, πως όταν κάποιος κόμβος που συμμετέχει στο δίκτυο επιθυμεί την εύρεση συγκεκριμένης πληροφορίας, τότε το ερώτημα αναζήτησης αυτής της

πληροφορίας θα πρέπει να κατακλυστεί μέσω του δικτύου ώστε να βρεθούν όσο το δυνατόν περισσότεροι χρήστες που μοιράζονται αυτά τα δεδομένα. Η "πλημμύρα" προκαλεί πολύ υψηλό όγκο σηματοδοτικής κίνησης στο δίκτυο, χρησιμοποιώντας έτσι περισσότερη μνήμη. Επιπλέον δεδομένου ότι δεν υπάρχει συσχέτιση μεταξύ των κόμβων, δεν υπάρχει εγγύηση ότι μέσα σε αυτή την αναζήτηση, το ερώτημα θα φτάσει στον κόμβο που παρέχει τα επιθυμητά δεδομένα και επομένως δε διασφαλίζεται η εύρεση της πληροφορίας. Ειδικότερα, δεδομένα με δημοφιλές περιεχόμενο, είναι πιθανό να είναι διαθέσιμο σε αρκετούς κόμβους και με αποτέλεσμα η έρευνα να δημιουργεί έναν φαύλο κύκλο. Ακόμα, η αναζήτηση σπάνιων δεδομένων που μοιράζονται μόνο μερικοί κόμβοι, είναι πολύ σπάνιο να είναι επιτυχής [29].

4.3.2 Δομημένα δίκτυα ομότιμων κόμβων

Σε αντίθεση με τα μη δομημένα δίκτυα ομότιμων κόμβων, τα δομημένα δίκτυα παρουσιάζουν μία οργανωμένη αρχιτεκτονική, επιτρέποντας στους κόμβους να αναζητούν αποτελεσματικά αρχεία, ακόμα κι αν το περιεχόμενο τους δεν είναι ευρέως διαθέσιμο. Αυτό επιτυγχάνεται μέσω συναρτήσεων κατακερματισμού οι οποίες διευκολύνουν την αναζήτηση στις βάσεις δεδομένων. Ο πιο διαδεδομένος τύπος δομημένων δικτύων υλοποίει έναν κατανεμημένο πίνακα κατακερματισμού (DHT), στον οποίο χρησιμοποιείται μία παραλλαγή της "συνεπούς" συνάρτησης κατακερματισμού (consistent hashing), ώστε να επιτευχθεί η ανάθεση κάθε αρχείου σε έναν συγκεκριμένο κόμβο. Ως αποτέλεσμα, η αναζήτηση δεδομένων μέσα στο δίκτυο γίνεται πιο αποτελεσματική, αφού μπορούν να ανακτηθούν εύκολα με τη βοήθεια του πίνακα κατακερματισμού. Ωστόσο, για την ομαλή και σωστή λειτουργία του δικτύου, οι κόμβοι πρέπει να διατηρούν λίστες γειτόνων οι οποίοι πληρούν συγκεκριμένα κριτήρια. Εξαιτίας της ανάγκης αυτής, το δίκτυο καθίσταται περισσότερο ευάλωτο σε συνθήκες καταιγισμού, δηλαδή υψηλού ρυθμού σύνδεσης και αναχώρησης κόμβων. Επίσης, ενώ τα δομημένα δίκτυα φαίνεται να είναι πιο αποδοτικά, τείνουν να παρουσιάζουν υψηλότερο κόστος εγκατάστασης και συντήρησης. Μερικά από τα ερευνητικά έργα που αξιοποιούν αυτό το είδος δικτύου περιλαμβάνουν το Chord project, το Kademlia και το P-Grid [29].

4.3.3 Υβριδικά μοντέλα δικτύων

Τα υβριδικά μοντέλα δικτύων συνδυάζουν το μοντέλο πελάτη – εξυπηρετητή με ορισμένες πτυχές της αρχιτεκτονικής του δικτύου ομότιμων κόμβων. Για παράδειγμα, ένα σύνηθες υβριδικό μοντέλο είναι η σχεδίαση ενός κεντρικού διαχειριστή ώστε να διευκολύνεται η σύνδεση μεταξύ των κόμβων στο δίκτυο και να βοηθάει στην εύρεση αυτών. Υπάρχουν ποίκιλα μοντέλα τα οποία συνδυάζουν την λειτουργία μέσω κεντρικής μονάδας που παρέχεται από το δίκτυο πελάτη – εξυπηρετητή και την ισότητα μεταξύ των κόμβων που

συναντάται στο δίκτυο ομότιμων κόμβων. Σε σύγκριση με τις άλλες δύο κατηγορίες δικτύων, τα υβριδικά μοντέλα τείνουν να παρουσιάζουν βελτιωμένη συνολική απόδοση λόγω του ότι αξιοποιούν βασικά πλεονεκτήματα από τον συνδυασμό των δύο δικτύων. Ορισμένες λειτουργίες, όπως η αναζήτηση πληροφορίας, απαιτούν τη χρήση κεντρικού διακομιστή, αλλά επωφελούνται και από την αποκεντρωμένη δομή των κόμβων. Η ακριβής λειτουργία της αλυσίδας μπορεί να ποικίλει με βάση το ποια τμήματα είναι αποκεντρωμένα και ποια όχι [27] [28].

4.3.4 Πλεονεκτήματα του δικτύου ομότιμων κόμβων στην τεχνολογία Blockchain

Η αρχιτεκτονική ομότιμων κόμβων στην τεχνολογία Blockchain προσφέρει αρκετά οφέλη. Μεταξύ των πιο σημαντικών είναι ότι τα δίκτυα αυτά προσφέρουν μεγαλύτερη ασφάλεια από τα παραδοσιακά μοντέλα πελάτη – εξυπηρετητή. Η κατανομή μεγάλου αριθμού κόμβων στην αλυσίδα την καθιστά σχεδόν ακλόνητη από επιθέσεις Denial-of-Service (DoS) που πλήττει πολλά συστήματα.

Ομοίως, επειδή η πλειονότητα των κόμβων πρέπει να καταλήξει σε συναίνεση πριν προστεθούν δεδομένα στην αλυσίδα, είναι σχεδόν αδύνατο για έναν εισβολέα να αλλάξει αυτά τα δεδομένα. Αυτό ισχύει περισσότερο για μεγάλα δίκτυα στα οποία συμμετέχουν αρκετοί χρήστες. Ως αποτέλεσμα, το κατανεμημένο δίκτυο ομότιμων κόμβων σε συνδυασμό με την απαίτηση της συναινετικής πλειοψηφίας, δίνει στην τεχνολογία Blockchain έναν σχετικά υψηλό βαθμό αντοχής σε κακόβουλη δραστηριότητα.

Πέρα από την ασφάλεια που παρέχει η χρήση της αρχιτεκτονικής του κατανεμημένου δικτύου στον μηχανισμό Blockchain και του Bitcoin, τον καθιστούν ανθεκτικό στη λογοκρισία από τις κεντρικές αρχές. Για παράδειγμα, σε αντίθεση με τους τραπεζικούς λογαριασμούς, τα "ηλεκτρονικά πορτοφόλια" δε μπορούν να παγώσουν. Η αντίσταση αυτή επεκτείνεται ακόμα παραπάνω, ενώ πλέον δεν είναι αναγκαία η δέσμευση από κάποιο τρίτο πρόσωπο.

4.4 Εξόρυξη Μπλοκ (Mining)

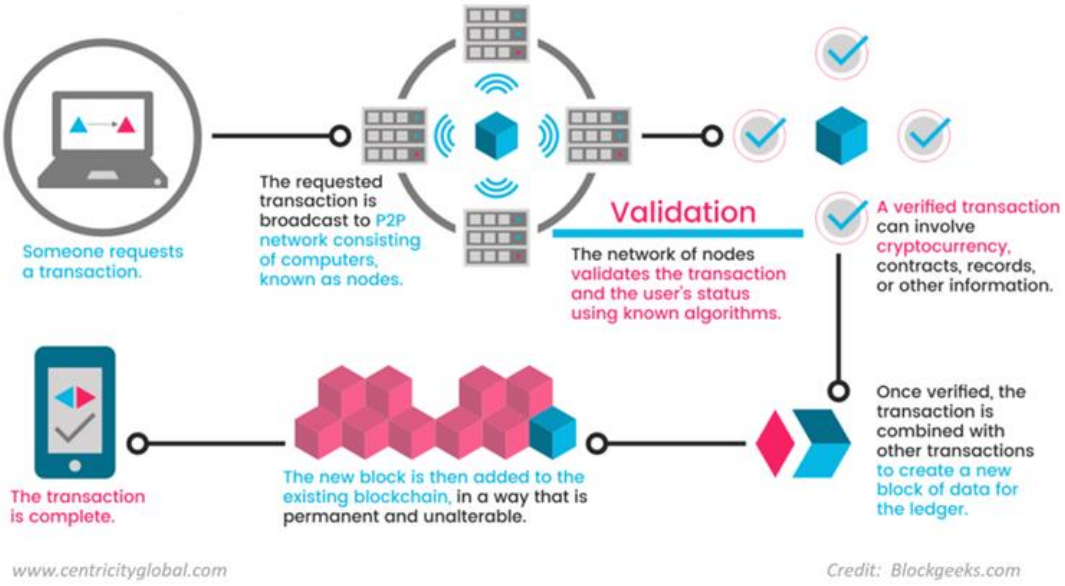
Η εξόρυξη είναι μία διαδικασία προσθήκης συναλλαγών και εγγραφών στο σύστημα του Blockchain. Στην ουσία δημιουργούνται επιπλέον μπλοκ μέσω της διαδικασίας. Ο πρωταρχικός σκοπός της εξόρυξης είναι να επιτρέψει στους χρήστες να φτάσουν σε μία ασφαλή και ανθεκτική στις παραβιάσεις συναίνεση. Οι κόμβοι που λαμβάνουν μέρος στην εξόρυξη ονομάζονται μεταλλωρύχοι (miners).

Ο μεταλλωρύχος είναι ο πλήρης κόμβος ο οποίος ομαδοποιεί τις συναλλαγές σε μπλοκ και συναγωνίζεται τους υπόλοιπους μεταλλωρύχους για το ποιος θα λύσει πιο γρήγορα ένα κρυπτογραφικό παζλ προκειμένου να προστεθεί το δικό του μπλοκ στην αλυσίδα. Εφόσον επιλέξει ποιες συναλλαγές επιθυμεί να εντάξει στο μπλοκ, τότε θα πρέπει να παράγει μία μοναδική κατακερματισμένη τιμή (hash) για το μπλοκ αυτό. Αυτό επιτυγχάνεται όταν ο μεταλλωρύχος μεταβάλλει μία τιμή nonce που περιέχεται στην επικεφαλίδα του μπλοκ μέχρι αυτή να γίνει μικρότερη από μία συγκεκριμένη τιμή στόχο (target) η οποία αναφέρθηκε και ως τιμή δυσκολίας (difficulty target). Ουσιαστικά θα πρέπει να λύσει την παρακάτω εξίσωση :

H(txs || nonce || parent block hash) < ε

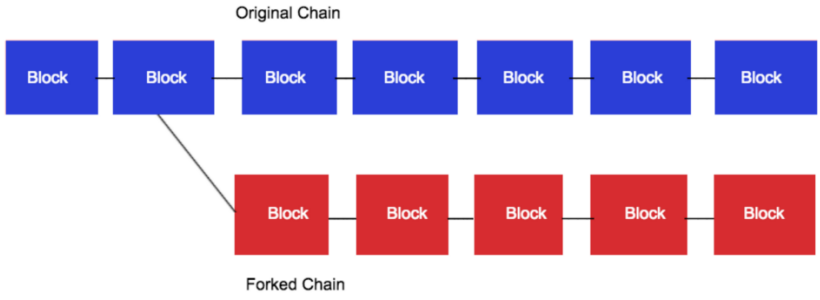
Η hash τιμή των έγκυρων μπλοκ ξεκινάει με ένα συγκεκριμένο πλήθος μηδενικών. Ο μεταλλωρύχος, μέσω μίας μαθηματικής διαδικασίας που ονομάζεται απόδειξη εργασίας, αλλάζει συνεχώς την παράμετρο Nonce μέχρι να κατασκευάσει την κατάλληλη hash τιμή με τον απαραίτητο αριθμό μηδενικών. Η τιμή Nonce είναι μία τυχαία τιμή μεγέθους 32 bits που οι μεταλλωρύχοι μεταβάλλουν συνεχώς ώστε να βρουν μία τιμή Hash που να ικανοποιεί την παραπάνω σχέση. Εκείνος που θα βρει πρώτος την τιμή για το μπλοκ, το δημοσιοποιεί στο δίκτυο με σκοπό να το ελέγξουν οι υπόλοιποι κόμβοι. Αν πράγματι είναι έγκυρο τότε η αλυσίδα ενημερώνεται και ο μεταλλωρύχος αμείβεται με κρυπτονομίσματα. Την παρούσα περίοδο το ποσό ανταμοιβής είναι 12,5 BTC. Με τον τρόπο αυτό, τελικά το δίκτυο πετυχαίνει συναίνεση (consensus).

Όσο η υπολογιστική ισχύς που επενδύεται σε κρυπτονομίσματα αυξάνεται, τόσο μεγαλύτερη γίνεται και η δυσκολία επίλυσης του κρυπτογραφικού παζλ ώστε να διατηρηθεί σταθερό το ποσοστό παραγωγής μπλοκ στην αλυσίδα. Όταν η αμοιβή είναι υψηλή, αξίζει για τους κόμβους να συμμετέχουν στην προσπάθεια της εξόρυξης, οδηγώντας σε υψηλό βαθμό δυσκολίας. Το γεγονός αυτό αποτρέπει από κάποιον κακόβουλο χρήστη την εκτέλεση σημαντικών επιθέσεων [39].



Εικόνα 4.4.α : Η διαδικασία της εξόρυξης ενός μπλοκ.

Στην περίπτωση που δημιουργηθούν δύο έγκυρα μπλοκ την ίδια χρονική στιγμή, τότε η κεντρική αλυσίδα Blockchain διαιρείται σε δύο ή περισσότερες αλυσίδες. Το φαινόμενο αυτό ονομάζεται **Fork**. Το fork δημιουργεί πρόβλημα στην αλυσίδα διότι δε μας επιτρέπει πλέον να έχουμε χρονολογική σειρά των μπλοκ. Αυτό λύνεται όταν προστεθούν μπλοκ στην αλυσίδα και κάποια από τις δύο διαιρούμενες γίνει μεγαλύτερη. Το δίκτυο δέχεται την αλυσίδα με το μεγαλύτερο μήκος. Αυτό οδηγεί στη συνέπεια μεταξύ των χρηστών του δικτύου.



Εικόνα 4.4.β : Το φαινόμενο Fork. Έχουν δημιουργηθεί δύο αλυσίδες από τις οποίες θα παραμείνει η μεγαλύτερη τελικά.

4.5 Μπλοκ Genesis

Το Genesis Μπλοκ (Block) είναι το πρώτο μπλοκ στην αλυσίδα του Blockchain. Είναι η βάση στην οποία προστίθενται μπλοκ για να σχηματίσουν την δομή της αλυσίδας. Είναι γνωστό και ως Block 0. Σε αντίθεση με τα υπόλοιπα μπλοκ, το πρώτο δεν περιλαμβάνει στην επικεφαλίδα του την τιμή hash του προηγούμενου μπλοκ καθώς δεν υπάρχει. Αυτή είναι προκαθορισμένη στο 0, δείχνοντας ότι δεν έχουν πραγματοποιηθεί προηγούμενες συναλλαγές πριν από το συγκεκριμένο μπλοκ.

Το πιο γνωστό Genesis Block μέχρι τώρα, είναι της αλυσίδας των κρυπτονομισμάτων Bitcoin, το οποίο κατασκεύασε ο Satoshi Nakamoto στις 3 Ιανουαρίου του 2009. Το μπλοκ αυτό είχε ανταμοιβή 50 BTC, η οποία όμως ήταν απρόσιτη. Δεν υπάρχει σαφής εξήγηση για την εξόρυξή του.

4.6 Πρωτόκολλα Συναίνεσης

Καθώς σε ένα δίκτυο που χρησιμοποιεί την τεχνολογία Blockchain, η κεντρική αρχή απουσιάζει με αποτέλεσμα να μην υπάρχει διαχειριστής ο οποίος να ελέγχει ποιες συναλλαγές θα καταγραφούν στην αλυσίδα, είναι αναγκαία η ύπαρξη ενός πρωτόκολλου συναίνεσης με βάση το οποίο οι συμμετέχοντες θα επαληθεύουν και θα εγκρίνουν συγκεκριμένες πληροφορίες προτού κατοχυρωθούν στο σύστημα. Έτσι επιτυγχάνεται η εμπιστοσύνη μεταξύ των αγνώστων κόμβων αλλά και η ακεραιότητα των δεδομένων. Το πρωτόκολλο συναίνεσης πρέπει να είναι ανθεκτικό σε οποιαδήποτε κακόβουλη ενέργεια. Τα δύο πιο ευρέως αξιοποιήσιμα πρωτόκολλα είναι η απόδειξη εργασίας (Proof – of – Work) και η απόδειξη στοιχήματος (Proof – of – Stake).

4.6.1 Proof – of – Work (PoW)

Ο αλγόριθμος Proof – of – Work έκανε για πρώτη φορά την εμφάνισή του το 1992 όταν ο ερευνητής Dwork παρουσίασε έναν μηχανισμό ασφάλειας ώστε να μειωθεί ο αριθμός των ανεπιθύμητων μηνυμάτων (spam) του ηλεκτρονικού ταχυδρομείου, καθιστώντας υπολογιστικά δύσκολη την ταυτόχρονη αποστολή πολλαπλών μηνυμάτων. Αυτό επιτυγχάνεται μέσω κρυπτογραφικών μεθόδων και συναρτήσεων κατακερματισμού, η χρήση των οποίων απαιτούσαν πολύπλοκους υπολογισμούς και κατανάλωση χρόνου, αποτρέποντας έτσι την αποστολή ανεπιθύμητων μηνυμάτων [30].

Αργότερα το 2002, χρησιμοποιήθηκε πάλι για την αποτροπή ανεπιθύμητης αλληλογραφίας αλλά με διαφορετική τεχνική. Με τη συνάρτηση κατακερματισμού SHA-1, το περιεχόμενο του μηνύματος, η χρονική του σφραγίδα, η διεύθυνση ηλεκτρονικού ταχυδρομείου του παραλήπτη αλλά και μία τιμή μετρητή επισυνάπτονται μέσα σε αυτή. Για τους χρήστες που επιθυμούν να κάνουν επίθεση με την αποστολή πολλαπλών ανεπιθύμητων μηνυμάτων, ο υπολογισμός των τιμών κατακερματισμού θα τους κοστίσει το χρόνο τους αλλά και ενέργεια, αποθαρρύνοντάς τους από το έργο αυτό [30].

