ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ ΕΞΥΠΝΕΣ ΣΥΜΒΑΣΕΙΣ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ – ΟΦΕΛΗ ΚΑΙ ΝΟΜΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ

Διπλωματική Εργασία

της

Σαρμπάνη Χρυσούλας

Θεσσαλονίκη, μμ/εεεε

ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΚΑΙ ΕΞΥΠΝΕΣ ΣΥΜΒΑΣΕΙΣ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ – ΟΦΕΛΗ ΚΑΙ ΝΟΜΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ

Σαρμπάνη Χρυσούλα

Πτυχίο Νομικής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2017
Πτυχίο Διοίκησης και Οικονομίας, Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Ηπείρου, 2003

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Φουληράς Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
.....	.....	.....

Σαρμπάνη Χρυσούλα

Περίληψη

Ο ανασχεδιασμός των δομικών και οργανωτικών δομών του Κράτους και των διαδικασιών του έχει ήδη ξεκινήσει, με τη βοήθεια των νέων τεχνολογιών. Μία από αυτές φιλοδοξεί να γίνει και η τεχνολογία Blockchain, η οποία βασίζεται στην θεωρία των δικτύων σε σχέση με το διαδίκτυο και αναπτύχθηκε για να παρακάμψει τους καθιερωμένους θεσμούς. Οι υποδειγματικές υλοποιήσεις εφαρμογών Blockchain σε διάφορους τομείς της οικονομίας από άλλες Ευρωπαϊκές Χώρες ή μη, αποτελούν τα πιο χαρακτηριστικά παραδείγματα. Το ανταγωνιστικό πλεονέκτημα της τεχνολογίας blockchain έγκειται στον τρόπο λειτουργίας της, καθώς συνήθως αναφέρεται ως μια αλυσίδα κοινοποιήσεων μέσα σε ένα δημόσιο δίκτυο όπου όλα τα μέλη του δικτύου έχουν ταυτόχρονα την ίδια πληροφορία η οποία είναι αδύνατο να τροποποιηθεί. Κάθε νέα συναλλαγή στο δίκτυο προστίθεται στην υπάρχουσα αλυσίδα συναλλαγών, ασφαλής από παρεμβάσεις, αφού πρώτα έχει γίνει αλγοριθμική επιβεβαίωση, για την ορθότητα της. Η αρχιτεκτονική της μορφή και τα ιδιαίτερα δομικά της στοιχεία την καθιστούν άκρως πρωτοποριακή. Παράλληλα όμως οι νέες τεχνολογίες δοκιμάζουν τα νομικά συστήματα, καθώς στην ουσία πρόκειται για περίπλοκες νομικές συμβάσεις ή ανεξάρτητα λογιστικά βιβλία σε μερικές γραμμές λογισμικού. Καθώς όλο και περισσότεροι συμβατικοί κανόνες και νομικές διατάξεις ενσωματώνονται στον έξυπνο κώδικα σύμβασης για να λειτουργήσει μια πλατφόρμα blockchain, η παραδοσιακή αντίληψη του νόμου μπορεί να χρειαστεί να εξελιχθεί σε κάτι που μπορεί να εξομοιωθεί με κώδικα.

Μελετώντας και άλλους τύπους εφαρμογών blockchain που συναντώνται στο οικοσύστημα των Τεχνολογιών Κατανεμημένου Μητρώου, καθώς και ένα επαρκές εύρος αντιπροσωπευτικών και διαδεδομένων εφαρμογών Blockchain, αναζητούνται οι αιτίες και οι προϋποθέσεις για να προτείνουμε μία λύση Blockchain στη Δημόσια Διοίκηση. Πεδία που χρήζουν ιδιαίτερης προσοχής είναι κυρίως νομικά σε διάφορα επίπεδα δικαίου με ειδική μνεία στον GDPR, καθώς και μια γενική ηθική προσέγγιση των πραγμάτων, ενώ πολύ σημαντική είναι η ασφάλεια των κυβερνητικών εγγράφων και πληροφοριών καθώς και η δημιουργία και κατοχύρωση συνθηκών ανοικτής και διαφανούς δημόσιας διοίκησης. Το έργο Hyperledger είναι μια από τις δημοφιλέστερες υποδομές blockchain το οποίο συνδέει της έξυπνη σύμβαση και την εξουσιοδοτούμενη αρχή. Παρουσιάζεται η δημιουργία ενός υβριδικού Hyperledger δικτύου στον Δημόσιο τομέα, με την υλοποίηση ενός σεναρίου μιας διαγωνιστικής διαδικασίας προμηθειών. Τέλος, γίνεται μια γενικότερη ανασκόπηση των συμπερασμάτων της παρούσας εργασίας και παρουσιάζονται οι προοπτικές επέκτασης της.

Λέξεις Κλειδιά:

Τεχνολογία blockchain, έξυπνες συμβάσεις Hyperledger Fabric, Ηλεκτρονική Διακυβέρνηση, Δημόσια Διοίκηση

Abstract

The redesign of the structural and organizational structures of the State and its processes has already begun, with the help of new technologies. Blockchain technology, which is based on the theory of networks in relation to the Internet and was developed to bypass the established institutions, aspires to become one of them. The exemplary implementations of Blockchain applications in various sectors of the economy from other European countries or not, are the most typical examples. The competitive advantage of blockchain technology lies in the way it works, as it is usually referred to as a notification chain within a public network where all members of the network have the same information at the same time which is impossible to modify. Each new transaction in the network is added to the existing chain of transactions, safe from interventions, after first algorithmic confirmation has been made, for its correctness. Its architectural form and its special structural elements make it extremely innovative. At the same time, however, new technologies are testing legal systems, as they are essentially complex legal contracts or independent accounting books on a few lines of software. As more and more contractual rules and regulations are incorporated into smart contract code to make a blockchain platform work, the traditional notion of law may need to evolve into something that can be embedded in code.

By studying other types of blockchain applications found in the Distributed Registry Technology ecosystem, as well as a sufficient range of representative and widespread Blockchain applications, the causes and conditions for proposing a Blockchain solution to Public Administration are sought. Areas that need special attention are mainly legal at various levels of law with special reference to the GDPR, as well as a general ethical approach, while the security of government documents and information as well as the creation and establishment of open and transparent public administration are very important. The Hyperledger project is one of the most popular blockchain infrastructures which connects the smart contract and the authorized authority. The creation of a hybrid Hyperledger network in the Public Sector is presented, with the implementation of a scenario of a competitive procurement process. Finally, a more general review of the conclusions of the present work is made and the prospects for its extension are presented.

Keywords:

Blockchain technology, smart contracts, Hyperledger Fabric, e-Government, Public Administration

Ευχαριστίες

Με την ευκαιρία της ολοκλήρωσης της διπλωματικής μου εργασίας, αρχικά και πάνω απ' όλα, θα ήθελα να εκφράσω τις πιο θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου, κ. Φουληρά Παναγιώτη, Επίκουρο Καθηγητή του Πανεπιστημίου Μακεδονίας, ο οποίος από την πρώτη στιγμή έδειξε εμπιστοσύνη στο πρόσωπό μου και στάθηκε δίπλα μου, ως συμπαραστάτης σε αυτή μου την προσπάθεια με κατανόηση, ευγένεια και υπομονή, καθ' όλη τη διάρκεια της συνεργασίας μας.

Θέλω, επίσης, να ευχαριστήσω την οικογένειά μου για την αμερόληπτη υποστήριξη της κατά την εκπόνηση της εργασίας μου, όσο και σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Τέλος, οφείλω ένα μεγάλο ευχαριστώ σε όλους τους συνοδοιπόρους του τμήματος του ΔΠΜΣ, καθώς με την ιδιαίτερη παρουσία τους, ο καθένας τους ξεχωριστά, με γέμισαν με αισιοδοξία, θυμίζοντας μου για μία ακόμη φορά, πως μαζί με τη συναρπαστική εμπειρία της γνώσης, μπορούν ακόμα και στις μέρες μας, να «χτιστούν» ισχυροί και ουσιαστικοί δεσμοί.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συμβολισμοί

AI	Artificial Intelligence
API	Automatic Programming Interface
BC	Blockchain
BTF	Byzantine Fault Tolerance
Cisco	Computer Information System Company
CNIL	Commission Nationale de l' Informatique et des Libertes
CPV	Common Procurement Vocabulary
DAG	Directed Acrylic Graph
DC	Data Contract
DESI	Digital Economy and Society Index
DFS	Digital Future Society
DHT	Distributed Hash Tables
DLT	Distributed Ledger Technology
DSL	Domain Specific Language
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
gRPC	google Remote Procedure Call
IBM	International Business Machines Corporation
IoT	Internet of Things
IP	Internet Protocol Address
P2P	Peer to Peer
PC	Register Contract
PoW	Proof of Work
RC	Register Contract
RIAA	Recording Industry Accosiation of America
SAP	System Anwendungen Produkte in der Datenverarbeitung
SMEs	Small and Medium - sized Enterprises
SWOT	Strengths – Weaknesses - Opportunities & Threats Analysis
TOKEN	Transformative Impact of Blockchain Public Technologies in Public Services
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΕ	Ευρωπαϊκή Ένωση

ΕΚΕΤΑ	Εθνικό Κέντρο Έρευνας και Τεχνολογίας Ανάπτυξης
ΗΔ	Ηλεκτρονική Διακυβέρνηση
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
Intel	Intergrated Electronics Corporation
ΙΠΤΗΛ	Ινστιτούτο Τεχνολογιών Πληροφορικής και Επικοινωνιών
ΚΠολΔ	Κώδικας Πολιτικής Δικονομίας
ΝΠΔΔ	Νομικό Πρόσωπο Δημοσίου Δικαίου
ΝΠΙΔ	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
ΤΚΚ	Τεχνολογία Κατανεμημένου Καθολικού

Κεφάλαιο 1ο

Εισαγωγή

Τα τεχνολογικά επιτεύγματα των τελευταίων ετών είναι άκρως υπερβατικά και έχουν μεταβάλλει σε μεγάλο βαθμό την καθημερινότητά μας. Η πιο πρόσφατη τάση στις νέες τεχνολογίες είναι η αυτόματη εκτέλεση συναλλαγών χωρίς την παρέμβαση του ανθρώπινου παράγοντα, καθώς το λογισμικό βάσει αλγοριθμικών υπολογισμών, αναλαμβάνει την επαλήθευση της ανταλλαγής δεδομένων σε επίπεδο υποβολής και εγκυρότητας, επιτρέποντας παράλληλα την συνεχόμενη και απρόσκοπτη ροή των διεργασιών. Το νέο δικτυακό λογισμικό βασίζεται στην αρχιτεκτονική φιλοσοφία των ομότιμων κόμβων και όχι του πελάτη – διακομιστή, καθιστώντας τις αποκεντρωμένες εφαρμογές ως την πλέον επαναστατική δομή του διαδικτύου διότι τα οφέλη σε κόστος, ασφάλεια, ταχύτητα και διαφάνεια μοιάζει να αποδίδουν στον μέγιστο δυνατό βαθμό. Το πιο σημαντικό όμως λειτουργικό χαρακτηριστικό τους είναι τα έξυπνα συμβόλαια, τα οποία περιέχουν τον κώδικα εκτέλεσής τους. Το αν αξίζει να δοκιμασθεί από τις επιχειρήσεις και κυρίως από Δημόσιους Φορείς είναι κάτι που θα διαπιστώσουμε στη συνέχεια. Επιδιωκόμενος στόχος της παρούσας διπλωματικής εργασίας είναι να παρουσιασθούν οι βασικές διαστάσεις της τεχνολογίας αποκεντρωμένων εφαρμογών - Blockchain και των έξυπνων συμβάσεων, καθώς και να προσδιορίσει περιγραμματικά, πως θα μπορούσε να αξιοποιηθεί στον χώρο της Δημόσιας Διοίκησης. Η τεχνολογία Blockchain θα μπορούσε δυνητικά να αποτελέσει μία παγκόσμια αποκεντρωμένη πηγή εμπιστοσύνης, προσφέροντας αξιοπιστία και πληροφοριακή ακεραιότητα;

Από νομική σκοπιά, η συνοχή με τους νομοθετικούς κανόνες είναι καθοριστικής σημασίας, ενώ είναι δύσκολη η μεταφορά της λογικής των αποκεντρωμένων κρυπτογραφημένων ψηφιακών καθολικών των συναλλαγών, σε ένα κανονιστικό πλαίσιο. Είναι μια τεχνολογία που ανταγωνίζεται τον ρόλο της Κυβέρνησης στην Κοινωνία και θα πρέπει απαραιτήτως να συνδυάζεται με θεσμική ενσωμάτωση.

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η προσέγγιση της ηλεκτρονικής διακυβέρνησης ήταν πάντοτε ιδιαίτερα εσωστρεφής, ενώ τα τελευταία χρόνια παρουσιάζει σημαντική πρόοδο. Το βασικό όμως πρόβλημα που διαπραγματευόμαστε εντοπίζεται κυρίως στις παθογένειες του δημόσιου τομέα στην Χώρα μας, καθώς παρατηρείται εδώ και χρόνια μια αναξιοποίητη χρήση του πλούτου της πληροφορίας, την οποία συνεχίζουν να συγκεντρώνουν τα επιμέρους πληροφοριακά συστήματα των Φορέων της και οφείλεται κυρίως στην έλλειψη ολοκληρωτικής διασύνδεσης των συστημάτων της. Παρόλα αυτά καθοριστικής σημασίας παράγοντας αποδείχθηκε η υιοθέτηση νέων εφαρμογών για τη διαχείριση της πληροφορίας, η οποία πραγματοποιείται πλέον με τη χρήση ανοικτών προτύπων, γεγονός το οποίο σταδιακά κατέστη ως μια προ απαιτούμενη υποχρέωση για τους Κρατικούς Φορείς.

Στα πλαίσια της παρούσας μελέτης, προσπαθήσαμε να αναδείξουμε τη σημαντικότητα μιας θεσμικής θωράκισης για την υποχρεωτική χρήση αναδυόμενων τεχνολογιών, καθώς κάτι τέτοιο θα συνέβαλε τα μέγιστα στο Κράτος, τους πολίτες και τις συνεργαζόμενες επιχειρήσεις.

Η τεχνολογία blockchain και τα έξυπνα συμβόλαια, μπορούν δυνητικά να επιφέρουν πολλαπλά επιθυμητά αποτελέσματα στο Δημόσιο εάν και εφόσον επιλεγούν από την Κυβέρνηση, να αποτελέσουν τις πλέον ιδανικές εφαρμογές για τις υπηρεσίες, στα πλαίσια της διεκπεραίωσης των αρμοδιοτήτων τους. Θα μπορούσε να εξαλειφθεί το κόστος των υφιστάμενων διαδικασιών με την απαλλαγή τήρησης αρχείων και αντιπαραβολής στοιχείων. Η τεχνολογία blockchain διαθέτει εκείνη τη δυναμική που απαιτείται για να επαναπροσδιορίσει τη σχέση μεταξύ Κυβέρνησης και πολιτών, προωθώντας τη διαφάνεια των διαδικασιών, την εμπιστοσύνη και την αξιοπιστία.

1.2 Σκοπός – Στόχοι

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του ΔΠΜΣ «Δίκαιο και Πληροφορική» και έχει ως σκοπό την γενικότερη παρουσίαση της τεχνολογίας του blockchain και των έξυπνων συμβάσεων, ως μεθόδου αποθήκευσης, κρυπτογράφησης και διαμοιρασμού δεδομένων. Το αντικείμενο της διπλωματικής είναι να επεξηγήσει τις βασικές λειτουργίες, τη λογική, να αναλύσει την αρχιτεκτονική και τα δομικά στοιχεία των πλατφορμών blockchain και να παρουσιάσει τον τρόπο με τον οποίο θα μπορούσε να χρησιμοποιηθεί σε Φορείς του Δημοσίου. Στα πλαίσια καταπολέμησης της διαφθοράς και εξασφάλισης της διαφάνειας των διαδικασιών, εντοπίζονται οι νομικές προκλήσεις που θα επιφέρει και τις οποίες καλούμαστε να αντιμετωπίσουμε αλλά και τα οφέλη της.

Το Blockchain είναι μια τεχνολογία θεσμικής διακυβέρνησης, που λειτουργεί ως υποδομή για έξυπνες πλατφόρμες συμβάσεων. Τα έξυπνα συμβόλαια είναι συμφωνίες που κωδικοποιούνται για να λειτουργήσουν σε ένα αποκεντρωμένο ή κατανεμημένο δίκτυο blockchain και εκτελούνται σε αυτό το δίκτυο, όταν επικυρώνονται συγκεκριμένες προϋποθέσεις. Στόχος της εργασίας μας είναι να ερευνήσουμε κατά πόσο μπορούν οι έξυπνες συμβάσεις να αποτελέσουν ξεχωριστά νομικά εργαλεία ή είναι απλά ψηφιακές εναλλακτικές λύσεις έναντι των παραδοσιακών νομικών συμβάσεων.

Ο κύριος στόχος της μελέτης είναι να εντοπίσει τα ερευνητικά θέματα που έχουν διεξαχθεί σχετικά με έξυπνα συμβόλαια που βασίζονται σε blockchain και να αναλύσει τις τρέχουσες νομικές προκλήσεις, που πρέπει να αντιμετωπιστούν σε μελλοντικές έρευνες.

Ο σκοπός της εργασίας είναι η δημιουργία ενός υβριδικού μοντέλου blockchain στην ιδανική κατά την γνώμη μας εφαρμογή δικτύου – Hyperledger Fabric - και η ανάπτυξη ενός σεναρίου χρήσης της, ως μιας αποκεντρωμένης εφαρμογής διακυβέρνησης στον Δημόσιο τομέα. Στόχος μας είναι η ανάλυση της λειτουργίας του για την διαπίστωση ή μη, της ταχύτερης πραγματοποίηση των συναλλαγών, χωρίς ενδιάμεσους, που θα ωφελήσει ταυτόχρονα όλους τους συμμετέχοντες του δικτύου.

1.3 Συνεισφορά

Η συνεισφορά αυτής της διπλωματικής εργασίας συνίσταται στα παρακάτω:

1. Στην παρουσίαση της τεχνολογίας blockchain και των έξυπνων συμβολαίων σε ένα ακαδημαϊκό πλαίσιο.
2. Στην επεξήγηση των λόγων που θα καθιστούσε την τεχνολογία αυτή αρωγό στην επιτάχυνση των διαδικασιών στον δημόσιο τομέα, με την ανάπτυξη έξυπνων σεναρίων
3. Στην αιτιολόγηση της χρησιμότητάς της, όταν και εφόσον υπάρξει θεσμοθετημένη από την Πολιτεία προοπτική για την ευρύτερη χρήση της.

1.4 Διάρθρωση της μελέτης

Η έρευνά μας συνδυάζει επιστημονικά δεδομένα δικαίου, οικονομίας και πληροφορικής. Στο παρόν κεφάλαιο παρουσιάζεται το αντικείμενο και ο σκοπός της εργασίας, ο προβληματισμός που πραγματεύεται, ο στόχος της καθώς και η διάρθρωσή της σε κεφάλαια. Η δομή της διπλωματικής εργασίας αποτελείται από το πρώτο μέρος της που είναι η εισαγωγή και αναφέρεται στο αντικείμενο της διπλωματικής εργασίας και απαρτίζεται από δέκα κεφάλαια. Στο δεύτερο μέρος πραγματοποιείται μια σύντομη επισκόπηση του τεχνολογικού περιβάλλοντος και της αρχιτεκτονικής δομής της τεχνολογίας blockchain. Αναπτύσσονται θεωρητικές έννοιες πληροφορικής και ασφάλειας επί των οποίων εδράζεται συνολικά η τεχνολογία blockchain με τρόπο κατανοητό, μετά από την συστηματική ομαδοποίηση βάσει ιδιοκτησίας του δικτύου, εκχώρησης δικαιωμάτων εγγραφής σε αυτό και χρησιμοποιούμενων μηχανισμών επίτευξης συναίνεσης. Στο τρίτο μέρος παρουσιάζονται οι δημοφιλέστερες πλατφόρμες ανάπτυξης εφαρμογών βασισμένων σε blockchain, απαριθμούνται τα κοινά χαρακτηριστικά τους, καθώς τα πλεονεκτήματα και μειονεκτήματά τους, ενώ παραθέτουμε κάποιες από τις πιο διαδεδομένες εφαρμογές τεχνολογίας blockchain. Στο τέταρτο μέρος σκιαγραφούμε τη φύση των έξυπνων συμβάσεων, δίνοντας την πρώτη νομική προσέγγιση και το πώς θα μπορούσαν να δημιουργηθούν και να λειτουργήσουν στον δημόσιο τομέα. Ενώ στη συνέχεια αναλύουμε και συγκρίνουμε τα έξυπνα συμβόλαια με τις συμβάσεις Ricardian, εντοπίζοντας βασικές ομοιότητες και κάποιες ουσιαστικές διαφορές τους. Στο πέμπτο μέρος προσπαθούμε να συσχετίσουμε τεχνικούς με νομικούς όρους, ως αυτοί εντοπίζονται για την λειτουργία πλατφορμών τεχνολογίας blockchain. Στη συνέχεια αναλύουμε την έννοια της εμπιστοσύνης στο blockchain σε επίπεδο

αντιπροσωπευτικότητας και επεξηγούμε την ανατροπή που εμφιλοχωρεί στο να μετατραπεί ο νόμος σε κώδικα. Στο έκτο κεφάλαιο παρουσιάζεται η στάση της Ευρωπαϊκής Ένωσης σχετικά με τις τεχνολογίες κατανεμημένων εφαρμογών και την τεχνολογία blockchain, ενώ συνοψίζονται οι προτεραιότητες του σχεδίου δράσης της και οι χρηματοδοτούμενοι τομείς της οικονομίας για τον σκοπό αυτό. Ακολουθούν παραδείγματα εφαρμογών διεθνώς στον ιδιωτικό και στον δημόσιο τομέα. Στη συνέχεια εξετάζουμε την ψηφιακή ωριμότητα του Δημόσιου τομέα σε σχέση με τις τεχνολογίες αιχμής και το κατά πόσο το blockchain θα συνέβαλε στο να δημιουργήσουμε ένα έξυπνο Κράτος. Εξετάζεται η συνεισφορά του blockchain στην καταπολέμηση της διαφθοράς και αναλύεται το παράδειγμα της Βόρειας Ελλάδας και της Κύπρου, οι οποίες έχουν επιλέξει να υιοθετήσουν αυτή την τεχνολογία στις υπηρεσίες τους. Στο έβδομο κεφάλαιο περιγράφουμε τη μετάβαση από ένα κεντρικοποιημένο μητρώο σε ένα διαμοιρασμένο μητρώο και συγκρίνουμε τα χαρακτηριστικά των δημοφιλέστερων πλατφορμών blockchain. Σχεδιάζουμε διάγραμμα ροής διαπραγματευόμενοι την ανάγκη να υιοθετηθεί η τεχνολογία blockchain ή όχι βάσει συγκεκριμένων κριτηρίων, ενώ παραθέτουμε μια ανάλυση SWOT για πλατφόρμα Hyperledger, εντοπίζοντας ταυτόχρονα τα σημεία υπεροχής του. Στο όγδοο κεφάλαιο αναλύουμε το προτεινόμενο σενάριο εφαρμογής τεχνολογίας blockchain στον Δημόσιο τομέα με τη δημιουργία ενός δικτύου Hyperledger Fabric, αφού πρώτα επαληθεύουμε ότι το βασικό εννοιολογικό του μοντέλο σχεδιασμού του, τα δομικά στοιχεία του καθώς και αιτιολογήσουμε γιατί μας εξυπηρετεί μια permissioned - υβριδική μορφή του. Περιγράφουμε την ροή των συναλλαγών του σε σχέση με τα smart contracts που το υλοποιούν, ενώ στη συνέχεια αναφερόμαστε την πολυπλοκότητα της σύναψης δημόσιας σύμβασης προμηθειών στο Δημόσιο, εξηγώντας τα βήματα της διαδικασίας. Παρατηρούμε στην πράξη το σενάριο βήμα - βήμα, ενώ περιγράφουμε τη διενέργεια μιας Ανοικτής Διαγωνιστικής διαδικασίας, μέσω του Hyperledger Fabric δικτύου. Στο ένατο κεφάλαιο εντοπίζουμε όλα τα εμπόδια και τις νομικές προκλήσεις που καλούμαστε να αντιμετωπίζουμε σε διάφορα πεδία δικαίου. Εξετάζεται η συμβατότητα της τεχνολογίας blockchain με τον GDPR, ζητήματα συμμόρφωσης με τον εν λόγω Κανονισμό ενώ προβάλλουμε και τους ηθικούς προβληματισμούς μας. Στο δέκατο κεφάλαιο προβλέπουμε την μελλοντική εξέλιξη της τεχνολογίας και παρουσιάζεται μια εναλλακτική αρχιτεκτονική, αυτή των Κατευθυνόμενων Άκυκλων Γράφων (Directed Acyclic Graphs), η οποία θεωρητικά μπορεί να βελτιώσει την τωρινή μορφή του blockchain, Ολοκληρώνουμε την εργασία μας με μια σύνοψη και τα συμπεράσματά μας, όπου παρατίθενται και ορισμένες άλλες καινοτόμες εφαρμογές, ως προτάσεις για μελλοντική μελέτη. Στο τέλος της διπλωματικής εργασίας καταγράφεται αναλυτικά η βιβλιογραφία που χρησιμοποιήθηκε.

1.5 Μεθοδολογία – Βιβλιογραφική επισκόπηση

Η μεθοδολογία της παρούσας εργασίας στηρίχθηκε κυρίως στην βιβλιογραφική ανασκόπηση δημοσιεύσεων από διαφορετικές επιστημονικές βάσεις δεδομένων. Μέσα από συστηματική χαρτογράφηση ερευνητικών τομέων που σχετίζονται τόσο με τα έξυπνα συμβόλαια όσο και με την τεχνολογία blockchain, επιλέχθηκαν οι λέξεις κλειδιά για πιο στοχευμένη αναζήτηση. Κυρίως έχουν

συμπεριληφθεί άρθρα τα οποία έχουν δημοσιευθεί σε συνέδρια, επιστημονικά περιοδικά και βιβλία. Εξαιρέθηκαν όσα έγγραφα δεν είχαν σχέση με τη μελέτη μας βάσει των τίτλων τους, διαβάζοντας σε δεύτερο χρόνο την περίληψή τους, καθώς και τα έγγραφα χωρίς πλήρες κείμενο αλλά και διαδικτυακά άρθρα αμφιβόλου αξιοπιστίας. Συλλέχθηκαν οι απαιτούμενες πληροφορίες προκειμένου να καταφέρουμε να τεκμηριώσουμε τα ερευνητικά μας ερωτήματα. Στη συνέχεια κωδικοποιήθηκαν τα ζητήματα που σχετίζονται με τις προκλήσεις από την ανάπτυξη των έξυπνων συμβολαίων στον δημόσιο τομέα και αναζητήθηκαν πιθανές απαντήσεις σε πρακτικά και δογματικά ζητήματα που θέσαμε. Διαπιστώσαμε ότι είναι εξαιρετικά περιορισμένη η διάθεση των πηγών σχετικά με τον συσχετισμό των έξυπνων συμβάσεων και την εφαρμογή τους στον Δημόσιο Τομέα.

Κεφάλαιο 2ο - Ιστορική αναδρομή και Θεωρητική τεκμηρίωση

❖ Η περίπτωση του Napster

Ο διαμοιρασμός αρχείων υπήρξε μια πρωτοποριακή ανακάλυψη, η οποία δημιούργησε επανάσταση το 1999, κυρίως όταν εμφανίστηκε το πρώτο P2P[1] δίκτυο, το Napster, με τον νεαρό δημιουργό του Shawn Fanning, να διαπρέπει. Χρήστες από όλο τον κόσμο είχαν τη δυνατότητα να αναζητήσουν και να αποθηκεύσουν τραγούδια, σε μορφή MP3 από υπολογιστές άλλων χρηστών της ίδιας υπηρεσίας. Οι χρήστες πολλαπλασιάστηκαν ραγδαία μέσα σε λίγους μόλις μήνες και ο τρόπος επικοινωνίας σε εφαρμογές πολυμέσων πήρε άλλη μορφή. Για την αναζήτηση των αρχείων αυτών υπήρχε ένας κεντρικός Server, όπου ήταν καταγεγραμμένοι οι τίτλοι των, προς διαμοιρασμό, τραγουδιών μαζί με τις ηλεκτρονικές διευθύνσεις των χρηστών αυτών. Με την σύνδεση ενός χρήστη στο συγκεκριμένο δίκτυο, το πρόγραμμα που είχε εγκαταστημένο στον υπολογιστή του, ενημέρωνε τον Server για τα τραγούδια που διατηρούσε ο χρήστης. Το ίδιο συνέβαινε και στην περίπτωση που κάποιος χρήστης αποχωρούσε από το δίκτυο. Τα ζητούμενα αρχεία μπορούσαν να ανακτηθούν μέσω της μηχανής αναζήτησης, που διατηρούσε ο Server για τους χρήστες. Η επικοινωνία όμως μεταξύ των χρηστών, προκειμένου να ξεκινήσει η αντιγραφή του αρχείου, επιτυγχάνονταν από το πρόγραμμα εγκατάστασης.

Εικόνα 1: Χρονοδιάγραμμα εμφάνισης σημαντικών τεχνολογιών αποκέντρωσης

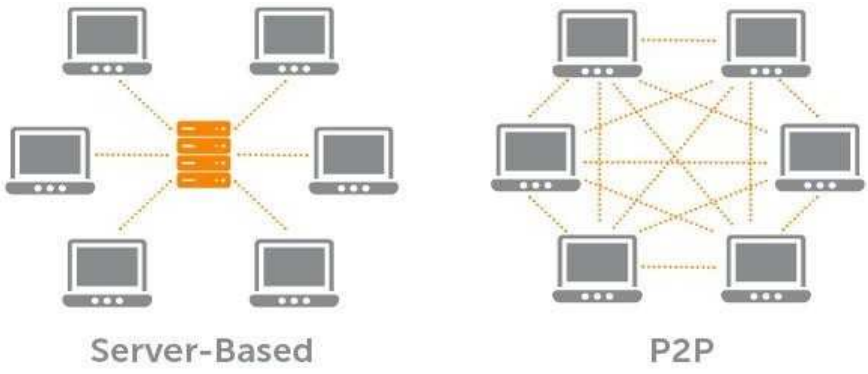
Το δημοφιλές Napster καταργήθηκε σχετικά νωρίς (Ιούλιος 2001), διότι πολλές δισκογραφικές εταιρείες, καλλιτέχνες αλλά κυρίως η Ένωση της Δισκογραφικής Βιομηχανίας της Αμερικής (RIAA), διεκδίκησε νομικά το δικαίωμα περί μη παραβίασης των πνευματικών δικαιωμάτων των ανταλλασσόμενων στο Napster μουσικών κομματιών. Η νέα όμως αρχιτεκτονική δικτύου τύπου P2Pήταν πλέον ισχυρή. Βάσει αυτής πρωτοστάτησε το downloading[2] στην πορεία, δημιουργώντας σταδιακά τα συστήματα κοινής χρήσης δεύτερης γενιάς P2P δίκτυα, με ανοιχτό πλέον κώδικα, όπου ο κάθε κόμβος θεωρούταν ισάξιος και δεν υπήρχε κάποιος κεντρικός Server[3]. Προβλήματα αποθηκευτικού χώρου και εύρους του δικτύου ήταν άμεσα και υπαρκτά, όμως επιλύθηκαν αρχικά με το σύστημα Fast Track, βάσει του οποίου προωθούνταν οι λίστες των αρχείων στους μεγαλύτερους

[1] Ένα δίκτυο υπολογιστών **peer-to-peer** ή **P2P,** (ομότιμο δίκτυο) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Πηγή : https://el.wikipedia.org/wiki/Peer-to-peer

[2] Λήψη δεδομένων από ένα απομακρυσμένο σύστημα. Πηγή : https://en.wikipedia.org/wiki/Download

[3] Εξυπηρετητής ή διακομιστής είναι υλικό ή και λογισμικό που αναλαμβάνει την παροχή διάφορων υπηρεσιών, «εξυπηρετώντας» αιτήσεις άλλων προγραμμάτων, γνωστών ως πελάτες (clients) που μπορούν να τρέχουν στον ίδιο υπολογιστή ή σε σύνδεση μέσω δικτύου.
Πηγή : https://el.wikipedia.org/wiki/%CE%95%CE%BE%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%84%CE%B7%CF%84%CE%AE%CF%82

κόμβους, οι οποίοι αναλάμβαναν τον ρόλο του «θεματοφύλακα», ενώ οι μικρότεροι κόμβοι συνδέονταν σε αυτούς. Εξαιρετικά παραδείγματα συστημάτων κοινής χρήσης αρχείων δεύτερης γενιάς αποτελούν τα: **Gnutella, Kazaa και Emule/Kademlia, eDonkey2000/Overnet, Ares Galaxy και τέλος το πρωτόκολλο BitTorrent,** όπου το κάθε αρχείο δεδομένων, που διατίθενται για διαμοιρασμό σε ένα τέτοιο δίκτυο, «σπάει» σε πολλά μικρά τμήματα. Σε αντίθεση με τα άλλα δίκτυα P2P, που έχουν μια δενδροειδή δομή και όπου η ανταλλαγή των αρχείων γίνεται κυρίως ανάμεσα σε δύο υπολογιστές, σε ένα δίκτυο που χρησιμοποιεί το BitTorrent πρωτόκολλο, οι χρήστες που διαμοιράζονταν ένα αρχείο σχημάτιζαν τα λεγάμενα «κοπάδια» (swarm). Σε αυτά τα δίκτυα, η εύρεση των κόμβων που μοιράζονται κάποιο αρχείο και η σύνδεση με αυτά γίνεται μέσω της **τεχνολογίας κατανεμημένων πινάκων κατακερματισμού DHT (Distributed Hash Tables)**, γεγονός που βοήθησε στην αντιμετώπιση του προβλήματος της διαθεσιμότητας καθώς μέσω της αντιγραφής και διατήρησης αρχείων σε γειτονικούς κόμβους από κάποιον άλλο κόμβο, η αναζήτηση γινόταν γρήγορα και αποτελεσματικά. **Κάπως έτσι γεννήθηκε η ιδέα της αποκέντρωσης, που θα παρουσιάσουμε διεξοδικά στη συνέχεια.**



Εικόνα 2: Μοντέλα διανομής δεδομένων

❖ Το πρόβλημα της διπλής δαπάνης

Σε ότι αφορά τις οικονομικές συναλλαγές εντός ενός δικτύου, αυτό που απασχόλησε έντονα τους τεχνικούς ήταν η λεγόμενη διπλή δαπάνη. Η διπλή δαπάνη έγκειται στο γεγονός της πιθανής αστοχίας μιας ψηφιακής συναλλαγής, όπου η ίδια η πληρωμή μπορεί να εμφανίζεται ως χρέωση για παραπάνω από μία φορές, με την δεύτερη πληρωμή να μην υφίσταται κατ' ουσία. Απόρροια τούτου είναι η δημιουργία της πεποίθησης ότι το ψηφιακό νόμισμα ενδέχεται εύκολα να αλλοιωθεί με δόλιο τρόπο από κακόβουλους χρήστες. Συνεπώς, λογικό είναι να υπάρχουν δεύτερες σκέψεις σχετικά με την υιοθέτηση ή την επέκτασή του στις συναλλαγές.

Στα πλαίσια της αναζήτησης λύσης στο εν λόγω πρόβλημα και συγκεκριμένα στην πρόληψή του, προτάθηκαν δύο τρόποι: **α) η Κεντρική αρχιτεκτονική μορφή δικτύου**, ή **β) η αποκεντρωμένη (ή κατανεμημένη)**. Κεντρική σημαίνει ότι υπάρχει μία κεντρική οντότητα (πχ μία τράπεζα), που ερευνά και επικυρώνει τη δαπάνη ενός ψηφιακού νομίσματος, ενισχύοντας κατά αυτόν τον τρόπο, την εμπιστοσύνη στο σύστημα, αρκεί να μην προκύψουν προβλήματα διαθεσιμότητας κατά τη λειτουργία του.

Η αντιπρόταση του Nakamoto **[50]** σε αυτό, ήταν να δημιουργηθεί ένα αποκεντρωμένο σύστημα, μέσω του οποίου η πρόληψη της διπλής δαπάνης θα ήταν ασφαλέστερη. Βάσει αυτής της φιλοσοφίας δημιουργήθηκε το κρυπτονόμισμα bitcoin, το οποίο και φέρει ως συστατικό του στοιχείο, την αποκεντρωμένη του μορφή. Ερωτήματα τέθηκαν σχετικά με την εμπιστοσύνη στον κυβερνοχώρο δίχως την ασφαλιστική δικλείδα μιας έμπιστης κεντρικής ενότητας. Η πιστοποίηση της ταυτότητας των μερών καθώς και η πιστοποίηση των δικαιωμάτων πρόσβασης καθιερώθηκαν τελικά ως οι βασικοί «πυλώνες» ασφαλείας εντός ενός δικτύου, το οποίο απαρτίζεται από άγνωστες οντότητες. **Τεχνολογία blockchain και εμπιστοσύνη άρχισαν να γίνονται πλέον έννοιες σχεδόν ταυτόσημες.**

❖ Το πρόβλημα των βυζαντινών στρατηγών

Τι συμβαίνει όμως με την πληθώρα των κόμβων εντός ενός δικτύου blockchain; Μας προσφέρει τελικά υψηλό βαθμό ασφάλειας και σταθερότητας; Με αφορμή τέτοιου είδους ερωτήματα, οι Lamport, Shostak, & Pease (1982) εισήγαγαν το πρόβλημα των Βυζαντινών Στρατηγών ως απάντηση, αναδεικνύοντας εμμέσως τη σπουδαιότητα της **συναίνεσης, με την οποία επικυρώνεται η αξιοπιστία των συμμετεχόντων (κόμβων) στο δίκτυο.** Το πρόβλημα των βυζαντινών αρχηγών αποτελεί μια μελέτη για τον τρόπου με τον οποίο στέλνουμε μια πληροφορία με ασφάλεια, παρουσία των αντιπάλων μας, εισάγοντας κατά κάποιον τρόπο την έννοια της κρυπτογραφίας.

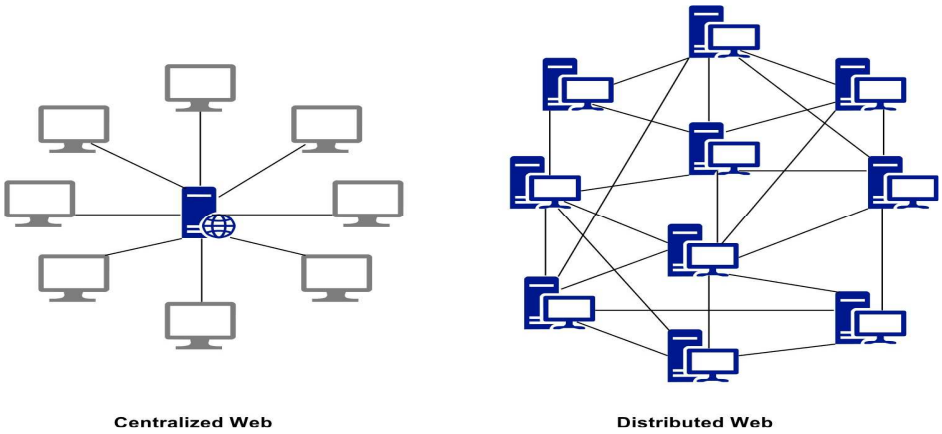
Το πρόβλημα των βυζαντινών αρχηγών παραστατικά περιγράφεται ως μια μάχη ανάμεσα σε **δύο αυτοκρατορίες, οι οποίες έχουν σχεδόν ισοδύναμες δυνάμεις.** Η μία αυτοκρατορία βρίσκεται μέσα στα όρια μιας περιχαρακωμένης πόλης ενώ η δεύτερη αυτοκρατορία έχει αρκετούς στρατηγούς, που περιβάλλουν αυτή την περιφραγμένη πόλη με τον στρατό της, έχοντας ως σκοπό την επίθεση. Αν όλοι οι στρατηγοί συμφωνήσουν να επιτεθούν ταυτόχρονα, θα έχουν αρκετή δύναμη για να κατακτήσουν την αυτοκρατορία και να κερδίσουν τη μάχη. Εάν, για οποιονδήποτε λόγο, δεν είναι σε θέση να συντονίσουν τις επιθέσεις τους ταυτόχρονα, και ακόμη και ένας στρατηγός χάσει το μήνυμα, η αυτοκρατορία που περιβάλλει την περιτειχισμένη πόλη θα χάσει τη μάχη και τον πόλεμο.

Κατ' αντιστοιχία με ένα αποκεντρωμένο δίκτυο Blockchain, συμπεραίνουμε ότι η δύναμη της υπολογιστικής ισχύος και του κατακερματισμού που δημιουργείται **εντός της αλυσίδας,** (και όχι έξω από αυτήν) ενισχύει με γεωμετρική πρόοδο την εμπιστοσύνη των συμμετεχόντων στο εν λόγω δίκτυο και καθιστά μη ανατρέψιμα τα μέχρι τότε δεδομένα. Και αυτό συμβαίνει διότι η επίθεση ενός ικανού αντιπάλου εντός ενός δικτύου με σημαντική υπολογιστική ισχύ όπως είναι το δίκτυο Blockchain, θα ήταν ιδιαίτερα δαπανηρή, **αν και επιτυχής**, καθώς ο «εισβολέας» θα βρίσκονταν στη δυσάρεστη θέση να βρεθεί τελικά αντιμέτωπος με την οικονομική εκμετάλλευση του συνολικού δικτύου, αποτρέποντάς τον από το να μεταβάλλει τα δεδομένα που έχουν ήδη επικυρωθεί μέχρι τη στιγμή εκείνη.

2.1 Ανάλυση τεχνολογικού περιβάλλοντος τεχνολογίας DLT

2.1.1 Κεντρικοποιημένα και κατανεμημένα συστήματα

Η αυθεντικότητα, η ακεραιότητα και η επαληθευσιμότητα αποτέλεσαν τα τρία βασικά συστατικά στοιχεία ενός αρχιτεκτονικού μοντέλου τεχνολογίας DLT[4], από τη στιγμή μάλιστα που οι συναλλαγές πραγματοποιούνται μεταξύ αγνώστων. Ο κάθε χρήστης αντιπροσωπεύει έναν κόμβο, μέσω του οποίου δημιουργούνται αλληλεπιδράσεις εντός ενός αποκεντρωμένου δικτύου. Οι συναλλαγές μεταξύ των χρηστών ή των κόμβων καταγράφονται και έτσι επαληθεύεται η αυθεντικότητα των δεδομένων του, τα οποία μεταδίδονται πλέον επικυρωμένα σε κάθε άλλο κόμβο που είναι συνδεδεμένος με αυτήν και στο τέλος διαδίδονται σε όλο το δίκτυο. Ο ανοικτός κώδικας είναι εκείνος που θα αναλάβει τον ρόλο του ελεγκτή – επικύρωση και όχι ο άνθρωπος.



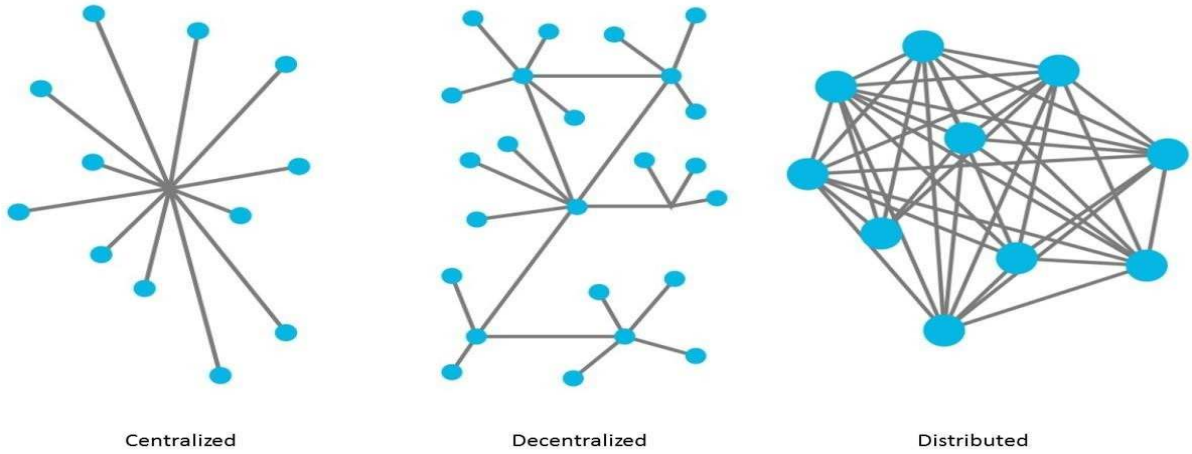
Εικόνα 3: Κεντρικοποιημένο και κατανεμημένο σύστημα

Δύο τύποι συστημάτων υφίστανται. Τα κεντρικοποιημένα και τα κατανεμημένα συστήματα. Τα κρίσιμα σημεία διαχωρισμού τους έγκειται στα εξής σημεία : **α) στον τρόπο με τον οποίο λαμβάνεται η κάθε απόφαση και β) στον τρόπο διαμοιρασμού της πληροφορίας στους κόμβους.** Αυτό όμως δεν αποκλείει και την επιλογή χρήσης ενός μικτού αρχιτεκτονικού μοντέλου εφαρμογής. Όταν οι δικτυακοί πόροι διατίθενται κεντρικά, ο έλεγχος λαμβάνει χώρα από μια κεντρική οντότητα. Ο κίνδυνος που ελλοχεύει εδώ είναι ότι σε μια ενδεχόμενη καταστροφή του κεντρικού κόμβου, η επικοινωνία θα καθίσταται ανύπαρκτη σε όλο το δίκτυο. ***Στην δε κατανομή στα κατανεμημένα συστήματα, δεν υπάρχει αντίστοιχο κεντρικό σημείο λήψης αποφάσεων για το δίκτυο. Κάθε κόμβος συμμετέχει αυτοτελώς στο δίκτυο και το σύνολο των αποφάσεων και συμπεριφορών καθορίζουν την συμπεριφορική δομή του συστήματος στο σύνολο του.***

[4] Η Τεχνολογία κατανεμημένου καθολικού (Distributed Ledger Technology – DLT) αναφέρεται στα πρωτόκολλα και στην υποστηριζόμενη υποδομή, που επιτρέπουν σε υπολογιστές σε διαφορετικές τοποθεσίες, να προτείνουν και να επικυρώνουν συναλλαγές και να ενημερώνουν με συγχρονισμένο τρόπο σύνολα δεδομένων μέσω ενός δικτύου. Πηγή : https://www.coin-report.net/gr/356/

2.1.2 Αποκεντρωμένα συστήματα

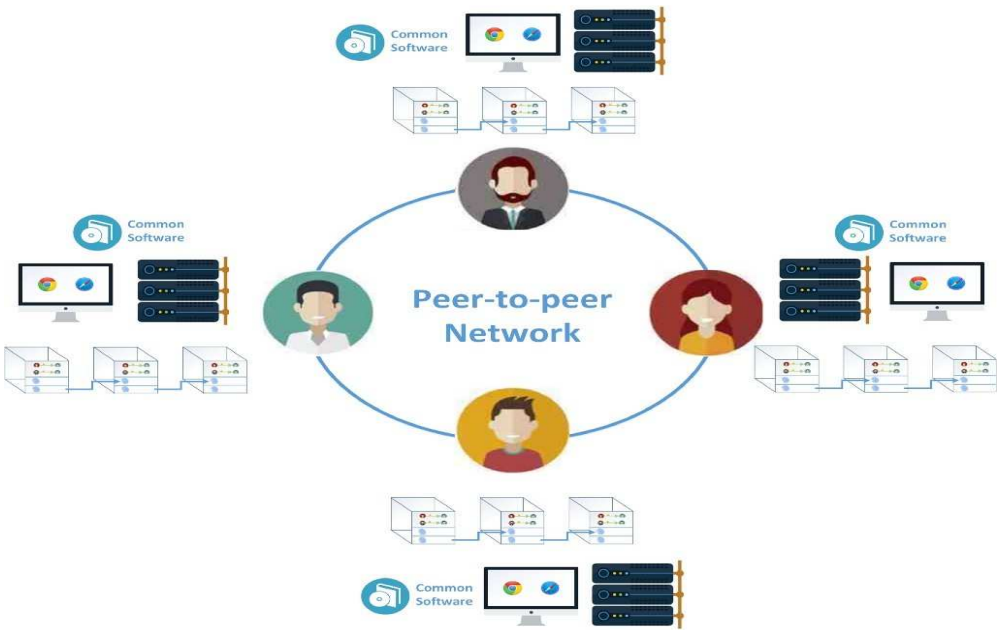
Μια υποκατηγορία των κατανεμημένων δικτύων είναι τα αποκεντρωμένα συστήματα. Στα συστήματα αυτά υφίσταται **κεντρικοί κόμβοι επικοινωνίας ομαδοποιημένοι** και ο έλεγχος εκτελείται από διαφορετικά στοιχεία.



Εικόνα 4: Κεντρικοποιημένα, αποκεντρωμένα και κατανεμημένα συστήματα [49]

2.1.3 Ομότιμα δίκτυα (Peer-to-Peer networks)

Το ομότιμο δίκτυο αποτελεί ένα αποκεντρωμένο κατανεμημένο δίκτυο χωρίς οιαδήποτε κεντρική διεργασία. Το σύνολο των κόμβων σχηματίζουν ένα δίκτυο όπου μοιράζονται ισότιμα τις υποχρεώσεις και τους πόρους, προσφέροντας, κατά περίπτωση, το εύρος ζώνης τους, την επεξεργαστική ισχύ τους ή και τον αποθηκευτικό τους χώρο. Ο ρόλος του διακομιστή και του πελάτη εναλλάσσονται κατά το δοκούν και βάσει της εκάστοτε διεργασίας του δικτύου.



Εικόνα 5: Peer to peer δίκτυο [36]

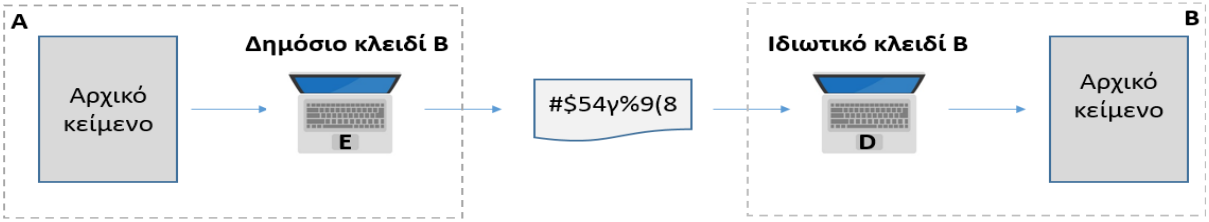
2.2 Κρυπτογραφία

2.2.1 Ασύμμετρη κρυπτογραφία

Η σύγχρονη κρυπτογραφία προέκυψε κατόπιν μαθηματικών ερευνών κατά τη μελέτη της επιστήμης των υπολογιστών. Υπάρχουν δύο είδη συστημάτων **α) τα συμμετρικά κρυπτογραφικά συστήματα** στα οποία χρησιμοποιούνται δύο ζευγάρια κλειδιών και **β) τα ασύμμετρα κρυπτογραφικά συστήματα** (συστήματα δημοσίου κλειδιού), όπου υπάρχει μόνο ένα ζευγάρι κλειδιών. Το ένα κλειδί (δημόσιο) κωδικοποιεί το μήνυμα που προορίζεται να παραληφθεί, ενώ το δεύτερο (ιδιωτικό) αποκωδικοποιεί το απεσταλμένο μήνυμα.

Εικόνα 6: Μηχανισμός κωδικοποίησης ασύμμετρου κρυπτογραφικού συστήματος

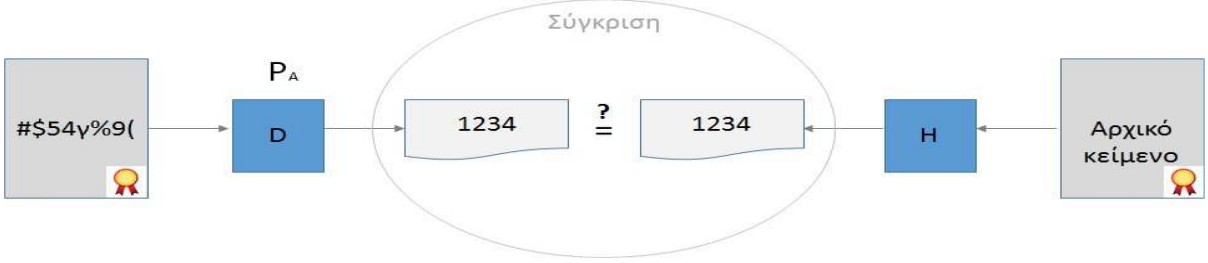
Η διαδικασία δύναται να είναι και αντίστροφη ή ακόμα και να υπάρχει σύνδεση των δύο κλειδιών.



Εικόνα 7: Διαδικασία κρυπτογραφίας δημόσιου κλειδιού

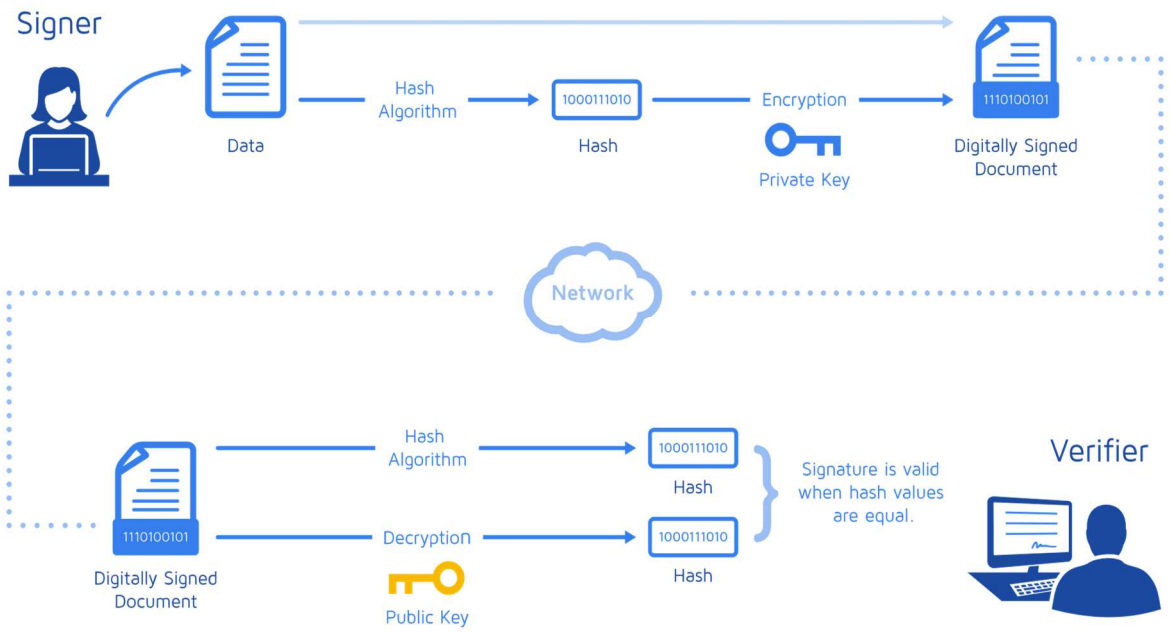
2.2.2 Ψηφιακή Υπογραφή

Η δημιουργία μιας συναλλαγής στο blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο ταυτότητας της συναλλαγής. Μια ψηφιακή υπογραφή είναι στην ουσία η κρυπτογράφηση της σύνοψης του μηνύματος. Μια τυπική ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις: **τη φάση υπογραφής και τη φάση επαλήθευσης,** ακριβώς όπως συμβαίνει με την ασύμμετρη κρυπτογραφία, τη λειτουργία της οποίας περιγράψαμε παραπάνω.



