ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Ψηφιακός Πολιτισμός, Έξυπνες Πόλεις, IoT και Προηγμένες Ψηφιακές Τεχνολογίες»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Blockchain και Fraud** **Blockchain and Fraud**
Ονοματεπώνυμο Φοιτητή	**Κωνσταντίνος Κριάρας**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΨΠΟΛ20039**
Επιβλέπων	**Κωνσταντίνος Πατσάκης**

Ημερομηνία Παράδοσης **Ιούνιος 2022**

Τριμελής Εξεταστική Επιτροπή

Κωνσταντίνος Πατσάκης	Δημήτριος Βέργαδος	Θωμάς Δασακλής
Αναπληρωτής	Καθηγητής	Επίκουρος
Καθηγητής		Καθηγητής

Π ε ρ ι ε χ ό μ ε ν α

Κ α τ ά λ ο γ ο ς Σ χ η μ ά τ ω ν

ΑΚΡΩΝΥΜΙΑ

P2P	Peer to peer
PoS	*Proof of Stake*
PoW	Proofof Work
DAG	*Directed Acyclic Graphs*
PoA	*Proof of Activity*
BFT	Byzantine Fault Tolerance
PBFT	*Practical Byzantine Fault Tolerance*
PoET	*Proof of Elapsed Time*
LPoS	*Leased Proof of Stake*
DPoS	*Delegated Proof-of-Stake*
PoB	*Proof of Burn*
PoC	*Proof of Capacity*
PoI	*Proof of Importance*
dBFT	*Delegated Byzantine Fault Tolerance*
sBFT	*Simplified Byzantine Fault Tolerance*
RPCA	Ripple Consensus Algorithm
DDoS	Distributed Denial of Service
IPO	Initial Public Offering
ICO	Initial Coin Offering
STO	*Security Token Offering*
DApps	Decentralized Applications
KSI	Keyless Signature Infrastructure
UAE	United Arab Emirates
HIPPA	Health Insurance portability and accountability act
EHR	Electronic health records
EMR	Electronic medical records
SHA-256	Secure hash algorithm
PHI	Personal health information
IPFS	InterPlanetary File System
PHR	Personal health records
KYC	Know Your Customer
EVM	Ethereum Virtual Machine
IoT	Internet of Things
GDPR	General data protection regulation
NSF	National Sanitation Foundation

Π Ε Ρ Ι Λ Η Ψ Η

Τα τελευταία χρόνια η τεχνολογία Blockchain έχει σημειώσει ραγδαία αύξηση ενδιαφέροντος , με αυξανόμενη χρήση της τεχνολογίας για πολλές εφαρμογές και επιχειρήσεις , από κρυπτονομίσματα μέχρι την εμπλοκή του σε πολλούς τομείς όπως στον τομέα υγείας, ναυτιλίας, χρηματοοικονομικό, εφοδιαστικό κ.α. Στην παρούσα διπλωματική περιγράφουμε τα βασικά στοιχεία του Blockchain με αναλυτική επισκόπηση και τις εφαρμογές της τεχνολογίας σε διάφορους τομείς με έμφαση σε τομείς και τις περιπτώσεις fraud . Ειδικότερα κάνουμε αναφορά σε περιστατικά διπλής ασφάλισης όπως ονομάζονται οι περιπτώσεις όπου ο πελάτης υποβάλει αξίωση αποζημίωσης από πολλές εταιρείες παράλληλα.

A B S T R A C T

In recent years, Blockchain technology has seen a rapid increase in interest, with increasing use of technology for many applications and businesses, from cryptocurrencies to its involvement in many sectors such as health, shipping, finance, logistics, etc. In this dissertation we describe the basic elements of Blockchain with a detailed overview and applications of technology in various areas with emphasis on areas and cases of fraud detection. In particular, we refer to cases of double dipping insurance as the cases are called where the customer submits a claim for compensation from several companies in parallel.

1

Εισαγωγή

1.1 Αντικείμενο της εργασίας-προκλήσεις

Στην παρούσα μεταπτυχιακή διατριβή εξετάζουμε την τεχνολογία blockchain και την εφαρμογή της στον τομέα του Fraud . Πιο συγκεκριμένα περιγράφεται η τεχνολογία Blockchain και οι τύποι της, θα γίνει μια σύντομη επισκόπηση στην ιστορία της, ενώ παράλληλα θα εντοπιστούν τα πλεονεκτήματα της σε σχέση με τεχνολογίες παλαιού τύπου και κατ' επέκταση η χρήση έξυπνων συμβολαίων και η δημιουργία πλατφόρμας- εφαρμογής ώστε να εφαρμοστεί κατάλληλα για να έχουμε αποτελεσματικότερη και αποδοτικότερη εφαρμογή της τεχνολογίας blockchain σε περιπτώσεις Fraud . Ειδικότερα στο σενάριο μας χρησιμοποιούμε δεδομένα πελατών το οποία χρήζουν ειδικής μέριμνας γιατί πρόκειται για ευαίσθητα προσωπικά δεδομένα τα οποία με τη σωστή διαχείριση της εφαρμογής θα βοηθήσουν στην αποφυγή περιπτώσεων απάτης ειδικότερα σε ασφαλιστικές εταιρείες με αποτέλεσμα την ευημερίας της κοινωνίας και διατήρηση της ποιότητας ζωής.

1.2 Μεθοδολογία

Για την εκπόνηση της συγκεκριμένης εργασίας αρχικά πραγματοποιήθηκε μια ανασκόπηση της βιβλιογραφίας, όπως επίσης επιστημονικά περιοδικά, επιστημονικές εφημερίδες και ηλεκτρονικές πηγές. Η αναζήτηση επιστημονικών άρθρων έγινε από την ιστοσελίδα Scopus όπου οι θεματικές ενότητες περιέλαβαν θέματα απάτης σε συνδυασμό με Blockchain . Επιπλέον πραγματοποιήθηκε αναζήτηση σχετικά με την τεχνολογία blockchain ,τα έξυπνα συμβόλαια, τις εφαρμογές που έχουν υλοποιηθεί και τους τρόπους ενσωμάτωσής της σε θέματα σχετικά με Fraud. Υπήρξε ιδιαίτερο ενδιαφέρον σε τομείς υγείας και ιατρικής βιομηχανίας και ασφάλισης.

1.3 Δομή της Διπλωματικής

Στην ενότητα αυτή περιγράφονται συνοπτικά τα επόμενα κεφάλαια της διπλωματικής εργασίας. Στο δεύτερο κεφάλαιο γίνεται εισαγωγή στην τεχνολογία Blockchain ,πως λειτουργεί και τα χαρακτηριστικά της τεχνολογίας. Επίσης περιγράφονται οι μηχανισμοί συναίνεσης που χρησιμοποιούνται, τα έξυπνα συμβόλαια και πληροφορίες σχετικά με το Ethereum που θα είναι η βασική τεχνολογία για το παράδειγμά μας. Στο τρίτο κεφάλαιο παρουσιάζονται τα πεδία που βρίσκει εφαρμογή το Blockchain και διάφορα παραδείγματα, με αναφορά και σε περιπτώσεις που χρησιμοποιούνται για ανίχνευση απάτης Στο τέταρτο κεφάλαιο παρουσιάζονται τα στοιχεία της έρευνας για απάτη σε ασφαλιστικές εταιρείες και η ανάλυση σεναρίου. Τέλος υπάρχουν η σύνοψη και τα συμπεράσματα της εργασίας.

2

Εισαγωγή στην τεχνολογία του Blockchain

2.1 Ορισμός του Blockchain

Το blockchain είναι ένας τύπος Τεχνολογίας Κατανεμημένου Λογαριασμού που μπορεί να καταγράφει όλες τις συναλλαγές και να τις μοιράζεται μέσω ενός δικτύου υπολογιστών peer-to-peer, χρησιμοποιώντας κρυπτογραφικούς μηχανισμούς εμπιστοσύνης και διασφάλισης. Είναι μια αποκεντρωμένη δομή δεδομένων όπου οι συναλλαγές αποθηκεύονται ταξινομημένα. Οι εγγραφές ονομάζονται μπλοκ και κάθε μπλοκ για να προστεθεί χρησιμοποιείται κρυπτογραφία. Σε κάθε μπλοκ υπάρχει ένα κομμάτι κώδικα κατακερματισμού (hash) του προηγούμενου μπλοκ μαζί με χρονοσήμανση των συναλλαγών και δεδομένων. Οι συναλλαγές που αποθηκεύονται στο blockchain μπορούν να διατηρηθούν σε όλους τους υπολογιστές του δικτύου επιτυγχάνοντας με τον τρόπο αυτό ότι τα δεδομένα είναι κατανεμημένα και ταυτόχρονα ότι κανένας δεν μπορεί να τα αλλάξει αρά είναι αμετάβλητα. Όταν ένα νέο μπλοκ θέλουμε να προστεθεί χρησιμοποιούνται αλγόριθμοι συναίνεσης όπου σε ελάχιστο χρονικό διάστημα γίνεται πραγματικότητα . Σε αυτή τη διαδικασία χρησιμοποιείται ο κρυπτογραφημένος κώδικας κατακερματισμού(hash) σε συνδυασμό με τον αλγόριθμο που επιλέγεται να το επικυρώσει. Υπάρχουν τα δημόσια blockchains οπου αυτό ονομάζεται εξόρυξη (mining). Αυτό είναι γνωστό ως απόδειξης της εργασίας (PoW) και ο στόχος είναι να επικυρώσει ότι η συναλλαγή είναι νόμιμη και ο αλγόριθμος είναι αληθής. Η τεχνολογία κατανεμημένου λογαριασμού αφορά τα πρωτόκολλα που χρησιμοποιούνται και στην υποδομή που χρειάζεται ώστε υπολογιστές που βρίσκονται σε διαφορετικά μέρη να προτείνουν, να επικυρώνουν τις συναλλαγές και να ενημερώνουν τις εγγραφές με συγχρονισμένο τρόπο σε ένα δίκτυο. Η βασική ιδέα του Blockchain είναι η ύπαρξή ενός κοινού χώρου διατήρησης και γνωστοποίησης δεδομένων συναλλαγής προσιτού σε όλα τα μέλη μιας κοινότητας. Για να γίνει κατανοητή η κύρια και διαχρονική ανάγκη που καλύπτει το blockchain, παρουσιάζεται ένα απλό παράδειγμα μιας προσπάθειας που έχει καταγραφεί πολύ πριν την δημιουργία του, αυτό είναι οι πέτρες Rai που χρησιμοποιούνταν στο νησί Yap του Ειρηνικού Ωκεανού το 500 μ.Χ. Οι πέτρες αυτές ήταν μια μορφή ασβεστολιθικού νομίσματος που συμβόλιζαν διαπραγματεύσεις που επικυρώνονταν με προφορική συμφωνία. Κατά τη διάρκεια μιας συναλλαγής, οι πέτρες δεν άλλαζαν χέρια (μερικές ζύγιζαν 4 τόνους), αλλά η ιδιοκτησία καταγραφόταν πάνω σε αυτές και στη συνέχεια λεκτικά γινόταν γνωστή η συναλλαγή σε όλη τη κοινότητα. Έτσι, δημιουργήθηκε ένα κοινό βιβλίο το οποίο ενημερωνόταν με ομαδική συναίνεση χωρίς την εμπλοκή ενδιάμεσων[1].

2.2 Τεχνολογία του Blockchain

Το Blockchain είναι ένας τύπος ή υποσύνολο της τεχνολογίας κατανεμημένου καθολικού .Το Blockchain είναι ένας μηχανισμός που χρησιμοποιεί την κρυπτογράφηση και χρησιμοποιεί μαθηματικούς αλγορίθμους για τη δημιουργία και επαλήθευση μιας συνεχώς αυξανόμενης δομής δεδομένων. Στη δομή αυτή μπορούν μόνο να προστεθούν δεδομένα αλλά δεν γίνεται να καταργηθούν τα ήδη υπάρχοντα, έτσι δημιουργείται η μορφή μιας αλυσίδας "μπλοκ συναλλαγών", η οποία λειτουργεί ως διανεμημένος λογαριασμός. Εάν κάποια από τις συναλλαγές σε ένα μπλοκ μεταβληθεί ελαφρώς, η αντίστοιχη έξοδος εξαγωγής θα αλλάξει δραστικά, πράγμα που θα σπάσει την αλυσίδα στο επόμενα μπλοκ στον blockchain. Επομένως, οποιαδήποτε μεταβολή στο περιεχόμενο ενός μπλοκ στο blockchain ανιχνεύεται εύκολα στο δίκτυο. Για το λόγο αυτό, μόλις μια συναλλαγή προστεθεί σε ένα blockchain, η συναλλαγή αυτή δεν μπορεί να μεταβληθεί ή να ακυρωθεί. Έτσι, πληροφορίες στο blockchain λέγεται ότι είναι αμετάβλητες. Η μετατόπιση είναι μια σημαντική ιδιότητα του blockchain η οποία εξασφαλίζει ότι τα αρχεία, όταν δημιουργηθούν, δεν μπορούν να ανακληθούν ή να τροποποιηθούν. Το blockchain μπορεί να θεωρηθεί ως κατανεμημένη βάση δεδομένων όπου οι προσθήκες ξεκινούν από ένα μέλος (δηλ. έναν από τους κόμβους του δικτύου), ο οποίος δημιουργεί ένα νέο "μπλοκ" που μπορεί να περιέχει κάθε είδους πληροφορία. Στη συνέχεια το νέο μπλοκ μεταδίδεται σε όλα τα μέρη του δικτύου κρυπτογραφημένα έτσι ώστε οι λεπτομέρειες της συναλλαγής να μην μπορούν να δημοσιευτούν. Όλοι οι κόμβοι του δικτύου (όλοι nodes-συμμετέχοντες του δικτύου) ορίζουν συλλογικά την ισχύ των μπλοκ σύμφωνα με μια προκαθορισμένη μέθοδο αλγοριθμικής επικύρωσης, κοινώς αναφερόμενη ως "Μηχανισμός συναίνεσης". Όταν γίνει η επικύρωση, το νέο μπλοκ προστίθεται στο blockchain, δηλαδή γίνεται ενημέρωση του μητρώου συναλλαγών και έπειτα προχωράει σε διανομή σε όλο το δίκτυο. Ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή αξίας και δύναται να εφαρμοστεί σε οποιαδήποτε στοιχείο μπορεί να μετατραπεί σε ψηφιακή μορφή. Τα μπλοκ υπογράφονται με ψηφιακή υπογραφή χρησιμοποιώντας ένα ιδιωτικό κλειδί. Κάθε χρήστης στο δίκτυο blockchain έχει ένα ιδιωτικό κλειδί το οποίο είναι η ψηφιακή υπογραφή του σε μια συναλλαγή κι ένα δημόσιο κλειδί, το οποίο είναι γνωστό σε όλους τους χρήστες στο δίκτυο. Το δημόσιο κλειδί χρησιμεύει ως διεύθυνση στο δίκτυο blockchain. και ως επαλήθευση της ψηφιακής υπογραφής / επικύρωσης της ταυτότητας του αποστολέα. Η προσθήκη νέων πληροφοριών στο blockchain μπορεί να γίνει από οποιονδήποτε κόμβου του δικτύου. Για να μπορέσει να γίνει αυτή η προσθήκη πληροφοριών, πρέπει να γίνει με νόμιμο τρόπο εφόσον οι κόμβοι έρθουν σε συμφωνία μεταξύ τους.

Ο μηχανισμός συναίνεσης είναι μια προκαθορισμένη, συγκεκριμένη μέθοδος επαλήθευσης που χρησιμοποιείται κρυπτογραφία και εξασφαλίζει τη σωστή ανάλυση της αλληλουχίας των συναλλαγών στο blockchain. Στα κρυπτονομίσματα η αλληλουχία χρησιμοποιείται για την αντιμετώπιση της διπλής δαπάνης όπου μεταφέρονται περισσότερες από μία φορές εάν οι μεταφορές δεν καταχωρούνται και ελέγχονται κεντρικά. Υπάρχουν διάφοροι τρόποι όπου μπορεί να εκτελεστεί ένας μηχανισμός συναίνεσης. Οι δύο πιο γνωστοί - στο πλαίσιο των κρυπτονομισμάτων είναι ο μηχανισμός της απόδειξης εργασίας (PoW) και της απόδειξης συμμετοχής (PoS). Όσον αφορά τον μηχανισμό απόδειξης εργασίας οι συμμετέχοντες στο δίκτυο πρέπει να επιλύσουν τα αποκαλούμενα "κρυπτογραφικά παζλ" για να προσθέσουν νέα "μπλοκ" στο blockchain. Η διαδικασία επίλυσης παζλ αναφέρεται συνήθως ως εξόρυξη**.** Τα κρυπτογραφικά παζλ αποτελούνται από όλες τις προηγούμενες πληροφορίες που καταγράφονται στο blockchain και ένα νέο σύνολο συναλλαγών που θα προστεθούν στο επόμενο μπλοκ. Όσο προχωράμε οι υπολογισμοί γίνονται πιο περίπλοκοι και η είσοδος κάθε παζλ γίνεται μεγαλύτερη. Αυτός ο μηχανισμός συναίνεσης απαιτεί τεράστιο όγκο υπολογιστικών πόρων άρα καταναλώνουν μεγάλα ποσά ηλεκτρικής ενέργειας. Όταν ένας κόμβος-συμμετέχων στο δίκτυο λύσει ένα κρυπτογραφικό παζλ, σημαίνει ότι έχει ολοκληρώσει το έργο, και ανταμείβεται με ψηφιακή μορφή αξίας (με μια νέα εξόρυξη νομίσματος). Σαν αποτέλεσμα η ανταμοιβή αυτή λειτουργεί ως κίνητρο για την υποστήριξη του δικτύου . Η Bitcoin κρυπτογράφηση βασίζεται σε μηχανισμό συναίνεσης PoW. Άλλα παραδείγματα περιλαμβάνουν τα Litecoin, Bitcoin Cash, Monero, κλπ. Όσον αφορά τον μηχανισμό απόδειξη συμμετοχής PoS, ο επικυρωτής συναλλαγής-κόμβος οφείλει να αποδείξει την ιδιοκτησία ενός συγκεκριμένου στοιχείου (μια ορισμένη ποσότητα κερμάτων) ώστε να μπορεί να έχει συμμετοχή στην επικύρωση συναλλαγών. Εδώ η πράξη επικύρωσης

ονομάζεται "σφυρηλάτηση" αντί για "εξόρυξη". Στην περίπτωση των κρυπτονομισμάτων, ο επικυρωτής πρέπει να αποδείξει το "ποντάρισμα" (share) όλων των υφιστάμενων κερμάτων που επιτρέπεται να επικυρώσουν μια συναλλαγή. Έτσι αναλογικά με το ποσό που έχει στην κατοχή του , έχει περισσότερες πιθανότητες ώστε να είναι αυτός που θα επικυρώσει το επόμενο μπλοκ (μεγαλύτερη αρχαιότητα στο δίκτυο, που σημαίνει πιο αξιόπιστη θέση). Εδώ ο επικυρωτής πληρώνει τέλη συναλλαγής για τις υπηρεσίες επικύρωσής του από τα υπόλοιπα μέλη. Παραδείγματα κρυπτονομίσματων που χρησιμοποιούν τέτοιο μηχανισμό συμφωνίας είναι τα Neo και Ada.

2.3 Πως λειτουργεί το blockchain

Ένα από τα κύρια χαρακτηριστικά του Blockchain είναι ότι είναι δύσκολο να αλλοιωθεί η πληροφορία που περιέχει. Αυτό όπως αναφέραμε και παραπάνω, συμβαίνει διότι ο κάθε συμπεριλαμβανόμενος κόμβος στο δίκτυο έχει ένα ακριβές αντίγραφο στο ψηφιακό καθολικό. Για να προστεθεί μια καινούργια συναλλαγή στο δίκτυο θα πρέπει ο κάθε κόμβος να ελέγξει την εγκυρότητα της. Εφόσον γίνει ο έλεγχος και εγκριθεί ως γνήσια συναλλαγή, τότε μόνο προστίθεται στο δίκτυο. Με πολλαπλούς συμμετέχοντες ταυτόχρονα για την έγκριση διαφορετικών τμημάτων συναλλαγών, θα ήταν δυνητικά δύσκολο να εντοπιστεί το αντίγραφο του καθολικού που θα ακολουθήσει. Οι συναλλαγές περιέχουν μια αναφορά στο προηγούμενο μπλοκ, ο σύνδεσμος αυτός κρυπτογραφείται χρησιμοποιώντας μια συνάρτηση κατακερματισμού (hash function) και με τον τρόπο αυτό δημιουργείται μια "αλυσίδα" μπλοκ. Η επιλογή του επόμενου έγκυρου block γίνεται με την χρήση ενός μοντέλου συναίνεσης, που καθορίζει το δίκτυο των κόμβων και θα πρέπει να υιοθετηθούν από το blockchain σε όλο το δίκτυο.

Ακόμα ένα ισχυρό χαρακτηριστικό στα blockchains, είναι ότι η ταυτότητα καθορίζεται χρησιμοποιώντας ένα ζευγάρι αριθμών που ονομάζεται ζεύγος κλειδιών, το οποίο αποτελείται από ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί είναι μυστικό και γνωστό μόνο στον ιδιοκτήτη, ενώ το δημόσιο κλειδί (ή μια διεύθυνση που προέρχεται από αυτό) είναι ορατό σε άλλους στο blockchain. Η ιδιοκτησία ενός ιδιωτικού κλειδιού είναι αυτό που ορίζει την ταυτότητα σε ένα blockchain. Πριν υποβάλει ένα άτομο συναλλαγή σε blockchain, πρέπει να υπογράψει τη συναλλαγή χρησιμοποιώντας το ιδιωτικό κλειδί του. Η υπογραφή είναι αυτή που επιτρέπει στο blockchain να επαληθεύσει την αυθεντικότητα της συναλλαγής. Είναι δυνατόν να συσχετιστεί ένα ιδιωτικό κλειδί με πολλά δημόσια κλειδιά. Στο blockchain δεν υπάρχει κάποια αρμόδια αρχή που επιμελείται τη δομή του ,αντί αυτού, υπάρχει ένα σύμπλεγμα κόμβων που διατηρεί το δίκτυο και το καθιστά αποκεντρωμένο. Εξαιτίας της απουσίας κεντρικής επιτήρησης, μας παρέχεται μια ενισχυμένη αίσθηση ασφάλειας διότι δεν δύναται ο οποιοσδήποτε να επέμβει στο δίκτυο αλλάζοντας τα χαρακτηριστικά του προς όφελος του, ενώ η χρήση της κρυπτογράφησης αυξάνει την ασφάλεια του συστήματος. Επιπλέον το καθολικό του δικτύου διατηρείται από όλους του χρήστες του συστήματος, αυτή η κατανομή της υπολογιστικής ενέργειας δια μέσου των υπολογιστών διευκολύνει τις συναλλαγές και τις καθιστά πλήρως γνωστοποιημένες ακόμη και σε μεγάλα και πολύπλοκα συστήματα. Τα blockchains χάρη στην αποκέντρωση του δικτύου προσφέρουν επιπλέον, ταχύτερη διευθέτηση συναλλαγών συγκριτικά με το παραδοσιακό τραπεζικό σύστημα. Έτσι ένας χρήστης είναι σε θέση να μεταφέρει χρηματικά ποσά πιο άμεσα, γεγονός που διευκολύνει τις συναλλαγές και μακροπρόθεσμα του εξοικονομεί χρόνο.

2.4 Τύποι του blockchain

Υπάρχουν τρεις κύριοι τύποι blockchains:

- **Τα δημόσια blockchains (Open blockchains)** είναι ανοικτά και επομένως δίνεται η δυνατότητα εκμετάλλευσης των ιδιοτήτων της κατανομής του δικτύου από πληθώρα ανθρώπων εφόσον δεν υπάρχουν περιορισμοί ως προς την πρόσβαση. Ακόμη, ο κάθε

χρήστης δύναται να συμμετέχει στα πρωτόκολλα ομοφωνίας, ενώ συνήθως για τη σωστή λειτουργία και την ασφάλεια του συστήματος δίνονται χρηματικές αμοιβές στους συμμετέχοντες ειδικά όταν χρησιμοποιούνται αλγόριθμοι *PoW*. Ο αλγόριθμος PoW δομεί τη διαδικασία με την οποία επιλέγεται το επόμενο μπλοκ, δίνει το κίνητρο για την εξεύρεση σωστής λύσης στο κρυπτογραφικό παζλ από τους συμμετέχοντες, επειδή παρέχεται μια ανταμοιβή. Αυτό το διακριτικό ή το κρυπτοεγχειρίδιο ενισχύει τη δημιουργία αξίας, η οποία είναι μια πολύ σημαντική έννοια στο blockchain και το διαφοροποιεί από τις παραδοσιακές, κεντρικές υπηρεσίες εφαρμογών. Τέλος, τα δημόσια blockchains έχουν το πλεονέκτημα ότι παρέχουν μια ασπίδα προστασίας των χρηστών από τους προγραμματιστές, διασφαλίζοντας ότι υπάρχουν ορισμένες σταθερές που ούτε οι ίδιοι οι δημιουργοί μιας εφαρμογής δεν έχουν τη δυνατότητα/εξουσιοδότηση να αλλάξουν.