Στη συνέχεια ο αλγόριθμος PoW εφαρμόστηκε από τον Satoshi Nakamoto στο Peer – to – Peer σύστημα ανταλλαγής κρυπτονομισμάτων Bitcoin, όπου οι συναλλαγές δεν απαιτούσαν την εμπλοκή τρίτου προσώπου. Είναι μία στρατηγική συναίνεσης για την προσθήκη συναλλαγών και την επέκταση της αλυσίδας των μπλοκ. Πριν την προσθήκη ενός μπλοκ στην αλυσίδα Blockchain, πρέπει να προηγηθεί η επικύρωση όλων των συναλλαγών του μπλοκ από τα πρόσωπα του δικτύου, κάτι που απαιτεί σύνθετους υπολογισμούς. Οι μεταλλωρύχοι πρέπει να εκτελέσουν και να λύσουν αυτούς τους υπολογισμούς προκειμένου να συμβάλλουν στην αλυσίδα. Ο πρώτος που θα φτάσει στην επίλυση του προκλητικού παζλ, θα είναι και εκείνος που θα δημιουργήσει το επόμενο μπλοκ στην αλυσίδα και θα ανταμειφθεί με έναν αριθμό κρυπτονομισμάτων.

Στην απόδειξη εργασίας, οι μεταλλωρύχοι πρέπει να συλλέξουν όλες τις εκκρεμείς συνναλαγές του νέου μπλοκ και να υπολογίσουν την κατακερματισμένη τιμή (Merkle Root) αυτών με τη χρήση του αλγορίθμου SHA-256, να συμπληρώσουν την τρέχουσα έκδοση του μπλοκ και την κατακερματισμένη τιμή του προηγούμενου μπλοκ. Όλα αυτά συνδυάζονται με μία τιμή Nonce η οποία μεταβάλλεται προκειμένου να βρεθεί η κατάλληλη κατακερματισμένη τιμή του μπλοκ. Αυτή συμπληρώνεται στην επικεφαλίδα του μπλοκ και μεταδίδεται στους υπόλοιπους κόμβους ώστε να γίνει επαλήθευση. Η διαδικασία εξόρυξης σταματάει και ελέγχεται η εγκυρότητα του μπλοκ. Μόλις αυτή γίνει δεκτή, το μπλοκ προστίθεται στο τέλος της αλυσίδας και ο μεταλλωρύχος λαμβάνει κρυπτονομίσματα ως επιβράβευση [31] [32].

Η διαδικασία επαλήθευσης των συναλλαγών στο μπλοκ που θα προστεθεί, η οργάνωση αυτών με χρονολογική σειρά στο μπλοκ, η ενημέρωση ολόκληρου του δικτύου για τη νέα προσθήκη δεν απαιτούν πολύ χρόνο και ενέργεια. Το μέρος που καταναλώνει την περισσότερη ενέργεια είναι η επίλυση του μαθηματικού παζλ ώστε να εγκριθεί και να προστεθεί το μπλοκ στην αλυσίδα [31].

Η δυσκολία επίλυσης του μαθηματικού προβλήματος μπορεί να μεταβάλλεται ανάλογα την ισχύ των μεταλλωρύχων. Αν αυτοί αυξηθούν στο δίκτυο με αποτέλεσμα να αυξηθεί η υπολογιστική τους δύναμη και τα μπλοκ να δημιουργούνται πιο γρήγορα, τότε αυξάνεται

και η δυσκολία. Ο αλγόριθμος βασίζεται στην αρχή ότι καμία οντότητα δε πρέπει να κατέχει περισσότερο από το 50% της συνολικής υπολογιστικής δύναμης, καθώς μία τέτοια οντότητα θα έχει τη δυνατότητα να ελέγχει αποτελεσματικά το σύστημα. Έτσι, προκειμένου κάποιος να επηρεάσει σε αρνητικό επίπεδο το δίκτυο, χρειάζεται να καταλάβει το 51% αυτής. Αυτή είναι η λεγόμενη 51% επίθεση. Βέβαια, όταν διαχειρίζεται το δίκτυο ένας μεγάλος αριθμός χρηστών, τότε αυτό είναι σχεδόν ακατόρθωτο. Όσο μεγαλύτερο είναι το δίκτυο, τόσο πιο ανθεκτικό είναι σε τέτοιου είδους επιθέσεις [34].

Στον αλγόριθμο συναίνεσης PoW και στη διαδικασία εξόρυξης υπάρχει η δυνατότητα να λάβει μέρος οποιοσδήποτε επιθυμεί και λειτουργεί σαν ένα ανοιχτό περιβάλλον. Κατά συνέπεια, δεν απαιτείται καμία γνώση ή πιστοποίηση από τους συμμετέχοντες, κλιμακώνοντας αυτό το μοντέλο με την υποστήριξη χιλιάδων κόμβων. Ωστόσο, όπως αναφέρθηκε, είναι σχετικά ευάλωτο σε επιθέσεις 51% όπου ένας μεταλλωρύχος μπορεί να ανακτήσει το 51% της υπολογιστικής δύναμης του δικτύου. Το πλεονέκτημά για τον εισβολέα είναι ότι μπορεί να διπλασιάσει τα δικά του κεφάλαια και να απορρίψει επιλεκτικά τις συναλλαγές που δεν επιθυμεί να συμπεριλαμβάνονται στο μπλοκ.

Μία άλλη έρευνα αποδεικνύει ότι ένας νέος τύπος επίθεσης κάνει την εμφάνισή του, γνωστός και ως εγωιστική εξόρυξη (selfish mining). Στην επίθεση αυτή, οι "ειλικρινείς" μεταλλωρύχοι βρίσκουν κίνητρο να υποστηρίξουν τους εισβολείς, και να συμμετάσχουν στην υλοποίηση μίας 51% επίθεσης. Ο επιτιθέμενος εκτελεί ακανόνιστη εξόρυξη, διατηρώντας μία ξεχωριστή αλυσίδα Blockchain. Δημοσιεύει επιλεκτικά πολλά μπλοκ, αναγκάζοντας το υπόλοιπο δίκτυο να απορρίψει τα δικά του και τελικά να χάσει έσοδα. Αυτό ενθαρρύνει τους "ειλικρινείς" μεταλλωρύχους να ενταχθούν με την πλευρά των εισβολέων, αυξάνοντας τα κέρδη τους τα οποία μπορεί να φτάσουν το 51% της εξόρυξης.

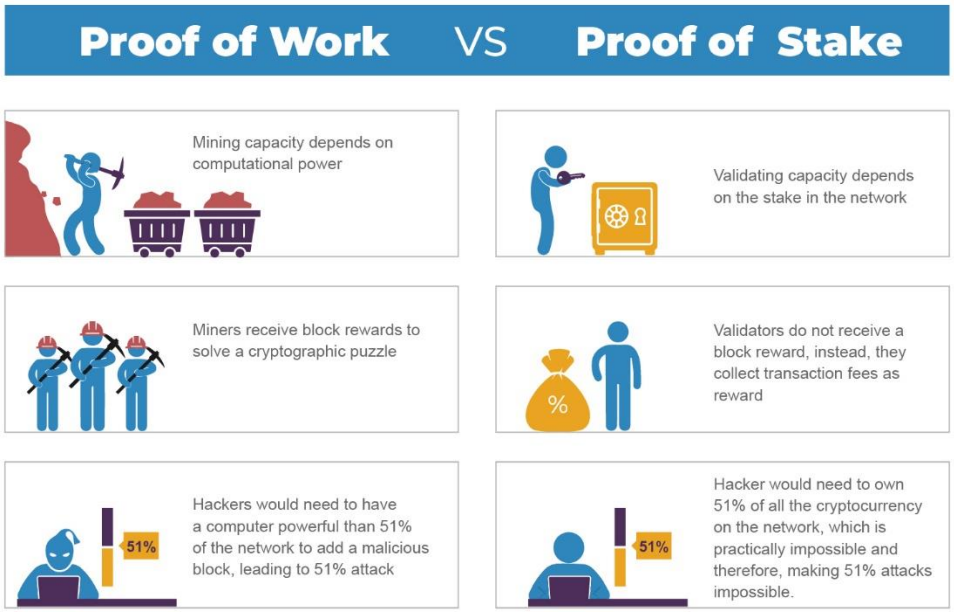
4.6.2 Proof – of – Stake (PoS)

Για την εξάλειψη της μεγάλης ποσότητας ενέργειας που καταναλώνει ο αλγόριθμος Proof – of – Work, το 2011 προτάθηκε η εναλλακτική λύση του αλγορίθμου Proof – of – Stake. Αν και οι δύο αλγόριθμοι μοιράζονται παρόμοιους στόχους, παρουσιάζουν κάποιες θεμελιώδεις διαφορές και ιδιαιτερότητες. Η εξόρυξη που πραγματοποιείται στο PoW αντικαθίσταται από έναν μηχανισμό όπου η επικύρωση των μπλοκ γίνεται με βάση το ποσό το οποίο θα στοιχηματίσουν οι υποψήφιοι. Επομένως, αντί οι μεταλλωρύχοι να επενδύσουν στην υπολογιστική ισχύ για να εξορύξουν ένα μπλοκ, διαθέτουν ένα ποσό ώστε να επιλεχθούν. Όσο μεγαλύτερο είναι το ποσό που θα στοιχηματίσει κάποιος, τόσες περισσότερες πιθανότητες έχει να επιλεχθεί για την εξόρυξη του μπλοκ.

Καθώς η επιλογή αυτή θεωρείται άδικη λόγω του ότι το πλουσιότερο άτομο επωφελείται και κυριαρχεί στο δίκτυο, υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να εφαρμοστεί ο αλγόριθμος. Ειδικότερα, στο Blockchain, εξετάζεται το χρηματικό ποσό του κόμβου και η ηλικία των νομισμάτων (ο αριθμός των ημερών που το χρηματικό ποσό έχει διατεθεί), σε συνδυασμό με έναν παράγοντα τυχαιοποίησης.

Σε σύγκριση με τον αλγόριθμο PoW, ο μηχανισμός του PoS, δεν καταναλώνει τόση ενέργεια και είναι πιο αποτελεσματική μέθοδος αλλά και φιλικό προς το περιβάλλον. Επιπλέον, εν αντιθέσει με την απόδειξη εργασίας (PoW) όπου οι ανθρακωρύχοι μπορούν να κατέχουν το 51% της χωρητικότητας του δικτύου, είναι δύσκολο έως και ακατόρθωτο για έναν χρήστη στο PoS να αποκτήσει το 51% των κρυπτονομισμάτων. Αυτό συμβαίνει επειδή στην περίπτωση αυτή η αξία του κρυπτονομίσματος θα έπεφτε. Κατά συνέπεια, ο αλγόριθμος PoS είναι πιο ασφαλής έναντι της 51% επίθεσης [30] [32].

Ωστόσο, το πρωτόκολλο αυτό δεν εμποδίζει τους κακόβουλους χρήστες από το να δημιουργήσουν μη έγκυρα μπλοκ. Ο κίνδυνος να ευνοηθούν οι πλουσιότεροι χρήστες και να εκμεταλλευτούν τη θέση τους μέσα στο δίκτυο παραμονεύει ακόμα. Επιπλέον, η ροή των συναλλαγών μειώνεται, καθώς οι χρήστες τείνουν να διατηρούν τα νομίσματά τους περισσότερο καιρό αποθαρρύνοντας έτσι τις χρηματοπιστωτικές συναλλαγές. Για τους λόγους αυτούς ερευνώνται διαφορετικές τεχνικές για τη διαδικασία εκλογής οι οποίες θα εξαλείφουν κατά μεγάλο βαθμό τους κινδύνους αυτούς.



Εικόνα 4.6 : Τα πρωτόκολλα συναίνεσης Proof – of -Work και Proof – of – Stake.

Οι αλγόριθμοι συναίνεσης είναι κρίσιμοι για τη διατήρηση της ακεραιότητας και της ασφάλειας ενός δικτύου που στηρίζεται σε συναλλαγές κρυπτονομισμάτων. Έχουν τον ρόλο ενός μέσου συναίνεσης μεταξύ των κόμβων του δικτύου για το ποιες συναλλαγές και ποια μπλοκ θα συμπληρώσουν την αλυσίδα. Η ομόφωνη απόφαση τους είναι απαραίτητη για την ομαλή λειτουργία του ψηφιακού συστήματος.

Ο αλγόριθμος Proof – of – Work θεωρείται μία από τις καλύτερες λύσεις στο πρόβλημα της κακομεταχείρισης. Αυτό σημαίνει ότι η αλυσίδα Blockchain είναι ιδιαίτερα ανθεκτική σε επιθέσεις, όπως της 51% επίθεσης που αναφέρθηκε παραπάνω. Αυτό οφείλεται όχι μόνο στο αποκεντρωμένο δίκτυο που χρησιμοποιεί αλλά και στον αλγόριθμο PoW. Το υψηλό κόστος που απαιτεί η διαδικασία εξόρυξης στην απόδειξη εργασίας καθιστά πολύ δύσκολη έως απίθανη την επένδυση πόρων από κακόβουλους χρήστες μόνο και μόνο για να βλάψουν το δίκτυο [33].

5

Διαδεδομένες εφαρμογές της τεχνολογίας Blockchain

5.1 Πλατφόρμες Ανάπτυξης Blockchain

Οι πλατφόρμες Blockchain επιτρέπουν την ανάπτυξη εφαρμογών που βασίζονται στην τεχνολογία Blockchain. Μπορούν να είναι είτε ιδιωτικές είτε δημόσιες. Μερικές από τις πιο διαδεδομένες πλατφόρμες αναγράφονται παρακάτω.

5.1.1 Ethereum

Το Ethereum είναι μία ανοικτού κώδικα, δημόσια πλατφόρμα η οποία βασίζεται στην τεχνολογία Blockchain αλλά και ένα λειτουργικό σύστημα το οποίο υποστηρίζει τη χρήση των έξυπνων συμβολαίων. Είναι ένα εναλλακτικό πρωτόκολλο για την οικοδόμηση αποκεντρωμένων εφαρμογών με ιδιαίτερη έμφαση σε καταστάσεις όπου η ταχεία ανάπτυξη και η ασφάλεια θα αλληλοεπιδρούν αποτελεσματικά. Στην ουσία είναι ένα δίκτυο Blockchain με μία ενσωματωμένη γλώσσα προγραμματισμού Turing η οποία επιτρέπει σε οποιονδήποτε χρήστη να δημιουργήσει έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές με τους δικούς τους κανόνες ιδιοκτησίας, απόρρητου και λειτουργίας [60].

Η ιδέα αναπτύχθηκε αρχικά από τον προγραμματιστή και ιδρυτή του “Bitcoin Magazine” Vitalik Buterin στα τέλη του 2013. Ωστόσο, αμφισβητήθηκε ότι ξεκίνησε αρκετά νωρίτερα. Προέρχεται από το έργο του στην κοινότητα του Bitcoin και μέσω της έρευνας που δημοσιεύτηκε, περιέγραψε το σχεδιασμό και τη λειτουργία του. Το Ether είναι το κρυπτονομίσμα που παράγεται από την πλατφόρμα Ethereum ως ανταμοιβή των κόμβων στην εξόρυξη και στην εκτέλεση πολύπλοκων υπολογισμών, ενώ ο μηχανισμός “Ethereum Virtual Machine (EVC)” υποστηρίζει διάφορες γλώσσες προγραμματισμού [62].

Παρά τα κοινά στοιχεία και τον τρόπο λειτουργίας του Ethereum και του Bitcoin διαφέρουν σε ορισμένα σημεία. Ένα τεράστιο πλεονέκτημα του Ethereum είναι το γεγονός ότι υποστηρίζει τη λειτουργία των έξυπνων συμβολαίων, εν αντιθέσει με το Bitcoin. Επιπλέον, ενώ το Bitcoin χρησιμοποιείται για την παρακολούθηση των ψηφιακών νομισμάτων, το Ethereum επικεντρώνεται στην εκτέλεση του προγραμματιστικού κώδικα οποιασδήποτε αποκεντρωμένης εφαρμογής [61].

Είναι το πιο διαδεδομένο εργαλείο ανάπτυξης εφαρμογών που είναι βασισμένες στην τεχνολογία Blockchain και χιλιάδες προγραμματιστές συνεισφέρουν καθημερινά στη βελτίωση και στην ανάπτυξή τους ενώ ταυτόχρονα σχεδιάζουν νέες εφαρμογές.

Εικόνα 5.1.1 : Λογότυπο της πλατφόρμας Ethereum

5.1.2 Hyperledger

Το Hyperledger είναι ένα ομαδικό project το οποίο βασίζεται σε ένα ανοιχτού κώδικα Blockchain και σχετικά εργαλεία, το οποίο ξεκίνησε το Δεκέμβριο του 2015 από τη Linux, και στο οποίο έχουν συνεισφέρει οι τεχνολογικές εταιρείες IBM (International Business Machines Corporation), Intel και SAP Ariba, για την υποστήριξη και την ανάπτυξη του έργου.

Στόχος του έργου είναι να προωθήσει τη διεπαγγελματική συνεργασία μέσα από την ανάπτυξη ενός δικτύου Blockchain και αποκεντρωμένων εφαρμογών, με ιδιαίτερη έμφαση τη βελτίωση της απόδοσης και της αξιοπιστίας αυτών των συστημάτων, ώστε να είναι σε θέση να υποστηρίξουν παγκόσμιες επιχειρηματικές συναλλαγές από μεγάλες τεχνολογικές, χρηματιστηριακές και βιομηχανικές εταιρείες. Το Hyperledger ενσωματώνει ανεξάρτητα ανοικτά πρωτόκολλα και μέσω ενός οργανωμένου πλαισίου περιλαμβάνει δικούς του μηχανισμούς συναίνεσης, ελέγχου και αποθήκευσης δεδομένων [63].

HYPERLEDGER

Εικόνα 5.1.2 : Λογότυπο της πλατφόρμας Hyperledger

5.1.3 OpenChain

Η πλατφόρμα OpenChain αναπτύχθηκε από τον οργανισμό του CoinPrism και είναι μία πλατφόρμα ανοιχτού κώδικα ειδικά διαμορφωμένη για βιομηχανίες που επιθυμούν να έχουν τον έλεγχο των δικών τους ψηφιακών οικονομικών στοιχείων και πληροφοριών. Είναι μία ασφαλής και με προοπτικές επέκτασης εφαρμογή, που μπορεί να υποστηριχτεί από ένα σύνολο μελών αλλά να διαχειριστεί από ένα μοναδικό πρόσωπο το οποίο θα είναι υπεύθυνο για την επικύρωση των συναλλαγών. Αποτελεί μία από τις πιο αποτελεσματικές πλατφόρμες Blockchain, καθώς η διαδικασία συναλλαγής είναι δωρεάν, χωρίς κόστος.