Εικόνα 8: Μηχανισμός ψηφιακής υπογραφής

Η δημιουργία ενός ζεύγους κλειδιών είναι ανάλογη με τη δημιουργία ενός λογαριασμού στο blockchain, καθώς το λογισμικό που δημιουργεί τον λογαριασμό, ουσιαστικά δημιουργεί ένα ιδιωτικό και ένα δημόσιο κλειδί για τον χρήστη, τα οποία συσχετίζονται με τον ανωτέρω μαθηματικό τρόπο. Επίσης, κάθε συναλλαγή που εκτελείται στο blockchain υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί του. Αυτή η υπογραφή διασφαλίζει ότι μόνο ο κάτοχος του λογαριασμού μπορεί να πραγματοποιήσει συναλλαγές από τον λογαριασμό αυτόν.



Εικόνα 9: Ανάλυση ψηφιακώς υπογεγραμμένου εγγράφου [42]

2.2.3 Κρυπτογραφικές Συναρτήσεις Σύνοψης (Hash)

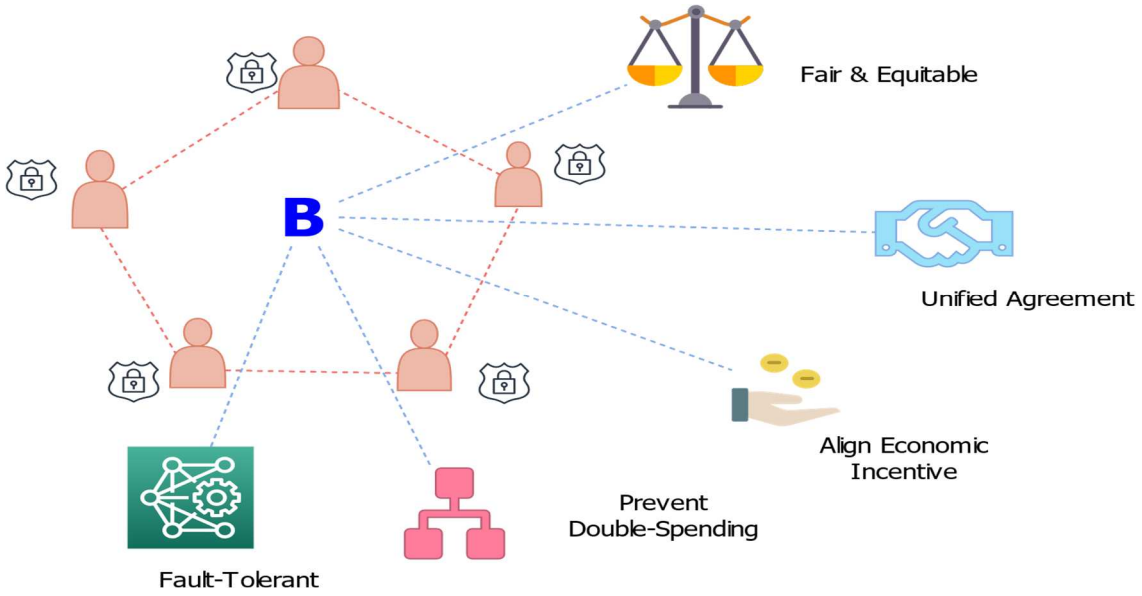
Μία συνάρτηση hash είναι μία μέθοδος μετατροπής δεδομένων τυχαίου μεγέθους σε μία **ψηφιακή αλφαριθμητική ακολουθία με προκαθορισμένο σταθερό μήκος**, η οποία λέγεται hash. Πρόκειται για μια αλφαριθμητική ακολουθία αλγορίθμων, που περιγράφουν ένα ψηφιακό αρχείο. Οι συναρτήσεις σύνοψης αποτελούν **το μοναδικό δακτυλικό αποτύπωμα του ψηφιακού αρχείου** και συμβάλλουν τα μέγιστα στην λειτουργία του Blockchain καθώς επίσης διαδραματίζουν πρωταγωνιστικό ρόλο στην κρυπτογραφία. Δεν θα χρειαστεί όμως να εμβαθύνουμε στα συστατικά στοιχεία της, καθώς κάτι τέτοιο δεν αποτελεί αντικείμενο της παρούσας εργασίας.

Εικόνα 10: Λειτουργία αλγορίθμων hash

2.3 Μηχανισμοί συναίνεσης

2.3.1 Περί συναίνεσης

Η έννοια της κεντρικής οντότητας σε ένα δίκτυο blockchain είναι ανύπαρκτη, γεγονός που δημιουργεί ανασφάλεια στους συναλλασσόμενους. Το γεγονός όμως ότι όλοι οι κατανεμημένοι κατάλογοι απαιτούν την **επικύρωση** των συναλλαγών, την οποία πάντα ακολουθεί η συναίνεση, δημιουργεί εμπιστοσύνη στους συμμετέχοντες στο δίκτυο. Τα blockchain μάλιστα συνδυάζουν **επαλήθευση και συναίνεση μαζί**, χρησιμοποιώντας πολλούς και διαφορετικούς μηχανισμούς.



Εικόνα 11: Στόχοι του μηχανισμού συναίνεσης

2.3.2 Byzantine Generals Problem

Ο ένας μηχανισμός βασίζεται στην φιλοσοφία που αναπτύχθηκε κατά την επίλυση του προβλήματος των Βυζαντινών Στρατηγών, για τη λογική της οποίας αναφερθήκαμε παραπάνω. Βάσει αυτής, δημιουργήθηκαν στατιστικά πορίσματα, που τελικά οδηγούν στην επαλήθευση μιας αξιόπιστης λειτουργίας ενός δικτύου Blockchain. Κι όλα αυτά στηρίζονται στο υποθετικό σενάριο, όπου το δίκτυο αναπαρίσταται από **μια ομάδα Στρατηγών** η οποία δεχόμενη επίθεση από τους αντιπάλους της, **αναζητά την βέλτιστη δυνατή στρατηγική**, βάσει της οποίας θα οδηγηθεί στη νίκη, ενόσω όμως απειλείται από μία άλλη ομάδα Στρατηγών, η οποία διαθέτει τις ίδιες ακριβώς σε επίπεδο δυναμικής, στρατιωτικές δυνάμεις. Για να καταφέρει να επιτύχει τον σκοπό της η συγκεκριμένη ομάδα Στρατηγών, οφείλει να επιδείξει ομοψυχία και κοινό στόχο, χωρίς να καθοδηγείται από ιδιοτελή κίνητρα. **Η ομαδικότητα και η ανιδιοτέλεια διαδραματίζουν τον σημαντικότερο ρόλο.** Αποδεικνύεται επιστημονικά, ότι σε περίπτωση που **το ένα τρίτο του συνόλου** των Στρατηγών αποφασίσει να δράσει με διαφορετικό τρόπο, το εγχείρημα αυτό, δεν θα φέρει το επιθυμητό αποτέλεσμα. Το προαναφερθέν

παράδειγμα **κατ' αναλογία με ένα δίκτυο blockchain** το οποίο είναι ένα κατανεμημένο δίκτυο, όπου δεν υφίσταται κεντρικός κόμβος λήψης απόφασης, το γεγονός οι πλέον των δύο τρίτων (2/3) κόμβοι δεν είναι ελαττωματικοί, λαμβάνεται υπόψη (βάσει συγκεκριμένου πρωτοκόλλου), ως προϋπόθεση για την αξιόπιστη λειτουργία του. Με τον μηχανισμό αυτό, **εντοπίζεται το σφάλμα και αποτρέπεται η πιθανότητα να λειτουργήσει ένα αναξιόπιστο δίκτυο,** παρέχοντας κατ' αυτόν τον τρόπο, προστασία στους συμμετέχοντες.

2.3.3 Χρήση Πρωτοκόλλων

Όταν αναφερόμαστε σε διαδεδομένα blockchain, εννοούμε δεδομένα που είναι ανοικτά και μη αδειοδοτούμενα. Ο κίνδυνος των επιθέσεων από μια μειοψηφία που θα προσπαθήσει αν αποκτήσει τον έλεγχο είναι υπαρκτός, με αποτέλεσμα να τίθενται υπό αμφισβήτηση η ακεραιότητα του δικτύου. Ο 'Nakamoto' εφάρμοσε μία καινοτόμο ιδέα για να καταπολεμήσει το πρόβλημα. Ο Nakamoto σκέφτηκε ότι θα ήταν εξαιρετικά ανατρεπτική για έναν κακόβουλο τρίτο – εισβολέα, η δημιουργία μιας «σπαζοκεφαλιάς» η οποία θα απαιτούσε χιλιάδες υπολογισμούς, προκειμένου να εκτελεστεί μια συναλλαγή εντός ενός δικτύου – κατανεμημένου μητρώου (ledger) blockchain - ώστε να επικυρωθεί μια τρέχουσα ομάδα συναλλαγών (block). Γι' αυτό φρόντισε για την αύξηση των απαιτήσεων σε υπολογιστική ισχύ, με τον αλγόριθμο συναίνεσης, μετατρέποντάς τον σε έναν μηχανισμό PoW[5] εξαιρετικά κοστοβόρο και κατ' ουσία μετουσίωσε τη διαδικασία αυτή **στην λεγόμενη 'εξόρυξη' (Mining).**

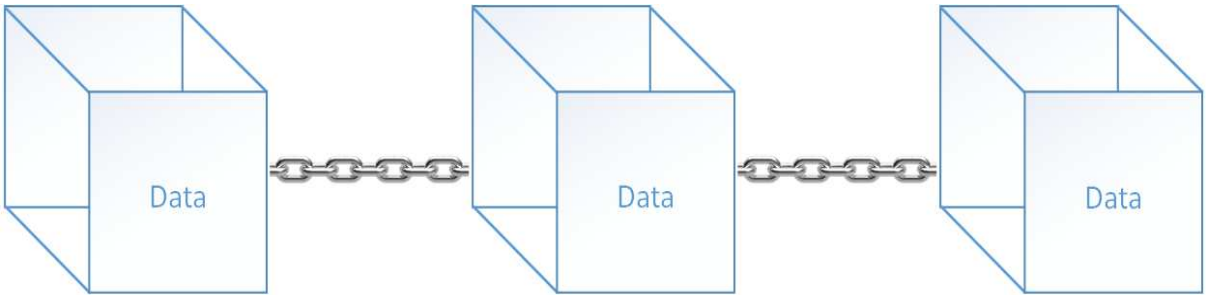
2.4 To Block

Μια βάση δεδομένων δύναται να αποτελείται είτε από συναλλαγές **άυλων αγαθών** (π.χ. οικονομικές αξίες - κρυπτονομίσματα), **είτε από υλικά αγαθά** (π.χ. τίτλοι ιδιοκτησίας υλικών αγαθών - ψηφιακά πιστοποιητικά - έξυπνα συμβόλαια, κλπ).Το block συγκροτεί το δομικό στοιχείο της αλυσίδας. Αποτελεί μια ιδιάζουσα μονάδα πληροφορίας

Εικόνα 12: Το μπλοκ της αλυσίδας [59]

[5] Το Proof of Work (PoW) περιγράφει ένα σύστημα που απαιτεί μια όχι ασήμαντη αλλά εφικτή προσπάθεια προκειμένου να αποτραπούν επιπόλαιες ή κακόβουλες χρήσεις υπολογιστικής ισχύος. Πηγή : https://www.investopedia.com/terms/p/proof-work.asp

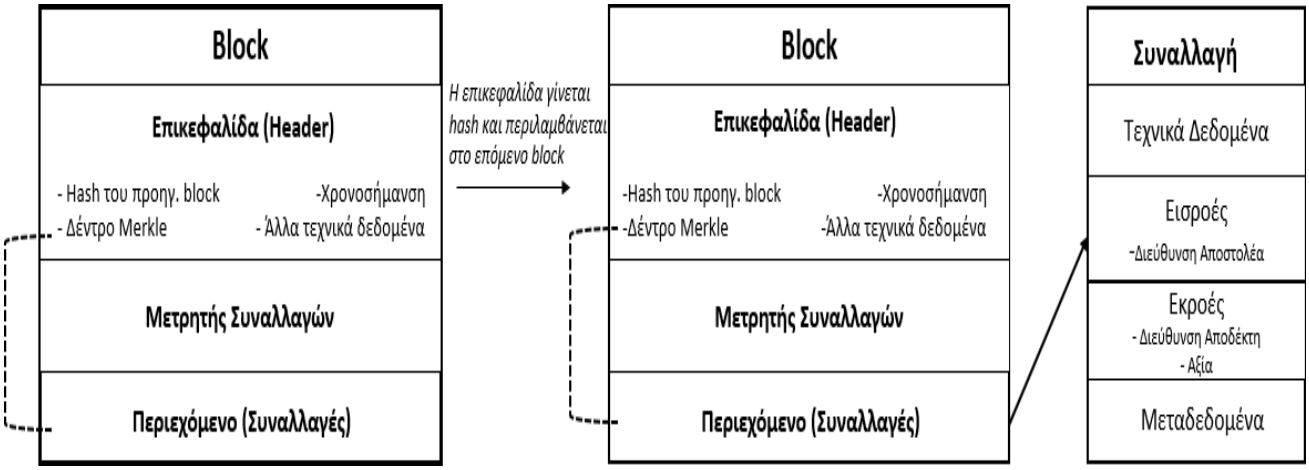
Μετά από την καταχώρηση συγκεκριμένων δεδομένων σε ένα μπλοκ, αυτά παραμένουν αμετάβλητα, δεν διαγράφονται, αλλά μετατρέπονται σε «αμάχητα τεκμήρια απόδειξης».



Εικόνα 13: Τα δεδομένα του μπλοκ της αλυσίδας [36]

Το σύνολο των εν λόγω συναλλαγών δημιουργούν τα block εντός της αλυσίδας blockchain.

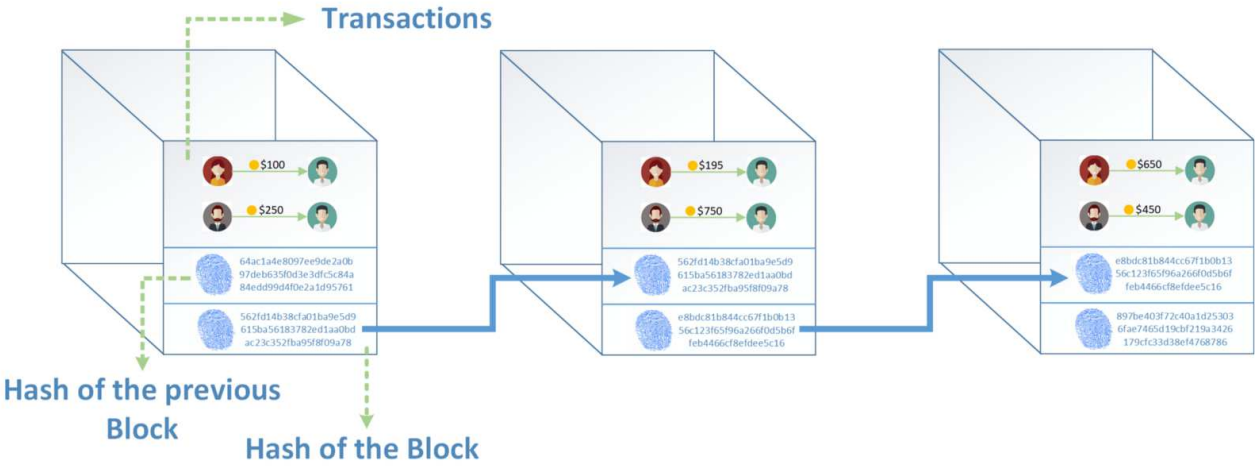
Εικόνα 14 : Εισαγωγή ενός μπλοκ σε έναν αλυσιδωτό κώδικα



Εικόνα 15: Περιεχόμενο ενός μπλοκ και μιας συναλλαγής

2.4.1 Συναλλαγές (transactions) – Δέντρα κατακερματισμού

Τα δεδομένα των συναλλαγών του μπλοκ **μετασχηματίζονται κρυπτογραφικά σε ένα δέντρο Merkle**. Τα δέντρα Merkle (ή δέντρα κατακερματισμού) είναι δυαδικά δέντρα τα οποία ονομάστηκαν έτσι προς τιμήν του επιστήμονα που τα πρότεινε, **με σκοπό την ανάπτυξη μίας νέας μεθόδου ψηφιακής υπογραφής βασιζόμενης σε συμβατικές συναρτήσεις κρυπτογράφησης**.



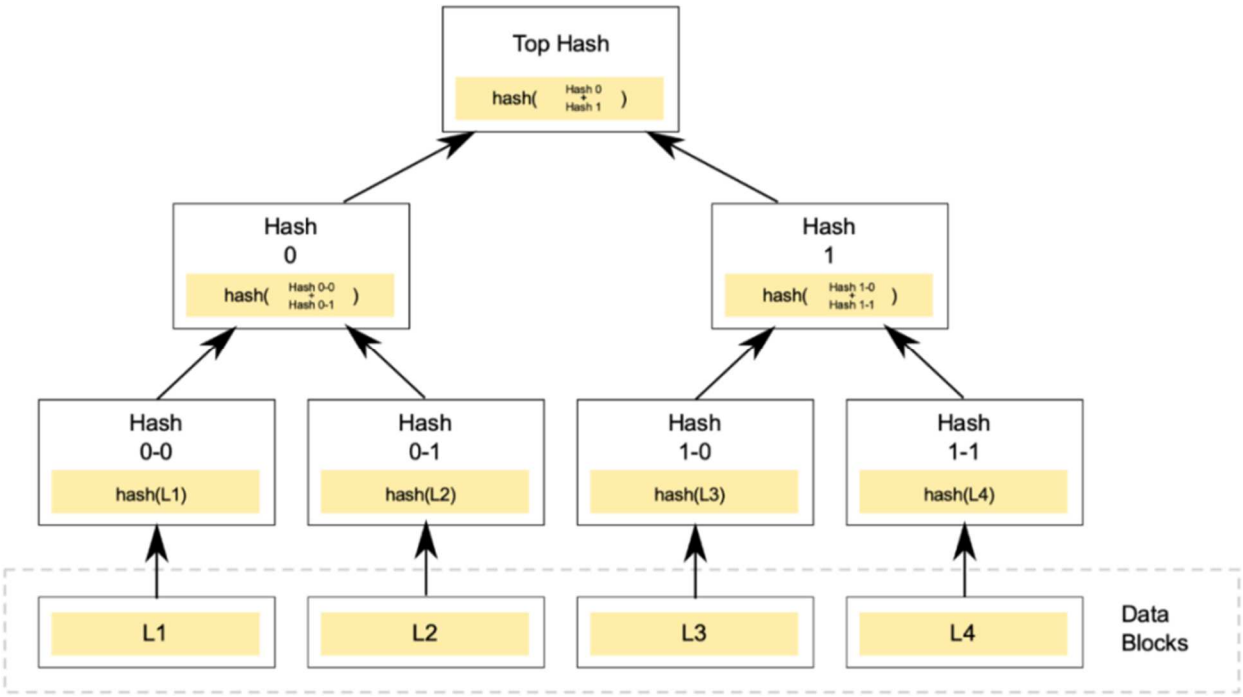
Εικόνα 16: Απεικόνιση συναλλαγών στο blockchain [36]

- Σε ένα block περιλαμβάνεται πλήθος συναλλαγών, η κάθε μία από αυτές κατακερματίζεται σε μία σύνοψη **(Transaction ID).**
- Κατόπιν σχηματίζουν ζεύγη, τα οποία στη συνέχεια αποτελούν τα φύλλα του δέντρου **(leaf nodes).**
- Για κάθε ζευγάρι δημιουργείται ένας **'πατέρας'** με δύο δείκτες κατακερματισμού που δείχνουν σε κάθε συναλλαγή.
- Αυτοί οι κόμβοι-πατέρες σχηματίζουν το επόμενο επίπεδο του δέντρου και ο κατακερματισμός συνεχίζεται μέχρι την εμφάνιση ενός και μοναδικού κόμβου **(Merkle Root).**
- Το κάθε block περιέχει εκατοντάδες συναλλαγές, αλλά μία και μόνο ρίζα Merkle.

Μια τυπική διάταξη ενός δέντρου Merkle έχει ως εξής:

1. Η **ρίζα καταχωρείται στην επικεφαλίδα**.
2. Ο κάθε κόμβος-φύλλο (**leaf node**) περιέχει μία σύνοψη δεδομένων.
3. Ο κάθε κόμβος - πατέρας (**non-leaf node**) περιέχει το αποτέλεσμα κρυπτογραφικού κατακερματισμού των περιεχομένων των κόμβων - παιδιών.
4. Η ρίζα του δέντρου (**Merkle root**) περιέχει μία σύνοψη όλων των δεδομένων του δέντρου, σχηματιζόμενη από συνεχείς κατακερματισμούς.

5. Εφόσον η ρίζα είναι διαθέσιμη, οποιοσδήποτε μπορεί να επαληθεύσει τα δεδομένα κάθε κόμβου με υπολογισμό ενός αριθμού́ κατακερματισμών των κόμβων των φύλλων του δέντρου, ακολουθώντας την αντίστοιχη διαδρομή κατακερματισμού (**Merkle branch**).

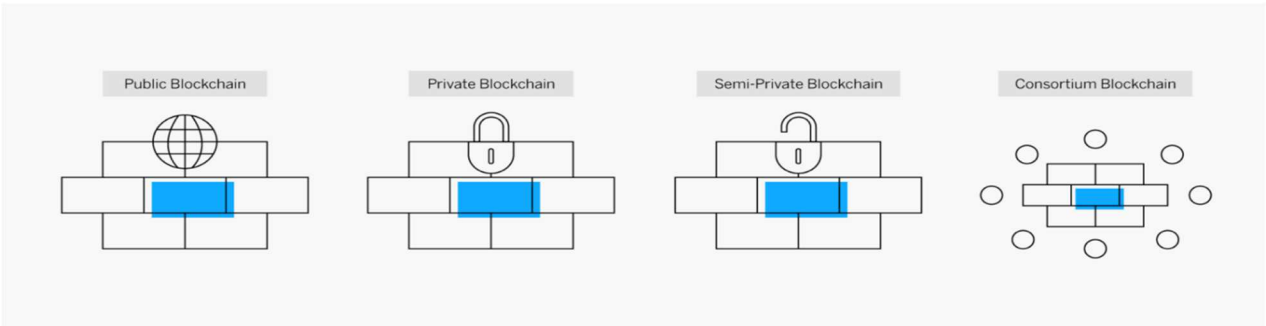


Εικόνα 17: Τυπική διάταξη Δέντρου Merkle [53]

Με τη βοήθεια του δέντρου Merkle, ο χρόνος αναζήτησης μιας επιβεβαιωμένης συναλλαγής στο block εκμηδενίζεται χρονικά, αφού **καθίσταται ιδιαίτερα ευχερής η επαλήθευση και η ακεραιότητα των δεδομένων** με μια και μόνο ματιά.

2.5 Διάκριση βάσει της ιδιοκτησίας του δικτύου

Η ταξινόμηση των blockchain προτάθηκε από τους Tasca & Tessone (**2017**). Στην παρούσα εργασία θα περιοριστούμε σε δύο βασικούς τρόπους διάκρισής τους, **α) βάσει ιδιοκτησίας του δικτύου, β) βάσει δικαιωμάτων των χρηστών,** ενώ παρέλκει της παρούσας εργασίας, να αναφερθεί εκτενώς η ταξινόμησή τους βάσει των χρησιμοποιούμενων μηχανισμών συναίνεσης.



Εικόνα 18: Τύποι blockchain βάσει ιδιοκτησίας δικτύου

2.5.1 Public blockchains

Το εύρος πρόσβασης στους χρήστες αποτελεί την ειδοποιό διαφορά μεταξύ ενός public και private blockchain, γεγονός που συνεπάγεται την ιδιοκτησία της υποδομής του. Οι διακομιστές είναι δημόσιοι και ανοικτοί, όλοι μπορούν να συμμετέχουν ανώνυμα εφόσον το επιθυμούν και έχουν δυνατότητα προσπέλασης της βάσης δεδομένων της. Η πρώτη αλυσίδα παγκόσμιας εμβέλειας τέτοιου είδους είναι το bitcoin. Η διαφάνεια, ο έλεγχος της πληροφορίας και η μέγιστη προοπτική διεύρυνσής του κατατάσσεται στα θετικά σημεία αυτής της μορφής δικτύου, σε αντιστάθμισμα με το κόστος που συνεπάγεται η υπερβολική χρήση πόρων η οποία ελαχιστοποιεί την απόδοση και την χωρητικότητα του δικτύου, στα πλαίσια μιας διευρυμένης χρήσης κρυπτογράφησης και κατακερματισμού. Η ιδιωτικότητα απειλείται σημαντικά, καθώς κάποια ευαίσθητα δεδομένα ενδέχεται να αποκωδικοποιηθούν από κακόβολους χρήστες, παρότι προβλέπονται αρκετοί μηχανισμοί συναίνεσης.

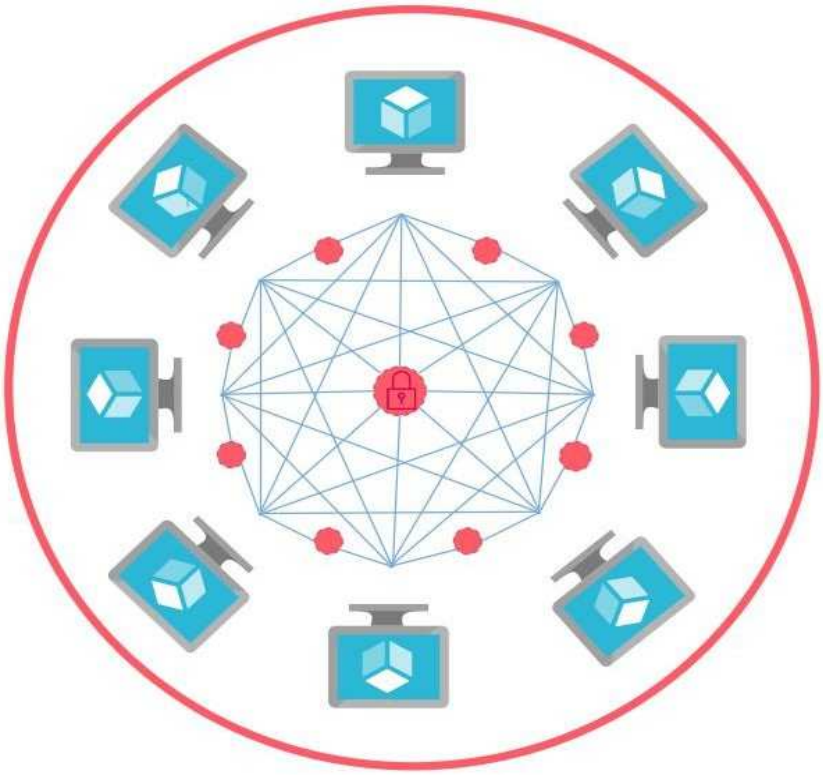
2.5.2 Private blockchains

Το πρόβλημα την ιδιωτικότητας επιλύεται εδώ, καθώς η πρόσβαση των χρηστών πραγματοποιείται μέσω ενός διαχειριστή ή μέσω ενός αυστηρού πρωτοκόλλου κανόνων, όπου οι υποψήφιοι κόμβοι θα είναι εκ των προτέρων αυθεντικοποιημένοι και πιστοποιημένοι. Πρόκειται για ένα blockchain ελεγχόμενο, κεντρικοποιημένο, τοποθετημένο σε ιδιωτικούς διακομιστές, όπου ορίζεται εξ αρχής ποιοι μπορούν να συμμετέχουν και να αναγνώσουν τη βάση δεδομένων του. Το μειονέκτημα σε αυτή την περίπτωση έγκειται στο γεγονός ότι ένας διαχειριστής ή ένας οργανισμός ουσιαστικά διευθύνει και ίσως ακόμα και να επεμβαίνει σε δεδομένα, «ακυρώνοντας» την ανατροπή που φιλοδοξεί να επιφέρει η τεχνολογία blockchain

2.5.3 Consortium blockchains

Μια μορφή μερικώς ιδιωτική και αποκεντρωμένη ονομάζεται υβριδική. Η έλλειψη εμπιστοσύνης των public blockchain προσομοιάζει να επιλύεται. Η ύπαρξη ομάδας κόμβων οι οποίες διαδραματίζουν τον ηγετικό ρόλο με συντονισμένες ενέργειες, προσδίδουν έναν συνεργατικό χαρακτήρα, όπου μοιράζεται η εμπιστοσύνη σε σύγκριση με τα private blockchain, τα οποία στηρίζονται σε μια μοναδική οντότητα. Ο μηχανισμός συναίνεσης και πρόσβασης ελέγχεται από προκαθορισμένους χρήστες, οργανισμούς ή επιχειρήσεις (κόμβοι). Δίνεται η δυνατότητα η ανάγνωση των δεδομένων να είναι και ελεύθερη (public) εφόσον εξυπηρετούνται οι σκοποί ή να είναι και αυτοί περιορισμένοι.

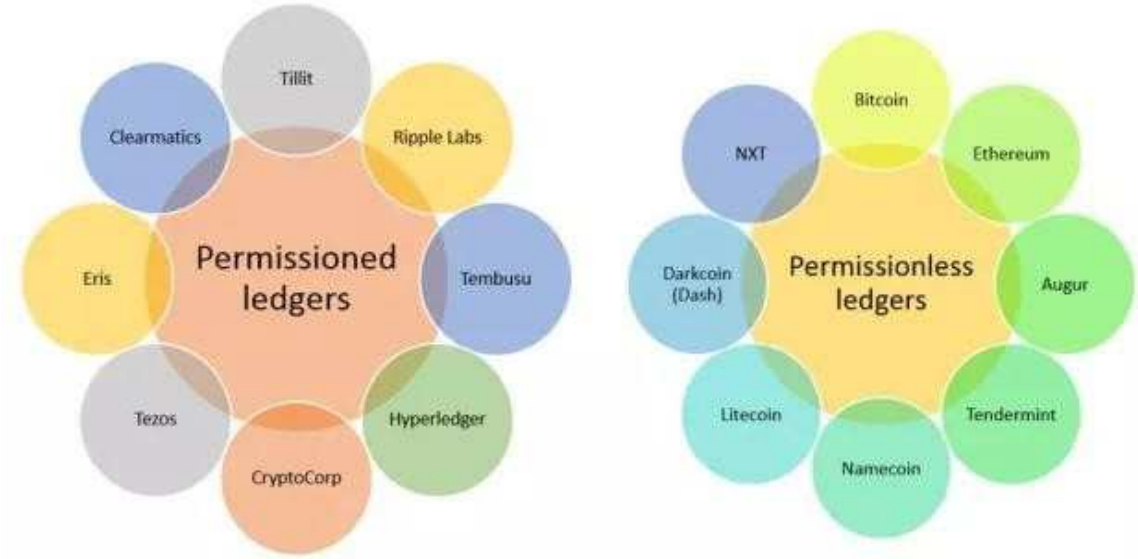
Σημαντικές τεχνικές διαφορές μεταξύ ενός private και consortium blockchain δεν υφίσταται. Είναι δυσδιάκριτος όμως ο διαχωρισμός τους, γι’ αυτό και οφείλουμε να εξετάσουμε τρόπους διαχείρισης κατά τη λειτουργία του, προκείμενου να καταλήξουμε σε ένα ασφαλές συμπέρασμα για τη μορφή του.



Εικόνα 19: Υβριδική μορφή δικτύου Blockchain [49]

2.6 Διάκριση βάσει δικαιωμάτων των χρηστών

Ο διαχωρισμός είναι συμπληρωματικός των προαναφερθέντων και έχει δημιουργήσει πολλές φορές παρανοήσεις συγχέοντας τους όρους public με permissionless και private με permissioned. Στην ουσία όμως αφορά στην αδειοδότηση για δικαίωμα εγγραφής στο μητρώο συναλλαγών και αναφέρεται στους μηχανισμούς συναίνεσης.



Εικόνα 20: Παραδείγματα εφαρμογών για permissioned και permissionless ledgers

2.6.1 Permissioned ledgers

Ειδικά δικαιώματα για κάθε έναν από τους χρήστες ή ομάδες χρηστών παραχωρούνται από τα αδειοδοτημένα μητρώα. Συνέπεια τούτου είναι η ευχέρεια παραμετροποίησης. Περιορισμοί επί των δικαιωμάτων πρόσβασης, όπως είναι η εκχώρηση δικαιώματος εγγραφής δεδομένων στην αλυσίδα, που έπεται τον περιορισμό συμμετοχής στον μηχανισμό συναίνεσης, οδηγούν στην «ασφάλεια» των αποφάσεων, η οποία προέρχεται από μια κεντρική αξιόπιστη οντότητα.

2.6.2 Permissionless ledgers

Η επιβολή ισχυρού μηχανισμού συναίνεσης κρίνεται επιβεβλημένη στην περίπτωση αυτή, αφού όλοι οι συμμετέχοντες έχουν το δικαίωμα εγγραφής και συμμετοχής στη διαδικασία συναίνεσης. Έχουν δηλαδή όλα τα δικαιώματα πλην της επεξεργασίας / τροποποίησης εγγραφών. Η πλήρως αποκεντρωμένη μορφή του μητρώου επιβάλλει τη συνεχή χρήση μηχανισμών συναίνεσης. Οι καθυστερήσεις επικοινωνίας μεταξύ των κόμβων, η δυσκολία επέκτασης της βάσης δεδομένων, η στασιμότητα του ρυθμού επεξεργασίας τους συνθέτουν τα βασικά μειονεκτήματα των δικτύων αυτής της μορφής. Πιθανοί συνδυασμοί που υφίστανται μεταξύ ιδιοκτησίας της υποδομής (public / private) και δικαιωμάτων επί του μητρώου (permissioned / permissionless), συνοδευόμενη από ενδεικτικές εφαρμογές, αποτυπώνονται στην παρακάτω εικόνα.

Εικόνα 21: Τέσσερις βασικοί τύποι των blockchains και οι εφαρμογές του [38]

Κεφάλαιο 3ο - Η τεχνολογία blockchain

3.1 Blockchain – Εισαγωγή

Η τεχνολογία blockchain αποτελεί μια από τις πιο υποσχόμενες τεχνολογίες για την επόμενη γενιά συστημάτων αλληλεπίδρασης στο Διαδίκτυο. **Οι γνώσεις περί κρυπτογράφησης, η κατανόηση για το πως λειτουργούν οι ηλεκτρονικές συναλλαγές, η γνώση συστημάτων πληροφοριών και φυσικά ένα επιστημονικό υπόβαθρο πάνω στο software αλλά και στο hardware των υπολογιστικών συστημάτων, αποτελούν βασικά επιθυμητά προσόντα.**

Με την τεχνολογία blockchain τα ίδια δεδομένα καταγράφονται και διατηρούνται σε πολλαπλούς κόμβους (υπολογιστές συνδεδεμένους σε ένα δίκτυο) που μπορεί να είναι γεωγραφικά απομακρυσμένοι μεταξύ τους. Επιτρέπουν στους χρήστες του δικτύου να μεταφέρουν ελεύθερα και με ασφάλεια δεδομένα μεταξύ τους χωρίς την ανάγκη μίας εδραιωμένης σχέσης εμπιστοσύνης. Λειτουργικά, ένα blockchain μπορεί να χρησιμεύσει ως «ένα ανοιχτό, κατανεμημένο καθολικό», που μπορεί να καταγράψει τις συναλλαγές μεταξύ δύο μερών αποτελεσματικά και με επαληθεύσιμο και μόνιμο τρόπο.

Σε αυτή την ενότητα θα κάνουμε μια επισκόπηση τέτοιων τεχνολογιών, εστιάζοντας κυρίως σε τρείς διαφορετικές πλατφόρμες blockchain, όπως αυτές αναπτύχθηκαν σε βάθος χρόνου και ως επί το πλείστον προσφέρονται για την ανάπτυξη έξυπνων συμβολαίων.

3.2 Η πρώτη γενιά τεχνολογίας Blockchain v 1.0 (Bitcoin)

Η αποκέντρωση είναι ένα θεμελιώδες μέρος της έξυπνης λύσης που μας έδωσε το Bitcoin, το πρώτο ευρέως επιτυχημένο ψηφιακό νόμισμα. Η ιδέα του Nakamoto να δημιουργήσει ένα ηλεκτρονικό σύστημα πληρωμών, βασισμένο στη κρυπτογραφική επαλήθευση και όχι σε ένα έμπιστο τρίτο μέρος, τον οδήγησε στην πρώτη εφαρμογή της τεχνολογίας Blockchain, τα κρυπτονομίσματα (bitcoin), τα οποία και έχουν αναδειχθεί ως η πρώτη γενιά τεχνολογίας blockchain. Τα κρυπτονομίσματα είναι βασικά ψηφιακά νομίσματα που βασίζονται σε κρυπτογραφικές τεχνικές και peer-to-peer network.

Συγκεκριμένα, το Bitcoin είναι ένα ηλεκτρονικό σύστημα πληρωμών που επιτρέπει σε δύο μη αξιόπιστα μέρη να πραγματοποιούν συναλλαγές ψηφιακού χρήματος μεταξύ τους με ασφαλή τρόπο χωρίς να παρεμβάλλονται μεσάζοντες στην εν λόγω συναλλαγή. Προς επίρρωση των ενεργειών τους στο δίκτυο, αυτές επαληθεύονται από ειδικούς κόμβους (που ονομάζονται miners). Η επαλήθευση μιας συναλλαγής σημαίνει τον έλεγχο του αποστολέα και το περιεχόμενο της συναλλαγής. Οι miners δημιουργούν ένα νέο μπλοκ συναλλαγών μετά την επίλυση ενός μαθηματικού παζλ (που ονομάζεται Proof of Work) και στη συνέχεια διαδίδουν αυτό το μπλοκ στο δίκτυο.

Άλλοι κόμβοι στο δίκτυο μπορούν να επικυρώσουν την ορθότητα του παραγόμενου μπλοκ και να το αναπτύξουν μόνο εάν δημιουργήθηκε σωστά. Ωστόσο, το Bitcoin έχει περιορισμένες δυνατότητες προγραμματισμού για την υποστήριξη σύνθετων συναλλαγών και συνεπώς δεν υποστηρίζει τη δημιουργία σύνθετων κατανεμημένων εφαρμογών. Το Bitcoin είναι κυρίως μια δημόσια πλατφόρμα blockchain που μπορεί να χρησιμοποιηθεί για την επεξεργασία συναλλαγών κρυπτογράφησης, αλλά με πολύ περιορισμένη δυνατότητα υπολογισμού. Η δυνατότητα δημιουργίας έξυπνου συμβολαίου με πλούσια λογική χρησιμοποιώντας γλώσσα δέσμης ενεργειών Bitcoin είναι πολύ περιορισμένη. Η σύνταξη συμβολαίων με πολύπλοκη λογική δεν είναι δυνατή λόγω των περιορισμών της γλώσσας δέσμης ενεργειών Bitcoin.

3.3 Η δεύτερη γενιά τεχνολογίας Blockchain v 2.0 (Ethereum)

Με την πεποίθηση ότι η πλατφόρμα θα μπορούσε να γίνει πολύ ισχυρή γενικεύοντας πέρα από την απλή ανταλλαγή νομισμάτων σε κάτι που θα μπορούσε να εκτελέσει οποιονδήποτε τύπο επεξεργασίας, δημιουργήθηκε μια νέα γενιά blockchain (v2.0). Είναι αυτή η γενιά που επιτρέπει τα λεγόμενα έξυπνα συμβόλαια, (Smart Contracts), δηλαδή μικρά προγράμματα λογισμικού να εκτελούνται μέσα στο Blockchain (BC). Το πιο διακεκριμένο BC 2.0 είναι αυτό του Ethereum, που δόθηκε στη δημοσιότητα στις 30 Ιουλίου 2015 από τον Vitalik Buterin.

Το Ethereum είναι ένα δημόσιο blockchain με ενσωματωμένη γλώσσα Turing που επιτρέπει τη σύνταξη έξυπνης σύμβασης και αποκεντρωμένης εφαρμογής. Το Ethereum επίσης δεν ελέγχεται από κάποια κεντρική αρχή, αλλά είναι μια πλατφόρμα ανοιχτού κώδικα. Κάθε μπλοκ διατηρείται και ενημερώνεται από πολλούς κόμβους, που είναι συνδεδεμένοι στο δίκτυο. Στην καρδιά του Ethereum βρίσκεται η εικονική μηχανή Ethereum Virtual Machine (EVM), η οποία μπορεί να εκτελέσει κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας. Κάθε κόμβος του δικτύου χρησιμοποιεί την EVM και εκτελεί ακριβώς τις ίδιες οδηγίες με τους υπόλοιπους κόμβους. Ο μηχανισμός που χρησιμοποιείται για την επικύρωση των καινούργιων μπλοκ είναι βασισμένος στο μοντέλο Proof-of-Work. Δηλαδή, και σε αυτή τη περίπτωση το κίνητρο των miners για την παροχή της επεξεργαστικής τους ισχύος και την εξόρυξη των μπλοκ είναι οικονομικό, όμως όχι σε bitcoin, αλλά στο λεγόμενο "gas", του οποίου η αξία είναι εκφρασμένη σε 'ether' (το αντίστοιχο κρυπτονόμισμα).

Ήδη από το 1994, ο Nick Szabo, επιστήμονας υπολογιστών και νομικός, δημιούργησε τον όρο *«έξυπνο συμβόλαιο»* και το όρισε ως: *« Ένα έξυπνο συμβόλαιο είναι ένα ηλεκτρονικό πρωτόκολλο συναλλαγών που εκτελεί τους όρους μιας σύμβασης »*. Προγράμματα υπολογιστών που τρέχουν στην πλατφόρμα Ethereum ονομάζονται έξυπνα συμβόλαια. Μπορούν να επιβάλουν συγκεκριμένους τύπους συμφωνιών μεταξύ των μερών, όπως ένα μηχάνημα αυτόματης πώλησης, αλλά δεν έχουν εγγενώς άμεση σχέση με τις νομικές συμβάσεις. Το έξυπνο συμβόλαιο Ethereum έγινε τόσο δημοφιλές που η έκδοση Ethereum ενός έξυπνου συμβολαίου έκλεισε την αρχική χρήση του όρου και πρόσθεσε μεγάλη σύγχυση ως προς το τι μπορεί να κάνει το blockchain. Γιατί είναι «σύμβαση»; Η αρχική ιδέα ήταν ότι αποτελούσε κάποιο είδος συμφωνίας μεταξύ των μερών. Γιατί είναι «έξυπνο»; Η αρχική ιδέα ήταν ότι θα μπορούσε να εκτελεστεί χωρίς την

ανάγκη συμμετοχής δικηγόρων ή άλλων ατόμων. Τι είναι λοιπόν ένα έξυπνο συμβόλαιο; Δεδομένου ότι η Ethereum ανακηρύχθηκε «αποκεντρωμένη πλατφόρμα που εκτελεί έξυπνα συμβόλαια», πραγματικά αναφέρεται μόνο σε έναν ειδικό τύπο προγράμματος λογισμικού. Καθίσταται σαφές ότι ανεξάρτητα εάν μπορεί να έχει ή να μην έχει νομικές επιπτώσεις, χρειάζεται ακόμη ένα παραδοσιακό νομικό πλαίσιο γύρω του, εάν πρέπει να χρησιμοποιηθεί ως μέρος μιας νομικής συναλλαγής.

3.4 Το Hyperledger Fabric

Το Hyperledger είναι ένα Project του Linux Foundation που ξεκίνησε το 2015, όταν πολλές επιχειρήσεις που ενδιαφέρονταν για την τεχνολογία του blockchain αποφάσισαν ότι θα ήταν προτιμότερο να ενώσουν τις δυνάμεις τους με σκοπό να παράγουν ένα open-source blockchain που θα μπορούσε να χρησιμοποιείται από τον καθένα.

Το Hyperledger Fabric είναι μια πλατφόρμα ανοιχτής πηγής τεχνολογίας κατανεμημένου καθολικού (DLT), σχεδιασμένη για χρήση σε εταιρικά πλαίσια, η οποία παρέχει ορισμένες βασικές δυνατότητες διαφοροποίησης σε σχέση με άλλες δημοφιλείς κατανεμημένες καθολικές ή πλατφόρμες blockchain.

Ένα βασικό σημείο διαφοροποίησης είναι ότι το Hyperledger ιδρύθηκε υπό το Ίδρυμα Linux, το οποίο το ίδιο έχει μια μακρά και πολύ επιτυχημένη ιστορία καλλιέργειας έργων ανοιχτού κώδικα.

Το Fabric έχει μια εξαιρετικά **αρθρωτή** και **διαμορφώσιμη** αρχιτεκτονική, επιτρέποντας την καινοτομία, την ευελιξία και τη βελτιστοποίηση για ένα ευρύ φάσμα περιπτώσεων χρήσης της βιομηχανίας, συμπεριλαμβανομένων τραπεζών, χρηματοοικονομικών, ασφαλίσεων, υγειονομικής περίθαλψης, ανθρώπινου δυναμικού ή και αλυσίδας εφοδιασμού. Το Fabric είναι η πρώτη πλατφόρμα κατανεμημένου καθολικού που υποστηρίζει **έξυπνα συμβόλαια που συντάσσονται σε γλώσσες προγραμματισμού γενικής χρήσης** , όπως Java, Go και Node.js, αντί για περιορισμένες γλώσσες για συγκεκριμένους τομείς (DSL)[6]. Αυτό σημαίνει ότι οι περισσότερες επιχειρήσεις διαθέτουν ήδη το σύνολο δεξιοτήτων που απαιτούνται για την ανάπτυξη έξυπνων συμβάσεων και δεν απαιτείται πρόσθετη εκπαίδευση για να μάθουν μια νέα γλώσσα ή DSL.

Μέσω της πλατφόρμας Fabric **επιτρέπεται** επίσης, σε αντίθεση με ένα δημόσιο δίκτυο χωρίς άδεια, οι συμμετέχοντες είναι γνωστοί ο ένας στον άλλο, αντί για ανώνυμους και ως εκ τούτου πλήρως αναξιόπιστοι. Αυτό σημαίνει ότι ενώ οι συμμετέχοντες μπορεί να μην εμπιστεύονται πλήρως ο ένας τον άλλον (μπορεί, για παράδειγμα, να είναι ανταγωνιστές στον ίδιο κλάδο), ένα δίκτυο μπορεί να λειτουργήσει υπό ένα μοντέλο διακυβέρνησης που είναι βασισμένο σε ένα πλαίσιο όπου υπάρχει εμπιστοσύνη μεταξύ των συμμετεχόντων, όπως νομική συμφωνία ή πλαίσιο για τη διαχείριση διαφορών.

[6] Ο όρος **Digital Subscriber Line (Ψηφιακή Συνδρομητική Γραμμή)** ή **DSL** ή **xDSL** περιγράφει μια οικογένεια τεχνολογιών που παρέχουν μετάδοση δεδομένων πάνω από το παραδοσιακά τηλεφωνικά καλώδια. Πηγή : https://el.wikipedia.org/wiki/DSL

Το πιο σημαντικό του χαρακτηριστικό που το διαφοροποιεί από τις άλλες πλατφόρμες είναι η υποστήριξή του σε **πρωτοποριακά πρωτόκολλα** που μπορούν να **ενσωματωθούν,** τα οποία επιτρέπουν στην πλατφόρμα να προσαρμόζεται πιο αποτελεσματικά ώστε να ανταποκρίνεται συγκεκριμένες περιπτώσεις χρήσης και μοντέλα εμπιστοσύνης.

Για παράδειγμα, όταν αναπτύσσεται σε μια μεμονωμένη επιχείρηση ή λειτουργεί από μια αξιόπιστη αρχή, το Fabric μπορεί να αξιοποιήσει πρωτόκολλα συναίνεσης που **δεν απαιτούν εγγενή κρυπτογράφηση,** για να τροφοδοτήσουν την έξυπνη εκτέλεση συμβολαίου. Η αποφυγή κρυπτογράφησης μειώνει ορισμένους σημαντικούς φορείς κινδύνου / επίθεσης και η απουσία κρυπτογραφικών εξορυκτικών λειτουργιών σημαίνει ότι η πλατφόρμα μπορεί να αναπτυχθεί με περίπου το ίδιο λειτουργικό κόστος σε σύγκριση με οποιοδήποτε άλλο κατανεμημένο σύστημα.

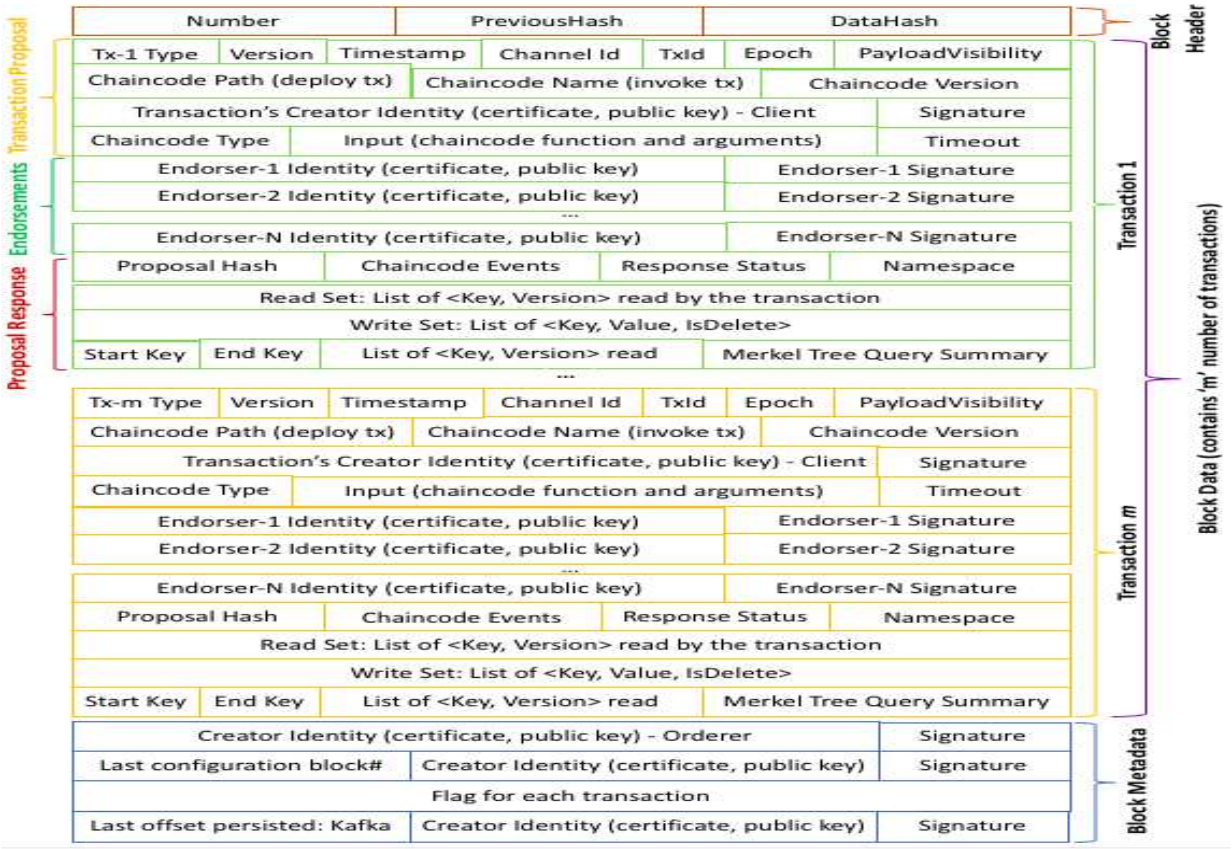
Επιπροσθέτως, τα κανάλια (τα λεγόμενα channels) επιτρέπουν στους συμμετέχοντες να σχηματίζουν εικονικές ομάδες και να διατηρούν τα ανεξάρτητα καθολικά τους, που είναι αόρατα από άλλα κανάλια. Τα κανάλια παρέχουν την ευελιξία για την κοινοπραξία επιχειρήσεων, να μοιράζονται με ασφάλεια πληροφορίες, μόνο με σχετικά μέρη.

Ο συνδυασμός αυτών των διαφοροποιημένων σχεδιαστικών δυνατοτήτων καθιστά το Fabric μία από τις **πλατφόρμες με την καλύτερη απόδοση που** διατίθενται σήμερα, τόσο από την άποψη της επεξεργασίας των συναλλαγών όσο και από τον χρόνο/ταχύτητα επιβεβαίωσης των συναλλαγών, ενώ επιτρέπει την **προστασία της ιδιωτικής ζωής και της εμπιστευτικότητας** των συναλλαγών και των έξυπνων συμβάσεων. Τα δε Έξυπνα συμβόλαια («αλυσίδα») εκτελούνται σε εξωτερικό περιβάλλον. Μπορούν να γραφούν σε τυπικές γλώσσες προγραμματισμού, αλλά δεν έχουν άμεση πρόσβαση στην κατάσταση του καθολικού.

Το Hyperledger καλύπτει ένα πλήρες φάσμα περιπτώσεων χρήσης, καθώς τα διαφορετικά σενάρια των διαφορετικών επιχειρήσεων που συμμετέχουν στην υλοποίηση του δημιουργούν διαφορετικές απαιτήσεις για τους χρόνους επικύρωσης, την αποκέντρωση, την εμπιστοσύνη και άλλα ζητήματα. Για να καλυφθεί το σύνολο των αναγκών των συμμετεχόντων στο Hyperledger, έχουν αναπτυχθεί διαφορετικά frameworks[7] και εργαλεία που βασίζονται σε αυτό. Ένα έξυπνο συμβόλαιο, ή αυτό που το Fabric αποκαλεί **«chaincode»**, λειτουργεί ως μια αξιόπιστη κατανεμημένη εφαρμογή που αποκτά την ασφάλεια / εμπιστοσύνη της από το blockchain. Είναι η επιχειρηματική λογική μιας εφαρμογής blockchain.

Συνεπώς, είτε πρόκειται για συναίνεση, πρωτόκολλα διαχείρισης ταυτότητας, πρωτόκολλα διαχείρισης κλειδιών ή κρυπτογραφικές βιβλιοθήκες, η πλατφόρμα έχει σχεδιαστεί στον πυρήνα της ώστε να ανταποκρίνεται στην ποικιλία των απαιτήσεων **περίπτωσης εταιρικής χρήσης.**

[7] Η δομή - η ρύθμιση και οι σχέσεις μεταξύ των τμημάτων ή των στοιχείων ενός περίπλοκου εγχειρήματος. Πηγή : https://el.opentran.net/



Εικόνα 22: Δομή του block του Hyperledger Fabric

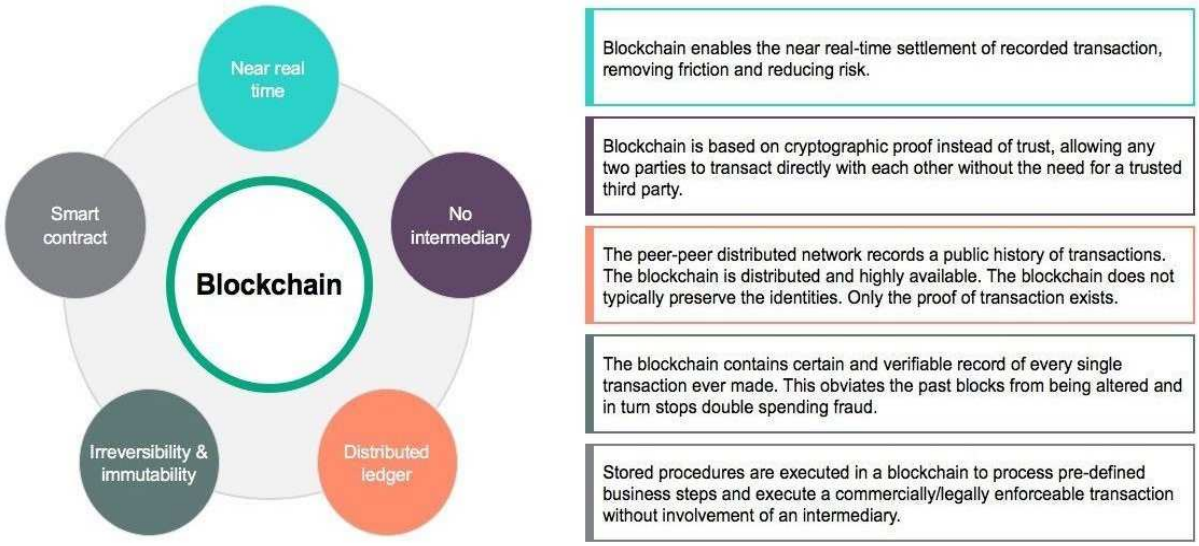
3.5 Κοινά χαρακτηριστικά των πλατφορμών blockchain

- **Αποκέντρωση.** Σε συμβατικά κεντρικά συστήματα συναλλαγών, κάθε συναλλαγή πρέπει να επικυρώνεται μέσω ενός αρμόδιου τρίτου φορέα ή επιχείρησης, κάτι το οποίο συνεπάγεται κόστος και μειωμένη απόδοση πόρων από τους κεντρικούς διακομιστές. Μια συναλλαγή στο δίκτυο blockchain μπορεί να πραγματοποιηθεί μεταξύ δύο ομότιμων δικτύων (P2P) χωρίς τον έλεγχο ταυτότητας από την κεντρική υπηρεσία.