- **Τα ιδιωτικά blockchains (Private blockchains)** δεν προσφέρουν ελεύθερη είσοδο σε όλους. Για να αποκτήσει κάποιος πρόσβαση σε αυτά θα έπρεπε να δοθεί έγκριση από τον κάτοχο του συστήματος. Η ομάδα ανθρώπων ή η εταιρεία που το αξιοποιεί έχει το δικαίωμα ελέγχου και δύναται να επέμβει όταν το επιθυμεί, μετατρέποντας τους κανόνες, ανατρέποντας τις συναλλαγές, τροποποιώντας τα ισοζύγια κλπ. Επιπλέον, στην περίπτωση αυτή, μειώνεται το κόστος τον συναλλαγών σε σύγκριση με ένα δημόσιο, διότι η συναλλαγή πρέπει να επαληθευτεί μόνο από κάποιους κόμβους που μπορούν να εμπιστευτούν την πολύ υψηλή επεξεργαστική ισχύ τους και δεν χρειάζεται να επαληθεύονται από χιλιάδες υπολογιστές. Επιπρόσθετα, οι επικυρωτές είναι συγκεκριμένοι, οπότε μειώνεται ο κίνδυνος επίθεσης. Ένα ακόμη πλεονέκτημα ενός ιδιωτικού Blockchain είναι η ταχύτερη επιδιόρθωση βλαβών χάρη στον γρηγορότερο εντοπισμό του προβλήματος που επιτρέπει την πιο άμεση επέμβαση για την επίλυση του. Αυτό συμβαίνει εξαπίας της καλής σύνδεσης των κόμβων, που επιτρέπουν τη χρήση αλγορίθμων συναίνεσης καταλήγοντας στο τελικό αποτέλεσμα ταχύτερα. Τέλος, τα ιδιωτικά blockchains παρέχουν μεγαλύτερη προστασία των προσωπικών δεδομένων εφόσον τα δικαιώματα ανάγνωσης είναι περιορισμένα.

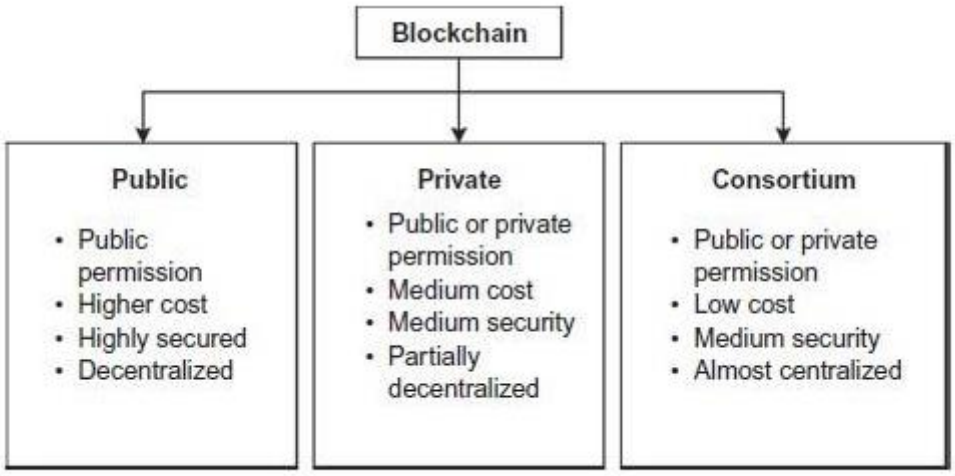
- **Τα consortium blockchain** είναι τα blockchain στα οποία η διαδικασία συναίνεσης γίνεται από ένα προ-επιλεγμένο σύνολο των κόμβων. Στην περίπτωση αυτή μπορούμε να φανταστούμε ένα συνεταιρισμό 25 ιδρυμάτων όπου καθένα ίδρυμα διαθέτει ένα κόμβο και των οποίων οι 15 θα πρέπει να υπογράψουν κάθε μπλοκ ώστε να μπορέσει το μπλοκ να θεωρηθεί έγκυρο. Η δυνατότητα για ανάγνωση του blockchain μπορεί να είναι είτε δημόσια είτε να περιοριστεί μόνο σε όσους συμμετέχουν, έτσι ώστε μέλη από το δημόσιο κοινό να πραγματοποιούν ερωτήματα και να παίρνουν πίσω κρυπτογραφικές αποδείξεις ορισμένων τμημάτων του blockchain. Τα consortium blockchains μπορεί να λογιστούν ως «μερικώς αποκεντρωμένα».

Κάθε blockchain αποτελείται από δύο στοιχεία:

- Τις συναλλαγές , που είναι οι ενέργειες που έγιναν από τους συμμετέχοντες στο σύστημα.
- Τα μπλοκ , που γίνεται η καταγραφή των συναλλαγών και βεβαιώνουν ότι είναι στη σωστή σειρά και δεν υπάρχει αλλοίωση. Στα μπλοκ εισάγεται και μια χρονοσφραγίδα, όταν γίνεται η προσθήκη συναλλαγών.

Συμπερασματικά, είναι φανερό ότι όλα τα είδη έχουν θετικά και αρνητικά στοιχεία, οπότε η επιλογή θα πρέπει να εξαρτάται από τη χρήση που απαιτείται να γίνει. Αν κάποιος επιθυμεί τη

μεταφορά ψηφιακών στοιχείων μεταξύ μιας κλειστής ομάδας ανθρώπων και τη διατήρηση του απορρήτου των συναλλαγών ή να έχει μεγάλο όγκο συναλλαγών ανά δευτερόλεπτο, τότε φαίνεται καταλληλότερη μια ιδιωτική μπλοκ αλυσίδα. Τα ιδιωτικά blockchains, έχουν συχνή εφαρμογή στη διατήρηση ιστορικών συμβάντων και για λογιστικούς σκοπούς γιατί με αυτή την επιλογή εξαλείφεται ο κίνδυνος απουσίας ελέγχου ή διαρροής ευαίσθητων δεδομένων στο γενικότερο δίκτυο. Αν αυτό που αναζητά είναι μια ανοιχτή και διαλειτουργική πλατφόρμα όπως το διαδίκτυο, είναι προτιμότερο να επιλέξει το δημόσιο blockchain. Τον επαγγελματικό και χρηματοοικονομικό τομέα φαίνεται να τον ενδιαφέρει περισσότερο οι εξελίξεις στο ιδιωτικό τύπο blockchain ,διότι εστιάζει στις δυνατότητες της τεχνολογίας αλλά δεν επιθυμεί τον μειωμένο έλεγχο που έχουν τα δημόσια δίκτυα. Οι σημαντικότερες εξελίξεις της τεχνολογίας blockchain στηρίζονται σε όλα τα προτερήματα που προέρχονται από το κοινό, το «ανοιχτό».



Εικ.1 Τύποι Blockchain

2.5 *Χαρακτηριστικά του Blockchain*

Το blockchain λόγω της αρχιτεκτονικής και του τρόπου που λειτουργεί έχει κάποια πολύ σημαντικά χαρακτηριστικά:

- **Αμετάβλητο (Immutable) – (permanent and tamper-proof)** Το blockchain είναι ένα μόνιμο αρχείο συναλλαγών. Εφόσον προστεθεί ένα block στον κόμβο δεν μπορεί να τροποποιηθεί. Αυτό οδηγεί στην ασφάλεια και στην εμπιστοσύνη

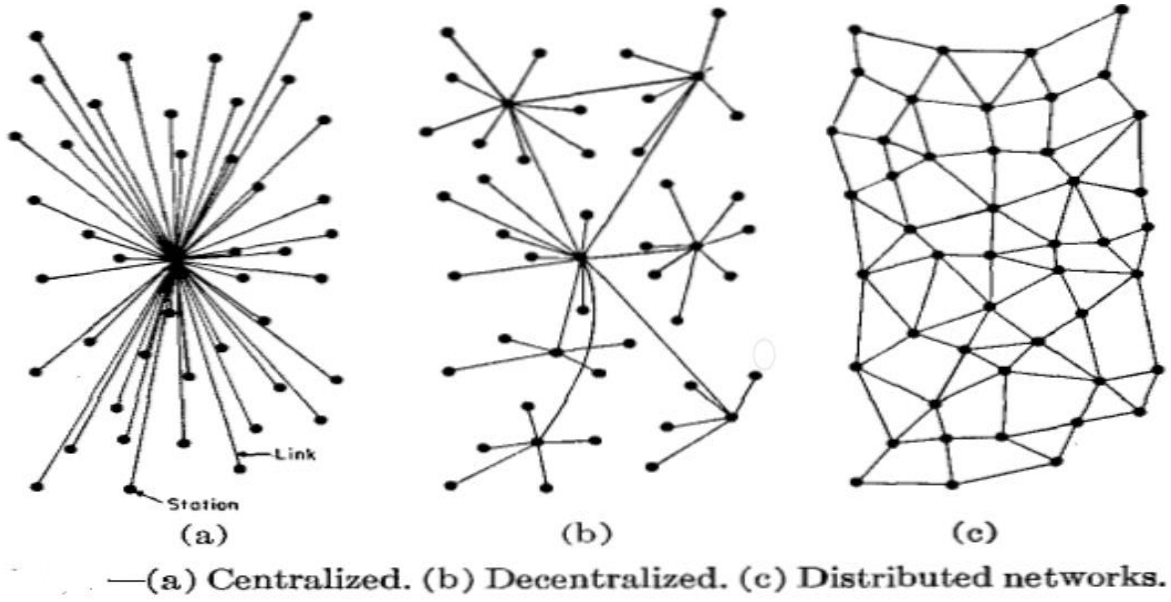
των συναλλαγών.

- **Αποκεντρωμένο** – Όλοι οι κόμβοι του δικτύου κατέχουν από ένα αντίγραφου του καθολικού. Έτσι, κανένας κόμβος δεν έχει παραπάνω εξουσία από κάποιον άλλο. Αυτή η αποκεντρωμένη δομή που βασίζεται στη συναίνεση καταργεί την ανάγκη διακυβέρνησης από μια κεντρική αρχή.

- **Κρυπτογράφηση (Encryption)** – Το Blockchain χρησιμοποιεί τεχνολογίες όπως τα δημόσια και ιδιωτικά κλειδιά επαλήθευσης για την ασφαλή και σχεδόν ανώνυμη καταγραφή των δεδομένων στα block. Οι συμμετέχοντες μπορούν να αλλάζουν την προσωπική τους ταυτότητα και άλλες πληροφορίες και να μοιράζονται μόνο ότι χρειάζεται σε μια συναλλαγή.

- **Τεκμηρίωση (Tokenization**) – Οι συναλλαγές και άλλες αλληλεπιδράσεις στο Blockchain συντελούν στην ασφαλή ανταλλαγή των περιουσιακών στοιχείων των συμβαλλόμενων μερών. Η συναλλαγή πραγματοποιείται με την μορφή νομισμάτων και χρησιμοποιούνται για την ανταλλαγή περιουσιακών στοιχείων μέσω ψηφιακών αγορών.

- **Διανομή (Distribution)** Τα συμμετέχοντα μέρη στο Blockchain βρίσκονται απομακρυσμένα μεταξύ τους αλλά παράλληλα συνδέονται σε ένα κοινό ηλεκτρονικό δίκτυο. Κάθε συμμετέχων στο δίκτυο διατηρεί ένα πλήρες αντίγραφο του καθολικού το οποίο ενημερώνεται με νέες συναλλαγές και καταχωρήσεις καθώς αυτές συμβαίνουν. Οποιοσδήποτε συμμετέχων μπορεί να δει οποιοδήποτε μέρος του καθολικού αλλά σε καμιά περίπτωση δεν μπορεί να το αλλάξει.



Εικ.2 Κεντροποιημένα, αποκεντρωμένα και διανεμημένα δίκτυα [46]

2.6 Προβλήματα και προκλήσεις (Πλεονεκτήματα-Μειονεκτήματα)

Αν και η τεχνολογία Blockchain έχει αυξανόμενη απήχηση στην αγορά υπάρχουν κάποιοι παράγοντες που εμποδίζουν την ευρεία αποδοχή αυτής της τεχνολογίας. Τα μεγαλύτερα προβλήματα που συναντάμε είναι η αποθήκευση των δεδομένων ,το κόστος της ενέργειας και ο όγκος των συναλλαγών. Όσον αφορά την επεκτασιμότητα του Blockchain το βασικότερο εμπόδιο είναι η αποθήκευση δεδομένων. Για παράδειγμα σε ένα δημόσιο Blockchain που είναι πλήρως αποκεντρωμένο το μέγεθος ενός μπλοκ γίνεται ολοένα μεγαλύτερο και γίνεται πιο δαπανηρή η αποθήκευση δεδομένων. Οι επιστήμονες ελπίζουν με την πρόοδο της συμπίεσης δεδομένων να μειωθεί αισθητά το κόστος αποθήκευσης δεδομένων. Προτείνεται η χρήση των Merkle Trees ώστε να βοηθήσει στην επαλήθευση των συναλλαγών, όπου χρειάζεται να κατέβει μόνο μια μερική μερίδα του συνόλου της αλυσίδας για να επαληθευτεί η συναλλαγή. Ακόμα από μόνο του το μέγεθος του μπλοκ αποτελεί σημαντικό παράγοντα στην αύξηση του όγκου συναλλαγών.

Μερικά από τα *Πλεονεκτήματα – Μειονεκτήματα* αναλόγως τη χρήση τους είναι :

- Διαφάνεια και αμεταβλητότητα : Ότι αλλαγές γίνονται σε ένα δημόσιο blockchain είναι ορατές σε όλα τα μέλη με αποτέλεσμα να υπάρχει διαφάνεια. Επίσης οι συναλλαγές που γίνονται είναι αμετάβλητες άρα δεν υπάρχει δυνατότητα να διαγραφούν είτε να τροποποιηθούν
- Αξιοπιστία και αντοχή : Επειδή είναι αποκεντρωμένα δικτύα στα blockchain δεν υπάρχει κεντρικό σημείο αποτυχίας άρα μπορούν να ανταπεξέλθουν σε εξωτερικές επιθέσεις
- Ακεραιότητα της διαδικασίας : Οι συναλλαγές γίνονται με βάση τα πρωτοκόλλα που έχουν οριστεί από την αρχή άρα υπάρχει εμπιστοσύνη μεταξύ των χρηστών
- *Αποδιαμεσολάβηση* : Δεν υπάρχει η ανάγκη για διαμεσολάβηση ενός τρίτου μέρους για να πραγματοποιηθεί μια συναλλαγή μεταξύ δύο χρηστών
- Υψηλής ποιότητας δεδομένα : Όλα τα δεδομένα που χρησιμοποιούνται σε ένα blockchain είναι έγκαιρα, πλήρης, συνεπής, ακριβή και πάντα διαθέσιμα
- Απλούστευση του οικοσυστήματος : Σε ένα ενιαίο δημόσιο καθολικό (ledger), υπάρχουν όλες οι συναλλαγές
- Χαμηλότερο κόστος συναλλαγών : Εφόσον δεν χρειάζονται τρίτα μέρη για την ανταλλαγή στοιχείων υπάρχει η δυνατότητα τα blockchains να μειώσουν τα έξοδα συναλλαγής.)
- Ταχύτερες συναλλαγές : Οι συναλλαγές που πραγματοποιούνται σε ένα blockchain μπορούν να μειώσουν το χρόνο συναλλαγής σε μερικά λεπτά και είναι διαθέσιμα 24/7 σε αντίθεση με τις τραπεζικές συναλλαγές
- Εκκολαπτόμενη τεχνολογία: Αν μπορέσουν και αντιμετωπιστούν τα προβλήματα που αναφέραμε παραπάνω , με το κόστος και τον όγκο των δεδομένων κυρίως, θα μπορέσει να γίνει το blockchain ευρέως αποδεκτό και εφαρμόσιμο)
- Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας: Αν και υπάρχουν τα ιδιωτικά blockchains και το γεγονός ότι χρησιμοποιείται ισχυρή κρυπτογράφηση υπάρχουν ακόμα ανησυχίες από μερίδα ανθρώπων και επιστημόνων για την ασφάλεια, ώστε να πειστεί το κοινό να χρησιμοποιήσει τα προσωπικά του δεδομένα σε ένα blockchain
- Μεγάλη κατανάλωση ενέργειας : Απαιτείται μεγάλη ποσότητα ενέργειας του υπολογιστή ώστε να μπορέσει να γίνει επικύρωση των συναλλαγών μέσω της διαδικασίας εξόρυξης όπου γίνονται σε ένα δίκτυο

- Αβέβαιο ρυθμιστικό καθεστώς : Επειδή οι κυβερνήσεις ορίζουν τα νομίσματα και όπως αναφέραμε δεν υπάρχει καθολική αποδοχή ώστε να γίνουν εφαρμόσιμα ευρέως και επειδή υπάρχουν αντιρρήσεις από τους ήδη υπάρχοντες χρηματοπιστωτικούς οργανισμούς δεν υπάρχει κάποιο σίγουρο ρυθμιστικό καθεστώς

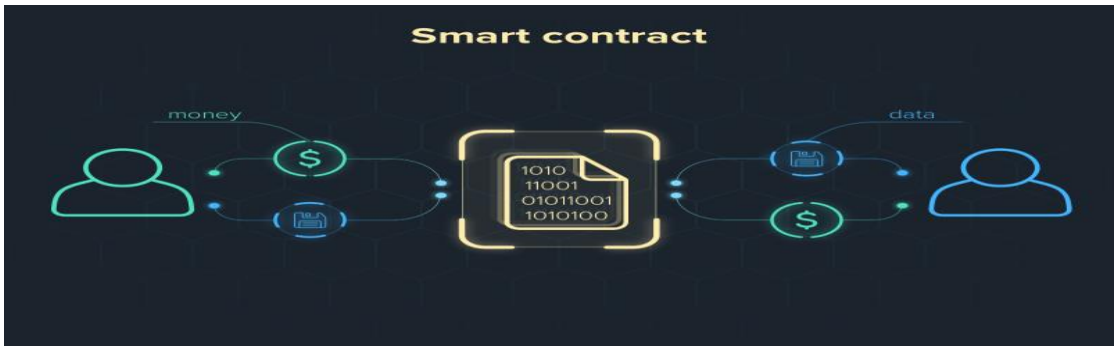
2.7 Έξυπνα συμβόλαια(Smart Contracts)

Ο Αμερικάνος επιστήμονας πληροφορικής και κρυπτογράφος Nick Szabo χρησιμοποίησε αρχικά τον όρο των έξυπνων συμβολαίων . Χρησιμοποίησε το παράδειγμα για την ενοικίαση ενός αυτοκινήτου με ένα έξυπνο συμβόλαιο ώστε να αποφευχθεί η κλοπή του στην περίπτωση που δεν εφαρμοστεί το πρωτόκολλο παράδοσης . Αυτό μπορεί να γίνει και με το παράδειγμα ενός τραπεζικού δανείου όπου ο ιδιοκτήτης μετά την αγορά του αυτοκινήτου δεν είναι σε θέση αποπληρώσει τις δόσεις άρα το έξυπνο συμβόλαιο προχωράει αμέσως στην κατάσχεση του από την τράπεζα του αυτοκινήτου [19].

Με τον όρο έξυπνα συμβόλαια εννοούμε αυτόνομα προγράμματα συνήθως μικρά που δέχονται ως είσοδο μια συναλλαγή, την επεξεργάζονται και σαν αποτέλεσμα έχουμε μια νέα έξοδο. Τα έξυπνα συμβόλαια με τη χρήση ενός blockchain αρχίζουν και εκτελούνται αυτόματα όπου με τις διάφορες προγραμματιστικές ιδιότητες που έχουν εξυπηρετούν τη λογική της χρήση του blockchain για να παράγουν το αντίστοιχο αποτέλεσμα. Το πλεονέκτημα με τη χρήση των έξυπνων συμβολαίων είναι ότι το blockchain παρέχει την εγγύηση ότι δεν μπορούν να τροποποιηθούν είτε να παραβιαστούν οι συμβατικοί όροι. Με την χρήση των συμβολαίων αυτών αναμένεται να αποφευχθεί μια απάτη σύμβασης και να μειωθεί το κόστος εκτέλεσης, ελέγχου και επαλήθευσης. Επιπλέον με τα έξυπνα συμβόλαια ο ηθικός κίνδυνος φαίνεται να υπερκεράζεται ως πρόβλημα .

Αρχικά τα έξυπνα συμβόλαια χρησιμοποιήθηκαν σε ένα blockchain για το Bitcoin υπό τη μορφή ενός είδους ψευδογλώσσας (scripting language). Όταν χρησιμοποιήθηκε παρουσιάστηκαν κάποια προβλήματα κατά την εκτέλεση κάποιων λειτουργιών οπότε αναγκάστηκαν να την περιορίσουν ακόμα πιο πολύ. Με τη χρήση του Ethereum τα έξυπνα συμβόλαια απέκτησαν πιο κεντρικό ρόλο , με την χρήση εικονικών μηχανών όπου γίνονταν η επεξεργασία των συναλλαγών . Χρησιμοποιείται μια γλώσσα υψηλότερου επιπέδου για να γραφτούν τα έξυπνα συμβόλαια ,συνήθως η Solidity, τα οποία στη συνέχεια μεταγλωττίζονται σε ψηφιακό κώδικα Ethereum Virtual Machine (EVM). Στη συνέχεια ο κώδικας και η λογική του συμβολαίου διαμοιράζονται στο δίκτυο ώστε να χρησιμοποιηθεί από τα υπόλοιπα μέλη για να επικυρωθούν και να επεξεργαστούν οι συναλλαγές. Το αποτέλεσμα της εσωτερικής κατάστασης του συμβολαίου γράφεται κατανεμημένα.

Σε επιχειρηματικό τομέα συνήθως χρησιμοποιείται το Hyperledger Fabric. Έχει δημιουργηθεί ένας κώδικας όπου γράφονται τα συμβόλαια και ονομάζεται chaincode. Αποτελείται από ένα μίγμα αλγορίθμων αλλά και από μία σουίτα επιπρόσθετων λειτουργιών που παρέχονται (Hyperledger Fabric Docs) . Μέσα από ένα σύνολο ρυθμίσεων που υπάρχουν αποφασίζεται ποιος κόμβος ή πόσοι ακριβώς από τους χρήστες θα τρέξουν τα έξυπνα συμβόλαια. Σαν αποτέλεσμα ένα σύνολο από κόμβους να εκτελεί μόνο μία συναλλαγή. Με αυτόν τον τρόπο επιτυγχάνεται να εκτελούνται παράλληλα πολλές συναλλαγές με στόχο την αύξηση της απόδοσης αλλά και της κλίμακας του συστήματος. Οι γλώσσες που χρησιμοποιούνται είναι οι Go είτε Node.js.



Εικ.3 Smart Contracts [44]

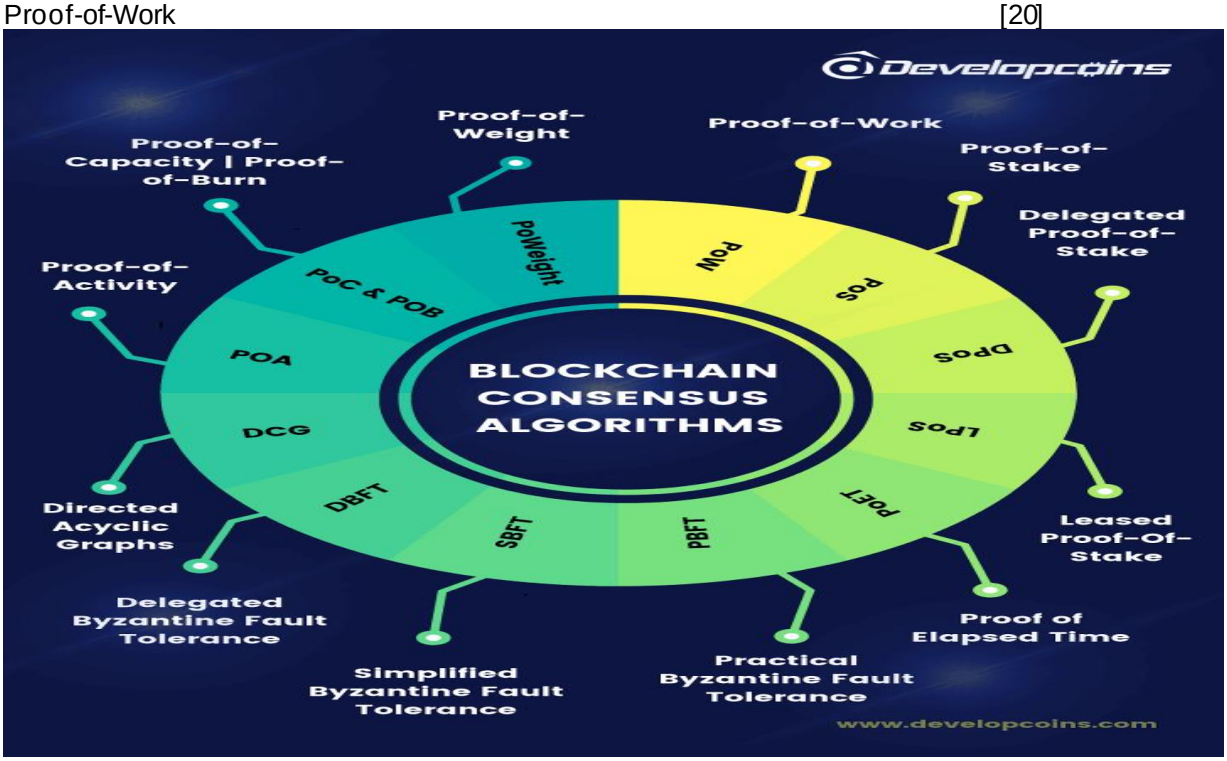
2.8 Συναίνεση (Consensus)

Με τον όρο συναίνεση σε blockchain ορίζουμε η διαδικασία όπου γίνεται η επικύρωση των αξιόπιστων συναλλαγών σε ολόκληρο το δίκτυο και απορρίπτονται οι ελαττωματικές διαδικασίες. Οι μηχανισμοί συναίνεσης είναι κανόνες και πρωτόκολλα διακυβέρνησης στο κατανεμημένο δίκτυο που επιτρέπουν την καταγραφή, την ολοκλήρωση και την εκτέλεση των συναλλαγών υπό ορισμένες προϋποθέσεις. Αλγόριθμοι συναίνεσης υπάρχουν πάρα πολλοί με διαφορετικά χαρακτηριστικά ο καθένας αλλά όλοι εξυπηρετούν τον ίδιο στόχο. Σε blockchain, όπως το bitcoin που είναι ανοιχτό γίνεται χρήση του αλγόριθμου PoW και απαιτείται μεγάλη υπολογιστική ισχύς . Υπάρχει ανταγωνισμός μεταξύ των εξορυκτών (miners) για το ποιος θα ολοκληρώσει πρώτος τις συναλλαγές στο δίκτυο ώστε να ανταμειφθούν. Ένα παράδειγμα που έχει μεγαλύτερη εμπιστοσύνη για τις επικυρώσεις συναλλαγών και επιλέγει τους επικυρωτές του μέσα από ένα σύνολο γνωστών επικυρωτών - validators, είναι το σύστημα συναλλαγών Ripple που ασχολείται με χρηματοπιστωτικές συναλλαγές . Σε αυτό εφαρμόζεται ο αλγόριθμος Ripple Consensus Algorithm κάθε μερικά δευτερόλεπτα από όλους τους κόμβους. Βασίζεται στην έννοια του proof of correctness και σαν αποτέλεσμα εχει να είναι πιο ταχύτερος και βέλτιστος σε σχέση με τον PoW. Μεγάλη εφαρμογή έχει και το PoS, που είναι ένα μοντέλο κατανεμημένης συναίνεσης. Σε τέτοιου τύπου εφαρμογής αλγορίθμου αυτός που θα δημιουργήσει το επόμενο μπλοκ θα γίνει μέσω τυχαίας επιλογής από κριτήρια που μπορεί να είναι η ηλικία , ο πλούτος κ.α, αυτό αποτελεί και το stake που απαιτείται για να κάνει την επικύρωση ενός μπλοκ. Ένας ακόμα γνωστός αλγόριθμος είναι ο Byzantine Fault Tolerance ο οποίος δεν χρειάζεται εξορυκτές και χρησιμοποιείται σε ιδιωτικά blockchain (Hyperledger Fabric) .