Εικόνα 5.1.3 : Λογότυπο της πλατφόρμας OpenChain

5.2 Έξυπνα Συμβόλαια

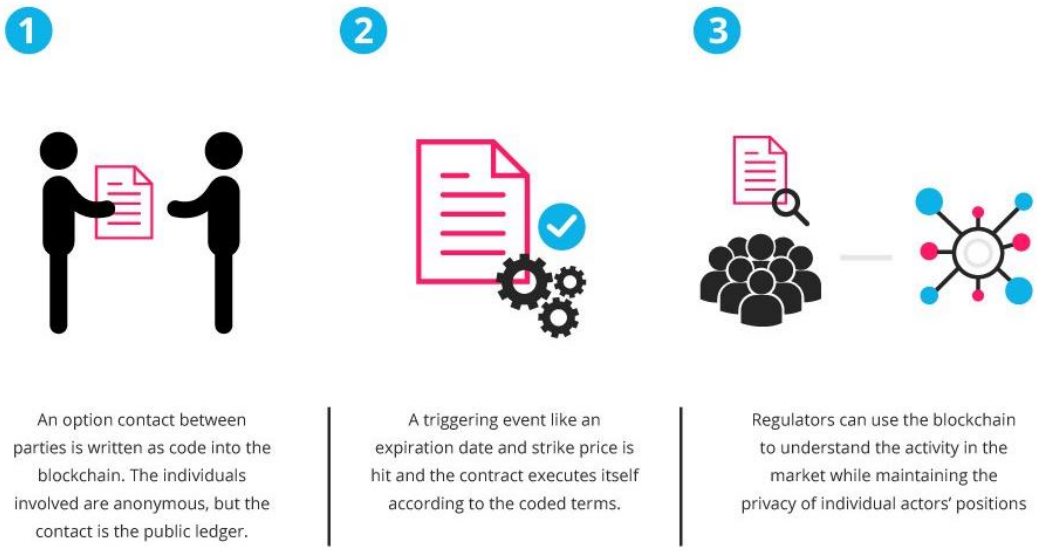
Ένα έξυπνο συμβόλαιο είναι ένα ψηφιακό πρωτόκολλο του οποίου σκοπός είναι να επαληθεύει ή να προωθεί τη διαπραγμάτευση ή την εκτέλεση μίας συμφωνίας. Τα έξυπνα συμβόλαια επιτρέπουν την εκτέλεση αξιόπιστων συναλλαγών χωρίς την ανάγκη τρίτου. Οι συναλλαγές είναι μη αναστρέψιμες και ταυτόχρονα παρακολουθούνται. Περιέχει κανόνες που οι συμμετέχοντες έχουν συμφωνήσει να τηρούν στις μεταξύ τους αλληλεπιδράσεις. Όταν οι προκαθορισμένες προϋποθέσεις ενός έξυπνου συμβολαίου ικανοποιηθούν, το συμβόλαιο ενεργοποιείται αυτόματα. Η συμπεριφορά του βασίζεται στους αλγορίθμους πάνω στους οποίους έχει χτιστεί.

Το μεγαλύτερο πλεονέκτημα των έξυπνων συμβολαίων είναι το γεγονός ότι μειώνουν δραματικά το κόστος των συναλλαγών. Ένα έξυπνο συμβόλαιο ορίζει τα δικαιώματα και τις υποχρεώσεις που τα συμμετέχοντα μέλη συμφωνούν να τηρούν. Ο έλεγχος τήρησης των υποχρεώσεων και η επιβολή του δικαιώματος που αποκτά κάθε μέλος δια του συμβολαίου διεκπεραιώνονται από ένα δίκτυο υπολογιστών τη στιγμή που οι προϋποθέσεις ικανοποιούνται. Με αυτό τον τρόπο δίνεται η δυνατότητα σύναψης συμβολαίων με μέλη για τα οποία δεν υπάρχουν πληροφορίες πρότερης φερεγγυότητας, καθώς και η πραγματοποίηση συναλλαγών που εμπλέκουν ποσά που δε θα δικαιολογούσαν το κόστος και φόρτο σύναψης συμφωνιών εάν επρόκειτο να προχωρήσουν με τον παραδοσιακό τρόπο. Τα έξυπνα συμβόλαια λειτουργούν συνεχώς και δεν επιβάλλουν περιορισμούς διαθεσιμότητας που σχετίζονται με χρόνο ή τοποθεσία. Τα έξυπνα συμβόλαια είναι αυτό-επαληθευόμενα, αυτό-εκτελέσιμα και μη παραβιάσιμα. Τυπικές περιπτώσεις χρήσης τους είναι περιπτώσεις στις οποίες τα μέλη που επιθυμούν να συνάψουν συμβόλαιο δεν είναι γνωστά μεταξύ τους και δεν εμπιστεύονται κατ’ ανάγκη το ένα το άλλο. Μπορούν να παρακάμψουν διαμεσολαβητές και μέσω του Blockchain να προσφέρουν την απαιτούμενη ασφάλεια.

Παρακάτω φαίνεται ο αλγόριθμος ενός έξυπνου συμβολαίου με χρήση της γλώσσας Solidity του Ethereum. Το ακόλουθο συμβόλαιο είναι μία γενική ιδέα μίας απλής δημοπρασίας όπου όλοι μπορούν να στείλουν τις προσφορές τους κατά τη διάρκεια μίας περιόδου υποβολής προσφορών. Οι προσφορές περιλαμβάνουν την αποστολή κρυπτονομισμάτων Ether για να δεσμεύσουν τους πλειοδότες στην προσφορά τους. Εάν αυξηθεί η υψηλότερη προσφορά, ο προηγούμενος υψηλότερος πλειοδότης επιστρέφει τα χρήματά του. Μετά το τέλος της περιόδου υποβολής προσφορών, το συμβόλαιο πρέπει να υλοποιηθεί χειροκίνητα για να λάβει ο δικαιούχος το ποσό που δικαιούται. Τα συμβόλαια δε μπορούν να ενεργοποιηθούν αυτόνομα.

```
pragma solidity ^0.4.22;

contract SimpleAuction {
    address public beneficiary;
    uint public auctionEnd;

    // Current state of the auction.
    address public highestBidder;
    uint public highestBid;

    // Allowed withdrawals of previous bids
    mapping(address => uint) pendingReturns;
    bool ended;

    // Events that will be fired on changes.
    event HighestBidIncreased(address bidder, uint amount);
    event AuctionEnded(address winner, uint amount);

    constructor(
        uint _biddingTime,
        address _beneficiary
    ) public {
        beneficiary = _beneficiary;
        auctionEnd = now + _biddingTime;
    }

    function bid() public payable {

        require(
            now <= auctionEnd,                          //Revert the call if the
            "Auction already ended."                    //bidding period is over
        );

        require(                                        //If the bid is not higher,
            msg.value > highestBid,                     //send the money back
            "There already is a higher bid."
        );

        if (highestBid != 0) {
            // Sending back the money by simply using
            // highestBidder.send(highestBid) is a security risk
            // because it could execute an untrusted contract.
            pendingReturns[highestBidder] += highestBid;
        }
        highestBidder = msg.sender;
        highestBid = msg.value;
        emit HighestBidIncreased(msg.sender, msg.value);
    }

    /// Withdraw a bid that was overbid.
    function withdraw() public returns (bool) {
        uint amount = pendingReturns[msg.sender];
        if (amount > 0) {
            pendingReturns[msg.sender] = 0;

            if (!msg.sender.send(amount)) {
                // No need to call throw here, just reset the amount owing
                pendingReturns[msg.sender] = amount;
                return false;            }
        }
        return true;    }

    /// End the auction and send the highest bid
    /// to the beneficiary.
    function auctionEnd() public {

        // 1. Conditions
        require(now >= auctionEnd, "Auction not yet ended.");
        require(!ended, "auctionEnd has already been called.");

        // 2. Effects
        ended = true;
        emit AuctionEnded(highestBidder, highestBid);

        // 3. Interaction
        beneficiary.transfer(highestBid);
    }}
```

Εικόνα 5.2.α : Παράδειγμα Έξυπνου Συμβολαίου Απλής Δημοπρασίας



Εικόνα 5.2.β : Η λειτουργία των έξυπνων συμβολαίων

6

Εφαρμογή της τεχνολογίας Blockchain στον τομέα της Υγείας

Ένας από τους τομείς στους οποίους θεωρείται ότι η τεχνολογία Blockchain έχει εξαιρετικές δυνατότητες είναι ο χώρος της υγείας. Η δημιουργία εξελιγμένων τεχνολογικών υποδομών στο χώρο της υγείας, μπορεί να βελτιώσει την ποιότητα των παρεχόμενων υπηρεσιών στους πολίτες και συνεπώς να διασφαλίσει μεγαλύτερη ευημερία στην κοινωνία. Συστήματα που είναι βασισμένα στην καινοτόμα τεχνολογία, θα μπορούσαν να ενισχύσουν την ασφάλεια και την αξιοπιστία των ιατρικών ηλεκτρονικών αρχείων των ασθενών, δεδομένου ότι ο καθένας θα είχε τον έλεγχο του δικού του ψηφιακού φακέλου. Τα συστήματα θα μπορούσαν επίσης να συμβάλλουν στην εδραίωση των δεδομένων των ασθενών, επιτρέποντας την ανταλλαγή ιατρικών αρχείων μεταξύ των ιδρυμάτων υγειονομικής περίθαλψης.

Η αποθήκευση των ιατρικών δεδομένων είναι υψίστης σημασίας για τον κλάδο της υγείας. Τα δεδομένα αυτά είναι πολύ ευαίσθητα και επομένως, πρωταρχικός στόχος κακόβουλων επιθέσεων. Για το λόγο αυτόν, είναι πολύ σημαντική η ασφάλειά τους. Η τεχνολογία και ο τρόπος λειτουργίας του Blockchain θα μπορούσαν να δώσουν τη λύση σε τέτοιου είδους προβλήματα, όπως την κατάχρηση ή την παράνομη παραποίηση των πληροφοριών και να αποκαταστήσουν την εμπιστοσύνη των ασθενών προς τους οργανισμούς παροχής υπηρεσιών υγείας, τους ερευνητικούς και κυβερνητικούς φορείς αλλά και τις βιομηχανίες που είναι συνδεδεμένες με το χώρο της ιατρικής.

6.1 Δυσλειτουργίες των παραδοσιακών συστημάτων υγείας

6.1.1 Έλλειψη Διαλειτουργικότητας

Ένα βασικό πρόβλημα στο χώρο της υγειονομικής περίθαλψης είναι η έλλειψη ασφαλών μηχανισμών που μπορούν να συνδέσουν όλα τα ανεξάρτητα συστήματα υγείας ώστε να δημιουργήσουν ένα ενιαίο δίκτυο από άκρο σε άκρο, προστατεύοντας ταυτόχρονα τα εμπλεκόμενα πρόσωπα με κάποιο επίπεδο ανωνυμίας.

Ως διαλειτουργικότητα στον τομέα της υγείας περιγράφεται η ικανότητα των ετερογενών πληροφοριακών συστημάτων, όπως τα συστήματα EHR (Electronic Health Records), να επικοινωνούν μεταξύ τους, να ανταλλάσσουν δεδομένα και να αξιοποιούν τα δεδομένα αυτά. Η επικοινωνία μεταξύ των συστημάτων μέσα σε ένα οργανωτικό πλαίσιο είναι ιδιαιτέρως σημαντική, αφού έτσι βελτιστοποιείται η παροχή υπηρεσιών υγείας στους ανθρώπους και στις κοινότητες. Για παράδειγμα, η διαλειτουργικότητα επιτρέπει την ασφαλή ανταλλαγή ιατρικών αρχείων των ασθενών μεταξύ των αρμόδιων προσώπων, ανεξαρτήτως την τοποθεσία και τη σχέση εμπιστοσύνης μεταξύ τους [57].

Η ασφαλής ανταλλαγή δεδομένων είναι απαραίτητη για την παροχή αποτελεσματικών θεραπειών στους ασθενείς, οι οποίες θα έχουν επιτευχθεί μέσω της συνεργασίας των υπεύθυνων, αλλά και μέσω των αποφάσεων σχετικών με τη χορήγηση της κατάλληλης ιατρικής φροντίδας. Η κοινή χρήση πληροφοριών στοχεύει σε μεγαλύτερη διαγνωστική ακρίβεια μέσω των περισσότερων συγκεντρωτικών στοιχείων και συστάσεων που συσσωρεύονται από ομάδες ιατρικών εμπειρογνωμόνων, καθώς και στην αποτροπή ανακριβειών και λαθών στο πλάνο της θεραπείας και της φαρμακευτικής αγωγής. Ομοίως, όσο περισσότερα μυαλά και ιδέες συγκεντρώνονται για την κατανόηση ενός φαινομένου, τόσο μεγαλύτερη είναι και η κατανόηση των αναγκών του ασθενή με αποτέλεσμα να εφαρμόζονται αποτελεσματικότερες θεραπείες.

Παρά τη σπουδαιότητα της ανταλλαγής ιατρικών δεδομένων, τα σημερινά συστήματα υγειονομικής περίθαλψης απαιτούν συχνά από τους ασθενείς να αποκτούν και να μοιράζονται το δικό τους ιατρικό αρχείο είτε μέσα από φυσικά αντίγραφα σε χαρτί, είτε ηλεκτρονικά μέσω των σκληρών δίσκων. Αυτή η διαδικασία είναι αναποτελεσματική για τους ακόλουθους λόγους [41].

- Η συγκεκριμένη διαδικασία είναι χρονοβόρα, καθώς οι ιατρικοί φάκελοι θα πρέπει να προετοιμαστούν και να συλλεχθούν από τον ασθενή.
- Δεν είναι ασφαλής τρόπος αφού υπάρχει πιθανότητα να χαθούν ή να κλαπούν κατά τη μεταφορά τους από τη μία τοποθεσία στην άλλη.
- Δεν υπάρχει ενιαία πηγή που να αποθηκεύει όλα τα ιατρικά αρχεία ενός ατόμου, οπότε οι ασθενείς θα πρέπει να είναι υπεύθυνοι για την παρακολούθηση των ιατρικών τους αρχείων και συνεχώς ενήμεροι για τις υπηρεσίες που έχουν λάβει, ώστε να γνωρίζουν το που να απευθυνθούν στην περίπτωση που θελήσουν κάποιο αντίγραφο.
- Στα σημερινά υγειονομικά συστήματα οι ασθενείς δεν έχουν τον έλεγχο των δικών τους αρχείων με αποτέλεσμα να μην είναι σε θέση να ξέρουν τις κινήσεις αυτών.

Η αναποτελεσματικότητα στη διαδικασία ανταλλαγής ιατρικών αρχείων οφείλεται εν μέρει στην έλλειψη εμπιστοσύνης μεταξύ των παροχών υπηρεσιών υγείας και στην έλλειψη διαλειτουργικότητας μεταξύ των συστημάτων πληροφορικής και των εφαρμογών που σχετίζονται με την υγεία. Η διαλειτουργικότητα ταξινομείται σε τρία επίπεδα :

1. **Θεμελιώδη Διαλειτουργικότητα**

Η θεμελιώδης διαλειτουργικότητα επιτρέπει την ανταλλαγή δεδομένων μεταξύ των συστημάτων υγειονομικής περίθαλψης. Δεν απαιτεί από τις υπηρεσίες που λαμβάνουν τα δεδομένα να μπορούν να τα ερμηνεύουν.

2. **Δομική διαλειτουργικότητα**

Η δομική διαλειτουργικότητα καθορίζει επιπλέον μορφές για την ανταλλαγή ιατρικών δεδομένων και εξασφαλίζει ότι τα δεδομένα που έχουν ληφθεί διατηρούνται και μπορούν να ερμηνευθούν χρησιμοποιώντας προκαθορισμένες μορφές.

3. **Σημασιολογική διαλειτουργικότητα**

Η σημασιολογική διαλειτουργικότητα απαιτεί την ερμηνεία των ανταλλασσόμενων δεδομένων όχι μόνο ως προς τη σύνταξη και τη δομή αλλά και ως προς τη σημασία τους.

Οι τρεις αυτές περιπτώσεις διασφαλίζουν ότι τα διαφορετικά συστήματα υγείας και οι εφαρμογές παρέχουν πληροφορίες με την απαιτούμενη ποιότητα και ασφάλεια δεδομένων [41] [43].

6.1.2 Αδυναμία στην Αυτόνομη Διαχείριση ιατρικών αρχείων

Ένα επίσης βασικό σημείο όπου τα υγειονομικά συστήματα συναντούν δυσκολία είναι η αδυναμία προσβασιμότητας των ασθενών στα δικά τους ιατρικά αρχεία. Οι ασθενείς πρέπει να έχουν εικόνα ολόκληρου του ιστορικού τους, γεγονός που θα μπορούσε να οδηγήσει στη μείωση των ανακριβειών στις πληροφορίες που προκαλούνται από καθυστέρηση επικοινωνίας ή έλλειψη συντονισμού και με τη σειρά τους στη βελτίωση της ποιότητας της υγείας και της φροντίδας του ασθενή.

Ιδανικά όλα τα συστήματα υγείας θα παρέχουν αυτόματες ειδοποιήσεις για τους ασθενείς ώστε να έχουν πρόσβαση στα κλινικά τους δεδομένα σε πραγματικό χρόνο. Επιπροσθέτως, είναι απαραίτητο οι ασθενείς να επιλέγουν τον τρόπο με τον οποίο επιθυμούν να μοιραστούν τα ιατρικά τους δεδομένα. Ως αποτέλεσμα, οι πληροφορίες θα βρίσκονται πάντα υπό τον έλεγχο του κατόχου [41].

Οι ασθενείς επωφελούνται όταν μπορούν να έχουν πρόσβαση στο ιατρικό ιστορικό τους και μία καθαρή εικόνα αυτού. Αυτό αποδεικνύεται ζωτικής σημασίας για την περίπτωση που οι ασθενείς αμφιβάλλουν για την εμπιστευτικότητα των αρχείων τους [44].

6.2 Εφαρμογές στο χώρο της Υγείας

6.2.1 Ερευνητικός κλάδος

Οι ερευνητές στο χώρο της υγείας χρειάζονται ένα ευρύ και πλήρες φάσμα δεδομένων ώστε να επιτευχθεί η κατανόηση των ασθενειών, η επιταχυμένη ανάπτυξη της βιοϊατρικής, η ανάπτυξη φαρμάκων και η σχεδίαση προσαρμοσμένων ατομικών θεραπευτικών προγραμμάτων με βάση τη γενετική των ασθενών, τον κύκλο ζωής και το περιβάλλον. Το κοινόχρηστο περιβάλλον του Blockchain θα παρέχει ένα εκτεταμένο σύνολο διαφορετικών δεδομένων, συμπεριλαμβάνοντας ασθενείς με διαφορετική εθνικότητα και διαφορετικά γεωγραφικά πεδία. Δεδομένου ότι η τεχνολογία Blockchain συλλέγει δεδομένα υγείας κατά τη διάρκεια ζωής ενός ασθενούς, αφήνει ιδανικά περιθώρια για διαχρονικές μελέτες.

Αρκετά σημαντικό είναι το γεγονός ότι ο μηχανισμός Blockchain ξεπερνάει το πρόβλημα της αλλοίωσης ή παραχάραξης ιατρικών αποτελεσμάτων και ερευνών που μπορεί να είναι αντίθετες με τα συμφέροντα των εταιρειών που τις χρηματοδοτούν ή των ίδιων των ερευνητών [45].

6.2.2 Κλινικές Δοκιμές

Οι κλινικές δοκιμές και η διαχείριση των εντολών προκειμένου να υπάρξει συγκατάθεση για την πραγματοποίησή τους, είναι ένας τομέας στον οποίο η τεχνολογία Blockchain έχει τη δυνατότητα να διασφαλίσει τον έλεγχο και την ακεραιότητα μετάδοσης δεδομένων μεταξύ των ενδιαφερόμενων ερευνητών και ιατρών.