- **Ανθεκτικότητα.** Δεδομένου ότι κάθε μία από τις συναλλαγές που διαδίδονται σε ολόκληρο το δίκτυο πρέπει να επιβεβαιωθεί και να καταγραφεί σε μπλοκ που διανέμονται σε ολόκληρο το δίκτυο, είναι σχεδόν αδύνατο να παραβιαστεί. Κάθε μπλοκ που μεταδίδεται επικυρώνεται από άλλους κόμβους και έτσι ελέγχονται οι συναλλαγές, με αποτέλεσμα να καθίσταται δύσκολη η οποιαδήποτε παραβίαση.

- **Ανωνυμία.** Κάθε χρήστης μπορεί να αλληλεπιδράσει με το δίκτυο blockchain με μια κρυπτογραφημένη διεύθυνση. Δεν υπάρχει κεντρικό μέρος που να διατηρεί τις προσωπικές πληροφορίες των χρηστών.

- **Επαλήθευση**. Δεδομένου ότι κάθε μία από τις συναλλαγές στο blockchain επικυρώνεται και καταγράφεται με χρονική σήμανση, οι χρήστες μπορούν εύκολα να επαληθεύσουν και να εντοπίσουν τις προηγούμενες εγγραφές μέσω της πρόσβασης σε οποιονδήποτε κόμβο στο κατανεμημένο δίκτυο. Το γεγονός αυτό βελτιώνει την ιχνηλασιμότητα και τη διαφάνεια των δεδομένων που είναι αποθηκευμένα στο blockchain



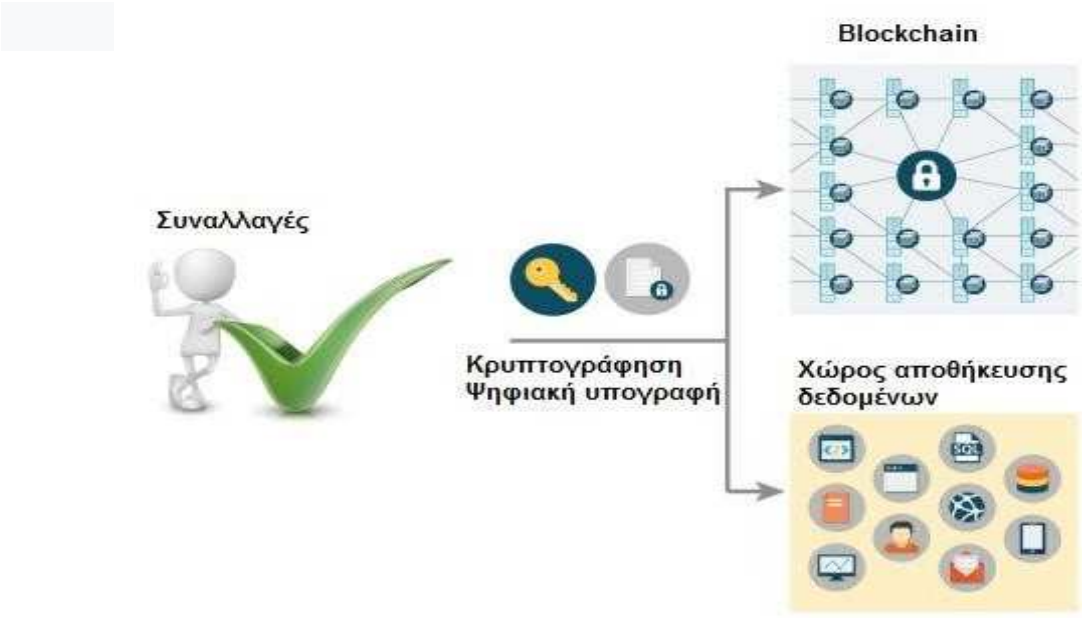
Εικόνα 23: Κοινά χαρακτηριστικά πλατφορμών blockchain [44]

3.6 Επισκόπηση διαδικασίας συναλλαγών blockchain

Οι συναλλαγές Blockchain αποθηκεύονται σε έναν υπολογιστή, που συνήθως αναφέρεται ως κόμβος. Οι δημοφιλείς πλατφόρμες blockchain έχουν δεκάδες χιλιάδες κόμβους που λειτουργούν ανά πάσα στιγμή.

- ✓ Κάθε κόμβος αποθηκεύει ένα πανομοιότυπο αντίγραφο όλων των εγγραφών των συναλλαγών. Ο κόμβος που επικυρώνει την επόμενη παρτίδα συναλλαγών, που αναφέρεται ως μπλοκ, ονομάζεται κόμβος εξόρυξης.
- ✓ Τα μπλοκ με τη σειρά τους επικυρώνονται από κάθε κόμβο εξόρυξης.
- ✓ Κάθε κόμβος στο δίκτυο αποθηκεύει ένα αντίγραφο όλου του λογισμικού , δεδομένα, υπόλοιπα λογαριασμών και κατάσταση συναλλαγής.
- ✓ Οι συναλλαγές μεταδίδονται μέσω Διαδικτύου μεταξύ κόμβων με τρόπο peer-to-peer.
- ✓ Η εξόρυξη αναφέρεται στην εικασία της λύσης σε ένα μαθηματικό πρόβλημα (μοναδικό για την ομάδα συναλλαγών) που δεν μπορεί να υπολογιστεί άμεσα. Ως εκ τούτου η εξόρυξη είναι επίσης γνωστή ως απόδειξη της εργασίας (PoW).
- ✓ Το μπλοκ εξόρυξης διανέμεται πίσω στο δίκτυο μέσω του Διαδικτύου και κάθε κόμβος θα επαληθεύει όλες τις περιλαμβανόμενες συναλλαγές πριν την αποδεχθεί
- ✓ Τελικά όλοι οι κόμβοι θα αποθηκεύσουν ένα αντίγραφο της κατάστασης του συστήματος που όλοι συμφωνούν.

Με αυτόν τον τρόπο, δεν είναι τόσο κατανεμημένος υπολογιστής όπως θα σκεφτόταν κανείς με την παραδοσιακή έννοια. Μοιάζει περισσότερο με έναν υπολογιστή με πολλούς κλώνους οι οποίοι λειτουργούν παράλληλα και αποθηκεύουν τις ίδιες πληροφορίες για να βεβαιωθεί ότι κανείς δεν θα εξαπατηθεί.



Εικόνα 24: Δομή blockchain εφαρμογής

3.7 Πλεονεκτήματα τεχνολογίας blockchain

- **Αυτονομία**

  Δύο μέρη είναι σε θέση να κάνουν μια συναλλαγή χωρίς την επίβλεψη ή την διαμεσολάβηση ενός τρίτου μέρους.

- **Εξουσιοδοτημένοι χρήστες**

  Οι χρήστες έχουν τον έλεγχο όλων των πληροφοριών και των συναλλαγών τους.

- **Υψηλής ποιότητας δεδομένα**

  Τα blockchain δεδομένα είναι πλήρη, έγκαιρα, ακριβή και ευρέως διαθέσιμα.

- **Αξιοπιστία**

  Λόγω των αποκεντρωμένων δικτύων, το blockchain είναι λιγότερο επισφαλές σε κακόβουλες επιθέσεις.

- **Ακεραιότητα της διαδικασίας**

  Οι χρήστες μπορούν να εμπιστευθούν ότι οι συναλλαγές θα εκτελούνται όπως ακριβώς ορίζουν οι εντολές του πρωτοκόλλου, καταργώντας την ανάγκη για ένα έμπιστο τρίτο μέρος.

- **Διαφάνεια και αμεταβλητότητα**

  Οι αλλαγές στο δημόσιο blockchain είναι ορατές στο κοινό από όλα τα μέρη δημιουργώντας διαφάνεια, καθώς και όλες οι συναλλαγές είναι αμετάβλητες, που σημαίνει ότι δεν μπορούν να τροποποιηθούν ή να διαγραφούν.

- **Απλούστευση**

  Όλες οι συναλλαγές προστίθενται σε ένα ενιαίο δημόσιο καθολικό (ledger), μειώνοντας έτσι την ακαταστασία και τις επιπλοκές των πολλαπλών ledgers (καθολικών).

- **Ταχύτερες συναλλαγές**

  Οι συναλλαγές πχ σε μία τράπεζα μπορεί ενδεχομένως να χρειαστούν μέρες για την εκκαθάριση και τελική διευθέτηση, ιδίως εκτός του ωραρίου εργασίας. Οι blockchain συναλλαγές μπορούν να μειώσουν το χρόνο συναλλαγής σε λεπτά.

- **Χαμηλότερο κόστος συναλλαγών**

  Με την εξάλειψη των μεσαζόντων τρίτων μειώνονται σημαντικά τα έξοδα συναλλαγής.

3.8 Μειονεκτήματα τεχνολογίας blockchain

- **Εκκολαπτόμενη τεχνολογία**

  Η επίλυση των προκλήσεων όπως η ταχύτητα των συναλλαγών, η διαδικασία επαλήθευσης, και τα όρια των δεδομένων θα είναι καθοριστικής σημασίας στο να γίνει το blockchain ευρέως εφαρμόσιμο.

- **Αβέβαιο ρυθμιστικό καθεστώς**

  Εφόσον παραμένει ακαθόριστο το ρυθμιστικό πλαίσιο της Κυβέρνησης σχετικά με τη νέα τεχνολογία, η ευρεία υιοθέτησή της γίνεται ακόμα πιο δυσχερής

- **Μεγάλη κατανάλωση ενέργειας**

  Οι miners του blockchain για το δίκτυο Bitcoin επιχειρούν 450.000 τρισεκατομμύρια λύσεις ανά δευτερόλεπτο για την επικύρωση των συναλλαγών, χρησιμοποιώντας σημαντικές ποσότητες ενέργειας του υπολογιστή.

- **Έλεγχος, ασφάλεια και προστασία της ιδιωτικότητας**

  Ενώ υπάρχουν λύσεις, συμπεριλαμβανομένων των ιδιωτικών blockchain και ισχυρή κρυπτογράφηση, εξακολουθούν να υπάρχουν ανησυχίες στον κυβερνοχώρο για την ασφάλεια, που πρέπει να αντιμετωπιστούν πριν το ευρύ κοινό αναθέσει τα προσωπικά του δεδομένα σε ένα blockchain.

- **Ανησυχίες ενσωμάτωσης**

  Οι blockchain εφαρμογές προσφέρουν λύσεις που απαιτούν σημαντικές αλλαγές, ή την πλήρη αντικατάσταση των υπαρχόντων συστημάτων. Για να πραγματοποιηθούν αυτές οι αλλαγές, οι

εταιρείες πρέπει να καταστρώσουν σχέδια στρατηγικής για την μετάβαση.

- **Αλλαγή πορείας**

  Το blockchain αντιπροσωπεύει μια πλήρη στροφή προς ένα αποκεντρωμένο δίκτυο που απαιτεί την συμφωνία μεταξύ των χρηστών και των φορέων της.

- **Κόστος**

  Το blockchain προσφέρει τεράστια εξοικονόμηση του κόστους, των συναλλαγών και του χρόνου, αλλά το υψηλό αρχικό κόστος κεφαλαίου θα μπορούσε να αποτελέσει αποτρεπτικό παράγοντα.

3.9 Διαδεδομένες εφαρμογές blockchain

Παρακάτω παρατίθενται οι πιο γνωστές εφαρμογές που βασίζουν τη λειτουργία τους στο blockchain και που προσφέρουν νέες προσεγγίσεις σε συναλλαγές και δραστηριότητες της καθημερινότητας.

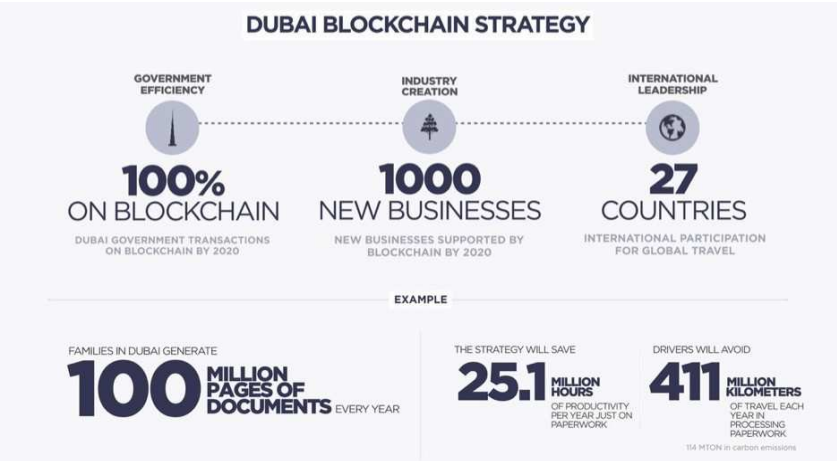
- **Ripple για Τραπεζικές Συναλλαγές**

  Το RippleNet, ή εν συντομία το Ripple, είναι ένα αποκεντρωμένο ιδιωτικό δίκτυο συναλλαγών το οποίο απευθύνεται σε τράπεζες και άλλους παρόχους υπηρεσιών μεταφοράς χρημάτων με στόχο την διεκπεραίωση των συναλλαγών αυτών εύκολα και γρήγορα. Η πλατφόρμα αυτή έχει σχεδιαστεί για την εκτέλεση γρήγορων τραπεζικών συναλλαγών χωρίς γεωγραφικούς ή άλλους οικονομικούς περιορισμούς. Ως «καύσιμο» χρησιμοποιεί το ομώνυμο νόμισμα Ripple (XRP).

Εικόνα 25: Το λογότυπο της εταιρίας Ripple [ripple.com]

- **Smart Dubai Blockchain για Πολιτική και Διακυβέρνηση**

  Με τη χρήση του blockchain το Dubai εξασφαλίζει την απεξάρτησή του από τα έντυπα δημόσια έγγραφα και έχει καταφέρει να ενοποιήσει πάνω από 20 διαφορετικές κρατικές υπηρεσίες στον τομέα της ταυτοποίησης των πολιτών και της καταγραφής των συναλλαγών τους.



Εικόνα 26: Η στρατηγική του Dubai για το blockchain σε νούμερα [xstrategy.ae]

- **Ubitquity για Αγορά Ακινήτων**

Η εταιρία ιδρύθηκε το 2015 στις Ηνωμένες Πολιτείες της Αμερικής και είχε ως στόχο τη δημιουργία μιας πλατφόρμας στην οποία θα μπορούν να καταγράφονται με ασφάλεια οι τίτλοι ιδιοκτησίας ακινήτων καθώς και ο συναλλαγές που σχετίζονται με αυτούς. Στην πλατφόρμα αυτή οι πελάτες της εταιρίας διατηρούν πλήρη και ενημερωμένα μητρώα ιδιοκτησίας ακινήτων, μειώνοντας το χρόνο που απαιτείται. Είναι συμβατή ακόμη και με υβριδικά δίκτυα στα οποία υπάρχουν πολλαπλές προσβάσεις και ελέγχονται από μία κεντρική ρυθμιστική αρχή.

Εικόνα 27: Το λογότυπο της Ubitquity [ubitquity.io]

- **OpenLaw για Νομικές Υπηρεσίες**

Η OpenLaw με τη χρήση των smart contracts, έχει δημιουργήσει μια δική της μορφή γλώσσας markup[8], η οποία είναι ικανή να αποτυπώσει στο blockchain οποιοδήποτε νομικό έγγραφο, διατηρώντας το αμετάβλητο και καταγράφοντας τη χρονική στιγμή της καταχώρησής του. Το πρότυπο αυτό έχει το μεγαλύτερο μέρος του κειμένου προσυμπληρωμένο, ενώ ο χρήστης της εφαρμογής χρειάζεται να συμπληρώσει μόνο τα στοιχεία που καθιστούν το συμβόλαιο μοναδικό. Όταν όλα τα πεδία έχουν συμπληρωθεί, τότε το πρόχειρο μετατρέπεται σε smart contract, το οποίο αποστέλλεται στους συμβαλλόμενους για υπογραφές και μετά την υπογραφή του καταγράφεται στο blockchain του Ethereum, θέτοντας το συμβόλαιο σε ισχύ.

Εικόνα 28 : Το λογότυπο της OpenLaw [openlaw.io]

- **Yantha για Διαμοιρασμό Διαδρομών**

Η Yantha είναι μία πλατφόρμα διαμοιρασμού διαδρομών με στόχο την κοινή χρήση αυτοκινήτων από πολλούς ανθρώπους για την ίδια ή παραπλήσια διαδρομή, αποτρέποντας την ανάγκη για διαρκή χρήση του GPS κινητών συσκευών αλλά και διατηρώντας τα δεδομένα της εφαρμογής ασφαλή και άμεσα προσβάσιμα μόνο από τα εμπλεκόμενα άτομα στη συναλλαγή.

[8] Η **γλώσσα σήμανσης** (αγγλικά: *markup language*) παρέχει τη δυνατότητα να υποσημειώσουμε ένα κείμενο κατά αντιστοιχία με τον παραδοσιακό τρόπο όπου με μπλε στυλό υποσημειώναμε ένα κείμενο προσθέτοντας πληροφορίες για τη σημασιολογία του ή παραπομπές σε άλλες σχετικές πηγές κτλ. Πηγή : https://el.wikipedia.org/wiki

Εικόνα 29: Το λογότυπο της πλατφόρμας Yantha [yantha.com]

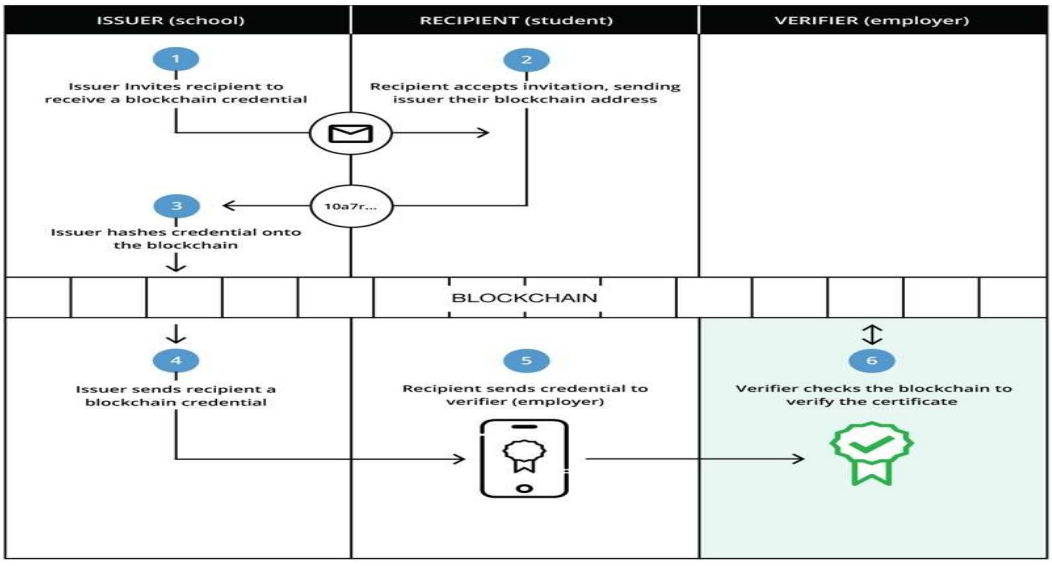
- **HireGo για Ενοικίαση Οχημάτων**

Το HireGo είναι μία εφαρμογή που αποσκοπεί στην ασφαλή ενοικίαση οχημάτων που ανήκουν σε εταιρίες ή ιδιώτες μέσω της καταγραφής των συναλλαγών ενοικίασης στο Ethereum Blockchain. Οι χρήστες της εφαρμογής μπορούν (χρησιμοποιώντας μία εφαρμογή στο κινητό τους τηλέφωνο) να εντοπίζουν οχήματα διαθέσιμα προς ενοικίαση στην περιοχή που βρίσκονται και να προχωρούν στην άμεση ενοικίαση και χρήση αυτών, χωρίς την αναγκαιότητα ύπαρξης ενδιάμεσου και χωρίς γραφειοκρατικές διαδικασίες. Με τη χρήση τεχνολογιών του Internet of Things, τα διασυνδεδεμένα διαθέσιμα οχήματα μπορούν να ξεκλειδώνουν και να ενεργοποιούνται με τη χρήση της εφαρμογής HireGo, τη στιγμή που τα χρειάζεται ο ενδιαφερόμενος και αφού ολοκληρώσει την πληρωμή.

Εικόνα 30: Το λογότυπο της εφαρμογής HireGo [hirego.io]

- **Blockcerts για την Εκπαίδευση**

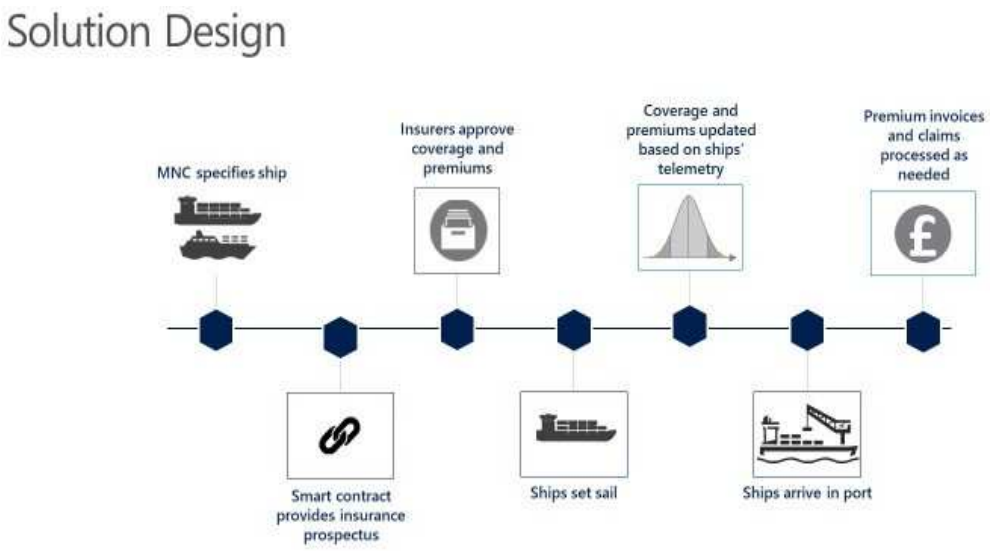
Το Blockcerts είναι ένα ανοιχτό πρότυπο για τη δημιουργία, την έκδοση, την προβολή και την υπογραφή πιστοποιητικών βασισμένο στο blockchain. Κάθε πιστοποιητικό καταγράφεται στο blockchain και η υπογραφή του κρυπτογραφείται ψηφιακά ώστε να είναι δυνατός ο διαμοιρασμός του και το περιεχόμενό του να παραμένει αναλλοίωτο. Στόχος της εφαρμογής είναι να αποτελέσει μία καινοτόμα λύση μεταξύ των ανθρώπων ώστε να μπορούν να διατηρούν τα δικά τους αυθεντικά πιστοποιητικά σε μία διαχρονική βάση δεδομένων.



Εικόνα 31: Η διαδικασία έκδοσης και επαλήθευσης πιστοποιητικού στο Blockcerts [blockcerts.org]

- **Insurwave για Ασφάλεια Θαλάσσιων Μεταφορών**

Η εφαρμογή χρησιμοποιεί το blockchain και την τεχνολογία της αποκεντρωμένης αποθήκευσης του Microsoft Azure για την καταγραφή αυτοματοποιημένων συναλλαγών μεταξύ εμπορικών πλοίων. Συνδέοντας τους συμμετέχοντες σε ένα ασφαλές ιδιωτικό δίκτυο το οποίο διατηρεί πλήρες κατάστιχο των συναλλαγών και των διαδικασιών που εκτελούνται για την διεκπεραίωση τους, η πλατφόρμα αποτελεί την πρώτη εφαρμογή ψηφιακής ασφάλισης αξιών



Εικόνα 32: Η λύση του Insurwave [customers.microsoft.com]

- **Alice για Διαχείριση Δωρεών – Φιλανθρωπικοί Οργανισμοί**

Το Alice είναι ένα αποκεντρωμένο δίκτυο βασισμένο στο Ethereum με έντονο κοινωνικό αντίκτυπο. Βοηθάει κοινωνικούς οργανισμούς να εκτελούν διάφορα φιλανθρωπικά έργα με απόλυτη διαφάνεια, χρησιμοποιώντας τη λογική των smart contracts του Ethereum για την καταγραφή και την εύκολη πρόσβαση του κοινού στο σύνολο των συναλλαγών που εκτελούνται στα πλαίσια της δράσης τους. Η χρηματοδότηση των ενεργειών αυτών γίνεται μέχρι ένα αρχικό ποσό για όλους τους συμμετέχοντες στην πλατφόρμα και στη συνέχεια, μόνο αν είναι εφικτή η απόδειξη της επίτευξης των αρχικών στόχων δικαιούνται επιπλέον χρηματοδότηση.

Εικόνα 33: Το λογότυπο του Alice [alice.si]

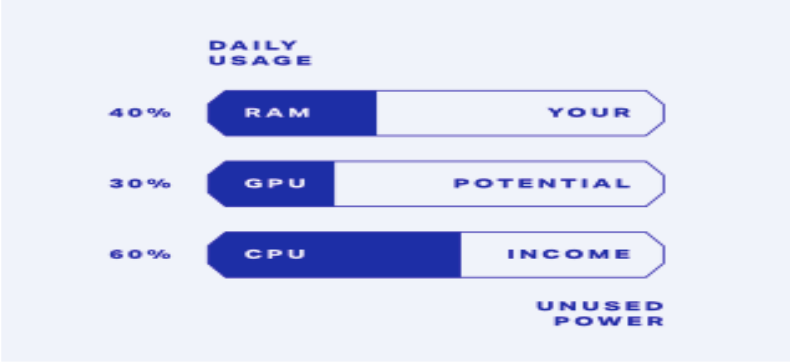
- **Storj για Αποθηκευτικό Χώρο**

Το Storj είναι μία αποκεντρωμένη λύση αποθηκευτικού χώρου βασισμένη σε λογισμικό ανοικτού κώδικα και στην πλατφόρμα του Ethereum. Στόχος της πλατφόρμας είναι η δημιουργία ενός αποκεντρωμένου δικτύου διαμοιρασμού αποθηκευτικού χώρου, όπου το κόστος θα είναι μικρότερο για τους χρήστες και η ταχύτητα ανάκτησης και λήψης των αρχείων τους μεγαλύτερη από τις συμβατικές υπηρεσίες, καθώς οι τελευταίες είναι περιορισμένες ανάλογα με τις δυνατότητες των data centers[9] τους. Επιπλέον της οικονομίας και της ταχύτητας, το Storj επιδιώκει την πλήρη ιδιωτικότητα στην πρόσβαση των αρχείων του κάθε χρήστη, καθώς χρησιμοποιεί μεθόδους και τεχνικές κρυπτογράφησης τόσο στα αρχεία, όσο και στην αποθήκευση των συναλλαγών στο blockchain στο οποίο βασίζεται.

Εικόνα 34: Το λογότυπο του Storj App [storj.io]

- **Golem για Υπολογιστική Ισχύ**

Το Golem είναι ο πρώτος αποκεντρωμένος υπολογιστής, σύμφωνα με την ομώνυμη εταιρία, καθώς βασίζεται στην αχρησιμοποίητη υπολογιστική ισχύ των χρηστών που έχουν εγκατεστημένη την εφαρμογή στους υπολογιστές τους για τη δημιουργία ενός παγκόσμιου υπερυπολογιστή προς ενοικίαση. Ο υπερυπολογιστής αυτός αντλεί την ισχύ του από τους αχρησιμοποίητους υπολογιστικούς πόρους των συμμετεχόντων στο δίκτυο peer—to—peer που έχει δημιουργηθεί για να συνδέονται οι «δότες» με τους «λήπτες» υπολογιστικής ισχύος.



Εικόνα 35: Η υπολογιστική ισχύς του δικτύου Golem [golem.network]

[9] **Κέντρο δεδομένων** (αγγλικά: data center) είναι ένα κτίριο ή ένας χώρος μέσα σε ένα κτίριο στο οποίο φιλοξενούνται υπολογιστές, αλλά και τηλεπικοινωνιακές και αποθηκευτικές υποδομές. Πηγή : https://el.wikipedia.org/wiki

Κεφάλαιο 4ο - Τα έξυπνα συμβόλαια

4.1 Οι εφαρμογές των smart contracts - Η κρυμμένη νομική πτυχή τους

Vebra volant, scripta manent – τα λόγια πετούν, τα γραπτά μένουν έλεγαν οι Ρωμαίοι. Προφανώς υπάρχει η ανάγκη για γραπτή αποτύπωση των συμφωνηθέντων ώστε να μειωθεί η ανασφάλεια, που δημιουργεί η έλλειψή της. Κι ενώ το «χαρτί» - έγγραφο έχει χάσει σταδιακά την αξία του, έχει καταγραφεί ως θεμελιώδες στο υποσυνείδητο των περισσότερων. Η καταγραφή των όποιων δεσμεύσεων σε ψηφιακή μορφή δημιούργησαν τα έξυπνα συμβόλαια, μια μορφή ψηφιακής συμφωνίας, με τη γραπτή συμφωνία όμως να παραμένει και να παρουσιάζεται απλά σε ηλεκτρονική μορφή. Η ουσία και η εκτέλεση των συμφωνιών εξαρτώνται από τον ανθρώπινο παράγοντα. Ένα συμβόλαιο μεταφράζεται ως μια αξιόπιστη συναλλαγή. Μια νομικά εκτελεστή σύμβαση επιτρέπει στα μέρη να συντονίζουν τις ενέργειές τους και να εμπιστεύονται ότι οι δεσμεύσεις μεταξύ τους θα εκπληρωθούν.

Οι έξυπνες συμβάσεις είναι ένα μέσο ενσωμάτωσης συμβατικών ρητρών σε ψηφιακά στοιχεία. Η λειτουργία των smart contracts δύσκολα μπορεί να αποσυνδεθεί από το blockchain, αφού μέσω της τεχνολογίας αυτής λειτουργούν ιδανικά. Συγκεκριμένα είναι ένας εκτελέσιμος κώδικας που τρέχει πάνω στο blockchain για να διευκολύνει, να εκτελεί και να επιβάλλει μια συμφωνία μεταξύ μη αξιόπιστων μερών, χωρίς τη συμμετοχή ενός αξιόπιστου τρίτου μέρους. Ο κεντρικός μεσάζοντας εκτελεί χρέη θεματοφύλακα της εμπιστοσύνης για την ασφάλεια της συναλλαγής. Η απουσία ενδιάμεσου που θα επωμίζονταν τον έλεγχο εκτέλεσης των όρων αλλά και τους όρους καθαυτούς της σύμβασης, δημιουργεί την πεποίθηση ότι ο Κώδικας είναι νόμος και ότι δεν απαιτείται η διενέργεια νομικών διαδικασιών, όπως είναι η επικύρωση της πιστότητας και της εγκυρότητας των καταγεγραμμένων στον κώδικα όρων. Εκτελείται αυτομάτως όταν οι ενσωματωμένοι όροι της πληρωθούν. Άλλωστε απώτερος στόχος είναι να ελαττωθούν οι κακόβουλες αλλά και αμελείς επεμβάσεις και να περιοριστεί η παρέμβαση των μεσαζόντων.

Κατά πόσο μια έξυπνη σύμβαση έχει τη δυναμική να δώσει στα συστήματα Η/Υ που εφαρμόζουν συμβόλαια, τον προσανατολισμό στα επιθυμητά δεδομένα που θα οδηγήσουν αυτομάτως στη συμμόρφωση ώστε να υλοποιηθεί ο όρος–συμφωνία; Σε ένα υπολογιστικό μοντέλο όπου ένας εξειδικευμένος νοητός υπολογιστής με συναρτήσεις μετάβασης που οδηγούν σε μια και μόνο κατάσταση, χωρίς να δίνεται το περιθώριο για παραπάνω από μια επιλογές, οι έξυπνες συμβάσεις υπόκεινται σε ορισμένα πρότυπα. Άλλωστε η αυτοματοποίηση αποτελεί εγγενές συστατικό τους.

Πώς όμως θα αντιμετωπιστούν νομικά ζητήματα ευθύνης, κωδικοποίησης, ασφάλειας, απορρήτου και απόδοσης σε περίπτωση που προκύψει κάποιο σχετικό θέμα; Ο κώδικας, εκτός από το γεγονός ότι είναι δυσνόητος για έναν νομικό, δεν αποτελεί λόγο αντιδικίας, που θα στήριζε μια αγωγή. Εάν το οικοσύστημα των έξυπνων συμβάσεων δεν επιτρέπει την εισαγωγή εξωτερικών δεδομένων τα οποία εφόσον αλληλοεπιδρούσαν, ίσως ρύθμιζαν το ζήτημα.

Πέρα από την ασφάλεια, την καινοτομία και το όραμα που υπόσχονται, οι έξυπνες συμβάσεις τελικά προσφέρουν λύση στα προβλήματα που αντιμετωπίζουμε με το δίκαιο των συμβάσεων; Δεν θα ήταν επωφελές να αντικαταστήσουν οι έξυπνες συμβάσεις το δίκαιο που τις καθορίζει. Τα έξυπνα συμβόλαια οφείλουν να πληρούν τις απαιτήσεις του νόμου περί συμβάσεων, εξυπηρετώντας διαφορετικό σκοπό από ότι το δίκαιο, το οποίο αποτελεί θεσμό αποκατάστασης. Τελικά η κρυμμένη νομική πτυχή των έξυπνων συμβολαίων προσδιορίζεται στην εξάλειψη των παραβιάσεων εκείνων σε επίπεδο μάλιστα διεθνούς δικαίου, που θα απασχολούσαν έντονα τα δικαστήρια. Η συνεργασία νομικών και προγραμματιστών για την από κοινού σύνταξη κώδικα με στοιχεία λογισμικού, ίσως μας έδινε την επιθυμητή λύση.

4.2 Πλεονεκτήματα έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια ενδέχεται να αλλάξουν ή ακόμη και να μεταμορφώσουν τον κόσμο. Τα οφέλη που θα παρέχουν θα δώσουν το έναυσμα να υιοθετηθούν από πληθώρα οργανισμών (δημόσιων ή ιδιωτικών) με την πάροδο του χρόνου, αφού θα τους προσδώσουν εξοικονόμηση κόστους, κέρδη απόδοσης και αυτοματοποίησης, ελαχιστοποίηση αλληλεπιδράσεων των μερών και αυτοματοποίηση των συμβατικών διαδικασιών. Ανεξάρτητα **από ηθικά και νομικά διλήμματα που δημιουργούνται,** τα πλεονεκτήματα είναι πολύ περισσότερα. Μερικά από αυτά είναι τα εξής :

- Αυτοεκτελούνται
- Αυτοεπαληθεύονται
- Παραμένουν αμετάβλητα
- Περιορίζουν το κόστος συναλλαγών
- Δεν απαιτείται η διαμεσολάβηση τρίτων ή μεσαζόντων
- Τα ψηφιακά στοιχεία αποθηκεύονται με ασφάλεια
- Είναι προκαθορισμένη η δημιουργία αντιγράφων ασφαλείας
- Μειώνονται τα ανθρώπινα σφάλματα
- Εκτελούνται απευθείας με αυτόνομο και αξιόπιστο τρόπο
- Είναι διαφανή και αποκεντρωμένα
- Ο πιο αξιόπιστος μεσάζοντας είναι η ψηφιακή τεχνολογία, βάσει της οποίας αναπτύσσονται
- Είναι ανέφικτη η τροποποίηση οποιασδήποτε καταχώρησης πληροφορίας
- Επεξεργάζονται πολλαπλές συναλλαγές οι οποίες είναι ανακτήσιμες ανά πάσα στιγμή
- Ο χαρακτήρας τους είναι απόλυτος

Μερικά από τα προαναφερόμενα στοιχεία έχουν διττή σημασία και θα μπορούσαν να χαρακτηριστούν και ως **μειονεκτήματα,** διότι οι δημόσιες συμβάσεις φέρουν κάποιες ιδιαιτερότητες, οι οποίες δημιουργούν επιφυλάξεις ως προς την αποτελεσματική εκτέλεσή τους με αυτόν τον τρόπο, καθώς δεν υφίστανται ακόμη κανονιστικές ρυθμίσεις ώστε να είναι εναρμονισμένα με το δίκαιο των συμβάσεων.

4.3 Η δημιουργία έξυπνων συμβάσεων στον δημόσιο τομέα

Η σύναψη συμβάσεων από δημόσιους φορείς, ανέκαθεν ήταν ένα περίπλοκο και ευαίσθητο θέμα αφού η πλειοψηφία των Φορέων του Δημόσιου Τομέα αποτελείται από εκλεγμένους αντιπροσώπους, οι οποίοι έχουν την εξουσία να χρησιμοποιούν τα δημόσια χρήματα για την Κρατική Διοίκηση. Συμβάσεις μονοδιάστατες και παρωχημένες πρωτοστατούσαν εδώ και χρόνια στον δημόσιο τομέα. Αποτυχημένες διαπραγματεύσεις επί των όρων μιας συμφωνίας ή η μη ικανοποιητική εκτέλεσή μιας σύμβασης, αποτελούσαν το πιο συχνό φαινόμενο. Πληθώρα πρόσφατων κανονισμών και διαδικασιών προσπαθούν να διασφαλίσουν ότι η Κυβέρνηση θα επιτύχει την καλύτερη σχέση ποιότητας–τιμής, εφαρμόζοντας δίκαιο ανταγωνισμού και διαφάνεια μεταξύ των συμμετεχόντων στη διαδικασία. Η ενίσχυση της νομοθεσίας με τη δημιουργία ενός κυβερνητικού μοντέλου που θα βασίζεται στις έξυπνες συμβάσεις και θα καθορίζει τον τρόπο ανάπτυξής τους μέσω της τεχνολογίας, φαντάζει ως η ιδανικότερη λύση. Στο σημείο όμως αυτό, βρισκόμαστε αντιμέτωποι με δύο αντιξοότητες. Από τη μία μεριά, η λογοδοσία προς το Κράτος περί δημοσίου συμφέροντος και από την άλλη η σωρεία των συμβατικών διατάξεων, δημιουργεί αρκετούς προβληματισμούς προς επίλυση.

Οι βραχυπρόθεσμες συμβάσεις έχει αποδειχθεί ότι είναι πιο βιώσιμες, αφού ικανοποιούν μια άμεση ανάγκη και βρίσκονται σε ικανοποιητικό επίπεδο εφαρμογής. Οι μακροπρόθεσμες όμως συμβάσεις απαιτούν την δημιουργία μιας αμοιβαίας κατανόησης περί των αποτελεσμάτων και των προσδοκιών του εκάστοτε συμβαλλόμενου μέρους, γεγονός που χρειάζεται στρατηγική. Το μόνο που απομένει είναι να αναπτυχθεί ως ένα έξυπνο συμβόλαιο. Άτομα, επιχειρήσεις και κυβερνήσεις θα μοιράζονται πόρους πλέον μέσω ενός κατανεμημένου καθολικού. Προτεραιότητα θα πρέπει να δοθεί στην ανάπτυξη της εμπιστοσύνης σε κυβερνητικά και διαδικτυακά αστικά συστήματα. Προτεινόμενα προγράμματα που δημιουργήθηκαν κατ' αποκλειστικότητα για Οργανισμούς του Δημοσίου τομέα, υλοποιούνται διεθνώς με επιτυχία. Αυτό που απομένει είναι η μοντελοποίηση των κυβερνητικών διαδικασιών με τη βοήθεια διαφόρων εταιρικών λύσεων, που βασίζονται σε τεχνολογία blockchain για τη **δημιουργία σεναρίων χρήσης** σε διάφορους τομείς αρμοδιοτήτων των υπηρεσιών (από τις προμήθειες έως και τη δημοσιονομική διαχείριση), γεγονός που θα μειώσει δραματικά το κόστος των συναλλαγών και θα αυξήσει κατακόρυφα την αποδοτικότητά τους, αρκεί φυσικά να προϋπάρχει ένα σαφές νομοθετικό πλαίσιο εφαρμογής τους.

4.4 Smart contracts έναντι Συμβάσεων RICARDIAN

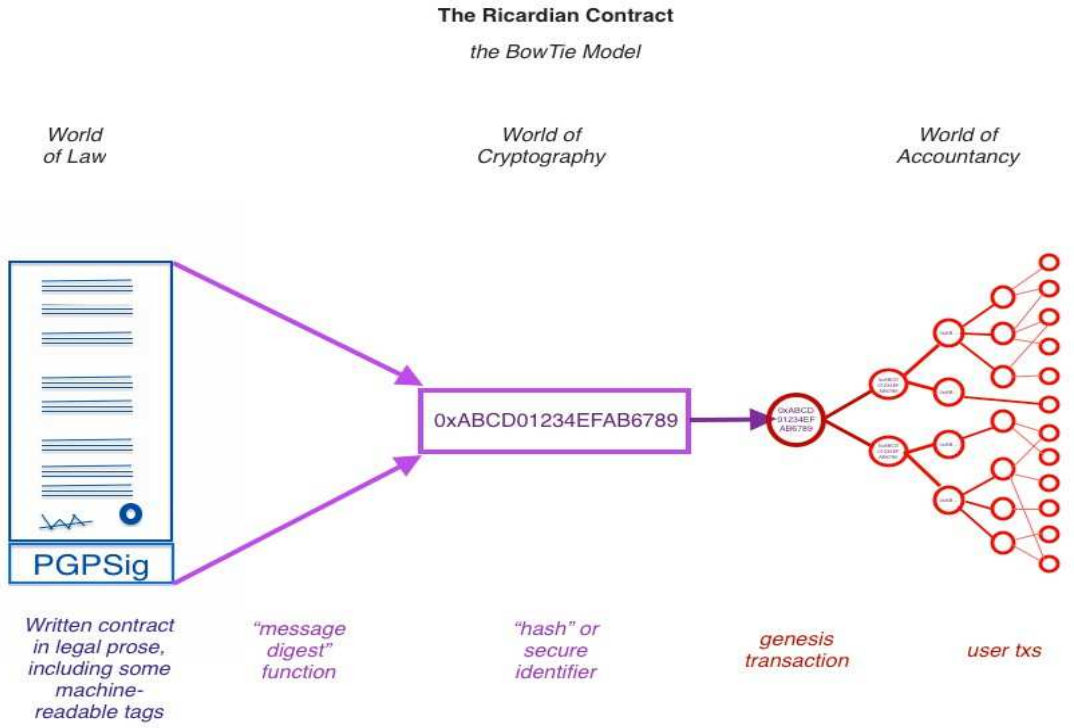
Οι λεγόμενες παραδοσιακές συμβάσεις είναι γραμμένες σε ανθρώπινη γλώσσα, γεγονός που δημιουργεί ασάφειες κατά την ερμηνεία των όρων της. Ειδικά η ελληνική γλώσσα, πλούσια σε έννοιες και διαφορετικούς ορισμούς, ενέχει τον κίνδυνο να διαστρεβλωθούν **σκόπιμα ή μη**, οι όροι–ρήτρες μιας γραπτής συμφωνίας. Αρκετές από αυτές τις συμβάσεις αποδεικνύεται ότι είναι δυσνόητες ή ατελείς. Δεν είναι λίγες οι φορές που τα συμβαλλόμενα μέρη εκλαμβάνουν με διαφορετικό τρόπο τις όποιες διαπραγματεύσεις πριν από την κατάρτιση του τελικού κειμένου. Στρέφονται τότε στη δικαιοσύνη για να δικαιωθούν, διαδικασία αρκετά χρονοβόρα και δαπανηρή. Σημεία στίξης αποτέλεσαν κάποτε την αφορμή να υπάρξουν απώλειες σημαντικών χρηματικών ποσών, για αυτό και όλες οι πιθανές γλωσσικές ερμηνείες δεν είναι επιθυμητές και θα πρέπει να αποκλειστούν. Οι παραδοσιακές συμβάσεις αντιπροσωπεύουν συμφωνία μεταξύ δύο τουλάχιστον εμπλεκόμενων μερών–συμμετεχόντων. Αυτές οι συμφωνίες **επικυρώνονται και επιβάλλονται από έναν υπάλληλο ή κάποιο τρίτο μέρος**. Οι οντότητες τρίτων είναι οι βασικοί συμμετέχοντες για την εξασφάλιση της επικύρωσης των όρων της σύμβασης καθώς επίσης και για την αξιολόγηση τρίτων περιστάσεων και γεγονότων, που θα μπορούσαν να επηρεάσουν την εκτέλεση της σύμβασης.

Πάντοτε ένα συμβόλαιο στηρίζεται σε υποχρεώσεις και δικαιώματα των μερών. Ο όρος έξυπνη σύμβαση είναι ένας όρος γνωστός εδώ και δεκαετίες από τον κρυπτογράφο και επιστήμονα **Nick Szabo**, ο οποίος ανακάλυψε την ιδέα στα μέσα της δεκαετίας του 1990. *Κατ' ουσίαν είναι ένα ηλεκτρονικό πρωτόκολλο συναλλαγών που εκτελεί τους όρους μιας σύμβασης, με γενικό στόχο την από κοινού ικανοποίηση των συμβαλλόμενων μερών*. Μόνο που τον ρόλο της διαχείρισης αυτής την αναλαμβάνει ο υπολογιστής **μέσω του κώδικα εντολών**. Η συμμόρφωση για το σύνολο των προϋποθέσεων **επιβεβαιώνεται αυτομάτως.** Στη συνέχεια επικυρώνονται όλα τα δεδομένα που απαρτίζουν τους όρους της σύμβασης και το συμβόλαιο αποθηκεύεται στην τελική του μορφή, παραμένοντας αμετάβλητο. Συνεπώς, τα Smart contracts μετατρέπονται σε κώδικα ηλεκτρονικού υπολογιστή, αποθηκεύονται και αναπαράγονται στο σύστημα, αφού πρώτα επαληθευτούν από το δίκτυο Η/Υ που τρέχει το **blockchain**. Συνέπεια αυτού είναι οι συναλλαγές να πραγματοποιούνται με διαφανή και μη αντικρουόμενο τρόπο και η εμπιστοσύνη να διασφαλίζεται μέσω ενός δικτύου Blockchain μεταξύ ανώνυμων μερών.

*Το **συμβόλαιο RICARDIAN*** **[39] είναι ένα έγκυρο νομικό συμβόλαιο**, **εκτυπώσιμο και με υπογραφή εκδότη (ψηφιακή),** το οποίο είναι αναγνώσιμο από τον άνθρωπο και το μηχάνημα. Όλες οι πληροφορίες του εγγράφου «μεταφράζονται» με τέτοιο τρόπο ώστε να μπορούν να «διαβαστούν» και να μετατραπούν σε εκτελέσιμο λογισμικό. Το συμβόλαιο RICARDIAN είναι απλά μια παραδοσιακή σύμβαση σε ψηφιακή μορφή. Ειδικότερα θεωρείται ως ένα υβριδικό μοντέλο αυτοματισμού και συμβατικού νομικού κειμένου. Πρακτικά αυτό σημαίνει ότι η Ρικαρδιανή σύμβαση αποτελείται από δύο μέρη : τους ανθρώπινα αναγνώσιμους και τους μηχανικά αναγνώσιμους όρους.

Κι ενώ παρατηρούμε ομοιότητες ανάμεσα σε ένα έξυπνο συμβόλαιο και ένα RICARDIAN, δεν είναι η κάθε σύμβαση RICARDIAN έξυπνο συμβόλαιο, ενώ το αντίθετο θα μπορούσε να το ισχυριστούμε. Η σύμβαση RICARDIAN καταγράφει με χρήση κώδικα ή με άντληση δεδομένων από εξωτερικά έγγραφα, τις προθέσεις

των μερών που επιθυμούν να καταλήξουν σε συμφωνία. Ο όρος συμβόλαιο χρησιμοποιείται επειδή θα πρέπει πρώτα να εκπληρώνονται όλες οι προϋποθέσεις ακριβώς όπως σε ένα συμβόλαιο, προκειμένου να εκτελεσθεί το πρόγραμμα. Εξακολουθούν να θεωρούνται παραδοσιακές συμβάσεις, παρά τον ψηφιακό χαρακτήρα τους, **λόγω της εγγενούς ανάγκης για επέμβαση νόμιμης εξουσίας, που δεν υπάρχει στις έξυπνες συμβάσεις.** Η διαφορά μεταξύ έξυπνων συμβολαίων και τύπου RICARDIAN έγκειται στο γεγονός ότι οι τελευταίες επικεντρώνονται περισσότερο στον σημασιολογικό πλούτο και την παραγωγή ενός εγγράφου που θα είναι κατανοητό από ανθρώπους και δη νομικούς, ενώ η έξυπνη σύμβαση αφορά αμιγώς στην εκτέλεση της σύμβασης. Ενδεχομένως η δημιουργία ενός έξυπνου τύπου συμβάσεως «**υβριδικής μορφής», θα επιλύσει κάποια από τα προβλήματα που απασχολούν έντονα τους νομικούς κύκλους σήμερα.**



Εικόνα 36: Συμβόλαιο Ricardian [39]

Κεφάλαιο 5ο - Τεχνολογία blockchain και νομική διάσταση

5.1 Τεχνικοί όροι σε πλατφόρμες τεχνολογίας Blockchain και νομικός συσχετισμός με νομική ορολογία

Είναι εξαιρετικά χρήσιμο να αποδώσουμε τις έννοιες των τεχνικών όρων που απαρτίζουν τη λειτουργία μιας πλατφόρμας που στηρίζεται σε τεχνολογία blockchain, κατ΄ αντιστοιχία με τη νομική τους ερμηνεία. Ακολουθεί σχετικός πίνακας.

Πίνακας 1: Συσχετισμός νομικής ορολογίας και τεχνικών όρων τεχνολογίας blockchain[10]

Νομική ορολογία	Νομική έννοια	Έννοια τεχνολογίας blockchain σε πλατφόρμες εφαρμογής της	Τεχνικός όρος
1. Συναίνεση κατά ομοφωνία	Όλα τα εμπλεκόμενα άτομα θεωρούνται ότι συναινούν για το ίδιο πράγμα με την ίδια έννοια	Ελεγχόμενοι κανόνες (πρωτόκολλο συναίνεσης) δημιουργίας και διαμοιρασμού αρχείων εντός ενός δικτύου blockchain. Οι κανόνες αυτοί συντάσσονται με βασικό γνώμονα την κατ' εξαίρεση ανάγκη για ύπαρξη εμπιστοσύνης ανάμεσα στα πρόσωπα που εμπλέκονται στο δίκτυο. Χρησιμεύει στη δημιουργία συμφωνίας, ως προϋπόθεση για την ροή συναλλαγών εντός του δικτύου, αφού με την συναίνεση επιβεβαιώνεται η ορθότητας του συνόλου των συναλλαγών, που αποτελούν ένα μπλοκ.	**consensus**
2. Συμμόρφωση	Ενιαίο νομικό πλαίσιο προστασίας το οποίο αναφέρεται σε μια υποχωρητική αντίδραση απέναντι σε κάποιο αίτημα	Κανόνες υποχρεωτικής προέγκρισης των προτεινόμενων προσομοιωμένων συναλλαγών σε μια αλυσίδα κώδικα	**endorsement policy**
3. Εκτέλεση	Εφαρμογή υποχρεωτικών και εξαναγκαστικών κανόνων οι οποίοι και ρυθμίζουν τις σχέσεις των διαβιούντων προσώπων σε μια κοινωνία.	Προσάρτηση επικυρωμένων συναλλαγών στο καθολικό για το συγκεκριμένο κανάλι	**committer**
4. Κώδικας	Ένα ενιαίο σύνολο νόμων ανά τομέα δικαίου	Λογική που κωδικοποιεί κανόνες για συγκεκριμένους τύπους συναλλαγών δικτύου - αλυσιδωτός κώδικας εντολών	**chaincode**

[10] Πηγή ορολογίας για blockchain : https://www.onassis.org/whats-on/blockchain-utopia-or-u-turn/glossary
Πηγή ορολογίας για Hyperledger : https://hyperledger-fabric.readthedocs.io/en/release-1.4/blockchain.html#what-is-hyperledger-fabric
Οι νομικοί ορισμοί αντλήθηκαν από κώδικες νομοθεσίας

5. Χρονική προτεραιότητα	Σε περίπτωση της σύγκρουσης μεταξύ δικαιωμάτων, εφαρμόζεται η αρχή της χρονικής προτεραιότητας ιδίως όταν πρόκειται για αλληλοσυγκρουόμενα δικαιώματα. Σύμφωνα με την αρχή αυτή, μεταξύ πχ πολλών μεταγραφών που έγιναν την ίδια ημέρα σχετικά με δικαιώματα βάρη πάνω στο ίδιο ακίνητο, προτιμάται εκείνη που στηρίζεται στον έστω και κατ' ελάχιστο χρόνο αρχαιότερα μεταγεγραμμένο τίτλο	Σύνολο εργασιών οι οποίες εκτελούνται με συγκεκριμένη σειρά από έναν επεξεργαστή αλλά με το συντομότερο δυνατό τρόπο, θεωρώντας την πρώτη χρονικά συναλλαγή ως τη μόνη έγκυρη σε περίπτωση αμφισβήτησης.	**transaction-confirmation time**
6. Σύμβαση	Η δικαιοπραξία μεταξύ δύο ή περισσότερων προσώπων με την οποία τα πρόσωπα δηλώνουν τη βούλησή τους να προβούν σε διάφορες ενέργειες και να συνεργαστούν με άλλα πρόσωπα, είναι δηλαδή δήλωση βούλησης.	Ο όρος **«έξυπνα συμβόλαια»** αναφέρεται σε ψηφιοποιημένα συμβόλαια στα οποία έχει ενσωματωθεί κώδικας υπό τη μορφή, τα οποία εκτελούνται αυτόματα αν πληρωθούν οι προϋποθέσεις που έχουν τεθεί.	**contract**
7. Επικύρωση	Η διαδικασία η οποία δίνει νομική ισχύ σε ένα έγγραφο (π.χ συμφωνία) με την έγκριση του αρμοδίου οργάνου του καθενός από των υπογραφόντων μερών	Κωδικός αλυσίδας συστήματος επικύρωσης για όλα τα μέρη που συναλλάσσονται εντός της αλυσίδας	**Validation system chaincode**
8. Γνωμοδότηση – Έγκριση	Η εκφρασμένη έγκυρη γνώμη νομικού σώματος ή οργάνου	Κωδικός αλυσίδας συστήματος έγκρισης για όλα τα μέρη που συναλλάσσονται εντός της αλυσίδας	**endorsement system chaincode**
9. Εκχώρηση δικαιώματος	Υποκατάσταση έναντι δικαιώματος άλλου προσώπου	Τελικός χρήστης ο οποίος υποκαθιστά όλα τα μέρη που συναλλάσσονται εντός της αλυσίδας	**end user**
10. Πρόταση	Η υπόσχεση η οποία αποτελείται από την πρόταση και την αποδοχή. Για να μετατραπεί μια πρόταση σε υπόσχεση, η αποδοχή πρέπει να είναι απόλυτη και ανεπιφύλακτη ή να εκδηλώθηκε κατά τον συνήθη και εύλογο τρόπο, εκτός αν η πρόταση καθορίζει συγχρόνως και τον τρόπο της αποδοχής.	Αίτημα συναλλαγής από έναν διαχειριστή σε έναν ομότιμό του στο δίκτυο (ανάπτυξη, επίκληση, ερώτημα ή αίτημα διαμόρφωσης)	**proposal**

5.2 Η έννοια της εμπιστοσύνης και το Blockchain

Η εμπιστοσύνη εντός μιας αλυσίδας blockchain, ενός τεχνολογικού αποκεντρωμένου μητρώου, είναι μια έννοια που δεν αποδίδει το χαρακτηριστικό της αυτό γνώρισμα σε κάποια ξεχωριστή οντότητα. Η δυναμική της εμπιστοσύνης καλλιεργείται από το αρθρωτό κρυπτογραφημένο αρχιτεκτονικό της μοντέλο, στο οποίο τα προφανώς τα δεδομένα είναι ασφαλή.