Μερικά παραδείγματα από διάφορους Μηχανισμούς Συναίνεσης:[20]

- Proof-of-Stake
- Proof-of-Weight
- Leased Proof-Of-Stake
- Proof-of-Burn
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity

- Simplified Byzantine Fault Tolerance
- Proof-of-Importance
- Proof-of-Capacity
- Delegated Proof-of-Stake
- Proof-of-Work [20]



Εικ.4 Μηχανισμοί Συναίνεσης[20]

Proof of Work (PoW)

Στα κρυπτονομίσματα, η απόδειξη εργασίας (συντομογραφία σε PoW) είναι ένα σύστημα που χρησιμοποιεί δύσκολες στον υπολογισμό αλλά εύκολα επαληθεύσιμες συναρτήσεις για να περιορίσει τα πλεονεκτήματα της εξόρυξης κρυπτονομισμάτων. Αρχικά χρονολογήθηκε από το 1993, η ιδέα Proof-of-Work αναπτύχθηκε για την πρόληψη επιθέσεων στον κυβερνοχώρο, όπως το DDoS . Μια επίθεση DDoS είναι μια κατάσταση όπου μια συσκευή όπως ένας υπολογιστής παραβιάζεται και γεμίζει με κίνηση, με αποτέλεσμα το σύστημά σας να κατακλύζεται και έτσι να εξαντλείται και να απενεργοποιείται. Το Proof of Work είναι ένας αλγόριθμος υπολογιστή που χρησιμοποιείται αυτή τη στιγμή από πολλά κρυπτονομίσματα όπως το Bitcoin, το Ethereum, το Litecoin και άλλα για την επίτευξη συμφωνίας - ή μάλλον μιας αποκεντρωμένης συμφωνίας - σχετικά με την προσθήκη ενός συγκεκριμένου μπλοκ στο blockchain. Το 2009 το Bitcoin κυκλοφόρησε έναν καινοτόμο τρόπο χρήσης του PoW ως αλγόριθμο συναίνεσης που χρησιμοποιείται για την επικύρωση συναλλαγών και τη μετάδοση νέων μπλοκ στο blockchain. Το Hashcash (SHA-256) είναι η συνάρτηση απόδειξης εργασίας που χρησιμοποιούν οι εξορύκτες Bitcoin για να λύσουν υπολογιστικά δύσκολα μαθηματικά προβλήματα προκειμένου να προσθέσουν μπλοκ στο blockchain. Αυτή η συνάρτηση κατακερματισμού παράγει ένα διαφορετικό είδος δεδομένων που χρησιμοποιούνται για να επαληθευτεί ότι έχει εκτελεστεί σημαντικός όγκος εργασίας. Η έννοια του PoW είναι μια ανάγκη να εξηγηθεί ένας δαπανηρός

υπολογισμός υπολογιστή, γνωστός ως εξόρυξη. Αυτή η διαδικασία αναπτύχθηκε για να επιβεβαιώσει τη νομιμότητα μιας συναλλαγής ή να αποφύγει ένα φαινόμενο που ονομάζεται Διπλή δαπάνη.

Proof of Stake (PoS)

Με όρους κρυπτογράφησης, το ποντάρισμα είναι το κρυπτονόμισμα που κατέχει ο χρήστης και δεσμεύεται για να συμμετάσχει στην επικύρωση. Το PoS είναι ένας τύπος μηχανισμού συναίνεσης στον οποίο οι χρήστες ενός δικτύου που βασίζεται σε blockchain πρέπει να ποντάρουν μέρος των νομισμάτων ή των διακριτικών τους, προκειμένου να έχουν την ευκαιρία να επαληθεύσουν τις συναλλαγές σε ένα μπλοκ. Μόλις ένας χρήστης επιλεγεί να επικυρώσει ένα μπλοκ και είναι σε θέση να επαληθεύσει όλες τις συναλλαγές σε αυτό το μπλοκ, τότε ανταμείβεται ένα ορισμένο ποσό κρυπτονομίσματος για την εργασία του. Το PoS είναι συγκρίσιμο με τον αλγόριθμο απόδειξης εργασίας (PoW) καθώς και οι δύο χρειάζονται τους συμμετέχοντες στο δίκτυο (ή τους κόμβους επικύρωσης) για να επιτύχουν μια κατανεμημένη συναίνεση. Επίσης, ένας από τους κύριους στόχους των αλγορίθμων συναίνεσης όπως το PoS είναι η διασφάλιση ενός δικτύου blockchain. Στο PoW, ένας χρήστης που επαληθεύει τις συναλλαγές ονομάζεται miner, αλλά όπως ορίζεται, στο PoS αναφέρεται ως πλαστογράφος. Υπάρχουν πολλά κρυπτονομίσματα που θέλουν να μετατραπούν σε ένα σύστημα απόδειξης στοιχήματος, καθώς είναι πολύ πιο συγκεντρωτικό και ενεργειακά αποδοτικό μακροπρόθεσμα και πολύ ελκυστικό για νέους επενδυτές με νεότερη ιδέα.

Delegated Proof-of-Stake (DPoS)

Ο αλγόριθμος συναίνεσης Delegated Proof of Stake δημιουργήθηκε από τον Daniel Larimer, το 2014. Bitshares, Steem, Ark και Lisk είναι μερικά από τα έργα κρυπτονομισμάτων που χρησιμοποιούν τον αλγόριθμο συναίνεσης DPoS. Ο αλγόριθμος DPoS που χρησιμοποείται σε ένα blockchain μετράει με ένα σύστημα ψηφοφορίας όπου οι ενδιαφερόμενοι επεκτείνουν την εργασία τους σε τρίτους. Δηλαδή είναι σε θέση να ψηφίσουν λίγους αντιπροσώπους που θα εξασφαλίσουν το δίκτυο για λογαριασμό τους. Οι εκπρόσωποι μπορούν επίσης να οριστούν ως μάρτυρες και έχουν την ευθύνη να επιτευχθεί συναίνεση κατά τη δημιουργία και την επικύρωση νέων μπλοκ. Εδώ ο κάθε χρήστης αναλογικά με το ποσό των νομισμάτων που κατέχει εχει και μεγαλύτερη δύναμη ψήφου. Το σύστημα ψηφοφορίας διαφέρει από έργο σε έργο, αλλά γενικά, κάθε εκπρόσωπος παρουσιάζει μια μεμονωμένη πρόταση όταν ζητά ψήφους. Συχνά, οι ανταμοιβές που συγκεντρώνουν οι εκπρόσωποι μοιράζονται αναλογικά με τους αντίστοιχους ψηφοφόρους τους. Κατά συνέπεια, ο αλγόριθμος DPoS δημιουργεί ένα σύστημα ψηφοφορίας που έχει εξάρτηση από τη φήμη αυτών που εκπροσωπούν. Έτσι έστω αν ένας κόμβος δεν λειτουργεί σωστά ή με ακρίβεια, τότε γρήγορα θα προχωρήσουν στην αφαίρεση του και κάποιος άλλος κόμβος θα πάρει τη θέση του. Οι αλυσίδες μπλοκ DPoS είναι πιο επεκτάσιμες, καθώς μπορούν να επεξεργάζονται περισσότερες συναλλαγές ανά δευτερόλεπτο (TPS) άρα είναι και πιο αποδοτικός ο αλγόριθμος σε σχέση με το PoW και το PoS.

Leased Proof of Stake (LPoS)

Το Leased Proof of Stake είναι μια προηγμένη έκδοση του αλγόριθμου Proof of Stake . Γενικά, στον αλγόριθμο PoS, κάθε κόμβος κατέχει ένα συγκεκριμένο ποσό κρυπτονομίσματος και είναι κατάλληλος για να προσθέσει το επόμενο μπλοκ στην αλυσίδα μπλοκ. Ωστόσο, με το LPoS, οι

χρήστες μπορούν να μισθώσουν το υπόλοιπό τους σε πλήρεις κόμβους. Όσο υψηλότερο είναι το ποσό που μισθώνεται, τόσο μεγαλύτερες είναι οι πιθανότητες να επιλεγεί ο πλήρης κόμβος για την παραγωγή του επόμενου μπλοκ. Εάν επιλεγεί ο κόμβος, ο χρήστης θα λάβει μέρος των τελών συναλλαγής που εισπράττονται από τον κόμβο. Το δίκτυο Waves λειτουργεί με έναν αλγόριθμο συναίνεσης με μισθωμένη απόδειξη στοιχήματος (LPoS) σε συνδυασμό με το πρωτόκολλο Waves-NG, επιτρέποντας υψηλό βαθμό επεκτασιμότητας και απόδοσης συναλλαγών.

Proof of Elapsed Time (PoET)

Το PoET είναι ένας αλγόριθμος συναινετικού μηχανισμού που χρησιμοποιείται συχνά στα επιτρεπόμενα δίκτυα blockchain για τον προσδιορισμό των δικαιωμάτων εξόρυξης ή των νικητών μπλοκ στο δίκτυο. Τα επιτρεπόμενα δίκτυα blockchain είναι εκείνα που χρειάζονται οποιονδήποτε υποψήφιο χρήστη να αναγνωρίσει τον εαυτό του πριν του επιτραπεί να ενταχθούν. Ετσι μιλώντας για ένα συστήματος λοταρίας που είναι δίκαιο, ο κάθε κόμβος έχει ίσες πιθανότητες να είναι νικητής. Ο μηχανισμός PoET βασίζεται στην κατανομή των πιθανοτήτων δίκαιης νίκης στον μεγαλύτερο δυνατό αριθμό χρηστών του δικτύου. Ο χρονοδιακόπτης είναι διαφορετικός για κάθε κόμβο. Σε κάθε χρήστη του δικτύου εκχωρείται ένας τυχαίος χρόνος αναμονής και ο πρώτος χρήστης που θα ολοκληρώσει την αναμονή πρέπει να δεσμεύσει το επόμενο μπλοκ στο blockchain. Συγκρίνετε με το τράβηγμα καλαμιών, αλλά αυτή τη φορά, το πιο κοντό στέλεχος στη στοίβα κερδίζει τη λαχειοφόρο αγορά.

Practical Byzantine Fault Tolerance (PBFT)

Το (PBFT) είναι ένας αλγόριθμος που βελτιστοποιεί πτυχές της BFT (με άλλα λόγια, προστασία από βυζαντινά σφάλματα) και έχει εκτελεστεί σε πολλά σύγχρονα κατανεμημένα συστήματα υπολογιστών, μέσα σε αυτά και πολλές πλατφόρμες blockchain. Αυτές οι μπλοκ αλυσίδες συνήθως χρησιμοποιούν έναν συνδυασμό pBFT και άλλων μηχανισμών συναίνεσης. Πρώτοι ο Miguel Castro και η Barbara Liskov εισήγαγαν τον αλγόριθμο (pBFT) σε μια εργασία που κυκλοφόρησε το 1999. Παρείχε αναπαραγωγή μηχανών βυζαντινής κατάστασης υψηλής απόδοσης, επεξεργαζόμενη χιλιάδες αιτήματα ανά δευτερόλεπτο με αυξημένη καθυστέρηση κατά δευτερόλεπτο του δευτερολέπτου. Δύο έργα που χρησιμοποιούν επί του παρόντος το pBFTείναι το Hyperledger Fabric και το Zilliqa.

Simplified Byzantine Fault Tolerance

Απλοποιημένη βυζαντινή ανοχή σφαλμάτων (SBFT), μια γεννήτρια μπλοκ θα συλλέξει όλες τις συναλλαγές κάθε φορά και θα τις επιβεβαιώσει αφού τις συγκεντρώσει μαζί σε ένα νέο τύπο μπλοκ. Η SBFT εφαρμόζει έναν νέο βυζαντινό αλγόριθμο ανοχής σε σφάλματα που αντιμετωπίζει τις προκλήσεις της επεκτασιμότητας και της αποκέντρωσης. Σε αντίθεση με πολλά προηγούμενα συστήματα BFT που λειτουργούσαν καλά μόνο όταν συγκεντρώνονταν γύρω από λιγότερα από 20 αντίγραφα, το SBFT είναι βελτιστοποιημένο για αποκέντρωση και μπορεί εύκολα να διαχειριστεί περισσότερα από 100 ενεργά αντίγραφα. Το SBFT παρέχει ένα έξυπνο περιβάλλον εκτέλεσης συμβολαίων που βασίζεται στον κώδικα byte EVM του Ethereum.

Delegated Byzantine Fault Tolerance

Το (dBFT) είναι ένας μηχανισμός συναίνεσης που έγινε δημοφιλής από ένα κρυπτονόμισμα που ονομάζεται NEO. Το dBFT στην πραγματικότητα λειτουργεί με παρόμοιο τρόπο με το σύστημα διακυβέρνησης μιας χώρας, έχοντας τους δικούς της πολίτες, αντιπροσώπους και ομιλητές για να διασφαλίσει ότι η χώρα (δίκτυο) είναι λειτουργική. Η μέθοδος είναι παρόμοια με το PoS παρά με το PoW, χρησιμοποιώντας ένα σύστημα ψηφοφορίας για την επιλογή εκπροσώπων και ομιλητή.

Directed Acyclic Graphs

Το DAG είναι κυρίως μια μορφή δομής δεδομένων. Ενώ οι περισσότερες από τις αλυσίδες μπλοκ είναι μια "αλυσίδα" από "μπλοκ" που περιέχουν δεδομένα, το DAG είναι ένα ιδανικό γράφημα όπου τα δεδομένα αποθηκεύονται τοπολογικά. Το DAG θα μπορούσε να είναι διαθέσιμο για χειρισμό συγκεκριμένων προβλημάτων όπως – επεξεργασία δεδομένων, δρομολόγηση, συμπίεση. Η ιδέα ενός κρυπτονομίσματος DAG (κατευθυνόμενο άκυκλο γράφημα) παρουσιάστηκε για πρώτη φορά το 2015 από τον Sergio Demian Lerner στην εργασία του που περιγράφει την ιδέα του για ένα ψηφιακό νόμισμα που ονομάζεται νόμισμα DAG. Η τεχνολογία DAG είναι ένα άλλο σύστημα που επιτρέπει στα κρυπτονομίσματα να λειτουργούν σε σύγκριση με αυτά που χρησιμοποιούν τεχνολογία blockchain χωρίς να χρειάζονται μπλοκ και εξορύκτες. Σε ένα DAG, κάθε συναλλαγή παρέχει επικύρωση η μία για την άλλη. Οι χρήστες του δικτύου είναι και εξορύκτες και επικυρωτές, αν και δεν μπορούν να επικυρώσουν τις δικές τους συναλλαγές. Αυτό συνήθως σημαίνει ότι σε μια DAG υπάρχει μικρή ή καθόλου ανάγκη πληρωμής τελών.

Proof of Activity (PoA)

Η απόδειξη δραστηριότητας είναι ένας από τους πολλούς αλγόριθμους συναίνεσης blockchain που χρησιμοποιούνται για να διασφαλιστεί ότι όλες οι συναλλαγές που ακολουθούν στο blockchain είναι αυθεντικές και ότι όλοι οι χρήστες καταλήγουν σε συναίνεση σχετικά με την ακριβή κατάσταση του δημόσιου καθολικού. Η απόδειξη δραστηριότητας είναι μια μικτή προσέγγιση που ενώνει τους άλλους δύο κοινώς χρησιμοποιούμενους αλγόριθμους—δηλαδή, απόδειξη (PoW) και (PoS).

Proof of Importance (PoI)

Το PoI είναι ένας αλγόριθμος συναίνεσης παρόμοιος με το PoS. Οι κόμβοι "γιλεκωνουν" το νόμισμα για να συμμετέχουν στη δημιουργία μπλοκ. Σε αντίθεση με το PoS, το PoI ποσοτικοποιεί την υποστήριξη του δικτύου από έναν χρήστη. Το Κίνημα Νέας Οικονομίας - New Economy Movement - χρησιμοποιεί την Απόδειξη Σημασίας.

Proof of Capacity(PoC)

Το (POC) είναι ένας αλγόριθμος συναινετικού μηχανισμού που χρησιμοποιείται σε blockchains που επιτρέπει στις διάφορες συσκευές εξόρυξης στο δίκτυο να χρησιμοποιούν τον χώρο στον σκληρό δίσκο για να αποφασίσουν τα δικαιώματα εξόρυξης, αντί να χρησιμοποιούν την υπολογιστική ισχύ της συσκευής εξόρυξης (όπως στην απόδειξη εργασίας, PoW) ή το ποντάρισμα του εξορύκτη στα κρυπτονομίσματα (PoS).

Proof-of-Burn (PoB)

Σε αντίθεση με το PoW, το (PoB) είναι ένας συναινετικός μηχανισμός που δεν σπαταλά ενέργεια. Η πραγματική υπολογιστική ισχύς δεν είναι κρίσιμη για την αποφυγή χειραγώγησης. Σε αυτή την περίπτωση, οι κόμβοι καταστρέφουν ή καίνε τα διακριτικά τους, εάν θέλουν να δημιουργήσουν τα επόμενα μπλοκ και να λάβουν μια ανταμοιβή. Με το PoB, κάθε φορά που ένας χρήστης αποφασίζει να καταστρέψει ένα μέρος των διακριτικών του, αγοράζει ένα μέρος της εικονικής υπολογιστικής ισχύος που του δίνει τη δυνατότητα να επικυρώσει τα μπλοκ. Έτσι όσες περισσότερες μάρκες καίνε, τόσο μεγαλύτερη είναι η πιθανότητα να λάβουν την ανταμοιβή. Μεταξύ των πιο διάσημων κρυπτονομισμάτων που χρησιμοποιούν με επιτυχία αυτόν τον μηχανισμό σήμερα είναι το το Factom (FCT),το Counterparty (XCP) και το SlimCoin (SLM) .

Proof of Weight (PoWeight)

Οι μηχανισμοί συναίνεσης απόδειξης βάρους βασίζονται στο μοντέλο Algor και συναίνεσης, που δημιουργήθηκε από ερευνητές στο Εργαστήριο Επιστήμης Υπολογιστών & Τεχνητής Νοημοσύνης του MIT. Το πρωτόκολλο Algorand απλοποιεί πολύ γρήγορες συναλλαγές βασιζόμενος σε ένα πρωτόκολλο βυζαντινής συμφωνίας, το οποίο το καθιστά επίσης ικανό να κλιμακωθεί σε πολλούς χρήστες.

Σημείωση

Χωρίς μηχανισμό συναίνεσης, πολλά από τα δίκτυα blockchain δεν θα ήταν σε θέση να λειτουργήσουν σωστά και να εκτελέσουν την πλήρη χωρητικότητά τους, ενώ θα εξακολουθούσαν να παραμένουν αποκεντρωμένα και πλήρως επαληθευμένα. Είτε πρόκειται για PoS, PoW είτε PoB (ή ακόμα και BFT), υπάρχουν πλέον πολλοί τρόποι χειρισμού της διαδικασίας επαλήθευσης όταν πρόκειται για την ασφάλιση κάθε νέου μπλοκ στο blockchain.

2.9 Ψηφιακά Αγαθά (Digital Tokens)

Τα tokens δεν είναι μία καινούρια έννοια, καθώς παραδοσιακά αντιπροσωπεύουν οποιαδήποτε μορφή οικονομικής αξίας. Από τα αρχαία χρόνια οι άνθρωποι αντάλλασσαν χάντρες, όστρακα και άλλα αντικείμενα με σκοπό την απόκτηση αγαθών. Νεότερα παραδείγματα αποτελούν οι μάρκες καζίνο, τα κουπόνια, και οι μετοχές. Τα χρήματα και τα νομίσματα είναι επίσης token. Τα ψηφιακά token αντιπροσωπεύουν το δικαίωμα άσκησης/διαχείρισης κάποιας λειτουργίας. Στον κόσμο της κρυπτογραφίας, τα tokens αναπαραστούν ενα συγκεκριμένο περιουσιακό στοιχείου, αγαθό ή χρησιμότητα με τη χρήση ενός κλειδιού. Το ψηφιακό αγαθό κυκλοφορεί στο blockchain αντιπροσωπεύοντας την υποκείμενη αξία του υλικού ή άυλου αγαθού του ιδιοκτήτη του οποίου είναι ο κάτοχος του κλειδιού. Δεν υπόκεινται περιορισμοί στο είδος των αγαθών που μπορούν να ψηφιοποιηθούν, έτσι το blockchain έχει δημιουργήσει απέραντες δυνατότητες: μετοχές, ακίνητα, εμπορεύματα, υπηρεσίες, μερίδια ιδιοκτησίας κλπ.

Η δημιουργία token (*tokenization)* είναι μια πολύ εύκολη διαδικασία, καθώς δεν χρειάζεται να τροποποιηθούν οι κωδικοί από ένα συγκεκριμένο πρωτόκολλο ή να δημιουργηθεί από την αρχή ένα blockchain. Αυτό που έχει να κάνει ο δημιουργός είναι να χρησιμοποιήσει μία πλατφόρμα (πχ. Ethereum, Waves) η οποία χρησιμοποιεί smart contracts για αυτό το σκοπό. Η διαφορά των tokens από τα κρυπτονομίσματα είναι πως τα πρώτα, δεν απαιτούν δικό τους

πρωτόκολλο, αλλά λειτουργούν πάνω σε υπάρχοντα blockchain (άλλων νομισμάτων πχ. Ethereum). Η αγορά των token από άλλους χρήστες γίνεται είτε μέσω fiat χρημάτων ή κρυπτονομισμάτων, σε ειδικές πλατφόρμες, τα ανταλλακτήρια/πορτοφόλια *(marketplaces). Σημαντικότερα είδη* token είναι τα ακόλουθα: [14]

Χρησιμότητας (Utility Tokens)

Χρησιμοποιούνται με αποκλειστικό σκοπό την αγορά προϊόντων ή υπηρεσιών της εταιρείας που τα εκδίδει. Διανέμονται στον κόσμο μέσω μίας αρχικής προσφοράς νομισμάτων (ICO), που αποτελεί μέσο χρηματοδότησης *(crowdfunding)* με παρόμοια λειτουργία με αυτή των IPO: όπως σε μία αρχική δημόσια εγγραφή (IPO) οι εταιρείες προσφέρουν μετοχές για να χρηματοδοτηθούν, αντίστοιχα στις ICO προσφέρουν token.

Χρεόγραφα (Security Tokens)

Ψηφιακά χρεόγραφα (επιτόκια, ομολογίες, μετοχές, χρέη κλπ.) τα οποία ονομάστηκαν έτσι από το ρόλο τους ως διατηρητές κάποιας αξίας. Αντιπροσωπεύουν δικαιώματα όπως ιδιοκτησία, μερίσματα, τίτλοι μεριδίων μελλοντικών κερδών ή ταμειακών ροών. Η κατοχή τους συνεπάγεται και την κατοχή των αγαθών, των τίτλων και των μερισμάτων. Είναι διαθέσιμα στις *Security Token Offering,* και υπόκεινται στη νομοθεσία των χρεογράφων *(securities). Διαφέρουν από τις* ICO, καθώς παρέχουν πρόσβαση σε ένα μελλοντικό προϊόν ή υπηρεσία, αλλά δεν παραχωρούν την κυριότητα του αγαθού. Οι STO μπορούν να χρησιμοποιηθούν για την ψηφιοποίηση *(tokenization)* παραδοσιακών δανείων, μετοχών, ιδιοκτησίας, αντίκας, αυτοκινήτου, διευθύνσεις IP κλπ.

Επιβράβευσης (Reward Token)

Δεν έχουν πραγματική αξία, αλλά αποτελούν έναν τρόπο παροχής επιβράβευσης για τη χρήση κάποιου συγκεκριμένου κρυπτονομίσματος ή πλατφόρμας blockchain.

Φυσικά αγαθά και εμπορεύματα (Natural Asset & Commodity Tokens)

Αντιπροσωπεύουν φυσικά αγαθά, τα οποία ψηφιοποιούνται μέσα από τη διαδικασία του tokenization. Είναι δυνατό να αγοραστεί κάποιο αγαθό ή μερίδιό του, όπως χρυσός και πετρέλαιο.

2.10 Βασικές Πλατφόρμες Blockchain

Οι πλατφόρμες blockchain επιτρέπουν την ανάπτυξη εφαρμογών που βασίζονται σε blockchain. Μπορούν είτε να έχουν άδεια είτε χωρίς άδεια. Διάφορες ονομασίες από τις πιο γνωστές είναι το Ethereum, Hyperledger, R3, Ripple , Bitcoin, Cardano, Solana, EOS κ.α .Πιο κάτω αναλύουμε μερικές από αυτές.