Διατηρώντας έναν αμετάβλητο κατάλογο του οποίου η πρόσβαση απαιτεί τη συγκατάθεση αρμόδιων προσώπων, εξασφαλίζεται η παρακολούθηση των κλινικών δοκιμών και η τήρηση των κανόνων. Το γεγονός αυτό είναι ιδιαίτερα σημαντικό για την εξάλειψη πολλών μορφών κλινικής απάτης, όπως για παράδειγμα η πλαστογράφηση και η μη συναινετική επεξεργασία δεδομένων. Όπως προτείνεται από τους ερευνητές Benchoufi, Porcher και Ravaud, εφαρμόζοντας ένα σύστημα που χρησιμοποιεί τα έξυπνα συμβόλαια, υπάρχει δυνατότητα να εμποδιστούν οι ιατρικοί ερευνητές από το να χρησιμοποιήσουν δεδομένα ασθενών έως ότου ελεγχθεί και εγκριθεί κάθε στάδιο της δοκιμής στην οποία συμμετέχουν. Βέβαια, αυτή η διαδικασία θα πρέπει να επιτρέπει την ανάκληση της συγκατάθεσης. Η εφαρμογή του μηχανισμού με την τεχνολογία Blockchain, δίνει στους συμμετέχοντες δύναμη ως προς την ιδιοκτησία των δικών τους δεδομένων, παρέχοντας μία διαδρομή ελέγχου σχετικά με τις κλινικές δοκιμές [55].

6.2.4 Παραγωγή και Παρακολούθηση Φαρμάκων

Η τεχνολογία Blockchain θα μπορούσε να συνεισφέρει σημαντικά στην εξάλειψη των αυξανόμενων κινδύνων γύρω από τα πλαστά και μη εγκεκριμένα φάρμακα. Με τη χρήση του καινοτόμου δικτύου και των έξυπνων συμβολαίων, ο εντοπισμός των συσκευασιών φαρμάκων που διακινούνται στην αγορά γίνεται ευκολότερος και παράλληλα η διαδρομή των φαρμάκων από τον αρχικό κατασκευαστή στον καταναλωτή είναι ασφαλής και έγκυρη.

Καταγράφοντας λεπτομερώς κάθε στάδιο κατασκευής του φαρμάκου, είναι πιο εύκολη η ανάκλησή του σε περίπτωση εντοπισμού λάθους, ενώ παρακολουθώντας την προέλευση και τα συστατικά, είναι εφικτό να αποφευχθεί η κλοπή και η απάτη από φαρμακευτικές βιομηχανίες σε οικονομικό και εμπορικό επίπεδο. Επίσης, διασφαλίζονται οι συνθήκες μεταφοράς του φαρμάκου στην περίπτωση που χρειαστεί ειδική μεταχείριση και ο έλεγχος συνταγογράφησης που συμπεριλαμβάνει το φάρμακο σε εγχώριο ή διεθνές επίπεδο για στατιστικούς ή επιδημιολογικούς λόγους [59].

6.2.3 Διαχείριση Αλυσίδας Εφοδιασμού Φαρμάκων

Μία επίσης τεράστια εφαρμογή της τεχνολογίας Blockchain στη βιομηχανία της ιατρικής περιλαμβάνει τη διαχείριση της αλυσίδας εφοδιασμού φαρμάκων, μία γενικότερη μορφή της παραγωγής φαρμάκων που αναφέρθηκε προηγουμένως. Η διαχείριση αλυσίδας εφοδιασμού είναι ένα κρίσιμο ζήτημα για την προστασία των δεδομένων της σε όλους τους τομείς, αλλά αποκτά μεγαλύτερη σημασία στον κλάδο της ιατρικής λόγω της αυξανόμενης πολυπλοκότητάς του. Αυτό συμβαίνει καθώς οποιαδήποτε μεταβολή σε αυτήν επηρεάζει την ευημερία του ασθενούς.

Οι αλυσίδες εφοδιασμού είναι ευάλωτες και περιλαμβάνουν σημεία που μπορούν να αποτελέσουν αφορμή για κακόβουλη επίθεση. Το Blockchain παρέχει μία ασφαλή πλατφόρμα για την εξάλειψη αυτού του προβλήματος και σε ορισμένες περιπτώσεις την πρόληψη της απάτης, εισάγοντας καλύτερη διαφάνεια των δεδομένων και βελτιωμένη ιχνηλασιμότητα του ιατρικού εξοπλισμού και των φαρμάκων [56].

6.3 Πλατφόρμες Ανάπτυξης για τα Ιατρικά αρχεία

6.3.1 MedRec

Η πλατφόρμα MedRec είναι μία καινοτόμα τεχνολογία η οποία σχεδιάστηκε με σκοπό να επικεντρωθεί στη διαχείριση των ιατρικών φακέλων των ασθενών από τους ίδιους. Καθώς οι ασθενείς μετακινούνται από τον έναν πάροχο υπηρεσιών υγείας στον άλλον, τα δεδομένα τους διασκορπίζονται με αποτέλεσμα να χάνεται η εύκολη πρόσβαση σε παλαιότερα αρχεία και να υπάρχει σημαντική απώλεια στο ατομικό ιστορικό του κάθε ασθενούς. Δεδομένου ότι κύριοι διαχειριστές των ηλεκτρονικών ιατρικών φακέλων (EHR) είναι οι πάροχοι υγείας, οι ασθενείς αντιμετωπίζουν σημαντικά εμπόδια κατά την εξέταση των αναφορών τους και τη διανομή των πληροφοριών [46].

Το MedRec είναι ένας συνδυασμός κοινωνικής ανάγκης με μία νέα τεχνολογία από τον οποίο γεννιέται ένα σύστημα που δίνει προτεραιότητα στην υπηρεσία ασθενών προσφέροντας μία διαφανή και προσιτή εικόνα στο ιατρικό ιστορικό. Το κάθε αρχείο είναι μοναδικό αποτύπωμα του κάθε ατόμου και η τεχνολογία MedRec είναι μία λύση που χρησιμοποιεί το μηχανισμό Blockchain ώστε να αποκαταστήσει τους κεντρικούς ενδιάμεσους φορείς.

Η εφαρμογή MedRec που κάνει χρήση της τεχνολογίας Blockchain αντιμετωπίζει τέσσερα σημαντικά θέματα :

1. την περιορισμένη και αργή πρόσβαση στα ιατρικά δεδομένα
2. την διαλειτουργικότητα του συστήματος που περιέχει τις πληροφορίες
3. την καλύτερη οργάνωση των αρχείων των ασθενών
4. τη βελτιωμένη ποιότητα και ποσότητα των δεδομένων για ιατρική έρευνα.

Ο μηχανισμός της εφαρμογής βασίζεται στην τεχνολογία του Ethereum και στα Έξυπνα Συμβόλαια (Smart Contracts) που υποστηρίζει το Blockchain. Για το MedRec, το περιεχόμενο του μπλοκ αντιπροσωπεύει δικαιώματα ιδιοκτησίας και προβολής των δεδομένων που μοιράζονται τα μέλη ενός ιδιωτικού Blockchain. Η τεχνολογία Blockchain υποστηρίζει τη χρήση Έξυπνων Συμβολαίων τα οποία επιτρέπουν την αυτοματοποίηση και παρακολούθηση ορισμένων ενεργειών. Σε συνδυασμό με κρυπτογραφικές μεθόδους, διασφαλίζεται η προστασία από κακόβουλες δραστηριότητες αλλά και η ακεραιότητα των δεδομένων. Οι πάροχοι έχουν τη δυνατότητα να προσθέσουν ένα νέο αρχείο ενώ επιτρέπεται και η ανταλλαγή πληροφοριών μεταξύ τους. Δικαίωμα πρόσβαση έχουν εκείνοι που τους έχει δοθεί η κατάλληλη εξουσιοδότηση [47].

Τα έξυπνα συμβόλαια του Ethereum χρησιμοποιούνται για τη δημιουργία αναπαραστάσεων των ιατρικών αρχείων που αποθηκεύονται στους επιμέρους κόμβους του δικτύου. Στα έξυπνα συμβόλαια αναγράφονται δεδομένα σχετικά με την κατοχή εγγράφων, τα δικαιώματα και την ακεραιότητα των πληροφοριών. Το παρόν σύστημα εφαρμόζει τρία είδη συμβολαίων στο δίκτυο του Blockchain [47].

- Register Contract (RC)

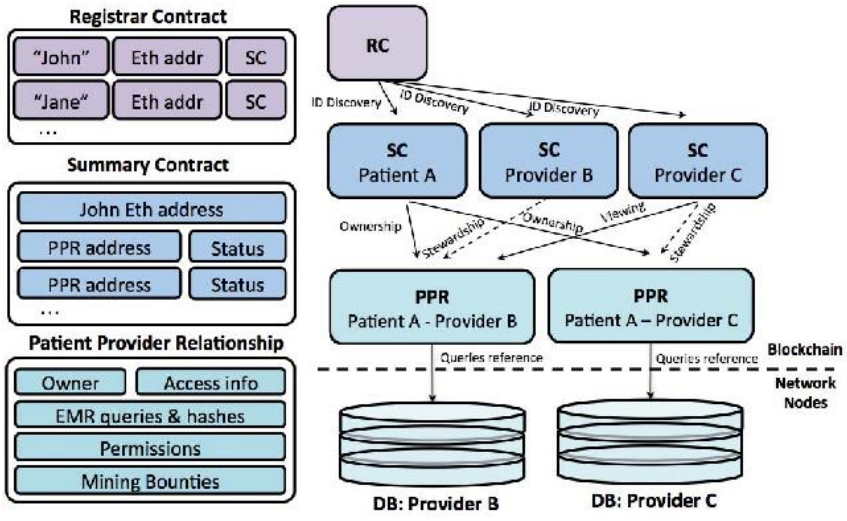
Το συγκεκριμένο συμβόλαιο χρησιμοποιείται για την αντιστοίχιση των ταυτοτήτων αναγνώρισης που κατέχουν οι χρήστες με τις διευθύνσεις τους στο δίκτυο του Ethereum. Λειτουργεί όπως ακριβώς και ένα δημόσιο κλειδί. Η πολιτική που ακολουθεί το συμβόλαιο είναι να ρυθμίζει την καταχώρηση νέων αναγνωριστικών ή την τροποποίηση των ήδη υπαρχουσών μόνο από πιστοποιημένους φορείς.

- Patient – Provider Contract (PRC)

Το συμβόλαιο "Patient – Provider Contract" εκδίδεται μεταξύ δύο κόμβων του συστήματος όταν ο ένας κόμβος αποθηκεύει και διαχειρίζεται τα ιατρικά αρχεία για τον άλλον, ενώ επεκτείνεται και στην απεικόνιση οποιασδήποτε άλλης αλληλεπίδρασης ανάμεσα σε κάποιο ζεύγος κόμβων. Το συμβόλαιο αυτό αποτελείται από αιτήματα τα οποία κάθε φορά που εκτελούνται επιστρέφουν ένα υποσύνολο δεδομένων που έχει ζητηθεί. Κάθε αίτημα επικολλάται με τη μοναδική κατακερματισμένη τιμή των δεδομένων ώστε να διασφαλιστεί ότι αυτά δεν έχουν αλλοιωθεί. Τα αιτήματα και οι σχετικές πληροφορίες δημιουργούνται από τον πάροχο και τροποποιούνται όταν γίνεται προσθήκη νέων εγγραφών.

- Summary Contract (SC)

Το παρόν συμβόλαιο λειτουργεί ως χάρτης για τους συμμετέχοντες του συστήματος για τον εντοπισμό του ιατρικού τους ιστορικού. Διαθέτει κατάλογο που αντιπροσωπεύει όλες τις προηγούμενες και τρέχουσες δεσμεύσεις του συμμετέχοντος με επιμέρους κόμβους του δικτύου και εφαρμόζει λειτουργίες οι οποίες συμβάλλουν στην ενημέρωση των σχέσεων μεταξύ των κόμβων αλλά και στην απόφαση ενός κόμβου για την αποδοχή ή την απόρριψη κάποιας εξ αυτών.



Εικόνα 6.3.1 : Αρχιτεκτονική των έξυπνων συμβολαίων της πλατφόρμας MedRec

6.3.2 Medicalchain

Το σύστημα Medicalchain είναι μία αποκεντρωμένη πλατφόρμα που επιτρέπει την ασφάλεια, την ταχύτητα, τη διαφάνεια στην ανταλλαγή και τη χρήση των ιατρικών δεδομένων. Χρησιμοποιεί την τεχνολογία Blockchain για να εστιάσει στη διαχείριση των αρχείων από τον ίδιο το χρήστη [58].

Η πλατφόρμα Medicalchain, επιτρέπει στους χρήστες να παρέχουν πρόσβαση, θέτοντας συγκεκριμένους όρους, σε διάφορους φορείς υγείας, όπως είναι οι ιατροί, τα νοσοκομεία, τα ερευνητικά εργαστήρια και οι ασφαλιστές. Κάθε αλληλεπίδραση των φορέων με τα ιατρικά δεδομένα, είναι ελεγχόμενη, ασφαλής και διαφανής και καταγράφεται ως μία συναλλαγή στο "ιατρικό βιβλίο" της πλατφόρμας. Κατά τη διάρκεια αυτής της διαδικασίας, το ιατρικό απόρρητο του ασθενούς προστατεύεται.

Το Medicalchain βασίζεται στην αρχιτεκτονική του Hyperledger Fabric, η οποία επιτρέπει ποίκιλα επίπεδα πρόσβασης. Οι χρήστες έχουν τη δυνατότητα να ελέγχουν ποια πρόσωπα θα έχουν πρόσβαση στα αρχεία τους, μέχρι ποιο σημείο και για ποιο χρονικό διάστημα. Η πλατφόρμα τροφοδοτείται από ένα είδος κρυπτονομισμάτων που καλείται "MedTokens" και εκδόθηκαν κατά τη δημιουργία του δικτύου και διανεμήθηκαν μέσω μίας διαδικασίας πώλησης.

Με τη συμμετοχή στο δίκτυο Medicalchain, οι χρήστες θα μπορούν να υπογράφουν ψηφιακά για τις εφαρμογές και τις υπηρεσίες στις οποίες θα χρησιμοποιούνται τα δεδομένα τους και ταυτόχρονα με τη χρήση των έξυπνων συμβολαίων, θα διασφαλίζεται η αποφυγή παραβιάσεων. Η πλατφόρμα αναπτύσσει δύο εφαρμογές που κινούνται παράλληλα. Η μία αφορά την τηλεϊατρική μεταξύ του ιατρού και του ασθενούς, ενώ η άλλη την αγορά ιατρικών δεδομένων για ερευνητικούς σκοπούς, με όνομα "Marketplace". Η τηλεϊατρική επιτρέπει στους χρήστες να απευθύνονται και να επικοινωνούν με πραγματικό ιατρό εξ αποστάσεως. Η αγορά δεδομένων επιτρέπει στους χρήστες του δικτύου να διαπραγματεύονται εμπορικούς όρους με τρίτα πρόσωπα για εναλλακτικές χρήσεις ή εφαρμογές των προσωπικών τους δεδομένων υγείας [58].

Εικόνα 6.3.2 : Το λογότυπο της πλατφόρμας Medicalchain

6.3.3 Gem Health Enterprise Blockchain Ecosystem

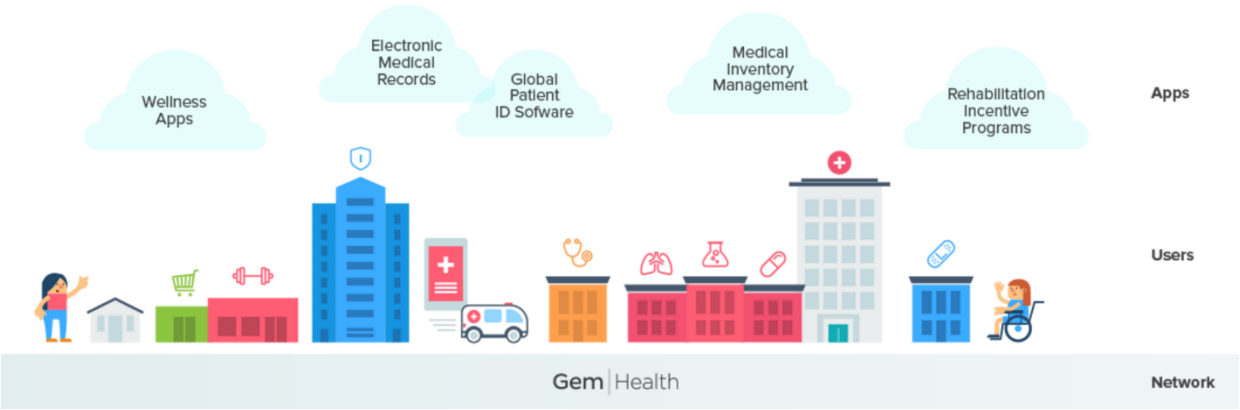
Σύμφωνα με μία συνέντευξη του Winkelspecht, CEO και ιδρυτής του Gem, στο "Bitcoin Magazine", οι πάροχοι υπηρεσιών υγείας και οι φορείς υγείας ξεκίνησαν να απευθύνονται στην πλατφόρμα Gem εξαιτίας προβλημάτων που επικεντρώνονταν στη συστηματική αδυναμία ανταλλαγής ιατρικών δεδομένων μεταξύ τους λόγω των "σφραγισμένων δεδομένων". Η πρόσβαση σε ιατρικά δεδομένα ήταν επίσης πραγματικό πρόβλημα για τους ασθενείς, ειδικά σε δύσκολες καταστάσεις.

Για να προχωρήσει σε μία λύση, η Gem ξεκίνησε να εφαρμόζει την πλατφόρμα Blockchain σε συγκεκριμένες περιπτώσεις στον τομέα της υγείας. Επομένως, άρχισε να σχεδιάζει ένα περιβάλλον υγειονομικής περίθαλψης, το Gem Health.

Για να επιτύχουν το στόχο τους, χρειάζονται ένα σύστημα επικεντρωμένο στον ασθενή. Ο ιδρυτής οραματίζεται μία εποχή όπου ένα παγκόσμιο, ασφαλές δίκτυο βασισμένο στο Blockchain θα μπορεί να διασυνδέσει όλα τα συστήματα υγείας. Μία τέτοια αλλαγή στη διαχείριση των δεδομένων θα επέτρεπε στα δεδομένα να ρέουν ελεύθερα όπου κι αν ήταν απαραίτητο.

Η πλατφόρμα Gem Health έχει εγγυημένη ακεραιότητα δεδομένων. Βασίζεται στο πλαίσιο Ethereum Blockchain. Στην προσπάθεια να εξαλείψει το πρόβλημα της διαλειτουργικότητας και της αδυναμίας ανταλλαγής δεδομένων, το Gem δημιουργεί ένα μοναδικό παγκόσμιο αναγνωριστικό για κάθε άνθρωπο, παρέχοντας διαφάνεια σε πραγματικό χρόνο στο σύνολο των συναλλαγών του και ταυτόχρονα δημιουργώντας μία ενοποιημένη εμπειρία χρήσης. Το αναγνωριστικό θα αποτελεί το μοναδικό ιατρικό φάκελο του κάθε ασθενούς.