Η ταυτόχρονη καταγραφή των δεδομένων σε ένα κοινό μητρώο, καθιστά όλους τους συμμετέχοντες κοινωνούς και κατόχους της ίδιας πληροφόρησης. Η εμπιστοσύνη στο λογισμικό υποκαθιστά τον κεντρικό διαχειριστή. Τα συμβόλαια που αναπτύσσονται σε αυτό αποτελούν έγγραφα εμπιστοσύνης.

Η ασύμμετρη κρυπτογραφία των δεδομένων της και οι ενσωματωμένες ψηφιακές υπογραφές καθιστούν τα δεδομένα στο blockchain αυθεντικά και ελεγχόμενα. Το Blockchain άλλωστε, ως ένα αδιαμφισβήτητο κατανεμημένο καθολικό συναλλαγών, χρησιμοποιεί κρυπτογραφικές αποδείξεις, για να επαληθεύσει τις συναλλαγές που πραγματοποιούνται. Όλες οι εγγραφές του δηλαδή συνδέονται κρυπτογραφικά με την αμέσως προηγούμενη καταχώρηση, ώστε οποιαδήποτε προσπάθεια αλλαγής καταχωρήσεων που έχουν προηγηθεί χρονικά, να οδηγήσει σε διακοπή της κρυπτογραφικής ακεραιότητας του blockchain και κατ' επέκταση να χαρακτηριστεί αυτομάτως ως αναξιόπιστη. ***Η συναίνεση είναι εκείνη η οποία θα επιτρέψει τη εκτέλεση των συναλλαγών, αφού όμως προηγηθεί η επαλήθευση από το λεγόμενο δίκτυο των επικυρωτών (miners).***

Το blockchain τελικά λειτουργεί υπό τη μορφή ενός νομικού συστήματος, αφού αναλαμβάνει εξουσιαστικό ρόλο, φροντίζοντας για την πιστή τήρηση των «κανόνων». Το γεγονός ότι οι πληροφορίες είναι ορατές σε κάθε κόμβο, καθιστούν την αναπτυσσομένη στην πλατφόρμα σύμβαση προστατευμένη από όσους θα ήθελαν να διεισδύσουν και να την παραβιάσουν, με τρόπο που θα προκαλούσε βλάβη ή θα καθιστούσε άχρηστη την επιδιωκόμενη συμφωνία.

5.3 Η σύναψη σύμβασης με τη χρήση πρακτόρων λογισμικού

Το αν υφίσταται ηλεκτρονική δήλωση βουλήσεως και τι χαρακτηριστικά αυτή φέρει, ήταν το πρώτο θέμα που προβλημάτισε τους νομικούς. Το κατά πόσο αυτή η δήλωση θα μπορούσε να φέρει αυτοματοποιημένη μορφή, είναι το δεύτερο ζητούμενο. Ανεξάρτητα από το τι ισχύει τελικά, η δήλωση αυτή δίδεται αναμφισβήτητα μέσω ηλεκτρονικού υπολογιστή και θα πρέπει να καταλογίζεται στον άνθρωπο–χρήστη της. Προκειμένου αυτή να είναι έγκυρη, απαιτείται η αυτόνομη δράση του νοήμονα πράκτορα–ηλεκτρονικού υπολογιστή να έχει αποκτήσει κανονιστικό χαρακτήρα, ήτοι να έχει θεσμοθετηθεί με τέτοιο τρόπο ώστε η μηχανή τελικά να δρα ως αντιπρόσωπος του ανθρώπου-χρήστη της.

Πρακτικά αυτό σημαίνει ότι αποκτά την ιδιότητα του αντιπροσώπου υπό την προϋπόθεση ότι υπάρχει ένα είδος διάδρασης με τον άνθρωπο. Απόρροια τούτου είναι να επιδιώξει να ικανοποιήσει το συμφέρον του χρήστη του. Ο πράκτορας όμως είναι ένα πρόγραμμα–μηχανή χωρίς δική της βούληση. Πως μπορεί να νοηθεί ως αντιπρόσωπος; Η ιδιότυπη φύση της αυτόνομης δράσης του πράκτορα ανατρέπει τη δημιουργία μιας συμβατικής σχέσης μεταξύ αντιπροσώπου και αντιπροσωπευόμενου. Η

δε προσφυγή σε νομικές κατασκευές τύπου πλάσμα δικαίου, το οποίο θα μας επέτρεπε να καλύψουμε το θεωρητικό υπόβαθρο της έννοιας της αντιπροσώπευσης από μια μηχανή, φαίνεται ότι είναι η μόνη αποδεκτή λύση.

5.4 Από το ο κώδικας είναι νόμος στο ο νόμος είναι κώδικας

Αναφέρθηκε και σε προηγούμενο κεφάλαιο ότι το αντικείμενο των έξυπνων συμβολαίων σε αντίθεση με τα κρυπτονομίσματα, δεν είναι απλά η μεταφορά χρηματικού ποσού από έναν λογαριασμό σε κάποιον άλλο και η διατήρηση αποκεντρωμένων λογιστικών βιβλίων, αλλά η ενσωμάτωση ενός κωδικοποιημένου συστήματος κανόνων και ορισμών σε ένα αποκεντρωμένο δίκτυο blockchain, που ορίζει τις σχέσεις και τις διαδικασίες συναλλαγής αξιών ανάμεσα σε δύο ή περισσότερα συμβαλλόμενα πρόσωπα.

Πολλές επιχειρήσεις και δημόσιοι φορείς έχουν στραφεί στην δημιουργία τεχνολογικών κανόνων, οι οποίοι ρυθμίζουν συμπεριφορές, δηλαδή η τεχνολογία πλέον αποτελεί ένα ακόμη μέσο για την επιβολή κανόνων, αποκτά νομική διάσταση. Νόμος και τεχνολογία πλέον αλληλοεπιδρούν. Η τεχνολογία χρησιμοποιείται ως μέρος υπακοής στο νόμο, ο οποίος την έχει ορίσει ως προϋπόθεση ορθής εφαρμογής του μέσω επιμέρους ειδικών διατάξεων αναφοράς του. Η ανάκτηση νομικών διατάξεων ή νομολογίας, η ανάλυση και σύγκρισή τους διευκολύνουν τους δικαστές να καταλήξουν σε ορθότερες αποφάσεις, παρόλο που τα νομικά πρότυπα δεν είναι ευέλικτα και είναι εξαρτώμενα από συγκεκριμένα μεταβαλλόμενα γεγονότα. Πρόκειται για νέου τύπου Νόμο ο οποίος στηρίζεται στον Κώδικα, για καθορισμό των κανόνων που τηρούν οι άνθρωποι. Επειδή οι τεχνικοί κανόνες είναι απολύτως τυποποιημένοι σε τέτοιο βαθμό που είναι σχεδόν αδύνατο να αμφισβητηθούν, εξαλείφεται η ανάγκη δικαστικής διαιτησίας, που οι παραδοσιακοί νομικοί κανόνες ελκύουν λόγω της ευελιξίας ή της διφορούμενης φύσης τους. Η ολοένα αυξανόμενη εξάρτηση από τον κώδικα όχι μόνο για την επιβολή των κανόνων δικαίου αλλά και την επεξεργασία και κατάρτιση αυτών των κανόνων δημιουργούν ασάφειες, διότι τα έξυπνα συμβόλαια δεν δρουν μόνο υποστηρικτικά αλλά έχουν αποκτήσει πρωταγωνιστικό ρόλο, φιλοδοξώντας να αντικαταστήσουν επαρκώς τις νομικές συμβάσεις. Στην πραγματικότητα όμως χρησιμοποιούνται για να μιμηθούν ή τουλάχιστον να προσομοιώσουν τη λειτουργία των νομικών συμβάσεων μέσω της τεχνολογίας, μετατρέποντας τον νόμο σε κώδικα. Είναι αυτό που ο Lawrence Lessig το 1999 αποκάλεσε ως **«ο Κώδικας είναι νόμος – Code is Law»**

Η πρώτη μέριμνα που δόθηκε σε επίπεδο Νομικής Πληροφορικής ήταν η μετάφραση των νομικών διατάξεων σε κώδικα υπολογιστή. Η μετατροπή των νομικών κανόνων σε τεχνικούς δεν είναι εύκολο, αφού οι τελευταίοι βασίζονται σε αλγορίθμους και μαθηματικά μοντέλα, τα οποία είναι απόλυτα και προκαθορισμένα, σε αντίθεση με τη φυσική γλώσσα, η οποία δημιουργεί αρκετές ασάφειες. Δίδεται εμμέσως η εξουσία στους προγραμματιστές–μηχανικούς λογισμικού να προσδώσουν τη δική τους ερμηνεία του νόμου. Άμεση συνέπεια τούτου, ο νόμος να αρχίζει σταδιακά να ενσωματώνει χαρακτηριστικά του κώδικα. Την τάση αυτή οφείλουν να ακολουθήσουν οι νομοθέτες σχεδιάζοντας

εξαρχής κανόνες με τέτοιο τρόπο, ώστε να συγκλίνουν με τους τεχνικούς κανόνες, αποτρέποντας τον κίνδυνο ο νόμος να μετατραπεί σταδιακά σε κώδικα.

Κεφάλαιο 6ο – Το ψήφισμα της ΕΕ – Διεθνής πρακτική Blockchain και Δημόσιο

6.1 Η πρόταση του ψηφίσματος του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις τεχνολογίες DLT και το σύστημα Blockchain

Το Ευρωπαϊκό Κοινοβούλιο ενέκρινε ψήφισμα σχετικά με τις τεχνολογίες κατανεμημένου καθολικού και το σύστημα **blockchain**, ζητώντας την **καθιέρωση ευνοϊκών καινοτόμων ρυθμίσεων**. Σύμφωνα με το ψήφισμα, η DLT μπορεί να βελτιώσει βασικούς τομείς της οικονομίας, καθώς και την ποιότητα των δημοσίων υπηρεσιών, παρέχοντας στους καταναλωτές και πολίτες, υψηλού επιπέδου συναλλακτική εμπειρία.

Το ψήφισμα εκτίμησε ότι η τεχνολογία αυτή θα ανατρέψει όλα τα δεδομένα, με γνώμονα τα προσφερόμενα χαρακτηριστικά της, όπως:

1. Τη δυνατότητα «αυτοδυναμίας» των πολιτών ως προς τον έλεγχο για την επιλογή και τον διαμοιρασμό των δεδομένων
2. Την απουσία διαμεσολαβητών
3. Τη δυνατότητα δημιουργίας ενιαίου ηλεκτρονικού προτύπου δεδομένων για την εκτέλεση των συναλλαγών
4. Την ψευδωνυμοποίηση του εκάστοτε χρήστη
5. Τη δυνατότητα ανίχνευσης και εντοπισμού παράνομων δραστηριοτήτων
6. Τη διαφύλαξη της ακεραιότητας των δεδομένων των χρηστών σε συνδυασμό με τη διαπίστευση, η οποία δημιουργεί συναισθήματα ασφάλειας ενώ ταυτόχρονα εγκαινιάζει ένα νέο μοντέλο δημόσιας διοίκησης
7. Την επιμέρους αποθήκευση των συναλλαγών σε μπλοκ αλληλοσυνδεόμενα κατά χρονολογική σειρά
8. Την αποτροπή κυβερνοεπιθέσεων εξαιτίας του τύπου τεχνολογίας κατανεμημένου καθολικού, το οποίο στηρίζεται σε αλυσίδα συστοιχιών, δημιουργώντας μεγάλο αριθμό αντιγράφων
9. Την προστασία των δεδομένων αφού οι εφαρμογές τεχνολογίας DLT αναπτύσσονται **με συστημικό τρόπο**, προωθώντας την ψηφιακή καινοτομία και την επιθυμητή μεταρρύθμιση, ανεξάρτητα από το γεγονός ότι αρκετοί από τους κινδύνους που καραδοκούν, δεν έχουν γίνει ακόμη ευρέως γνωστοί.

6.1.1 Σε πλήρη λειτουργία το 2020 η Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain (EBSI)

Σημαντικές πρωτοβουλίες ακολούθησαν μετά το εν λόγω ψήφισμα. Στις 10 Απριλίου 2018, 21 κράτη μέλη της ΕΕ και η Νορβηγία συμφώνησαν να υπογράψουν μια κοινή δήλωση για τη δημιουργία της Ευρωπαϊκής Εταιρικής Σχέσης Blockchain και να συνεργαστούν για τη δημιουργία μιας ε**υρωπαϊκής υποδομής υπηρεσιών blockchain (EBSI)**, η οποία θα υποστηρίζει την παροχή διασυνοριακών ψηφιακών δημόσιων υπηρεσιών, με τα υψηλότερα πρότυπα ασφάλειας και ιδιωτικότητας. Αυτή τη στιγμή βρίσκεται πλέον σε πλήρη λειτουργία ο νεοσύστατος συνεταιρισμός **European Blockchain Partnership** (EBP), στον οποίο μετέχουν συνολικά 26 κράτη - μέλη της ΕΕ (Αυστρία, Βέλγιο, Βουλγαρία, Γαλλία, Γερμανία, Δανία, Ελλάδα, Εσθονία, Κύπρος, Ιρλανδία, Ισπανία, Ιταλία, Λετονία, Λιθουανία, Λουξεμβούργο, Μάλτα, Ολλανδία, Πολωνία, Πορτογαλία, Σλοβακία, Σλοβενία, Σουηδία, Ρουμανία, Τσεχία και Φιλανδία) καθώς και η Νορβηγία και το Λιχτενστάιν. Στόχος της λειτουργίας της πλατφόρμας Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain (EBSI) είναι **η γνησιότητα των εγγράφων καθώς και αυθεντικοποίησή τους** (π.χ. ευρωπαϊκοί τίτλοι σπουδών), ώστε ο κάθε χρήστης, π.χ. μια εταιρεία ή οργανισμός που θέλει να προσλάβει εργαζόμενο/η, να μπορεί να διασταυρώσει την αξιοπιστία τους. Με τον τρόπο αυτό υπάρχει η πεποίθηση ότι θα αποφευχθούν οι μεμονωμένες προσεγγίσεις των Κρατών – Μελών, **επιτυγχάνοντας τη δια λειτουργικότητα των υπηρεσιών που θα βασίζονται στην τεχνολογία blockchain.**

6.1.2 Horizon 2020

Το πρόγραμμα "Horizon 2020" αποτελεί το μεγαλύτερο πρόγραμμα έρευνας και καινοτομίας της ΕΕ με προϋπολογισμό σχεδόν 80 δισ. ευρώ για 7 έτη (2014-2020). Η Ευρωπαϊκή Επιτροπή χρηματοδότησε έργα **Blockchain** μέσω **ερευνητικών προγραμμάτων**, θέτοντας ως κύριους άξονες του προγράμματος την Επιστημονική Αριστεία, την Βιομηχανική Υπεροχή και τις Κοινωνικές Προκλήσεις

- **Άξονας «Βιομηχανική Υπεροχή»**

i. Εκδόθηκε πρόσκληση με τίτλο *'**Blockchains for Social Good'***. Σκοπός ήταν η ενίσχυση πρωτοβουλιών που έχουν στόχο την ανάπτυξη αποδοτικών και αποτελεσματικών αποκεντρωμένων λύσεων για την αντιμετώπιση των κοινωνικών προκλήσεων (European Commission, 2018).

ii. Εκδόθηκε η πρόσκληση με τίτλο '***Blockchain and distributed ledger technologies (DLT) for SMEs'*** (European Commission, 2018). Σκοπός της πρόσκλησης ήταν η επιλογή έργων που θα καταφέρουν να βρουν βιώσιμες λύσεις στα μειονεκτήματα της τεχνολογίας DLT, όπως αυτά που σχετίζονται με τη δια λειτουργικότητα, τα πρότυπα και την προστασία των δεδομένων.

❖ **Άξονας «Κοινωνικές Προκλήσεις»**

i. Εκδόθηκε πρόσκληση με τίτλο ***'Blockchain Enabled Healthcare'*** **(European Commission, 2018)**. Σκοπός της πρόσκλησης είναι να αναπτυχθεί ένα ενιαίο οικοσύστημα ανάπτυξης, παρασκευής και διανομής φαρμάκων, βασισμένο στη τεχνολογία blockchain, που να αντιμετωπίζει τα προβλήματα του κλάδου της φαρμάκου, όπως η πολυπλοκότητα των διαδικασιών και η έλλειψη διαφάνειας.

ii. Εκδόθηκε πρόσκληση με τίτλο ***'Socioeconomic and cultural Transformations in the Context of the 4th Industrial Revolution'***, που εμπεριέχει τον άξονα 'Transformative impact of disruptive technologies in public services', με τον οποίο χρηματοδοτήθηκαν πιλοτικά έργα, για να αξιολογήσουν το αντίκτυπο των τεχνολογιών που μπορούν να διαταράξουν (disruptive) το υπάρχον μοντέλο παροχής των δημόσιων υπηρεσιών, και να πειραματιστούν με αυτές.

6.1.3 Παρατηρητήριο και Φόρουμ Blockchain

Εκτός από τα χρηματοδοτικά εργαλεία, η ΕΕ εγκαινίασε το **Ευρωπαϊκό Παρατηρητήριο και Φόρουμ για το Blockchain** τον Φεβρουάριο του 2018. Στόχος του η Ευρώπη να εντοπίσει και αξιοποιήσει με τον καλύτερο δυνατό τρόπο τις νέες ευκαιρίες που προσφέρει το **blockchain** και να καλλιεργήσει εμπειρογνωμοσύνη στο πεδίο. Με την συγκέντρωση των πληροφοριών και την παρακολούθηση-ανάλυση των τάσεων, φιλοδοξεί να προσεγγίσει **νεοφυείς επιχειρήσεις**, όπως συνέβη με την εταιρεία ConsenSys η οποία επιλέχθηκε μετά από πρόσκληση υποβολής προσφορών το έτος 2017, ως εταίρος για να υποστηρίξει τις δράσεις του Παρατηρητηρίου. Η εταιρεία αυτή χρησιμοποιώντας την πλατφόρμα του Ethereum, η οποία έχει μετεξελιχθεί σε έναν παγκόσμιο οργανισμό ανάπτυξης λύσεων και υποδομών **blockchain**.

6.1.4 Προτεραιότητες σχεδίου δράσης για εφαρμογές με DLT τεχνολογία

Ακολουθεί μια συνοπτική περιγραφή των προτεραιοτήτων του σχεδίου δράσης της Επιτροπής

- ✓ Μείωση δαπανών διαμεσολάβησης–περιβάλλον εμπιστοσύνης μεταξύ των συναλλασσόμενων μερών.
- ✓ Εναρμόνιση με τη δομή της δημόσιας διακυβέρνησης, όπου ο ρόλος των θεσμών θα διαδραματίζει πρωταγωνιστικό ρόλο ως προς την υιοθέτηση δημόσιων δικτύων, τα οποία θα βασίζονται στη συγκεκριμένη τεχνολογία.
- ✓ Ανάπτυξη σεναρίων εφαρμογών σε όλους τους τομείς της οικονομίας, όπως είναι την ενέργεια και το περιβάλλον, τις μεταφορές, την υγειονομική περίθαλψη, τις αλυσίδες εφοδιασμού, την

εκπαίδευση, τις δημιουργικές βιομηχανίες και τα δικαιώματα πνευματικής ιδιοκτησίας και φυσικά στον χρηματοπιστωτικό τομέα.

- ✓ Υιοθέτηση οικοσυστήματος τεχνολογίας το οποίο εξασφαλίζει τη διαφάνεια των συναλλαγών μέσα από την αυτό, όπως είναι η ταυτοποίηση και ψευδωνυμοποίηση, η οποία δημιουργεί μια πρωτοποριακή ψηφιακή ταυτότητα απλουστεύοντας τις συναλλαγές, παρόλο που καταστρατηγείται το δικαίωμα στη λήθη.
- ✓ Έκδοση κατευθυντήριων γραμμών περί εναρμόνισης των τεχνολογιών DLT με τον ΓΚΠΔ από τον αρμόδιο Ευρωπαϊκό Επόπτη προστασίας Δεδομένων.
- ✓ Κατοχύρωση εμπιστοσύνης μέσω κρυπτογραφικών αλγόριθμων, με τους οποίους στην ουσία επικυρώνονται, διασφαλίζονται και προστατεύονται τα δεδομένα «διαρρηγνύοντας» κατά κάποιον τρόπο το ρόλο του τρίτου διαμεσολαβητή.
- ✓ Μεμονωμένη περιπτωσιακή μελέτη χρήσης των έξυπνων συμβάσεων, οι οποίες αναπτύσσονται εντός ενός περιβάλλοντος DLT, προκειμένου να αντιμετωπιστούν οι νομικές συνέπειες που θα επιφέρουν σε κάθε Κράτος–Μέλος.
- ✓ Ψηφιακή κρυπτογραφημένη υπογραφή η οποία θα αποτελεί τον πιο κρίσιμο παράγοντα ασφάλειας δικαίου.
- ✓ Ανάπτυξη τεχνικών προτύπων βάσει του ισχύοντος νομικού πλαισίου των Κρατών–Μελών, τα οποία θα μπορούσαν να συγκλίνουν νομοθετικά στο πλαίσιο μια ψηφιακής ενιαίας αγοράς. (Σημαντικά τεχνολογικά χαρακτηριστικά όπως η δια λειτουργικότητα, η τυποποίηση και η κλιμακωσιμότητα, ενισχύουν την πεποίθηση πως θα ήταν συνετό να καθοριστούν πρότυπα ενιαίας εφαρμογής εντός της ΕΕ).
- ✓ Ασφάλεια της υποδομής της ώστε να εκτιμώνται ενδεχόμενοι κίνδυνοι και να καθίστανται ανθεκτικές οι πλατφόρμες DLT.
- ✓ Σε ότι αφορά τις δημόσιες υποδομές στα πλαίσια της νέας πραγματικότητας που στοχεύει στην ηλεκτρονική διακυβέρνηση, ενισχύεται, μέσω της τεχνολογίας DLT, η απαίτηση για λογοδοσία από τους πολίτες, γεγονός το οποίο έχει κοινωνικό αντίκτυπο.
- ✓ Οι μικρομεσαίες επιχειρήσεις να έχουν τη δυνατότητα να εισέλθουν ευκολότερα στις ψηφιακές αγορές, έχοντας πρόσβαση στις χρηματοδοτήσεις.
- ✓ Κοινές πρωτοβουλίες των Κρατών-Μελών για κατάρτιση των πολίτων, των εργαζομένων στις επιχειρήσεις και των απασχολούμενων στη δημόσια διοίκηση στις ψηφιακές δεξιότητες σχετικά με την DLT και στην υλοποίηση εφαρμογών αλυσίδων συστοιχιών εντός ενός ενιαίου ευρωπαϊκού νομικού πλαισίου.
- ✓ Κανονιστική αντιμετώπιση τεχνολογίας DLT που θα πρέπει να διέπεται από τις αρχές της ουδετερότητας και του επιχειρηματικού προτύπου.
- ✓ Οι μηχανισμοί κρυπτόθεσης και ελέγχου δύναται να καθιερώσουν ένα ηλεκτρονικό πρότυπο, που εκδημοκρατίζει τα δεδομένα, βελτιώνει την εμπιστοσύνη και τη διαφάνεια, προσφέροντας ασφαλείς και αποτελεσματικούς δίαυλους για την εκτέλεση των συναλλαγών.

- ✓ Η αξιοποίηση της τεχνολογίας DLT στο πλαίσιο της διαφάνειας και με σκοπό να μειώσει τη διαφθορά, μπορεί να εντοπίσει τη φοροδιαφυγή, να επιτρέψει την ιχνηλάτηση παράνομων πληρωμών, να διευκολύνει πολιτικές κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και να ανιχνεύσει την υπεξαίρεση περιουσιακών στοιχείων.

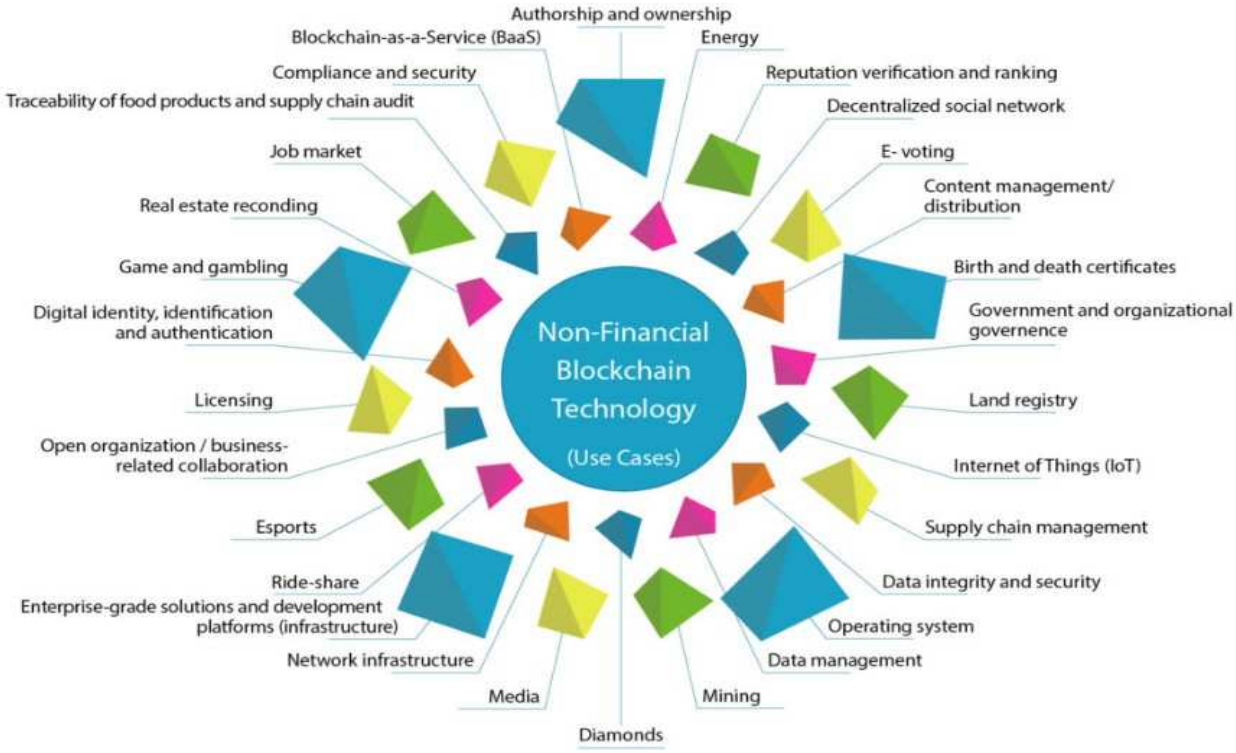
Σημαντικοί οργανισμοί συμμετέχουν ήδη σε έργα πιλοτικής εφαρμογής, βασισμένα σε τεχνολογία Blockchain, ενώ πολλά Κράτη–Μέλη έχουν λάβει σημαντικές πρωτοβουλίες.

6.1.5 Τομείς που χρηματοδοτούνται από την ΕΕ για ανάπτυξη εφαρμογών Blockchain

Προκειμένου να συγκεντρωθεί η απαραίτητη τεχνογνωσία, σε φάση υλοποίησης βρίσκονται αρκετά projects ιδιωτικά, δημόσια και κυρίως χρηματοδοτούμενα από την ΕΕ, ώστε να δοθεί το έναυσμα για να επιλέξει κανείς την τεχνολογία blockchain κατά προτεραιότητα, δίνοντας της επάξια τον πρωταγωνιστικό ρόλο. Μεγαλύτερη προοπτικής ανάπτυξης εφαρμογών blockchain έχουν οι επτά κάτωθι αναφερόμενοι τομείς:

1. **Η εφοδιαστική αλυσίδα**. Δεν μπορεί να αμφισβητήσει κανείς την υψηλή αξιοπιστία, διαφάνεια και ασφάλεια, που προσφέρει το blockchain στον τομέα αυτό, αφού και ανά πάσα στιγμή, μπορεί κάποιος να γνωρίζει από πού προήλθε, πού κατευθύνεται και πού βρίσκεται ένα προϊόν.
2. **Η ενέργεια**. Έξυπνα συμβόλαια που συνάπτονται μέσω blockchain, εξασφαλίζουν διαφάνεια στις συναλλαγές μεταξύ μεγάλων εταιριών, όπως είναι οι λεγόμενες εταιρείες ΑΠΕ (Ανανεώσιμες Πηγές Ενέργειας).
3. **Η υγεία και η φαρμακοβιομηχανία**. Δεδομένα τέτοιας μορφής όπως είναι τα ιατρικά αρχεία και τα αρχεία των ασθενών οφείλουν οι αρμόδιοι να τα διαφυλάξουν και να μην υπάρχει καμία απολύτως υποψία ότι αυτά θα διαρρεύσουν περαιτέρω. Σε ότι αφορά την παραποίηση–πλαστογράφηση των φαρμάκων, η τεχνολογία blockchain έχει τη δυνατότητα να την ελαχιστοποιήσει, αν όχι να την εκλείψει, στον μεγαλύτερο δυνατό βαθμό.
4. **Το Ίντερνετ των Πραγμάτων** (IoT)
5. **Τα αυτόνομα αυτοκίνητα και γενικά τα αυτοκίνητα**. Αρχεία δεδομένων με τεχνικά χαρακτηριστικά και στοιχεία απόδοσης τα οποία καταγράφονται με την πάροδο του χρόνου, δίδουν μια σαφή και πλήρη εικόνα για την κατάσταση του αυτοκινήτου, καθιστώντας αρωγό τον ίδιο τον ιδιοκτήτη του, για την ορθή επιτήρηση του οχήματός μου, μέχρι να έρθει η στιγμή που εγκαίρως θα απαιτηθεί η αντικατάστασή του.
6. **Οι χρηματοοικονομικές συναλλαγές και οι πληρωμές.** Οι τράπεζες έχουν αναπτύξει σχετικές εφαρμογές. Επρόκειτο για μια συνειδητοποιημένη ενέργεια, αφού υπάρχει πλήρη επίγνωση για την επανάσταση που η τεχνολογία blockchain έχει φέρει στον τομέα αυτό.
7. **Η ηλεκτρονική διακυβέρνηση. Στο σημείο αυτό, το οποίο αποτελεί και μέρος της παρούσας μελέτης, βρισκόμαστε** μεταξύ οράματος και πραγματικότητας. Ο δημόσιος τομέας έχει αναβαθμιστεί σημαντικά μέσω των ψηφιακών τεχνολογιών. Σε μια συστηματική προσπάθεια εφαρμογής πρακτικών **e-government σε επίπεδο Ε.Ε, η δημόσια διοίκηση εντάχθηκε στην "Ηλεκτρονική Ευρώπη – Η Κοινωνία της Πληροφορίας για όλους",** ήδη **από τον Δεκέμβριο του 1999**. Συγκεκριμένα υλοποιήθηκε το σχέδιο δράσης ***"Europe 2002 – Κοινωνία πληροφοριών για όλους" εγκαινιάζοντας πλέον το λεγόμενο " ηλεκτρονικό Κράτος "***. Η χρονική αφετηρία υπολογίζεται περίπου τότε, αφού ενισχύθηκαν σημαντικά οι διαδικτυακές υπηρεσίες και η γενικότερη

πρόσβαση των πολιτών σε αυτές, ενώ επιπροσθέτως αναπτύχθηκαν ραγδαία τα νέα πληροφοριακά συστήματα. Το ζητούμενο πλέον είναι η πρόσβαση του Κράτους στις ψηφιακές υπηρεσίες, τις οποίες πρέπει να υλοποιήσει με τον βέλτιστο τεχνικά τρόπο. Μια σημαντική ευκαιρία είναι η αξιοποίηση της τεχνολογία blockchain στις παρεχόμενες υπηρεσίες της.



Εικόνα 37: Οι περιπτώσεις χρήσης της τεχνολογίας blockchain [54]

6.2 Η διεθνής πρακτική για ένα αποκεντρωμένο και «έξυπνο» Κράτος

Εικόνα 38: Blockchain για ψηφιακή Κυβέρνηση [41]

Εμφανώς διαπιστώνουμε ότι οδεύοντας δυναμικά προς έναν ψηφιακό μετασχηματισμό χρησιμοποιώντας αποκλειστικά τις **αναδυόμενες τεχνολογίες στον δημόσιο τομέα**, οφείλουμε να διανύσουμε μεγάλη απόσταση από το σημείο που βρισκόμαστε σήμερα στη Χώρα μας, παρόλο που προαναφέρθηκε ότι έχουν πραγματοποιηθεί σπουδαία βήματα προόδου τα τελευταία χρόνια.

Το **Digital Future Society (DFS)**, ένα **think tank**[11] **- Ινστιτούτο Ερευνών** με έδρα τη Βαρκελώνη της Ισπανίας, ιδρύθηκε με σκοπό να **βοηθήσει τη δημόσια διοίκηση στη χάραξη πολιτικών**. Το DFS αναφέρεται στην Ευρωπαϊκή Ένωση, ενώ ασπάζεται πλήρως την άποψη της Ευρωπαϊκής Επιτροπής ότι «*οι επιτυχημένες προσπάθειες καινοτομίας για τη δημόσια πολιτική, όχι μόνο δημιουργούν καλύτερες δημόσιες υπηρεσίες, αλλά αυξάνουν την εμπιστοσύνη των πολιτών στις κυβερνήσεις*». Σε μία έκθεση με απτές συμβουλές και καλές πρακτικές ως προς την υιοθέτηση της Τεχνητής Νοημοσύνης και του Blockchain στη δημόσια διοίκηση, παρατίθενται παρακάτω τα συμπεράσματα της έκθεσης αυτής.

[11] **Δεξαμενή σκέψης** ή **ομάδα προβληματισμού** (αγγλικά: **think tank** ή *policy institute* ή *research institute*) είναι όρος ο οποίος χρησιμοποιείται για να χαρακτηρίσει ερευνητικούς οργανισμούς οι οποίοι ασχολούνται με μελέτες αντιμετώπισης μιας ευρύτατης ποικιλίας ζητημάτων (π.χ. πολιτικά, οικονομικά, τεχνολογικά και αμυντικά).

Διαπιστώθηκε λοιπόν ότι με την Τεχνητή Νοημοσύνη οι δημόσιες υπηρεσίες καθίστανται πιο «έξυπνες», διότι η επιδιωκόμενη ανάλυση πολλών δεδομένων μέσω εργαλείων και συστημάτων της, επιτυγχάνεται μιμούμενη ανθρώπινες λειτουργίες. Η δε τεχνολογία Blockchain αποτελεί ένα **νέο τρόπο οργάνωσης δικτύων χρηστών**, οι οποίοι ανταλλάσσουν μεταξύ τους δεδομένα με τρόπο γρήγορο, ασφαλή και κυρίως άμεσο, δηλαδή αποτελεί ένα **εργαλείο αποκεντρωμένων και αξιόπιστων συναλλαγών κράτους και πολιτών**. Και διερωτώμεθα, **θα μπορούσαν να συγκλίνουν μεταξύ τους**; Φυσικά και θα μπορούσαν. Με τον τρόπο αυτό θα προσδίδονταν ένα σημαντικό πλεονέκτημα στον έλεγχο της "ποιότητας" των εισερχόμενων δεδομένων σε ένα σύστημα AI. Τα εκ προθέσεως παραλλαγμένα δεδομένα σε ένα σύστημα AI, δίνουν ένα λανθασμένο ή αλλιώς παραποιημένο αποτέλεσμα. Η τεχνολογία blockchain μπορεί να προσφέρει τις **κατάλληλες δικλείδες ασφαλείας έτσι ώστε ένα σύστημα AI να είναι βέβαιο ότι διαβάζει τα σωστά δεδομένα.** Από την άλλη μεριά, μια πλατφόρμα που στηρίζεται σε τεχνολογία blockchain, αξιοποιώντας τις τεχνικές AI, θα επεξεργαστεί τα δεδομένα πιο «έξυπνα».

6.2.1 *Παραδείγματα εφαρμογών Blockchain διεθνώς στον ιδιωτικό τομέα*

Πασίγνωστες λιανεμπορικές αλυσίδες, ναυτιλιακές εταιρείες ή αρχές λιμένων σε ορισμένα από τα σημαντικότερα εμπορικά λιμάνια του κόσμου, έχουν επενδύσει σε αυτή την τεχνολογία. Στα λιμάνια της Σαγκάης και της επαρχίας Γκουάνγκτον, μέσω των οποίων διακινείται περίπου το 50% του εισαγωγικού και εξαγωγικού εμπορίου της Κίνας, οι λιμενικές αρχές έχουν **ήδη επενδύσει στο blockchain και την τεχνητή νοημοσύνη**, με μελλοντικό στόχο την αναβάθμιση των υπηρεσιών τους από λιμάνι σε λιμάνι και από αποθήκη σε αποθήκη.

Εταιρείες-κολοσσοί όπως η «Walmart» έχουν εντάξει το blockchain στα συστήματά τους. Με τη χρήση της τεχνολογίας του blockchain, μια έρευνα για τον εντοπισμό (tracing) - στην πηγή τους - φυλλωδών λαχανικών, που έχουν, π.χ. μολυνθεί από κάποιο μικρόβιο ή βακτήριο, η οποία μέχρι πρότινος διαρκούσε επτά ημέρες, μπορεί να ολοκληρωθεί σε χρόνο dt.

Μεγάλοι τραπεζικοί όμιλοι ανά τον κόσμο, εταιρείες που δραστηριοποιούνται σε κλάδους υγείας και φαρμακοβιομηχανίας, της αυτοκινητοβιομηχανίας, του πετρελαίου/αερίου, των χρηματοοικονομικών υπηρεσιών, των καταναλωτικών προϊόντων και μεταποίησης, της τεχνολογίας, των μέσων μαζικής ενημέρωσης και των τηλεπικοινωνιών καθώς επίσης και των τροφίμων, έχουν συνειδητοποιήσει πλήρως τις ραγδαίες αλλαγές που η τεχνολογία blockchain θα επιφέρει σε όλων των ειδών τις συναλλαγές μέσα στα επόμενα χρόνια και επενδύουν στην ανάπτυξη σχετικών project.

6.2.2 *Παραδείγματα εφαρμογών Blockchain διεθνώς στο δημόσιο*

- **Εσθονία και ψηφιακή ταυτότητα πολίτη**

Τεχνολογίες συναφείς με το Blockchain χρησιμοποιούνται προκειμένου οι πολίτες αλλά και οι δημόσιες υπηρεσίες να διαπιστώνουν την ακρίβεια των δεδομένων πολιτών, που κρατά το κράτος και να ελέγχουν το αν έχουν υποστεί αλλαγή στο χρόνο. Η ψηφιακή ταυτότητα πολίτη που δημιουργήθηκε από μία Εσθονική εταιρία, τη Guardtime, εδώ και αρκετά χρόνια,είναι η βάση όλων των ψηφιακών υπηρεσιών που απολαμβάνουν οι πολίτες.

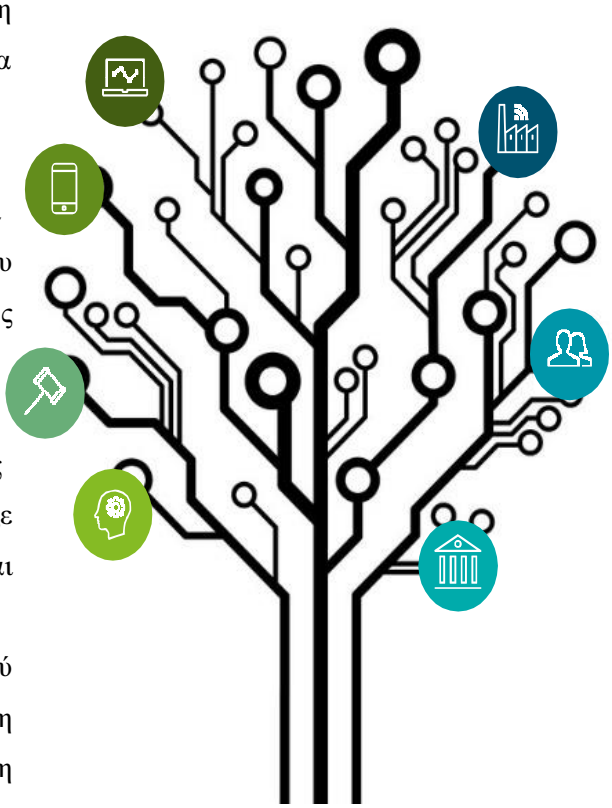
- **Ντουμπάι και πλήρης ψηφιοποίηση**

Το Ντουμπάι φιλοδοξεί να καταφέρει οι δημόσιες υπηρεσίες του να μην χρησιμοποιούν έντυπα και χαρτιά σε καμία μορφή, αλλά να είναι όλα ψηφιοποιημένα. **Με τη χρήση πλατφόρμας Blockchain** που δημιούργησε με την IBM, η Κυβέρνησή τους ισχυρίζεται ότι χρονοβόρες συναλλαγές μη ψηφιοποιημένες, πλέον πραγματοποιούνται μέσα σε λίγα δευτερόλεπτα εντελώς ψηφιακά.

Στην Ελλάδα, η έλλειψη καταρτισμένων ανθρώπων που θα γνωρίζουν να τα χειρίζονται και να τα δημιουργούν, αποτελεί ένα από τα σημαντικότερα προβλήματα. Παρόλα αυτά, **η τεχνολογία blockchain διαφαίνεται να αποτελεί το πιο δημοκρατικό μέσο συναλλαγής**, αφού τίθενται κανόνες από τους ίδιους τους χρήστες του, δημιουργώντας έντονα το συναίσθημα της ασφάλειας.
Προβληματίζει όμως το γεγονός ότι ενώ στα δημόσια δίκτυα η χειραγώγηση είναι κάτι παραπάνω από απίθανη, καθώς συμμετέχουν πολλοί χρήστες και δημιουργούν έναν γρίφο με μια τεράστια αλυσίδα συναλλαγών, στα ιδιωτικά ή υβριδικού τύπου δίκτυα, ο κίνδυνος αυτός είναι υπαρκτός. Σε επίπεδο λοιπόν υιοθέτησης και αποδοχής των εν λόγω τεχνολογιών στον δημόσιο τομέα, υπήρξαν διχογνωμίες. Όμως, πληθώρα αντικειμενικών ισχυρισμών ειδικών επιστημόνων αναφέρουν τα οφέλη χρήσης τους και τους λόγους για τους οποίους είναι θεμιτό να επενδύσουν σε αυτές οι δημόσιες υπηρεσίες, ανεξάρτητα από την ασάφεια και το ρίσκο που ενδεχομένως τέτοιου είδους ενέργειες συνεπάγονται. Εκτενέστερη αναφορά σχετικά με την προοπτική και τις πρωτοβουλίες δημόσιων φορέων στη Χώρα μας, ακολουθεί σε επόμενο υποκεφάλαιο.

6.3 Το έξυπνο Κράτος - Η σχέση του Blockchain με τη δημόσια διοίκηση

6.3.1 *Η ψηφιακή ωριμότητα του Δημόσιου τομέα*



Το ζητούμενο σε κάθε σύγχρονη κοινωνία είναι η υιοθέτηση αξιακών προτύπων, που δύναται να αναβαθμίζουν ποιοτικά και διαχρονικά τη διοίκηση.

Η αποτελεσματικότητα, η αποδοτικότητα και η αξιολόγηση υπήρξαν ανέκαθεν επιθυμητοί στόχοι στον ιδιωτικό τομέα. Στην περίπτωση του δημοσίου τομέα και ειδικότερα της δημόσιας διοίκησης αντίστοιχες επιδιώξεις καθυστέρησαν αρκετά να εδραιωθούν, αφού στη συλλογική συνείδηση των δυτικών κοινωνιών υπήρχε το πρότυπο ενός παρεμβατικού Κράτους, το οποίο ρύθμιζε συστηματικά ένα ευρύ φάσμα της οικονομικής και κοινωνικής ζωής.

Βασικά δομικά χαρακτηριστικά ενός γραφειοκρατικού μοντέλου αποτελούν η αυστηρή ιεραρχική δομή, η τυποποίηση καθηκόντων και αρμοδιοτήτων και η προσήλωση στις εκάστοτε κανονιστικές ρυθμίσεις. Έκτοτε, τα χαρακτηριστικά αυτά τείνουν να εκλείψουν καθώς μέσα σε ένα μεταβαλλόμενο ανταγωνιστικό οικονομικό περιβάλλον σε τοπικό και διεθνές επίπεδο, τα χαρακτηριστικά αυτά δεν αποτελούν πλέον εγγυήσεις σταθερότητας, αξιοπιστίας και επάρκειας. Αντιθέτως, τείνουν να μετεξελιχθούν σε εγγενείς αδυναμίες της δημόσιας διοίκησης. Η δημόσια διοίκηση οφείλει να αντιμετωπίζει τους πολίτες της με ανάλογη εξυπηρέτηση και τις αντίστοιχες αρχές του ιδιωτικού τομέα, και να μη λειτουργεί ως μία σειρά από μεμονωμένες, ασύνδετες υπηρεσίες. Σημαντική αρχή σε αυτήν την κατεύθυνση αποτελεί η εφάπαξ καταχώριση δεδομένων σε συστήματα του δημοσίου κατά την αλληλεπίδραση με τους φορείς της δημόσιας διοίκησης (“once-only principle ”).

Υπάρχει όμως μια πολύ σημαντική αρχή η οποία είναι αδύνατο να παραβλεφθεί. Αναφερόμαστε στην δράση της δημόσιας διοίκησης η οποία καθοδηγείται από την αρχή της νομιμότητας και αποτελεί θεμελιώδη αρχή, σύμφυτη με την έννοια του Κράτους Δικαίου και αποβλέπει στην εξυπηρέτηση του δημοσίου συμφέροντος. Η δομή της διοικητικής δράσης θεμελιώνεται σε κανόνες δικαίου. Αυτή η προσήλωση στους εξαντλητικά λεπτομερείς κανόνες που ρυθμίζουν, οριοθετούν και διέπουν σχεδόν κάθε πτυχή της οργανωτικής δράσης, εγγυάται τη σταθερότητα και προβλεψιμότητα, την άρση των αβεβαιοτήτων, την περιθωριοποίηση των παρεκκλίσεων και της αυθαίρετης συμπεριφοράς και την

γρήγορη απόκριση στην αντιμετώπιση, γνωστών κυρίως, προβλημάτων. Η δε προβλεψιμότητα των ενεργειών συμβάλλει στη δημιουργία ενός αισθήματος ασφάλειας, διευκολύνοντας την κατάρτιση σχεδίων δράσης από τους αρμοδίους των φορέων.

Το νέο σύστημα αρχών που πλέον υιοθετήθηκε υπό την προσέγγιση του New Public Management, ήρθε να αμφισβητήσει το παγιωμένο πρότυπο δημόσιας διοίκησης και να διαταράξει αρχές όπως είναι η μονιμότητα, εισάγοντας νέες όπως τη στοχοθεσία, την αποτελεσματικότητα, την αποδοτικότητα και τη λογοδοσία. Όμως, η έλλειψη διαχρονικού και ουσιαστικού οράματος, παρότι τυπικά κατά καιρούς έχουν δημοσιοποιηθεί αρκετές σχετικές προσεγγίσεις, δημιούργησε πολλές «ευκαιριακές» υλοποιήσεις, μεμονωμένες πρωτοβουλίες, ενίοτε εκπλήρωση αποσπασματικών σχεδιασμών συγκεκριμένων φορέων, ασαφείς αρμοδιότητες με πολλούς εμπλεκόμενους φορείς, προβληματικό θεσμικό πλαίσιο καθώς και δυσκολίες διαμοιρασμού / δια λειτουργικότητας / συνεργασίας συντείνοντας σε έναν έντονο κατακερματισμό. Βασικό πρόβλημα αποτελούν η έλλειψη διασύνδεσης μεταξύ των συστημάτων του δημοσίου και η αδυναμία αποτελεσματικής διαχείρισης και επαναχρησιμοποίησης του πλούτου της πληροφορίας που είναι συγκεντρωμένος στα διάφορα πληροφοριακά συστήματα και που θα μπορούσε να αξιοποιηθεί σημαντικά για την καλύτερη λήψη αποφάσεων μέσα στο δημόσιο.

Από την άλλη μεριά, αρκετές μεταρρυθμιστικές προσπάθειες έχουν συναντήσει έντονες αντιδράσεις και αντιστάσεις, τόσο από τις κατά καιρούς πολιτικές ηγεσίες των δημόσιων οργανισμών όσο και από τα διοικητικά στελέχη σε όλα τα ιεραρχικά επίπεδα. Σημαντικό είναι επίσης το γεγονός ότι δεν υφίσταται ακόμη ένα πρότυπο μοντέλο διοίκησης, η αυστηρή οριοθέτηση του οποίου, να οδηγεί στην επιτυχία. Παρόλα αυτά, το νέο Δημόσιο Management προσφέρει πλεονεκτήματα και ευκαιρίες, ενώ οι προσδοκίες διαφαίνεται ότι φέρουν θετικό πρόσημο τα τελευταία χρόνια, με την τεχνολογία να πρωτοστατεί σε πολλά νέα εγχειρήματα.

6.3.2 *Blockchain τεχνολογία ως παράγοντας ψηφιακού μετασχηματισμού*

Ο ψηφιακός εκσυγχρονισμός της δημόσιας διοίκησης δεν είναι ένα αμιγώς τεχνοκρατικό θέμα· πρόκειται για ένα **βαθιά κοινωνικό ζήτημα** με επίκεντρο τον άνθρωπο. Γι' αυτό, η οριοθέτηση και η αντιμετώπισή του οφείλει να αποτελεί βασική προτεραιότητα των κυβερνώντων, αλλά και της ίδιας της κοινωνίας των πολιτών και των φορέων της. Ο ψηφιακός μετασχηματισμός προβλέπεται ότι θα άρει τις υφιστάμενες δυσλειτουργίες, με αποτέλεσμα τη βελτίωση της ποιότητας εξυπηρέτησης του πολίτη και τη μείωση του διοικητικού φόρτου που επιβαρύνει καθημερινά πολίτες και επιχειρήσεις κατά την αλληλεπίδρασή τους με το δημόσιο.

Προτεραιότητα της Ευρωπαϊκής Επιτροπής είναι η υιοθέτηση της τεχνολογίας Blockchain, αφού έχει αποδειχθεί εξαιρετικά αποτελεσματική για τις δημόσιες διοικήσεις σε παγκόσμιο επίπεδο, σε σχέση πάντα με τις ιδιαιτερότητες της ελληνικής δημόσιας διοίκησης. Παρά την πρόοδο που παρατηρείται τα τελευταία έτη στη χώρα, η συνολική αποτίμηση της ηλεκτρονικής διακυβέρνησης δεν μπορεί να χαρακτηριστεί θετική. Όπως αναδεικνύει ο δείκτης DESI, ο πιο δημοφιλής δείκτης για την

ηλεκτρονική διακυβέρνηση στην Ευρώπη, η Ελλάδα όχι απλώς υστερεί σε σχέση με το σύνολο σχεδόν των χωρών-μελών της Ευρωπαϊκής Ένωσης, αλλά μεγαλώνει το χάσμα, κατατάσσοντας τη Χώρα μας πλέον 27η σε σύνολο 28 χωρών και με συνεχώς πτωτική τάση. Ως θετικά στοιχεία σημειώνονται ορισμένα κομβικά έργα και υποδομές που πλέον υφίστανται και όπου βλέπουμε εν γένει μία εντονότερη δραστηριοποίηση τα τελευταία έτη.

Στρατηγική προτεραιότητα αποτελεί η αξιοποίηση των δεδομένων που βρίσκονται αποθηκευμένα στα συστήματα του δημοσίου. Αυτός ο πλούτος πληροφορίας μπορεί να προσφέρει πραγματικό περιεχόμενο στο επιτελικό κράτος υποστηρίζοντας τη λήψη τεκμηριωμένων αποφάσεων και τον πιο αποτελεσματικό σχεδιασμό δημόσιων πολιτικών και προσφερόμενων υπηρεσιών. Στόχοι της εν λόγω κατεύθυνσης λογίζονται η αύξηση της λογοδοσίας και της διαφάνειας στις αποφάσεις της Διοίκησης, η βελτίωση της πρόσβασης στην πληροφορία σχετικά με τη διοικητική διαδικασία, καθώς και η ενίσχυση του κράτους δικαίου και της νομιμότητας μέσω βελτίωσης της πρόσβασης στην εθνική και ευρωπαϊκή νομοθεσία, αλλά και τις αποφάσεις ευρωπαϊκών δικαστηρίων. **Η ψηφιακή εξυπηρέτηση με τον** περιορισμό της χρήσης του χαρτιού αποτελεί ταυτόχρονα και στόχο αλλά και υποκείμενο της αλλαγής που πρέπει να επιτευχθεί.

Σε τεχνικό επίπεδο, η εξασφάλιση της δια λειτουργικότητας μεταξύ των συστημάτων του δημοσίου, η χρήση ανοικτών προτύπων και ανοιχτού λογισμικού, η αξιοποίηση των ανοιχτών δεδομένων, καθώς και η υιοθέτηση ενός κεντρικού αποθετηρίου δια λειτουργικότητας και συνεργασίας για τις εφαρμογές του δημοσίου, αξιοποιώντας το παράδειγμα του **https://joinup.ec.europa.eu/,** αποτελούν βασικά συστατικά για την εύρυθμη λειτουργία του δημοσίου τομέα και απαραίτητες προϋποθέσεις για την υλοποίηση του ψηφιακού μετασχηματισμού. Ενώ ακόμη και η προώθηση δράσεων ανοικτής διακυβέρνησης και συμμετοχικότητας μπορούν να ενισχύσουν τη λογοδοσία, τη διαφάνεια και τη νομιμότητα στη διοικητική δράση, και να υποστηρίξουν κάτι πολύ σημαντικό, τη **διαδικασία ανάκτησης της εμπιστοσύνης των πολιτών προς το κράτος και κατ' επέκταση την ενίσχυση των δημοκρατικών θεσμών.**

6.3.3 *Η Blockchain τεχνολογία ως όπλο κατά της διαφθοράς*

Η ύπαρξη ενός περίπλοκου και ασαφούς νομοθετικού πλαισίου, η παρεμβατικότητα του Κράτους, η απουσία ή ελλιπής εφαρμογή προληπτικού και κατασταλτικού ελέγχου καθώς και ποινικών ή πειθαρχικών κυρώσεων ενθαρρύνουν επί σειρά ετών τα φαινόμενα διαφθοράς. Η διαφθορά αποτελεί έναν από τους βασικότερους αποσταθεροποιητικούς παράγοντες των σύγχρονων κοινωνιών, επιβάλλοντας σε κράτη και οργανισμούς την ανάπτυξη ολοκληρωμένων και αποτελεσματικών συστημάτων για την πρόληψη και καταστολή της. Στη διεθνή βιβλιογραφία καθώς και στα επίσημα κείμενα και έγγραφα εργασίας των περισσοτέρων κυβερνήσεων και διεθνών οργανισμών, **η**

διαφθορά[12] **ορίζεται ως η κατάχρηση της δημόσιας θέσης για ιδιωτικό όφελος** (the misuse or abuse of public office for private gain). Πρόκειται για έναν ορισμό ο οποίος είναι γνωστός και σαν **«ο ορισμός των οκτώ λέξεων»** και έχει δεχθεί έντονη κριτική σχετικά με τα προβλήματα που δημιουργεί τόσο από επιστημολογική άποψη όσο και από εκείνη της συνεισφοράς του στην αποτελεσματική αντιμετώπιση του φαινομένου.