Bitcoin

Τα τελευταία χρόνια παρατηρούμε ότι τα κρυπτονομίσματα έχουν εισέλθει σε πολλές αγορές και τομείς και επιτρέπουν ταχύτερες, πιο ευέλικτες και πιο καινοτόμες πληρωμές και τρόπους για την χρηματοδότηση αγαθών και υπηρεσιών. Ανάμεσα τους ένα έχει ξεχωρίσει σημαντικά. Το Bitcoin

είναι ένα από τα πιο γνωστά ψηφιακά νομίσματα που υπάρχουν σήμερα. Το πρόβλημα με τις διπλές δαπάνες μπορεί να λυθεί χρησιμοποιώντας ένα peer-to-peer δίκτυο. Με το peer-to-peer δίκτυο θα μπορέσει να γίνουν συναλλαγές ηλεκτρονικές από το ένα άτομο στο άλλο χωρίς να χρειάζεται να μεσολαβήσει κάποιο χρηματοπιστωτικό ίδρυμα. Αν και οι ψηφιακές υπογραφές είναι μέρος της λύσης τα κύρια οφέλη δε θα αποδοθούν αν χρειάζεται ένα τρίτο έμπιστο μέλος για την αποφυγή της διπλής δαπάνης. Αρα καταληγουμε ότι το Bitcoin είναι ένα οικοσύστημα ψηφιακών χρημάτων που αποτελείται από ένα μείγμα τεχνολογιών κ νέων εννοιών . Όταν μιλάμε για μονάδες Bitcoin εννοούμε το εικονικό νόμισμα κάνουν χρήση όσοι συμμετέχουν στο δίκτυο. Η επικοινωνία τους γίνεται μέσω πρωτοκόλλου πάνω στο διαδίκτυο και είναι προσβάσιμη τόσο από κάθε είδος υπολογιστή όσο και από κινητά.

Έτσι όλοι οι συμμετέχοντες έχουν τη δυνατότητα κάνουν τις συναλλαγές τους σαν να χρησιμοποιούν κανονικά νομίσματα και παράλληλα δίνει στο Bitcoin τα χαρακτηριστικά ενός πραγματικού αγαθού αφού μπορεί να ανταλλαχθεί είτε να πωληθεί. Επειδή το Bitcoin όπως είπαμε δεν έχει υλική μορφή οι συναλλαγές που πραγματοποιούνται είναι ανταλλαγές αξίας. Όλοι οι χρήστες έχουν στην κατοχή τους ένα κλειδί . Τα κλειδιά αυτά αποθηκεύονται στο wallet του κάθε λογαριασμού. Με αυτό τον τρόπο υπάρχει απόλυτος έλεγχος των συναλλαγών λόγω της ύπαρξης των κλειδιών αυτών. Η παρουσία κάποιου κέντρου για έλεγχο δεν είναι αναγκαία γιατί το νόμισμα δημιουργείται μέσω της εξόρυξης. Οι χρήστες χρησιμοποιούν την υπολογιστική ισχύ από τους υπολογιστές ώστε να λύσουν το κρυπτογραφικό παζλ πιο γρήγορα και να ολοκληρώσουν τη συναλλαγή.

Ethereum

Αποτελεί μια ανοιχτή πλατφόρμα blockchain που επιτρέπει σε όλους να χρησιμοποιήσουν αποκεντρωμένες εφαρμογές σε blockchain τεχνολογία. Δεν χρειάζεται κάποιο κέντρο ελέγχου ή διακομιστή για να τρέξει και είναι ανοιχτού πηγαίου κώδικα. Σε σύγκριση με το Bitcoin, είναι πιο προσαρμόσιμο και ευέλικτο. Όλοι μπορούν να φτιάξουν εφαρμογές και να τις δοκιμάσουν και είναι εξίσου ασφαλές για όποιον τις χρησιμοποιεί.

Είναι ένα αποκεντρωμένο πρωτόκολλο blockchain και με τα αυτόνομα προγράμματα που τρέχουν (έξυπνα συμβόλαια) από τη στιγμή που θα εφαρμοστούν χωρίς να σταματήσουν. Όπως και στο Bitcoin έχουμε και εδώ το άυλο νόμισμα με τα ίδια χαρακτηριστικά που ονομάζεται Ether που χρησιμοποιείται στην πλατφόρμα Ethereum. Η σημαντική όμως διαφορά του του Ethereum είναι ότι περιλαμβάνει μια πλήρη γλώσσα προγραμματισμού. Έτσι αυτό δίνει στους προγραμματιστές τη δυνατότητα να φτιάχνουν καλύτερες και μεγαλύτερες εφαρμογές για το δίκτυο. Με λίγα λόγια η πλατφόρμα δίνει τη δυνατότητα σε προγραμματιστές να φτιάξουν “Αποκεντρωμένες Εφαρμογές” (Decentralized Apps), που ένας απλός χρήστης βλέπει μια σχεδόν ίδια τυπική εφαρμογή web, αλλά η κύρια βάση δεδομένων και ο server είναι το blockchain. Οι εφαρμογές που γίνονται μέσω Ethereum έχουν σκοπό να καλύψουν τομείς που σχετίζονται με διαφάνεια και ειλικρίνεια. Τα τελευταία χρόνια πολλές επιχειρήσεις χρησιμοποιούν τη διαφάνεια σε διαδικασίες αποφάσεων. Το Boardroom είναι ένα τέτοιο παράδειγμα Ethereum πλατφόρμας που χρησιμοποιείται για τη διαφάνεια μιας εταιρείας όσων αφορά τις εγκρίσεις που θα πάρει για έργα , επενδύσεις κα. Ένα άλλο παράδειγμα βασισμένο στην πλατφόρμα Ethereum είναι το Augur, το οποίο κατασκευάζει μία έξυπνη πλατφόρμα πρόγνωσης [12],[10].

Το ***Ethereum*** αποτελείται από 7 μέρη:

- Blockchain: μια κατανεμημένη βάση δεδομένων.
- Κρυπτονόμισμα: το Ether.
- Μηχανισμός συναίνεσης: προστατεύει τη βάση δεδομένων με την επίλυση εξισώσεων κρυπτογράφησης και hashing.
- Mining: διαδικασία που γίνεται ώστε να επιβεβαιωθεί η συναλλαγή και να μπορέσουν οι χρήστες να προσθέσουν ένα νέο μπλοκ στην αλυσίδα.

- Προγραμματισμός: όπως αναφέραμε παραπάνω εδώ επιτρέπονται τα αυτόνομα προγράμματα αλλιώς έξυπνα συμβόλαια που χρησιμοποιούνται για να γίνουν όλες οι λειτουργίες του δικτύου.
- Εικονική μηχανή: είναι μια υπηρεσία cloud που επιτρέπει στα προγράμματα που δημιουργούνται να εκτελεστούν
- Mist πρόγραμμα περιήγησης: εδώ χρησιμοποιούνται όσες εφαρμογές αποκεντρωμένες έχουν γίνει πάνω στο Ethereum.

Hyperledger Project

Το 2015 δημιουργήθηκε απο το Linux Foundation το Hyperledger Project. Αποτελείται από blockchains και εργαλεία που χρησιμοποιούνται για να φτίαξουν σε επιχειρηματικό επίπεδο μια δομή ανοιχτού κώδικα για κατανεμημένα καθολικά (Distributed Ledger). Για να γίνει αυτό συμμετείχαν μεγάλες εταιρείες όπως η Cisco, η IBM, η SAP και η Intel. Όταν μιλάμε για Hyperledger Fabric είναι πλατφόρμα κατανεμημένου καθολικού με έξυπνα συμβόλαια, αξιοποιώντας αποδεδειγμένες τεχνολογίες και χρησιμοποιώντας αρχιτεκτονική που επιτρέπει χρησιμοποιούνται διάφορες λειτουργίες για να επιτευχθεί το επιθυμητό αποτέλεσμα . Αυτός είναι ο λόγος που χρησιμοποιείται ευρέως για διάφορα blockchain. Ακόμα δίνει τη δυνατότητα να δημιουργούνται ξεχωριστά επίπεδα ασφαλείας και επιτρέπει μόνο σε όσους χρήστες είναι του δικτύου να έχουν πρόσβαση. Τα χαρακτηριστικά αυτά σε συνδυασμό με την κρυπτογράφηση που χρησιμοποιεί για τις συναλλαγές αποτελεί πόλο έλξης για επιχειρήσεις που θέλουν να επιτύχουν εμπιστευτικότητα και προστασία προσβασιμότητας από τους χρήστες. Έστω ένα παράδειγμα σε ένα δίκτυο για βιομηχανίες αυτοκινήτων όπου οι διαφορετικές βιομηχανίες δεν έχουν πρόσβαση σε όλες τις πληροφορίες που αφορούν τους ανταγωνιστές αλλά μόνο σε όσες έχουν αποφασίσει να μοιραστούν μεταξύ τους. Σαν αποτέλεσμα να υπάρχει η εμπιστοσύνη μεταξύ των διάφορων βιομηχανιών στο τι πληροφορίες μοιράζονται σε συνδυασμό με όλα τα οφέλη του blockchain. Εδώ χρησιμοποιείται αλγόριθμος συναίνεσης BTF σε σχέση με το PoW που χρησιμοποείται στο Bitcoin[4].

3

Εφαρμογές του Blockchain

3.1 Τομείς Εφαρμογής Τεχνολογίας Blockchain

Η τεχνολογία του blockchain έχει φέρει επανάσταση στη διαχείριση των δεδομένων, αποτελώντας ένα χρήσιμο εργαλείο σε πολλά πεδία. Οι πρώτες εφαρμογές του blockchain αφορούσαν τον οικονομικό τομέα· καθώς όμως οι βιομηχανίες αναγνώρισαν την ευρύτερες δυνατότητές του, εξαπλώθηκε ραγδαία και πλέον εφαρμόζεται σχεδόν σε όλα τα πεδία. Ιδιαίτερα σε συνδυασμό με άλλες τεχνολογίες της βιομηχανικής επανάστασης, όπως το διαδίκτυο των πραγμάτων (IOT) τα οφέλη είναι απεριόριστα σε πάρα πολλούς τομείς που ακόμα αναπτύσσεται προς όλες τις κατευθύνσεις. Οι πιο σημαντικοί τομείς είναι:

Χρηματοοικονομικοί Οργανισμοί

Το παγκόσμιο χρηματοπιστωτικό σύστημα διαχειρίζεται τρισεκατομμύρια δολάρια ημερησίως, εξυπηρετεί εκατομμύρια ανθρώπους και υποστηρίζει τη διεθνή οικονομία, έχοντας αξία μεγαλύτερη από 100 τρισεκατομμύρια δολάρια. Στις μέρες μας για να ολοκληρωθεί μία συναλλαγή εμπλέκονται πολλά μέλη, με αποτέλεσμα η επεξεργασία και εκκαθάριση συναλλαγών να είναι αργή και δαπανηρή. Καθένα από αυτά τα μέρη έχει δικό του αρχείο, αυξάνοντας τις πιθανότητες για σφάλματα, ανακολουθίες και κατάχρηση. Οι διεθνείς συναλλαγές πραγματοποιούνται μέσω της μεθόδου SWIFT, όπου τα χρήματα μεταφέρονται από τη μία τράπεζα στην άλλη μέσω μίας σειράς ενδιάμεσων τραπεζών, οι οποίες χρεώνουν τη δική τους αμοιβή. Το χρηματοπιστωτικό σύστημα έχει ανάγκη ένα σύστημα που να επιτρέπει την ασφαλή και γρήγορη μεταφορά αρχείων.

Με τη χρήση του blockchain δεν χρειάζεται πλέον να υπάρχει κάποιο τρίτο μέρος ως ενδιάμεσο, κάνοντας πιο απλή τη διαδικασία και επιπλέον πετυχαίνει να μειώσει το χρόνο που απαιτείται για να γίνει η επιβεβαίωση και η εκκαθάριση μας συναλλαγής άσχετα με το πόσο μακριά μπορεί να βρίσκονται οι χρήστες. Διατηρείται μόνιμο ιστορικό των συναλλαγών, γεγονός που συνεπάγεται την *εξάλειψη απατών και ξεπλύματος χρήματος*. Με τη χρήση έξυπνων συμβολαίων, αυτοματοποιούνται λογιστικές διαδικασίες και δίνεται η δυνατότητα στις επενδυτικές

τράπεζες να εξοικονομήσουν έως και $12 δις. ετησίως. Το blockchain έχει πολλά να προσφέρει και στις αγορές κεφαλαίου. Για χρόνια οι εταιρείες και οι οργανισμοί προσπαθούν να διευκολύνουν τη διαδικασία αγοραπωλησίας και ανταλλαγής μετοχών, οι οποίες πλέον αυτοματοποιούνται. Με την ψηφιοποίηση των χρηματοοικονομικών προϊόντων και υπηρεσιών, οι παραδοσιακές επενδύσεις αναβαθμίζονται, ανοίγουν νέες αγορές και διευκολύνεται το εμπόριο. Το blockchain παρέχει έναν έμπιστο τρόπο επικύρωσης της ταυτότητας των πελατών, το πολύτιμο εργαλείο (KYC). Όλο και περισσότεροι χρηματοπιστωτικοί οργανισμοί στρέφονται προς αυτή την τεχνολογία, ώστε να εκμεταλλευτούν τα πλεονεκτήματα της . Για παράδειγμα το 2016 η Barclays σε συνεργασία με την εταιρεία Wave κατάφερε να φέρει εις πέρας την πρώτη συναλλαγή που έγινε χρησιμοποιώντας τεχνολογία blockchain. Η συναλλαγή αφορούσε πιστωτικό τίτλο και διεκπεραιώθηκε σε 4 ώρες, αντί μίας εβδομάδας. Το Μάιο του 2019, η Barclays επένδυσε στην blockchain start-up Crowdz, που βοηθάει εταιρείες στη συλλογή πληρωμών και αυτοματοποίηση ψηφιακών invoice. Η IBM συνεργάστηκε με τη Stellar και δημιούργησαν το δίκτυο World Wire, το οποίο συνδέει απευθείας τις τράπεζες του κόσμου χωρίς μεσάζοντες. Οι συναλλαγές και οι διασυνοριακές πληρωμές γίνονται σημαντικά ταχύτερες, με ελάχιστα τέλη. Η JP Morgan για παράδειγμα δημιούργησε δικό της κρυπτονόμισμα, το JPMCoin, που έχε ισοτιμία με το δολάριο στοχεύοντας τις άμεσες πληρωμές που θα γίνονται μεταξύ των πελατών. Εφόσον χρησιμοποιείται για την πληρωμή ή την αγορά κάποιου τίτλου, το κρυπτονόμισμα καταστρέφεται και μετά το αντίστοιχο ποσό αποδίδεται σε δολάρια στους πελάτες[18].

Κτηματομεσιτικά

Η κτηματομεσιτική βιομηχανία έχει αντιμετωπίσει αρκετές αναταραχές τα τελευταία χρόνια. Οι συναλλαγές ακινήτων είναι αργές, δαπανηρές, ο όγκος γραφειοκρατίας μεγάλος και οι εξαπατήσεις συχνό φαινόμενο. Οι ψηφιακές λύσεις χρεώνουν ψηλές προμήθειες στους χρήστες, ενώ τα δεδομένα ιδιοκτησιών συχνά είναι εσφαλμένα και η επικοινωνία μεταξύ των ηλεκτρονικών κατακερματισμένων βάσεων δεδομένων αναποτελεσματική. Η επίδραση τεχνολογιών blockchain στην κτηματομεσιτική βιομηχανία είναι καταλυτική, καθώς προσφέρει λύσεις στα ανωτέρω προβλήματα, με τη χρήση μίας ενιαίας, αποκεντρωμένης βάσης δεδομένων: όλες οι πληροφορίες σχετικά με κατοχή γης (πχ κυριότητα, μεταβίβαση, υποθήκη) μπορούν πολύ εύκολα και μόνιμα να αποθηκευτούν σε ένα blockchain. Καθώς τα δεδομένα αποθηκεύονται, επικυρώνονται και μεταφέρονται μέσω του δικτύου, η ανάγκη για ενδιάμεσους ελαττώνεται, εξασφαλίζεται σημαντικός χρόνος και τα κόστη μειώνονται δραματικά. Τα ενδιαφερόμενα μέρη (μεσίτες, ιδιοκτήτες, αγοραστές κλπ.) έχουν περισσότερο έλεγχο στα δεδομένα τους, καθώς μπορούν να συνάψουν συμβόλαια διαδικτυακά, και η πολύπλοκη διαδικασία της διαχείρισης ιδιοκτησίας *(property management)* απλοποιείται σημαντικά.

Κυβερνήσεις και Δημόσιος τομέας

Υπάρχουν αρκετές λειτουργίες της κυβέρνησης που μπορούν να υποστηριχτούν από τις τεχνολογίες blockchain. Τα μοντέλα ηλεκτρονικής κυβέρνησης *(e-government)* χρησιμοποιούνται για την παροχή δημόσιων υπηρεσιών στους πολίτες διαδικτυακά. Δεν πρόκειται για καινούρια μοντέλα καθώς έχουν ήδη ενταχθεί σε αρκετές χώρες, το blockchain όμως τα εξελίσσει προσφέροντας νέες λύσεις και δυνατότητες. Δεδομένου ότι η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για να ελεγχθούν αν υπάρχουν λανθασμένες καταχωρήσεις είτε διπλοεγγραφές μια εμφανής χρήση της είναι για τομείς μητρώων όπως το ληξιαρχείο, κτηματολόγιο, ασφαλιστικά ταμεία και φορολογικό μητρώο. Ένας ακόμα τομέας είναι το μητρώο πνευματικής ιδιοκτησίας. Σε αυτό η χρήση του blockchain βοηθάει να αποδειχθεί ποιος είναι ο κύριος κάτοχος αλλά αναδεικνύει και τη χρονική προτεραιότητα που είναι μια δύσκολη διαδικασία . Η χρήση της τεχνολογία blockchain μας δίνει τη δυνατότητα να έχουμε ένα τρόπο καταχώρησης πιο ασφαλή βοηθώντας να εντοπιστούν τυχόν παρατυπίες όπως πλαστά αντίγραφα και επιπλέον προσφέρει διαφάνεια στους δικαιούχους για την κατανομή αμοιβών. Ακόμα πιστοποιείται από τις αστυνομικές αρχές η χρήση ασφαλών ή μη τροποποιήσιμων πιστοποιητικών. Εάν εφαρμοστεί στις ηλεκτρονικές ταυτότητες καταργείται η

πλαστογραφία, αλλά και ο κάθε πολίτης έχει τον έλεγχο της ψηφιακής του ταυτότητας. Το ίδιο ισχύει για τα διαβατήρια. Οι πολίτες δεν χρειάζεται να εμφανίζονται αυτοπροσώπως στις αρμόδιες υπηρεσίες για να λάβουν τις πληροφορίες και τα πιστοποιητικά που έχουν ανάγκη, αλλά μπορούν να χρησιμοποιήσουν το δίκτυο, καθώς η ίδια η αρχιτεκτονική του εξασφαλίζει πως τα πιστοποιητικά τους είναι έγκυρα και ασφαλή. Οι ψηφοφορίες μπορούν να γίνουν ηλεκτρονικά, μέσα από μία αξιόπιστη και έμπιστη διαδικασία. Η ταυτότητα των ψηφοφόρων επικυρώνεται διαδικτυακά, οι ψήφοι αποθηκεύονται με ασφάλεια και ανωνυμία, και ο νικητής εκλέγεται εύκολα, θεμιτά και γρήγορα. Σαν αποτέλεσμα, μπορεί να εξοικονομηθεί μεγάλο κεφάλαιο για το κράτος, να εξαλειφθούν οι απάτες και να κινητοποιηθούν περισσότεροι πολίτες να καταβάλουν την ψήφο τους. Ψηφοφορίες μπορούν όμως να πραγματοποιηθούν και για ζητήματα που αφορούν άμεσα τους πολίτες, οι οποίοι αποκτούν φωνή και ενισχύεται το αίσθημα της δημοκρατίας. Η κυβέρνηση του Ντουμπάι σχεδιάζε μέχρι το 2020, να μεταφέρει όλα τα κυβερνητικά έγγραφα και συστήματα σε ένα blockchain, σε μία paperless πρωτοβουλία, αποσκοπώντας να γίνει πρωταγωνίστρια στο χώρο και να αυξήσει την αποδοτικότητα σε όλους τους τομείς. Ένα άλλο παράδειγμα είναι της γερμανικής κυβέρνησης που έχει αρχίσει συζητήσεις με διάφορους φορείς ώστε να μπορέσει να βρεί τρόπο αποτελεσματικό για να εκμεταλλευτεί τα πλεονεκτήματα που προσφέρει η τεχνολογία blockchain για ανάπτυξη της οικονομία . Σε ένα τέτοιο πλάνο μπορούν να συμμετέχουν διάφοροι κλάδοι όπως της φαρμακοβιομηχανιας, δημόσιας διοίκησης, αυτοκινητοβιομηχανίας, της ενέργειας αλλά και απο start-up εταιρείες. Το blockchain ευδοκιμεί ιδιαίτερα και στην Αυστραλία, της οποίας η κυβέρνηση αφαίρεσε τους φόρους από συναλλαγές και εμπόριο που πραγματοποιούνται με τη χρήση bitcoin[11],[15].

Εφοδιαστική Αλυσίδα

Η εφοδιαστική αλυσίδα έχει ως τελευταίο σταθμό, τη διάθεση στον πελάτη μέσω λιανικών καταστημάτων ή μη (ισχύει τόσο στις περιπτώσεις που ο πελάτης αγοράζει μέσω φυσικού καταστήματος αλλά και μέσω ηλεκτρονικού καταστήματος). Είναι λοιπόν φυσιολογική η ύπαρξη μεγάλης αλληλεπίδρασης μεταξύ των δύο κλάδων. Για να έχει μια επιχείρηση την καλύτερη απόδοση που επιθυμεί χρειάζεται μια εφοδιαστική αλυσίδα με πάρα πολλή καλή οργάνωση , που διασφαλίζει την ποιότητα, τη συνέπεια, τη διαφάνεια και την ασφάλεια των προϊόντων που κινούνται κατά μήκος της . Για να φτάσει ένα προϊόν στο ράφι ενός καταστήματος, έχει σίγουρα περάσει αρκετά έως και πολλά στάδια, αναλόγως του τόπου στον οποίο παράχθηκε, τους ενδιάμεσους σταθμούς μεταποίησης (εάν χρειάστηκαν), τα κέντρα διανομής και τους ενδιάμεσους εμπόρους που μεσολάβησαν. Όλα τα μέσα και ολοι αυτοί οι σταθμοί που χρησιμοποιούνται για την επίτευξη της μεταφοράς ενός προϊόντος από την παραγωγή μέχρι τη διαθεσιμότητα στον τελικό καταναλωτή, συνθέτουν μια νοητή αλυσίδα σταθμών, η οποία αναφέρεται ως εφοδιαστική αλυσίδα. Καθ' όλο το μήκος της εφοδιαστικής αλυσίδας ρέουν υλικά και πληροφορίες. Ένας ορισμός από τους διάφορους ορισμούς που έχουν δοθεί για την εφοδιαστική αλυσίδα είναι ο εξής: *'Μια αλυσίδα εφοδιασμού είναι ένα δίκτυο εταίρων που συλλογικά μετασχηματίζουν ένα βασικό αγαθό σε ένα τελικό προϊόν στο οποίο δίδεται αξία από τους τελικούς πελάτες και οι οποίοι διαχειρίζονται τις επιστροφές σε κάθε στάδιο'* [7][5].

Ασφάλειες

Η ασφαλιστική βιομηχανία είναι αρκετά περίπλοκη, με διεθνείς κανονισμούς, γραφειοκρατία, συναλλαγές και συμβόλαια. Οι ασφαλιστικές απαιτήσεις καταναλώνουν χρόνο και χρήματα για να επεξεργαστούν. Το blockchain μπορεί να συνεισφέρει στην εξάλειψη ψευδών ασφαλιστικών απαιτήσεων και να αυξήσει την ταχύτητα επεξεργασίας τους με έμπιστο και διαφανές τρόπο. Με την εφαρμογή των έξυπνων συμβολαίων *(smart contracts) οι απαιτήσεις (claims)* μπορούν να επικυρωθούν και να πληρωθούν αυτόματα. Με την απουσία των μεσαζόντων δίνεται η δυνατότητα για γρήγορες και χαμηλότερου κόστους διαδικασίες οπουδήποτε στον κόσμο. Οι ασφαλιστές, βασισμένοι σε ιστορικά δεδομένα, μπορούν να εστιάσουν στον υπολογισμό και στην εξάλειψη ρίσκου, αλλά και στην εξισορρόπηση προσφοράς και ζήτησης. Ασφαλιζόμενοι και

ασφαλιστές έχουν εμπιστοσύνη στο σύστημα και συνεργάζονται καλύτερα. Επιπλέον, σε συνδυασμό με τεχνολογίες IoT, όταν προκύπτει ένα ατύχημα δίνεται η δυνατότητα καταγραφής του και βάσει ειδικών μετρήσεων να υπολογιστεί η αποζημίωση. Ακόμη και στη περίπτωση που δεν καλύπτονται οι προδιαγραφές για να χορηγηθεί η αποζημίωση, το blockchain το αναγνωρίζει και παρακρατεί την πληρωμή[11].