Μέχρι στιγμής, η Gem Health έχει ανακοινώσει έναν μόνο δημόσιο αλλά τεράστιο συνεργάτη, την εταιρεία PHILIPS. Παρόλα αυτά, ο Winkelspecht ότι εξακολουθούν να εργάζονται στο στάδιο της απόδειξης. Εστιάζουν σε μικρά πιλοτικά προγράμματα που περιλαμβάνουν μικρές ομάδες και έχουν συγκεκριμένες χρήσεις. Ταυτόχρονα το μακροπρόθεσμο όραμα παραμένει μία καθολική πλατφόρμα βασισμένη στο Blockchain που θα προκύψει σταδιακά και σταθερά από αυτές τις περιπτώσεις αρχικής χρήσης.

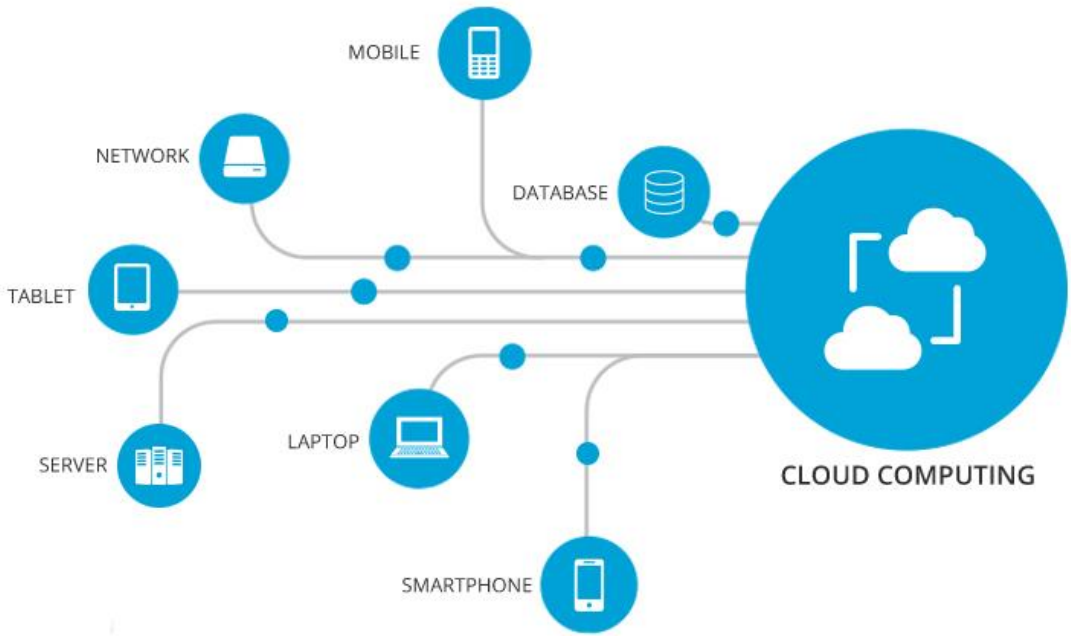


Εικόνα 6.3.3 : Όραμα για καθολική χρήση Blockchain πλατφόρμας στο παγκόσμιο σύστημα υγείας.

7

Ανάλυση Μοντέλου για το Διαμοιρασμό των Μεγάλων Ιατρικών Δεδομένων

Η σημασία των δεδομένων και η αξία που συνεπάγεται η διάδοσή τους έχουν δημιουργήσει επιχειρηματικές οντότητες που συλλέγουν, επεξεργάζονται, αναλύουν και αποθηκεύουν μεγάλα σύνολα αυτών. Η εποχή των μεγάλων δεδομένων (Big Data) που έχει επέλθει τα τελευταία χρόνια, προσφέρει ελκυστικές προοπτικές. Αυτό έχει προκαλέσει το ενδιαφέρον πολλών επιστημόνων με έμφαση στους μηχανισμούς αποθήκευσης και επεξεργασίας, στην ανάλυση των δεδομένων και την προέλευσή τους, καθιστώντας τις βιομηχανίες να εξαρτώνται από τη διαθεσιμότητα, τις λειτουργίες τους και την ερμηνεία τους. Για την επίτευξη των υψηλών απαιτήσεων στην αποθήκευση μεγάλων δεδομένων, αρκετοί ενδιαφερόμενοι κατέφυγαν στο μηχανισμό του Cloud Computing για να προσφέρουν λύση στις σημαντικές απαιτήσεις αποθήκευσης και επεξεργασίας. Το αυξημένο ενδιαφέρον έχει επεκταθεί και στο χώρο της υγείας συμπεριλαμβάνοντας ιατρικά και ερευνητικά ιδρύματα και τη μεταξύ τους συνεργασία. Η τεχνολογία του Cloud Computing είναι εκείνη που μπορεί να παρέχει μία ελεγχόμενη και ευέλικτη ανταλλαγή ιατρικών δεδομένων στους χώρους αποθήκευσης των τελευταίων [48] [49].



Εικόνα 7 : Το Cloud Computing προσφέρει ευελιξία, αποδοτικότητα και ασφάλεια

Παρά τα πλεονεκτήματα που προσφέρει το Cloud Computing, μειονεκτεί στη λειτουργία που σχετίζεται με την ανταλλαγή δεδομένων εξαιτίας των κινδύνων που επικρατούν στην έκθεση του περιεχόμενού του. Για τους κατόχους δεδομένων, υπάρχει ο κίνδυνος ότι τα δεδομένα που συλλέγονται θα είναι ευάλωτα στα χέρια κακόβουλων χρηστών. Μέσα στο πλαίσιο αυτό, ο φόβος για την παραβίαση των κανονισμών και την εκμετάλλευση των δεδομένων, δημιουργεί μία ατμόσφαιρα δυσπιστίας που δεν εξασφαλίζει την υλοποίηση της ανταλλαγής δεδομένων [50].

Για τον καθορισμό κινήσεων που αποσκοπούν στην ανταλλαγή των δεδομένων σε συνδυασμό με τα χαρακτηριστικά που προσφέρει το Cloud Computing, παραμένει ζήτημα ο έλεγχός τους. Όταν αυτά εγκαταλείπουν το σύστημα δεν υπάρχει επίβλεψη στη χρήση τους από τον επόμενο χρήστη, επιτρέποντας έτσι στους κακόβουλους χρήστες να κάνουν κατάχρηση και να προκαλούν μία σειρά από νομικά ζητήματα στους ιδιοκτήτες τους. Η τεχνολογία Blockchain είναι ικανή να προσφέρει την κατάλληλη λύση για την αντιμετώπιση αυτού του προβλήματος μέσω των ελκυστικών του ιδιοτήτων, όπως η αποκεντρωμένη και αμετάβλητη φύση του [51].

Το μοντέλο που περιγράφεται βασίζεται στον μηχανισμό του Blockchain και συγκεκριμένα στις ιδιότητες των έξυπνων συμβολαίων, αλλά και στο Cloud Computing, και αξιοποιείται για την ανταλλαγή ιατρικών αρχείων μεταξύ των παροχών υπηρεσιών, παρέχοντας έλεγχο δεδομένων και ταυτόχρονα κατάλληλη διαχείριση του μεγάλου όγκου τους. Οι ενέργειες των δικαιούχων παρακολουθούνται συνεχώς με τη συμβολή διαφόρων μηχανισμών και οι παραβιάσεις αντιμετωπίζονται με ανάλογο τρόπο.

7.1 Βασικές λειτουργίες του συστήματος

7.1.1 Δίκτυο Blockchain

Για την αποθήκευση των πληροφοριών στο συγκεκριμένο σύστημα, οι κόμβοι συναίνεσης και επεξεργασίας είναι ολοκληρωτικά υπεύθυνοι για τη μετάδοση του μπλοκ στο δίκτυο Blockchain. Τα αιτήματα που λαμβάνει το σύστημα από τους εξωτερικούς χρήστες για την πρόσβαση σε επιθυμητά δεδομένα, εξελίσσονται σε μπλοκ και αργότερα μεταδίδονται στην αλυσίδα κατά τη διάρκεια παράδοσης του πακέτου στον χρήστη. Η τελευταία ενέργεια κορυφώνει την ολοκλήρωση δημιουργίας του μπλοκ και επιτρέπει την εκπομπή του στο δίκτυο Blockchain. Κάθε μπλοκ αναγνωρίζεται από τη μοναδική του τιμή η οποία είναι και ταυτότητά του.

Η σημασία της υλοποίησης των πλευρικών μπλοκ στο δίκτυο, είναι η διατήρηση ενός αποτελεσματικού αρχείου καταγραφής και της αποτελεσματικής ανάκτησης των μπλοκ με σκοπό την έρευνα και την εμφάνιση παραβιάσεων όρων. Προσαρτώνται στα γονικά μπλοκ και περιλαμβάνουν ευρετηριασμένες αναφορές, πανομοιότυπες με εκείνες που αναγράφονται στη βάση δεδομένων των έξυπνων συμβολαίων. Η δημιουργία πολλαπλών συνδέσεων στο δίκτυο, συγκεντρώνει μία ολοκληρωμένη συλλογή αναφορών.

Όπως αναφέρθηκε, ένα μπλοκ δημιουργείται από μία επεξεργασμένη φόρμα, η οποία αντιπροσωπεύει ένα αίτημα που έχει ληφθεί από κάποιον εξωτερικό χρήστη. Περιέχει πληροφορίες σχετικές με την παραλαβή του αιτήματος, την επεξεργασία και την παράδοση των δεδομένων. Οι κόμβοι επεξεργασίας και συναίνεσης είναι εξ ολοκλήρου υπεύθυνοι για τη συντήρηση του δικτύου Blockchain. Στην πραγματικότητα είναι οι μόνες οντότητες με άμεση πρόσβαση. Κατά την παρακολούθηση του δικτύου και συγκεκριμένα των πλευρικών μπλοκ, οι κόμβοι προειδοποιούν το σύστημα για παραβιάσεις στη χρήση των δεδομένων.

7.1.2 Κλειδιά Κρυπτογράφησης

Τα κλειδιά κρυπτογράφησης επισημαίνονται για την εκτέλεση συγκεκριμένων εργασιών που σχετίζονται με την ασφάλεια αυτών στο σύστημα. Για την ανταλλαγή και μετάδοση δεδομένων μεταξύ "μη αξιόπιστων" κόμβων, απαιτούνται τα κλειδιά κρυπτογράφησης, εξασφαλίζοντας ένα επίπεδο ασφάλειας στο σύστημα. Παρακάτω φαίνεται η περιγραφή τους.

- Ιδιωτικό Κλειδί του χρήστη

Ο χρήστης που στέλνει στο σύστημα το αίτημα για πρόσβαση στα δεδομένα, δημιουργεί το δικό του ιδιωτικό κλειδί και το χρησιμοποιεί για να βάλει τη δική του "ψηφιακή υπογραφή" επάνω σε αυτό.

- Δημόσιο Κλειδί του χρήστη

Ο χρήστης στέλνει σε συνδυασμό με το αίτημα, το δημόσιο κλειδί που έχει δημιουργήσει ώστε να χρησιμοποιηθεί για την επαλήθευση της ταυτότητάς του μέσα από τον έλεγχο της ψηφιακής υπογραφής.

- Κλειδί Έξυπνου Συμβολαίου

Ένα ζεύγος κλειδιών παράγεται από τον αυθεντικοποιητή τα οποία επισυνάπτονται στο έξυπνο συμβόλαιο που παραδίδεται στον χρήστη ώστε να μπορεί να αποκρυπτογραφήσει

ο ίδιος τα δεδομένα που παρέλαβε, αλλά ταυτόχρονα να τηρούνται οι κανόνες του έξυπνου συμβολαίου ώστε να υπάρχει έλεγχος στη χρήση των δεδομένων από το σύστημα.

Περιληπτικά, ένας χρήστης ο οποίος επιθυμεί να αποκτήσει πρόσβαση σε σύνολα αρχείων από το σύστημα και από τον κάτοχο των δεδομένων, δημιουργεί ένα ζεύγος κλειδιών (ένα ιδιωτικό και ένα δημόσιο), αποθηκεύει το ιδιωτικό κλειδί και μοιράζεται το δημόσιο κλειδί με τον κάτοχο των δεδομένων. Ο χρήστης υπογράφει χρησιμοποιώντας το ιδιωτικό του κλειδί και στέλνει ένα αίτημα στο σύστημα. Κατά τη λήψη, ο κάτοχος των δεδομένων επιβεβαιώνει την εγκυρότητα του αιτήματος και την ταυτότητα του χρήστη, επαληθεύοντας την υπογραφή με το δημόσιο κλειδί του χρήστη.

Τα αποτελέσματα που έχουν προκύψει από την ανάκτηση των ζητούμενων αρχείων υποβάλλονται σε μία διαδικασία επεξεργασίας από το σύστημα και στη συνέχεια πριν παραδοθεί το αρχείο στο χρήστη, κρυπτογραφείται με ένα "κλειδί σύμβασης", το οποίο επισυνάπτεται στο έξυπνο συμβόλαιο που αποστέλνεται μαζί με τα δεδομένα. Με την αποκρυπτογράφηση του αρχείου, ο κάτοχος δεδομένων αποκτά πλήρη έλεγχο στις ενέργειες που πραγματοποιούνται από το χρήστη, καθώς αυτόματα ενεργοποιείται το έξυπνο συμβόλαιο.

Για να διασφαλιστεί επαρκώς η μεταφορά των ενεργειών που εκτελούνται στα δεδομένα από τον αιτούντα στο σύστημα, οι αναφορές που δημιουργούνται κατά τη χρήση τους, κρυπτογραφούνται χρησιμοποιώντας το κλειδί σύμβασης που έχει επισημανθεί στο συμβόλαιο και τελικά αποστέλλονται σε μία ασφαλή βάση δεδομένων.

7.1.3 Εντολές μετάφρασης (Triggers)

Οι εντολές μετάφρασης είναι οντότητες που συνδέουν τις διεργασίες μεταξύ της δομής που λαμβάνει τα αιτήματα και του δικτύου Blockchain. Ο βασικός ρόλος της εφαρμογής των triggers στο σύστημα, είναι να επιτρέψει στα έξυπνα συμβόλαια την έμμεση σύνδεση του συστήματος με το εξωτερικό περιβάλλον του συστήματος, αφού τα τελευταία δεν είναι εφικτό να αλληλοεπιδράσουν άμεσα με δομές εκτός δικτύου. Δεν κρατούν καμία πληροφορία και λειτουργούν μόνο ως διαμεσολαβητές για την ομαλή επικοινωνία του επιπέδου των αιτημάτων με το επίπεδο επεξεργασίας αυτών. Τα triggers, ενημερώνουν επίσης, τις καταστάσεις διεργασίας από και προς το επίπεδο των αιτημάτων που βασίζονται σε χαρακτηριστικά του έξυπνου συμβολαίου.

7.2 Σχεδιασμός του συστήματος

7.2.1 Χρήστες του Συστήματος

Είναι όλοι οι χρήστες των οποίων η πρόθεση είναι να αποκτήσουν πρόσβαση στα ιατρικά δεδομένα, είτε για ερευνητικούς λόγους είτε για άλλους χρήσιμους σκοπούς. Παραδείγματα αυτών είναι οι οργανισμοί υγειονομικής περίθαλψης, όπως τα νοσοκομεία, ερευνητικά ινστιτούτα, πανεπιστήμια και επιστήμονες που διεξάγουν προσωπική έρευνα. Οι χρήστες στέλνουν αιτήματα στο σύστημα για πρόσβαση στα δεδομένα, τα οποία υποβάλλονται σε μία διαδικασία επεξεργασίας.

Εικόνα 7.2.1 : Οι Χρήστες του Συστήματος

7.2.2 Πεδίο Παραλαβής Αιτημάτων

Το μοντέλο αποτελείται από δομές οι οποίες λαμβάνουν, επεξεργάζονται και ανταποκρίνονται στα αιτήματα που τοποθετούνται στο σύστημα και σχετίζονται με την πρόσβαση στα υπάρχοντα δεδομένα. Το συγκεκριμένο επίπεδο αλληλεπιδρά άμεσα με το επίπεδο επεξεργασίας και μετάδοσης δεδομένων και διαθέτει ενσωματωμένους μηχανισμούς ωστέ να ερμηνεύει και να μεταφράζει ενέργειες μεταξύ του εσωτερικού και του εξωτερικού περιβάλλοντος. Επιπλέον, οι χρήστες, επικοινωνούν απευθείας με το μηχανισμό αυτόν για την αποστολή αιτημάτων. Τα συστατικά του στοιχεία είναι :

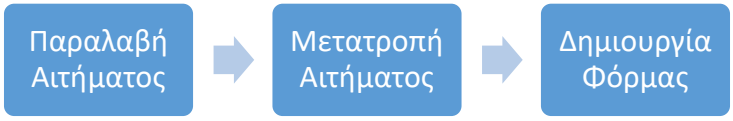
- ***Δομή Μετατροπής Αιτημάτων***

Είναι υπεύθυνο για τη μετατροπή των αιτημάτων σε μία μορφή η οποία θα μπορεί να αναγνωριστεί από το πεδίο επεξεργασίας και μετάδοσης δεδομένων. Από τη μετατροπή προκύπτει μία τιμή η οποία αντικαθιστά το αίτημα και μπορεί να διαβαστεί από το σύστημα για την ανάκτηση των ζητούμενων πληροφοριών. Ο τελικός του ρόλος είναι η

ανταπόκριση και η αποστολή “απάντησης” στον αιτούντα με βάση το αίτημα που έχει καταβάλλει.

- ***Δομή “Μετάφρασης” Έξυπνων Συμβολαίων***

Το παρόν σύστημα έχει την ευθύνη να μεταφράζει τις ενέργειες των έξυπνων συμβολαίων από και προς το περιβάλλον τους αφού αυτό δε μπορέι να λειτουργήσει έξω από ένα δίκτυο Blockchain αυτόνομα.



Εικόνα 7.2.2 : Η επεξεργασία που υποβάλλεται το αίτημα ενός χρήστη

7.2.3 Επεξεργασία και Μετάδοση Δεδομένων

Το μοντέλο περιλαμβάνει μεμονωμένα εξαρτήματα που συμβάλλουν στην επεξεργασία του αιτήματος του χρήστη για την πρόσβαση στη βάση δεδομένων. Επιπροσθέτως, εκτελούνται υπολογισμοί στα ζητούμενα δεδομένα και προστίθενται λειτουργίες οι οποίες ανιχνεύουν οποιαδήποτε ενέργεια εκτελείται πάνω σε αυτά. Αλγόριθμοι και διάφορες δομές εφαρμόζονται επάνω στα δεδομένα και αναλαμβάνουν να δίνουν αναφορά σχετικά με τις ενέργειες που πραγματοποιούνται. Οι αναφορές αποθηκεύονται και ευρετηριάζονται σε μία βάση δεδομένων, και σε περίπτωση παραβίασης, ενεργοποιούνται μηχανισμοί φραγής. Τα αποτελέσματα κάθε ενέργειας η οποία έχει ολοκληρωθεί μεταδίδονται σε ένα αμετάβλητο δίκτυο που εγγυάται το δίκαιο έλεγχο. Το σύστημα έχει επίσης την ευθύνη της αυθεντικοποίησης κάθε αιτήματος και ενέργειας η οποία αφορά την πρόσβαση στους ιατρικούς ηλεκτρονικούς φακέλους. Οι υπάρχουσες οντότητες του επιπέδου αναγράφονται παρακάτω.