Η υπευθυνότητα, η αυτοματοποίηση και η ασφάλεια που προσφέρει το blockchain για το χειρισμό δημόσιων αρχείων θα μπορούσε τελικά να εμποδίσει τη διαφθορά και να καταστήσει τις κυβερνητικές υπηρεσίες πιο αποτελεσματικές. **Το blockchain της διακυβέρνησης** στοχεύει στην παροχή των ίδιων υπηρεσιών που προσφέρονται από το κράτος και τις αντίστοιχες δημόσιες αρχές του με αποκεντρωμένο και αποτελεσματικό τρόπο διατηρώντας παράλληλα την ίδια ισχύ. **Η ενσωμάτωση των ψηφιακών τεχνολογιών στην καθημερινή ζωή** απαιτεί μηχανισμούς που μπορούν να προσδιορίσουν με ακρίβεια ποιοι είναι οι χρήστες και να πιστοποιούν τα βασικά χαρακτηριστικά τους όπως όνομα, διεύθυνση, πιστωτικό αρχείο, καθώς και άλλα προσωπικά στοιχεία τους. Η Stampery είναι μια εταιρεία πιστοποίησης που χρησιμοποιεί blockchain για να δημιουργήσει μια σφραγίδα email ή εγγράφων. Το σημαντικότερο όλων όμως είναι **ότι οι πληροφορίες που αποθηκεύονται στο blockchain, μπορούν να επαληθευτούν και να ελεγχθούν.**

Το προαναφερθέν πλαίσιο αξιών, αρχών και στόχων της εξουσίας, **συνοψίζεται η έννοια της Καλής Διακυβέρνησης (Good Governance), όπως αυτή ορίζεται από την Παγκόσμια Τράπεζα**, η οποία θέτει ως βασικές προϋποθέσεις της τα εξής: τη διαμόρφωση μίας εμποτισμένης με επαγγελματικό ήθος γραφειοκρατίας, την ύπαρξη μίας εκτελεστικής εξουσίας που είναι υπεύθυνη (accountable) και λογοδοτεί για τις πράξεις της και την ανάπτυξη μίας ισχυρής κοινωνίας πολιτών που συμμετέχει στις δημόσιες υποθέσεις. Εν κατακλείδι, η ικανότητα ανάπτυξης ολοκληρωμένων και αποτελεσματικών συστημάτων ελέγχου της διαφθοράς μέσω της τεχνολογίας blockchain θα μπορούσε να αποτελέσει την πρωτεύουσα μεταβλητή και απαραίτητη προϋπόθεση για την αύξηση των επιπέδων ανάπτυξης της Καλής Διακυβέρνησης.

[12] Ο ορισμός αυτός προτάθηκε πρώτη φορά το 1996 από τον P. Bardhan, ειδικό συνεργάτη του Ο.Ο.Σ.Α. και έκτοτε αποτέλεσε, με διάφορες παραλλαγές, τον κυρίαρχο ορισμό για τη διαφθορά. Βλ. Λάζος Γ., Διαφθορά και Αντιδιαφθορά, εκδ. Νομική Βιβλιοθήκη, 2005, σελ. 40

6.3.4 *Το παράδειγμα της Βόρειας Ελλάδας*

Μετά την Εσθονία, την Ισπανία, την Ολλανδία και τη Μάλτα, όπου συναντάται η αντίστοιχη τεχνολογία, εκδηλώθηκε ενδιαφέρον και από ελληνικούς δήμους. Συγκεκριμένα, **ο Δήμος Κατερίνης** συμμετέχει σε ευρωπαϊκό έργο και ειδικότερα ο Δήμος Παύλου Μελά έχει επιδείξει ενδιαφέρον για τη χρήση του Blockchain περί διενέργειας ηλεκτρονικής ψηφοφορίας, ενώ παράλληλα αναζητούνται κι άλλοι τομείς στους οποίους μπορούν να εφαρμοστούν τέτοιου είδους λύσεις, όπως η λογιστική, η ταμειακή διαχείριση και ο προϋπολογισμός. Το πρόγραμμα αυτό λειτουργεί πιλοτικά στον Δήμο Κατερίνης μέσω μιας εφαρμογής υποστηριζόμενη από τεχνολογίες Blockchain. Την σχεδίαση και την υλοποίηση της εφαρμογής αυτής έχει αναλάβει να συντονίσει το Ινστιτούτο Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΙΠΤΗΛ) του Εθνικού Κέντρου Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ) στο πλαίσιο του Horizon 2020 του ευρωπαϊκού έργου με την κωδική ονομασία TOKEN (Transformative Impact Of Blockchain Technologies In Public Services).

Το χαρακτηριστικό στοιχείο της διαφάνειας της τεχνολογίας Blockchain έγκειται στο γεγονός ότι το ιστορικό ενεργειών δεν επιτρέπει τη διαγραφή στοιχείων, που έχουν καταχωρηθεί από πιστοποιημένους χρήστες. Καταγράφονται αυστηρώς διαδοχικά οι εντολές, οι πράξεις και οι πληρωμές σε κάθε στάδιο για την προμήθεια ή την εκτέλεση μιας υπηρεσίας. Η ψηφιακή υπογραφή καθιστά εφικτή την παρακολούθηση της χρονικής αλληλουχίας των ενεργειών και της απόδοσης των χρημάτων με έναν τρόπο απόλυτα διαφανή. Μια ηλεκτρονική ψηφοφορία για πολιτιστικές δράσεις, ζητήματα εκπαίδευσης ή δημοσίων έργων, καθίσταται αμετάβλητη, αφού επιπροσθέτως δίδεται η δυνατότητα για την παρακολούθηση στον επιμερισμό των χρημάτων ανά τομέα ή και την παρακολούθηση της ροής των εργασιών από τους πολίτες.

Παρατηρείται ότι η τεχνολογία αυτή εξελίσσεται διαρκώς, τα πεδία εφαρμογής της διευρύνονται και οι εμπλεκόμενοι φορείς αναζητούν δυνατότητες υλοποίησης του Blockchain, προσδοκώντας τα οφέλη της διαφάνειας, της ηλεκτρονικής δημοκρατίας και της ασφάλειας. Συνετό θα ήταν να ακολουθήσουν και άλλες πόλεις μια παρόμοια διαδρομή.

6.3.5 *Το παράδειγμα της Κύπρου*

Η Κυπριακή Δημοκρατία, συμπορευόμενη με το ευρωπαϊκό και παγκόσμιο ρεύμα προόδου έχει επίσης επιχειρήσει να δημιουργήσει το κατάλληλο περιβάλλον, σε επίπεδο επιχειρήσεων, εταιρειών, υπηρεσιών και επενδύσεων, υιοθετώντας καινοτόμες πρακτικές και διαδικασίες, όπως είναι η τεχνολογία Blockchain. Στα πλαίσια της Εθνικής Στρατηγικής της, το πρόγραμμα με τίτλο «Αποκεντρωμένες Τεχνολογίες» κρίθηκε ότι αποτελεί την πιο αποτελεσματική μορφή μεταρρύθμισης και βελτίωσης της παραγωγικότητας στον δημόσιο τομέα.

Η Κυπριακή Δημοκρατία υπέγραψε την *Ευρωπαϊκή Συνεργασία Τεχνολογίας Blockchain* στις 4 Ιουνίου 2018 και μαζί με άλλα έξι κράτη μέλη της Ευρωπαϊκής Ένωσης (Μάλτα, Γαλλία, Ελλάδα, Ιταλία, Πορτογαλία και Ισπανία) υπέγραψε την κοινή *Δήλωση των χωρών του Νότου της*

Μεσογείου για την Τεχνολογία Κατανεμημένου Καθολικού (‘*Declaration of the Southern Mediterranean Countries on Distributed Ledger Technologies*’) στις 4 Δεκεμβρίου 2018, με στόχο να ενισχύσουν τη συνεργασία στον ψηφιακό τομέα και να καταστήσουν τον Νότο της Ευρώπης, ηγέτη στις αναδυόμενες τεχνολογίες, όπως είναι η ΤΚΚ.[13] Επιπροσθέτως, το Υπουργικό Συμβούλιο αποφάσισε τη δημιουργία AdHoc[14] Ομάδας Εργασίας για την Ανάπτυξη της Τεχνολογίας Blockchain (“*AdHoc Επιτροπή*”), προκειμένου η Κύπρος να αξιολογήσει και να αντιμετωπίσει προορατικά τις ευκαιρίες και τις προκλήσεις που αντιπροσωπεύουν η τεχνολογία ΤΚΚ και η αλυσίδα συστοιχιών[15]. Όπως τεκμηριώνεται από το *Παρατηρητήριο της Ευρωπαϊκής Ένωσης για το Blockchain* (European Union Blockchain Observatory and Forum), η ακαδημαϊκή κοινότητα στην Κύπρο, είναι ιδιαίτερα δραστήρια στον τομέα των αλυσίδων συστοιχιών. Μάλιστα, η Επιτροπή Κεφαλαιαγοράς Κύπρου δημιούργησε το 2018 τον Κόμβο Καινοτομίας που επικεντρώνεται στην χρηματοπιστωτική τεχνολογία (Fintech) και στην τεχνολογία κανονιστικής συμμόρφωσης (RegTech), συμπεριλαμβανομένης της χρησιμοποίησης της τεχνολογίας Blockchain και άλλων τεχνολογιών ΤΚΚ. Ο Κόμβος Καινοτομίας έχει σχεδιαστεί προκειμένου να λαμβάνει αξιολογεί και να διευκολύνει την πρόοδο σε τεχνολογικές εφαρμογές στον χρηματοπιστωτικό τομέα, και να προαγάγει μία πιο αποτελεσματική σχέση μεταξύ των εταιριών χρηματοπιστωτικής τεχνολογίας. Η Κεντρική Τράπεζα της Κύπρου σκοπεύει να δημιουργήσει επίσης κόμβο καινοτομίας.

Με γνώμονα λοιπόν την υιοθέτηση μιας τεχνολογίας που θα δώσει τη δυνατότητα στους πολίτες να ελέγχουν τα δικά τους δεδομένα και μέσω της οποία θα παρακάμπτονται οι μεσάζοντες για την εκτέλεση συναλλαγών, επιλέχθηκαν τα έξυπνα συμβόλαια, μεγιστοποιώντας κατά συνέπεια τα οφέλη της αποκέντρωσης. Προβλέπεται ότι με αυτό τον τρόπο, θα έχουν τη δυνατότητα οι εταιρίες αλλά και οι δημόσιοι φορείς να αναδιαμορφώνουν ή να δημιουργήσουν νέα επιχειρηματικά μοντέλα.

Η τεχνολογία blockchain κρίθηκε ότι είναι μια μοναδική ευκαιρία για μετασχηματισμό/μεταρρύθμιση του εθνικού του προϊόντος, καθώς η Κύπρος μπορεί να αποτελέσει από τα κορυφαία κέντρα καινοτομίας και ανάπτυξης παγκοσμίως με ισχυρή τεχνολογική υποδομή. Προκειμένου όμως να πραγματοποιηθεί κάτι τέτοιο, θα πρέπει να δημιουργηθεί το κατάλληλο κανονιστικό και θεσμικό πλαίσιο αλλά και στήριξη σε κυβερνητικές επιχειρήσεις και σε επιχειρήσεις για να επιταχυνθεί η επιχειρησιακή ετοιμότητα της αλυσίδας συστοιχιών.

---

[13] Τεχνολογίες κατανεμημένου καθολικού (αγγλική απόδοση όρου DLT)

[14] ***ad hoc*** σημαίνει μια λύση σχεδιασμένη για ένα συγκεκριμένο πρόβλημα ή έργο, μη γενικεύσιμο, και δεν προορίζεται να είναι σε θέση να προσαρμόζεται για άλλους σκοπούς (Πηγή : https://el.wikipedia.org/wiki/Ad_hoc)

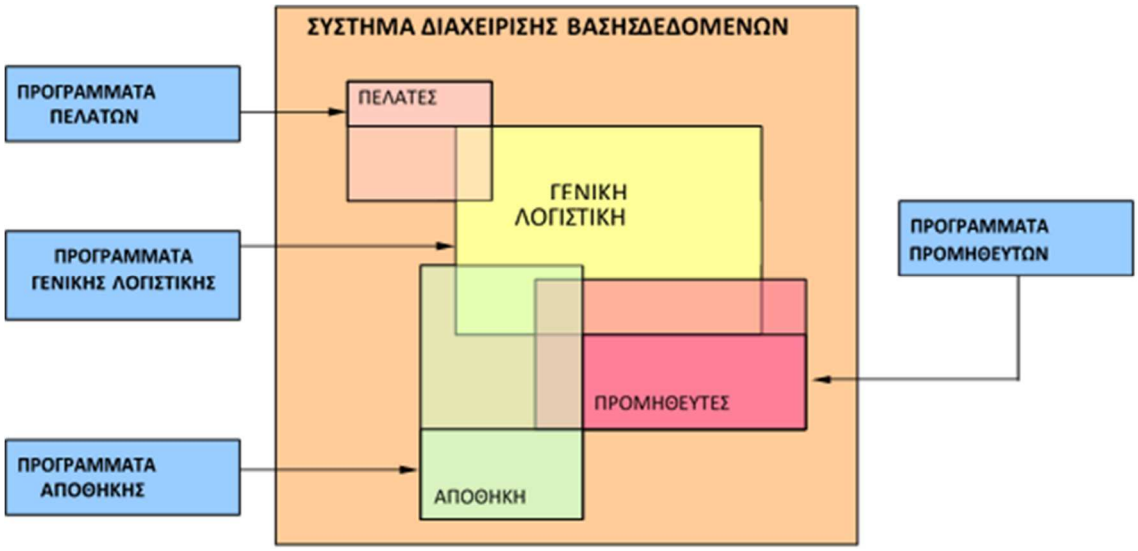
[15] **Blockchain** (στα ελληνικά ο αγγλικός όρος αποδίδεται ποικιλοτρόπως, ως *αλυσίδα μπλοκ* ή *μπλοκ αλυσίδας*, *αλυσίδα συστοιχιών*, *τεχνολογία κατανεμημένης εγγραφής*, *αλυσίδα ομάδων συναλλαγών*, *αλυσίδα κοινοποιήσεων*. *Πηγή : https://el.wikipedia.org/wiki/Blockchain*

Κεφάλαιο 7ο - Η προστιθέμενη αξία των πλατφορμών blockchain

7.1 Από ένα κεντροποιημένο μητρώο σε ένα διαμοιρασμένο μητρώο

Η τακτική τήρησης χειρόγραφων λογιστικών βιβλίων από τις επιχειρήσεις, αποτελεί μια πεπαλαιωμένη μέθοδο για την καταγραφή των διάφορων κινήσεων και συναλλαγών που πραγματοποιούνται καθώς και για την αποθήκευση του ιστορικού αυτών των κινήσεων. Με την εμφάνιση των υπολογιστών, αυτή η διαδικασία **ψηφιοποιήθηκε.** Είναι γεγονός ότι οι οργανισμοί και οι επιχειρήσεις τηρούν πληθώρα αρχείων δεδομένων. Επειδή όμως πολλά από αυτά εμφανίζονταν αρκετές φορές και δυσχέραιναν τις διαδικασίες κατά το στάδιο **λήψης των επιχειρησιακών αποφάσεων**, επινοήθηκαν **οι λεγόμενες Βάσεις Δεδομένων (Databases)**. Τα δεδομένα πλέον εξελίχθηκαν σε ολοκληρωμένα (integrated) και καταμερισμένα (shared) αρχεία έτσι ώστε, αφενός μεν **τα πλεονάζοντα (redundant) δεδομένα να αποθηκεύονται όσο το δυνατόν λιγότερες φορές, αφετέρου δε να είναι προσπελάσιμα, από διάφορους χρήστες και να αξιοποιούνται από ποικίλες εφαρμογές.** Για την ενημέρωση ενός δεδομένου αρκεί μόνο μία αλλαγή, η οποία αυτομάτως επηρεάζει το ίδιο δεδομένο το οποίο βρίσκεται σε διαφορετικά αρχεία, με αποτέλεσμα την επίσπευση των διαδικασιών, αφού τα αποτελέσματα της ενημέρωσης, είναι προσπελάσιμα από όλους τους χρήστες και τις εφαρμογές του Οργανισμού ή της Επιχείρησης **συγχρόνως.**

Παραδείγματος χάριν, μια τράπεζα έχει τα δικά της μητρώα με τις πληροφορίες που χρειάζεται: τα στοιχεία των πελατών, τις συναλλαγές και διάφορες άλλες κινήσεις που συμβαίνουν, τις καταστάσεις των λογαριασμών κοκ. Για να αγοραστεί ένα σπίτι, ο αγοραστής θα χρειαστεί να παρουσιάσει αποδεικτικά στοιχεία για την οικονομική του κατάσταση, ενώ ο ιδιοκτήτης θα πρέπει να αποδείξει ότι του ανήκει το κτήριο. Ο μεν λοιπόν θα ζητήσει τα σχετικά στοιχεία από την βάση δεδομένων της τράπεζας ή της εφορίας και ο δε θα πάρει το τίτλο ιδιοκτησίας από τον συμβολαιογράφο. Παραδείγματα σαν κι αυτά, δείχνουν τον τρόπο λειτουργίας των εν λόγω βάσεων δεδομένων καθώς και τις σχέσεις γύρω από αυτές. Θα λέγαμε ότι αυτά τα μητρώα είναι κεντροποιημένα, με την έννοια ότι είναι ιδιοκτησία των συγκεκριμένων φορέων/ οργανισμών και η πρόσβαση σε αυτά γίνεται μόνο μέσω αυτών. Το γεγονός ότι δεν μπορεί ο καθένας να έχει πρόσβαση στο τραπεζικό ή ιατρικό ιστορικό του οποιουδήποτε, δεν είναι στοιχείο της "κεντροποίησης" αλλά της ασφάλειας. Όπως επίσης και το γεγονός ότι οι πληροφορίες είναι έγκυρες, είναι στοιχείο της αξιοπιστίας του εκάστοτε οργανισμού. Οι διάφοροι φορείς/οργανισμοί/επιχειρήσεις εγγυώνται για την ασφάλεια και γνησιότητα των δεδομένων και έτσι οι πελάτες/πολίτες τους εμπιστεύονται για τις όποιες διαδικασίες. Ενώ λοιπόν το μελάνι στο χαρτί αντικαταστάθηκε από τα bits στους σκληρούς δίσκους, το βασικό μοντέλο λειτουργίας έμεινε το ίδιο: **μια βάση δεδομένων που δημιουργείται, ανανεώνεται, επιβεβαιώνεται, ασφαλίζεται και συντηρείται με τον ίδιο συγκεκριμένο τρόπο**. Η γενική ιδέα της Βάσης Δεδομένων διαφαίνεται στο παρακάτω σχήμα.



Εικόνα 39: Η γενική ιδέα της Βάσης Δεδομένων

Επρόκειτο δηλαδή για μία οργανωμένη συλλογή από συσχετιζόμενα δεδομένα που χρησιμοποιούνται από όλες τις εφαρμογές ενός Οργανισμού ή μιας Επιχείρησης, **ένα πλήρως ενημερωμένο λογιστικό βιβλίο.** Το blockchain είναι στην ουσία ένα νέου τύπου λογιστικό βιβλίο (ledger). Διότι… αυτό το βιβλίο/μητρώο δεν είναι αποθηκευμένο κάπου κεντρικά. **Υπάρχει, ανανεώνεται και συντηρείται σε κάθε κόμβο ενός δια-μοιρασμένου (distributed) δικτύου.** Κάθε κόμβος έχει ένα αντίγραφο ολόκληρου αυτού του μητρώου: τις καταστάσεις των κόμβων, το ιστορικό των μεταξύ τους συναλλαγών κλπ. Για την ασφάλειά του έχει επιλεγεί ή μέθοδος της κρυπτογραφίας, ενώ μέσω αλγορίθμων και διαφόρων άλλων τεχνικών επισφραγίζεται η γνησιότητα των πληροφοριών

Πίνακας 2: Σύγκριση μεταξύ παραδοσιακών εγγραφών, βάσεων δεδομένων και blockchain μεταφρασμένο [37]

	Αξιοπιστία (τα αρχεία δεν μπορούν να χαθούν)	Ευκολία (εύκολη εισαγωγή και προβολή)	Διαφάνεια (ελεγχόμενα αρχεία)	Εγκυρότητα (τα αρχεία δεν μπορούν να παραποιηθούν)
Εφαρμογές καταγραφής με βάση το χαρτί	✗	✗	✗	✗
Εφαρμογές καταγραφής με τοπική βάση δεδομένων	✗	✓	✓	✗
Εφαρμογές καταγραφής με διαδικτυακή βάση δεδομένων	✓	✓	✓	✗
Blockchain	✓	✓	✓	✓

7.2 Σύγκριση χαρακτηριστικών Bitcoin, Ethereum και Hyperledger

Οι περιπτώσεις χρήσης των διαφόρων εφαρμογών blockchain έχουν ήδη μετασχηματίσει το τεχνολογικό υπόβαθρο. Αρχικά αναπτύχθηκε το bitcoin προκειμένου να ενισχύσει τον χρηματοπιστωτικό φορέα. Στην συνέχεια, έκαναν την εμφάνισή τους εφαρμογές blockchain για οικονομικά αντικείμενα, όπως είναι οι έξυπνες συμβάσεις, οι ασφάλειες και το crowdfunding, ενώ τα τελευταία χρόνια βρίσκει εφαρμογή ακόμη ή και σε συστήματα ψηφοφορίας.

Το Bitcoin αποτελεί το χρυσό πρότυπο των ψηφιακών περιουσιακών στοιχείων. Πέραν τούτου είναι ένα καθολικό βιβλίο, το οποίο καταγράφει τις συναλλαγές που πραγματοποιούνται στο δίκτυο Bitcoin.

Το Ethereum είναι μία αποκεντρωμένη πλατφόρμα που αξιοποιείται κυρίως για την συγγραφή και την εφαρμογή έξυπνων συμβολαίων. Με την προγραμματιστική γλώσσα που χρησιμοποιεί, δημιουργεί έξυπνα συμβόλαια και επιτρέπει σε περίπλοκες εφαρμογές όπως είναι οι χρηματοοικονομικές συναλλαγές, να εκτελούνται στην αποκεντρωμένη πλατφόρμα. Έχει γρήγορη ανάπτυξη και παρέχει ασφάλεια παρόλο που αναπτύσσονται παράλληλα πολλές εφαρμογές, οι οποίες αλληλοεπιδρούν μεταξύ τους. Το Ethereum άνοιξε ένα νέο δρόμο στην οργάνωση των επιχειρήσεων και των κυβερνήσεων.

Το Hyperledger Fabric συνιστά θεμέλιο για την ανάπτυξη των περισσότερων blockchain εφαρμογών, διότι επιτρέπει στους προγραμματιστές να χρησιμοποιούν κομμάτια του Fabric χωρίς να δεσμεύονται σε όλη του τη λειτουργικότητα και επιπλέον μπορεί να δημιουργήσει έξυπνα συμβόλαια. Το Fabric είναι permissioned blockchain και δεν χρησιμοποιεί κρυπτονόμισμα. Αυτό σημαίνει, ότι όλοι οι συμμετέχοντες είναι γνωστοί μεταξύ τους σε αντίθεση με ένα τυπικό δημόσιο Blockchain, στο οποίο όλοι οι συμμετέχοντες είναι ανώνυμοι από προεπιλογή. Το Fabric λειτουργεί όπως τα περισσότερα Blockchain, δηλαδή καταγράφει τα ψηφιακά γεγονότα σε ένα βιβλίο. Τα γεγονότα είναι δομημένα ως συναλλαγές και μοιράζονται στους συμμετέχοντες. Όλες οι συναλλαγές είναι ασφαλείς και ιδιωτικές.

Το Hyperledger Project ξεκίνησε το 2015 από το Linux Foundation. Είναι ένα σύνολο από blockchain και εργαλεία (frameworks) πάνω σε αυτό, που έχουν ως στόχο να δημιουργήσουν σε επιχειρηματικό επίπεδο **μια δομή ανοιχτού κώδικα για κατανεμημένα καθολικά** (Distributed Ledger). Μέλη και υποστηρικτές σε αυτό το εγχείρημα είναι μεγάλες εταιρείες του κλάδου όπως η IBM, η Intel, η Cisco και η SAP. Επιτρέπει την δημιουργία ξεχωριστών επιπέδων ασφαλείας και αδειοδοτεί μόνο πιστοποιημένους χρήστες. Λόγω της κρυπτογράφησης των συναλλαγών είναι ιδανικό για επιχειρηματικά περιβάλλοντα μιας και πετυχαίνει την εμπιστευτικότητα των συναλλαγών και την

επιλεκτική πρόσβαση μεταξύ των συμμετεχόντων. Το Hyperledger Fabric βασίζεται στον αλγόριθμο συναίνεσης BTF (Byzantine Fault Tolerant)[16]σε αντίθεση με το PoW[17] του Bitcoin. Η υπηρεσία εντολών (orderer) του Hyperledger πρέπει να ελέγχεται από κοινού, από τα μέλη του δικτύου, χρησιμοποιώντας έναν αλγόριθμο BFT που αντιστέκεται σε κακόβουλες δραστηριότητες.

Στον πίνακα που ακολουθεί συγκρίνονται τα βασικά χαρακτηριστικά από τρία μεγάλα blockchains, το Bitcoin, το Ethereum και το Hyperledger Fabric.

Πίνακας 3: Σύγκριση χαρακτηριστικών Bitcoin, Ethereum και Hyperledger (Friebe, 2017) [43]

Χαρακτηριστικά	Bitcoin	Ethereum	Hyperledger Fabric
Πρόσβαση	Permissionless	Permissionless	Permissioned
Ιδιωτικότητα δεδομένων	Δημόσια	Δημόσια ή Ιδιωτικά	Ιδιωτικά
Συναίνεση	Proof-of-Work	Proof-of-Work	PBFT
Επεκτασιμότητα	Υψηλή κόμβου Χαμηλή απόδοσης	Υψηλή κόμβου Χαμηλή απόδοσης	Χαμηλή κόμβου Υψηλή απόδοσης
Κεντρικός έλεγχος	Χαμηλός, αποκεντρωμένες αποφάσεις που λαμβάνονται από την κοινότητα/miners	Μέτριος, κύρια ομάδαανάπτυξης αλλά και EIP διαδικασία	Χαμηλός, ανοιχτής διακυβέρνησης μοντέλο βασισμένο στο μοντέλο Linux
Ανωνυμία	Ψευδοανωνυμία, χωρίς κρυπτογράφηση	Ψευδοανωνυμία, χωρίς κρυπτογράφηση	Όχι, με κρυπτογράφηση
Νόμισμα	Ναι, το bitcoin	Ναι, το ether	Όχι
Κόστος συναλλαγής	Ναι	Ναι	Όχι
Ψευδογλώσσα	Περιορισμένη δυνατότητα, stack-based	Υψηλή δυνατότητα, turing-complete, υψηλού επιπέδου	Υψηλή δυνατότητα, turing-complete, υψηλού επιπέδου

[16] Γνωστό ως consensus. Θέλουμε τα μέρη να συμφωνήσουν σε ένα σύνολο δεδομένων ακόμη και υπό την παρουσία κακόβουλων αντιπάλων. Προστίθεται νέο μπλοκ εάν περισσότερα από τα 2/3 όλων των ομότιμων επαληθεύσεων υποβάλουν την ίδια απάντηση.

17 Οι εξορύκτες -miners πρέπει να λύσουν ένα υπολογιστικό δύσκολο πρόβλημα για να εξασφαλίσουν την εγκυρότητα των νέων συναλλαγών

7.3 Διάγραμμα ροής περί υιοθέτησης της τεχνολογίας blockchain

Για να υιοθετηθεί μια τεχνολογία blockchain από μια επιχείρηση ή έναν οργανισμό, θα πρέπει να αποδεικνύεται ότι αποτελεί την ιδανικότερη λύση, διότι υπερτερεί με πλεονεκτήματα, τα οποία δεν παρουσιάζουν αντίστοιχα άλλες διαθέσιμες τεχνολογικές λύσεις. Αποτελεί κοινή διαπίστωση ότι η τεχνολογία αυτή **αποτελεί την βέλτιστη λύση όταν αναζητούμε ένα προγραμματιστικό περιβάλλον, το οποίο θα πληροί τις κάτωθι προϋποθέσεις**: **[51]**

I. Υπάρχει ανάγκη για μια κοινή βάση δεδομένων.

II. Τα μέρη που συμμετέχουν στο σύστημα έχουν αντικρουόμενα κίνητρα ή δεν υφίσταται επαρκής εμπιστοσύνη μεταξύ τους.

III. Υπάρχουν ενιαίοι κανόνες που διέπουν τους συμμετέχοντες στο σύστημα.

IV. Δεν υπάρχει ανάγκη για συχνές τροποποιήσεις και αλλαγές στα δεδομένα.

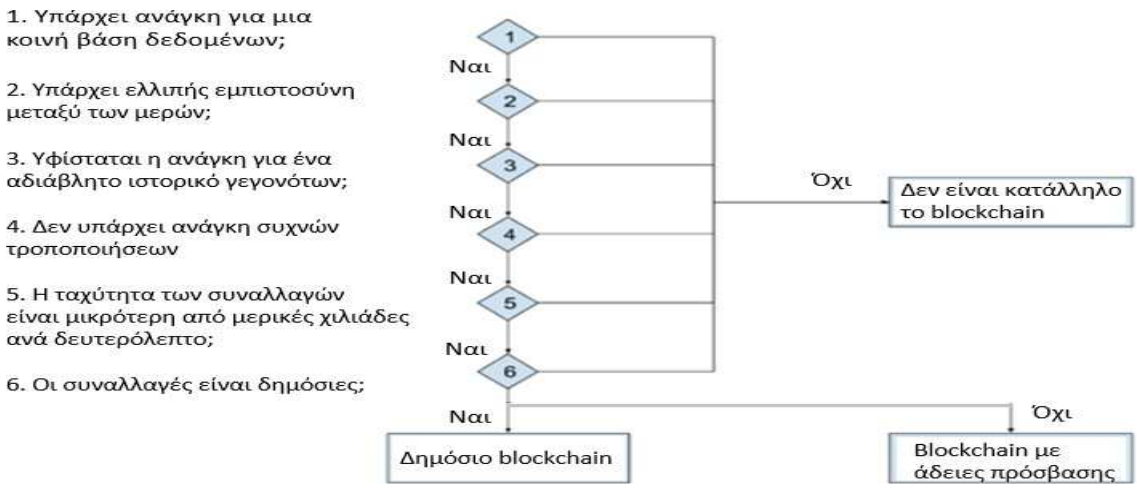
V. Υφίσταται ανάγκη για ένα ακέραιο και αδιάβλητο ιστορικό γεγονότων.

VI. Η ταχύτητα των συναλλαγών δεν υπερβαίνει τις μερικές χιλιάδες ανά λεπτό.

Κι εδώ, το μέγεθος της επιχείρησης διαδραματίζει σημαντικό ρόλο. Αν πρόκειται **για έναν μόνο οργανισμό ή για μια μικρή ομάδα οργανισμών** μεταξύ των οποίων επικρατούν **σχέσεις εμπιστοσύνης και κοινοί κανόνες**, είναι πιθανό η λύση **μιας σχεσιακής βάσης δεδομένων** να αποτελεί καταλληλότερη επιλογή. Εάν επίσης υφίσταται ανάγκη συχνής τροποποίησης ή και διαγραφής των δεδομένων, η επιλογή για την ανάπτυξη μιας εφαρμογής μέσω της τεχνολογίας blockchain, δεν αποτελεί την ιδανικότερη επιλογή. Ο όγκος των αναμενόμενων συναλλαγών είναι ένας ακόμη παράγοντας που θα πρέπει να συνεκτιμηθεί.

Στα πλαίσια **της ερευνητικής διαδικασίας περί της καταλληλότητας ή μη για την υιοθέτηση μιας εφαρμογής που στηρίζεται στην τεχνολογία blockchain**, είναι συνετό να σχεδιαστεί ένα διάγραμμα ροής με κρίσιμα ερωτήματα, τα οποία σταδιακά μας οδηγούν στην απάντηση.

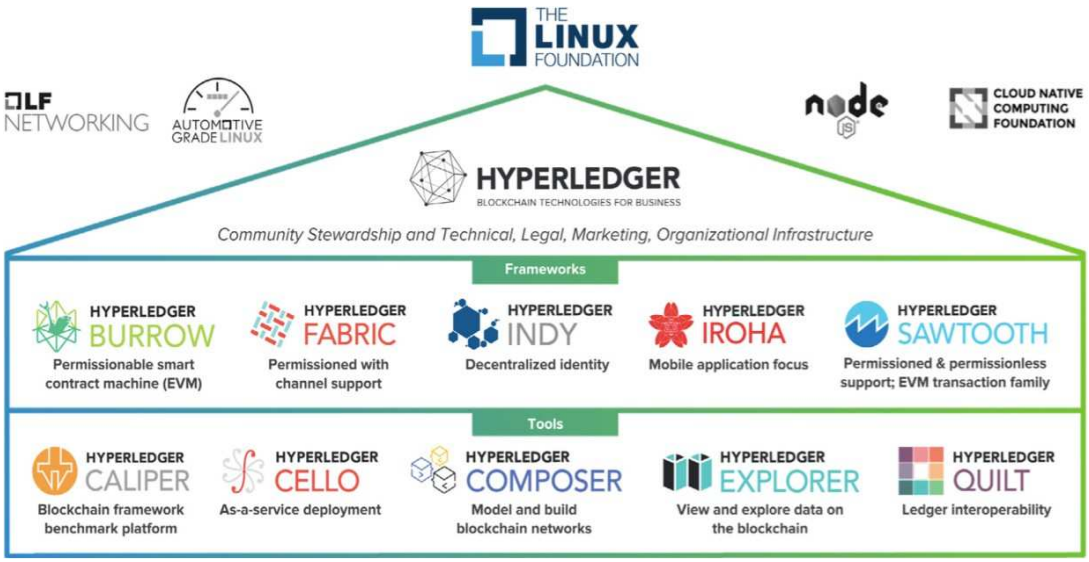
Σχήμα 1 : Διάγραμμα ροής για την υιοθέτηση ή μη της τεχνολογίας blockchain



7.4 Η δομή του Hyperledger

Με το Hyperledger δημιουργήθηκε μια νέα γενιά εφαρμογών όπου η εμπιστοσύνη, η λογοδοσία και η διαφάνεια αποτελεί τον πυρήνα ύπαρξής τους, ενώ παράλληλα ενισχύθηκε η ροή των επιχειρηματικών διαδικασιών και επαναπροσδιορίσθηκε το ζήτημα των νομικών περιορισμών**. [52]**

Το Hyperledger προσφέρει πρότυπα, κατευθυντήριες γραμμές και εργαλεία, για την κατασκευή μπλοκ ανοιχτού κώδικα και σχετικών εφαρμογών για χρήση σε διάφορες βιομηχανίες. Χρησιμοποιώντας τα διαθέσιμα εργαλεία, μια επιχείρηση δύναται να βελτιώσει σημαντικά την απόδοση των λειτουργιών της και την αποτελεσματικότητα των επιχειρηματικών διαδικασιών της. Όλα τα έργα του Hyperledger ακολουθούν τη μεθοδολογία σχεδιασμού, η οποία υποστηρίζει **μια αρθρωτή και επεκτάσιμη προσέγγιση**, με πολλά χαρακτηριστικά ασφαλείας. Τα έργα δεν διαθέτουν συγκεκριμένο διακριτικό ή κρυπτογράφηση, παρόλο που ο χρήστης μπορεί να δημιουργήσει ένα αν το χρειάζεται.
Για να καλυφθεί το σύνολο των αναγκών των συμμετεχόντων στο Hyperledger, έχουν αναπτυχθεί **διαφορετικά framework[18] και εργαλεία που βασίζονται σε αυτό**. Η επιλογή του κατάλληλου framework θα πρέπει να γίνει ανάλογα με τις απαιτήσεις της κάθε εφαρμογής ως προς την προσβασιμότητα και τα δικαιώματα, τη χρήση της εφαρμογής από κινητές συσκευές, καθώς και τη δια λειτουργικότητα με άλλες εφαρμογές.
Το οικοσύστημα του Hyperledger φαίνεται στην παρακάτω εικόνα του Linux Foundation.



Εικόνα 40: Το οικοσύστημα του Hyperledger project [hyperledger.org]

[18] Πλαίσιο εργασίας, συλλογή έτοιμου επαναχρησιμοποιήσιμου κώδικα, που ενδεχομένως συνοδεύεται με βοηθητικά προγράμματα, παρέχοντας στον προγραμματιστή ένα συγκεκριμένο, τυποποιημένο, δοκιμασμένο τρόπο χρήσης του στην υλοποίηση μιας εφαρμογής.
Πηγή : https://el.wiktionary.org/wiki/framework

7.5 Επιχειρησιακή Ανάλυση

- **Ανάλυση SWOT για πλατφόρμα HYPERLEDGER**

Πέρα από τα πλεονεκτήματα και τις ευκαιρίες που εντοπίζουμε για τη συγκεκριμένη πλατφόρμα, πάντοτε εμφιλοχωρούν και κάποια μειονεκτήματα ή απειλές.

✓ Πλεονεκτήματα

- **Ενισχυμένη ασφάλεια και αμεταβλητότητα**

  Οι πιθανότητες για απάτη ελαχιστοποιούνται καθώς η αποθήκευση των πληροφοριών σε ένα δίκτυο πολλών κόμβων (υπολογιστών), ευνοεί την ασφάλεια, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

- **Μικρότερη πιθανότητα αποτυχίας του συστήματος**

  Ένας τουλάχιστον πλήρης κόμβος σε λειτουργία δύναται να «διασώσει» το σύστημα, όταν ένας από τους επιμέρους κόμβους αδρανήσει. Αυτό οφείλεται στην αποκεντρωμένη αρχιτεκτονική δομή του, βάσει της οποίας, το σύστημα αναπτύσσεται σε πολλά διασπορπισμένα στοιχεία. Δεν υπάρχει μια κεντρική δομή. Το στοιχείο αυτό του προσδίδει αυθεντικότητα.

- **Διαλειτουργικότητα**

  Μπορεί να αποτελέσει σημείο σύγκλισης για ετερογενείς πληροφορίες με άλλα τεχνολογικά συστήματα και εφαρμογές λογισμικού χωρίς φραγμούς ή περιορισμούς, ανταλλάσσοντας δεδομένα σύμφωνα με τις εκάστοτε ανάγκες ενός οργανισμού. Σε ένα αμιγώς διαλειτουργικό δίκτυο, τα δεδομένα που συλλέγονται θα μπορούσαν να ενσωματωθούν με ασφάλεια σε έναν μοναδικό ηλεκτρονικό φάκελο, ο οποίος ενδεχομένως να χρησιμοποιηθεί και μελλοντικά, καταπολεμώντας έτσι την μάστιγα της γραφειοκρατίας.

- **Αυξημένη διαφάνεια**

  Το κατανεμημένο βιβλιάριο συναλλαγών, όπου όλοι οι συμμετέχοντες στο δίκτυο μοιράζονται τις ίδιες πληροφορίες, ενημερώνεται μόνο συλλογικά με ακρίβεια και διαφάνεια, ενώ επίσης όλα τα στοιχεία είναι διαθέσιμα σε όλους τους συμμετέχοντες, που έχουν δυνατότητα πρόσβασης. Ειδικότερα, στον δημόσιο τομέα είναι πολύ σημαντικό να διασφαλιστούν οι διαφανείς διαδικασίες

- **Αυξημένη αποτελεσματικότητα**

  Καθώς η αποθήκευση των αρχείων πραγματοποιείται σε ένα ενιαίο βιβλιάριο συναλλαγών, κοινό σε όλους τους συμμετέχοντες, υφίσταται καλύτερη οργάνωση και καλλιεργείται ευκολότερα εμπιστοσύνη, χωρίς να χρειάζονται πολλοί ενδιάμεσοι για την ολοκλήρωση μιας συναλλαγής.

- **Ευελιξία - Ταχύτητα**

  Τα δεδομένα συλλέγονται, επικυρώνονται και διανέμονται σε όλα τα εμπλεκόμενα μέρη, ενώ ο εκάστοτε φορέας μπορεί να έχει εύκολη και γρήγορη πρόσβαση μέσω του Blockchain.

✓ Ευκαιρίες

- **Παρέχει μια πλατφόρμα για Μεγάλα Δεδομένα και την αναλυτική έρευνα**

  Προσφέρονται νέες δυνατότητες για αναλυτική έρευνα, διότι τα Μεγάλα δεδομένα είναι ομαδοποιημένα και ανωνυμοποιημένα, αλλά ταυτοχρόνως και διαθέσιμα σε όποιον τα ζητήσει για τέτοιο σκοπό. **Τα έξυπνα συμβόλαια μπορούν να οδηγήσουν στη δημιουργία νέων επιχειρηματικών μοντέλων**, Η διασφάλιση της εμπιστοσύνης έγκειται στις συμβατικές προϋποθέσεις και τους όρους ενός έξυπνου συμβολαίου, που αποτυπώνονται με τη μορφή κώδικα. Με το που ικανοποιείται μια από τις διατυπωμένες σε αυτό συνθήκη, τότε αυτό υλοποιείται αυτομάτως, χωρίς καμία άλλη τρίτη παρέμβαση.

✓ Αδυναμίες

- **Ελλιπή συμμόρφωση με τον ΓΚΠΔ**

  Σε αντίθεση με τα δεδομένα της συναλλαγής, τα ίδια τα αρχεία πρέπει τελικά να αποθηκεύονται τις περισσότερες φορές σε εξωτερικές βάσεις δεδομένων. Αυτό συμβαίνει στα πλαίσια της συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ, ο οποίος ορίζει ότι οι υπεύθυνοι επεξεργασίας πρέπει να επιτρέπουν τη διαγραφή των προσωπικών δεδομένων, εφόσον τους ζητηθεί.

- **Ελλιπής προστασία χρηστών**

  Δεν υφίσταται συγκεκριμένη διαδικασία για να μπορέσει ο χρήστης της υπηρεσίας να αμφισβητήσει μια συναλλαγή.

- **Ηθικό Πλαίσιο, Αδυναμία Διαγραφής και Ανθρώπινο Λάθος**

  Η απουσία ενός νομοθετικού και ηθικού πλαισίου γύρω από την αποθήκευση δεδομένων σε Blockchain, εκθέτουν σε κίνδυνο την ιδιωτική ζωή των χρηστών. Σε μια παραδοσιακή βάση δεδομένων, ένας χρήστης μπορεί να δημιουργήσει, να αναγνώσει, να ενημερώσει και να διαγράψει δεδομένα. Ο σχεδιασμός ενός Blockchain επιτρέπει μόνο την ανάκτηση και την πρόσθεση – εγγραφή δεδομένων στο δίκτυο.

- **Πολυπλοκότητα και Περιορισμοί Αποθήκευσης**

  Στον κάθε προσαρτημένο και αμετάβλητο κόμβο του δικτύου, αποθηκεύονται απεριόριστα δεδομένα. Η αδυναμία διαγραφής ή τροποποίησης στοιχείων και δεδομένων εντός του δικτύου, δημιουργεί όλο και περισσότερο την ανάγκη για επιπλέον αποθηκευτικό χώρο.

- **Εξοικείωση με την τεχνολογία - Εκπαίδευση προσωπικού**

  Ένα χρονικό διάστημα εξοικείωσης του προσωπικού με τη συγκεκριμένη τεχνολογία είναι επιβεβλημένο, ώστε να αυτό να εκπαιδευτεί κατάλληλα, προκειμένου να κάνει χρήση μιας νέας πρωτοπόρας πλατφόρμας. Σε μια κοινωνία που δεν είναι εξοικειωμένη σε ικανοποιητικό βαθμό με τις νέες τεχνολογίες, οι τεχνολογίες blockchain φαντάζουν δυσπρόσιτες, πόσο μάλλον όταν κάποιος δεν κατανοεί την αξία που αυτές μπορούν να προσδώσουν.

✓ Απειλές

- **Δυσκολία επεκτασιμότητας**

  Όσο εξελίσσονται οι συναλλαγές προκειμένου να δημιουργηθεί ένας πλήρες κόμβος, προστίθενται ένα ακόμα μπλοκ στην αλυσίδα το οποίο περιέχει δεδομένα, τα οποία μεταφέρονται σε όλο το ιστορικό των προηγούμενων συναλλαγών. Η ενέργεια αυτή λειτουργεί επιβαρυντικά στην πρόοδο των διαδικασιών του συστήματος, αφού απαιτείται επαλήθευση από τους χρήστες πριν από την επικύρωση και προσάρτησή τους.

- **Κβαντικοί υπολογιστές**

  Αν υλοποιηθούν στο μέλλον οι κβαντικοί υπολογιστές, θα αποκτήσουν τέτοια ισχύ, ώστε να είναι σε θέση να αποκρυπτογραφήσουν τα δεδομένα που βρίσκονται αποθηκευμένα. Γενικότερα, η τεχνολογία Blockchain μπορεί να οδηγήσει σε ένα ανταγωνιστικό μέλλον στον δημόσιο τομέα, όχι μόνο λόγω της εξοικονόμησης κόστους, αλλά και εξαιτίας της διαφάνειας των συναλλαγών καθώς και της αυτοματοποίησης του συνόλου των διαδικασιών σε όλα τα στάδια, όπου μειώνεται σημαντικά ο χρόνος υλοποίησης και πλέον ο παραδοσιακός τρόπος διεκπεραίωσης των εργασιών, μετατρέπεται σε μια παρελθοντική λύση.

7.6 Κρίσιμοι παράγοντες υπεροχής του Hyperledger Fabric

Αντιδιαμετρικά από το bitcoin και το ethereum, βάσει των σχεδιαστικών επιλογών ιδιωτικότητας, βρίσκονται τα private permissioned blockchains, αντιπροσωπευτικό των οποίων είναι το Hyperledger Fabric, ή απλώς Fabric. **Οι κρίσιμοι παράγοντες υπεροχής του Hyperledger Fabric, οι οποίοι συμβάλλουν ώστε να θεωρηθεί ως η καταλληλότερη πλατφόρμα blockchain για τα προτεινόμενα σενάρια χρήσης της παρούσας εργασίας, προσδιορίζονται στα εξής σημεία:**

- ✓ **Αποτελεί μια ευέλικτη εργαλειοθήκη**

  Η **μοντέρνα, αρθρωτή και επεκτάσιμη αρχιτεκτονική** του, επιτρέπει την προσαρμογή σε ένα πλήθος εφαρμογών διαφόρων κλάδων από τραπεζικές υπηρεσίες και υγειονομική περίθαλψη έως αλυσίδες εφοδιασμού. Θα μπορούσαμε λοιπόν να το **προσομοιάσουμε** με μια ευέλικτη εργαλειοθήκη.

- ✓ **Διαφύλαξη του απορρήτου των συναλλαγών**

  Η διαφύλαξη του απορρήτου θεωρείται βέβαιη, λόγω του εγκεκριμένου τρόπου λειτουργίας του και τον λεπτομερή έλεγχο πρόσβασης στα αρχεία του, αφού επρόκειτο καταρχήν για ένα αδειοδοτημένο δίκτυο, το οποίο περιορίζει την ορατότητα των δεδομένων που διακινούνται σε αυτό, αποκλειστικά και μόνο στους αδειοδοτημένους χρήστες του και αναλόγως των κατά περίπτωση εκχωρημένων δικαιωμάτων σε αυτούς.. **Οι συμμετέχοντες εφόσον επιλέγονται εκ των προτέρων, είναι ταυτοποιήσιμοι.** Συνεπώς, όσα από τα δεδομένα **είναι αποθηκευμένα στο καθολικό**, δεν είναι προσβάσιμα **σε όλους τους συμμετέχοντες**, με αποτέλεσμα **να τηρείται το απόρρητο στον υψηλότερο δυνατό βαθμό.** Η ιδιωτικότητα και η εμπιστευτικότητα των συναλλαγών που πραγματοποιούνται και των δεδομένων που διακινούνται, είναι διασφαλισμένη. Θα πρέπει επιπλέον να σημειωθεί ότι το Fabric δύναται να σχηματίζει πληθώρα δικτύων που αλληλοεπιδρούν μεταξύ τους, με την πρόσβαση των χρηστών τους να περιορίζεται σε όσους είναι μέλη.

- ✓ **Ταχύτερη απόδοση**

  Η συναίνεση μεταξύ κόμβων δεν προκύπτει κατόπιν εξόρυξης δεδομένων, όπως αντίστοιχα συμβαίνει σε άλλες παρόμοιες τεχνολογίες διανεμημένου καθολικού, με αποτέλεσμα να επιταχύνεται **η απόδοση της επεξεργασίας των συναλλαγών και να μην προκύπτουν ζητήματα κλιμάκωσής της, καθώς η επικύρωση επιτυγχάνεται ταχύτερα**. Μόνο τα μέρη που συμμετέχουν σε μια συναλλαγή πρέπει να καταλήξουν στη συναίνεση αυτή. Η ροή μηνυμάτων μεταξύ των καναλιών, σημαίνει ότι οι πελάτες-χρήστες βλέπουν μόνο τα μηνύματα και τις σχετικές συναλλαγές των καναλιών στα οποία συνδέονται και δεν γνωρίζουν άλλα κανάλια. Το μοντέλο execute-order-validate που υποστηρίζεται εδώ καθώς η πολιτική επικύρωσης, που ακολουθείται, καθορίζει ποιοι ή πόσοι χρήστες απαιτείται κάθε φορά να

εγγυηθούν την εκτέλεση ενός συμβολαίου, επιτυγχάνοντας παράλληλη εκτέλεση συναλλαγών και βελτιώνοντας θέματα απόδοσης και επεκτασιμότητας. Διαδικαστικά, προτείνεται από ένα χρήστη ένα συμβόλαιο προς εκτέλεση, αυτό επικυρώνεται βάσει της πολιτικής του δικτύου για την ορθότητά του και τοποθετείται σε σειρά αναμονής βάσει του πρωτοκόλλου συναίνεσης. Η συναλλαγή επικυρώνεται εφόσον κληθεί από μία εξωτερική εφαρμογή και γίνει αποδεκτή από τα συναλλασσόμενα μέρη. Με αυτόν τον τρόπο, η πρόσβαση σε συναλλαγές περιορίζεται σε εμπλεκόμενα μέρη μόνο, με συνέπεια η ***επικύρωση*** πρέπει **να επιτευχθεί μόνο σε επίπεδο συναλλαγής και όχι σε επίπεδο καθολικού**.

- ✓ **Ευέλικτη ροή συναλλαγών**

  Η ροή συναλλαγών στο Fabric ξεκινάει από **την πρόταση μιας συναλλαγής στο δίκτυο έως τη δέσμευσή της στο καθολικό**. Οι διάφοροι κόμβοι αναλαμβάνουν διαφορετικούς ρόλους και εργασίες στη διαδικασία επίτευξης της συναίνεσης. Συνέπεια των ανωτέρω είναι η υψηλή απόδοση των συναλλαγών του.

- ✓ **Αρχιτεκτονικός σχεδιασμός – Ενσωμάτωση στοιχείων**

  Το Fabric διαθέτει έξυπνα συμβόλαια με την έννοια του έξυπνου κώδικα συμβολαίου που μπορεί να γραφτεί σε Go ή Java. Ο όρος "chaincode" χρησιμοποιείται ως συνώνυμο της έξυπνης σύμβασης. Το σημαντικό στοιχείο εδώ είναι ότι λόγω της αρθρωτότητας του αρχιτεκτονικού του σχεδιασμού, μπορεί να προσφέρει και μια πιο εξωσυμβατική εμπειρία, ενσωματώνοντας στοιχεία από άλλες πλατφόρμες - πχ Corda., όπου εκεί οι έξυπνες συμβάσεις δεν αποτελούνται μόνο από κώδικα, αλλά επιπλέον επιτρέπουν τη μορφή απλού κειμένου, αναγνώσιμου από τους ανθρώπους, ώστε να διατυπώνονται όροι και κανόνες με τρόπο που μπορούν να εκφραστούν και να εφαρμοστούν στον κώδικα των έξυπνων συμβάσεων, δίνοντας στον κώδικα ένα είδος νομικής δεσμευτικότητας. Μια τέτοια κατασκευή ονομάζεται Ricardian Contract [19] και δύναται να σχεδιαστεί με τρόπο που να καλύπτει τις απαιτήσεις ακόμα και του πιο απαιτητικού - ελεγχόμενου περιβάλλοντος ενός συγκεκριμένου τομέα εφαρμογής.

- ✓ **Εγγενές νόμισμα**

  Το Fabric δεν διαθέτει ένα ενσωματωμένο κρυπτονόμισμα όπως το Ethereum, διότι ούτως ή άλλως δεν απαιτείται ενσωματωμένη κρυπτογράφηση, αφού η συναίνεση εδώ δεν επιτυγχάνεται μέσω της εξόρυξης. Ωστόσο, είναι δυνατό να αναπτυχθεί ένα εγγενές νόμισμα εντός της αλυσίδας.

- ✓ **Γνώση της ταυτότητας των συμμετεχόντων**

  Το Fabric, ως permissioned δίκτυο, επιβάλλει γνώση της ταυτότητας των συμμετεχόντων. Αν και η γνώση της ταυτότητας κάποιου δεν ταυτίζεται με την εμπιστοσύνη σε αυτόν, σε αντιστοιχία με τον πραγματικό κόσμο, **η υιοθέτηση ενός πλαισίου κανόνων και**

[19] Είναι μια μοναδική νομική συμφωνία ή έγγραφο που είναι αναγνώσιμο για προγράμματα υπολογιστών καθώς και για ανθρώπους ταυτόχρονα. Πηγή : https://101blockchains.com/ricardian-contracts/

πρωτοκόλλων επιβάλλουν την απαιτούμενη μερική εμπιστοσύνη που απαιτείται για τη λειτουργία του δικτύου με **παράκαμψη του έμπιστου τρίτου μέρους για κάθε συναλλαγή.** Συνοπτικά, τα θεμελιώδη χαρακτηριστικά που δίνουν στο Fabric το στοιχείο της υπεροχής είναι: α) ο ακριβής έλεγχος της συναίνεσης, β) η περιορισμένη πρόσβαση σε συναλλαγές που οδηγεί σε βελτιωμένη επεκτασιμότητα απόδοσης και γ) η προστασία της ιδιωτικότητας.

Είναι ένα λογισμικό ανοικτού κώδικα μέσω του οποίου μπορούν να δημιουργηθούν εφαρμογές έξυπνων συμβολαίων χωρίς να χρησιμοποιούνται δημόσια blockchain όπως τα blockchain του Bitcoin και του Ethereum. Η βασική ιδέα είναι ότι αντί κάθε επιμέρους βιομηχανία να δημιουργεί τη δική της λύση blockchain, να χρησιμοποιηθεί μια κοινά αποδεκτή πλατφόρμα αποτελούμενη από επιμέρους τμήματα τα οποία μπορούν να επιλεγούν και να συνδυαστούν έτσι ώστε να παρέχουν μεμονωμένες λύσεις.