Τομέας Υγείας

Η τεχνολογία blockchain είναι ιδιαίτερα χρήσιμη στο χώρο της υγείας. Συγκεκριμένα χρησιμοποιείται σε περιπτώσεις διευθέτησης ενός θέματος όπου χρειάζεται η εμπλοκή πολλών συμβαλλόμενων μελών και επιπρόσθετα σε διαδικασίες όπου απαιτείται μεγαλύτερη εμπιστοσύνη από την ήδη υπάρχουσα μεταξύ των συμμετεχόντων, η χρήση της κρίνεται βοηθητική. Ακόμα η τεχνολογία blockchain μπορεί να εφαρμοστεί σε καταστάσεις όπου η διαμεσολάβηση τρίτων ατόμων δύναται να παραλειφθεί, ενισχύοντας έτσι την εμπιστοσύνη ή την αποτελεσματικότητα του συστήματος. Τέλος η χρήση της είναι δόκιμη, όταν είναι αναγκαία η αξιόπιστη παρακολούθηση των δραστηριοτήτων του συστήματος ή όταν τα δεδομένα πρέπει να παραμείνουν αξιόπιστα με την πάροδο του χρόνο. Το Blockchain μπορεί να χρησιμοποιηθεί ως αποκεντρωμένο δίκτυο διαχείρισης ιατρικών δεδομένων, κοινό σε όλους τους ενδιαφερόμενους, με ελεγχόμενη πρόσβαση σε ιατρικά αρχεία, χωρίς την επίβλεψη κάποιας κεντρικής αρχής. Η ιδιότητα του αμετάβλητου του blockchain δίνει τη δυνατότητα για βελτίωση της ασφάλειας των δεδομένων υγείας που αποθηκεύονται σε αυτό, γιατί εφόσον γίνει η αποθήκευση στο blockchain δεν μπορούν να αλλοιωθούν ή να ανακληθούν. Όλα τα δεδομένα για την υγεία στο blockchain είναι κρυπτογραφημένα, με χρονοσήμανση και η προσάρτηση τους στο δίκτυο γίνεται με χρονολογική σειρά. Ακόμα ενισχύεται η προστασία της ταυτότητας ή της ιδιωτικής ζωής των ασθενών γιατί τα δεδομένα που αποθηκεύονται χρησιμοποιείται κρυπτογράφηση με κλειδιά. Η διαβεβαίωση ότι δεν γίνεται κακή χρήση των δεδομένων των ασθενών ενισχύεται μέσω των blockchains χάρη στην ισχυρή κρυπτογράφηση, τα πρωτόκολλα και τις καθορισμένες έξυπνες συμβάσεις που περιλαμβάνει . Οι εγγραφές στο blockchain αντιγράφονται σε πολλαπλούς κόμβους, έτσι τα δεδομένα που αποθηκεύονται είναι διαθέσιμα σε όλους από το μπλοκ αλυσίδα γιατί το σύστημα έχει τη δυνατότητα να αποφεύγει τις απώλειες ή τη διαφθορά δεδομένων και επιτρέπει την επαλήθευση των αρχείων που είναι αποθηκευμένα σε blockchain. Αυτό είναι ένα πολύ χρήσιμο στοιχείο στους τομείς υγειονομικής περίθαλψης, για παράδειγμα στον έλεγχο εφοδιαστικής αλυσίδας φαρμάκων αλλά ακόμα και στον τομέα του ασφαλιστικού για επιβεβαίωση απαιτήσεων [38][39].

Παραδείγματα Εφαρμογών

Παρακάτω αναφέρω μερικά παραδείγματα σε διάφορους τομείς όπου η χρήση της τεχνολογίας blockchain έχει επιφέρει σημαντικές αλλαγές κ λύσεις σε πολλά προβλήματα που υπήρχαν μέχρι τότε.

Δημιουργία Ιατρικών Φακέλων

Μία από τις πιο δημοφιλείς και κοινές περιπτώσεις χρήσης blockchain στον τομέα της υγειονομικής περίθαλψης είναι η διαχείριση ηλεκτρονικών ιατρικών φακέλων (Electronic Medical Record), που χρειάζονται για την ηλεκτρονική δημιουργία, την αποθήκευση αλλά και τη

διαχείριση των ιατρικών δεδομένων των ασθενών. Η τεχνολογία blockchain δίνει τη δυνατότητα στους ασθενείς να ασκούν προσωπικό έλεγχο στα δεδομένα που συλλέγονται για εκείνους. Αυτό καθιστά τη λειτουργία ενός γιατρού ευκολότερη, δημιουργώντας ένα υψηλότερο επίπεδο οργάνωσης και προσβασιμότητας με τη χρήση ψηφιακών εργαλείων που εξοικονομούν χρόνο και ταυτόχρονα δημιουργούν μια αμεσότερη επαφή του ασθενή με την κατάσταση της υγείας του. Το Blockchain καθίσταται κατάλληλο για την αποθήκευση και τη διαχείριση των ηλεκτρονικών ιατρικών αρχείων των ασθενών. Αυτό συμβαίνει, εξαιτίας της ιδιότητας της αποκέντρωσης, της αμεταβλητότητας, και της αξιοπιστίας της προέλευσης των δεδομένων που παρέχουν τα έξυπνα συμβόλαια. Το blockchain συμμορφώνεται με την ευρωπαϊκή πολιτική για τα προσωπικά δεδομένα (GDPR), σύμφωνα με την οποία δεν επιτρέπεται να γίνεται επεξεργασία των ευαίσθητων προσωπικών δεδομένων των ασθενών μόνο και εφόσον δοθεί έγκριση από τους ίδιους τους ασθενείς. Η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί ώστε να αναπτυχθεί μια νέα ενιαία πλατφόρμα για τον τομέα της υγειονομικής περίθαλψης ώστε να δώσει την δυνατότητα στους ασθενείς να ελέγχουν το πώς και με ποιους θα μοιράζονται τα δεδομένα τους. Η διαδικασία απόκτησης δεδομένων μπορεί να απλοποιηθεί δραματικά με τη χρήση ενός συστήματος βασισμένο σε blockchain. Ένα τέτοιο σύστημα επιτρέπει στον χρήστη την άμεση φόρτωση των δεδομένων του απευθείας στο σύστημα και την αδειοδότηση χρήσης των δεδομένων αυτών από όποιους συμμετέχοντες αυτός επιθυμεί. Επίσης, μπορεί να εγγυηθεί την παρακολούθηση όλων των δραστηριοτήτων χρήσης των δεδομένων. Η υπόσχεση μιας τέτοιας λύσης είναι η δυνατότητα των χρηστών να αποκτήσουν την κυριότητα των δεδομένων τους και να αποκτήσουν πρόσβαση στα προνόμια που μπορούν να τους προσφέρουν [41,42,43].

Guard time

Το 2011 η κυβέρνηση της Εσθονίας και πιο συγκεκριμένα η Εσθονική Αρχή Ηλεκτρονικής υγείας συνεργάστηκε με την εταιρεία Guard Time μία εταιρεία ασφαλείας δεδομένων . Σκοπός αυτής της συνεργασίας ήταν η δημιουργία ενός πλαισίου βασισμένου σε blockchain για την επικύρωση των ταυτοτήτων των ασθενών. Ολοι οι πολίτες είχαν εκδώσει μία έξυπνη κάρτα η οποία συνδέει τα EHR με την blockchain based ταυτότητα. Οποιαδήποτε ενημέρωση στο EHR κατακερματίζεται (hashed) και καταχωρείται στο blockchain. Με αυτόν τον τρόπο μπορούμε να εξασφαλίσουμε ότι τα στοιχεία που υπάρχουν στο EHR έχουν μία μεταβλητή διαδρομή και ότι τα αρχεία αυτά δεν θα τροποποιηθούν με κάποιο τρόπο. Οποιαδήποτε τροποποίηση στο EHR είναι ασφαλής και ελεγχόμενη. Τα μεταβλητά αρχεία καταγραφής δεδομένων με σφραγίδα χρόνου μπορούν να χρησιμοποιηθούν για να γίνει αρχειοθέτηση των στοιχείων από τις Β.Δ Υγειονομικής περίθαλψης που χρησιμοποιούνται ήδη. Έτσι για να καταχωρηθεί ένα ραντεβού στη Β.Δ Υγειονομικής περίθαλψης έχει χορηγηθεί χρονική σφραγίδα και έχει υπογραφεί και ορθογραφικά σε ένα μπλοκ. Η εφαρμογή αυτής της blockchain λύσεις οδήγησε μέχρι το 2016 στην αποθήκευση ενός εκατομμυρίου ιατρικών αρχείων των πολιτών επιτρέποντας στους ασθενείς να ελέγχουν την πρόσβαση σε δεδομένα μέσω του Keyless Signature Infrastructure . Αυτή η καινοτομία ήταν ένας τρόπος να βοηθήσει στην επίλυση της πρόκλησης για αύξηση της ανταλλαγής κλινικών δεδομένων και της διαλειτουργικότητας για την υγεία και συνεπώς βελτίωση της διαφάνειας των δεδομένων. Η χρήση της τεχνολογίας blockchain από την Εσθονία την έχει καταστήσει μία χώρα όπου το 100% των ιατρικών αρχείων είναι online με ασφαλή και ποιοτική μέθοδο. Η επιτυχία της Εσθονίας έδωσε εμπιστοσύνη και σε άλλες περιοχές όπως στα UAE και σε έναν σημαντικό πάροχο Υγειονομικής περίθαλψης εκεί. Τέλος αυτή η πλατφόρμα χρησιμοποιήσε εκτός από τη βάση δεδομένων blockchain και την Oracle για τη διαχείριση των EHR και θεωρείται ως η μεγαλύτερη blockchain πλατφόρμα στον κόσμο[24].

Health bank

Η Health Bank εταιρεία με έδρα την Ελβετία χρησιμοποιεί τη χαρακτηριστική φράση: “my data my choice, my healthbank” . Ο έλεγχος δεδομένων αφήνετε στο χρήστη ο οποίος μπορεί να επιλέξει να παρέχει τα δεδομένα του για ιατρική έρευνα και ίσως λάβει οικονομική αποζημίωση για αυτή

του την επιλογή. Ο χρήστης μπορεί να ανταμειφθεί με υψηλότερο ποσοστό από το κανονικό εάν τα δεδομένα του έχουν σημαντική αξία. Με αυτόν τον τρόπο η Health Bank γίνεται ένα σύστημα που βασίζεται στον ασθενή (patient- driven System) και το blockchain ερευνάται περισσότερο για να εξασφαλίσει τη γρήγορη ασφαλή και πιστοποιημένη αυθεντικότητα στην πρόσβαση στα δεδομένα των ασθενών. Αυτό θεωρείται ως ένα καλό παράδειγμα για τη βελτίωση της διαφάνειας και της ασφάλειας στην παγκόσμια κοινότητα των κλινικών ερευνών [25].

Patientory

Είναι μία εταιρεία με έδρα της στην Ατλάντα των ΗΠΑ. Η φράση κλειδί της εταιρείας είναι « your Health at your fingertips». Η εταιρεία ενισχύει τους τελικούς χρήστες παγκοσμίως με τη χρήση ασφαλούς πλατφόρμας για τη διαχείριση και μεταφορά των δεδομένων υγείας τους και την επίτευξη ενεργών πληροφοριών για βελτιωμένα αποτελέσματα υγείας. Το Patientory δίνει τη δυνατότητα στους ασθενείς, τους κλινικούς ιατρούς και τους οργανισμούς Υγειονομικής περίθαλψης να έχουν ασφαλή πρόσβαση και μεταφορά προστατευμένων πληροφοριών για την υγεία παρέχοντας παράλληλα χρήσιμες πληροφορίες για τη βελτίωση των αποτελεσμάτων της υγείας. Το Patientory χρησιμοποιεί τεχνολογία blockchain μέσω του PTOYNnetwork για να εξασφαλίσεις κρυπτογράφηση από άκρη σε άκρη ενώ τηρεί τις κανονιστικές οδηγίες και τις απαιτήσεις συμμόρφωσης και είναι συμβατό με το HIPPA. Οι ασθενείς συνεργάζονται πιο στενά με τους παρόχους Υγειονομικής περίθαλψης για τη μετάδοση των δεδομένων. Η εφαρμογή για κινητές υπηρεσίες υγείας έχει βοηθήσει τους ασθενείς να παρακολουθούν το ιατρικό ιστορικό τους, τους λογαριασμούς τους, τα φάρμακά τους, την ασφάλιση τους και ούτω καθεξής . Επίσης οι ασθενείς μπορούν να συνδεθούν με άλλους ασθενείς με παρόμοια προβλήματα υγείας [26].

iSolve

Η Advanced Digital Ledger Technology είναι μία λύση του iSolve που διαχειρίζεται τον κύκλο ζωής ανάπτυξης φαρμάκων και τη φαρμακευτική εφοδιαστική αλυσίδα (drug supply chain) στη βιοφαρμα και στη βιομηχανία της Υγειονομικής περίθαλψης χρησιμοποιώντας το blockchain ως μηχανισμό παρακολούθησης ελέγχου και καταγραφής καθόλη τη διάρκεια της εφοδιαστικής της κυκλοφορίας των φαρμάκων. Η κοινή χρήση των δεδομένων data sharing και η διαφάνεια αποτελούν βασικά στοιχεία του συστήματος. Υπάρχει ανάγκη για σχολαστική παρακολούθηση των φαρμάκων λόγω παραποιημένων και δόλιων φαρμάκων. Αυτό το ζήτημα επισημαίνεται περισσότερο σε περιοχές όπου τα κανονιστικά και νομικά πλαίσια δεν είναι ώριμα και δεν γίνονται οι κατάλληλοι έλεγχοι και παρακολούθηση. Το blockchain μπορεί να χειριστεί τον κύκλο ζωής των φαρμάκων από την ανάπτυξη ως τη διανομή. Παραδείγματος χάριν οι ημερομηνίες λήξης μπορούν να οδηγήσουν με ακρίβεια και να αναιρέσουν πιθανούς λόγους επαναπροσδιορισμού στις αλλαγές ημερομηνιών . Το iSolve διαχειρίζεται επίσης την απόκτηση των IP αγαθών, και στοχεύει στην αύξηση της χρηματοδότησης και στην προώθηση μέσω Smart market περισσότερων φαρμάκων για να μπορούν οι πληροφορίες να διαχειρίζονται με ασφαλή μέθοδο και να είναι ανιχνεύσιμες, αμετάβλητες και ορατές σε οποιοδήποτε επενδυτή ή πάροχο της αγοράς[27].

Genomes

Πρόκειται για μία πλατφόρμα αποθήκευσης γονιδιωματικών πληροφοριών εκτός αλυσίδας και εντός αλυσίδας (off chain, on chain) η οποία προτάθηκε από τον Hannel. Το Genomes παρέχει επίσης μία πλατφόρμα για την ασφάλεια ανταλλαγή βιολογικών πληροφοριών μεταξύ τρίτων. Ως μέσο συναλλαγής εισήχθησαν τα GENE-tokens [28].

Universal Health Coin

Πρόκειται για ένα κρυπτονόμισμα που βασίζεται σε blockchain και A.I για την ανταλλαγή δεδομένων μεταξύ των ενδιαφερομένων και το οποίο πρότεινε ο Gordon. Ο χρήστης αυτού του συστήματος μπορεί να επικοινωνήσει απευθείας με τον κάθενα ιδιοκτήτη ή επεξεργαστή δεδομένων για να αγοράσει και να πουλήσει δεδομένα με αυτό το νόμισμα, UHC. Ολες αυτές τις συναλλαγές και τα δεδομένα είναι κρυπτογραφημένα και ασφαλή με ένα είδος κλειδιών ιδιωτικού δημοσίου [29].

Modum

Η εταιρεία Modum ιδρύθηκε το 2016 με σκοπό να βελτιώσει την παρακολούθηση της αλυσίδας εφοδιασμού φαρμάκων (Pharmaceutical supply Chain). Η ανιχνευσιμότητα και η συμμόρφωση είναι δύσκολο να επιτευχθεί στα τρέχοντα σενάρια το blockchain μπορεί να παρέχει ένα πιο ανθεκτικό σύστημα παρακολούθησης που ελέγχεται καθόλη τη διάρκεια. Ιδιαίτερως στη φαρμακοβιομηχανία όπου σε ορισμένους κανονισμούς είναι απαραίτητο να αναφέρονται απόκλιση στη θερμοκρασία, τις συνθήκες φωτός, την υγρασία καθως οι IoT αισθητήρες παρακολουθούν τη θερμοκρασία των προϊόντων και τα δεδομένα των αισθητήρων και μεταφέρονται στο blockchain. Ενα έξυπνο συμβόλαιο (smart contract) πραγματοποιείται στη συνέχεια και οι εγγραφές δεδομένων συγκρίνονται με τις μετρήσεις έναντι απαίτησης συμμόρφωσης . Αυτή είναι και ακεραιότητα που προσφέρει το σύστημα. Εάν προκύψει κάποια απόκλιση τότε με μία ειδοποίηση ενημερώνονται τα εμπλεκόμενα μέρη που πρέπει να γνωρίζουν[30].

Gem Health

Είναι μία εταιρεία από την Καλιφόρνια η οποία σε συνεργασία με την εταιρεία κολοσσό Philips δημιούργησαν ένα blockchain οικοσύστημα για την υγειονομική περίθαλψη ονομαζόμενο Gem Health Network. Πρόκειται για μία πλατφόρμα που βρίσκεται στην κορυφή της blockchain αρχιτεκτονικής και μπορεί εύκολα να αναπτύξει κατανεμημένες εφαρμογές .Ο στόχος είναι να συνδέσει όλους τους διαφορετικούς βραχίονες της υγειονομικής περίθαλψης (ασθενεις, παροχοι, βιομηχανία) έχοντας ως επίκεντρο τον ασθενή για την ανταλλαγή δεδομένων υγείας. Δεδομένου ότι είναι ένα permissioned blockchain μπορεί να ελέγξει ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες και να διασφαλίσει επίσης την ανωνυμία. Το Gem Health παρέχει ένα σύστημα διαφανές και σε πραγματικό χρόνο για κάθε ισχυρισμό υγείας. Οι επιστήμονες αναφέρουν ότι σε συνεργασία με την εταιρεία Philips αυτή η πλατφόρμα θα μπορεί επίσης να μεταφέρει δεδομένα υγειονομικής περίθαλψης σε πραγματικό χρόνο [31].

Model-chain

Οι Kuo και Ohmo-Machado πρότειναν την αρχιτεκτονική μοντέλου αλυσίδας όπου ένας επιστημονικός ερευνητής μπορεί να συνεργαστεί για δεδομένα σχετικά με την υγεία. Η μελέτη εισήγαγε ένα ιδιωτικό blockchain για τη διαχείριση των μεταδιδόμενων πληροφοριών που έχουν σχέση με την υγεία. Το Model-chain υιοθετεί επίσης το blockchain για την ασφαλή και ισχυρή διάδοση μοντέλων πρόβλεψης (privacy-preserving predictive models) με σκοπό να προστατεύουν την ιδιωτική ζωή μεταξύ των ιδρυμάτων και Υγειονομικής περίθαλψης διότι διαδίδει μόνο προγνωστικά μοντέλα αλλά όχι PHI. Αυτή η μελέτη χρησιμοποίησε μαζί blockchain και machining learning για τη διευκόλυνση της PCOR έρευνας και τη συνεργασία μεταξύ των θεσμικών οργάνων (patient centered outcomes research). Επίσης η διαδικασία του machine-learning χρειάζεται αρκετή ώρα για να τρέξει έτσι ταχύτητα συναλλαγής στο blockchain γίνεται σχετικά αμελητέα. Επίσης το Model-chain υιοθετεί permissioned blockchain networks και έτσι οι

κακόβουλοι κόμβοι δεν θα μπορέσουν να συμμετάσχουν αυθαίρετα στο δίκτυο και ως εκ τούτου ο κίνδυνος μιας επίθεσης 51% είναι ελάχιστος [32].

Pokitdoc

Η αμερικανική πλατφόρμα API as-a-service του Pokitdoc το καθιστά γρήγορο και εύκολο για τους οργανισμούς Υγειονομικής περίθαλψης να φέρουν στην αγορά νέες εφαρμογές και υπηρεσίες. Οι χρήστες μπορούν να αλληλεπιδρούν και να συνδέονται απευθείας με περισσότερους από 700 εμπορικούς συνεργάτες για την ενσωμάτωση των δεδομένων σε πραγματικό χρόνο και να διαχειρίζονται τις ταυτότητες τους για την επικύρωση των συναλλαγών. Οι χρήστες μπορούν να αποκτήσουν πρόσβαση στο 93% των εγκαταλειμμένων ζώων των ΗΠΑ από μία πηγή. Είναι συμβατό ως προς τη συμμόρφωση και ασφάλεια με τους HIPPA, HITRUST, PCI, EHNAC, SOC 2, COR [33].

Burst IQ

Πρόκειται για μία αμερικανική τεχνολογία στην ανάπτυξη ερευνητικών οργανισμών η οποία βασίζεται στο blockchain. Το Burst IQ προσφέρει ένα οικοσύστημα διαχείρισης δεδομένων του χρήστη μέσω διαφόρων υπηρεσιών κυρίως πλατφορμών. Συγκεκριμένα παρέχει μία διαδραστική πλατφόρμα για την κατανομή των big data μεταξύ ατόμων ,χρηστών, οργανισμών. Μέσω της πλατφόρμας αναπτύσσουν γραφήματα προσωπικής ζωής (life graphs) γράφεις με τα δεδομένα του χρήστη τα οποία αποθηκεύονται σε ένα πορτοφόλι υγείας (health wallet). Ο χρήστης μπορεί να μοιραστεί, να διαχειριστεί, να πουλήσει και να δωρίσει ατομικές πληροφορίες από αυτό το πορτοφόλι. Για τη σωστή διαχείριση των big data το Burst IQ χρησιμοποιεί επίσης τη μηχανική μάθηση. Το Burst IQ είναι συμβατό με το HIPPA, GDPR, NIST [34].

Medical Chain

Πρόκειται για ένα κατανεμημένο καθολικό που επιτρέπει το permissioned based blockchain να αποθηκεύσει με ασφάλεια τα αρχεία υγείας ασθενών και ο χρήστης μπορεί να παραχωρήσει άδεια στους επαγγελματίες της υγείας (ιατροί, φαρμακοποιοί, νοσοκομεία, εργαστήρια) για πρόσβαση στα προσωπικά του ιατρικά δεδομένα. Οι συναλλαγές καταγράφονται και ελέγχονται με ένα διαφανή τρόπο αλλά το απόρρητο ασθενούς έχει καίρια σημασία. Αυτό φροντίζει τα ζητήματα της διαλειτουργικότητας και το σενάριο για τον κατακερματισμό των υπηρεσιών υγείας χρησιμοποιώντας απλά χαρακτηριστικά για να διευκολύνουν την αλληλεπίδραση με τους ασθενείς. Σε μία έρευνα που πραγματοποίησε το νοσοκομείο Τζον Χόπκινς των ΗΠΑ συμπεραίνεται ότι τα ιατρικά λάθη είναι ο τρίτος κύριος λόγος θανάτου. Οι πλήρεις κόμβοι λειτουργούν ως διακομιστής δεδομένων και θανάτων στις ΗΠΑ. Με βάση αυτήν την έρευνα εάν οι πληροφορίες θα μπορούσαν να είναι πιο ολοκληρωμένες και η προσέγγιση των δεδομένων υγειονομικής περίθαλψης πιο συντονισμένη θα είχαμε μείωση των ιατρικών σφαλμάτων [35].

Blockchain Health

Πρόκειται για μία αμερικανική εταιρεία λογισμικού η οποία διαχειρίζεται τα δεδομένα που έχουν σχέση με την υγειονομική περίθαλψη. Ο Smith ανέπτυξε μία υπηρεσία το Pokitdoc μεσω της οποίας πάνω από 700 ασθενείς και ερευνητές μπορούν να μοιραστούν πληροφορίες Οι συμμετέχοντες χρησιμοποιούν την Dokchain η οποία βασίζεται σε μία υποδομή αποθήκευσης δεδομένων εντός και εκτός αλυσίδας (on-chain and off-chain data storing) για την επαλήθευση της ταυτότητας σε κάθε κόμβο υπάρχει ένα ζεύγος κλειδιών. Αυτό το σύστημα χρησιμοποιεί ως αλγόριθμο συναίνεσης το PoET. Η συνεχής παρακολούθηση και ασφάλεια των αποθηκευμένων πληροφοριών εξασφαλίζεται μέσω μιας ισχυρής ταυτότητας. Αυτή η πλατφόρμα είναι συμβατή με το HIPPA [36].

MedRec

Πρόκειται για μια εφαρμογή blockchain που έχει σχεδιαστεί για να επιτρέπει στους ασθενείς να μοιράζονται εύκολα τα δεδομένα τους με τα ιδρύματα που επιτρέπουν. Ο ArielEkblaw και ο AsaphAzaria σχεδίαζαν την πρώτη εφαρμογή του MedRec και αναλύεται λεπτομερώς στη WhitePaper "A Case Study for Blockchainin Healthcare". Το *MIT* Media Lab και το ιατρικό κέντρο *Beth Israel Dracones Health Center* νοσοκομείο της Ιατρικής σχολής του Χάρβαρντ ανέπτυξαν από κοινού ένα blockchain based μοντέλο με Ethereum Smart contracts που ονομάζεται MedRec**.** Σκοπός του να διαχειριστεί τα EHRs ενσωματώνοντας ένα αποκεντρωμένο μοντέλο το οποίο θα παρέχει στους ασθενείς ένα ολοκληρωμένο αμετάβλητο αρχείο καταγραφής και εύκολη πρόσβαση στις ιατρικές του πληροφορίες με τρόπο ασφαλή και με εγγυημένη την ακεραιότητα των δεδομένων μεταξύ των παροχών - ιστοτόπων θεραπείας. Το MedRec δημιουργήθηκε για να διαχειριστεί πτυχές όπως υπευθυνότητα, αυθεντικότητα, εμπιστευτικότητα οι οποίες είναι απαραίτητες απαιτήσεις για την τρέχουσα κατάσταση παραβίασης δεδομένων (data breach) παραβίαση του κώδικα δεοντολογίας και άλλα συναφή εγκλήματα που σχετίζονται με τα δεδομένα υγειονομικής περίθαλψης. Το MedRec αποτελεί μία ολοκληρωμένη πλατφόρμα για τον έλεγχο ταυτότητας των ασθενών και την ανταλλαγή μεταξύ των ενδιαφερομένων. Πιο συγκεκριμένα προσφέρει μία αποκεντρωμένη προσέγγιση στη διαχείριση των αδειών, την εξουσιοδότηση και την ανταλλαγή των δεδομένων μεταξύ των Συστημάτων Υγειονομικής περίθαλψης.