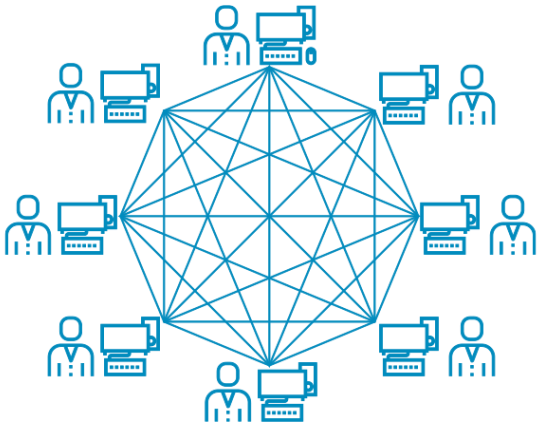
- ***Αυθεντικοποιητής***

Ο αυθεντικοποιητής είναι υπεύθυνος για την επαλήθευση της “νομιμότητας” των αιτημάτων που προέρχονται από τους χρήστες. Παράγει κλειδιά τα οποία χρησιμοποιούνται για να κρυπτογραφήσουν ενέργειες στα δεδομένα από το περιβάλλον του χρήστη στο περιβάλλον επεξεργασίας δεδομένων. Επισημαίνει τα κλειδιά κρυπτογράφησης στην οντότητα που είναι υπεύθυνη για την αναφορά τέτοιων ενεργειών. Αναλαμβάνει, επίσης, να κρυπτογραφήσει το πακέτο που περιέχει τα δεδομένα τα οποία τελικά παραδίδονται στον αιτούντα.

Εικόνα 7.2.3.α : Ιδιωτικό και Δημόσιο κλειδί

- ***Κόμβοι Επεξεργασίας και Συναίνεσης***

Οι κόμβοι επεξεργασίας και συναίνεσης επεξεργάζονται τις φόρμες οι οποίες δημιουργούνται από τα αιτήματα τα οποία αργότερα αναπτύσσονται σε μπλοκ και μεταδίδονται στο δίκτυο Blockchain. Επιπλέον, ο κόμβος συναίνεσης δημιουργεί τα πακέτα που περιέχουν τα ζητούμενα δεδομένα και το έξυπνο συμβόλαιο τα οποία τελικά παραδίδονται στα χέρια του χρήστη. Οι κόμβοι μπορεί να είναι από ιατρικοί φορείς ή ερευνητικά ιδρύματα

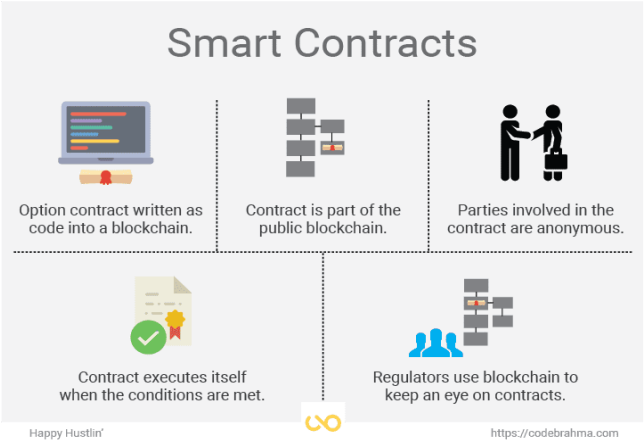


Εικόνα 7.2.3.β : Κόμβοι που συμμετέχουν στην επεξεργασία του αιτήματος

- ***Δομή Παραγωγής Έξυπνων Συμβολαίων***

Τα έξυπνα συμβόλαια είναι σχεδιασμένες λειτουργίες που ενεργοποιούνται και εκτελούνται κατά τη λήψη μιας ενέργειας. Τα συμβόλαια που παράγονται από το κέντρο αυτό, έχουν ενσωματωμένα κλειδιά κρυπτογράφησης που επιτρέπουν στα συμβόλαια να κρυπτογραφούν αναφορές οι οποίες δημιουργούνται κατά την διαχείριση των δεδομένων από το χρήστη. Στην ουσία, ο κύριος ρόλος ενός έξυπνου συμβολαίου είναι να προσδιορίσει ενέργειες οι οποίες εκτελούνται στα δεδομένα που αποστέλλονται και να τα καταγράψει στη βάση δεδομένων των συμβολαίων. Ακόμα, τα έξυπνα συμβόλαια

αποτρέπουν την πρόσβαση στα δεδομένα σε περίπτωση που παραβιαστεί κάποιος κανόνας.



Εικόνα 7.2.3.γ : Έξυπνα Συμβόλαια

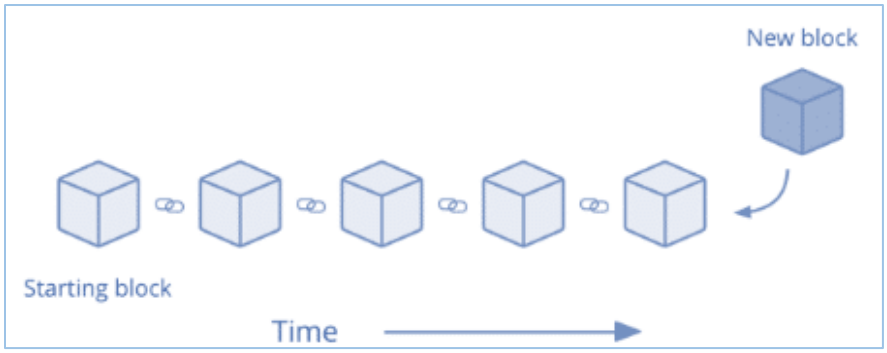
- ***Βάση Δεδομένων των Έξυπνων Συμβολαίων***

Η βάση δεδομένων των έξυπνων συμβολαίων είναι ένας μηχανισμός αποθήκευσης οποιασδήποτε κακόβουλης ενέργειας, ο οποίος ενεργοποιείται κατά τη λήψη κάποιας αναφοράς σχετικά με την παραβίαση των δεδομένων, από τους κόμβους επεξεργασίας και συναίνεσης. Από τη στιγμή, που παραβιαστεί κάποιος όρος που αναγράφεται στο συμβόλαιο, αναφέρεται αυτόματα στο σύστημα, με την αναφορά να αποθηκεύεται στη βάση αυτή.

Εικόνα 7.2.3.δ : Βάση Δεδομένων Έξυπνων Συμβολαίων

- ***Δίκτυο Blockchain***

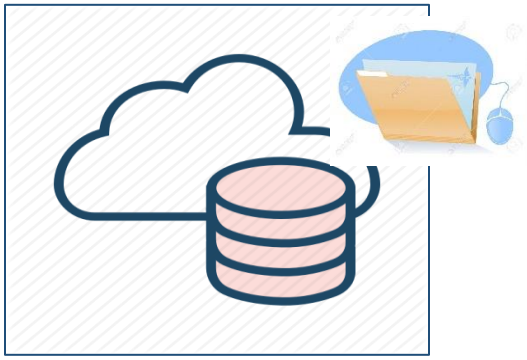
Το δίκτυο Blockchain αποτελείται από τα μπλοκ που μεταδίδονται σε αυτό και σχηματίζουν μία αλυσίδα μεταξύ τους σε μία χρονολογική σειρά. Ο βασικός του ρόλος είναι να διατηρήσει μία χρονολογικά κατανεμημένη βάση δεδομένων από ενέργειες οι οποίες θα αφορούν τα ζητούμενα δεδομένα και την παράδοσή τους. Η αλυσίδα κατασκευάζει πλευρικά μπλοκ για μεμονωμένες ενέργειες σχετικές με συγκεκριμένες πληροφορίες που αναγράφονται στα έξυπνα συμβόλαια.



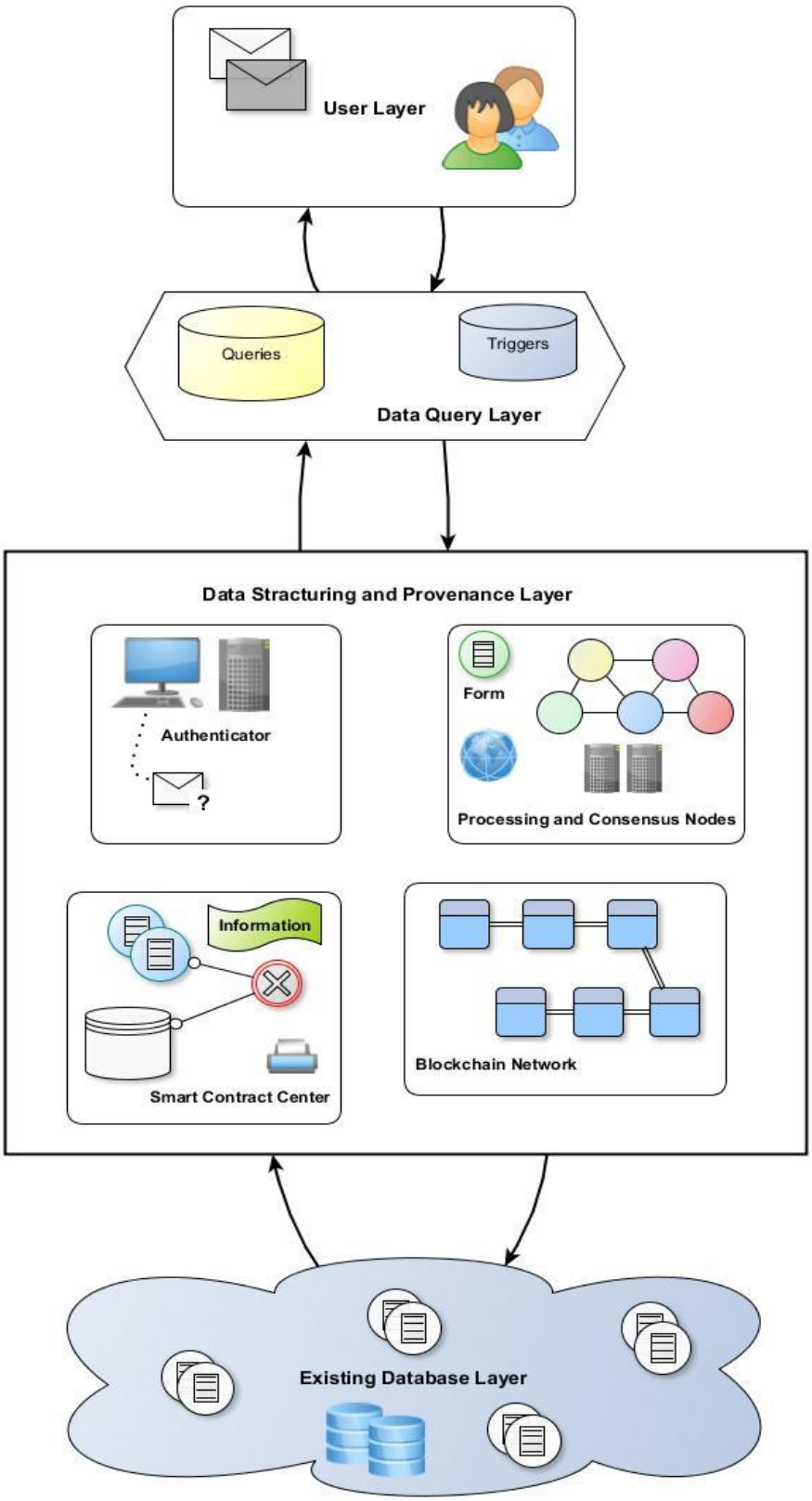
Εικόνα 7.2.3.ε : Αλυσίδα Blockchain

7.2.4 Βάση Δεδομένων Cloud Computing

Η βάση δεδομένων περιέχει λειτουργίες οι οποίες χρησιμοποιούνται για την εκτέλεση συγκεκριμένων εργασιών. Σε αυτό το σύστημα, πρόσβαση έχει μόνο εξουσιοδοτημένο προσωπικό από τους κόμβους συναίνεσης, δεδομένου ότι φιλοξενούν ευαίσθητες πληροφορίες οι οποίες απαιτούν ασφαλείς μηχανισμούς για την επαρκή προστασία τους. Για την πρόσβαση στα δεδομένα αυτής της βάσης, οι απαιτούμενες πληροφορίες διαβιβάζονται μέσω υπολογισμών για να μπορέσει να γίνει εφικτή η κοινή χρήση τους.



Εικόνα 7.2.4 : Βάση Δεδομένων με τους Ιατρικούς φακέλους



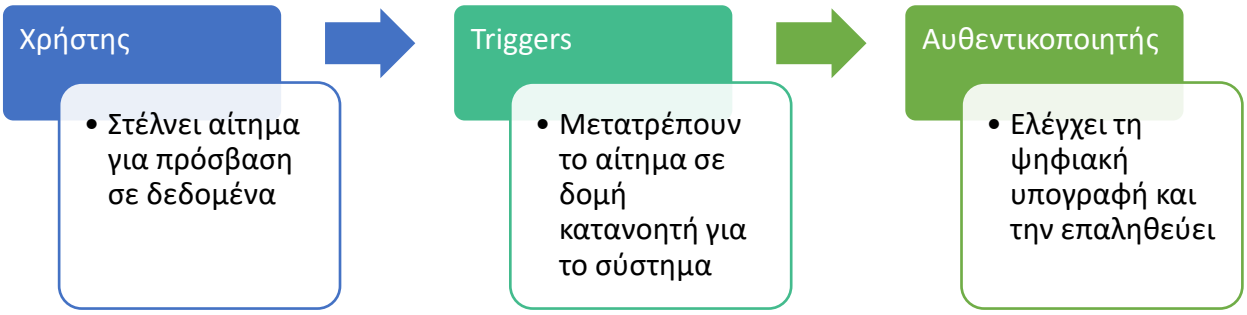
Εικόνα 7.2 : Η Δομή του Μοντέλου

7.3 Λειτουργία του συστήματος

7.3.1 Παραλαβή Αιτήματος

Ο χρήστης στέλνει ένα αίτημα ώστε να αποκτήσει πρόσβαση σε συγκεκριμένα δεδομένα που επιθυμεί. Το αίτημα υπογράφεται ψηφιακά από το χρήστη μέσω του ιδιωτικού του κλειδιού το οποίο έχει δημιουργηθεί προγενέστερα. Το αίτημα αρχικά συναντάει το επίπεδο παραλαβής αιτημάτων. Τα triggers που βρίσκονται στο σύστημα μεταβάλλουν το αίτημα σε μία δομή η οποία θα μπορεί να διαβαστεί από το σύστημα που επεξεργάζεται και μεταδίδει τα δεδομένα και το μεταβιβάζουν στο επίπεδο αυτό.

Αρχικά ο αυθεντικοποιητής επαληθεύει τη νομιμότητα του αιτήματος ελέγχοντας την υπογραφή, χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί του αιτούντος το οποίο έχει διανεμηθεί από το χρήστη κατά την αποστολή του αιτήματός του. Αν η υπογραφή είναι έγκυρη, τότε η διαδικασία συνεχίζεται, διαφορετικά διακόπτεται και θεωρείται ως μη έγκυρο αίτημα.



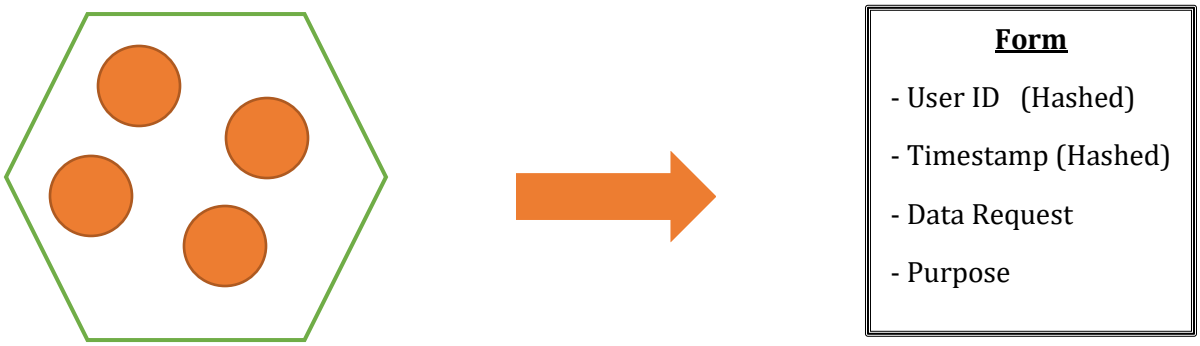
Εικόνα 7.3.1 : Διεργασία Αποδοχής Αιτήματος στο Σύστημα

7.3.2 Επεξεργασία Αιτήματος

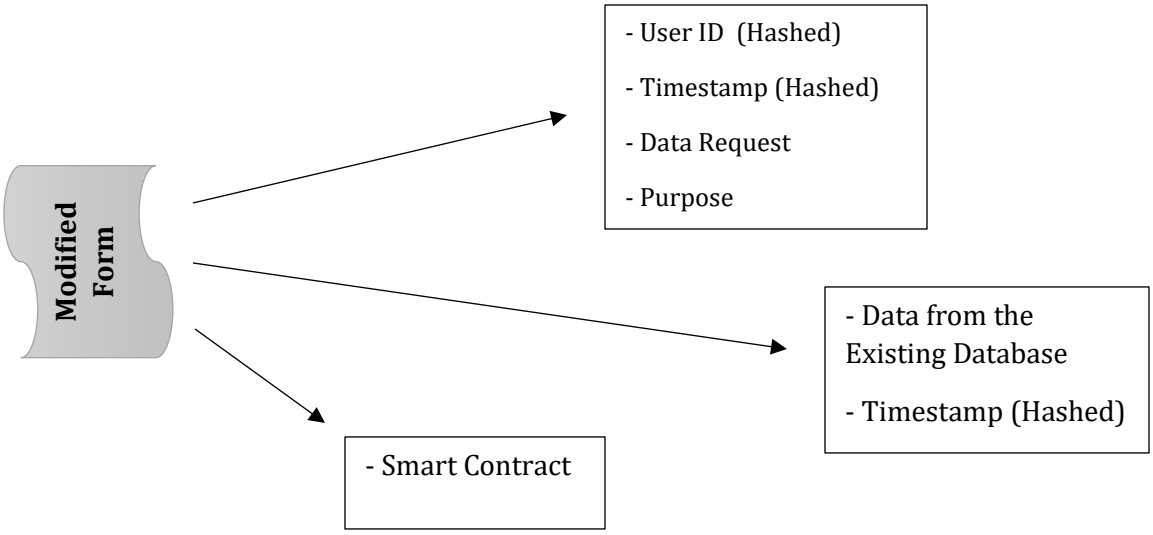
Από τη στιγμή που εγκρίνεται το αίτημα, οι κόμβοι επεξεργασίας και συναίνεσης αναλαμβάνουν να το μετατρέψουν σε μία κατάλληλη φόρμα η οποία θα περιλαμβάνει, εκτός των επιθυμητών δεδομένων, μία μοναδική τιμή που εκπροσωπεί την ταυτότητα του αιτούντος (User ID), αλλά και μία χρονολογική σφραγίδα σχετικά με το χρόνο παραλαβής του αιτήματος (Timestamp). Οι δύο τιμές προσαρτώνται στη φόρμα, αφού πρώτα κατακερματιστούν, μέσα από μία μαθηματική συνάρτηση κατακερματισμού (Hash

Function). Ο λόγος επίσης, για τον οποίο ζητούνται τα συγκεκριμένα δεδομένα επισημαίνεται στη φόρμα και τελικά η τελευταία μεταφέρεται στην υπάρχουσα βάση δεδομένων.