Κεφάλαιο 8ο – Προτεινόμενο σενάριο εφαρμογής τεχνολογίας blockchain στον Δημόσιο τομέα

8.1 Η επιλογή του Hyperledger – Εισαγωγικές επισημάνσεις

Για την ανάπτυξη ενός προτεινόμενου σεναρίου σε υπηρεσίες του δημοσίου τομέα, επιλέξαμε το Hyperledger Fabric, για το οποίο ήδη υπάρχει ειδική μνεία περί της υπεροχής του, σε σύγκριση με άλλες γνωστές πλατφόρμες τεχνολογίας blockchain, σε προηγούμενο κεφάλαιο της παρούσας μελέτης. Στο παρόν κεφάλαιο θα παρουσιασθούν διεξοδικά **τα τεχνικά και λειτουργικά χαρακτηριστικά** αυτής της κατανεμημένης, ανοιχτού κώδικα, private πλατφόρμας, στοιχεία τα οποία την διαφοροποιούν αισθητά από άλλες blockchain λύσεις, καθώς είναι πρωτίστως σχεδιασμένη για επιχειρηματικό περιεχόμενο. Υπενθυμίζουμε ότι δημιουργήθηκε υπό την αιγίδα του Linux Foundation και έκτοτε εξελίσσεται δυναμικά. Σχηματικά απεικονίζεται ως ένας κόμβος, με διάφορα μεμονωμένα blockchain, ένα μοτίβο που οριοθετεί την φιλοσοφία σχεδίασής του. Η αξιοπιστία που το Hyperledger προσφέρει, εντός ενός πρωτοποριακού τεχνολογικού πλαισίου το οποίο βασίζεται σε μπλοκ, το κατατάσσει στην κορυφή των πιο εναλλακτικών εφαρμογών πληροφορικής.

Ο προορισμός της **ανάπτυξης ενός οικοσυστήματος Hyperledger** ήταν να συνεισφέρει στην συνεργασία μεταξύ διαφόρων επιχειρήσεων και οργανισμών χωρίς τη χρήση δημόσιων blockchain εφαρμογών. Σε ένα ιδιαίτερα ευέλικτο και μοντελοποιημένο σύστημα, το Hyperledger Fabric χρησιμοποιεί **λειτουργίες κλειδιά της blockchain τεχνολογίας** (συναίνεση και υπηρεσίες προσχώρησης), ώστε με τη μέθοδο plug and play, να ενσωματωθούν επαρκώς στην όποια μεμονωμένη λύση επιλεγεί από μια επιχείρηση ή έναν οργανισμό. Στα πλαίσια λοιπόν της **βελτίωσης των επιχειρηματικών διαδικασιών μιας υπηρεσίας δημόσιας ή ιδιωτικής**, το Hyperledger προσφέρει όλες εκείνες τις διαθέσιμες λύσεις για τη σημαντική βελτίωση της απόδοσής τους.

Αξίζει να επισημανθεί ότι δεν περιλαμβάνει κρυπτονομίσματα, χρησιμοποιεί όμως συμβατούς αλγορίθμους για να πετύχει τον ίδιο σκοπό. **Η συναίνεση (consensus) για την επαλήθευση των συναλλαγών του**, εξασφαλίζει τη διαφάνεια, την αμεταβλητότητα και την ευχερέστερη πρόσβαση στο ιστορικό τους. Για την **διαχείριση των χρηστών και των υπηρεσιών** μιας εφαρμογής της, χρησιμοποιείται το επονομαζόμενο **chaincode,** το οποίο επιτρέπει την αυτοματοποίηση της όλης διαδικασίας. Η υποστηρικτική αυτή δομή του, του επιτρέπει να αναπαριστά με μια αυθαίρετη τιμή οποιαδήποτε στοιχείο περιουσιακό ή μη.

Παρόλο που δεν διαθέτει κρυπτογράφηση, εντούτοις υπάρχει η δυνατότητα οι χρήστες του να δημιουργήσουν έναν κωδικό, αν το κρίνουν ως μια απαραίτητη προϋπόθεση. **Η διαχείριση της ταυτότητας του κάθε χρήστη**, η πιστοποίηση τους καθώς και τυχόν εξουσιοδοτήσεις ανάλογα τις ανάγκες, είναι μερικές από τις τακτικές που έχει καθιερώσει και χρησιμοποιεί, ανταποκρινόμενο

πλήρως στις νέες απαιτήσεις που τέθηκαν για το **επιχειρηματικό περιβάλλον** (ιδιωτικό δίκτυο, ταυτότητα χρηστών, ταχύτητα συναλλαγών, εμπιστευτικότητα), βασιζόμενο σε ένα αρχιτεκτονικό εύκολα παραμετροποιήσιμο μοντέλο σχεδιασμού με στοχευμένη δράση.

Το Fabric **ως permissioned blockchain**, προσεγγίζει τις έννοιες Ιδιωτικότητα και την Εμπιστευτικότητα από μια διαφορετική σκοπιά, καθώς του το επιτρέπει η αρχιτεκτονική του, αφού επιπροσθέτως στηρίζεται σε **κανάλια επικοινωνίας, τα οποία λειτουργούν ως δίαυλοι επικοινωνίας μεταξύ των χρηστών**, με δυνατότητα να ορισθούν **τα δεδομένα τους ως ιδιωτικά** και να επιτραπεί σε συγκεκριμένοι χρήστες να αποκτήσουν την ευχέρεια πρόσβασης σε αυτά. Οι **συμμετέχοντες δημιουργούν ένα υποδίκτυο** όπου το κάθε μέλος έχει πρόσβαση σε συγκεκριμένο σύνολο συναλλαγών, κάτι το οποίο είναι επιθυμητό στον Δημόσιο Τομέα. Μόνο όσοι συμμετέχοντες απαρτίζουν το συγκεκριμένο κανάλι **προσχωρούν στα smart contracts** που θα χρησιμοποιηθούν **καθώς και στα δεδομένα**, που θα γίνουν **αντικείμενο συναλλαγών στο υποδίκτυο**. Συνεπώς, αν και η σχεδιαστική του φιλοσοφία ακολουθεί μια **πλήρως επεκτάσιμη προσέγγιση, εντούτοις προσφέρει ασφάλεια.**

8.2 Το βασικό εννοιολογικό μοντέλο σχεδιασμού του Hyperledger – Θεωρητική προσέγγιση

Πριν από την ανάπτυξη της πρότασής μας για την ψηφιοποίηση σεναρίου διεξαγωγής μιας διαγωνιστικής διαδικασίας προμηθειών στον Δημόσιο τομέα μέσω μιας εφαρμογής Blockchain, όπως είναι το Hyperledger Fabric, θα πρέπει να συνοψίσουμε περιγραφικά το στοιχειώδες εννοιολογικό μοντέλο που το χαρακτηρίζει, βάσει του οποίου χαρτογραφούνται τόσο **οι οντότητες που θα συμμετέχουν σε αυτό** όσο και το **modus operandi [20]της όλης διαδικασίας**.

Τέσσερα είναι τα επιμέρους στοιχεία του.

1. οι **κόμβοι, δηλαδή** οι οντότητες που συμμετέχουν στην εφαρμογή. Οι κόμβοι μπορούν να εκπροσωπούν έναν Φορέα – Οργανισμό και τις υπομονάδες του.
2. **οι συναλλαγές** οι οποίες περιλαμβάνουν τις αλληλεπιδράσεις μεταξύ των διαφόρων φορέων που εμπλέκονται.
3. **τα δεδομένα** είναι εκείνα που παράγονται από τις συναλλαγές και τις σχετικές διαδρομές ελέγχου[21].
4. η **λογική,** που είναι η επιχειρησιακή λογική[22] που δεσμεύει τα παραπάνω τρία επίπεδα, καθορίζοντας τον **πηγαίο κώδικα** που στηρίζει το σύστημα.

[20] είναι λατινική φράση, σημαίνει *τρόπος του λειτουργείν* και συνοψίζει όλες τις εφαρμοσμένες αρχές, μεθόδους, πρακτικές λειτουργίας που ένα φυσικό ή νομικό πρόσωπο (π.χ. μια επιχείρηση) χρησιμοποιεί στον εργασιακό χώρο ή στην προσέγγιση της επαγγελματικής και κοινωνικής του ζωής, που το χαρακτηρίζουν.

[21] εκτέλεση εντολών του λειτουργικού συστήματος, λειτουργιών αρχικοποίησης, δρομολόγησης πακέτων και ελέγχου δικτυακής διασύνδεσης.

[22] Πως οι επιχειρησιακές διαδικασίες θα μετεξελιχθούν σε επιχειρησιακούς κανόνες μέσω της "ηλεκτρονικοποίησης" των διαδικασιών ενός οργανισμού

Λαμβάνοντας υπόψη τις **ιδιομορφίες που διέπουν τον Δημόσιο τομέα** και φέροντας αυτές σε αντιπαραβολή με **τις λειτουργικές απαιτήσεις που φέρει η εν λόγω εφαρμογή** η οποία βασίζεται στην τεχνολογία blockchain, στοιχεία τα οποία αναλύθηκαν διεξοδικά στα προηγούμενα κεφάλαια της εργασίας μας, καταλήξαμε στα εξής

- ✓ Η διαπίστευση και η δικαιοδοσία των χρηστών είναι εξασφαλισμένη
- ✓ Η επιχειρησιακή του λογική του είναι η ενδεδειγμένη
- ✓ Οι διαχειριστικές του λειτουργίες κρίνονται ικανοποιητικές, αφού τόσο το σύστημα καταγραφής των συναλλαγών όσο και το μοντέλο συναίνεσης που χρησιμοποιεί, είναι στοιχεία που το κάνουν να ξεχωρίζει για την επαλήθευση της ακεραιότητας των συναλλαγών εντός του δικτύου και την ταχύτητα εκτέλεσης των επιμέρους διεργασιών.
- ✓ Το περιβάλλον λειτουργίας του συγκεκριμένου λογισμικού, επιτρέπει στους εμπλεκόμενα μέρη – χρήστες του και στην επιχειρησιακή ομάδα έργου, να αλληλοεπιδρούν με τον βέλτιστο δυνατό τρόπο
- ✓ Το οριοθετημένο σχεδιαστικό αρχιτεκτονικό του πλαίσιο, μοντελοποιεί ιδανικά τις προδιαγραφές ενός σεναρίου, αφού ο τρόπος κλιμάκωσής του, εξασφαλίζει την μέγιστη δυνατή απόδοση και ασφάλεια

8.3 Τεκμηρίωση για την επιλογή ενός Permissioned - Consortium blockchain

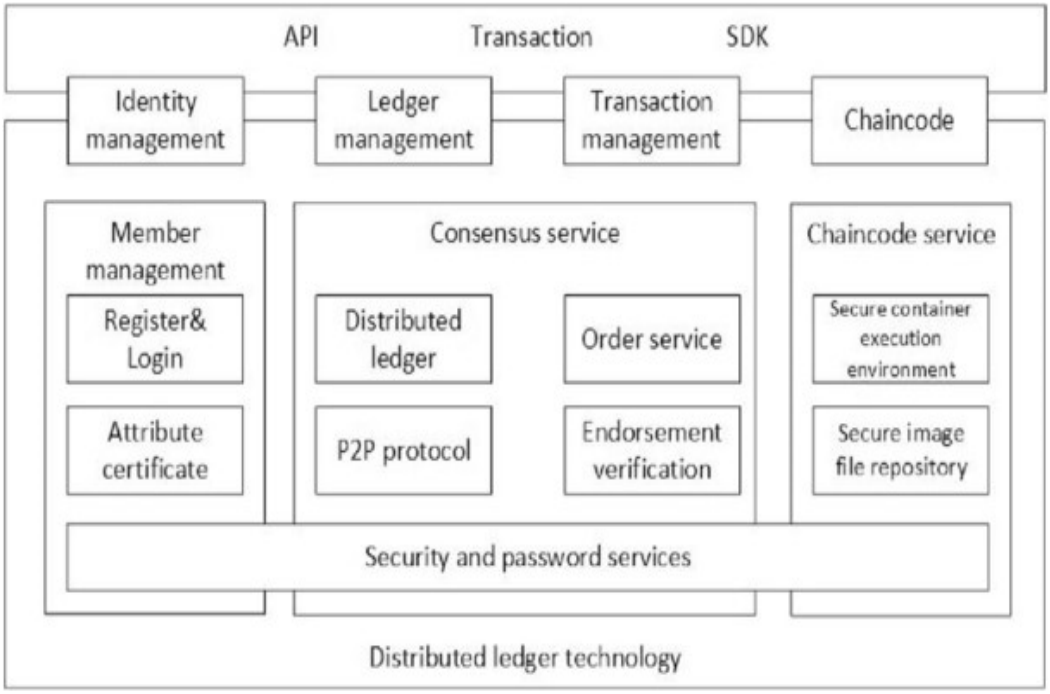
Στην περίπτωσή μας, επιλέχθηκε το εξουσιοδοτημένο Blockchain διότι παρόλο που διατηρεί και αυτό ένα κατανεμημένο καθολικό δεδομένων, οι συμμετέχοντες ελέγχονται από μια Κεντρική Αρχή, η οποία τους αναγνωρίζει και τους δίνει τα προβλεπόμενα δικαιώματα, βάσει του σκοπού που καλούνται να εξυπηρετήσουν. Επίσης, μπροστά στο δίλλημα να επιλέξουμε ένα public blockchain οπού διακυβεύεται η εμπιστοσύνη ή ένα private blockchain το οποίο παρουσιάζει μια εσωστρέφεια, καθώς προσδίδει εξ' ολοκλήρου εμπιστοσύνη σε μια και μοναδική οντότητα, θα προτιμήσουμε μία υβριδική μορφή, ένα consortium blockchain το οποίο φέρει κυρίως διαχειριστικές διαφορές, ως προς την υλοποίησή του και όχι τεχνικές. **Περισσότεροι λοιπόν από ένας οργανισμοί – επιχειρησιακές μονάδες (Περιφέρεια Ηπείρου – Περιφερειακές Ενότητές της) δύναται να επικοινωνούν μεταξύ τους και να συναλλάσσονται**. Άλλωστε, χαρακτηριστικό του γνώρισμα είναι η συνεκτικότητα που δημιουργείται ανάμεσά τους, αφού όλη αυτή η διαδικασία **διεξάγεται εντός καναλιών, τα οποία διαθέτουν αντίστοιχα peers στο δίκτυο.**

Φέροντας δομή **μερικώς ιδιωτική και αποκεντρωμένη**, απαρτίζεται από **έναν μικρό αριθμό προκαθορισμένων κόμβων** οι οποίες εφαρμόζουν τον επιλεγόμενο **μηχανισμό συναίνεσης** (μηχανισμών αντοχής σε σφάλματα βυζαντινού τύπου (BFT) όπως ο PBFT) και **πρόσβασης στις συναλλαγές.** Η 'ηγεσία' ασκείται από **ομάδα κόμβων** και όχι από έναν κεντρικό. Η δε ανάγνωση συγκεκριμένων δεδομένων δύναται να είναι ελεύθερη (public) ή με περιορισμένη λειτουργία ανάγνωσης. Διαφαίνεται να είναι ένα οργανωτικό σχήμα το οποίο εξυπηρετεί πλήρως τις ανάγκες **συνεργαζόμενων ο**ργανισμών - επιχειρήσεων.

8.4 Ποια δομικά στοιχεία του αρχιτεκτονικού σχεδιασμού του Hyperledger μας εξυπηρετούν

Παρακάτω απαριθμούνται τα βασικά δομικά στοιχεία που εξυπηρετούν το προτεινόμενο σενάριο που θα αναπτύξουμε.

1. **Επίπεδο συναίνεσης** - φροντίζει για τη δημιουργία μιας συμφωνίας μετά από την ταξινόμηση και την επιβεβαίωση της ορθότητας του συνόλου των συναλλαγών που συνιστούν ένα μπλοκ.
2. **Smart Contract Layer** – είναι υπεύθυνο για την επεξεργασία αιτημάτων συναλλαγών και την έγκριση μόνο έγκυρων συναλλαγών
3. **Επίπεδο επικοινωνίας** - φροντίζει peer-to-peer μεταφορές μηνυμάτων.
4. **Υπηρεσία Διαχείρισης Ταυτότητας** – διαθέτει την απαραίτητη λειτουργία για τη διατήρηση και επικύρωση των ταυτοτήτων των χρηστών και των συστημάτων και για την εδραίωση της εμπιστοσύνης στο blockchain
5. **API ή διεπαφή προγραμματισμού εφαρμογών**, η οποία επιτρέπει σε εξωτερικές εφαρμογές και πελάτες να διασυνδέονται με το blockchain.



Εικόνα 41: Η αρθρωτή αρχιτεκτονική του Hyperledger Fabric

8.5 Πως λειτουργούν τα Smart Contracts στο Hyperledger Fabric – Η αρχιτεκτονική του κύκλου ζωής των συναλλαγών

Το σύνολο των συναλλαγών της καταγράφεται σε ένα κατανεμημένο ledger (δίκτυο κόμβου χρηστών), το οποίο αποτελεί το κέντρο του δικτύου της. Ένα δίκτυο βασισμένο στην αρχιτεκτονική του Hyperledger Fabric, που αποτελείται από κόμβους, χρησιμοποιεί τα έξυπνα συμβόλαια για την συμμετοχή τους στο κατανεμημένο κατάστιχο. **Τα smart contracts στο Fabric ονομάζονται chaincode**. Η ικανότητα τους να παράγουν παράλληλες διεργασίες εντός του δικτύου, αποδεικνύεται ιδιαίτερα επωφελής.

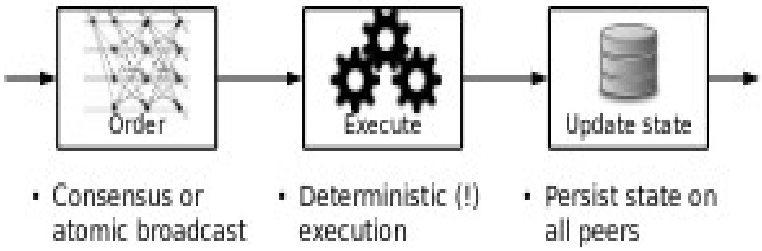
Στο σημείο αυτό αξίζει να επαναλάβουμε τον τρόπο λειτουργίας του **πρωτοκόλλου συναίνεσης** που χρησιμοποιεί. Διότι είναι κάτι το οποίο προσδίδει προστιθέμενη αξία στο Hyperledger Fabric, καθώς εφαρμόζεται **το τρίπτυχο execute – order – validate** (υποβολή – διάταξη – επικύρωση), και όχι η order – execute [23], χρησιμοποιώντας μάλιστα γλώσσα προγραμματισμού γενικού σκοπού (java, Go, Node.js), εξαλείφοντας κατ' αυτόν τον τρόπο μη ντετερμινιστικά στοιχεία [24], για την ανάπτυξη του chaincode. **Η ροή μιας συναλλαγής διαχωρίζεται σε 3 επιμέρους διακριτά στάδια.** Πιο συγκεκριμένα :

- **Execute**: Είναι το στάδιο αυτό κατά το οποίο υποβάλλεται μία συναλλαγή και ελέγχεται ως προς την ορθότητα της.
- **Order**: Η κάθε συναλλαγή καταλαμβάνει μια συγκεκριμένη θέση (διάταξη) στο δίκτυο. Τον ρόλο αυτό αναλαμβάνει το **Ordering Service** του συστήματος. Οι συναλλαγές που υποβάλλονται (execute), **πρώτα ταξινομούνται δηλαδή και στη συνέχεια κατανέμονται σε block**. Αυτή η διαδικασία δύναται να διενεργηθεί παράλληλα για πολλές συναλλαγές και από διαφορετικούς χρήστες, εφόσον το ordering service φέρει αποκεντρωμένο σχεδιασμό. Συνεπώς, οι κόμβοι του ordering service συντονίζονται μαζικά και δημιουργούν μια διατεταγμένη λίστα, μια αλληλουχία συναλλαγών προκειμένου να τις οργανώσουν σε block. **Τα block αυτά αποθηκεύονται στο ledger του orderer και στη κατανέμονται στους peers που ανήκουν στο συγκεκριμένο κανάλι επικοινωνίας.**

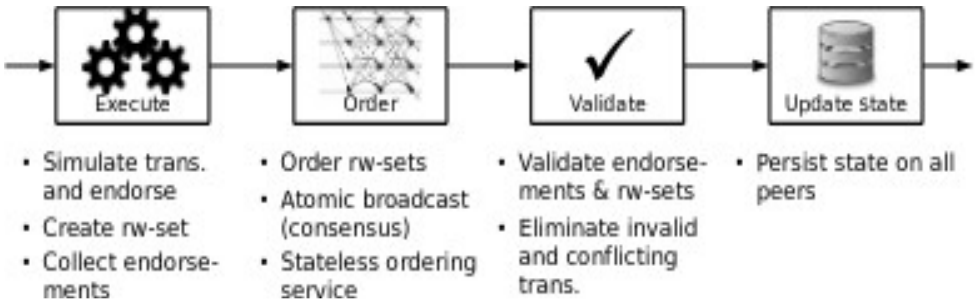
[23] (επαλήθευση – μετάδοση στους χρήστες, οι οποίοι κατόπιν εκτελούν τις συναλλαγές σειριακά, χρησιμοποιώντας γλώσσες ειδικού σκοπού – που δημιουργούν προβλήματα απόδοσης και κλιμάκωσης του συστήματος). Στις περισσότερες υλοποιήσεις Blockchain το πρωτόκολλο συμφωνίας πρώτα ορίζει μία σειρά μεταξύ των συναλλαγών (order) και στην συνέχεια τις στέλνει σε όλους τους κόμβους, οι οποίοι τις εκτελούν με την σειρά (execute). Το μοντέλο order-execute απαιτεί σειριακή εκτέλεση των συναλλαγών σε όλους τους κόμβους, πράγμα που επηρεάζει αρνητικά την απόδοση του συστήματος.

[24] Στη θεωρία υπολογισμού, το μη ντετερμινιστικό πεπερασμένο αυτόματο (αγγλικά: nondeterministic finite-state automaton (NFA)) είναι ένα πεπερασμένο αυτόματο που από μία κατάσταση, διαβάζοντας ένα σύμβολο εισόδου, μπορεί να μεταβεί σε μία ή και παραπάνω καταστάσεις, σε αντίθεση με το ντετερμινιστικό πεπερασμένο αυτόματο (DFA) που μπορεί να μεταβεί σε μία μόνο κατάσταση. Πηγη : https://el.wikipedia.org/

- **Validate:** Στο στάδιο αυτό επαληθεύονται οι συναλλαγές με βάση κάποια συγκεκριμένη πολιτική που καθορίζεται, πριν από την υποβολή των συναλλαγών στο blockchain. **Για την κάθε εφαρμογή έχει εκ των προτέρων ορισθεί πόσοι κόμβοι ή ποιοι από αυτούς πρέπει να εγγυηθούν για την ορθή λειτουργία του chaincode.** Συνεπώς, κάθε συναλλαγή χρειάζεται να εκτελεστεί από ένα υποσύνολο των κόμβων. Το καινοτόμο είναι ότι στο Hyperledger Fabric οι συναλλαγές έχουν ήδη υποβληθεί πριν καθοριστεί η τελική τους χρονική σειρά.



Εικόνα 42: Η αρχιτεκτονική order-execute



Εικόνα 43: Η αρχιτεκτονική execute-order-validate

8.6 Η διαδικασία σύναψης σύμβασης προμηθειών Δημοσίου και η πολυπλοκότητά της

Ξεκινώντας από **το κρίσιμο στοιχείο** το οποίο θα προσδιορίσει εάν αναφερόμαστε σε μια δημόσια σύμβαση ή όχι, θα θέλαμε να επισημάνουμε ότι αυτό το στοιχείο δεν είναι το οργανικό, δηλαδή αν πρόκειται για ΝΠΔΔ ή ΝΠΙΔ, **αλλά λειτουργικό**. Άπαξ και ο Φορέας ελέγχεται σε επίπεδο **χρηματοδότησης ή διοίκησης από το δημόσιο και διαχειρίζεται δημόσιο χρήμα**, καταλήγουμε στο συμπέρασμα ότι πρόκειται για μια δημόσια σύμβαση, ως αυτή ερμηνεύεται σχηματικά από το ενωσιακό δίκαιο.

Ένας Κρατικός Φορέας – οι Κυβερνητικές Αναθέτουσες Αρχές, πριν από τη διενέργειας μιας διαγωνιστικής διαδικασίας, στα πλαίσια της σύναψης σύμβασης προμηθειών, παροχής υπηρεσιών ή έργων, οφείλουν να **προγραμματίζουν, να διαχειρίζονται, να εκτελούν και να υλοποιούν** το εν λόγω εγχείρημα, τηρώντας τα κάτωθι:

1. Κατάρτιση της προϋπολογισθείσας δαπάνης και τήρηση του χρονοδιαγράμματος υλοποίησης της, με ταυτόχρονη πρόβλεψη των μελλοντικών αναγκών του Φορέα.
2. Προσεγμένη και ορθή σύνταξη και των διακηρύξεων, των όρων της καθώς και του συνόλου των εγγράφων ενός διαγωνισμού ανάλογα με τη διαδικασία ανάθεσης (ανοικτή, κλειστή, συνοπτική) και το αντικείμενο της σύμβασης (έργο, προμήθεια, υπηρεσία). Το κανονιστικό κείμενο – Διακήρυξη ενεργεί αμφιμερώς – Οι όροι δεσμεύουν συμμετέχοντες και Αναθέτουσα Αρχή και αποτελεί το θεμέλιο του διαγωνισμού αφού βάσει αυτής καθορίζονται : Οι όροι διεξαγωγής, οι προϋποθέσεις συμμετοχής των διαγωνιζομένων, το αντικείμενο της προμήθειας, οι Τεχνικές προδιαγραφές και ο τρόπος αξιολόγηση των προσφορών.
3. Τήρηση της δομής και του περιεχομένου των εγγράφων ενός διαγωνισμού βάσει της ισχύουσας νομοθεσίας. (Αποτελεί ευτύχημα το γεγονός ότι οι σχετικές διατάξεις του νόμου ν.4412/20216, αποτελούν πλέον ένα **ενιαίο νομοθετικό πλαίσιο** για το σύνολο των υπηρεσιών του Δημοσίου, το οποίο συμμορφώνεται με τους Ευρωπαϊκούς Κανονισμούς στα πλαίσια της εφαρμογής δίκαιου ανταγωνισμού και διαφάνειας μεταξύ των συμμετεχόντων στη διαδικασία).
4. Χρήση πρότυπων εγγράφων διαγωνισμών, για την διευκόλυνση ακριβούς και πλήρους απάντησης των υποψηφίων και εύκολης αναζήτησης των απαντήσεών τους
5. Καθορισμός υποκειμενικών και αντικειμενικών κριτηρίων επιλογής, τα οποία θα οδηγούν σε μια σταθμισμένη αξιολόγηση των προτάσεων. (Πρόβλεψη λόγων αποκλεισμού -Υποχρεωτικών και δυνητικών κατά περίπτωση)
6. Χρήση των διεθνώς αναγνωρισμένων τεχνικών προδιαγραφών των διαφόρων ειδών
7. Δημοσίευση των Διακηρύξεων, αφού η κάθε πληροφορία που παρέχεται στους ενδιαφερόμενους, θα πρέπει να διατίθεται εξίσου σε όλα τα ενδιαφερόμενα μέρη. **[16]**

8. Τήρηση κανόνων χρηματοοικονομικής διοίκησης από την διαδικασία για την επιλογή αναδόχου ως την τελική ανάθεση δημόσιας σύμβασης με έναν οικονομικό φορέα.
9. Ορισμός ομάδας υπαλλήλων που θα επιφορτιστεί με τη διεξαγωγή και την αξιολόγηση των υποβληθέντων προσφορών, από το στάδιο της κατάθεση της προσφοράς μέχρι την τελική επιλογή αναδόχου και την υπογραφή της προκαθορισμένης σύμβασης
10. Παροχή συμβουλών από την Ανεξάρτητη Αρχή δημοσίων συμβάσεων, η οποία συντάσσει κατευθυντήριες γραμμές και γνωμοδοτήσεις επί των διαδικασιών, δημοσιοποιώντας εγχειρίδια, οδηγούς εφαρμογής, πρότυπα έγγραφα και υποδείγματα και τέλος
11. Ευλαβική τήρηση **βασικών αρχών δικαίου**, όπως :

- **Η αρχή της ίσης μεταχείρισης και αποφυγής διακρίσεων**

Οι όροι του διαγωνισμού δεν είναι δυνατόν να αποκλείσουν επιχειρήσεις που εδρεύουν σε άλλες Χώρες ή ορισμένη κατηγορία επιχείρησης της ίδιας Χώρας εισάγοντας πολιτική διακρίσεων

- **Η αρχή της αμοιβαίας αναγνώρισης**

Η ελεύθερη κυκλοφορία των εμπορευμάτων και υπηρεσιών πρέπει να εξασφαλίζεται χωρίς να είναι αναγκαία η εναρμόνιση των εθνικών νομοθετημάτων των κρατών μελών

- **Η αρχή της διαφάνειας των διαδικασιών**

Η διαδικασία ανάθεσης μιας σύμβασης πρέπει να βασίζεται σε κανόνες, οι οποίοι έχουν δημοσιοποιηθεί και είναι γνωστοί εκ των προτέρων άλλα είναι κατανοητοί, σαφείς και ισχύουν καθόλα τη διάρκεια του διαγωνισμού.

- **Η αρχή της δημοσιότητας**

Οι κανόνες δημοσιότητας είναι συγκεκριμένοι και προβλέπουν τη γνωστοποίηση της πρόθεσης του Φορέα για σύναψη σύμβασης. Οι διαδικασίες ανάθεσης του πρέπει να γίνονται γνωστές στου ενδιαφερόμενους μέσω του Εθνικού ημερήσιου και εβδομαδιαίου Τύπου, της Εφημερίδας Υπηρεσιών Επίσημων Εκδόσεων της ΕΕ, του Επιμελητηρίου, του διαδικτύου κλπ., ΔΙΑΥΓΕΙΑ, ΚΗΜΔΗΣ, ΕΣΗΔΗΣ

- **Η αρχή της αναλογικότητας**

Οι όροι των διακηρύξεων πρέπει να είναι ανάλογα προς τον επιδιωκόμενο σκοπό, δηλαδή την ειδική ανάγκη που εξυπηρετεί για την υλοποίηση της προμήθειας. Οι όροι των διακηρύξεων πρέπει να έχουν τους λιγότερους δυνατούς καταναγκασμούς για τους προμηθευτές και να διευκολύνουν τη συμμετοχή τους στη διαδικασία και την ανάπτυξη του ανταγωνισμού

- Ένα συμβατικό κείμενο κοινά αποδεκτό από την Αναθέτουσα Αρχή και τον οικονομικό φορέα, ολοκληρώνει τη διαδικασία

Πίνακας 4: Ενδεικτικό διάγραμμα εργασιών για την διεξαγωγή ανοικτής διαγωνιστικής διαδικασίας

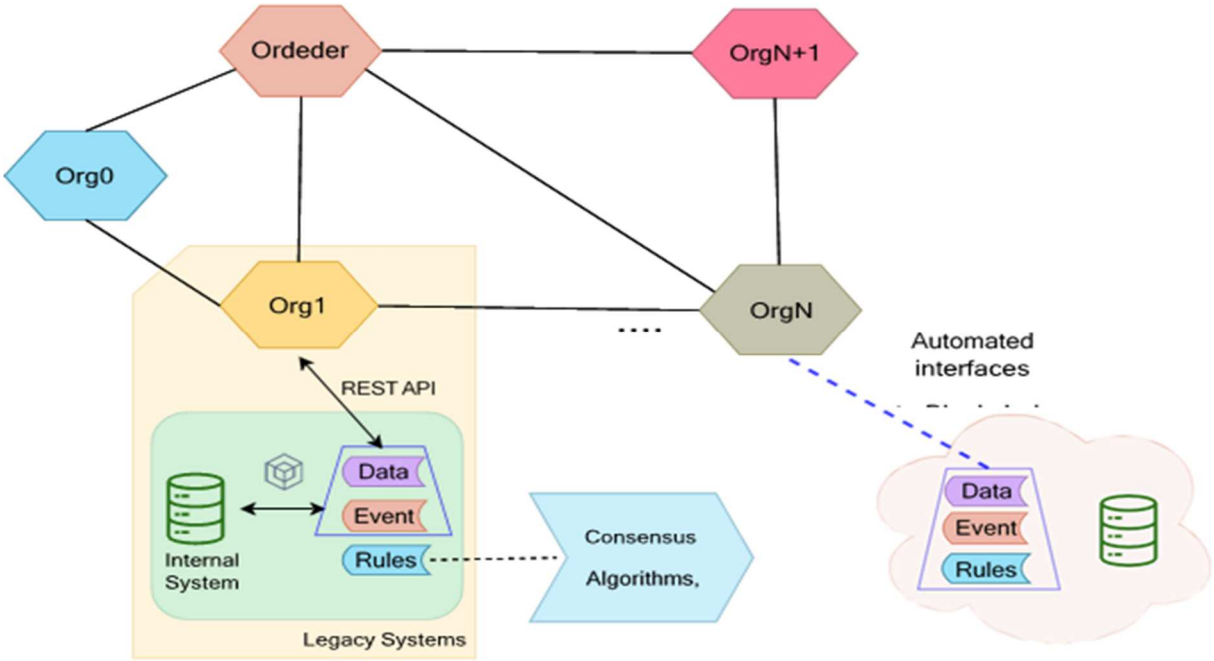
1	Έγκριση Προϋπολογισμού
2	Σχεδιασμός χρονοδιαγράμματος σύναψης της σύμβασης
3	Σύνταξη τεχνικών προδιαγραφών ειδών – Έρευνα αγοράς
4	Διαμόρφωση κριτηρίων αξιολόγησης αναδόχου
5	Σύνταξη όλων των εγγράφων του Διαγωνισμού – Διακήρυξη και Παραρτήματα
6	Ορισμός Ομάδας εργασίας / Συγκρότηση Επιτροπών Διενέργειας και Αξιολόγησης
7	Δημοσίευση Προκήρυξης Διαγωνισμού (Επίσημη Εφημερίδα της ΕΕ/ Τοπικός Τύπος κλπ.)
8	Υποβολή προσφορών
9	Αξιολόγηση προσφορών
10	Απόφαση ανάθεσης/ εφαρμογή της προβλεπόμενης προθεσμίας για προσφυγή στην Ανεξάρτητη Αρχή Προδικαστικών Προσφυγών
11	Συγκέντρωση από τον Ανάδοχο των απαραίτητων δικαιολογητικών κατακύρωσης για την υπογραφή της σύμβασης
12	Υπογραφής της σύμβασης – Σύναψη συμφωνίας

Ο Κεντρικός σχεδιασμός των διαγωνιστικών διαδικασιών για προμήθειες Δημοσίου και η διαχείρισή τους επιβάλλεται να πραγματοποιείται μέσω ηλεκτρονικών εφαρμογών τα τελευταία χρόνια. Την παρούσα στιγμή λειτουργεί ένα ολοκληρωμένο Πληροφοριακό σύστημα ΕΣΗΔΗΣ το οποίο περιλαμβάνει όλα επιμέρους στάδια που ακολουθεί μια Αναθέτουσα Αρχή από την δημοσίευση της Διακήρυξης μέχρι και τη σύναψη της σύμβασης με την ηλεκτρονική υποβολή των προσφορών. Επικουρικά λειτουργεί το ΚΗΜΔΗΣ, με βασικό σκοπό τη συλλογή, την επεξεργασία και τη δημοσιοποίηση στοιχείων που αφορούν συμβάσεις οι οποίες συνάπτονται γραπτώς ανεξαρτήτου διαδικασίας ανάθεσης. Αρμόδια Εποπτική Αρχή είναι η ΕΑΑΔΗΣΥ**.** Παρόλα αυτά συνεχίζουν να παρατηρούνται καθυστερήσεις κυρίως εξαιτίας των Επιτροπών, που διενεργούν, αξιολογούν και κατακυρώνουν την όλη διαδικασία.

Γίνεται εύκολα αντιληπτό ότι πρόκειται για μια εξαιρετικά εξαντλητική διαδικασία με πληθώρα προπαρασκευαστικών βημάτων πριν από την έναρξή της, ποσό μάλλον κατά την υλοποίησή της. Γι΄ αυτό επιβάλλεται να προωθηθεί μια καινοτομική λύση, που θα συμβάλλει ως επί το πλείστον **στην έκπτωση του χρόνου για στάδια εκείνα τα οποία επιβραδύνουν περαιτέρω την διεξαγωγή της.**

8.7 Συνοπτική παρουσίαση του σχεδιασμού και της αρχιτεκτονικής του προτεινόμενου σεναρίου

Οι όροι που διέπουν την παροχή προμηθειών, υπηρεσιών ή έργων από έναν δημόσιο Φορέα ορίζεται σε μια δημόσια σύμβαση που συνάπτεται μετά από μια διαδικασία, ως αυτή περιγράφεται στο υποκεφάλαιο 8.6. Και εδώ αναρωτιόμαστε. Μπορεί η δημόσια διοίκηση να χρησιμοποιήσει smart contracts για να ενσωματώσει τους όρους που διέπουν την παροχή προμηθειών, υπηρεσιών ή έργων; Αρχικά οφείλουμε να αξιολογήσουμε τα βασικά στοιχεία μια σύμβασης, προκειμένου να καθοριστεί εάν ένα έξυπνο συμβόλαιο πληροί τις απαιτήσεις. Ποια είναι τα κύρια εμπόδια ; Θα μπορούσαμε να προτείνουμε μια πιθανή λύση;



Εικόνα 44: Τρόποι ενσωμάτωσης του Blockchain στα συμβατικά πληροφοριακά συστήματα

Δεν πρέπει να εθελοτυφλούμε στις νέες τάσεις της τεχνολογίας, χωρίς μάλιστα να εντοπίζουμε τομείς στους οποίους θα μπορούσαμε να εφαρμόσουμε νέες και βελτιωμένες λύσεις. Το προτεινόμενο σενάριο δεν καλύπτει ολόκληρο τον κύκλο ζωής των δημοσίων συμβάσεων **παρά μόνο τον τρόπο διεξαγωγής της διαγωνιστικής διαδικασίας.** Σε σύγκριση με τις αναποτελεσματικές και δαπανηρές διαδικασίες επικύρωσης των δημόσιων μπλοκ αλυσίδων, οι οποίες ενδεχομένως δεν θα βελτίωναν αισθητά τα μέχρι στιγμής δεδομένα, επιλέχθηκε το Hyperledger ως η ιδανική επιλογή.

Ας υποθέσουμε ότι έχουμε αναλάβει της διεξαγωγή ενός Ανοικτού Διαγωνισμού (Επιλογή συγκεκριμένου τύπου – είδους διαδικασίας βάσει συγκεκριμένων παραμέτρων, που ορίζονται στην σχετική νομοθεσία). Αναφερόμαστε στο στάδιο που προηγείται πριν από τη σύναψη της σύμβασης. Η πρότασή μας περιλαμβάνει μια συγκεκριμένη ροή εργασιών. Θέτοντας ως πρωταρχικό στόχο μας την

διασφάλιση της αποδοτικότητας ενός τέτοιου εγχειρήματος, τηρώντας την αρχή της διαφάνειας των διαδικασιών, παραθέτουμε μια συνοπτική παρουσίαση υλοποίησης δικτύου του προτεινόμενου σεναρίου, που βασίζεται σε **θεμελιώδη στοιχεία (η ανάλυσή τους θα ακολουθήσει στη συνέχεια) του δικτύου Hyperledger Fabric :**

- **Έναν Orderer (Organization)** – Περιφέρεια Ηπείρου, ο οποίος είναι υπεύθυνος για το ordering service (Raft)
- **Τέσσερις Οργανισμούς (Organizations)** – Περιφερειακές Ενότητες, όπου ο κάθε ένας από αυτούς έχει έναν χρήστη (peer) – Αρμόδιοι υπάλληλοι της εκάστοτε Περιφερειακής Ενότητας.
- **Ένα κανάλι επικοινωνίας (channel),** στο οποίο συνδέονται οι οργανισμοί, ενώ παράλληλα εκεί γίνεται deploy (επίκληση) του chaincode.

- **Συσχετίσεις δεδομένων και smart contracts στο προτεινόμενο σενάριο**

Σε πρώτη φάση, δημιουργούμε smart contracts με τις αντίστοιχες συσχετίσεις στο προτεινόμενο δίκτυο.
Συγκεκριμένα:

- ✓ **Το Register Contract (RC) Σύμβαση Μητρώου**

Αυτό το Smart Contract το οποίο ενεργεί **ως μητρώο όλων των χρηστών του συστήματος**.
Αν θεωρήσουμε ότι οι χρήστες χωρίζονται σε πέντε διαφορετικές κατηγορίες – οντότητες, δηλαδή:

(i) Κεντρική Αναθέτουσα Αρχή
(ii) Οι επιχειρησιακές μονάδες της
(iii) Οικονομικοί φορείς - Προμηθευτές
(iv) Επιτροπή διενέργειας και αξιολόγησης του διαγωνισμού
(v) Οικονομική Επιτροπή

Η σύμβαση μητρώου περιέχει μια αντιστοίχιση ενός χρήστη του συστήματος μέσω του μοναδικού αναγνωριστικού πεδίου του (π.χ. id) με μια μοναδική διεύθυνση smart contract που ονομάζεται Data Contract (DC) και αντιστοιχεί σε δεδομένα. Αυτό το μοναδικό αναγνωριστικό πεδίο θα πρέπει να είναι μοναδικό ανά χρήστη και να μην μπορεί να αποκαλύψει την ταυτότητά του.

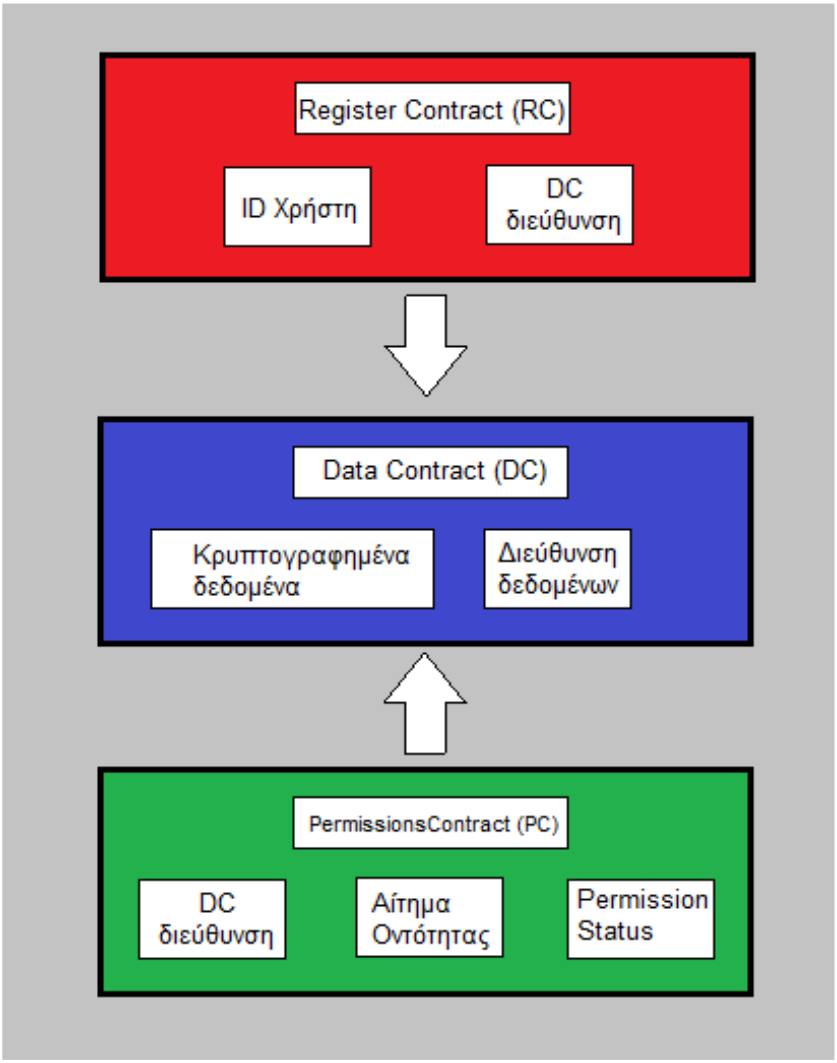
- ✓ ***Το Data Contract (DC) Σύμβαση Δεδομένων***

Αυτό το smart Contract είναι μοναδικό για κάθε χρήστη και περιέχει τα **κρυπτογραφημένα δεδομένα του μαζί με μια διεύθυνση για το που βρίσκονται**. Χρησιμοποιείται ένα κρυπτογραφημένο αντίγραφο των δεδομένων προκειμένου οι οντότητες που επιθυμούν πρόσβαση στα δεδομένα να είναι σε θέση να επαληθεύσουν την ακεραιότητα τους, αντιμετωπίζοντας έτσι παράλληλα το μοντέλο απειλών διαχειριστή κακόβουλων δεδομένων.

- ✓ ***Permissions Contract (PC) Σύμβαση Αδειών***

Αυτό το Smart Contract αφορά **τη διαχείριση δικαιωμάτων των δεδομένων των χρηστών**. Συγκεκριμένα, περιέχει μια αντιστοίχιση της διεύθυνσης της σύμβασης δεδομένων (DC) ενός χρήστη με κάποιον άλλο χρήστη. Αυτά τα smart contracts προσδιορίζονται με μοναδικό τρόπο μέσω ενός πεδίο που ονομάζεται "Status" το οποίο **περιέχει το είδος της έγκριση-πρόσβασης που δίνει ο ιδιοκτήτης των εκάστοτε δεδομένων σε κάποιον άλλο χρήστη.**

Οι έξυπνες συμβάσεις του συστήματος μαζί με τα δεδομένα που περιέχουν και τις σχέσεις υψηλού επιπέδου μεταξύ τους απεικονίζονται στη παρακάτω εικόνα.



Εικόνα 45: Smart Contracts με τα δεδομένα τους και τις μεταξύ τους συσχετίσεις

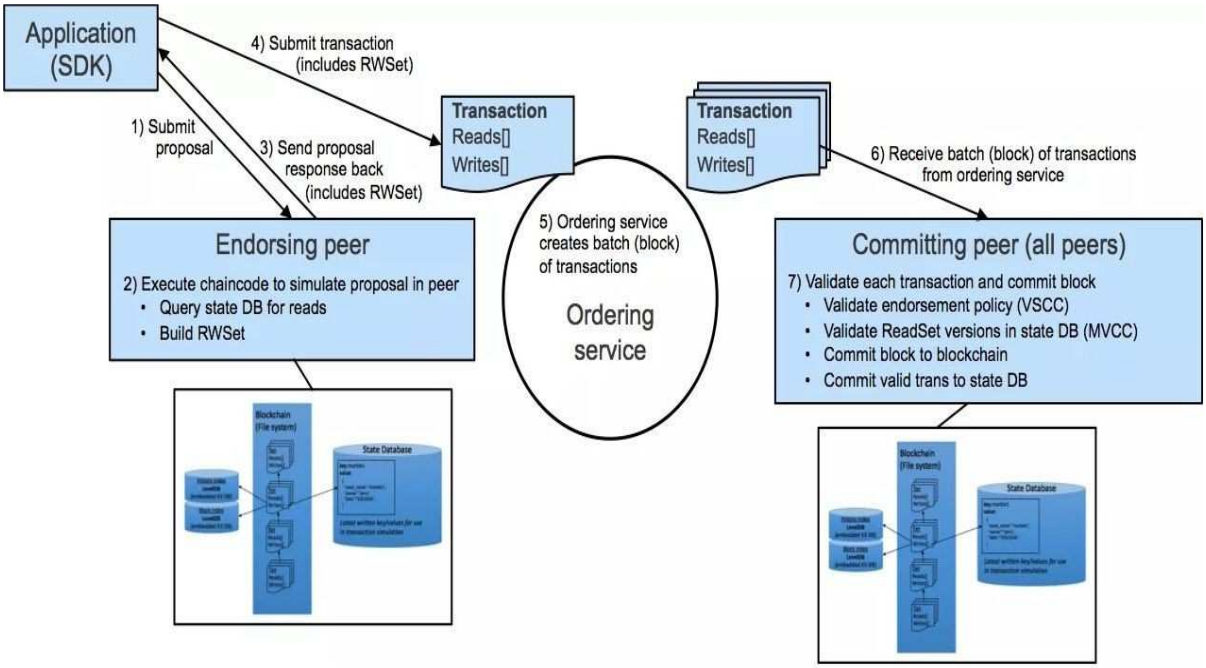
- **Καθορισμός των ρόλων των μελών του στο δικτύου στο Hyperledger Fabric του προτεινόμενου σεναρίου**

Στη συνέχεια, θα αποδώσουμε τους ρόλους στο δίκτυο το οποίο αναπτύσσεται σε περιβάλλον Hyperledger Fabric, για την υλοποίηση ενός σεναρίου διαγωνιστικής διαδικασίας για προμήθειες δημοσίου. Τα μέλη του δικτύου δηλαδή α**) η Αναθέτουσα Αρχή και οι επιχειρησιακές μονάδες της, β) οι Οικονομικοί φορείς - Προμηθευτές, γ) η Επιτροπή διενέργειας και αξιολόγησης, δ) η Οικονομική Επιτροπή** συνάπτουν smart contracts - τα γνωστά ψηφιακά συμβόλαια - που δημιουργούνται και εκτελούνται στο Blockchain και καθορίζουν :

- ✓ **τις αρμοδιότητες του κάθε μέλους,**
- ✓ **τον αριθμό και τα διαπιστευτήρια των χρηστών**
- ✓ **τις πληροφορίες που πρέπει να διατίθενται στην πλατφόρμα,**
- ✓ **τον χρόνο απόκρισης,**
- ✓ **την προθεσμία για την υποβολή των δικαιολογητικών,**
- ✓ **τον βαθμό πρόσβασης στα δεδομένα και**
- ✓ **τη διασφάλιση του απορρήτου ιδιαίτερων πληροφοριών ή συναλλαγών.**

8.8 Ανάπτυξη του σεναρίου – Αναλυτική περιγραφή Διενέργειας Ανοικτής Διαγωνιστικής Διαδικασίας για την σύναψη δημόσιας σύμβασης στο Hyperledger Fabric

Με γνώμονα λοιπόν τη εξασφάλιση της εμπιστοσύνης, τη λογοδοσία και την μείωση των ενδιάμεσων μερών, στο σημαντικότερο στάδιο διαχείρισης του κύκλου ζωής των συμβολαίων, δημιουργούμε **ένα Σενάριο χρήσης στην Διακυβέρνηση**. Πρόκειται για ένα **δίκτυο από 4 Περιφερειακές Ενότητες** που στο σύνολό τους απαρτίζουν μια Περιφέρεια και επιτρέπουμε σε **κατάλληλα εξουσιοδοτημένους συμμετέχοντες** (διαθέτουν ψηφιακή υπογραφή και δραστηριοποιούνται στο αντικείμενο βάσει κωδικού CPV[25] που προκηρύξαμε διαγωνισμό) **να υποβάλουν και ενδεχομένως να ανταγωνίζονται και να διαπραγματεύονται (εφόσον το επιτρέπει το επιλεγόμενο είδος του διαγωνισμού)** τις οικονομικές τους προσφορές, εντός των καναλιών.



Εικόνα 46: Hyperledger Fabric function system

[25] Κωδικοί CPV Είδος δραστηριοτήτων – δημιουργεί ένα σύστημα **ενιαίας ταξινόμησης** για δημόσιους διαγωνισμούς το οποίο βοηθά στην τυποποίηση των αναφορών που χρησιμοποιούνται από τις αναθέτουσες αρχές, για **την περιγραφή των δημοσίων συμβάσεων (Πηγή :** https://www.promitheies.gr/CPV-kwdikoi**). Στο σενάριο μας θα αποτελεί τον Αναγνωρίσιμο Κωδικό, βάσει του οποίου θα « παράγεται » ένα Αυτοματοποιημένο Μήνυμα μέσω Επιμελητηρίου**.

- **Ο Φορέας / Οργανισμός/ Αναθέτουσα Αρχή θα καθορίσει την πολιτική έγκρισης των μελών του καναλιού Endorsement policy**. Ορίζονται εξαρχής τα κριτήρια και οι παράμετροι. Στα μέλη του καναλιού προσδίδεται επίσης δικαίωμα άρνησης. Ο end – user είναι εκείνος ο χρήστης – διαχειριστής που θα εκχωρεί τα δικαιώματα στα μέλη.
- **Για τα Organizations μας (Περιφερειακές Ενότητες) που θα λειτουργούν ως ξεχωριστοί κόμβοι** (Περιφερειακή Ενότητα Ιωαννίνων, Περιφερειακή Ενότητα Άρτας, Περιφερειακή Ενότητα Πρεβέζης, Περιφερειακή Ενότητα Θεσπρωτίας) και συμμετέχουν στο channel, θα υπάρχουν τα **απαραίτητα ψηφιακά πιστοποιητικά αλλά θα δημιουργηθούν επιπλέον τα private keys τους** για **την πρόσβαση, την υπογραφή και την επικύρωση των πράξεων** τους στην εφαρμογή – (permissioned blockchain), τα οποία ονομάζονται crypto material και είναι τα μονοσήμαντα αναγνωριστικά στοιχεία τους εντός του δικτύου.
- **Υποσημείωση** : Οι Περιφερειακές Ενότητες θα έχουν παρόμοια προσβασιμότητα στα δεδομένα που τα αφορούν, διενεργούν συναλλαγές και ενημερώνονται από το δίκτυο σχετικά με την έκβαση των αιτημάτων τους.
- Η διαχείριση της ταυτότητας των χρηστών θα λαμβάνει χώρα μέσω των **Membership Services** Αυτό σημαίνει ότι **κάθε μέλος του δικτύου – peer**, αποκτά δικό του αρχείο στο Membership Service Provider (MSP), το οποίο χρησιμοποιείται για να επιτρέπει στους κόμβους και στους χρήστες, να αναγνωρίζονται ως μέλη του δικτύου.
- Το Hyperledger Fabric διαθέτει **υπηρεσία αρχής έκδοσης πιστοποιητικών Certificate Authority (CA)** Ο κόμβος Certificate Authority (CA) διατηρεί τις ταυτότητες όλων τον κόμβων του δικτύου (clients, peers, orderers) και είναι υπεύθυνος για την αντιστοίχιση ψηφιακών πιστοποιητικών σε κάθε κόμβο που θα χρησιμοποιηθούν για την ταυτοποίησή τους κατά την λειτουργία του δικτύου. Το Fabric χρησιμοποιεί κρυπτογραφικά πιστοποιητικά X509 για την υλοποίηση της ταυτοποίησης και της αυθεντικοποίησης των κόμβων του δικτύου. Το Fabric παρέχει δικιά του υλοποίηση του CA, παρόλα αυτά, σύμφωνα με την αρθρωτή αρχιτεκτονική του, μπορεί να χρησιμοποιηθεί και διαφορετική υλοποίηση.
- Το Fabric χρησιμοποιεί δύο διαφορετικές τεχνικές για την αρχικοποίηση των κρυπτογραφικών πιστοποιητικών του κάθε κόμβου του δικτύου. Στην πρώτη, όλα δημιουργούνται πριν την δημιουργία του δικτύου από έναν CA και κατανέμονται σε κάθε κόμβο. Στην δεύτερη, δημιουργείται πρώτα ένας CA ο οποίος στην συνέχεια, για κάθε οντότητα του δικτύου (πχ peer) που έρχεται η ώρα να δημιουργηθεί, δυναμικά δημιουργεί τα πιστοποιητικά του.