Η χρήση blockchain σε αυτή την εφαρμογή έχει ως στόχο να δώσει στους ασθενείς την ικανότητα να έχουν την υπηρεσία και τη γνώση του αν κάποιος έχει προσβασιμότητα στα δεδομένα υγειονομικής περίθαλψης. Αυτά τα δικαιώματα μπορούν να μοιραστούν σε ένα blockchain και να δημιουργήσουν μία αυτοματοποιημένη προσέγγιση με σκοπό την κοινή χρήση των δεδομένων για κλινική και ερευνητική χρήση παρόλο που τα πραγματικά δεδομένα της υγειονομικής περίθαλψης δεν αποθηκεύονται στο blockchain. Ενώ οι άδειες, η θέση αποθήκευσης δεδομένων και τα ημερολόγια ελέγχου διατηρούνται στο blockchain όλα τα στοιχεία της υγειονομικής περίθαλψης παραμένουν στα EHR συστήματα και απαιτούν πρόσθετα στοιχεία λογισμικού για την επίτευξη πραγματικής διαλειτουργικότητας. Το MedRec δουλεύει με διαφορετικό τρόπο για την αποθήκευση των δεδομένων σε σύγκριση με το παραδοσιακό τρόπο αποθήκευσης δεδομένων στο EHR. Σε ένα blockchain αποθηκεύει την υπογραφή του αρχείου αντί για τα πραγματικά αρχεία υγείας. Ετσι διασφαλίζει το αμετάβλητο και έπειτα ειδοποιεί τον ασθενή ο οποίος είναι υπεύθυνος για το αρχείο και καθορίζει την κίνηση του αρχείου με βάση την απαίτηση .Η αποθήκευση του αμετάβλητου αντιγράφου του αρχείου εξασφαλίζεται με την υπογραφή στο αρχείο. Σε αυτό το μοντέλο ο ασθενής είναι υπεύθυνος για τα δεδομένα και αν τυχόν ο ασθενής δεν ενδιαφέρεται η φροντίδα των δεδομένων τότε κάποιος οργανισμός εξυπηρέτησης θα παίξει αυτό το ρόλο. Τα δεδομένα εισάγονται από τον ιατρό μέσω του MedRec provider App οπου η πρόσβαση στα αποθηκευμένα δεδομένα γίνεται μέσω του κατακερματισμενου συνδέσμου (hashed link). Το Ethereum blockchain ελέγχει τις άδειες και ο ασθενής έχει δικαίωμα λήψης ανά πάσα στιγμή καθώς το blockchain επικυρώνει έγκυρα δικαιώματα. Αντί να δημιουργούνται διαφορετικές διεπαφής χρήστη (user interfaces) για διαφορετικά ιδρύματα το σύστημα MedRec απλοποιεί τη λειτουργία του διατηρούν τα blockchain. Οι κόμβοι αυτοί συντηρούνται από τις εταιρείες που παράγουν δεδομένα, τα έξυπνα συμβόλαια ορίζουν την πρόσβαση και τα δικαιώματα στα δεδομένα και είναι η γλώσσα στην οποία ορίζεται το blockchain. Τα πορτοφόλια των ασθενών αποτελούν τη διεπαφή με λίγα λόγια ώστε να μπορούν να έχουν πρόσβαση σε blockchain. Τα πορτοφόλια περιέχουν κλειδιά που παρέχουν πρόσβαση στα κατάλληλα δεδομένα.

Οπως αναφέραμε και πιο πάνω τα δεδομένα παραμένουν στον οργανισμό που τα δημιούργησε και όχι στο MedRec. Αυτός ο οργανισμός λειτουργεί τώρα ως κάτοχος ή αποθετήριο δεδομένων όταν εκτελείται με πλήρη κόμβο. Κατά την εκτέλεση του κόμβου ο οργανισμός συμφωνεί να είναι το κριτήριο των έξυπνων συμβολαίων που αποθηκεύονται στο blockchain και των δεδομένων που δημιουργούνται, να τηρεί τις οδηγίες στα έξυπνα συμβόλαια για να είναι διαθέσιμα τα δεδομένα που χρειάζονται με άδεια. Επίσης το MedRec μετατράπηκε περαιτέρω σε ένα PoS μοντέλο : 1) δεν υπάρχουν τέλη συναλλαγής για τη μετακίνηση των δεδομένων για τη χρήση συμβόλαιο, 2) δεν υπάρχει νόμισμα που πρέπει να εξοριστεί για τις συναλλαγές, 3) διατηρείται από την ομάδα των ενδιαφερομένων που συνθέτουν οι οργανώσεις Υγειονομικής περίθαλψης που συμμετέχουν στο MedRec blockchain. Το πρόγραμμα MedRec έχει δοκιμαστεί

ως απόδειξη της ιδέας proof of concept με τα δεδομένα φαρμάκων και τους προγραμματιστές να προσπαθούν συνεχώς να ενισχύσουν το εύρος του έργου προσθέτοντας περισσότερους τύπους δεδομένων, συνδρομητές δεδομένων και χρήστες. Οπως αποδεικνύεται από το Proof-of-Concept, η Βιοϊατρική και τα αποτελέσματα έρευνας μπορούν να επωφεληθούν σημαντικά από την εφαρμογή του blockchain για την παροχή ταχείας και ασφαλούς πρόσβασης σε διαχρονικά ερευνητικά δεδομένα[37].

3.2 Fraud και Blockchain

Η διαφθορά (απάτη) που σχετίζονται με κυβερνητικούς φορείς συχνά οδηγεί σε πολλά κοινωνικά και οικονομικά προβλήματα, εάν παραμείνουν ανεξέλεγκτα. Η απάτη είναι δύσκολο να αποτραπεί και να εντοπιστεί επειδή είναι μια ακανόνιστη, ανεπαίσθητα κρυμμένη, χρονικά εξελισσόμενη και συνήθως προσεκτικά σχεδιασμένο έγκλημα που μπορεί να λάβει πολλές μορφές. Αύξηση του ποσοστού των περιπτώσεων διαφθοράς επηρεάζει αρνητικά την ανάπτυξη οποιασδήποτε χώρας. Το Blockchain καθίσταται κατάλληλο για την αποθήκευση και τη διαχείριση των ηλεκτρονικών αρχείων και δεδομένων όλων των τύπων. Αυτό συμβαίνει, εξαιτίας της ιδιότητας της αποκέντρωσης, της αμεταβλητότητας, και της αξιοπιστίας της προέλευσης των δεδομένων που παρέχουν τα έξυπνα συμβόλαια. Λόγω της κρυπτογράφησης των πληροφοριών blockchain, η προστασία της ιδιωτικής ζωής διατηρείται, διότι κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση μόνο στις πληροφορίες στις οποίες δικαιούται με την κατοχή των σωστών κρυπτογραφικών κλειδιών. Οι πληροφορίες που περιέχονται στο blockchain είναι ακριβείς, και καταγράφονται με κοινό τρόπο για όλους, η καθεμία πληροφορία περιέχει μια αδιάσπαστη αλυσίδα, πανομοιότυπη με τις άλλες αλυσίδες που περιλαμβάνονται στο δίκτυο ,οι οποίες μπορούν να ελέγχονται προκειμένου να εξασφαλιστεί η ακεραιότητα των δεδομένων. Όταν η τεχνολογία εφαρμόζεται κατά της απάτης το πιο κοινό θέμα στην εφαρμογή της είναι η εμπιστοσύνη μεταξύ όλων των μερών που εμπλέκονται σε μια επιχειρηματική συναλλαγή. Ορισμένα χαρακτηριστικά μοναδικά για το blockchain που μπορούν να μετριάσουν τον κίνδυνο απάτης είναι:

- Ακεραιότητα – Η δομή του Blockchain δημιουργεί ένα επαληθεύσιμο αρχείο κάθε συναλλαγής που έχει πραγματοποιηθεί και αυτές οι συναλλαγές μπορούν να δημιουργηθούν ή/και να τροποποιηθούν μόνο με τη συγκατάθεσή τους.
- Ιχνηλασιμότητα – Το τελικό και αμετάβλητο του Blockchain αφήνει μια μόνιμη, χρονικά σφραγισμένη διαδρομή ελέγχου για κάθε στάδιο μιας επιχειρηματικής συναλλαγής και διαδικασίας.
- Διαφάνεια – Το αποκεντρωμένο δίκτυο του Blockchain συμβάλλει σε μια διαφανή πλατφόρμα στην οποία μπορούν εύκολα να εντοπιστούν και να επισημανθούν δόλιες πληροφορίες και συναλλαγές.
- Ασφάλεια – Η μη απόρριψη και η διαμεσολάβηση της αποθήκευσης δεδομένων από το Blockchain αποτρέπει οποιονδήποτε μεμονωμένο συμμετέχοντα από την κατάχρηση περιουσιακών στοιχείων της εταιρείας, μια από τις πιο κοινές και δαπανηρές μορφές οικονομικής απάτης.

Παραθέτω μερικά παραδείγματα όπου αντιμετωπίζουμε το φαινόμενο απάτης- fraud σε διάφορους τομείς:

Απάτη σε εφοδιαστική αλυσίδα τροφίμων

Στις μέρες μας οι εφοδιαστικές αλυσίδες τροφίμων έχουν εξελιχθεί σε μεγάλο βαθμό με αποτέλεσμα να αποτελούνται από πάρα πολλούς ενδιάμεσους κρίκους. Όπως γνωρίζουμε όλοι ότι έχει να κάνει με το φαγητό είναι ένας ευαίσθητος τομέας και αντιμετωπίζει πολλά προβλήματα. Για αυτό και η επίλυση αυτών των προβλημάτων είναι δύσκολη επειδή ο κάθε κρίκος αυτής της αλυσίδας κρατάει δικό του αρχείο. Σαν αποτέλεσμα να έχουμε πιο συχνά φαινόμενα απάτης είτε περιπτώσεις που έχει προκληθεί κάποια αλλοίωση προϊόντος. Σύμφωνα με μια έρευνα της NSF, οι περιπτώσεις απάτης που έχουν γίνει κοστίζουν στη βιομηχανία τροφίμων περίπου 49 δισεκατομμύρια δολάρια παγκοσμίως ανά έτος και αφορά κυρίως προϊόντα όπως γαλακτοκομικά, τσάι, καφέ, φρούτα, ελαιόλαδο αλλά και πολλά άλλα. Έχουμε ακούσει διάφορα παραδείγματα με σκάνδαλα ακατάλληλων κρεάτων (π.χ αλόγου) που βρέθηκαν στις αγορές είτε γαλακτομικών προϊόντων. Ο Παγκόσμιος Οργανισμός Υγείας αναφέρει ότι σύμφωνα με έρευνες 1 στους 10 ανθρώπους όταν καταναλώσει τροφή που έχει χαλάσει είτε είναι μολυσμένη αρρωσταίνει, ενώ επίσης σημειώνονται 420.000 θάνατοι ετησίως. Η τεχνολογία blockchain επιτρέπει σε όλους τους κρίκους αυτής της αλυσίδας να συνδέονται μεταξύ τους. Δηλαδή, από τους πρώτους κρίκους που μπορεί να είναι οι αγρότες είτε οι παραγωγοί ενός προϊόντος με τη χρήση του blockchain μπορούν να αποθηκεύσουν πληροφορίες για τα προϊόντα όπως φωτογραφίες είτε άλλα χρήσιμα αρχεία από την καλλιέργεια , και αυτές οι πληροφορίες να είναι προσβάσιμες από όλους τους συμμετέχοντες κατά μήκος της εφοδιαστικής αλυσίδας. Επιπλέον τα εργοστάσια που επεξεργάζονται αυτές τις πρώτες ύλες μπορούν να καταχωρούν τις απαραίτητες πληροφορίες για να ξέρουν οι πωλητές ότι τα προϊόντα που θα αγοράσουν διατηρούν την άριστη ποιότητά τους. Στη συνέχεια με την προσθήκη συσκευών IoT μπορούμε εξασφαλίσουμε ότι τα προϊόντα θα φτάσουν ασφαλή κατά τη διάρκεια της μεταφοράς τους από τους διανομείς. Άρα τελικά ο καταναλωτής έχει τη δυνατότητα να γνωρίζει αν το προϊόν κατά μήκος της αλυσίδας έχει υποστεί κάποια αλλοίωση και είναι καλό να το αγοράσει ή όχι. Παρατηρούμε ότι με τον τρόπο αυτό εξασφαλίζεται η ποιότητα γιατί όλα τα στάδια κατά μήκος της εφοδιαστικής αλυσίδας έχουν καταγραφεί άρα αποτρέπεται η απάτη. Όλες οι πληροφορίες και οι συναλλαγές γίνονται μέσα σε λίγα λεπτά. Ένα ακόμη πρόβλημα που αντιμετωπίζεται με τη χρήση blockchain είναι η σπατάλη και η άσκοπη χρήση φαγητού . Ακόμα μπορούμε να προβλέψουμε το χρονικό διάστημα που έχει περάσει από τη παραγωγή μέχρι τη διανομή ενός προϊόντος άρα πότε πρέπει να καταναλωθεί μια τροφή ώστε να διατηρεί την ποιότητα και να είναι φρέσκο. Ένα χαρακτηριστικό παράδειγμα είναι η εταιρεία Walmart η οποία προχώρησε σε συνεργασία με την IBM στη δημιουργία ενός blockchain εντοπισμού φαγητού. Το αποτέλεσμα ήταν η δημιουργία μιας πλατφόρμας με το όνομα IBM Food Trust η οποία αύξησε την αξία της εταιρείας Walmart. Επίσης παρατηρήθηκε αύξηση στην απόδοση, βελτιώθηκε η διαύγεια και η διαφάνεια της εφοδιαστικής αλυσίδας και μειώθηκε ο χρόνος που απαιτείται να εντοπιστεί ένα προϊόν. Ένα άλλο παράδειγμα είναι η εταιρεία MyStory η οποία χρησιμοποιεί την τεχνολογία blockchain για τον εντοπισμό στην προέλευση κρασιών. Η DNV GL δημιούργησε μια εφαρμογή που μέσω κινητού μπορεί και σκανάρει ένα κωδικό QR που έχει στην ετικέτα του κάθε κρασί. Για την υλοποίηση της εφαρμογής χρησιμοποιήθηκε η πλατφόρμα VeChain και έχει ως βάση το Ethereum. Έτσι διαβάζοντας τον κωδικό θα πάρουμε λεπτομέρειες για το κρασί από τί σταφύλια χρησιμοποιήθηκαν , την ποιότητα , το μπουκάλι αλλά και την τελική διανομή του. Για αυτούς τους λόγους ήδη κάποιές ιταλικές εταιρείες χρησιμοποιούν την εφαρμογή [49].

Απάτη σε Έξυπνα Δίκτυα Ενέργειας (Smart Grid)

Ένα έξυπνο δίκτυο διαχείρισης ενέργειας όπως η ηλεκτρική έχει πολλά πλεονεκτήματα, αντιμετωπίζει όμως εξαιρετικά σοβαρές απειλές, οι οποίες χωρίζονται κυρίως σε φυσικές απειλές και ανθρωπογενείς απειλές. Μεταξύ των πολλών απειλών, η πιο συνηθισμένη είναι ότι οι κλέφτες ηλεκτρικής ενέργειας ή οι χρήστες ενέργειας εξαπατούν τις εταιρείες ηλεκτρικής ενέργειας με μια σειρά από τρόπους και στη συνέχεια επιφέρουν μη τεχνικές απώλειες σε ολόκληρο το έξυπνο δίκτυο. Τα τελευταία χρόνια, όχι μόνο το φαινόμενο της κλοπής ηλεκτρικής ενέργειας γίνεται όλο και πιο σοβαρό, αλλά και οι μέθοδοι κλοπής ηλεκτρικής ενέργειας που χρησιμοποιούν οι χρήστες κλοπής ηλεκτρικής ενέργειας είναι ολοένα και πιο ποικίλες και τα μέσα κλοπής ηλεκτρικής ενέργειας γίνονται όλο και πιο εξελιγμένα. Εκτός από τις παραδοσιακές μεθόδους κλοπής ρεύματος, όπως η μέθοδος υπότασης και η μέθοδος υπόγειου ρεύματος , υπάρχουν επίσης μέθοδοι κλοπής ηλεκτρικής ενέργειας υψηλής τεχνολογίας, όπως ισχυρές μαγνητικές παρεμβολές, κλοπές ρεύματος από παροχή ρεύματος υψηλής συχνότητας και επιθέσεις δικτύου σε ευφυείς μετρητές ή κέντρα δεδομένων . Η συμπεριφορά των κλοπών ηλεκτρικής ενέργειας γίνεται ολοένα και πιο εξελιγμένη τεχνικά. Μπορεί να φανεί ότι, στο παρελθόν, τα μέσα στα οποία βασίζονταν οι χρήστες για να κλέψουν ηλεκτρική ενέργεια, όπως η καταστροφή παραδοσιακών μετρητών ηλεκτρικής ενέργειας ή ιδιωτικών γραμμών ηλεκτρικής ενέργειας, έχουν μετατραπεί σε επιθέσεις σε έξυπνους μετρητές μέσω της τεχνολογίας ψηφιακής αποθήκευσης και της τεχνολογίας δικτυακών επικοινωνιών . Η απάτη είναι να μειωθεί ο αντίστοιχος χρόνος κατανάλωσης ενέργειας ή να επανέλθει απευθείας στο μηδέν μέσω παραβίασης δεδομένων, προκειμένου να μειωθεί ο πληρωτέος λογαριασμός ρεύματος. Το blockchain χρησιμοποιείται για την αποθήκευση των δεδομένων του δικτύου διανομής , τη δυσκολία παραβίασης της κατάστασης των έξυπνων μετρητών και σε συνδυασμό με την εφαρμογή κατάλληλων αλγόριθμων ομαδοποίησης καταλήγουμε στον εντοπισμό απάτης. Δηλαδή τοποθετώντας τους μετρητές πάνω σε ένα δίκτυο blockchain μπορούμε να ελέγξουν τις απώλειες που εντοπίζονται από την αρχική διανομή ισχύος μέχρι να φτάσει στους μετρητές. Κάθε φορά που το blockchain μεγαλώνει, τα αποθηκευμένα δεδομένα είναι πιο ασφαλή. Επομένως, η εταιρεία ενέργειας μπορεί να ελέγξει τα αποθηκευμένα δεδομένα του blockchain. Έχει αποδειχθεί ότι η τεχνολογία blockchain έχει κάποια επίδραση στην ακριβή και έγκαιρη ανίχνευση ανωμαλιών κατανάλωσης ηλεκτρικής ενέργειας [48].

Απάτη σε εφοδιαστική αλυσίδα ενέργειας

Άλλος ένας τομέας που η χρήση blockchain μπορεί να εφαρμοστεί για την αποφυγή απάτης είναι ο εφοδιασμός της ενέργειας. Οι περισσότερες εταιρείες που ασχολούνται με τον εφοδιασμό ενέργειας έχουν εγκαταστάσεις και εξοπλισμό που κοστίζουν ακριβά και οι εταιρείες έχουν επενδύσει ακόμα περισσότερα για να φτάσει το προϊόν στον τελικό χρήστη της εφοδιαστικής αλυσίδας (από εξόρυξη μέχρι την μεταφορά ενέργειας). Οι έλεγχοι που πρέπει να περάσουν είναι απαιτητικοί και τα μέσα που χρησιμοποιούνται συνεχώς εκσυγχρονίζονται. Ο τομέας του εφοδιασμού ενέργειας είναι από τους πιο κεντροποιημένους . Και σε αυτόν τον τομέα η χρήση blockchain μπορεί να δώσει τη δυνατότητα στους προμηθευτές καυσίμων να έχουν πρόσβαση σε όλη τη διαδρομή , που έχει ακολουθήσει για να φτάσουν τα καύσιμα σε αυτούς , από διύλιση και εξόρυξη μέχρι καταναλωτή. Έτσι μπορούν να ελέγχουν την ποιότητα αλλά και να μην έχει υπάρξει κάποια νοθεία κατά τη διάρκεια της διανομής. Όλα τα μέλη – κρίκοι της εφοδιαστικής αλυσίδας μπορούν να κάνουν χρήση μίας πλατφόρμας όπου εκεί να αποθηκεύουν τις απαραίτητες πληροφορίες που χρειάζονται για τον εφοδιασμό αλλά και να καταγράφονται όλες οι συναλλαγές που γίνονται από όλα τα μέλη. Με τη διαδικασία αυτή μειώνονται σημαντικά τα έξοδα που απαιτούνται, οι απώλειες και οι νοθείες αλλά τηρούνται και οι κανόνες και οι κανονισμοί που ορίζονται από τις αρμόδιες αρχές. Με τη χρήση του blockchain τα διάφορα προβλήματα που

παρουσιάζονται όπως οι ευαίσθητες πληροφορίες από τις εταιρείες αλλά και οι έλεγχοι που απαιτούνται από τους αρμόδιους φορείς αντιμετωπίζονται άμεσα αλλά και με διαφάνεια και διαύγεια. Ένα παράδειγμα χρήσης της τεχνολογίας blockchain για την εφοδιαστική αλυσίδα ενέργειας μπορεί να γίνει μέσω ψηφιοποίησης αγαθών (tokenization). Δηλαδή δίνεται η δυνατότητα να αγοραστεί ένα αγαθό με κρυπτονομίσματα, όπου αγαθό στη δικιά μας περίπτωση είναι μια μορφή ενέργειας. Αυτό μπορεί να γίνεται μέσω μιας πλατφόρμας όπου επιτρέπεται τέτοια ανταλλαγή. Ένα παράδειγμα είναι η εταιρεία Transactive grid η οποία μέσω μιας πλατφόρμας βασισμένη στο Ethereum δίνει τη δυνατότητα στους χρήστες της να κάνουν συναλλαγές από ένα αποκεντρωμένο σύστημα , δηλαδή να παράγουν , να αγοράζουν αλλά και να πωλούν ενέργεια . Επίσης άλλη μια καινοτόμα ιδέα της εταιρείας είναι να εκμεταλλευτεί την ενέργεια από τη θερμότητα που βγαίνει από τους ηλεκτρονικούς υπολογιστές κατά τη χρήση τους. Η ιδέα της εκμετάλλευσης της ενέργειας μεταξύ χρηστών είναι πολλή σημαντική γιατί βοηθάει στην αντιμετώπιση προβλημάτων όπως η η διακύμανση τιμών και η ανεπάρκεια.

Καταπολέμηση της παραχάραξης φαρμάκων

Η εταιρεία Nuco θέλησε να αντιμετωπίσει την παραχάραξη των φαρμάκων που συμβαίνει με την τροποποίηση των αριθμών και την αλλαγή της αρχικής συνταγής, το διπλασιασμό συνταγών (π.χ. φωτοτυπία) και των λεγόμενων «ιατρικών αγορών», όπου ορισμένα άτομα επισκέπτονται πολλούς γιατρούς για να συγκεντρώσουν όσο το δυνατόν περισσότερες αρχικές συνταγές. Για να το καταφέρει αυτό, ζήτησε να εγκατασταθούν προγράμματα παρακολούθησης που θα βελτιώνουν την πρόσβαση και τον χρόνο απόκρισης, θα σαρώνουν τα δεδομένα για να επισημαίνουν ύποπτα πρότυπα αγορών και θα ενημερώνουν τους γιατρούς και τους φαρμακοποιούς για τα αποτελέσματα. Η εταιρία Nuco αναγνωρίζει το πρόβλημα ως πρόβλημα "ανοικτού βρόχου", αυτό σημαίνει ότι υπάρχει ατέρμονη ανατροφοδότηση μεταξύ των γιατρών και των φαρμακοποιών. Έστω ο ασθενής λαμβάνει ιατρική συνταγή από έναν γιατρό, ο οποίος στη συνέχεια τη παραδίδει σε έναν (ή περισσότερους) φαρμακοποιούς. Ένας φαρμακοποιός δεν γνωρίζει εάν η συνταγή είναι πρωτότυπη, ακριβής ή έχει συμπληρωθεί προηγουμένως. Άρα για να κλείσει ο βρόχος, οι συναλλαγές αποθηκεύονται σε ένα blockchain .Κάθε ενδιαφερόμενος μπορεί να έχει πρόσβαση και να προσθέσει δεδομένα στα blockchains, ανάλογα με την περίπτωση. Για παράδειγμα, ένας γιατρός μπορεί να προσθέσει την εγγραφή της αρχικής συνταγής και ένας φαρμακοποιός μπορεί να ελέγξει ότι η συνταγή είναι αναλλοίωτη. Ένας φαρμακοποιός μπορεί να καταγράψει τις ενέργειες που έχουν συμβεί και ο γιατρός ή άλλος φαρμακοποιός μπορεί να ελέγξει την κατάστασή του [23].

Φαρμακοβιομηχανία και Απάτη

Η χρήση της τεχνολογίας blockchain γίνεται ευρέως στον τομέα της φαρμακοβιομηχανίας γιατί χρησιμεύει στον εντοπισμό των προϊόντων κατά όλο το μήκος της αλυσίδας από την παραγωγή μέχρι τον τελικό καταναλωτή. Αποτελεί ένα ευαίσθητο κλάδο στον τομέα της βιομηχανίας γιατί τα προϊόντα πρέπει να φτάνουν στον καταναλωτή άθικτα και να διατηρείται η ποιότητα. Με τη χρήση ειδικών ετικετών όπως QR είτε barcode οι καταναλωτές έχουν τη δυνατότητα να ελέγξουν τις συνθήκες από την παραγωγή ενός φαρμάκου μέχρι και την τελική διανομή ώστε να γνωρίζει για την τελική ποιότητα και την πιθανή αλλοίωση του. Επιπλέον με τη χρήση της τεχνολογίας IoT μπορούμε να δούμε τις απαραίτητες πληροφορίες όσον αφορά τους προμηθευτές αλλά και τους μεταφορείς. Μπορούμε να ελέγξουμε για παράδειγμα σε τι βαθμούς έγινε η διανομή του συγκεκριμένου φαρμάκου ώστε να αποφευχθεί η αλλοίωσή του αλλά και να μην έχει γίνει κάποια

νοθεία και να αποφύγουμε την απάτη. Ο ρόλος των έξυπνων συμβολαίων είναι σημαντικός γιατί με τη σωστή χρήση τους μπορούμε να ελέγξουμε τις απαραίτητες προδιαγραφές που θέλουμε να έχουμε κι αν παρατηρηθεί κάποια απόκλιση να επαναδρομολογηθεί νέα διαδικασία. Ένα παράδειγμα είναι η εταιρεία modum.io η οποία με τα απαραίτητα μέσα παρακολουθεί καθ'όλη τη διάρκεια της μεταφοράς των φαρμάκων τη θερμοκρασία και την υγρασία. Όταν αυτά φτάσουν στον προορισμό τους εκεί οι πληροφορίες αυτές στέλνονται σε ένα blockchain όπου αναλαμβάνουν το ρόλο τους τα έξυπνα συμβόλαια και ελέγχουν για τυχόν παρατυπίες και αν ναι για τις απαραίτητες διορθωτικές κινήσεις.