Η υπάρχουσα βάση δεδομένων λαμβάνει τη φόρμα, ανακτά τα δεδομένα τα οποία ζητούνται και τα στέλνει πίσω στο επίπεδο επεξεργασίας και προέλευσης όπου θα ακολουθήσει η πρώτη τροποποίηση από τους κόμβους συναίνεσης. Η χρονολογική σφραγίδα του αιτήματος η οποία δημιουργήθηκε στη φόρμα, θα σημειωθεί στις ανακτώμενες πληροφορίες. Στη συνέχεια, οι κόμβοι συναίνεσης στέλνουν αίτημα στο κέντρο των έξυπνων συμβολαίων για τη θεσμοθέτηση κανόνων σχετικά με τα ζητούμενα δεδομένα. Το αντίστοιχο έξυπνο συμβόλαιο θα παραχθεί και θα ενσωματωθεί στη φόρμα μαζί με τα δεδομένα.



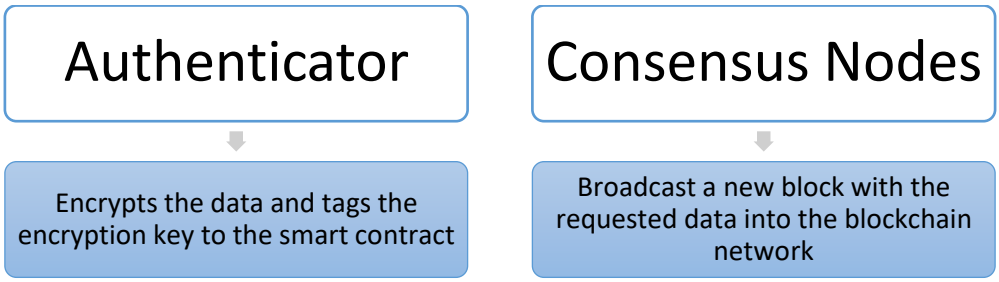
Εικόνα 7.3.2.Α : Δημιουργία της φόρμας από τους κόμβους συναίνεσης



Εικόνα 7.3.2.Β : Τροποποιημένη Φόρμα

7.3.3 Διανομή των ζητούμενων Δεδομένων

Η νέα πλέον φόρμα που είναι αποτέλεσμα της προηγούμενης επεξεργασίας αποστέλλεται στον αυθεντικοποιητή ώστε να περάσει από το τελικό στάδιο. Ο αυθεντικοποιητής παράγει ένα κλειδί κρυπτογράφησης και το επισημαίνει στο έξυπνο συμβόλαιο που έχει δημιουργηθεί. Με το κλειδί, ο χρήστης θα έχει τη δυνατότητα να αποκρυπτογραφήσει τα δεδομένα που έχει ζητήσει. Το γεγονός αυτό είναι σημαντικό για να επιτευχθεί η ασφαλής μετάδοση και η ανίχνευση των πληροφοριών. Ταυτόχρονα οι κόμβοι συναίνεσης κατασκευάζουν ένα μπλοκ βασισμένο στις πληροφορίες που έχουν ζητηθεί από το χρήστη και το μεταδίδουν στην αλυσίδα Blockchain σύμφωνα με τη χρονολογική σειρά κατά την οποία έχει δημιουργηθεί. Όπως είναι αναμενόμενο, το μπλοκ θα έχει τη μοναδική αναγνωριστική του τιμή, ύστερα από τις κρυπτογραφικές μεθόδους στις οποίες θα έχει υποβληθεί, όπως γίνεται γενικότερα σε ένα δίκτυο Blockchain.



Εικόνα 7.3.3 : Οι διεργασίες πριν την παράδοση των δεδομένων στον χρήστη

Το πακέτο το οποίο έχει δημιουργηθεί από την επεξεργασία των ζητούμενων δεδομένων που ανακτώνται από την υπάρχουσα βάση δεδομένων, περιλαμβάνει τα δεδομένα, την τιμή της "ταυτότητάς" τους (Data ID) και το έξυπνο συμβόλαιο με τους όρους χρήσης των δεδομένων. Τελικά, το πακέτο κρυπτογραφείται ολόκληρο από τον αυθεντικοποιητή ώστε να μπορεί να αναγνωριστεί μόνο από τον κάτοχο του κατάλληλου ιδιωτικού κλειδιού και συγκολλώντας την αναγνωριστική τιμή του χρήστη (User ID), αποστέλλεται πίσω στο σύστημα παραλαβής αιτημάτων από όπου ξεκίνησε. Το έξυπνο συμβόλαιο είναι η αιτία για την αποτελεσματική παρακολούθηση του πακέτου.

7.3.4 Παράδοση των δεδομένων στο χρήστη

Ο χρήστης λαμβάνει το επεξεργασμένο πακέτο και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Θα πρέπει με κάποιον τρόπο να επικυρωθεί η ασφάλεια του. Στο σημείο αυτό, θα παίξουν καταλυτικό ρόλο τα συμβόλαια που έχουν διαμορφωθεί από το σύστημα επεξεργασίας.

Με το κλειδί που βρίσκεται προσαρτημένο στο έξυπνο συμβόλαιο, ο χρήστης αποκρυπτογραφεί τα δεδομένα και αυτόματα εκείνο ενεργοποιείται. Οποιαδήποτε ενέργεια πάνω στα αποκρυπτογραφημένα δεδομένα που έλαβε ο χρήστης, αναφέρεται και αποστέλλεται στο επίπεδο παραλαβής αιτημάτων, από όπου μεταφράζεται και μεταφέρεται στο επίπεδο επεξεργασίας και συγκεκριμένα στους κόμβους συναίνεσης. Εκείνοι με τη σειρά τους, αποθηκεύουν την αναφορά στην αλυσίδα Blockchain σε ένα πλευρικό μπλοκ το οποίο συνδέεται άρρηκτα με το μπλοκ που προστέθηκε κατά την διάρκεια της προηγούμενης διαδικασίας. Η αιτία για την οποία κρατείται το αρχείο που περιέχει τις ενέργειες που πραγματοποιούνται στα στοιχεία είναι για την αποφυγή κακόβουλης χρήσης τους. Η εγκατάσταση τέτοιων αναφορών απεικονίζει την ικανότητα που έχει το έξυπνο συμβόλαιο να ενεργοποιεί συγκεκριμένες προϋποθέσεις κατά την εκτέλεση οποιασδήποτε πράξης που συνδέεται άμεσα με τα ζητούμενα δεδομένα. Μέσω της συγκεκριμένης ιδιότητας, επιτυγχάνεται ο έλεγχος των εγγράφων που διαθέτει ο χρήστης.

7.3.5 Η Λειτουργία των Έξυπνων Συμβολαίων

Τα έξυπνα συμβόλαια λειτουργούν ως μηχανές οι οποίες εκτελούν προκαθορισμένες οδηγίες κατά την πραγματοποίηση ενεργειών, οι οποίες ακολουθούν ένα οργανωμένο πλαίσιο. Αξιοποιούνται για την αναφορά ενεργειών σχετικά με τα δεδομένα που ρωτήθηκαν από το σύστημα του χρήστη και επιτρέπουν στους κάτοχους των δεδομένων την ασφάλεια και τον έλεγχο τους, δεδομένου ότι θα παρακολουθούνται μέσα σε ένα ελεγχόμενο περιβάλλον εξαλείφοντας τη σχέση εμπιστοσύνης που απαιτείται να υπάρχει μεταξύ του τελευταίου και του χρήστη.

Όπως προαναφέρθηκε, οι αναφορές για τις ενέργειες των δεδομένων που προκύπτουν από το σύστημα του χρήστη, αναπροσαρμόζονται και μεταδίδονται στο δίκτυο Blockchain. Σε κάποιες περιστάσεις, οι αναφορές αποθηκεύονται και σε μία άλλη βάση δεδομένων των έξυπνων συμβολαίων και ταξινομούνται με βάση την αναγνωριστική τιμή των δεδομένων (Data ID). Ένα σύνολο ενεργειών μπορούν να εφαρμοστούν πάνω στα δεδομένα που λαμβάνει ο χρήστης, οι οποίες θα ενεργοποιούν τα έξυπνα συμβόλαια ώστε να αποσταλεί μία έκθεση με βάση τους κανόνες που έχουν προκαθοριστεί.

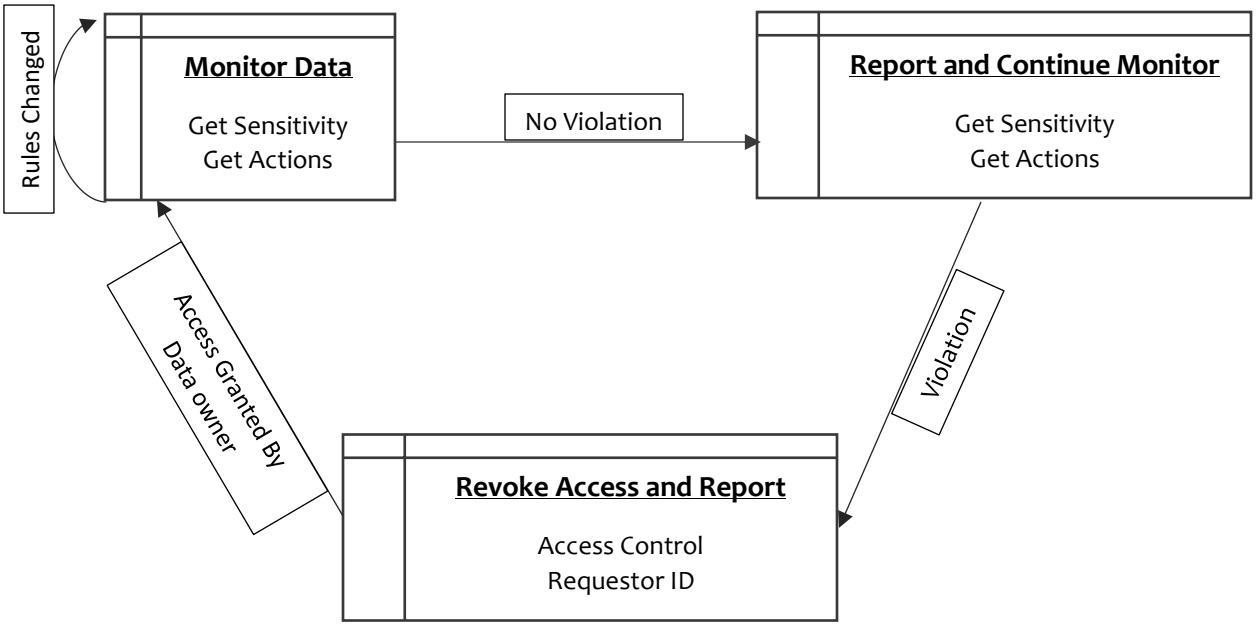
Η ευαισθησία των δεδομένων μπορεί να κατηγοριοποιηθεί σε υψηλή και χαμηλή. Αυτό καθορίζεται από τους κόμβους συναίνεσης όταν αποκτούν τα δεδομένα από την υπάρχουσα βάση. Με βάση το βαθμό σημαντικότητας του πακέτου, ορισμένες ενέργειες εξαιρούνται από τη λίστα κακόβουλων πράξεων, ενώ άλλες αποτελούν παραβιάσεις.

Για χαμηλό βαθμό σημαντικότητας, οι κόμβοι συναίνεσης μπορούν να τροποποιήσουν τα έξυπνα συμβόλαια ώστε να αποφευχθεί η αναφορά και η αποθήκευση εξωτερικών ενεργειών. Για υψηλής ευαισθησίας δεδομένα, το έξυπνο συμβόλαιο υποχρεούται να αναφέρει οποιαδήποτε ενέργεια, για την αποτελεσματική παρακολούθηση των λειτουργιών που εκτελούνται στα δεδομένα, εξασφαλίζοντας τον εντοπισμό παραβιάσεων επάνω σε αυτά.

Η ταυτότητα των δεδομένων που διευκρινίζεται στα έξυπνα συμβόλαια προσδίδει πλεονέκτημα στη δημιουργία ενός αποτελεσματικού μέσου, ώστε οι κόμβοι συναίνεσης να έχουν τη δυνατότητα να αντιστοιχίσουν, να επεξεργαστούν και να επαληθεύσουν το αντίστοιχο μοναδικό μπλοκ. Τα σχόλια παράγονται για να περιγράψουν τις εκτελεσμένες ενέργειες του χρήστη στα δεδομένα. Στις περισσότερες περιπτώσεις είναι σχόλια παράβασης ή εξαίρεσης. Με την εξαγωγή ενός κλειδιού, μέσω συγκεκριμένων εντολών, αυτά κρυπτογραφούνται και αποθηκεύονται στη βάση δεδομένων των έξυπνων συμβολαίων. Τα δικαιώματα που δηλώνει ο κάτοχος των δεδομένων ορίζονται πάνω στα έξυπνα συμβόλαια. Σε περίπτωση παραβίασης της σύμβασης, η πρόσβαση στα δεδομένα ανακαλείται και εκκρεμεί επανεξέταση από τους κόμβους συναίνεσης οι οποίοι έχουν την επιλογή να παραχωρήσουν εκ νέου νέα πρόσβαση ή να καταστείλουν την παραχώρηση των δεδομένων από τον αιτούντα. Η αναξιόπιστη μεταχείριση των δεδομένων αντιμετωπίζεται με ανάλογο τρόπο από τον κάτοχο τους.

```
Require: Initialization of parameters:
getAction, getSensitivity, getRequestorID, getOwnerID,
getDataID, getKey, getMetaIndex, retrieve, encrypt, comment,
report, accessControl;
Ensure: Setting up functions:
func (getSensitivity)
func (getAction)
func (comment)
func (accessControl)
MONITORING OF PACKAGE:
for func (getAction) DD decrypt do
func (comment)  Potray, Data with DataID has been
decrypted.
retrieve (getKey)
encrypt (comment)
report (commentǁgetRequestorIDǁgetOwnerID)
end for
if func (getSensitivity) DD Low then
func (getAction)  Exemptions on data.
Ignore
else if func (getSensitivity) DD Low then
func (getAction)  Not exemptions on data (violation).
func (comment)  Data violation concatenated with
DataID
func (accessControl)  Revokes access to data.
retrieve (getKey)
encrypt (comment)
report (commentǁgetRequestorIDǁgetOwnerID)
else {func (getSensitivity) DD High}
func (getAction)  Violation.
func (comment)  Data violation concatenated with
DataID
func (accessControl)  Revokes access to data.
retrieve (getKey)
encrypt (comment)
report (commentǁgetRequestorIDǁgetOwnerID)
end if
```

Εικόνα 7.3.5.Α : Έξυπνο Συμβόλαιο για την προστασία των δεδομένων



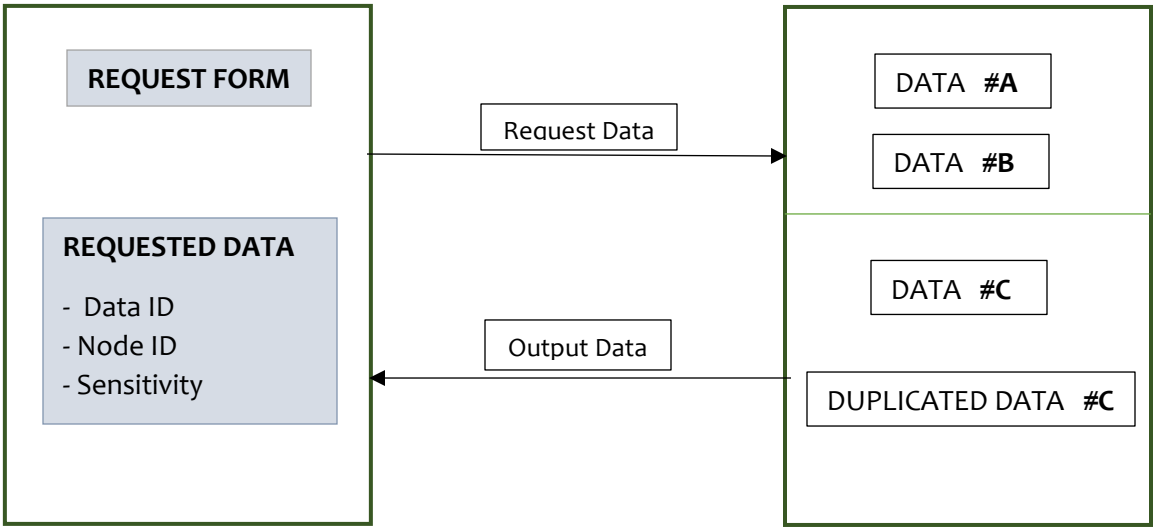
Εικόνα 7.3.5.Β : Διαχείριση Έξυπνων Συμβολαίων

7.3.6 Ανταλλαγή Δεδομένων μεταξύ της Βάσης και των κόμβων συναίνεσης

Η ανταλλαγή δεδομένων μεταξύ της υπάρχουσας βάσης δεδομένων και των κόμβων συναίνεσης είναι κρίσιμη για την αποτελεσματική και ασφαλή λειτουργία του συστήματος διαμοιρασμού πληροφοριών μεταξύ οντοτήτων όπου δεν υπάρχει εμπιστοσύνη. Τα δεδομένα που εκδίδονται από τη βάση, πρέπει να διατηρούν την ακεραιότητα και για το λόγο αυτόν, οι μέθοδοι ανταλλαγής τους είναι αναγκαίο να σχεδιαστούν και να δομηθούν με μεγάλη προσοχή.

Για το αίτημα που έχει εγκριθεί, η υπάρχουσα βάση δεδομένων δημιουργεί αντίγραφο των ζητούμενων στοιχείων και τα προωθεί στους κόμβους συναίνεσης οι οποίοι είναι υπεύθυνοι για τη διαμόρφωση ολόκληρου του πακέτου. Το πακέτο περιλαμβάνει εκτός των δεδομένων, μία αναγνωριστική τιμή αυτών (Data ID) αλλά και μία αναγνωριστική τιμή του κόμβου συναίνεσης που ανέλαβε την επεξεργασία. Ο αρμόδιος για την τροποποίηση κόμβος, επαληθεύει τα δεδομένα που παρέλαβε συγκρίνοντας τον τύπο τους με το αίτημα που κατοχυρώθηκε. Εκείνα ταξινομούνται σε μία κλίμακα που χαρακτηρίζεται από υψηλή ή χαμηλή ευαισθησία. Για ένα υψηλής ευαισθησίας σύνολο δεδομένων, υπάρχει ανάγκη για μεγαλύτερη ασφάλεια και ανωνυμία. Οι ενέργειες που εκτελούνται αξιοποιώντας τις απεσταλμένες πληροφορίες, καταγράφονται σε μία μορφή που θα τις μετατρέψει τελικά σε μπλοκ και θα προστεθεί στο δίκτυο. Το αποτέλεσμα που προκύπτει από την διαχείριση των δεδομένων, γίνεται διαθέσιμο και σε ένα δεύτερο κόμβο

ώστε να επικυρωθεί η εργασία που πραγματοποιήθηκε από τον πρώτο κόμβο. Μόλις αυτή θεωρηθεί ακριβής, τότε επιστρέφονται στον πρώτο κόμβο.