- **Σημειώνεται ότι ο κάθε κόμβος του Fabric ζει απομονωμένος μέσα σε ένα περιβάλλον εικονικοποίησης (docker container) και επικοινωνεί με τους υπόλοιπους με την χρήση του πρωτοκόλλου gRPC[26].** Η μετάδοση των μηνυμάτων και των συναλλαγών θα πραγματοποιείται **μέσω κόμβων (nodes)**

- **Μόνο όσοι κόμβοι - υπολογιστές συμμετέχουν σε ένα κανάλι, έχουν πρόσβαση στα έξυπνα συμβόλαια κ**αι στην πραγματοποίηση συναλλαγών, διατηρώντας το απόρρητο των ιδιωτικών τους δεδομένων

- Οι κόμβοι αυτοί **διατηρούν ένα αντίγραφο του ημερολογίου, το οποίο έχει επαληθευτεί από ένα μηχανισμό συναίνεσης και οι συναλλαγές ομαδοποιούνται σε bloc**k που περιλαμβάνουν ένα hash το οποίο συνδέει το κάθε block με το προηγούμενό του

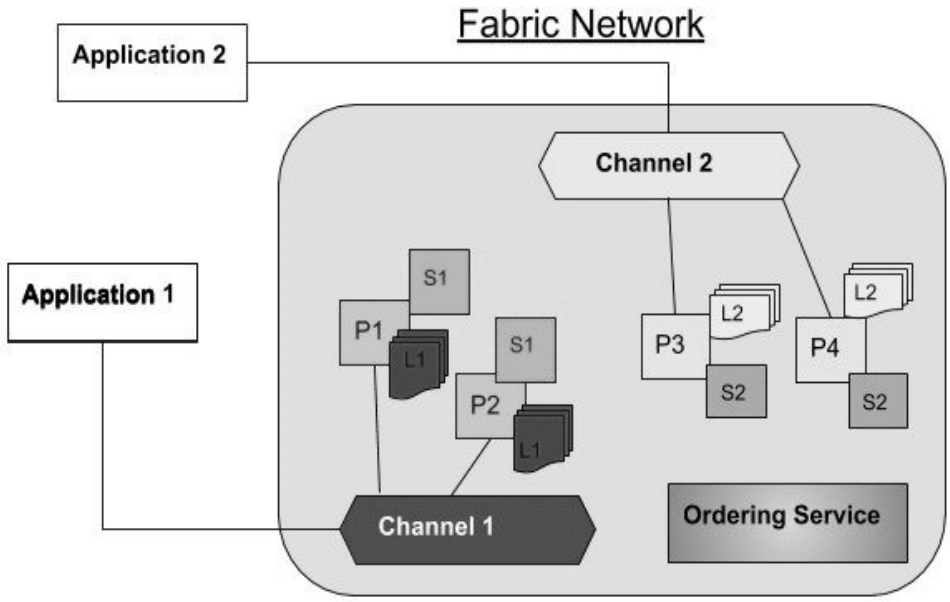
- **Στο Ledger** το οποίο προσομοιάζει με ένα λογιστικό βιβλίο, υπάρχει το καθολικό των συναλλαγών. Γνωρίζουμε ότι στο Hyperledger Fabric **το Ledger αποτελείται από δύο επιμέρους στοιχεία** : 1. **το World Estate**, όπου περιγράφει τη κατάσταση του ledger για κάποια δεδομένη χρονική στιγμή, περιέχει τις **τωρινές τιμές των καταχωρήσεων** που υπάρχουν στην αλυσίδα και 2. **το Ημερολόγιο Συναλλαγών (Transaction Log)** στο blockchain, όπου καταγράφονται όλες τις συναλλαγές που οδηγούν σε κάθε κατάσταση στο World State., **περιέχει χρονολογικά όλες τις συναλλαγές που έχουν γίνει**. Με αυτόν τον τρόπο επιταχύνεται η πρόσβαση στα δεδομένα, ειδικά για την απλή ανάγνωση τιμών. Κι επειδή πρόκειται για αποκεντρωμένο δίκτυο - distributed, η καταγραφή των συναλλαγών στο σενάριό μας θα πραγματοποιείται από όλους ταυτόχρονα. Όλοι θα είναι κοινωνοί και κάτοχοι της ίδιας πληροφορίας, γεγονός που εξασφαλίζει τη διαφάνειας της διαδικασίας.

- Αμέσως μετά, δημιουργείται το αρχικό block - **genesis block** του orderer στο κανάλι του συστήματος (system channel). Το block αυτό είναι απαραίτητο προκειμένου να λειτουργήσουν οι **orderer κόμβοι, στην περίπτωση μας ένας ordener (επικεφαλής υπάλληλος της Περιφέρειας Ηπείρου) και να δημιουργηθούν κανάλια εφαρμογών (application channels).** Το genesis block είναι πολύ σημαντικό καθώς επιπλέον **ορίζει μία κοινοπραξία (consortium) η οποία αναφέρει ποιοι organizations αναγνωρίζονται από το δίκτυο.**

[26] Είναι ένα σύστημα κλήσης απομακρυσμένης διαδικασίας ανοιχτού κώδικα (RPC) και χρησιμοποιεί το HTTP/2 για μεταφορά, τα πρωτόκολλα buffer ως γλώσσα περιγραφής διεπαφής και παρέχει λειτουργίες όπως έλεγχος ταυτότητας, αμφίδρομη ροή και έλεγχος ροής, αποκλεισμού ή μη αποκλεισμού δεσμεύσεων και ακυρώσεων και χρονικών ορίων. Δημιουργεί συνδέσεις πελατών και διακομιστών μεταξύ πλατφορμών για πολλές γλώσσες

- **Αφού δημιουργηθούν τα crypto material και το genesis block μπορούμε να δημιουργήσουμε το κανάλι της εφαρμογής.**

- **Τα Channels** θα διασφαλίζουν ότι μόνο συγκεκριμένοι συμμετέχοντες μιας συναλλαγής μπορούν να την δουν και έτσι θα δημιουργείται ξεχωριστό καθολικό των συναλλαγών τους, στο οποίο όμως πολλαπλά διαφορετικά μέρη μπορούν να διαδράσουν με την ίδια οικουμενική πηγή αλήθειας, με ασφαλή τρόπο.



Εικόνα 47: Η χρήση καναλιών για απομόνωση των αλυσίδων

- Τρεις τύποι συναλλαγών - transactions θα εκτελούνται μέσα στα κανάλια από τον admin user

1. Deploy **Ανάπτυξη** **ερωτήματος**	**2. Invoke** **Επίκληση** **ερωτήματος**	**3. Query** **Υποβολή** **ερωτήματος**

- **Στη συνέχεια, μπορούμε να εγκαταστήσουμε και να εκκινήσουμε το chaincode μας στο κανάλι**. Το chaincode αποτελεί την ενσωματωμένη λογική που θα κωδικοποιεί τους κανόνες για συγκεκριμένους τύπους συναλλαγών δικτύου και θα επικυρώνεται από ένα κατάλληλα εξουσιοδοτημένο μέλος. Ο κωδικός αλυσίδας εκτελεί συναλλαγές δικτύου, οι οποίες όταν και εφόσον επικυρωθούν, θα προσαρτηθούν στο κοινόχρηστο καθολικό. Οι Οργανισμοί δύναται να διαφοροποιούνται στις επικυρώσεις προς το συμφέρον τους.

Η δομή του chaincode περιλαμβάνει συναρτήσεις που καθορίζουν τη λειτουργία του συστήματος και είναι οι εξής :

- ✓ Συναρτήσεις Εκκίνησης (Initiation) : κατά την εκκίνηση γίνεται εγγραφή των χρηστών και υπηρεσιών στο ledger για σκοπούς ευκολίας επίδειξης της λειτουργίας του συστήματος.
- ✓ Συναρτήσεις Ερώτησης (Query) : Συναρτήσεις που έχουν ως σκοπό να διαβάσουν δεδομένα από το ledger.
- ✓ Συναρτήσεις Ενημέρωσης (Update) : Οι συναρτήσεις αυτές έχουν ως σκοπό την εγγραφή δεδομένων στο ledger.

- ➢ Αρχικά το **chaincode εγκαθίσταται στους επιλεγμένους peers για τους οποίους θα αναφερθούμε αναλυτικά στη συνέχεια**. Υπενθυμίζουμε ότι η εκτέλεση του chaincode - έξυπνου συμβολαίου συμβαίνει σε απομονωμένο περιβάλλον από το περιβάλλον του endorsing peers, γεγονός που απομονώνει τα έξυπνα συμβόλαια τόσο από τους peers, όσο και μεταξύ τους. Εκτός από το chaincode που αντιπροσωπεύει το έξυπνο συμβόλαιο σε επίπεδο εφαρμογής, μέσα στον peer τρέχει και chaincode συστήματος, το οποίο υλοποιεί πολλές λειτουργικότητες που είναι απαραίτητες για την λειτουργία του δικτύου.
- ➢ Στη συνέχεια **κάθε peer Organization πρέπει να εγκρίνει τον κώδικα**.
- ➢ Αφού ο **κώδικας εγκριθεί από όλους τους peer Organizations, υποβάλλεται στο κανάλι και είναι πλέον έτοιμος να χρησιμοποιηθεί.**
- ➢ Για να εκκινήσει **καλούμε την συνάρτηση εκκίνησης**.
- ➢ Τα **συμβάντα - events** θα αποτελούν **τα στάδια του διαγωνισμού**

Το κάθε στάδιο θα ενεργοποιεί το chain code και θα στηρίζεται σε χρονικά όρια – προθεσμίες που έχουν τεθεί από την Αναθέτουσα Αρχή.

Πίνακας 5: Τα συμβάντα – events του προτεινόμενου σεναρίου

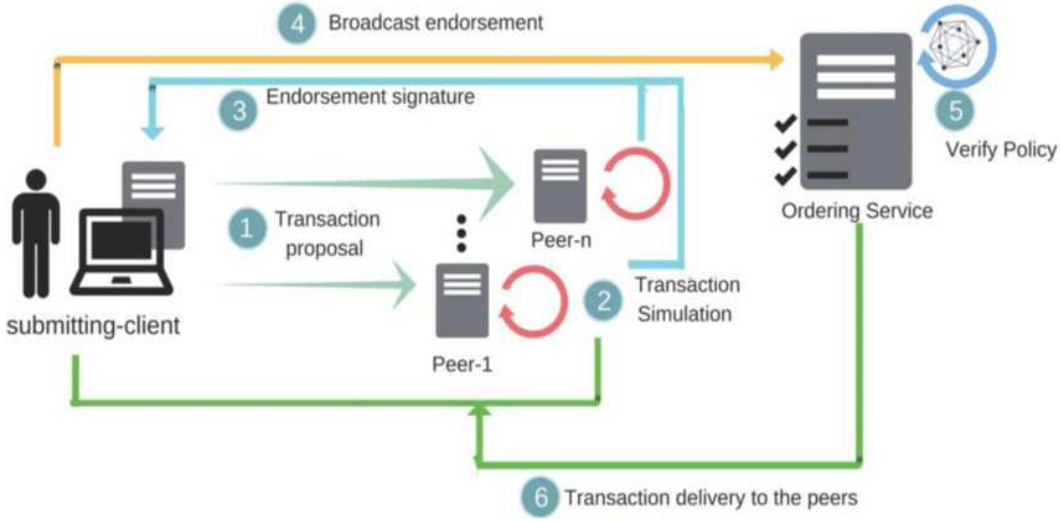
Events	**Στάδια Ανοικτής διαγωνιστικής διαδικασίας**
1ο Event	Δημοσίευση Διακήρυξης στην πλατφόρμα
2ο Event	Υποβολή δικαιολογητικών - προσφορών
3ο Event	Αξιολόγηση τεχνικής – οικονομικής προσφοράς
4ο Event	Αξιολόγηση δικαιολογητικών κατακύρωσης
5ο Event	Ανάθεση – Σύναψη συμφωνίας

- ➢ **Οι clients (Οικονομικοί φορείς - Προμηθευτές) είναι εξωτερικά στοιχεία του δικτύου**. Αντικατοπτρίζουν τον τελικό χρήστη της εφαρμογής και είναι υπεύθυνοι για την δημιουργία συναλλαγών. Επικοινωνούν τόσο με **τους peers όσο και με τους orderers για τους οποίους θα αναφερθούμε παρακάτω. Η Ψηφιακή υπογραφή** θα είναι το διαπιστευτήριο που απαιτείται για να έχουν ανοικτή πρόσβαση οι **clients**. Στη Διακήρυξη θα περιγράφεται επιπλέον στους όρους της, ποιοι κανόνες που διέπουν τις συναλλαγές στο δίκτυο και οφείλουν να τηρηθούν από τους συμμετέχοντες.

- **Οι peers αποτελούν ένα από τα βασικότερα κομμάτια του δικτύου**. Οι peers είναι οι κόμβοι του δικτύου που κρατάνε αντίγραφο της αλυσίδας και του έξυπνου συμβολαίου που εκτελείται από κάθε κανάλι του δικτύου. **Οι Οργανισμοί** αποτελούν τις οντότητες στις οποίες "ανήκουν" οι peers. Χρησιμεύουν για την προσαρμογή του δικτύου σε σενάρια του πραγματικού κόσμου. Κάθε peer ανήκει σε έναν οργανισμό.
- **Οι peers χωρίζονται σε δύο κατηγορίες: τους endorsers (endorsing peers – Μέλη της αρμόδιας Επιτροπής Αξιολόγησης) και τους committers (committing peers – Μέλη της Οικονομικής Επιτροπής Περιφέρειας Ηπείρου), ανάλογα με τον διακριτό ρόλο που έχουν στο δίκτυο**.

- **Οι endorsers** είναι peers που έχουν οριστεί από την πολιτική του δικτύου ως κόμβοι που εκτελούν προσομοιώσεις συναλλαγών κατά την διαδικασία **υποβολής μιας συναλλαγής**, απαντώντας σε αιτήματα endorsement requests. Οι endorsers ουσιαστικά υλοποιούν το στάδιο **execute** της αρχιτεκτονικής execute-order-validate. Υπεύθυνος για την έγκριση των συναλλαγών θα οριστεί **η Επιτροπή Αξιολόγησης του διαγωνισμού** μέσω **endorsing peers που αντιστοιχούν σε συγκεκριμένους κόμβους** και οι οποίοι έχουν άμεση σχέση μεταξύ τους, δημιουργούν μια αλληλεξαρτώμενη ενότητα. Βάσει του ενδεδειγμένου μηχανισμού συναίνεσης της πλατφόρμας θα εγκρίνουν τις συναλλαγές. Ένας ρόλος που τους προσδίδει την γνωμοδοτική αρμοδιότητα.
- **Οι committers** είναι υπεύθυνοι για την **επαλήθευση των blocks και των συναλλαγών** που αυτά περιέχουν και είναι αυτοί που εν τέλει καταγράφουν και **προσθέτουν το block** στην αλυσίδα. Οι commiters ουσιαστικά υλοποιούν το στάδιο **validate** της αρχιτεκτονικής execute-order-validate, δηλαδή **επικυρώνει τις συναλλαγές**. **Ως committer θα ορίσουμε την αρμόδια Οικονομική Επιτροπή**, σε έναν ρόλο που του προσδίδει την αποφασιστική αρμοδιότητα. Στην περίπτωσή μας όμως η τελική επικύρωση θα επιτραπεί μία δεδομένη χρονική στιγμή και συγκεκριμένα στο στάδιο της κατακύρωσης αφού έχουμε επιλέξει να διενεργήσουμε ανοικτή διαγωνιστική διαδικασία και αυτό ορίζει η σχετική νομοθεσία.
  - **Όλοι οι peers έχουν τον ρόλο του committer**, όμως συγκεκριμένοι peers έχουν επιπροσθέτως τον ρόλο του endorser.
  - **Orderers** αρμόδιοι υπάλληλοι της κάθε Περιφερειακής Ενότητας ή ένας μόνο υπεύθυνος Περιφέρειας όπως στο σενάριο μας. **Οι Orderers απαρτίζουν το Ordering Service** που είναι υπεύθυνο για την συμφωνία στην σειρά με την οποία οι συναλλαγές θα καταγραφούν στην αλυσίδα. (Υπάρχουν διάφορες υλοποιήσεις για το Ordering Service, καθώς το Fabric επιτρέπει την δημιουργία τόσο ενός κεντρικού Ordering Service με μόνο έναν Orderer, όσο και κατανεμημένων και αποκεντρωμένων Ordering Services που περιλαμβάνουν πολλούς Orderers οι οποίοι χρησιμοποιούν κάποιο πρωτόκολλο συμφωνίας για να επικοινωνήσουν μεταξύ τους).

- **Πολιτική Endorsement** Η πολιτική Endorsement μεσολαβεί και δρα ως ασφαλιστική δικλείδα, αφού μέσω αυτής, ορίζεται για το ποιοι και πόσοι από το σύνολο των endorsing peers πρέπει να εκτελέσουν προσομοίωση της συναλλαγής, ώστε αυτή να γίνει αποδεκτή από το δίκτυο. Η πολιτική αποτελεί χαρακτηριστικό του chaincode στο οποίο αναφέρεται, που σημαίνει ότι σε ένα δίκτυο με πολλά κανάλια, αντίστοιχα πολλά chaincode μπορούν να υπάρχουν διαφορετικές πολιτικές. Η πολιτική Endorsement μπορεί να απαιτεί συγκεκριμένους endorsers ή ένα μίνιμουμ ποσοστό από αυτούς. Πολύ σημαντικό στοιχείο αφού στις Επιτροπές απαιτείται συνήθως η πλειοψηφία των μελών της.



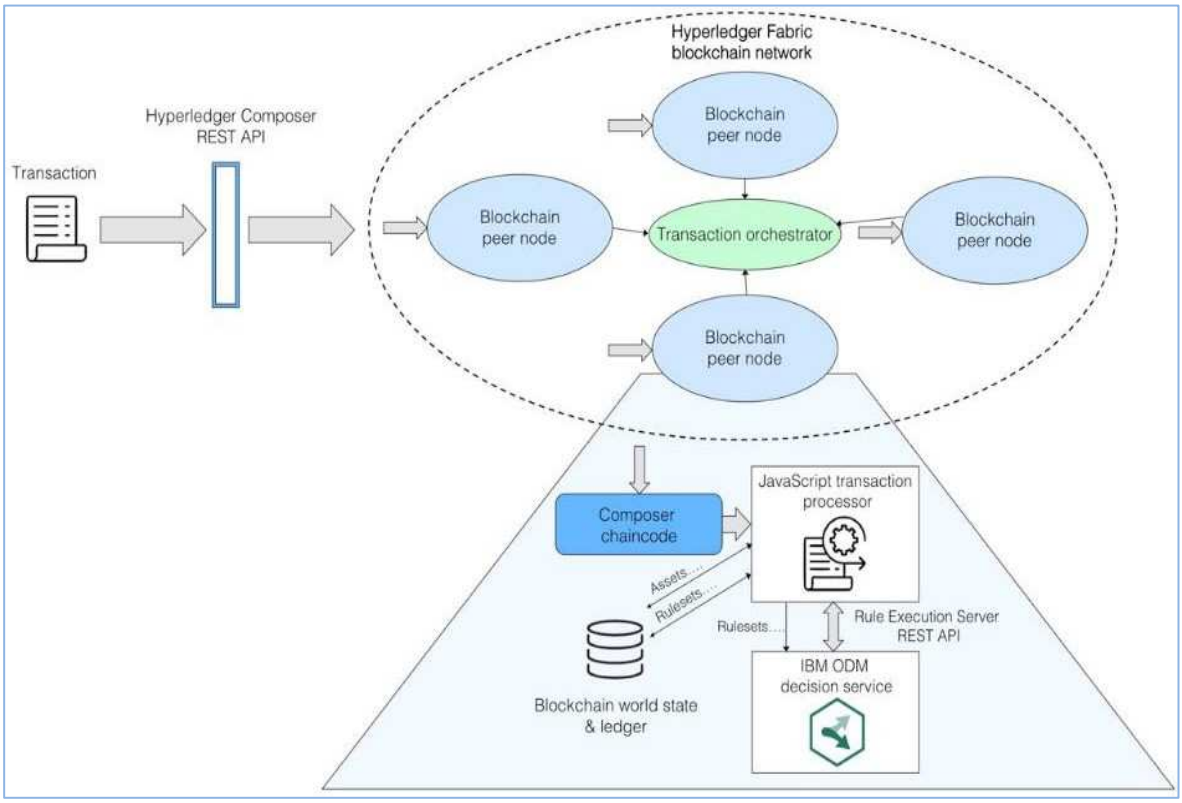
Εικόνα 48 : Ο κύκλος ζωής μίας συναλλαγής στο fabric

<u>Σημαντικές επισημάνσεις επί του προτεινόμενου σεναρίου :</u>

- Όλα τα δεδομένα θα αποθηκεύονται εκτός Blockchain σε ένα χώρο αποθήκευσης δεδομένων. Αυτοί οι χώροι αποθήκευσης δεδομένων θα μπορούν να αποθηκεύσουν μια μεγάλη ποικιλία δεδομένων, αφού θα διατίθενται σε υποδομή cloud.
- Οι πληροφορίες που αποθηκεύονται στους χώρους δεδομένων θα κρυπτογραφηθούν και θα υπογραφούν ψηφιακά για να διασφαλιστεί η ιδιωτικότητα και η αυθεντικότητα των πληροφοριών τους.
- Κάθε φορά που θα αποθηκεύονται πληροφορίες στο χώρο αποθήκευσης δεδομένων, ένας δείκτης στο αρχείο καταγραφής, θα καταχωρείται στο Hyperledger μαζί με το μοναδικό αναγνωριστικό του χρήστη.
- Ο οικονομικός φορέας - προμηθευτής θα ενημερώνεται αυτομάτως ότι τα δεδομένα του έχουν υποβληθεί στην αλυσίδα
- Η πρόσβαση στην πλατφόρμα θα επιτρέπεται μόνο σε κάποιον που έχει έννομο συμφέρον και διαθέτει τα κατάλληλα διαπιστευτήρια
- Η όλη ως άνω περιγραφόμενη διαδικασία είναι αδύνατον να διακοπεί αυθαίρετα ή να τροποποιηθεί με ανθρώπινη παρέμβαση.
- Με την ολοκλήρωση της διαδικασίας ενεργοποιείται το chaincode, για την ανάπτυξη του συμβολαίου – σύναψη σύμβασης εντός της εφαρμογής.

Οι δημόσιες συμβάσεις διαθέτουν τα εχέγγυα προκειμένου να προωθηθούν – ενθαρρυνθούν πρακτικές καινοτομίας, αφού διαδραματίζουν σημαντικό ρόλο στην επιχειρηματική δραστηριότητα. Το Hyperledger αποτελεί μια πρωτοπόρα λύση λογισμικού, μία νέα οργανωτική μέθοδο επιχειρηματικής πρακτικής, η οποία δύναται να φέρει αποτελέσματα όπως αποδοτικότητα, παραγωγικότητα, ποιότητα και ταχύτητα. Απώτερος στόχος οι ισότιμοι όροι ανταγωνισμού για όλους τους οικονομικούς φορείς που συμμετέχουν, καθώς και η ανάπτυξη μιας **πιο φιλικής προσέγγισης και ενίσχυσης της συμμετοχής των μικρομεσαίων επιχειρήσεων στις δημόσιες συμβάσεις**, καθώς διαδραματίζουν θεμελιώδη ρόλο στην οικονομία και την απασχόληση στη Χώρα μας. Η αποτελεσματικότητα των Αναθετουσών Αρχών στον Δημόσιο Τομέα, θα επέλθει μέσα από πρωτοβουλίες μεταρρυθμίσεων σαν αυτή.

Η χρήση του Hyperledger θα μπορούσε να λειτουργήσει ως πρότυπο λογισμικό για διαδικασίες διακυβέρνησης και να συμβάλλει **όχι μόνο του στην έξυπνη οργάνωση των διαδικασιών προμηθειών δημοσίου, αλλά και σε άλλους τομείς όπως η μισθοδοσία των υπαλλήλων ή η εκκαθάριση των δαπανών.**



Εικόνα 49: Η ροή των συναλλαγών στο Hyperledger

Κεφάλαιο 9ο – Οι νομικές προκλήσεις της τεχνολογίας blockchain και των έξυπνων συμβολαίων ανά πεδίο δικαίου, ο GDPR, ηθική διάσταση

9.1 Αστικό Δίκαιο, Δημόσιο Δίκαιο και Δίκαιο προστασίας του καταναλωτή

9.1.1 Smart Contracts

Η εισαγωγή του Blockchain αλλά και η ψηφιοποίηση της επικοινωνίας στην καθημερινότητα η οποία **αναπτύχθηκε ραγδαία κυρίως με τα έξυπνα συμβόλαια στις συναλλαγές**, συνεπάγεται εγγενείς νομικές προκλήσεις, που σχετίζονται αρχικά με τους κανόνες που διέπουν την κατάρτιση και την εκπλήρωση της σύμβασης, την ενδοσυμβατική ευθύνη κατά το αστικό και δημόσιο δίκαιο, την ένταξή τους στο οικείο δικονομικό πλαίσιο, ιδίως αυτό που διέπει την απόδειξη και κυρίως στην συμβατότητα των διατάξεων περί προστασίας των δεδομένων προσωπικού χαρακτήρα, αφού επρόκειτο για μια τεχνολογία με ιδιαίτερη δομή-αρχιτεκτονική και με πρωτοποριακό τρόπο εγγραφής των δεδομένων της.

Οι **έννομες σχέσεις που αναπτύσσονται εντός μιας πλατφόρμας blockchain**, μεταφράζονται ως μια «έξυπνη σύμβαση» μεταξύ των μερών, με αυτοματοποιημένη τη διαδικασία εκτέλεσής-εκπλήρωσή της. Εφόσον πληρούνται δηλαδή συγκεκριμένες προϋποθέσεις, εκτελούνται προκαθορισμένες ενέργειες. **Ποιος και πώς μπορεί κανείς να προσφύγει στην ιδέα της αντικειμενικής ευθύνης για την ικανοποίηση εκατέρωθεν συμφερόντων; Πρέπει το αστικό δίκαιο να αναθεωρήσει θεμελιώδεις έννοιές του, λαμβάνοντας υπόψη ζητήματα της παθολογίας της σύμβασης;**

Πριν από την εξέταση αυτή, οφείλουμε να τονίσουμε ότι ο **Αστικός Κώδικας εφαρμόζεται κατ' αρχήν ευθέως και στο δημόσιο δίκαιο**. Από καμία διάταξή του δεν προκύπτει ότι εφαρμόζεται μόνο στις ιδιωτικές έννομες σχέσεις ή μόνο μεταξύ συναλλασσόμενων ευρισκομένων στο ίδιο επίπεδο εξουσίας και διαπραγματευτικής δυνατότητας. **Εντούτοις, οι διατάξεις του Αστικού Κώδικα, όταν εφαρμόζονται στο δημόσιο δίκαιο και δη στο πεδίο των δημόσιων συμβάσεων, ιδιωτικών και διοικητικών, πρέπει να προσαρμοστούν στις ιδιοτυπίες του Δημοσίου Δικαίου.** Στο δημόσιο δίκαιο το εάν θα συναφθεί η διοικητική σύμβαση είναι συνήθως νομοθετικά προσδιορισμένο [27]. **Στο ιδιωτικό δίκαιο υφίσταται ελευθερία των συμβάσεων ενώ στο δημόσιο δίκαιο ισχύει η αρχή της νομιμότητας της διοικητικής συμβάσεως**.

[27] Βλ. άρθρο 129 ν.4270/2014, το οποίο ορίζει τα εξής: «*Συμβάσεις, από τις οποίες δημιουργούνται υποχρεώσεις σε βάρος του Δημοσίου, δεν δύναται να συνομολογηθούν εάν δεν προβλέπονται από γενικές ή ειδικές διατάξεις ή δεν συντελούν στην εκπλήρωση των σκοπών του*».

Συμβάσεις είναι όλες οι συμφωνίες οι οποίες καταρτίζονται με την ελεύθερη συναίνεση μερών ικανών προς το συμβάλλεσθαι, για νόμιμη αντιπαροχή και νόμιμο σκοπό. Η δικαιοπραξία που δημιουργεί την εγγραφή που εντάσσεται στο Blockchain, **δεν χάνει τα στοιχεία της ως μία αυτοτελής σύμβαση δικαίου**. Επομένως, το είδος της σύμβασης, οι αμοιβαίες υποχρεώσεις των μερών και κάθε άλλο στοιχείο σχετικά με αυτήν, καθορίζεται από τους γενικούς και ειδικούς κανόνες που την απαρτίζουν. **Η νομική μεταχείριση της εκάστοτε δικαιοπραξίας δεν επηρεάζεται από την ένταξή της στην πλατφόρμα Blockchain αλλά από το οικείο νομοθετικό πλαίσιο** («αρχή της αυτοτέλειας») συνοδευόμενο από τα δικαιώματα που απορρέουν από αυτό.

Βασικό δικαίωμα στο δίκαιο των συμβάσεων αποτελεί το δικαίωμα του συμβάλλεσθαι το οποίο περιλαμβάνει επιμέρους δικαιώματα όπως είναι: α) το δικαίωμα προσχώρησης ή μη σε μια σύμβαση, β) το δικαίωμα επιλογής του αντισυμβαλλόμενου, γ) το δικαίωμα διαμόρφωσης του περιεχομένου της σύμβασης και το δ) δικαίωμα καταγγελίας της. **Πως θα αποτυπωθεί σε κάποια πλατφόρμα Blockchain μια ενδεχόμενη ανατροπή της σύμβασης** (πχ υπαναχώρηση, πλήρωση αναβλητικής αίρεσης, ακυρότητα);. **Η αντίστοιχη εγγραφή δύναται να μεταβληθεί;** Γνωρίζουμε ότι ο κάθε κόμβος διατηρεί στο υπολογιστικό του σύστημα τουλάχιστον ένα τμήμα της αλυσίδας με τα αντίστοιχα μπλοκ και τις εγγραφές του, που σημαίνει ότι απαιτείται αντίστοιχη ενέργεια από όλους τους κόμβους του δικτύου, που διατηρούν το οικείο μπλοκ. Συνεπώς, **μια ενδεχόμενη ανατροπή της δικαιοπραξίας, δεν μπορεί να επηρεάσει αυτοτελώς την αντίστοιχη εγγραφή.**

Στα πλαίσια διερεύνησης ως προς το κατά πόσο προστατεύεται νομικά ένας πελάτης-καταναλωτής αυτής της τεχνολογίας, οφείλουμε να ερευνήσουμε τις βασικές αρχές, που άπτονται του δίκαιου του καταναλωτή. Είναι προφανές ότι το αποκεντρωμένο σύστημα λειτουργίας του blockchain, εξαλείφει την ανάγκη για την ύπαρξη ενός κεντρικού μεσάζοντα, **ο οποίος θα μπορούσε να αναλαμβάνει την εγγραφή της δικαιοπραξίας** σε ένα blockchain. Η ένταξη και μόνο μιας εγγραφής σε κάποιο μπλοκ από τους miners, δεν μπορεί να τους προσδώσει έναν τέτοιο επιτελικό ρόλο, διότι δεν προβαίνουν σε κάποιον ουσιαστικό έλεγχο της ακρίβειας της εγγραφής αυτής, παρά μόνο στην τυπική επιβεβαίωσή της, γι' αυτό και δεν μπορούν να θεωρηθούν **ως προμηθευτές κάποιας διαδικτυακής υπηρεσίας**. Λαμβάνοντας υπόψη ότι η καταναλωτική νομοθεσία στην Ελλάδα (Ν 2251/1994), προϋποθέτει να υφίσταται έννομη σχέση μεταξύ **προμηθευτή-καταναλωτή** (άρθρο 2 §1 για γενικούς όρους συναλλαγών και άρθρο 3α §1 εδ.α΄ για συμβάσεις εξ αποστάσεως), καθίσταται σαφές ότι αυτή δεν μπορεί να εφαρμοσθεί. Το ίδιο ισχύει και για ΠΔ 131/2003 (Οδηγία 2000/31) με το οποίο καθορίζονται κάποιες ελάχιστες απαιτήσεις για όσες συμβάσεις συνάπτονται με την χρήση τεχνολογιών του διαδικτύου, διότι αυτές εδώ δεν πληρούνται.

9.1.2 Κρυπτονομίσματα

Η λειτουργία των κρυπτονομισμάτων προσιδιάζει περισσότερο σε ψηφιακά περιουσιακά στοιχεία η αξία των οποίων είναι συνδεδεμένη και υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας ενός συγκεκριμένου πρωτοκόλλου blockchain (παρά σε νόμισμα). Η ΕΚΤ όρισε τα εικονικά νομίσματα ως ***«μία ψηφιακή αποτύπωση αξίας, η οποία δεν εκδίδεται από μία κεντρική τράπεζα, χρηματοπιστωτικό ίδρυμα ή ένα ίδρυμα ηλεκτρονικού χρήματος και μπορεί σε ορισμένες περιπτώσεις, να χρησιμοποιηθεί ως εναλλακτική του παραδοσιακού χρήματος».*** Η ελκυστική τους φύση ως προς τη δυνατότητα κεφαλαιοποίησής τους, με τον προσπορισμό εισοδήματος-κερδών, που αυτά δύναται να αποφέρουν, δελεάζουν ακόμα περισσότερο τους χρήστες οι οποίοι επενδύουν, με ενδεχόμενο κίνδυνο να παραπλανηθούν και ίσως εξαπατηθούν.

Το ασαφές νομικό καθεστώς των κρυπτονομισμάτων, η άγνωστη ταυτότητα των βασικών παραγόντων του, δεν εξασφαλίζουν τα εχέγγυα της ζητούμενης νομικής προστασίας, με συνέπεια οι χρήστες του να βρίσκονται συχνά εκτεθειμένοι σε διάφορους κινδύνους, όπως είναι πχ η διακοπή έκδοσης ή ισχύος των κρυπτονομισμάτων. Σε επίπεδο αστικού δικαίου, οι χρήστες δεν προστατεύονται από τα δικαιώματα επιστροφής των χρημάτων τους, δεν υπάρχει ένας πάροχος υπηρεσιών πληρωμών στον οποίο μπορούν να στραφούν, αλλά και ούτε ένας κεντρικός οργανισμός επίλυσης διαφορών. Γι' αυτό και ο αινιγματικός τρόπος λειτουργίας των κρυπτονομισμάτων για τους χρήστες τους, εγείρουν ζητήματα προς διερεύνηση, ζητήματα νομικά που άπτονται επιπροσθέτως και του δικαίου του καταναλωτή.

9.2 Δίκαιο της Απόδειξης

Η τεχνολογία Blockchain προβληματίζει τους νομικούς κύκλους σε ό,τι ορίζει **το δίκαιο της απόδειξης** και κατά πόσον αυτό βρίσκει εφαρμογή. Το Blockchain αποτελεί πρωτίστως ένα αποδεικτικό μέσο, αφού βρίσκει κανείς **πρόσβαση στο αποδεικτικό υλικό, που είναι μάλιστα ακριβές και αμετάβλητο**. Είναι πλέον γνωστό ότι η απόδειξη βάσει των εγγραφών που λαμβάνουν χώρα σε κάποια τέτοια πλατφόρμα φέρει πλέον την φύση της ηλεκτρονικής απόδειξης. Ειδικότερα, οι εγγραφές στο Blockchain συνιστούν ιδιωτικά ηλεκτρονικά έγγραφα. Κι εφόσον αυτά συντάσσονται με την χρήση ενός συστήματος ηλεκτρονικής ταυτοποίησης, εξομοιώνονται με τα συνήθη ιδιωτικά, ως φέροντα ιδιόχειρη υπογραφή του συντάκτη τους (άρθρα 443 και 445 ΚΠολΔ σε συνδ. με 25 §2 Κανονισμού 910/2014). Τα δε παραπάνω ηλεκτρονικά έγγραφα διαθέτουν βέβαιη χρονολογία, μέσω της χρονοσφραγίδας που φέρουν.

Η επαυξημένη ασφάλεια του εν λόγω αποκεντρωμένου και κατανεμημένου τρόπου λειτουργίας αυτού του συστήματος δεν έγκειται μόνο στα προαναφερθέντα σημεία αναφοράς, αλλά στην λεγόμενη αρχή της πλειοψηφίας. Η αποκεντρωμένη αρχιτεκτονική του Blockchain, μέσω της διάχυσης των εγγραφών και της συνακόλουθης δημιουργίας αντιγράφων σε περισσότερους κόμβους, **αποσκοπεί ακριβώς σε αυτό. Αδιαμφισβήτητα,** σε περίπτωση σύγκρουσης ανάμεσα στις εγγραφές διαφορετικών μπλοκ, προκύπτει το **αμάχητο τεκμήριο ότι ακριβής είναι εκείνη η εγγραφή που υφίσταται στα περισσότερα μπλοκ,** αφού αυτή

συγκεντρώνει μεγαλύτερο αριθμό συναινέσεων. Πρόκειται για μια **λειτουργία που δρα αποτρεπτικά** στο να αλλοιώσει κανείς τα ψηφιακά δεδομένα ενός μεγάλου αριθμού κόμβων. Σε περίπτωση που κάποιος εναντιωθεί σε αυτό, οφείλει να φέρει το **βάρος απόδειξης των ισχυρισμών** του, δεδομένου ότι στην ουσία βάλλει κατά της ίδιας της αποτελεσματικότητας και της δομής ενός συστήματος συναλλαγών, **το οποίο έχει ο ίδιος αυτοβούλως αποδεχθεί για την εκπλήρωση των υποχρεώσεών του.**

Με μόνη λοιπόν την προσκόμιση των στοιχείων που αφορούν την καταχώρισή τους σε μία δημόσια και διαθέσιμη πλατφόρμα blockchain, σε επίπεδο δικονομίας και κυρίως αποδεικτικών μέσων, είναι βέβαιο ότι η απόδειξη των εκάστοτε συναλλαγών, το βέβαιο της χρονολογίας των πραγματικών περιστατικών ή και οι γνωστοποιήσεις με βέβαιο χρονολογίας, βέβαιο περιεχόμενο και βέβαιη παραλαβή (επιδόσεις εγγράφων) γίνεται σχεδόν «αυτοδίκαια» δεκτή από τον δικαστή χωρίς να ζητηθεί η συνδρομή ειδικών-πραγματογνωμόνων, ενώ εξετάζεται ακόμα και η δυνατότητα υπαγωγής των μερών σε διαιτητική πραγματογνωμοσύνη (διενεργούμενη από τους κόμβους), μέσω των αντίστοιχων εγγραφών στο μπλοκ

9.3 Δίκαιο προστασίας δεδομένων προσωπικού χαρακτήρα και blockchain

Η ποσότητα των δεδομένων στον κόσμο μας αυξάνεται γεωμετρικά. Τα φυσικά πρόσωπα έχουν λίγο ή καθόλου έλεγχο στα δεδομένα που είναι αποθηκευμένα για αυτά, ενώ ταυτόχρονα αγνοούν τον τρόπο χρήσης τους. Αμφιλεγόμενα περιστατικά σχετικά με την προστασία της ιδιωτικής ζωής έχουν οδηγήσει σε επιβολή προστίμων, με δημοφιλέστερο εκείνο των 50 εκ. Ευρώ στη Google από τη Γαλλική Επιτροπή Προστασίας Δεδομένων (CNIL, 2019). Ένα από τα βασικότερα στοιχεία πλέον που απασχολούν τους χρήστες κατά τη χρήση οποιουδήποτε ψηφιακού προϊόντος, είναι η προστασία των προσωπικών τους δεδομένων.

Προσωπικά δεδομένα είναι όλες οι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο, το οποίο καλείται **υποκείμενο των δεδομένων**. Τα προσωπικά δεδομένα περιέχουν πληροφορίες όπως: όνομα, διεύθυνση, αριθμός δελτίου ταυτότητας/διαβατηρίου, εισόδημα, πολιτισμικό προφίλ, κωδικός πρωτοκόλλου διαδικτύου (IP), δεδομένα που διατηρούν νοσοκομεία ή γιατροί (με αποκλειστικό σκοπό την ταυτοποίηση προσώπου για ιατρικούς λόγους). Υπάρχουν όμως και οι λεγόμενες **ειδικές κατηγορίες δεδομένων**, για τα οποία δεν επιτρέπεται η επεξεργασία. Τέτοια δεδομένα είναι τα εξής: η φυλετική ή εθνοτική καταγωγή, ο σεξουαλικός προσανατολισμός, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστικές οργανώσεις, τα γενετικά ή βιομετρικά δεδομένα και δεδομένα υγείας, εξαιρουμένων ειδικών περιπτώσεων, τα προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα, εκτός αν αυτό επιτρέπεται από τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία. Σε ό,τι αφορά το blockchain, τα κρυπτογραφημένα δεδομένα είναι προσωπικά δεδομένα τα οποία εμπίπτουν σε μια **νέα κατηγορία δεδομένων προσωπικού χαρακτήρα που δημιουργήθηκε από τον ΓΚΠΔ, τα ψευδώνυμα δεδομένα.**

Η νέα τεχνολογία blockchain λοιπόν αποτελεί έναν νέο τρόπος καταχώρησης και αποθήκευσης δεδομένων, γι' αυτό οφείλουμε να εξετάσουμε **τις παραμέτρους που την συσχετίζουν με το δίκαιο**

της προστασίας προσωπικών δεδομένων, δηλαδή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Νομοθεσίας. Πρόκειται για ένα νομοθέτημα το οποίο θεσπίστηκε για να καλύψει το σύνολο των δεδομένων όλων των φυσικών προσώπων, που είτε διαμένουν στην ΕΕ, είτε είναι γενικώς πολίτες αυτής. Παρόλο που ο **ΓΚΠΔ δίνει ιδιαίτερη έμφαση στην προληπτική προστασία των δεδομένων**, προτρέποντας τον υπεύθυνο ανάπτυξης βάσεων δεδομένων, είτε εκ σχεδιασμού (by Design) και προεπιλογής, είτε εξ' ορισμού (by Default), να ενσωματώσει στο σύστημα τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί η προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων, αυτό δεν αρκεί.

Στο πλαίσιο μιας ανοιχτής αποκεντρωμένης πλατφόρμας **blockchain** παραμένουν αναπάντητα τα ερωτήματα, όπως για παράδειγμα, **ποιος θεωρείται ο υπεύθυνος της επεξεργασίας και ποιος ο εκτελών την επεξεργασία**. Μία επικρατούσα άποψη είναι ότι το κάθε πρόσωπο που συμμετέχει σε μία τέτοια πλατφόρμα πρέπει να αντιμετωπίζεται ως υπεύθυνος των δεδομένων που επεξεργάζεται. Ωστόσο, ζήτημα τίθεται αν αυτά τα πρόσωπα μπορούν να θεωρηθούν από κοινού υπεύθυνοι επεξεργασίας κατά το άρθρο 26 ΓΚΠΔ, καθώς η διάταξη αυτή προϋποθέτει συμφωνία μεταξύ των υπευθύνων. **Τέτοια συμφωνία δεν υφίσταται κατά κανόνα στις ανοιχτές πλατφόρμες Blockchain**. Ωστόσο, στις **κλειστές πλατφόρμες**, στις οποίες υπάρχει κάποιος «διαχειριστής» (Administrator) – υπό την μη τεχνική έννοια του όρου – ο οποίος ιδρύει και λειτουργεί την πλατφόρμα προς ίδιον όφελος, αυτό είναι εφικτό.

Ο ΓΚΠΔ ορίζει επιπροσθέτως μια σειρά ψηφιακών δικαιωμάτων, όπως για παράδειγμα είναι, μεταξύ άλλων, **το δικαίωμα διαγραφής ("right to erasure") των προσωπικών δεδομένων**, το οποίο συνίσταται στη δυνατότητα του ατόμου να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή προσωπικών δεδομένων, που το αφορούν. Με ποιο τρόπο όμως θα μπορούσαν να ικανοποιηθούν σε μία βάση δεδομένων κι άλλα παρόμοια δικαιώματα, όπως αυτό της πρόσβασης, της ενημέρωσης ή ακόμη και της φορητότητας των υποκειμένων προσωπικών δεδομένων; **Σε μια βάση μάλιστα η οποία τηρείται ταυτόχρονα σε χιλιάδες αντίτυπα και από την οποία είναι αδύνατον είτε να τροποποιηθούν, είτε να αφαιρεθούν δεδομένα, υπάρχει δυνατότητα συμμόρφωσης με τον ΓΚΠΔ;** Σε θέματα συμμόρφωσης θα αναφερθούμε παρακάτω. Ας δούμε αναλυτικότερα ποια είναι θεμελιώδη χαρακτηριστικά της τεχνολογίας αυτής, που δημιουργούν εύλογους σχετικούς προβληματισμούς:

1. Το **μόνιμο ιστορικό που δημιουργείται στην αλυσίδα λόγω της αμεταβλητότητας των δεδομένων** της, προσκρούει στο προβλεπόμενο στο άρθρο 17 ΓΚΠΔ **δικαίωμα του υποκειμένου των δεδομένων στην λήθη**, δεδομένου του ότι η επεξεργασία ανίχνευσης δεδομένων σε πολλούς και άγνωστους κόμβους εντός ενός δικτύου blockchain, με απώτερο σκοπό τη διαγραφή, καθίσταται δυσχερής.
2. **Ο καταλογισμός της ευθύνης σε κάποιο πρόσωπο που παραβιάζει τα δεδομένα προσωπικού χαρακτήρα ή προβαίνει σε παράνομη επεξεργασία τους, πως αποδίδεται;** Η **ανωνυμία** που χαρακτηρίζει τέτοιου είδους πλατφόρμες, καθώς και **η ανυπαρξία ενός τρίτου έμπιστου μέρους**, αποτελεί ανατρεπτικό παράγοντα για τον εντοπισμό του δράστη. Άλλωστε,

τα αδικήματα που μπορούν να διαπραχθούν στο σημείο αυτό ποικίλουν. Παρατηρούνται τόσο φαινόμενα παράνομης κτήσης δεδομένων όσο και περιπτώσεις όπου κάποιοι κόμβοι γνωστοποιούν περαιτέρω δεδομένα, που αφορούν τρίτα πρόσωπα. Ο δε ρόλος των miners περιπλέκει ακόμα περισσότερο το ζήτημα, αφού η παραβίαση αυτή τους καθιστά ως "παραυτουργούς", διότι ακουσίως συμμετέχουν σε αυτό το «αδίκημα» κατά την επικύρωση των εν λόγω συναλλαγών.

Από τα παραπάνω, διαπιστώνουμε ότι ο αποκεντρωμένος χαρακτήρας του Blockchain δεν συμβαδίζει με τις διατάξεις του ΓΚΠΔ, διότι είναι προφανές πως έχουν σχεδιασθεί λαμβάνοντας υπόψη τη δομή ενός κεντρικού συστήματος-δικτύου. Κι ενώ για τις **έννομες σχέσεις** που διαμορφώνονται με τη χρήση της τεχνολογίας blockchain, το δίκαιο προστασίας προσωπικών δεδομένων προσφέρει κάποιες λειτουργικές λύσεις, εγγενείς περιορισμοί που απορρέουν από τα ιδιαίτερα χαρακτηριστικά της, είναι ακόμη υπαρκτοί. Καθίσταται επιβεβλημένη **μια νομοθετική παρέμβαση για τέτοιου είδους πλατφόρμες**, με θεμελιώδεις όρους που θα ρυθμίζουν εύστοχα τις βασικές πτυχές της.

9.3.1 Blockchain και GDPR – Συμβατότητα της τεχνολογίας

Οι έννοιες ιδιωτικότητα και πληροφόρηση αποτελούν δύο αποκλίνουσες έννοιες, οι οποίες συγκρούονται δυναμικά τα τελευταία χρόνια, υπό το πρίσμα μιας δημοκρατικής διακυβέρνησης σε μια αναπτυσσόμενη σύγχρονη οικονομία. Στα πλαίσια της υιοθέτησης ενός νομοθετικού πλαισίου προστασίας δεδομένων, λοιπόν, δημιουργήθηκε ο ΓΚΠΔ.

Σε ένα πλαίσιο διερεύνησης της συμβατότητα της τεχνολογίας του Blockchain με το ΓΚΠΔ, οφείλουμε να εξετάσουμε και κάποια άλλα βασικά σημεία, θέτοντας όρια σε έννοιες σχεδόν ταυτόσημες, όμως τόσο διαφορετικές επί της ουσίας. Έννοιες όπως είναι η ανωνυμία και η ιδιωτικότητα. Το κατά πόσο η ανωνυμία θα μπορούσε να αποτελέσει την ασφαλιστική δικλείδα που επιθυμούμε είναι κάτι αμφίσημο. Το μόνο σίγουρο είναι ότι μπορεί να χρησιμοποιηθεί και για σκοπούς αντίθετους από αυτούς που επιδιώκουμε.

Η ανωνυμία κυριολεκτικά σημαίνει απουσία ονόματος, είτε παντελή έλλειψη οποιασδήποτε ταυτότητας, είτε απλά τη μη χρήση πραγματικής ταυτότητας. Στο πλαίσιο της επιστήμης των υπολογιστών και με δεδομένο ότι δεν υφίσταται άλλο στοιχείο ταυτοποίησης, **η ανωνυμία αναφέρεται ουσιαστικά στην ψευδωνυμία συνδυαζόμενη με τη μη-συνδεσιμότητα (unlinkability). Η ψευδωνυμία, αυτονόητα, είναι η χρήση ενός χαρακτηριστικού που δεν παραπέμπει στην πραγματική ταυτότητα του χρήστη. Η μη-συνδεσιμότητα, δε, αφορά στην ιδιότητα του εκάστοτε δικτύου να μην επιτρέπει σε έναν επιτιθέμενο, να ταυτοποιήσει το ψευδώνυμο με την πραγματική ταυτότητα του χρήστη, εκμεταλλευόμενος τις ψηφιακές του κινήσεις**. Στο πλαίσιο των αποκεντρωμένων μητρώων, η σχέση μεταξύ αποκέντρωσης και διαφύλαξης ανωνυμίας, φαίνεται πως είναι αντιστρόφως ανάλογη και οι έννοιες μάλλον ασύμβατες στην υλοποίηση τους.

Η γαλλική αρχή προστασίας προσωπικών δεδομένων (CNIL) έχει ασχοληθεί με τις τεχνολογίες blockchain και τα προσωπικά δεδομένα και υποστηρίζει σε μελέτη της ότι πρόκειται για μία τεχνολογία, **που μπορεί να συνεισφέρει στην υποστήριξη διαφόρων μορφών επεξεργασίας**. Σύμφωνα με την έρευνα, όταν το Blockchain αφορά προσωπικά δεδομένα **εφαρμόζεται ο GDPR επί της ουσίας. Ο GDPR δεν έχει ως σκοπό τη ρύθμιση τεχνολογιών κάθε αυτή, αλλά του περιβάλλοντος εντός του οποίου γίνεται η χρήση των τεχνολογιών αυτών σε πλαίσιο που περιλαμβάνει προσωπικά δεδομένα.**

Η CNIL χρησιμοποιώντας λαμβάνοντας υπόψη την κατηγοριοποίηση τους σε δημόσια, περιορισμένης πρόσβασης και ιδιωτικά blockchain, διαπίστωσε τα εξής :

- τα δημόσια Blockchain είναι προσβάσιμα σε οποιονδήποτε χρήστη. **Κάθε πρόσωπο μπορεί να πραγματοποιήσει μια συναλλαγή, να συμμετάσχει στη διαδικασία επικύρωσης των «μπλοκ» ή να αποκτήσει ένα αντίγραφο του Blockchain.**
- τα Blockchain στα οποία η πρόσβαση απαιτεί άδεια έχουν κανόνες που ορίζουν ποια πρόσωπα μπορούν να συμμετάσχουν στη διαδικασία επικύρωσης ή ακόμα και να πραγματοποιήσουν συναλλαγές. **Μπορούν, κατά περίπτωση, να έχουν πλήρη ή περιορισμένη πρόσβαση**.
- τα Blockchain τα οποία καλούνται «ιδιωτικά» βρίσκονται υπό τον έλεγχο ενός χρήστη ο οποίος αποκλειστικά διασφαλίζει τον έλεγχο της συμμετοχής και της επικύρωσης. Σύμφωνα με ορισμένους ειδικούς, οι εν λόγω χρήσεις δεν ακολουθούν τις κλασικές ιδιότητες του Blockchain, ιδίως την αποκέντρωση και την καταμερισμένη επικύρωση. **Σε κάθε περίπτωση, δεν εγείρουν κάποιο συγκεκριμένο ζήτημα ως προς τη συμβατότητά τους με τον GDPR, καθώς πρόκειται απλώς για «κλασικές» βάσεις διανεμόμενων δεδομένων.**

- **Επιπλέον, η CNIL διακρίνει τρεις τύπους χρηστών σε ένα Blockchain:**
- οι «έχοντες πρόσβαση», οι οποίοι έχουν δικαίωμα ανάγνωσης και απόκτησης αντιγράφου της αλυσίδας.
- οι «συμμετέχοντες», οι οποίοι έχουν δικαίωμα ανάγνωσης (η δημιουργία μίας συναλλαγής την οποία θέτουν προς επικύρωση).
- οι «δευτερεύοντες χρήστες», οι οποίοι επικυρώνουν μία συναλλαγή και δημιουργούν τα «μπλοκ» εφαρμόζοντας τους κανόνες του Blockchain, προκειμένου να γίνουν «αποδεκτοί» από την κοινότητα.
- **Επί της ουσίας, ένα Blockchain μπορεί να περιέχει δύο κατηγορίες δεδομένων προσωπικού χαρακτήρα:**
- την ταυτοποίηση των συμμετεχόντων και των δευτερευόντων χρηστών: κάθε συμμετέχων/ δευτερεύων χρήστης **διαθέτει ένα δημόσιο κλειδί, το οποίο επιτρέπει την εξακρίβωση της ταυτότητας του αποστολέα και του παραλήπτη μίας συναλλαγής.**

- τα συμπληρωματικά δεδομένα, τα οποία εγγράφονται «μέσα» σε μία συναλλαγή (πχ νομιμοποιητικά έγγραφα). Στην περίπτωση που αυτά τα δεδομένα **αποδίδονται σε φυσικά πρόσωπα**, **ενδεχομένως άλλα από τους συμμετέχοντες, άμεσα ή έμμεσα ταυτοποιήσιμα**, πρόκειται για προσωπικά δεδομένα.

Ο GDPR έχει ήδη επιφέρει αλλαγή στο σύστημα λογοδοσίας. Κάθε χρήστης, υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, οφείλει να είναι σε θέση να αποδεικνύει τη συμμόρφωση αυτών των μορφών επεξεργασίας με τις υποχρεώσεις που επιβάλλει ο GDPR. Σχετικές προτάσεις συμμόρφωσης θα αναφερθούν εκτενέστερα παρακάτω.

9.3.2 Ζητήματα συμμόρφωσης με τον Κανονισμό

Οι τεχνολογίες αιχμής εξελίσσονται τόσο ραγδαία που είναι σχεδόν ακατόρθωτο να συμμορφώνονται με τα νομικά κείμενα. Μοναδική λύση σε αυτό αποτελεί η εκ των υστέρων **εναρμόνιση με τις σχετικές διατάξεις τους.** Γι' αυτό κρίνεται απαραίτητο να εξετάσουμε σε ποιες περιπτώσεις έχουμε συμμόρφωση με τον Κανονισμό εξαρχής και σε ποιες περιπτώσεις οφείλουμε να βρούμε τον τρόπο, ακόμη και με διάφορες τεχνικές, ώστε να τηρούμε ευλαβικά την κανονιστική νομοθεσία περί των προσωπικών δεδομένων.

- **Συγκατάθεση υποκειμένου δικαιωμάτων**

Η επιλογή κάποιου να συμμετέχει σε ένα blockchain, τον καθιστά αυτοδίκαια υπόλογο για τα εμμέσως προσβάσιμα προσωπικά του δεδομένα στην αποκεντρωμένη βάση δεδομένων. Ελλείψει κάποιας καθορισμένης σύμβασης με συγκεκριμένους όρους και γραπτό τύπο, η ενέργεια αυτή λογίζεται για τον νομικό κόσμο, **ως συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα**, η οποία όμως **περιορίζεται στην συναλλακτική καθαυτή και μόνο πράξη του**.