Παραβίαση ιατρικών δεδομένων

Η ασφάλεια των δεδομένων και της ιδιωτικής ζωής παραβιάζονται συχνά τόσο ακούσια όσο και από παράνομους χρήστες. Οι διαφορετικοί χρήστες των ιατρικών δεδομένων έχουν διαφορετικούς ρόλους και η πρόσβαση στα δεδομένα θα πρέπει να διέπεται από τα δικαιώματα που χορηγούνται σε αυτούς τους ρόλους. Εξαπίας της εμφάνισης του σύγχρονου τομέα υγειονομικής περίθαλψης τα δεδομένα που παράγονται είναι τεράστια. Διάφορα ιατρικά αρχεία είναι διαθέσιμα από διάφορες πηγές όπως ακτινογραφίες, υπέρηχοι , μαγνητικές αλλά και από IOT συσκευές. Όλη η διαδικασία συλλογής αυτών των δεδομένων μέσω αγνώστων δικτύων επικοινωνίας ενδέχεται να είναι ευάλωτη σε παραβιάσεις ασφαλείας και ιδιωτικότητα . Το *MyHealth - MyData (MH-MD*) είναι μια καινοτομίας του προγράμματος Horizon 2020 που στοχεύει στην ουσιαστική αλλαγή στον τρόπο που μοιράζονται τα ευαίσθητα δεδομένα . Το MH-MD είναι ένα ανοιχτό δίκτυο βιοϊατρικής πληροφόρησης με επίκεντρο τη σύνδεση μεταξύ οργανώσεων και ατόμων, ενθαρρύνοντας τα νοσοκομεία να αρχίσουν να διαθέτουν ανώνυμα τα δεδομένα για ανοιχτή έρευνα, παροτρύνοντας τους πολίτες να γίνουν οι τελικοί ιδιοκτήτες και ελεγκτές των δεδομένων υγείας τους. Το MH-MD προορίζεται να γίνει μια πραγματική αγορά πληροφοριών, βασισμένη σε νέους μηχανισμούς εμπιστοσύνης και σχέσεις αξίας μεταξύ πολιτών της Ευρωπαικής Ένωσης , νοσοκομείων, ερευνητικών κέντρων και επιχειρήσεων. Το My Health - My Data (MH-MD) στοχεύει στη χρήση της τεχνολογίας Blockchain για να επιτρέπει την αποθήκευση και τη μετάδοση των ιατρικών δεδομένων με ασφάλεια και αποτελεσματικότητα. Η ανάπτυξη μιας πλατφόρμας δεδομένων για την υγεία, βασισμένης σε τεχνολογία Blockchain έχει ως αποτέλεσμα να επιτρέπει στους πολίτες της να διαχειρίζονται και να μοιράζονται με ασφάλεια τα κλινικά δεδομένα τους, για να βελτιώσουν την ποιότητα της υγειονομικής περίθαλψης και την προώθηση κλινικής έρευνας και καινοτομίας. Το My Health - My Data στοχεύει να δημιουργήσει μια πλατφόρμα που βασίζεται σε τεχνολογία Blockchain, ένα ψηφιακό βιβλίο όπου οι συναλλαγές δεδομένων είναι ορατές σε ολόκληρο το δίκτυο των ενδιαφερομένων, ελαχιστοποιώντας κάθε πιθανότητα ανεπιθύμητης χρήσης. Μια διεπαφή δυναμικής συγκατάθεσης, θα επιτρέψει στους χρήστες να δίδουν, να αρνούνται ή να ανακαλούν τη συγκατάθεσή τους για πρόσβαση σε δεδομένα, για διαφορετικές χρήσεις, σύμφωνα με τις προτιμήσεις τους. Το έργο θα διερευνήσει τη σκοπιμότητα των εφαρμογών αξιοποιώντας την αξία των μεγάλων συνόλων κλινικών δεδομένων, ιδιαίτερα τις προηγμένες αναλύσεις δεδομένων, τις μηχανές ανάκτησης ιατρικών σχολιασμών και τα μοντέλα συγκεκριμένων ασθενών για φυσιολογική πρόβλεψη [50].

4

Fraud σε Ασφαλιστικές Εταιρείες

4.1 Η απάτη σε Ασφαλιστικές Εταιρείες

Ο κλάδος των ασφαλιστικών εταιρειών(είτε υγειονομικής περίθαλψης είτε αυτοκινήτου είτε κατοικίας) είναι ένας από τους σημαντικότερους παρόχους υπηρεσιών που βελτιώνουν τη ζωή των ανθρώπων. Ένα από τα κύρια καθήκοντα της ασφάλισης υγείας είναι ότι πρέπει να παρακολουθούν και να διαχειρίζονται τα δεδομένα και να παρέχει υποστήριξη στους πελάτες. Λόγω κανονισμών οι ασφαλιστικές εταιρείες δεν μοιράζονται το απόρρητο του ασθενούς - δεδομένα αλλά επειδή τα δεδομένα δεν είναι ενσωματωμένα και δεν συγχρονίζονται μεταξύ των ασφαλιστικών φορέων, έχει αυξηθεί ο αριθμός με απάτες που συμβαίνουν στον τομέα της υγείας. Συχνά παρουσιάζονται ψευδείς πληροφορίες στις ασφαλιστικές εταιρείες ή διπλοεγγραφές ώστε να διεκδικήσει οφέλη από πολλαπλούς ασφαλιστικούς φορείς.

Με βάση τον αντίστοιχο τομέα η απάτη χωρίζεται σε 2 κατηγορίες, την «Οργανωμένη» (Hard fraud or Organized fraud) και την «Ευκαιριακή» (Soft fraud or Opportunistic fraud). Οργανωμένη απάτη ονομάζεται κάθε οργανωμένο σχέδιο με στόχο την απάτη. Συνήθως υπάρχει κάποιο πλάνο ώστε κάποιος να αποκομίσει όφελος από ασφαλιστικές εταιρείες μέσω αποζημίωσης. Στις περισσότερες περιπτώσεις εμπλέκονται περισσότερα από ένα άτομο με στόχο μεγάλες απάτες. Μπορούμε να τους πούμε και «επαγγελματίες» γιατί συνθέτουν οργανωμένο έγκλημα με στόχο τις ασφαλιστικές αποζημιώσεις. Ευκαιριακή απάτη ονομάζεται η απάτη η οποία κρύβεται μέσα στην κακή νοοτροπία. Στις περισσότερες από αυτές τη συναντάμε με τη μορφή της υπερτιμολόγησης μιας ζημιάς. Συνήθως όταν υπάρχει μια πραγματική ζημιά οι ασφαλισμένοι προσπαθούν να αποκαταστήσουν τη ζημιά και παράλληλα να αποκομίσουν και κέρδος από αυτή τη διαδικασία. Η περίπτωση της ευκαιριακής απάτης δεν πρέπει να υποτιμηθεί, γιατί αποτελεί το σημαντικότερο κομμάτι όσον αφορά τον τομέα της ασφαλιστικής απάτης.

Παγκοσμίως , οι αιτίες (the insurance fraud mechanism) που μπορούν να οδηγήσουν κάποιον να κάνει μία ασφαλιστική απάτη είναι τρείς :

1) Η κακή νοοτροπία των ανθρώπων

Όσον αφορά τη νοοτροπία των ανθρώπων θα μπορούσαμε να πούμε ότι είναι ένα θέμα ηθικής. Συνήθως οι ασφαλισμένοι πιστεύουν ότι επειδή πληρώνουν πάρα πολλά λεφτά σε ασφάλιστρα είναι θεμιτό όταν τους παρουσιαστεί η ευκαιρία να κάνουν την απάτη για να κερδίσουν πίσω τα χρήματα τους.

2) Το οικονομικό στρες ή οικονομική δυσχέρεια

Λόγω των αυξανόμενων ρυθμών της ζωής στις μέρες μας μεγαλώνει η πίεση που ασκείται πολλές φορές σε ένα άτομο και λόγω της οικονομικής δυσχέρειας που μπορεί να βρίσκεται τον οδηγούν στην ασφαλιστική απάτη για να μπορέσει να κερδίσει κάποια από τα χρήματα που έχει δώσει.

3) Η έλλειψη ικανού ελέγχου. Η ευκολία της απάτης

Η ευκολία υποκρύπτει την ευκαιρία, αλλά και η πεποίθηση ότι δεν υπάρχει ικανός έλεγχος, ενισχύει την προοπτική να διαπράξει κάποιος μια ασφαλιστική απάτη.

Υπάρχει η εντύπωση ότι η ασφαλιστική απάτη αφορά τις ασφαλιστικές εταιρείες που καλούνται να πληρώσουν τη ζημιά. Στην πραγματικότητα είναι μια βαθιά αντικοινωνική συμπεριφορά που την επιβαρύνεται το σύνολο της κοινωνίας. Πολύ απλά οι ασφαλιστικές εταιρείες όταν δεν καταφέρνουν να εντοπίσουν ή να αποδείξουν την απάτη και αποζημιώνουν ψεύτικες ζημιές οδηγούνται νομοτελειακά σε διορθωτικές αυξήσεις ασφαλίστρων. Τελικώς:

Η υπόλοιπη κοινωνία πληρώνει την απάτη με ακριβότερο κόστος ασφάλισης.

- Ενώ οι οικονομικά αδύναμες κοινωνικές ομάδες θα υποστούν τη μεγαλύτερη πίεση αφού λόγω των αυξήσεων πιθανώς να μην μπορούν να διατηρήσουν την ασφαλιστικής τους προστασία.

Έτσι η ζημιά που προκαλείται είναι :

- *Οικονομική*

Αφού κάποια δισ. κάθε χρόνο παγκοσμίως κλέβονται από την ασφαλιστική βιομηχανία. Ενώ επίσης σημαντικοί είναι και οι πόροι που διοχετεύονται στη διερεύνηση των υποθέσεων για τη διαπίστωση και απόδειξη της απάτης.

- *Φήμης & Αξιοπιστίας*

Οι ασφαλιστικές εταιρείες δέχονται πολλές φορές επιθέσεις διαμαρτυρίας καθώς με διάφορους μηχανισμούς προσπαθούν να ελέγξουν τις απάτες και να εξασφαλίσουν δίκαιες αποζημιώσεις. Ο έλεγχος αυτός προφανώς δεν είναι τις περισσότερες φορές ευχάριστος και αυτό πλήττει τη φήμη και την αξιοπιστία τους. Είναι ένας ζημιογόνος φαύλος κύκλος στα θεμέλια ενός μηχανισμού που δημιουργήθηκε για να επιτρέπει στον άνθρωπο να επιχειρεί και να πορεύεται με ασφάλεια [47].

Κύριες μορφές που συναντάμε σε ασφαλιστικές απάτες στα αυτοκίνητα στην Ελλάδα από τα στοιχεία των ασφαλιστικών εταιρειών που συλλέγουν – με βάση την συχνότητα και τον οικονομικό αντίκτυπο – είναι οι εξής

1. Να υπάρξει αλλοίωση των συνθηκών όταν ένα συμβάν δηλώνεται

2. Να υπερκοστολογήσουν τις ζημίες που προκαλούνται

3. Η δημιουργία ψεύτικου συμβάντος

4. Να δηλώσουν ψεύτικα στοιχεία ασφάλισης(απόκρυψη νέου οδηγού)

5. Πλαστές/ψεύτικες ασφάλειες

Σύμφωνα με τα στοιχεία που έχει η ***συλλέξει η ασφαλιστική εταιρεία Hellas Direct*** διακρίνει τις τρεις πιο συχνά εμφανιζόμενες απάτες από τους ασφαλισμένους της, οι οποίες είναι

1. Θραύση Κρυστάλλων : Είναι η πιο συχνή αιτία απάτης. Ενώ υπάρχει ένα κρύσταλλο που μπορεί να έχει σπάσει πολύ πριν κάνει ο πελάτης κάποια ασφάλεια , μόλις ενεργοποιηθεί το ασφαλιστήριο από την ασφαλιστική εταιρεία δηλώνεται το συμβάν με αποτέλεσμα η ασφαλιστική να καλύψει την επισκευή του ακόμα και την πλήρη αντικατάστασή του σε κάποιες περιπτώσεις.

2. Κλοπή : Σε αυτές τις περιπτώσεις συνήθως ο ασφαλισμένος έχει με κάποιο τρόπο εξαφανίσει το όχημά του και αξιώνει από την εταιρεία την αποζημίωση για την κλοπή του.

3. Δήλωση εξυπηρέτησης : Αυτή η μορφή απάτης γίνεται συνήθως μεταξύ γνωστών προσώπων. Ο ένας δηλώνει ότι προκάλεσε μία ζημιά στο όχημα του άλλου με σκοπό η ασφαλιστική να επισκευάσει το αυτοκίνητο. Συνήθως πρόκειται για εικονικά ατυχήματα.

Κατά τη διαδικασία που γίνεται ώστε να ανιχνευτούν οι πιθανές ασφαλιστικές απάτες εντοπίζονται οι πιο συχνές περιπτώσεις που δηλώνουν οι ασφαλισμένοι και έχουν ομαδοποιηθεί ως:

• Οι ζημίες που προκαλούνται χωρίς να συμμετέχουν οχήματα

• Οι ζημιές που δηλώνονται αμέσως μετά την έναρξη μιας ασφάλειας είτε μετά την επέκτασή της.

• Οι ζημιές που δεν συμβαδίζουν με τις συνθήκες του ατυχήματος

• Η απαίτηση να κοστολογηθεί η ζημιά παραπάνω από την πραγματική αξία που έχει

• Έγγραφα που έχουν παραποιηθεί είτε είναι πλαστά

• Οι περιπτώσεις να μην μπορούν οι ασφαλιζόμενοι να προσκομίσουν αποδεικτικά στοιχεία γιατί το συμβάν έγινε σε περιοχή μη προσβάσιμη εύκολα είτε απομακρυσμένη

• Οι ασυνεπείς δηλώσεις

• Περιπτώσεις που δηλώνουν συνέχεια τις ίδιες ζημιές

• Περιπτώσεις που ο ίδιος ασφαλιστικός φορέας δηλώνει τις ζημιές που έγινα σε ένα περιστατικό

• Συμβάντα να έχουν γίνει αργά τις νυχτερινές ώρες

4.2 Ανάλυση Σεναρίου

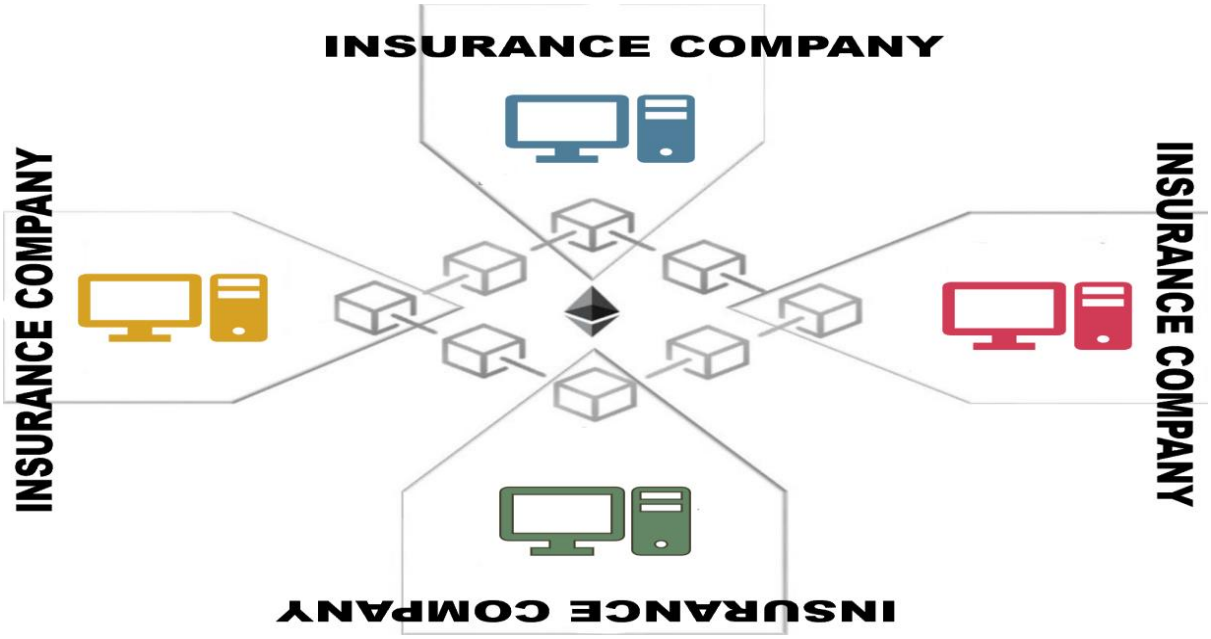
Η τεχνολογία τα τελευταία χρόνια έχει κάνει τρομερά βήματα εξέλιξης και η ενσωμάτωση της σε όλους τους τομείς είναι απαραίτητη. Το ίδιο έχει κάνει και ο ασφαλιστικός τομέας. Οι νέες τεχνολογίες (machine learning ,social media, artificial intelligence, IoT, blockchain, κ.α.) αλλά και οι αναπτυσσόμενοι Insurtech μπορούν να προσφέρουν νέες, ενδιαφέρουσες και αποδεδειγμένες προτάσεις αλλά και λύσεις για τον ασφαλιστικό τομέα αλλά και για τους ίδιους τους πελάτες. Ένα παράδειγμα αποτελεί η λύση για το πρόβλημα της ασφαλιστικής απάτης που ονομάζεται double dipping. Όταν αναφερόμαστε στο double dipping εννοούμε την ασφαλιστική απάτη που γίνεται όταν κάποιος ζητάει- αξιώνει από δύο ή και περισσότερες ασφαλιστικές εταιρείες αποζημίωση για το ίδιο περιστατικό. Σε τέτοιες περιπτώσεις οι εταιρείες ξεχωριστά η καθεμία προχωράνε στην αποζημίωση του ασφαλισμένου για την ίδια περίπτωση ζημιάς. Έστω ένα παράδειγμα που κάποιος συμμετέχει σε ένα ατύχημα αυτοκινήτου και μετά ζητάει αποζημίωση από δύο διαφορετικές ασφαλιστικές εταιρείες. Σε πολλές από τις περιπτώσεις αυτές που συναντάται η διπλή αξίωση μπορεί να θεωρηθεί ως αδίκημα αν ο απώτερος σκοπός για αυτόν που το επιδιώκει είναι το κέρδος μέσω αμοιβής από τραυματισμό ή ζημιά.

Η ρίζα του κακού της συγκεκριμένης απάτης και ο λόγος που δεν μπορεί να εντοπιστεί είναι επειδή *ο διαμοιρασμός των δεδομένων (data-sharing) ανάμεσα στις ασφαλιστικές εταιρείες δεν είναι εφικτός για τον ασφαλιστικό τομέα στην Ελλάδα.* Σε αντίθεση με τις άλλες χώρες του εξωτερικού στις οποίες οι ασφαλιστικές μπορούν να μοιράζονται τα δεδομένα τους και όποια άλλα στοιχεία θέλουν, διαπιστώνουμε ότι εκεί η αντιμετώπιση της συγκεκριμένης μορφής απάτης αντιμετωπίζεται πολύ εύκολα. Σημαντικό ρόλο παίζει η τεχνολογία Blockchain η οποία μπορεί να χρησιμοποιηθεί για να δοθεί λύση για τον εντοπισμό πιθανών περιπτώσεων τέτοιας απάτης αλλά και να προσφέρει την απαραίτητη ασφάλεια για τα δεδομένα και την τήρηση των απαραίτητων συνθήκων βάσει GDPR .

Πριν περάσουμε στην επεξήγηση του σεναρίου πρέπει να αναφέρουμε ότι στις περιπτώσεις που έχουν διαπιστωθεί απάτες τέτοιου τύπου και έχουν πάει δικαστικά, η εταιρεία που υποχρεούται να αποζημιώσει τον πελάτη είναι πάντα αυτή που έχει υπογράψει τελευταία ασφαλιστήριο. Για αυτό το λόγο οι πελάτες όταν θέλουν να πραγματοποιήσουν μια απάτη και κάνουν διπλές και τριπλές ασφαλίσεις στα αμάξια τους δεν ενημερώνουν τις εταιρείες ή προσέχουν να κάνουν την απάτη το χρονικό διάστημα που λήγει η μία ασφάλεια και έχει ήδη ξεκινήσει η άλλη. Οπότε έτσι μπορούν να ζητήσουν αποζημίωση π.χ για κλοπή από όλες τις

εταιρείες χωρίς να γίνουν αντιληπτοί εφόσον δεν έχουν διαμοιρασμό των στοιχείων τους οι ασφαλιστικές.

Αρχικά ας παρουσιάσουμε το παράδειγμα μας όπως φαίνεται από το σχεδιάγραμμα :



Εικόνα 6. Διάγραμμα Εφαρμογής Σεναρίου

Γιατί όμως να χρησιμοποιήσουμε Blockchain στο παράδειγμά μας: Μέχρι σήμερα τα πιο ευρέως συστήματα για ανάπτυξη κατανεμημένων συστημάτων είναι τύπου client-server. Εδώ εντοπίζουμε δύο προβλήματα. Το ένα έχει να κάνει με την σημαντική θέση που κατέχει ο server όπου σε περίπτωση που πέσει παραλύει ολόκληρο το σύστημα. Ενώ στην περίπτωση του Blockchain κάθε κόμβος είναι συνδεδεμένος με τον άλλο οπότε μετριάζουμε την απώλεια. Και το δεύτερο έχει να κάνει με την πιθανότητα αν και υπάρχουν μέτρα προστασίας τα δεδομένα που αποθηκεύονται στο server να χαθούν είτε να αλλαχθούν. Και εδώ με τα χαρακτηριστικά του Blockchain που παρέχουν στα δεδομένα του αμεταβλητότητα σε συνδυασμό με τους μηχανισμούς συναίνεσης μπορούμε να αποφύγουμε την αλλοίωσή τους.

Στο παράδειγμά μας οι πληροφορίες που θα χρησιμοποιηθούν για τον έλεγχο (πινακίδα αυτοκινήτου) είναι διαθέσιμες σε όλες τις ασφαλιστικές. Κάθε εταιρεία έχει ένα αντίγραφο δεδομένων και κώδικα στο Blockchain. Έστω ένα πελάτης θέλει να κάνει μια ασφάλιση αυτοκινήτου. Πάει λοιπόν σε μια ασφαλιστική και κάνει αίτηση. Εκεί με τον ασφαλιστή δίνει τα απαραίτητα έγγραφα που θα του ζητήσουν, όπως ταυτότητα, αριθμό πινακίδας , χαρακτηριστικά αμαξιού κ.α. Εφόσον τα βρουν με τον ασφαλιστή για τους όρους που θα γίνει η ασφάλεια μένει να επικυρώσουν την ασφάλεια. Εκεί ο ασφαλιστής ανεβάζει το συμβόλαιο στο Blockchain δίκτυο ώστε ένα smart contract να ενεργοποιηθεί. Σκοπός είναι να διαπιστωθεί αν υπάρχει για το ίδιο όχημα κάποια ενεργή ασφάλεια ήδη (σε αλλη ασφαλιστική) . Εφόσον δεν υπάρξει κάποια αντιστοιχία (ο έλεγχος γίνεται με την πινακίδα αυτοκινήτου) τότε ενεργοποιείται το ασφαλιστήριο

και η πληροφορία γίνεται διαθέσιμη στο δίκτυο blockchain. Έτσι αποφεύγεται να γίνει απάτη double dipping.

Είναι γεγονός ότι μια εταιρεία δεν επιθυμεί ποτέ να μοιραστεί κρίσιμες επιχειρηματικές πληροφορίες με έναν ανταγωνιστή, καθώς μπορεί να έχει συνέπειες όσον αφορά το μερίδιο αγοράς της. Στη συγκεκριμένη περίπτωση της πρόληψης της απάτης οι ασφαλιστικές εταιρείες ενδέχεται να επωφεληθούν από την ανταλλαγή ορισμένων στοιχείων πληροφοριών σχετικά με τους πελάτες τους (μόνο αν υπάρχει ενεργή ασφάλεια χωρίς να ξέρουμε σε ποια ασφαλιστική). Τα κοινά δεδομένα (αριθμός πινακίδας) που αποθηκεύονται στο blockchain δεν έχουν ανταγωνιστική αξία για τις ασφαλιστικές εταιρείες, αλλά μπορεί να τους επιτρέψουν να αποφύγουν κάποιους μελλοντικούς πονοκεφάλους όσον αφορά τις αποζημιώσεις που θα έπρεπε να πληρώσουν σε όσους έκαναν την απάτη.

Για την υλοποίηση του σεναρίου μπορούμε να φτιάξουμε Smart Contract με τις εξής συναρτήσεις

- setClient(string _Name ,uint _AMKA, string _claims) public onlyOwner

  Εφόσον ο πελάτης δεν έχει άλλη αίτηση που να εκκρεμεί προχωράμε στην κατάθεση της αίτησης όπου καταχωρούνται τα στοιχεία του πελάτη .Αυτό γίνεται μόνο από εξουσιοδοτημένο φορέα. Τα στοιχεία μπορεί να είναι χαρακτηριστικά μοναδικά για τον πελάτη όπως πινακίδα αυτοκινήτου ,κ.α, ένα χαρακτηριστικό για το αν εκκρεμεί αιτηση , ένα timestamp τελευταίας αίτησης ή ποτέ έκανε-παρέλαβε προηγούμενη αίτηση, αλλά και μια διεύθυνση hash όπου θα αποθηκεύουμε περαιτέρω πληροφορίες για την αίτηση και τον πελάτη μέσω IPFS

- setOffice(address _address) onlyOwner)

  Οποιοσδήποτε φορέας μπορεί εξουσιοδοτηθεί από τους stakeholders είτε την αρμόδια υπηρεσια να δέχεται αιτήσεις και να οριστικοποιεί τις ασφάλειες

- setInsurance(address _uId, uint _amountU) returns (string)

  Εδώ ο εξουσιοδοτημένος εφόσον έχει ολοκληρωθεί η αίτηση του πελάτη καταχωρεί την αποζημίωση βαση ασφαλιστηρίου πελάτη αν τα στοιχεία ελέγχου που έχει θέσει η κάθε ασφαλιστή πληρούνται.