Εικόνα 7.3.6 : Ανάκτηση Πληροφοριών από τη Βάση Δεδομένων

Ο κόμβος συναίνεσης στέλνει ένα αίτημα στο οποίο αναγράφεται το επίπεδο ευαισθησίας των δεδομένων, στη γεννήτρια έξυπνων συμβολαίων ώστε να παραχθεί η ανάλογη σύμβαση με τους κανόνες. Τελικά προσαρτάται μαζί με τα ζητούμενα δεδομένα και το ολοκληρωμένο πλέον αρχείο κρυπτογραφείται από τον αυθεντικοποιητή με το δημόσιο κλειδί του χρήστη και εξάγεται μία χρονική σφραγίδα κατά την ολοκλήρωση της διαδικασίας. Όλες οι χρονικές στιγμές από την επεξεργασία καταγράφονται από τον κόμβο συναίνεσης ώστε να επιτραπεί βελτιστοποίηση με γνώμονα την αποδοτικότητα. Επιπλέον, στη φόρμα με τις εκτελούμενες ενέργειες συμπεριλαμβάνεται και η συμβολή του δεύτερου κόμβου. Το αρχείο αναδιαμορφώνεται σε μπλοκ και είναι πλέον έτοιμο να προστεθεί στην αλυσίδα Blockchain.

7.3.7 Δομή του Κύριου Μπλοκ στην αλυσίδα Blockchain

Κάθε μπλοκ, όπως είχε αναφερθεί και στην περιγραφή της τεχνολογίας Blockchain, προσδιορίζεται με μοναδικό τρόπο και περιγράφεται από μία κατακερματισμένη τιμή που έχει υπολογιστεί. Το μπλοκ περιλαμβάνει το μέγεθός του (Block Size), καθώς και την επικεφαλίδα του μπλοκ (Block Header). Η επικεφαλίδα έχει περάσει από τη διαδικασία του κατακερματισμού μέσω του αλγορίθμου SHA-256 και διαδραματίζει σπουδαίο ρόλο στην αλυσίδα Blockchain, καθιστώντας την αναλλοίωτη και αμετάβλητη. Περιέχει την

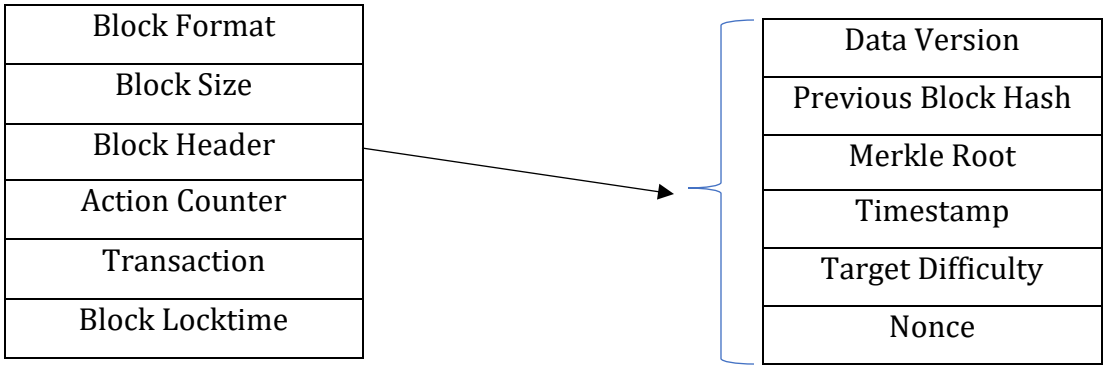
κατακερματισμένη τιμή του προηγούμενου μπλοκ που είχε προστεθεί στην αλυσίδα, επομένως οποιαδήποτε αλλαγή σε κάποιο μπλοκ θα πρέπει να μεταβάλλει ολόκληρη την αλυσίδα ξεκινώντας από το αρχικό μπλοκ, το Genesis μπλοκ. Το γεγονός αυτό, εξασφαλίζει σημαντικά την ακεραιότητα του δικτύου, αφού υπάρχει μέγιστη εγγύηση ότι δεν είναι δυνατή η επίτευξη του συγκεκριμένου στόχου. Ο μηχανισμός εγγυάται επίσης την προέλευση των δεδομένων, ώστε στην περίπτωση κακόβουλης δραστηριότητας, η αναντιστοιχία των μπλοκ θα προειδοποιήσει το σύστημα για την ενεργοποίηση ακριβούς εξακρίβωσης των δεδομένων.

Η επικεφαλίδα του μπλοκ αποτελείται από την έκδοση του μπλοκ (Block Version) που υποδεικνύει τους κανόνες που πρέπει να ακολουθηθούν για την επικύρωση δεδομένων στο μπλοκ και τις ιδιότητες θα που έχουν. Πέρα από την κατακερματισμένη τιμή του προηγούμενου μπλοκ που περιέχεται στην επικεφαλίδα, μέρος της αποτελεί και η ρίζα Merkle Tree, η οποία συμμετέχει στην ασφάλεια της αλυσίδας διασφαλίζοντας ότι κανένα από τα μπλοκ δε δύναται να τροποποιηθεί χωρίς το μετασχηματισμό της επικεφαλίδας. Η ρίζα Merkle Tree προκύπτει από τον κατακερματισμό όλων των εγγραφών που δέχεται το μπλοκ. Η έξοδος είναι αποτέλεσμα του αλγορίθμου SHA-256 όπως χρησιμοποιείται και σε ολόκληρη την επικεφαλίδα. Σημαντικό κόμματι της επικεφαλίδας αποτελεί η χρονική σφραγίδα της δημιουργίας του μπλοκ (Timestamp) αλλά και η τιμή δυσκολίας στόχου (Difficulty Target) η οποία συμβάλλει στον τρόπο με τον οποίο η επεξεργασία επιτυγχάνεται από τους κόμβους συναίνεσης. Η τιμή αυτή είναι μοναδική στο σύστημα για να καταστήσει την επεξεργασία δύσκολη για κακόβουλους κόμβους αλλά αποτελεσματική και επιλύσιμη από τους επαληθευμένους κόμβους συναίνεσης του συστήματος. Τέλος, η επικεφαλίδα περιλαμβάνει μία τιμή Nonce, η οποία είναι ένας αυθαίρετος αριθμός που ορίζουν οι κόμβοι συναίνεσης για τη δημιουργία της κατακερματισμένης τιμής της επικεφαλίδας σε συνδυασμό με την τιμή δυσκολίας στόχου.

Στο μπλοκ περιέχεται ένας μετρητής δραστηριοτήτων, η λειτουργία του οποίου είναι να καταγράψει τον συνολικό αριθμό κακόβουλων ενεργειών σε σχέση με τα δεδομένα που είναι καταγεγραμμένα σε αυτό. Κατηγοριοποιείται σε δύο κομμάτια, τις χρονικές σφραγίδες και το τμήμα δεδομένων. Οι χρονικές σφραγίδες κατατάσσονται με βάση το χρόνο παραλαβής του αιτήματος, το χρόνο που απαιτείται για την επεξεργασία του και το χρόνο που χρειάζεται για την αποστολή του αρχείου στο χρήστη. Το τμήμα δεδομένων αποτελείται από την ταυτότητα του ιδιοκτήτη των δεδομένων, την ευαισθησία τους, το σκοπό του αιτήματος, την ταυτότητα και την υπογραφή του κόμβου επεξεργασίας και συναίνεσης.

Η δομή που ορίζει ολόκληρο το μπλοκ είναι ο χρόνος κλειδώματος. Πρόκειται για μία χρονική σήμανση που καταγράφει την τελευταία καταχώρηση της συναλλαγής καθώς και

το κλείσιμο του μπλοκ. Όταν πληρούνται οι συνθήκες για αυτό το πεδίο, το μπλοκ είναι έτοιμο να μεταδοθεί στην αλυσίδα.



Εικόνα 7.3.7 : Η δομή του Κύριου μπλοκ

7.3.8 Δομή του Πλευρικού Μπλοκ

Ένα πλευρικό μπλοκ είναι μία μορφή που προέρχεται από την προσάρτηση ενός τμήματος σε ένα κύριο μπλοκ, παράγοντας ένα νέο μπλοκ με δική του ταυτότητα. Το πλευρικό μπλοκ αποτελείται από το μέγεθός του (Block size) αλλά και από την επικεφαλίδα με τα τμήματα που συναντώνται στο κύριο μπλοκ. Ειδικότερα, την έκδοση του μπλοκ που προσδιορίζει με μοναδικό τρόπο τις αναφορές που χρησιμοποιούνται για τη δημιουργία του, την κατακερματισμένη τιμή του προηγούμενου μπλοκ, τη ρίζα Merkle Tree όλων των εγγραφών, τη χρονική σφραγίδα δημιουργίας του, την τιμή δυσκολίας στόχου και την τιμή Nonce. Τα αναφερόμενα συστατικά έχουν τις ίδιες ιδιότητες με εκείνα του γονικού μπλοκ αλλά συνδέονται με τα πλευρικά μπλοκ.

Αντίστοιχα με το μπλοκ γονέα, το πλευρικό μπλοκ διαθέτει επίσης έναν μετρητή για τις κακόβουλες δραστηριότητες, οι οποίες καταγράφονται σε μία αναφορά. Αποτελείται από τη χρονική σήμανση της ενέργειας, την ίδια την ενέργεια, την ταυτότητα του κάτοχου των δεδομένων, την ταυτότητα του χρήστη, αλλά και την ταυτότητα και υπογραφή του κόμβου συναίνεσης. Το μπλοκ “κλειδώνεται” χρονικά και προσαρτάται στο γονικό μπλοκ της αλυσίδας Blockchain. Τα ίχνη των δεδομένων και της αναφοράς μπορούν πλέον να εντοπιστούν.

7.4 Συμπεράσματα

Η ανταλλαγή δεδομένων και η συνεργασία μέσω συστημάτων που βασίζονται στο Cloud Computing, διαθέτει τεράστια ισχύ με την αυξανόμενη πρόοδο των σύγχρονων τεχνολογιών που οδηγούν τη σημερινή κοινωνία. Η απαίτηση που δημιουργείται από την ανάλυση μεγάλων δεδομένων, την αναγνώριση προτύπων και τη μηχανική μάθηση, αποτελεί βασικό συστατικό αυτής της προόδου, καθώς αναπτύσσονται νέα μέσα θεραπείας από την ανάλυση των ιατρικών δεδομένων. Ποίκιλες μέθοδοι και διάφοροι μηχανισμοί έχουν τεθεί σε λειτουργία για τη ρύθμιση της ροής των ιατρικών δεδομένων από σημείο σε σημείο, καθώς οποιαδήποτε κακόβουλη μεταχείριση τους μπορεί να προκαλέσει αδιαίρετες ζημιές.

Το μοντέλο που αναλύθηκε, βασίζεται στο σχεδιασμό ενός δικτύου ανταλλαγής δεδομένων, μεταξύ συστημάτων που χρησιμοποιούν το Cloud Computing αξιοποιώντας την τεχνολογία του Blockchain. Ο σχεδιασμός εμπεριέχει τη χρήση των έξυπνων συμβολαίων και άλλων μηχανισμών με σκοπό την αποτελεσματική ανίχνευση της συμπεριφοράς των δεδομένων και την ανάκληση της πρόσβασης σε πιθανές περιπτώσεις παραβίασης των κανόνων ως προς τον τρόπο χρήσης τους. Με την εφαρμογή του μοντέλου, τα συστήματα θα μπορούν να επιτύχουν με ασφάλεια τη μετάδοση, τον έλεγχο και την ανίχνευση των δεδομένων, ενώ παράλληλα θα μοιράζονται τα ιατρικά δεδομένα με άλλους ιατρικούς φορείς και ερευνητικά ινστιτούτα, χωρίς κανέναν κίνδυνο για την ιδιωτικότητα τους.

Βιβλιογραφία

[1] *Blockchain: Η τεχνολογία που αλλάζει για πάντα οικονομία και διαδίκτυο*. (2017, December 10). Ανάκτηση από https://www.insider.gr/epiheiriseis/tehnologia/69555/blockchain-i-tehnologia-poy-allazei-gia-panta-oikonomia-kai-diadiktyo

[2] Βικιπαίδεια. (n.d.). *Blockchain*. Ανάκτηση από https://el.wikipedia.org/wiki/Blockchain

[3] Media, G. (2019). *Blockchain: η τεχνολογία πίσω από το Bitcoin.*

[4] Rodriguez, T. S. (2018, December 2). *Blockchain for Dummies.* Ανάκτηση από https://medium.com/swlh/blockchain-for-dummies-d3daf2170068

[5] Thamas, Y. (2019, March 11). The Importance of Blockchain Technology and Decentralization.

[6] Academy, B. (n.d.). *History of Blockchain*.

[7] From Wikipedia, t. f. (n.d.). *Satoshi Nakamoto*. Ανάκτηση από https://en.wikipedia.org/wiki/Satoshi_Nakamoto

[8] *The History of Blockchain*. (2017). Ανάκτηση από https://ecommerceguider.com/history-of-blockchain/

[9] GOYAL, S. (2018, November 3). The History of Blockchain Technology: Must Know Timeline.

[10] Ganne, E. (2018). Can Blockchain revolutionize international trade? Switzerland: WTO Publications, World Trade Organization.

[11] Yahn, B. (2018, January 19). A Brief History of BitCon.

[12] Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* USA: O'Reilly Media Inc.

[13] Jun WANG, P. W. (2017). *The outlook of blockchain technology for construction.*

[14] Dmitry Efanov, P. R. (2018). *The All-Pervasiveness of the Blockchain Technology.* Elsevier B.V.

[15] PRENEEL, B. (2003, February). *Analysis and Design of Cryptographic Hash Functions.*

[16] Jonathan Emmett, P. A. (2016). *Method and system for protecting execution of cryptographic hash functions. USA.*

[17] R.L. Rivest, A. S. (1977). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.

[18] W. Diffie, M. H. (1976, November). *New directions in cryptography.* IEEE.

[19] Paul, E. (2017, September 12). *What is Digital Signature- How it works, Benefits, Objectives, Concept.* Ανάκτηση από https://www.emptrust.com/blog/benefits-of-using-digital-signatures

[20] TechTarget. (2020). Digital signature.

[21] DocuSign. (2018). Understanding digital signatures.

[22] GeeksforGeeks. (n.d.). Digital Signatures and Certificates.

[23] Zibin Zheng, S. X. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data.*

[24] Audience, J. S.-G. (2018, May 6). How does blockchain work in 7 steps — A clear and simple explanation.

[25] Antonopoulos, A. M. (2014). Mastering Bitcoin.

[26] Academy, B. (n.d.). *Peer-to-Peer Networks Explained.* Ανάκτηση από https://academy.binance.com/blockchain/peer-to-peer-networks-explained

[27] Wiki, P. F. (2019). *Peer to Peer.* Ανάκτηση από https://wiki.p2pfoundation.net/Peer_to_Peer

[28] From Wikipedia, t. f. (2020). *Peer-to-peer.* Ανάκτηση από https://en.wikipedia.org/wiki/Peer-to-peer

[29] Marco Danelutto, P. F. (2017). *Making Grids Work: Proceedings of the CoreGRID Workshop on Programming Models Grid and P2P System Architecture Grid Systems.* Heraklion, Crete, Greece.

[30] Amitai Porat, A. P. (2018). Blockchain Consensus: An analysis of Proof-of-Work and its applications.

[31] Parikshit Hooda, G. (n.d.). *Proof of Work (PoW) Consensus*. Ανάκτηση από https://www.geeksforgeeks.org/proof-of-work-pow-consensus/

[32] Zibin Zheng, S. X. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data.*

[33] Academy, B. (n.d.). *What Is a Blockchain Consensus Algorithm?* Ανάκτηση από https://academy.binance.com/blockchain/what-is-a-blockchain-consensus-algorithm

[34] Arthur Gervais, G. O. (2016, October). On the Security and Performance of Proof of Work Blockchains.

[35] Daniel. (2018, July 19). What's A Merkle Tree? A Simple Guide To Merkle Trees.

[36] Blaise Gassend, G. E. (2002). Caches and Merkle Trees for Efficient Memory Authentication. MIT Laboratory for Computer Science.

[37] Du Mingxiao, M. X. (2017, October 5-7). *A Review on Consensus Algorithm of Blockchain.*

[38] Baliga, A. (2017). *Understanding Blockchain Consensus Models.*

[39] Fan Zhang, I. E. (2017, August 18). REM: Resource-Efficient Mining for Blockchains. Canada.

[40] TecraCoin. (2019, September 18). *What is Genesis Block and why Genesis Block is needed?*

[41] Peng Zhang, D. C. (2018). *Blockchain Technology Use Cases in Healthcare.* United States.

[42] Ευστάθιος Ζάχος, Α. Π. (2015). *Υπολογιστική Κρυπτογραφία.*

[43] Stagnaro, C. (n.d.). *White Paper: Innovative Blockchain Uses in Healthcare.* Freed Associates.

[44] Ariel Ekblaw, A. A. (2016). A Case Study for Blockchain in Healthcare : " MedRec " prototype for electronic health records and medical research data.

[45] Laure A. Linn, M. B. (n.d.). Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.

[46] Lab, M. M. (2018). MedRec, Overview.

[47] Asaph Azaria, A. E. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data.*

[48] Omar, A. A. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment.

[49] A New Ecosystem for a New Era. (n.d.).

[50] Kuo, A. M.-H. (2011, September). Opportunities and challenges of cloud computing to improve health care services.

[51] Thomas Hardjono, N. S. (2016, May). Cloud-Based Commissioning of Constrained Devices.

[52] GeeksforGeeks. (n.d.). *Types of Blockchain and Chain Terminology*. Ανάκτηση από https://www.geeksforgeeks.org/types-of-blockchain-and-chain-terminology/

[53] Thibodeau, M. (2019, April 17). *3 Types of Blockchain Explained*. Ανάκτηση από https://hedgetrade.com/3-types-of-blockchain-explained/

[54] Community, D. (2019, April 18). *What Different Types of Blockchains are There?* Ανάκτηση από https://dragonchain.com/blog/differences-between-public-private-blockchains

[55] Liam Bell, W. J. (2018). Applications of Blockchain Within Healthcare.

[56] Barakat M. (2018). *An Introduction to Cryptography*.

[57] Gaby G. Dagher, J. M. (2018). Ancile: Privacy-preserving framework for access control and interoperability. Στο *Sustainable Cities and Society.*

[58] team, M. (2018). *Medicalchain_WhitePaper 2.1.* Ανάκτηση από https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[59] Bhardwaj, G. (2018, June 19). *How blockchain will revolutionise clinical trials*. Ανάκτηση από https://pharmaphorum.com/views-and-analysis/how-blockchain-will-revolutionise-clinical-trials-clinical-trials/

[60] GitHub. (2020). *Ethereum Whitepaper*. Ανάκτηση από https://ethereum.org/en/whitepaper/

[61] Cryptodaily. (n.d.). *The History Of Ethereum*. Ανάκτηση από https://cryptodaily.co.uk/the-history-of-ethereum

[62] From Wikipedia, t. f. (2020). *Ethereum*. Ανάκτηση από https://en.wikipedia.org/wiki/Ethereum

[63] From Wikipedia, t. f. (2020, January 12). *Hyperledger*. Ανάκτηση από https://en.wikipedia.org/wiki/Hyperledger

[64] WILLIAM, S. (2012). *ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ.* ΙΩΝ.