Στο αντίστοιχο link υπάρχει ο κώδικας του σεναρίου:

https://gist.github.com/Kri-Kost/ea540fe8c9b2e72269547ed18ac101c3

Με τη χρήση της τεχνολογίας blockchain μπορούμε μειώσουμε την γραφειοκρατία που απαιτείται μεταξύ των συμφωνιών που γίνονται όταν κάποιο ασφαλιστήριο-συμβόλαιο υπογράφεται , όπως επίσης και τον χρόνο από όλη αυτή τη διαδικασία . Γλιτώνουμε χρόνο από τις συναλλαγές που γίνονται μέσω blockchain και επιπλέον μας δίνει μεγαλύτερη ελεγξιμότητα. Το blockchain προσφέρει ασφάλεια, διαφάνεια και διαύγεια. Επιπλέον η χρήση του προσφέρει τη δυνατότητα να δημιουργηθούν σχέσεις εμπιστοσύνης μεταξύ των εμπλεκόμενων μελών και παρέχει ένα συνεπές, αυτόματο περιβάλλον εκτέλεσης μιας σύμβασης . Μπορούμε να πούμε ότι υπάρχει μία βάση όπου αποθηκεύονται όλες οι συναλλαγές και τα συμβόλαια, με σκοπό να μειωθεί το διοικητικό φόρτο εργασίας αλλά και να εξασφαλιστεί η συνεπή εκτέλεσης των ασφαλιστηρίων .Σκοπός είναι αξιοποίηση όπως τεχνολογίας του Ethereum blockchain για την ανάπτυξη μιας αποκεντρωμένης εφαρμογής (Dapp) . Αυτό βασίζεται στην ανάπτυξη των έξυπνων συμβολαίων (smart contracts), τα οποία θα αποτελέσουν την καρδιά του συστήματος. Τα έξυπνα συμβόλαια θα περιέχουν τον κώδικα που θα εκτελείται στο Ethereum blockchain, στην ουσία θα υλοποιούν όλη την λειτουργικότητα και θα δώσουν στην εφαρμογή αποκεντρωμένο χαρακτήρα. Για τον έλεγχο του πιθανού σεναρίου μπορούμε να χρησιμοποιήσουμε:

Ethereum Virtual Machine

Το Ethereum είναι με λιγα λόγια ένα blockchain που προγραμματίζεται. Δίνει τη δυνατότητα στους χρήστες του να φτιάχνουν μόνοι τους τις λειτουργίες που θέλουν να εκτελούνται σε αντίθεση με το Bitcoin που παρέχει στους χρήστες του ένα στάνταρ σύνολο λειτουργιών. Έτσι οι χρήστες όπως είπαμε μπορούν να χρησιμοποιήσουν το Ethereum ως πλατφόρμα για να φτίαξουν διάφορες αποκεντρωμένες εφαρμογές blockchain που μπορεί αν θέλουν να περιλαμβάνουν και κρυπτονομίσματα. Δηκαδή μπορούμε να πούμε ότι το Ethereum είναι ένα σύνολο από πρωτοκόλλα για δημιουργία αποκεντρωμένων εφαρμογών μέσω πλατφόρμας. Στον πυρήνα του συναντάμε το (EVM) στο οποίο εκτελείται ο κώδικας. Αν χρησιμοποιήσουμε επιστημονικούς όρους το Ethereum είναι "Turing complete". Οι χρήστες που το επιλέγουν μπορούν να φτιάξουν προγράμματα, εφαρμογές με γλώσσες προγραμματισμού όπως JavaScript και Python.

Το Ethereum όπως κάθε blockchain περιλαμβάνει ένα πρωτόκολλο δικτύου P2P . Όλοι οι κόμβοι που συμμετέχουν στο δίκτυο ενημερώνουν και συντηρούν τη βάση δεδομένων του blockchain.Το Ethereum πολλές φορές συναντάμε να το αναφέρουν ως «ο υπολογιστής του κόσμου» γιατί ο καθένας κόμβος του διαχειρίζεται το EVM εκτελώντας τις ίδιες εντολές. Το να εκτελούνται παράλληλα όλες αυτές οι λειτουργίες στο δίκτυο Ethereum δεν έχει σαν αποτέλεσμα πιο γρήγορους υπολογισμούς. Αντιθέτως με τον τρόπο αυτό επιδιώκεται ώστε οι υπολογισμοί που γίνονται να είναι πιο αργοί και πιο ακριβείς με στόχο τη συναίνεση στο δίκτυο . Με αυτή τη διαδικασία επιτυγχάνεται ανοχή στα σφάλματα και παρέχεται ασφάλεια και ακεραιότητα για τα δεδομένα που αποθηκεύονται στο blockchain α.

Όπως με όλες τις γλώσσες προγραμματισμού έτσι και με την πλατφόρμα Ethereum οι χρήστες είναι αυτοί που θα αποφασίσουν πως θα χρησιμοποιήσουν κάθε εφαρμογή που φτιάχνουν. Παρόλα αυτά κάποιες εφαρμογές εκμεταλλεύονται τις δυνατότητες που προσφέρει το Ethereum περισσότερο από άλλες. Για παράδειγμα η χρήση του για εφαρμογές που έχουν να κάνουν με την αλληλεπίδραση μεταξύ των κόμβων ή άλλες που έχουν να κάνουν με τη συντονισμένη δράση της ομάδας σε ένα δίκτυο. Αν και οι εφαρμογές και οι τομείς που μπορεί να χρησιμοποιηθεί το Ethereum είναι άπειρες στην πράξη οικονομικές συναλλαγές είτε αλληλεπιδράσεις μεταξύ των κόμβων του δικτύου θα μπορούσαν να πραγματοποιηθούν αυτόματα και αξιόπιστα. Επίσης η χρήση του σε άλλους τομείς όπως σε περιπτώσεις διατήρησης μητρώων περιουσιακών στοιχείων παρέχει ασφάλεια , εμπιστοσύνη και διαφάνεια.

Solidity

Έκδοση που χρησιμοποιήθηκε: ^0.8

Η Solidity είναι μία «συμβολαιοστρεφής», υψηλού επιπέδου γλώσσα προγραμματισμού που εκτελείται στο (EVM) και έχει δημιουργηθεί για να μεγεθύνει όπως δυνατότητες όπως ιδεατής όπως μηχανής. Χρησιμοποιείται κυρίως για την δημιουργία έξυπνων συμβολαίων (smart contracts) για το Ethereum blockchain. Ο πηγαίος κώδικας όπως στο Ethereum είναι γραμμένος σε Solidity. Έχει παρόμοια σύνταξη με τη γώσσα JavaScript, οπότε γίνεται εύκολα κατανοητή από έναν πολύ μεγάλο πλήθος προγραμματιστών.

Remix

Το Remix είναι μία σουίτα εργαλείων για την αλληλεπίδραση με το Ethereum blockchain. Το Remix IDE είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης, προσβάσιμο από φυλλομετρητή για την ανάπτυξη έξυπνων συμβολαίων (Solidity smart contracts), την μεταγλώττιση και κατόπιν την δημιουργία (deploy) και εκτέλεσή όπως στο Ethereum blockchain. Πιο συγκεκριμένα μέσω του Remix πραγματοποιήθηκε το deployment των συμβολαίων στο δίκτυο του Ethereum.

MetaMask

Το MetaMask είναι ένα plugin διαθέσιμο για τους φυλλομετρητές Google Chrome, Mozilla Firefox, Brave και Opera. Το MetaMask είναι στην πραγματικότητα το μέσο μέσα από το οποίο ενας browser έχει πρόσβαση στις κατανεμημένες εφαρμογές (DApps), που για να λειτουργήσουν βασίζονται στο Ethereum. Η σημαντικότερη δυνατότητα που προσφέρει το MetaMask είναι ότι δεν απαιτείται η πλήρης εκτέλεση του κόμβου Ethereum στο μηχάνημα του χρήστη σε αντίθεση με τον Mist. Περιλαμβάνει μία ασφαλή κρύπτη και δίνει τη δυνατότητα στο χρήστη να διαχειρίζεται τους Ethereum λογαριασμούς/διευθύνσεις του και να αλληλοεπιδρά με τις ιστοσελίδες, στέλνοντας είτε υπογράφοντας τις συναλλαγές και να υπογράφει δεδομένα. Σύμφωνα με τους δημιουργούς του, ο σκοπός του είναι να κάνει το Ethereum προσβάσιμο σε όσο το δυνατόν περισσότερο κόσμο

IPFS

Το IPFS είναι ένα πρωτόκολλο που χρησιμοποιεί P2P δίκτυο για αποθήκευση δεδομένων. Παρέχει ασφαλή αποθήκευση δεδομένων καθώς τα δεδομένα που αποθηκεύονται στο IPFS προστατεύονται από οποιαδήποτε αλλαγή. Χρησιμοποιεί ένα κρυπτογραφικό αναγνωριστικό που προστατεύει τα δεδομένα από αλλοίωση, καθώς κάθε προσπάθεια αλλαγής στα δεδομένα που είναι αποθηκευμένα στο IPFS θα μπορούσε να γίνει μόνο με την αλλαγή του αναγνωριστικού. Όλα τα αρχεία δεδομένων που είναι αποθηκευμένα στο IPFS περιέχουν μια τιμή κατακερματισμού που δημιουργείται κρυπτογραφικά. Είναι μοναδικό και χρησιμοποιείται για την αναγνώριση αποθηκευμένων αρχείων δεδομένων στο IPFS. Αυτή η στρατηγική ασφαλούς αποθήκευσης του πρωτοκόλλου IPFS το καθιστά μια ευνοϊκή επιλογή για την αποθήκευση κρίσιμων και ευαίσθητων δεδομένων. Ο κρυπτογραφικός κατακερματισμός που δημιουργείται θα μπορούσε να αποθηκευτεί στην αποκεντρωμένη εφαρμογή για τη μείωση των εξαντλητικών υπολογιστικών λειτουργιών στο blockchain. Το πρωτόκολλο IPFS λειτουργεί χρησιμοποιώντας ένα δίκτυο (P2P), αυτό το δίκτυο περιέχει μια δομή δεδομένων γνωστή ως αντικείμενο IPFS που περιέχει δεδομένα και σύνδεσμο σε αυτό. Τα δεδομένα είναι μη δομημένα δυαδικά δεδομένα και ο σύνδεσμος αποτελείται από έναν πίνακα. Το πρωτόκολλο IPFS λειτουργεί με τον ακόλουθο τρόπο. Στα

αρχεία που είναι αποθηκευμένα στο IPFS εκχωρείται όπως μοναδικός κρυπτογραφικός κατακερματισμός Δεν επιτρέπεται να υπάρχουν διπλότυπα αρχεία στο δίκτυο IPFS Όπως κόμβος στο δίκτυο αποθηκεύει το περιεχόμενο και όπως πληροφορίες ευρετηρίου του κόμβου.

5

Σύνοψη - Συμπεράσματα

Σύνοψη

Στην παρούσα διπλωματική εξετάστηκε ενδελεχώς η τεχνολογία blockchain και ο τρόπος με τον οποίο επηρεάζει τον κλάδο των ασφαλιστικών εταιρειών στην αποφυγή απάτης . Στο πρώτο κεφάλαιο υπάρχει το αντικείμενο της διπλωματικής και η δομη της. Στο δεύτερο κεφάλαιο εξετάστηκε η τεχνολογία blockchain και τα βασικα χαρακτηριστικά που διαθέτει , περιγράφεται η αρχιτεκτονική των Blockchains και επισημαίνονται η δομή και τα χρήσιμα στοιχεία αυτής της τεχνολογίας. Στο τρίτο κεφάλαιο παρουσιάστηκαν τρόποι εφαρμογής των blockchains σε διάφορους τομείς , με παραδείγματα εφαρμογών όπως και παραδείγματα που χρησιμοποιούνται για την ανίχνευση απάτης. Στο τέταρτο κεφάλαιο αναλύεται η απάτη στον ασφαλιστικό τομέα και περιγράφεται το σενάριο υλοποίησης που χρησιμοποιώ.

Συμπεράσματα

Η blockchain τεχνολογία έχει αρκετές δυνατότητες και προσδοκίες να είναι το νέο κύμα καινοτομίας που θα οδηγήσει και θα προωθήσει την εφαρμογή νέων επιχειρηματικών μοντέλων, αξιοποιώντας και μετατρέποντας τα ήδη υπάρχοντα συστήματα και διαδικασίες. Λόγω της αποκεντρωμένης φύσης της τεχνολογίας blockchain η εμπιστοσύνη εναποτίθεται στο ίδιο το σύστημα, χωρίς την ανάγκη παρουσίας ενδιάμεσων μερών. Η τεχνολογία blockchain χάρει στην αρχιτεκτονική που διαθέτει επιτρέπει την καταγραφή όλων των κινήσεων που γίνονται πάνω στο δίκτυο από όλους τους συμμετέχοντες. Με αυτόν τον τρόπο όλα τα δεδομένα είναι αμετάβλητα γιατί δεν υπάρχει η δυνατότητα διαγραφής τους από κανέναν. Άρα όλοι έχουν πρόσβαση στο ιστορικό κινήσεων γιατί πάντα αφήνει ένα αποτύπωμα. Οι καταχωρήσεις παρέχουν εγγύηση για τη συμμόρφωση με τους κανονισμούς, μειώνονται οι απάτες και αναγνωρίζονται πιθανά λάθη. Επιπλέον, με την ενοποίηση των άλλοτε κατακερματισμένων συστημάτων μειώνεται η

ασυμμετρία στην πληροφόρηση. Επιλέχθηκε η αποκεντρωμένη πλατφόρμα του Ethereum σε συνδυασμό ανάπτυξης έξυπνων συμβολαίων για την λειτουργία μίας αποκεντρωμένης εφαρμογής (DApp) . Αξιολογώντας τα διάφορα blockchain που υπάρχουν , κρίθηκε ότι το Ethereum είναι η πιο κατάλληλη τεχνολογία για τον σκοπό του σεναρίου μας. Αυτό διότι, είναι ένα από τα πιο διαδεδομένα blockchain, πιο συγκεκριμένα είναι δεύτερο μετά από αυτό του Bitcoin και είναι το μόνο οικοσύστημα που συνδυάζει την δημοφιλία με την δυνατότητα ανάπτυξης έξυπνων συμβολαίων. Επιπλέον στο Ethereum παρέχονται τα περισσότερα μέσα και εργαλεία για την ανάπτυξη και λειτουργία αποκεντρωμένων εφαρμογών. Το Ethereum δηλαδή επιλέχθηκε όχι μόνον λόγω των δυνατοτήτων που προσφέρει για την λειτουργία αποκεντρωμένων εφαρμογών, αλλά και λόγω της δημοφιλίας του και της υιοθέτησης της τεχνολογίας του από τους χρήστες.

Παρόλα μπορούμε να ανιχνεύσουμε κάποιες αδυναμίες σε όλο το σύστημα που παρουσιάστηκε. Καθώς διαδίδεται η χρήση της τεχνολογίας, όλο και περισσότερες εταιρείες ενσωματώνουν blockchain στις λειτουργίες τους με αποτέλεσμα ο όγκος των δεδομένων που χρησιμοποιούνται να αυξάνεται συνέχεια. Για αυτό το λόγο τα συστήματα πρέπει να είναι ικανά να αντιμετωπίσουν αυτήν την απότομη αύξηση καταχωρήσεων και πληροφοριών και να συνεχίσουν να λειτουργούν αποδοτικά ώστε να μην υπάρξει κάποιο πρόβλημα. Επίσης απαιτείται μεγάλη κατανάλωση ενέργειας. Οι αλγόριθμοι που χρησιμοποιούνται στο blockchain τις περισσότερες φορές απαιτούν μεγάλη κατανάλωση υπολογιστικής ισχύος το οποίο μεταφράζεται σε μεγάλη κατανάλωση ηλεκτρικού ρεύματος. Η τεχνολογία blockchain είναι αρκετά σοφιστικέ, καθώς χρησιμοποιεί κρυπτογραφία, μαθηματικά και πληροφορική. Μπορούμε να πούμε οτι βρίσκεται ακόμη σε πρώιμο στάδιο και έχουν δημιουργηθεί πολλοί διαφορετικοί ορισμοί που οδηγούν σε λανθασμένα συμπεράσματα. Εδώ μπορούμε να προσθέσουμε την άρνηση των υποψήφιων πελατών στον έλεγχο των στοιχείων τους (για έλεγχο ενεργής ασφάλισης στο παράδειγμα μας) με πρόσχημα την καταπάτηση προσωπικών δεδομένων. Υπάρχουν και κάποιες απειλές που οφείλονται σε εξωτερικούς παράγοντες . Ένα τέτοιο παράδειγμα είναι ότι υπάρχει η πιθανότητα η κοινή γνώμη και οι αγορές να δυσφημούν τέτοιου είδους τεχνολογίες χαρακτηρίζοντας τες ως μη ασφαλείς και αναξιόπιστες. Σημαντικές αιτίες για να υποστηριχθεί ένα τέτοιο παράδειγμα οι ανεπιθύμητες παρεμβολές στον κώδικα (bugs), η αστάθεια των ψηφιακών νομισμάτων κ.α.. Ακόμα από την πλευρά τους οι διάφορες κυβερνήσεις θα μπορούσαν να παίξουν σημαντικό ρόλο προς αυτήν την κατεύθυνση αν αποτρέπουν τον κόσμο και την ευρεία γνώμη από το να δοκιμάσουν και να χρησιμοποιήσουν τέτοια τεχνολογία υποδεικνύοντας την ως επικίνδυνη. Υπάρχει ακόμα η πιθανότητα μερικά άτομα από τις ίδιες τις ασφαλιστικές εταιρείες να σαμποτάρουν τη χρήση της νέας τεχνολογίας για τον λόγο ότι θεωρούν την παραδοσιακή τεχνολογία πιο ασφαλή και αξιόπιστη από αυτή. Αυτό έχει σαν αποτέλεσμα το ποσοστό των χρηστών της τεχνολογίας blockchain να παραμένει χαμηλό άρα θα παρουσιαστεί πρόβλημα στην υιοθέτηση της από τον κόσμο. Επιπλέον το κόστος ενσωμάτωσης τεχνολογιών blockchain και η αντικατάσταση και ψηφιοποίηση των υπαρχόντων συστημάτων είναι χρονοβόρες, περίπλοκες και ακριβές διαδικασίες. Οι κύριοι παίκτες στο χώρο συμμετέχουν σε κοινοπραξίες-συνεργασίες ώστε να μειώσουν το ρίσκο και το κόστος.

Συνολικά, καταδεικνύεται ότι η εφαρμογή της τεχνολογίας blockchain έχει ιδιαίτερη αξία. Αυτό φαίνεται και από το συνεχώς αυξανόμενο ερευνητικό ενδιαφέρον γύρω από το blockchain, σε τομείς όπου παραδοσιακά δεν είχε εφαρμογή. Συμπερασματικά, το blockchain είναι πολλά περισσότερα από ένα απλό υπολογιστικό σύστημα, καθώς παρέχει νέες δυνατότητες, επεκτείνει την ελευθερία και επιτρέπει στον άνθρωπο να εισέλθει σε μία νέα, «έξυπνη» οικονομία. Η τεχνολογία υπάρχει, απλά πρέπει να προσδιοριστεί η σωστή διαχείρισή της.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

[1] A. J. Mount, "Bitcoin's status isn't as simple as ruling if it is more a private token or a public ledger," *Win-Vector Blog*, 07-Nov-2015. [Online]. Available: http://www.win-vector.com/blog/2015/11/bitcoins-status-isnt-as-simple-as-ruling-if-it-is-more-a-private-token-or-a-public-ledger/. [Accessed: 22-Oct-2019].

[2] Patil, Kadam, and Katti, 'Security Enhancement of Forensic Evidences Using Blockchain'.

[3] Nuzzolese, 'Electronic Health Record and Blockchain Architecture: Forensic Chain Hypothesis for Human Identification'.

[4] Hyperledger, (2020) *'Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric'*

[5] IBM, (2018) *'Improving Global Trade with Blockchain: Benefits Across the Supply Chain'*

[6] IBM, (2017) *'Walmart, JD.com, IBM and Tsinghua University Launch a Blockchain Food Safety Alliance in China'*

[7] Harisson, A. και Van Hoen, R. (2013) *'Logistics: Μάνατζμεντ και στρατηγική',* Rosili

[8] Haber, S. and Stornetta, W.S. (1991) '*How to time-stamp a digital document*'. Journal of Cryptology

[9] Lewis, A. (2016) '*Understanding Blockchain Technology and What It Means for Business'.* DBS Asian Insights

[10] Beyer, S. (2018) *'Blockchain Before Bitcoin: A History*

[11] Bashir, I. (2017), Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained, Birmingham UK: Packt Publishing Ltd.

[12] Buterin, V. (2014), Ethereum White Paper: A next generation smart contract & decentralized application platform.

[13] Castor, A. (2017), A Short Guide to Blockchain Consensus Protocols

[14] Deloitte (2017), Are token assets the securities of tomorrow?

[15] Laurence, T. (2017), Blockchain For Dummies, New Jersey: John Wiley & Sons.

[16] Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic cash system paper

[17] Swan, M. (2015), A blueprint for a new economy [First Edition], O'Reilly Media

[18] Szabo, N. (1996), The Idea of Smart Contracts.

[19] Szabo, N. (1997), The God Protocols.

[20] https://www.developcoins.com/blockchain-consensus-algorithms

[21] Patil, Kadam, and Katti, 'Security Enhancement of Forensic Evidences Using Blockchain'.

[22] Nuzzolese, 'Electronic Health Record and Blockchain Architecture: Forensic Chain Hypothesis for Human Identification'.

[23] Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | TIM Review.

[24] Mettler M. (2016), Blockchain technology in healthcare: the revolution starts here. IEEE 18th International Conference on e-Health Networking, September 14–16, 2016. Piscataway, NJ: IEEE. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749510 . Accessed March 3, 2017. In: Suveen Angraal, MBBS; Harlan M. Krumholz, MD, SM; Wade L. Schulz, MD, PhD (2017) Guardtime secures over a million Estonian healthcare records on the blockchain. http://www.ibtimes.co.uk/guardtime-secures-over-million estonian-healthcare-records-blockchain1547367 Accessed 25 Jan 2017. In: Mehdi Benchoufi and Philippe Ravaud (2017), Blockchain technology for improving clinical research quality : DOI 10.1186/s13063-017-2035-z

[25] https://www.healthbank.coop/

[26] https://patientory.com/

[27] https://isolve.io/

[28] M. Hahnel, Blockchain Enabled Genome Security From the Moment It Is Sequenced, Retrieved from: https://www.genomes.io/wp-content/uploads/2018/03/The-genomes.io-Whitepaper-V-1.1.4.pdf, 2018. Accessed 14 June 2018

[29] G. Jones, Universal Health Coin (UHC), Retrieved from: https://www.universalhealthcoin.com/, 2017. Accessed 14 June 2018.

[30] https://modum.io/

[31] https://enterprise.gem.co/health/ [35] T.T. Kuo, L. Ohno-Machado, ModelChain (2018): Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks, 2018. arXiv preprint arXiv:1802.01746. In: Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong

Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare-challenges and solutions # 2019 Elsevier Inc. All rights reserved.

[32] https://pokitdok.com/

[33] Burst IQ, Retrieved from: https://www.burstiq.com/, 2015. Accessed 14 June 2018.

[34] https://medicalchain.com/en/

[35] Healthcombix, Retrieved from:https://healthcombix.com/, 2016. Accessed 14 June 2018.

[36] B. Smith, DokChain, Retrieved from:https://pokitdok.com/dokchain/, 2016. Accessed 14 June 2018.

[37] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, Hee-Cheol Kim (2019), Big Data Analytics for Intelligent Healthcare Management, chapter 8 : blockchain in healthcare -challenges and solutions # 2019 Elsevier Inc. All rights reserved.

[38] Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | TIM Review.

[39] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthc. Basel Switz.*, vol. 7, no. 2, Apr. 2019, doi: 10.3390/healthcare7020056.

[40] "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector | TIM Review." [Online]. Available: https://timreview.ca/article/1111. [Accessed: 13-Nov-2019].

[41] "Blockchain distributed ledger technologies for biomedical and health care applications | Journal of the American Medical Informatics Association | Oxford Academic." [Online]. Available: https://academic.oup.com/jamia/article/24/6/1211/4108087. [Accessed: 13 - Nov-2019].

[42] "Patients and Privacy: GDPR Compliance for Healthcare Organizations - Security News - Trend Micro DK." .
[43] "Blockchain Technology | Circulation: Cardiovascular Quality and Outcomes." [Online]. Available: https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.117.003800. [Accessed: 13-Nov-2019]

[44] https://www.techtimes.com/articles/257804/20210308/how-to-get-started-with-smart-contract-development.html

[45] https://bitsonblocks.net/2015/09/28/gentle-introduction-digital-tokens

[46] https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868

[47] https://asfalistikomarketing.gr

[48] Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations, Mohammad Kamrul Hasan et al

[49] Identifying Food Fraud using Blockchain, Hoi Wen Leung, Adriane Chapman a and Nawfal F. Fadhel b School of Electronics and Computer Science, University of Southampton, Southampton, U.K.

[50] My Health My Data," *My Health My Data*. [Online]. Available: http://www.myhealthmydata.eu/. [Accessed: 17-Nov-2019].