- **Εύρεση του Υπεύθυνου Επεξεργασίας**

Η διαδικασία που θα ακολουθηθεί για αποκεντρωμένες βάσεις δεδομένων, προκειμένου να ορισθεί υπεύθυνος επεξεργασίας **διαφέρει και εξαρτάται από τον τύπο blockchain για τον οποίο αναφερόμαστε** (δημόσιο ή ιδιωτικό, αδειοδοτούμενο ή μη, ή κοινοπρακτικό blockchain), επιλέγοντας κατά περίπτωση:

1. Ένα συγκεκριμένο φυσικό ή νομικό πρόσωπο, ή ομάδα συν-υπευθύνων για το σύνολο των δεδομένων της βάσης.
2. Απόδοση του ρόλου στους ελεγκτές/επικυρωτές κάθε block ως προς τα δεδομένα που περιέχονται σε αυτό ή ως προς όλα τα δεδομένα.
3. Ταύτιση Υποκειμένου και Υπευθύνου, όπου ο χρήστης καθίσταται υπεύθυνος επεξεργασίας ή εκτελών των δεδομένων του.

Στα ιδιωτικά (private ή consortium) blockchain θα ορισθεί ως υπεύθυνος επεξεργασίας ο **ιδιοκτήτης ή ο προγραμματιστής τους**. Σε κεντρικού χειρισμού blockchains, η πλήρης συμμόρφωση με τον ΓΚΠΔ είναι εφικτή **καθώς υπάρχει πάντα ένας κεντρικός παράγοντας**.

Το πρόβλημα εντοπίζεται στην περίπτωση που το αρχικό πρωτοκόλλου λόγω συναίνεσης των κόμβων «μετατοπιστεί» στους κόμβους επικύρωσης, Ένα πλήρως αποκεντρωμένο blockchain θεωρεί συν-υπεύθυνους επεξεργασίας και πιθανούς Εκτελώντες όλους τους συμμετέχοντες. Το πρόβλημα στην περίπτωση αυτή εντοπίζεται στον ψευδώνυμο χαρακτήρα των συμμετεχόντων, που προκαλεί ανασφάλεια σχετική με τη διαβίβαση δεδομένων σε τρίτες χώρες, εκτός Ευρώπης. Είναι λοιπόν σοφότερο **να θεωρήσουμε στο δίκτυο μεμονωμένα υπευθύνους ή εκτελώντες σε κάθε κόμβο για τα δεδομένα που αυτός επεξεργάστηκε.**

Εάν το δίκτυο είναι αδειοδοτούμενο αλλά ελεύθερο (public permissioned) παίζει ουσιαστικό ρόλο ο τρόπος καθορισμού των ελεγκτών/επικυρωτών και αν αυτός προέρχεται εξαρχής από τον σχεδιαστή, αν είναι τυχαίος ή αν ορίζεται βάσει προτοποθετημένου αλγορίθμου. Εφόσον οι ίδιοι δεν συμμετέχουν στην επεξεργασία των δεδομένων αλλά έχουν προκαθορίσει τους κόμβους επικυρωτές να καθορίζονται τυχαία ή με μη επεμβατικό τρόπο και έχουν εκχωρήσει τη δυνατότητα σε αυτούς να εξελίσσουν το πρωτόκολλο, **η ευθύνη μετακυλίεται**. Αντίθετα, εάν ο καθορισμός εκτελείται άμεσα και παρεμβατικά ή υπάρχει οιοσδήποτε έλεγχος επί της εξέλιξης του δικτύου, τότε οι κόμβοι λαμβάνουν το ρόλο του Εκτελώντα και η ευθύνη του υπεύθυνου επεξεργασίας βαραίνει αποκλειστικά τους δημιουργούς του λογισμικού ή του πρωτοκόλλου κατ' αντιστοιχία με ένα ιδιωτικό αδειοδοτούμενο blockchain.

Τα πλήρως αποκεντρωμένα blockchains αποτελούν και τη μεγαλύτερη πρόκληση, καθώς το μόνο σημείο αναφοράς τους, είναι **η έλλειψη οποιασδήποτε αρχής, που να ασκεί σαφή εξουσία**. Η αρχική ευθύνη επεξεργασίας δεδομένων προσωπικού χαρακτήρα που **βαραίνει την ομάδα που ανέπτυξε ένα ανοιχτό δημόσιο δίκτυο, μετακυλίεται άμεσα τους πρώτους κόμβους που θα προβούν σε επεξεργασία των δεδομένων και εκτέλεση του πρωτοκόλλου συναίνεση**ς.

Πίνακας 6: Υπεύθυνοι και Εκτελούντες ανά τύπο blockchain

Ιδιοκτησία	Αδειοδότηση	Υπεύθυνος	Εκτελών
Public	Permissioned	Συμμετέχοντες στον καθορισμό του πρωτοκόλλου συναίνεσης	Κόμβοι εκτέλεσης πρωτοκόλλου συναίνεσης
	Permissionless	Κόμβοι εκτέλεσης πρωτοκόλλου συναίνεσης	Χρήστες με εμπορική / επιχειρηματική ιδιότητα
Private	Permissioned	Ιδιοκτήτης ή νόμιμος εκπρόσωπος αυτού	Κόμβοι εκτέλεσης πρωτοκόλλου συναίνεσης
	Permissionless	Ιδιοκτήτης ή νόμιμος εκπρόσωπος αυτού	Χρήστες με εμπορική / επιχειρηματική ιδιότητα

Σχετικά με τα <u>έξυπνα συμβόλαια</u>, εκτιμάται ότι θα πρέπει να αντιμετωπίζονται ισότιμα είτε αναπτύσσονται εντός ενός ιδιωτικού δικτύου είτε εντός ενός πλήρως αποκεντρωμένου blockchain, διότι παράγονται σε αυτά δεδομένα τα οποία υπάγονται στην ευθύνη του

προγραμματιστή αλλά και του παραλήπτη τους. Υπεύθυνος επεξεργασίας μπορεί να είναι ο **προγραμματιστής του έξυπνου συμβολαίου**, υπό την προϋπόθεση ότι επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του συμμετέχοντος.

- **Προάσπιση των Δικαιωμάτων του Υποκειμένου**

Τα δικαιώματα στην πρόσβαση, την τροποποίηση, τη διαγραφή και τη φορητότητα έχουν άμεση σχέση με το πώς αυτά εμφανίζονται και προσπελαύνονται σε ένα blockchain. Διάφορες προτεινόμενες προσεγγίσεις αποτελούν μεταξύ άλλων:

α) η καταστροφή των κλειδιών κρυπτογράφησης και της τήρησης των προσωπικών δεδομένων εκτός αλυσίδας, είτε σε έναν εξωτερικό διακομιστή, είτε σε μία παράλληλη αλυσίδα. Η διατήρηση των προσωπικών δεδομένων εκτός αλυσίδας (off-chain) υπό τον έλεγχο ενός αναγνωρίσιμου Υπεύθυνου, διαδικασία γνωστή ως hashing-out, δίνοντας τη δυνατότητα σε ένα τρίτο μέρος να ελέγχει τα δεδομένα, **καταλύοντας την έννοια της εμπιστοσύνης που το blockchain υπηρετεί**.

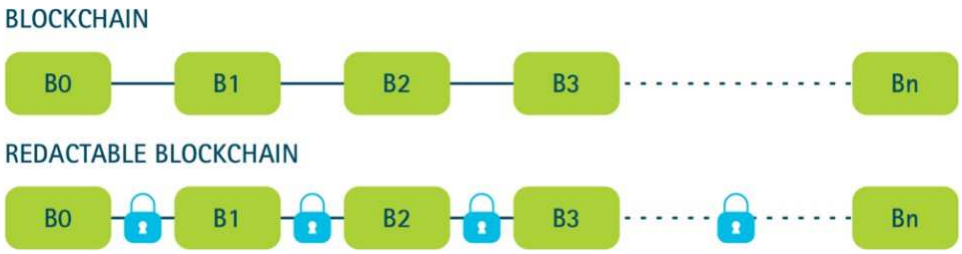
β) Τήρηση των δεδομένων τους αποκλειστικά από τους χρήστες εκτός αλυσίδας με ταυτόχρονη χρήση νέου ζεύγους κλειδιών για κάθε συναλλαγή. Η τροποποίηση των δεδομένων, αν και δυσκολότερη τεχνικά, συμπεριλαμβάνει και τη διαγραφή τους, όταν απαιτείται να γίνει εντός της αλυσίδας

γ) Μία επιπλέον λύση που ξεπερνά την ανάγκη για τήρηση των δεδομένων off-chain είναι ο κατακερματισμός 'χαμαιλέοντα' [4]. Με την τεχνική αυτή εισάγεται η δυνατότητα αλλαγής των δεδομένων που περιέχει **χωρίς να απαιτείται ο επανυπολογισμός όλης της αλυσίδας.** Ο κώδικας μπορεί να τηρείται από ένα έμπιστο τρίτο μέρος ή να προστεθεί εξαρχής στο πρωτόκολλο. Δικλείδα ασφαλείας αποτελεί η απαίτηση να επιτευχθεί συναίνεση σε κάθε τροποποίηση, ακόμα και αν ένας κακόβουλος τρίτος προσπαθήσει να επεξεργαστεί ένα blockchain προς όφελός του. Η πρόταση, εκ πρώτης δεν μπορεί να εφαρμοστεί σε ήδη υπάρχοντα blockchains, αλλά η εταιρεία Accenture προτείνει μία εφαρμογή της που είναι σε θέση να «επεξεργάζεται, να ξαναγράψει ή να αφαιρεί προηγούμενα block πληροφοριών χωρίς να σπάσει την αλυσίδα». Αυτή η εφεύρεση **λειτουργεί μέσω μίας βελτιωμένης έκδοσης κατακερματισμού του 'χαμαιλέοντα'[28] που θεωρητικά επαναδημιουργεί αλγορίθμους μέσω της χρήσης ενός ασφαλούς ιδιωτικού κλειδιού**. Μετά την ενημέρωση του block, η αλυσίδα δεν θα επηρεαστεί και συνεπώς παραμένει σε λειτουργία, οπότε δεν υπάρχει καμία απαίτηση για επανυπολογισμό των επόμενων blocks ή για κάποια σκληρή διακλάδωση.

Η ιδέα πίσω από αυτό το 'επεξεργάσιμο' blockchain είναι η τοποθέτηση ενός εικονικού λουκέτου στην αλυσίδα που βρίσκεται ανάμεσα σε κάθε block, το οποίο θα μπορεί να

[28] ο υπογράφων μπορεί να δημιουργήσει την υπογραφή χαμαιλέοντα χωρίς να αλληλεπιδράσει με τον καθορισμένο παραλήπτη και ο τελευταίος θα μπορεί να επαληθεύσει την υπογραφή χωρίς να αλληλεπιδρά με τον υπογράφοντα.

‘ξεκλειδώσει’ με ένα κλειδί κατακερματισμού ‘χαμαιλέοντα’ ώστε να επιτραπεί η τροποποίηση ή διαγραφή δεδομένων. Εάν το block περιέχει προσωπικά δεδομένα που πρέπει να τροποποιηθούν, τότε μπορεί **να αντικατασταθεί με μια ενημερωμένη έκδοση χωρίς να χρειαστεί να σπάσει η αλυσίδα. Η αρχιτεκτονική αυτή επισημαίνει τα τροποποιημένα ή σβησμένα block με μια μόνιμη «ουλή» έτσι ώστε οι άλλοι συμμετέχοντες στην αλυσίδα να γνωρίζουν ότι τα δεδομένα τροποποιήθηκαν ή αφαιρέθηκαν.**



Εικόνα 50: Τροποποιήσιμο blockchain

δ) Η πρόταση για υπερσύγχρονη κρυπτογράφηση μπορεί να εξασφαλίσει ότι τα δεδομένα προστατεύονται σε μεγαλύτερο βαθμό, αλλά δεν θα υπάρχει πλέον η πολυπόθητη ανωνυμία. Για όσο διάστημα είναι διαθέσιμο το κλειδί ή τα αρχικά δεδομένα (ακόμη και στην περίπτωση ενός αξιόπιστου τρίτου, συμβατικά δεσμευμένου για την παροχή ασφαλούς υπηρεσίας φύλαξης), δεν εξαλείφεται πλήρως η δυνατότητα ταυτοποίησης του υποκειμένου δεδομένων. Μεγάλη σημασία έχει η ύπαρξη του κλειδιού, ακόμη και πίσω από τείχη προστασίας, και έτσι η καταστροφή τόσο των αρχικών δεδομένων όσο και του κλειδιού (δεδομένου ενός πλήρους κρυπτογραφημένου συνόλου δεδομένων) είναι αυτό που εξασφαλίζει τον υπεύθυνο.

9.4 Ηθικά ζητήματα

Το ηθικό πλαίσιο σε κάθε χώρα, αλλά και σε κάθε άνθρωπο ξεχωριστά, είναι διαφορετικό. Οι ηθικές ανοχές ποικίλλουν καθώς πολλοί είναι εκείνοι που επιθυμούν να είναι οι μοναδικοί υπεύθυνοι για τα ψηφιακά ιδιωτικά τους δεδομένα, τις συναλλαγές και τις πληρωμές που έχουν πραγματοποιήσει. Ο συγγραφέας **Τζέφφρεϊ Ροθφίντερ (Jeffrey Rothfeder) ισχυρίζεται (Βιβλίο Privacy for Sale) [1]** ότι αυτή η διαδεδομένη απόκτηση και ανταλλαγή δεδομένων μπορεί να οδηγήσει σε **αίσθημα αδυναμίας απέναντι στη διείσδυση της ιδιωτικής ζωής**. Επίσης συμπληρώνει, ίσως η αυξανόμενη συνάθροιση προσωπικών δεδομένων που τεκμηριώνουν τις λεπτομέρειες των φυσικών χαρακτηριστικών και των ελαττωμάτων, συμπεριφορών, επιθυμιών, συμπεριφορών, αποτυχιών και επιτευγμάτων μας, να δημιουργεί τελικά μια εικονική εκπροσώπηση (το λεγόμενο «ηλεκτρονικό άλγος»).

Πέρα από αυτό που αναλύθηκε διεξοδικά προηγουμένως, οφείλουμε να εξετάσουμε το ζήτημα και υπό ένα άλλο πρίσμα. **Κρίσιμο χαρακτηριστικό των ανθρώπινων σχέσεων είναι η εμπιστοσύνη**. Το ζητούμενο είναι πώς αυτή χτίζεται και συντηρείται ανάμεσα στους

ανθρώπους. Σε πρακτικό επίπεδο κάποιος που κρατάει τον λόγο του σε βάθος χρόνου και ο ρόλος του επαληθεύεται, θεωρείται ως ένας έμπιστος και αξιόλογος άνθρωπος. Στην περίπτωση τέλεσης ενός αδικήματος, ο αρμόδιος κρατικός φορέας είναι εκείνος που θα επικυρώσει το συμβάν και θα καθοδηγήσει το θύμα προκειμένου να δικαιωθεί. Λειτουργεί δηλαδή ως ένας "έμπιστος τρίτος φορέας" (trusted third party), όπως άλλωστε είναι ανέκαθεν και η τεχνολογία. Τα δε συμβόλαια πάσης φύσεως και κατ΄επέκταση τα έξυπνα συμβόλαια, **είναι κι αυτά "έγγραφα εμπιστοσύνης"** και λειτουργούν ως έγκυρες αποδείξεις Οι έξυπνες συμβάσεις αποθηκεύονται σε Η/Υ με τη διαδικασία και το περιεχόμενο των οποίων να καθορίζεται από τον κώδικα και όχι από τις παραδοσιακές γραπτές ρήτρες. Η Lex Machina [29] ένα πρόγραμμα Η/Υ για την εξόρυξη δεδομένων που δημιουργήθηκε στο Πανεπιστήμιο του Στάνφορντ το 2006, χρησιμοποιήθηκε στις ΗΠΑ ακόμη και για την αναζήτηση μοτίβων που βοηθούν στην πρόβλεψη της έκβασης των υποθέσεων. Στην ουσία δηλαδή **εμπιστευόμαστε έμμεσα τον τεχνικό που τα δημιούργησε μέσω αλγορίθμων, όμως αυτή η εμπιστοσύνη μεσολαβείται από την μηχανή.**

Η τεχνολογία μιας "αλυσίδας κουτιών" είναι βασισμένη σε ένα σκεπτικό, όπου θα υπάρχει απόλυτη εχεμύθεια. Για τον λόγο αυτό χαρακτηρίστηκε εξ αρχής ως μια επαναστατική αλλαγή στον τρόπο με τον οποίο πλέον γίνονται οι συναλλαγές, αφού επιδιώκει να «χτίσει» μια σχέση εμπιστοσύνης με τους χρήστες της

Με το blockchain ο φορέας που εγγυάται την γνησιότητα της αξίας, είναι η τεχνολογία. Υπάρχει η ομοφωνία από τους συμμετέχοντες ότι στις συγκεκριμένες συναλλαγές ο εκάστοτε αλγόριθμος είναι αυτός που εξασφαλίζει την εγκυρότητά τους. **Εδώ παρατηρούμε πως ένας εξορύκτης "παράγει" εμπιστοσύνη.** Η διαδικασία του υπολογισμού της τιμής μέσω της συνάρτησης hash υπήρχε και στο παρελθόν. Όπως υπήρχαν και τα "διαμοιρασμένα δίκτυα", η κρυπτογράφηση, ακόμα και οι "αλγόριθμοι ομοφωνίας". Ο συνδυασμός τους, με την ενσωμάτωση του στοιχείου της "απόδειξης της εργασίας" είναι που κάνει το blockchain "καινούργιο". Ο λόγος για τον οποίο αποκτά αξιοπιστία ο κάθε "εξορύκτης" είναι ότι παραγάγει αξία, την αξία που έχει η εμπιστοσύνη. **Μπορούν όμως οι μηχανές να παράξουν αξία;** Η πρώτη εφαρμογή του blockchain ήταν τα ψηφιακά νομίσματα. Η απόδειξη ότι δεν μπορείς να αγοράσεις κάτι επειδή ο λογαριασμός σου είναι άδειος, είναι μια μαθηματική διαδικασία που εύκολα υλοποιείται από έναν αλγόριθμο. Η διαδικασία που αποδεικνύει ότι είσαι παράνομος για κάτι όμως, υπερβαίνει τα μαθηματικά.

Αυτόνομοι, νοήμονες, λογισμικοί πράκτορες φιλτράρουν πληροφορίες στο διαδίκτυο, λειτουργούν μέσω αλγορίθμων και αναπτύσσουν διαδραστικότητα με το περιβάλλον τους. **Κι εδώ έγκειται η συνεργασία μηχανής και ανθρώπου. Ποια όμως είναι τα όρια ανάμεσα στον**

[29] Εταιρεία που παρέχει Legal Analytics σε νομικούς επαγγελματίες. Ξεκίνησε ως εταιρεία έρευνας διαφορών IP και τώρα είναι τμήμα της LexisNexis. Η εταιρεία ξεκίνησε ως έργο στο Πανεπιστήμιο του Στάνφορντ στη νομική σχολή και το τμήμα επιστήμης υπολογιστών του πανεπιστημίου πριν ξεκινήσει ως startup στο Menlo Park της Καλιφόρνια . Η Lex Machina παρέχει ένα προϊόν SaaS σε νομικούς επαγγελματίες για να τους βοηθήσει στην πρακτική, την έρευνα και τις επιχειρήσεις τους. Πηγή : https://en.wikipedia.org/wiki/Lex_Machina

άνθρωπο και τη μηχανή; Σε ποιο βαθμό η γνωστική διαδικασία που εκτελείται από τη μηχανή ανάγεται σε ανθρώπινη επιρροή; Ηλεκτρονική λοιπόν δήλωση βουλήσεως υπάρχει. Ο αλγόριθμος αναλαμβάνει άλλωστε τη σύναψη και την εκτέλεση της σύμβασης. Ο λογισμικός πράκτορας δεν επιδιώκει το ατομικό του συμφέρον αλλά την ικανοποίηση του ανθρώπου/χρήστη του.

Δεν είναι τα δεδομένα που προδιαγράφουν την απόφαση, αλλά η ανάλυσή τους από τον αλγόριθμο. Συνεπώς, ο νοήμων πράκτορας θα πρέπει να λογίζεται ως υποκείμενο δικαίου, με το Ευρωπαϊκό Κοινοβούλιο μάλιστα να κάνει λόγο για νομική προσωπικότητα που σημαίνει ότι μπορεί να διαθέτει και ικανότητα εκπροσώπησης. Στο βαθμό όμως που ο πράκτορας είναι απλά πρόγραμμα και μηχανή χωρίς ιδία βούληση, δεν μπορεί να νοείται ως αντιπρόσωπος. **Πως όμως η δικαιοπρακτική βούληση μπορεί να προ-εγγραφεί στον κώδικα του αλγορίθμου έτσι ώστε ο νοήμων πράκτορας να προσαρμόζεται, να μαθαίνει, να αποφασίζει και να εκφράζει αυτόνομη κρίση.**

Συνεπώς τι θα γίνει όταν προκύψει :

1. **Το ενδεχόμενο η αυτονομία μιας τέτοιας τεχνολογίας να εξελιχθεί σε τέτοιο βαθμό, ώστε πίσω από τη δράση του πράκτορα να μην υφίσταται χρήστης ;**
2. **Επειδή τα συστήματα αυτό- πολλαπλασιάζονται σε μη- διακριτά αντίγραφα, με σκοπό να κατανείμουν την εκτέλεση των λειτουργιών μεταξύ τους, να μην μπορεί κανείς να βρει τον υπεύθυνο – δράστη για να καταλογισθούν οι ευθύνες ;**
3. **Ποια ενδεχομένως θα είναι η νομική ευθύνη για "ζημιές" που προκάλεσε κάποιο μηχάνημα; Ποιο είναι το εύρος της αυτονομίας τους ;**

Ποιες οι συνέπειες μιας τεχνολογίας **blockchain** σε έναν χώρο όπου πρωταρχική σημασία έχουν τα νομικά δικαιώματα, η αίσθηση της δικαιοσύνης καθώς και η ανθρώπινη αλληλεπίδραση και καθοδήγηση ;

Όλα τα παραπάνω βρίσκονται σε εξέλιξη και ερευνώνται.

Κεφάλαιο 10ο – Προτεινόμενη λύση για την ταχύτερη επεξεργασία των συναλλαγών

10.1 Κατευθυνόμενοι άκυκλοι γράφοι

Αναμφισβήτητα η τεχνολογία blockchain αποτελεί την λύση σε αρκετούς γρίφους, που «βασάνιζαν» τους δημιουργούς διαφόρων εφαρμογών του ψηφιακού κόσμου. Έχει σαφή υπεροχή ως μια τεχνολογία του μέλλοντος. Σε πρακτικό όμως επίπεδο, δεν θα μπορούσε κάποιος να παραβλέψει τις αστοχίες που παρουσιάζονται κατά την ρεαλιστική εφαρμογή της. Μία εξ' αυτών είναι ο μεγάλος αριθμό χρηστών που οφείλει να εξυπηρετήσει.

Ειδικότερα: Τα προβλήματα κλιμάκωσης είναι κάτι παραπάνω από εμφανή, αφού χρησιμοποιούνται συγκεκριμένοι αλγόριθμοι συναίνεσης, όπως αναφέρθηκε και σε προηγούμενα κεφάλαια. Το πρόβλημα κυρίως εντοπίζεται στην επεξεργασία των συναλλαγών, δεδομένου του ότι κάθε πλήρης κόμβος πρέπει να επεξεργάζεται αυτοτελώς την κάθε συναλλαγή, ως απόρροια της λεγόμενης αποκεντρωμένης δομής της συγκεκριμένης τεχνολογίας. Ο κάθε κόμβος στο δίκτυο αποθηκεύει ένα πλήρες αντίγραφο της συνολικής κατάστασης του δικτύου, δρώντας ως μια ασφαλιστική δικλείδα, ως ένας ανώνυμος μηχανισμός συναίνεσης ναι μεν, αλλά επιβραδύνοντας την ταχύτητα των εκάστοτε συναλλαγών, καθώς και τον όγκο των επεξεργάσιμων ή προς αποθήκευση δεδομένων.

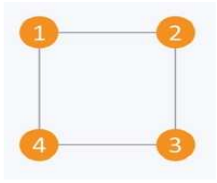
Πρακτικά αυτό σημαίνει ότι η αλλοίωση της ταυτότητας του μπλοκ δύναται να δημιουργήσει σοβαρά προβλήματα, αφού με μόνη την αφαίρεση ενός μπλοκ από αυτά, η σειρά της αλυσίδας δεν θα επιβεβαιωθεί και η επιθυμητή αλληλουχία μεταξύ των μπλοκ, δεν θα υφίσταται. Θα πρέπει να γίνει επανυπολογισμός των ταυτοτήτων των μπλοκ ολόκληρης της αλυσίδας, μέχρι να επιτευχθεί η σωστή αλληλουχία. Μια διαδικασία που είναι εξαιρετικά δύσκολη, χρονοβόρα και κοστοβόρα, σχεδόν αδύνατη. *Σε περίπτωση όμως που αυτό επιτευχθεί, θα πρέπει επιπροσθέτως να γίνει ενημέρωση όλων των κόμβων που διαμοιράζουν τη λίστα με τις συναλλαγές αλλά και ψηφιακή πιστοποίηση των συναλλαγών από όλα τα μέρη* [30].

Το αρχιτεκτονικό μοντέλο των κατευθυνόμενων άκυκλων γραφημάτων, στο οποίο δεν υπάρχουν διαδρομές που αρχίζουν και τελειώνουν στον ίδιο κόμβο, αποτελεί την μελλοντική εξέλιξη της τεχνολογίας αυτής, προκειμένου να αντιμετωπιστούν τέτοιου είδους προβλήματα.

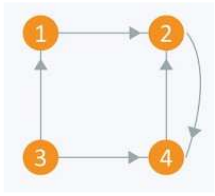
Πριν αναλύσουμε το συγκεκριμένο μοντέλο, πρέπει πρωτίστως να αναφερθούν και κάποιοι σχετικοί ορισμοί.

[30] https://blog.farmacon.gr/katigories/texniki-arthrografia/georgia-akriveias/item/2303-ti-einai-i-texnologia-blockchain-pithanes-efarmoges-sti-georgia

- **Ένας γράφος** είναι μια δομή που αποτελείται από ένα σύνολο κορυφών ή κόμβων (nodes) και ένα σύνολο ακμών (edges) μεταξύ των κορυφών



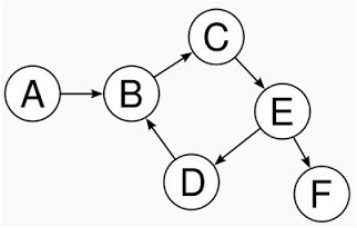
- **Μη-Κατευθυνόμενος Γράφος** (undirected): Μη-κατευθυνόμενος γράφος σημαίνει ότι οι ακμές του μπορεί να γραφτούν με διαφορετική σειρά. Π.χ. η ακμή (1,2) μπορεί να γραφτεί και ως (2,1).



- **Κατευθυνόμενος Γράφος** (directed): Κατευθυνόμενος γράφος σημαίνει ότι οι ακμές του δεν μπορεί να γραφτούν με διαφορετική σειρά. Π.χ. η ακμή (1,2) δεν μπορεί να γραφτεί σαν (2,1). Δηλαδή, κάθε μια από τις ακμές του είναι προσανατολισμένη προς μία κατεύθυνση.

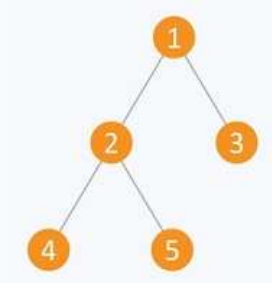
  Ο κατευθυνόμενος γράφος με 4 κορυφές (1, 2, 3, 4) στο σχήμα, μας δείχνει ότι για να μεταβούμε από την κορυφή 1 στην κορυφή 4 δεν υπάρχει απευθείας ακμή, αφού πρέπει πρώτα να περάσουμε από την 2. Η ακολουθία των ακμών από τις οποίες περνάμε για να φτάσουμε στον τελικό προορισμό, λέγεται μονοπάτι (path). Το μονοπάτι από την κορυφή 1 στην κορυφή 4 συμβολίζεται με 1->2->4 και έχει μήκος 2 αφού αποτελείται από 2 ακμές. Δηλαδή, το μήκος ενός μονοπατιού είναι το πλήθος των ακμών του μονοπατιού.

- **Κύκλος (cycle):** Κύκλος σε ένα γράφο ονομάζεται μια διαδρομή που ξεκινά από ένα κόμβο και καταλήγει στον ίδιο κόμβο.
- Ένας γράφος που δεν περιέχει κύκλους ονομάζεται **άκυκλος (acyclic)**



- **Δέντρο (Tree)**

  Ένας γράφος στον οποίο υπάρχει μονοπάτι μεταξύ δυο οποιωνδήποτε κορυφών, και δεν περιέχει κυκλικές διαδρομές, λέγεται δέντρο. Αναφερόμαστε στα στοιχεία του δέντρου ως κόμβους. Κάθε κόμβος συνδέεται με έναν ή περισσότερους κόμβους στους οποίους αναφερόμαστε, ως παιδιά του ή απογόνους του. Οι κόμβοι που δεν έχουν απογόνους και βρίσκονται στο τελευταίο επίπεδο λέγονται φύλλα του δέντρου. Κάθε κόμβος έχει ακριβώς έναν πρόγονο, εκτός από τη ρίζα, που βρίσκεται συνήθως στην κορυφή του δέντρου.



  Πως λειτουργεί λοιπόν ; Ποια βήματα ακολουθούνται ;

  Κι εδώ ο κανόνας της χρονικής προτεραιότητας [31] είναι ισχυρός και δεν αλλάζει. Διότι θέλουμε να ορίσουμε ένα σύνολο εργασιών οι οποίες θα εκτελούνται με συγκεκριμένη σειρά από έναν επεξεργαστή αλλά με το

[31] Συσχέτιση με νομική ορολογία. Ο κανόνας αφορά τα περιορισμένα εμπράγματα δικαιώματα και σύμφωνα με αυτόν σε περίπτωση συρροής περισσότερων τέτοιων δικαιωμάτων σε πράγμα ή δικαίωμα προτιμάται εκείνο που η σύστασή του προηγείται χρονικά, κανόνας που αποδίδεται με τη λατινική φράση prior tempore potior jure. Εκ την ερμηνείας του άρθρου 973 ΑΚ

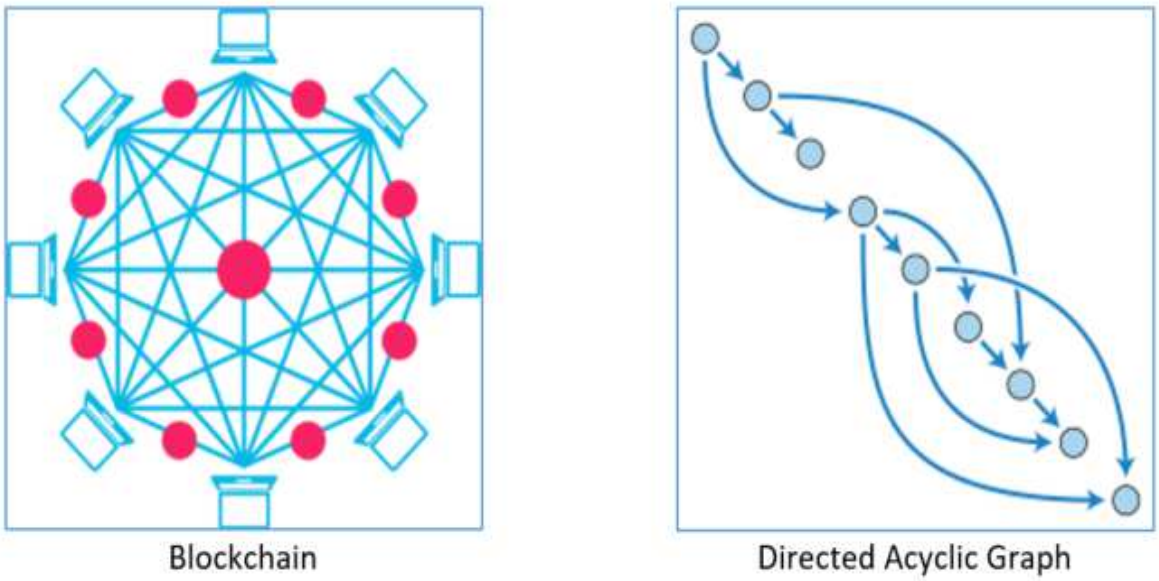
συντομότερο δυνατό τρόπο. Το πρόβλημα λοιπόν αναπαρίσταται σε έναν κατευθυνόμενο γράφο ως εξής :

- Οι κορυφές του γράφου αντιστοιχούν σε κάθε μια από τις εργασίες, και
- η ύπαρξη ακμής από την κορυφή Α στην κορυφή Β δηλώνει ότι η εργασία Α πρέπει να εκτελεστεί πριν από τη Β.

Η χρήση της λεγόμενης τοπολογικής ταξινόμησης[32], θα συνέβαλε σημαντικά στην εξάλειψη του προβλήματος. Διότι σε μια τέτοια δομή, τα μπλοκ δεν είναι αυστηρά ταξινομημένα το ένα μετά το άλλο όπως σε ένα κλασικό blockchain, αλλά το κάθε μπλοκ μπορεί να επικυρώσει πολλά άλλα μπλοκ και συναλλαγές. Συνέπεια των προαναφερθέντων αποτελούν τα κατωτέρω :

1. Αρχικά προδιορίζονται οι πατρικές συναλλαγές από το σύστημα
2. Κατόπιν προστίθενται οι επόμενες συναλλαγές υπογράφοντας ψηφιακά το hash. Το κάθε μπλοκ διασυνδέεται πίσω από 2 προγενέστερα μπλοκ, τα οποία έχουν εξεταστεί για την εγκυρότητά τους με κάποιον αλγόριθμο συναίνεσης και τέλος
3. Δημιουργείται ένα δέντρο από συναλλαγές στο οποίο κάθε συναλλαγή θεωρείται επικυρωμένη και αμετάβλητη. Αναπτύσσονται δηλαδή πολλά παράλληλα επικυρωμένα μπλοκ.

10.1.1 *Συνδυασμός blockchain και κατευθυνόμενων ακυκλικών γραφημάτων*

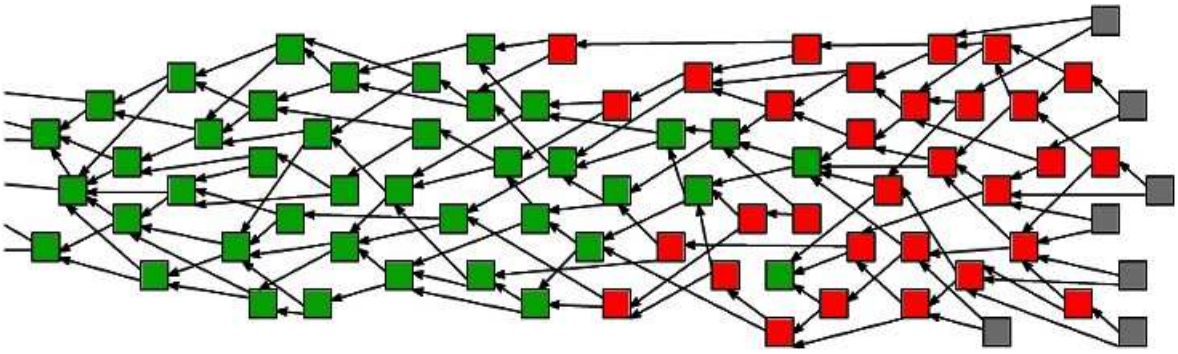


Εικόνα 51: Αναπαράσταση τεχνολογίας blockchain και κατευθυνόμενου ακυκλικού γράφου

[32] όπου η ανάπτυξή του να μπορεί να προχωρήσει μόνο προς τη μία κατεύθυνση - από τα πρώτα μπλοκ προς τα επόμενα

Συμπερασματικά, τα κατευθυνόμενα άκυκλα γραφήματα βασίζονται στην **ιδέα των παράλληλων αλυσίδων μπλοκ,** όπου στο καθένα εκτελούνται διαφορετικοί τύποι συναλλαγών την ίδια χρονική στιγμή. Αυτό σημαίνει ότι λαμβάνονται ταυτόχρονα πολλά hashes προς επιλογή από τους πολλούς χρήστες του. Η ταχύτητα της συναλλαγής που επιστρέφει στο δίκτυο βασίζεται στο πλήθος των συναλλαγών που την συνοδεύουν, γεγονός που καθιστά τη συναλλαγή πιο ασφαλή. Όταν μια συναλλαγή επικυρωθεί, συσχετίζεται με μια παρόμοια υπάρχουσα συναλλαγή εντός του δικτύου blockchain του κατευθυνόμενου άκυκλου γραφήματος, γεγονός που σημαίνει ότι οι συναλλαγές είναι σχεδόν στιγμιαίες. Η συγκεκριμένη δομή που δεν επιτρέπει τους αποκλεισμούς, καθιστά τη διαδικασία ταχύτερη, απαιτώντας σαφώς λιγότερους διαθέσιμους πόρους σε σύγκριση με τα μπλοκ αλυσίδων που βασίζονται στο μοντέλο Proof-of-Work ή άλλα παρόμοια μοντέλα συναίνεσης, εξαλείφοντας την έννοια της εξόρυξης, αφού η επιβεβαίωση πραγματοποιείται σε ελάχιστο χρόνο (βλ. εικόνα 52) [33]

Τα κατευθυνόμενα άκυκλα γραφήματα λοιπόν χρησιμοποιούνται σε περιπτώσεις, όπου η ταχύτητα των συναλλαγών είναι εξαιρετικά σημαντική, όπως είναι οι μεταγλωττιστές, η τεχνητή νοημοσύνη, οι διάφορες στατιστικές μέθοδοι καθώς και η μηχανική μάθηση. Δύο από τις κύριες υλοποιήσεις του είναι οι Hashgraph και Tangle.



Εικόνα 52: Κατευθυνόμενος ακυκλικός γράφος (DAG)

[33] Το block θεωρείται επιβεβαιωμένο (στην εικόνα με πράσινο), όταν μπορεί να προσπελαστεί από οποιοδήποτε ανεπιβεβαίωτο (με γκρι).

Επίλογος

Η τεχνολογία blockchain συγκαταλέγεται ανάμεσα στις τεχνολογίες αιχμής και θα απασχολήσει σημαντικά την παγκόσμια κοινότητα πληροφορικής, κυρίως τα επόμενα χρόνια, αφού δημιούργησε μια νέα γενιά εφαρμογών με πρωτοποριακά χαρακτηριστικά. Η αξιοποίησή της επιβάλλεται ειδικά σε τομείς της οικονομίας, που έχουν ως πρωταρχικό στόχο την εμπιστοσύνη και ην ασφάλεια. Η τεχνολογία blockchain που βασίζεται στα κατανεμημένα καθολικά, προτάσσει εμμέσως νέους τρόπους συνεργασίας.

Ριζικές αναθεωρήσεις πεπαλαιωμένων πεποιθήσεων και ένα πιο ευέλικτο σχήμα των διαδικασιών των διοικητικών μοντέλων του δημοσίου, μπορούν να καθορίσουν ένα ευοίωνο μέλλον. Η Πολιτεία οφείλει να υιοθετήσει τη χρήση των έξυπνων συμβολαίων από τους Δημόσιους Φορείς, να αναγνωρίσει την χρηστικότητάς τους και κατ' επέκταση να θεσμοθετήσει τον ρόλο τους, αξιοποιώντας το είδος αλληλεξάρτησης που αυτές εμφανίζουν, με την τεχνολογία blockchain. Η νομική επιστήμη πρέπει να σταθεί ως αρωγός, οριοθετώντας συγκεκριμένους κανόνες, οι οποίοι θα μεταφραστούν με τεχνικούς όρους και θα ενσωματωθούν, για την ορθή λειτουργία και εκτέλεση τους.

Με αυτή την αφορμή, οι δημόσιοι οργανισμοί θα επενδύουν στην τεχνολογία blockchain, έχοντας την καθοδήγηση της Πολιτείας, η οποία με εξειδικευμένη στόχευση, θα έχει πλέον προσαρμόσει το δίκαιο στα νέα δεδομένα. Ίσως μόνο τότε γίνει απόλυτα αντιληπτό ότι οι Δημόσιοι Φορείς θα έχουν ουσιαστικά αποκτήσει το ανταγωνιστικό πλεονέκτημα.

Σύνοψη και συμπεράσματα

Στο κεφάλαιο αυτό συνοψίζεται η έρευνα που έγινε σχετικά με τις τεχνολογίες του blockchain στον δημόσιο τομέα. Διατυπώνονται τα συμπεράσματα, οι προβληματισμοί και οι περιορισμοί της έρευνας. Τέλος, προτείνονται κάποιες μελλοντικές επεκτάσεις της.

Η σύγχρονη τεχνολογία λειτουργεί σε ένα συνδεδεμένο περιβάλλον εντός του οποίου ανταλλάσσονται πολλαπλά και ετερογενή δεδομένα. Μέσω της τεχνολογίας Blockchain επιτυγχάνεται η ανταλλαγή αξιόπιστων πληροφοριών ανάμεσα σε μια κοινότητα. Η όλη διαδικασία περιλαμβάνει τον καθολικό συντονισμό όλων των ενεργειών των συμμετεχόντων στο δίκτυο, ενώ δεν υπάρχει εξάρτηση από την εξουσία μια μεμονωμένης οντότητας. Αυτό που εμφανώς προκύπτει από τα προαναφερθέντα είναι ότι η blockchain τεχνολογία διαθέτει όλες τις δυνατότητες, για να καθιερώσει ένα είδος καινοτομίας, που θα μετεξελίξει τα επιχειρηματικά μοντέλα των υπηρεσιών, τροποποιώντας σημαντικά τις υφιστάμενες διαδικασίες.

Η ηλεκτρονική διακυβέρνηση δεν στοχεύει μόνο στην προσφορά δημόσιων υπηρεσιών στο διαδίκτυο για πολίτες και επιχειρήσεις αλλά και στην εξοικονόμηση χρόνου και κόστους με τη χρήση διαδικτυακών καναλιών, που θα καταστήσουν ποιοτικές τις υπηρεσίες που προσφέρουν. Ο ψηφιακός μετασχηματισμός της Δημόσιας Διοίκησης θα ενισχύει την εμπιστοσύνη στις κυβερνήσεις, θα αυξήσει τη διαφάνεια, την αποτελεσματικότητα, την αξιοπιστία και την ακεραιότητα της δημόσιας διακυβέρνησης. Καθοριστικός ο ρόλος της τεχνολογίας blockchain.

Βασικά στοιχεία του Blockchain αποτελούν τα έξυπνα συμβόλαια (smart contracts), το αρχείο καταγραφής συναλλαγών (ledger) και οι αλγόριθμοι συναίνεσης (consensus algorithms). Τα smart contracts είναι εκείνα που καθορίζουν τους ρόλους και τα όρια των χρηστών, μια απολύτως διάφανη διαδικασία, που προλογίζει σχέσεις συνεργασίας και εμπιστοσύνης για τον διαμοιρασμό της πληροφορίας μεταξύ τους. Συνεπώς, γραφειοκρατικές και λογιστικές διαδικασίες στο μέλλον μπορούν να αντικατασταθούν από την τεχνολογία μέχρι εκείνο τον βαθμό που αυτό είναι επιτρεπτό.

Όλοι γνωρίζουμε ότι οι παραδοσιακές δημόσιες συμβάσεις έχουν συνήθως τη μορφή ιδιωτικών γραπτών κειμένων, με σαφείς και συγκεκριμένους όρους, που έχουν συμφωνηθεί αμφιμερώς. Αυτό που προβληματίζει έντονα τον νομικό κόσμο έχει να κάνει με την αυτό - εκτελεστότητα των έξυπνων συμβάσεων. Πιο συγκεκριμένα οι νομικοί αναλογίζονται το εξής : Τελικά τα μέρη δεσμεύονται σύμφωνα με την βούλησή τους; Πως γνωρίζουν ότι η σύμβαση αντικατοπτρίζει τις προθέσεις τους αν δεν μπορούν να τις διαβάσουν ; Οι όροι μιας σύμβασης μπορούν να εκτιμηθούν καθοριστικά από ένα πρόγραμμα υπολογιστή ; Μήπως υποβαθμίζουν την εξουσία του νόμου; Ποια διαδικασία θα εφαρμοσθεί για διόρθωση ενός έξυπνου συμβολαίου σε περίπτωση αθέτησης από οποιοδήποτε μέρος ;

Σε τεχνικό επίπεδο, τα μέρη εδώ δεν είναι άτομα, αλλά κρυπτογραφημένα ιδιωτικά κλειδιά. Το ιδιωτικό κλειδί θεωρείται ότι αντιπροσωπεύει το άτομο με βάση μια μαθηματική σχέση με το σχετικό δημόσιο κλειδί, Αξιοσημείωτο είναι ότι δεν έχει ακόμη επέλθει νομική αναγνώριση ως προς αυτό, όπως συμβαίνει με τα ψηφιακά πιστοποιητικά που διαθέτουν ψηφιακή υπογραφή, η οποία ισοδυναμεί με την χειρόγραφη υπογραφή του συντάκτη τους, ως ορίζεται σχετικά μετά από νομοθετική παρέμβαση.

Εξετάστηκαν πολλές διαφορετικές τεχνολογίες υλοποίησης blockchain, ώστε να βρεθεί η πιο κατάλληλη, για την ασφαλή, αξιόπιστη, γρήγορη, αποδοτική και διάφανη ροή πληροφοριών για την δημόσια διοίκηση. Τελικά, αξιολογήθηκε και επιλέχθηκε η αποκεντρωμένη υβριδική πλατφόρμα του Hyperledger Fabric. Κομβικό ρόλο για την επιλογή της ήταν μια σειρά από χαρακτηριστικά που υπερτερούσαν από τις υπόλοιπες. Το Hyperledger δεν αποτελεί μια αποκλειστικά νομισματική εφαρμογή , όπως είναι το Bitcoin αλλά δημιουργήθηκε για την ανάπτυξη βιομηχανικών εφαρμογών τεχνολογίας blockchain. Εφόσον λοιπόν ένας δημόσιος φορέας καταγράψει βήμα - βήμα και προτυποποίησει τις επιχειρησιακές του διαδικασίες, το

Hyperledger θα αποτελέσει την ιδανική λύση, με δικαιώματα χρηστών και φιλικό περιβάλλον ανάπτυξης. Σε ένα τέτοιο δίκτυο η καταγραφή των συναλλαγών είναι ασφαλής, αφού καταγράφονται μόνιμα στο καθολικό βιβλίο και οι πληροφορίες διαμοιράζονται, μόνο σε συγκεκριμένα εξουσιοδοτούμενα στον κόμβο, άτομα, γεγονός που οφείλεται στην σχεδιασμένη αρχιτεκτονική λύσης της. Με αυτόν τον τρόπο διατίθεται όλη η ιστορικότητα των κινήσεων διότι αφήνει πάντοτε το αποτύπωμά του. Είναι η πιο δημοφιλής υλοποίηση σε permissioned blockchain, καθώς επίσης χρησιμοποιεί προϋπάρχοντα συστήματα, όπως web υπηρεσίες (api services)[34] με αποτέλεσμα τον αυτοματισμό της συλλογής των πληροφοριών. Από την άλλη μεριά, ο διαμοιρασμό της πληροφορίας και συγκεκριμένα οι όροι και οι προϋποθέσεις του συμβολαίου είναι ορατές μόνο για τον κάθε συμμετέχοντα κρίκο, γεγονός που εκμηδενίζει την αμφισβήτηση και ενισχύει την εμπιστοσύνη. Μια ολοκληρωμένη τελική πληροφορία είναι το αποτέλεσμα της σύνθεσης τμημάτων αδιάβλητης πληροφόρησης του κάθε επιμέρους σταδίου.

Σε ότι έχει να κάνει με τα μειονεκτήματά της τεχνολογίας blockchain γενικά, εντοπίστηκε μία πτυχή που πρέπει να ληφθεί σοβαρά υπόψη. Ένα εύλογο ερώτημα είναι ποια δεδομένα θα αποθηκεύονται στο blockchain, εφόσον διατηρούνται και αντιγράφονται τα σε όλα τα κατανεμημένα αντίγραφα του καθολικού του, ιδιαίτερα μετά την θέσπιση και θέση σε ισχύ του ΓΚΠΔ. Μία προτεινόμενη λύση είναι κάποια ευαίσθητα δεδομένα να αποθηκεύονται στις εξωτερικές ΒΔ των οργανισμών και μόνο με την κρυπτογραφική τους σύνοψη στο blockchain. Τον ρόλο αυτό θα μπορούσαν να αναλάβουν ένας υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, με υποχρεωτικό ορισμό τους από τον Οργανισμό. Από τη μια πλευρά, blockchain πλατφόρμες όπως το Enigma[35] **[9]** ανταποκρίνονται πολύ κατάλληλα στο θέμα των χρηστών της ιδιωτικότητας και μπορεί αισιοδοξώς να υλοποιηθεί ως βέλτιστη πρακτική στον κλάδο. Σε ότι αφορά την τροποποίηση κάποιας σύμβασης, η ενσωμάτωση της τροποποίησης σε ένα ξεχωριστό στο έξυπνο συμβόλαιο με τη μορφή της προσθήκης στο 1ο τύπου αποτελεί μια πιθανή επιλογή.

Έχουμε αφιερώσει ξεχωριστό κεφάλαιο για το ευρωπαϊκό κοινοβούλιο το οποίο έχει ψηφίσει σχετικές δράσεις και προτείνει την υιοθέτηση της τεχνολογίας blockchain στα Κράτη μέλη της, προωθώντας την έρευνα και την ανάπτυξη της τεχνολογίας σε διάφορους τομείς. Τα έργα blockchain που βρίσκονται σε εξέλιξη διεθνώς, αποτυπώνουν την ανοδική τάση της εν λόγω τεχνολογίας τα τελευταία χρόνια, ανοικτό και προσπελάσιμο από όλους και ταυτόχρονα ασφαλές και χρήσιμο για όλους τους εμπλεκόμενους στηρίζεται στην υιοθέτηση κοινών προτύπων δια λειτουργικότητας και εφαρμογής αποτελεσματικών πανευρωπαϊκών υπηρεσιών ΗΔ με κέντρο τον πολίτη. Στην Ελλάδα, η ηλεκτρονική διακυβέρνηση φιλοδοξεί να μετασχηματίσει τον ρόλο, που

[34] Μια διεπαφή προγραμματισμού εφαρμογών (API) είναι μια σύνδεση μεταξύ υπολογιστών ή μεταξύ προγραμμάτων υπολογιστή. Πηγή : https://en.wikipedia.org/wiki/API

[35] Ο Guy Zyskind, ο Oz Nathan και ο Alex Sandy Pentland ανέπτυξαν μία πλατφόρμα που ονομάζεται Enigma, ένα δίκτυο peer-to-peer το οποίο βασίζεται σε ένα αποκεντρωμένο σύστημα διαχείρισης των προσωπικών δεδομένων, που επιτρέπει σε διαφορετικά συμβαλλόμενα μέρη την από κοινού την αποθήκευση και τον υπολογισμό των δεδομένων, διατηρώντας παράλληλα τα δεδομένα εντελώς ιδιωτικά

διαδραματίζει η τεχνολογία στο χώρο της δημόσιας διοίκησης. Να μην χρησιμοποιείται πλέον ως υποστηρικτικός μηχανισμός για τη μηχανοργάνωση, αλλά να ανασχεδιασθούν συθέμελα οι διαδικασίες. Οι οργανωσιακές αλλαγές που προέρχονται από το νέο δημόσιο management[36] αποτελούν απαραίτητη προϋπόθεση ώστε να δημιουργηθεί ένα νέο μοντέλο διοίκησης εξ΄ ολοκλήρου βασιζόμενο στην ηλεκτρονική διακυβέρνηση. Προαπαιτούμενο είναι η σχετική τεχνογνωσία για την υλοποίηση τέτοιων έργων. Καταλήγουμε ότι η Πολιτεία οφείλει να θεσπίσει το κατάλληλο κανονιστικό και ρυθμιστικό πλαίσιο, που θα εξαλείψει τους νομικούς προβληματισμούς, που ανακύπτουν και επιζητούν επίλυση.

Όρια και περιορισμοί της έρευνας

Στο παρόν κεφάλαιο γίνεται μια σύντομη ανάλυση στα όρια και στους περιορισμούς που αντιμετωπίστηκαν κατά την έρευνα γι' αυτήν την εργασία. Μία καινοτόμος λύση σε επίπεδο πληροφορικής στον Δημόσιο τομέα, για να μπορεί να είναι εφαρμόσιμη, θα πρέπει οι εμπλεκόμενοι υπάλληλοι που θα απασχοληθούν να είναι πλήρως καταρτισμένοι, ενώ σημαντικός παράγοντας είναι μια πλήρης και σαφής απεικόνιση των επιχειρησιακών λειτουργιών ενός Οργανισμού. Ως μια νέα και ραγδαία αναπτυσσόμενη τεχνολογία η οποία έχει προκαλέσει ιδιαίτερο ενδιαφέρον στην επιστημονική κοινότητα, το blockchain και συγκεκριμένα για το Hyperledger, το οποίο επιλέξαμε για την ανάπτυξη του προτεινόμενου σεναρίου μας, εντοπίστηκαν πολλές ασαφείς αναφορές που καθιστούν κάποιες πληροφορίες αναξιόπιστες. Δεν υπάρχει ακόμα έγκυρη και ολοκληρωμένη βιβλιογραφία που να κεντρίσει το ενδιαφέρον των προγραμματιστών που ασχολούνται με τον κλάδο των αποκεντρωμένων εφαρμογών να επενδύσουν στην ανάπτυξη τέτοιου είδους εφαρμογών.

Παρόλο που εφαρμόζεται πλέον σε αρκετούς τομείς, δεν έχει διαδοθεί εκτενώς η υπεροχή της σε σχέση με τις υπάρχουσες τεχνολογίες. Σπάνια δημοσιεύονται τα αποτελέσματά της από εταιρείες που χρηματοδοτούν τέτοιου είδους εφαρμογές, καθόσον κερδοσκοπικά συμφέροντα ματαιώνουν μια τέτοια πρωτοβουλία, ενώ ανύπαρκτα είναι τα άρθρα που αναλύουν την αποτελεσματικότητα από την σκοπιά ενός προγραμματιστή και όχι ενός χρήστη. Το Bitcoin είναι η δημοφιλέστερη πλατφόρμα αυτού του είδους και έχει μονοπωλήσει σημαντικά το ενδιαφέρον σε σύγκριση με τις υπόλοιπες εφαρμογές τεχνολογίας blockchain. Δεν υπάρχει ακόμη σχετική νομοθεσία που να επιτρέπει σε επιχειρήσεις και οργανισμούς να υλοποιούν εφαρμογές blockchain, ενώ οι υλοποιήσεις τους μέχρι τώρα βρίσκεται σε πειραματικό στάδιο και δεν έχουν ακόμα συνταχθεί οι βέλτιστες πρακτικές για την υιοθέτησή τους.

[36] Το **Νέο Δημόσιο Μάνατζμεντ** πρόκειται για μία νέα προσέγγιση διοίκησης δημόσιων φορέων και οργανισμών, η οποία χρησιμοποιεί μεθόδους μάνατζμεντ από τον ιδιωτικό τομέα για να βελτιώσει την αποτελεσματικότητα της λειτουργίας του δημόσιου τομέα. Όπως ο ιδιωτικός τομέας εστιάζει κυρίως στην εξυπηρέτηση του πελάτη, έτσι και το Νέο Δημόσιο Μάνατζμεντ επικεντρώνεται στην επίτευξη της ικανοποίησης του πολίτη, που είναι ο τελικός αποδέκτης των υπηρεσιών του δημόσιου τομέα. Πηγή : https://el.wikipedia.org/wiki/

Μελλοντικές Επεκτάσεις

Μετά από την καταγραφή της υφιστάμενης κατάστασης σε θέματα ψηφιακού μετασχηματισμού, αναλύοντας τις αδυναμίες, τις αναγκαίες προσαρμογές και τις προκλήσεις που θα υπάρξουν, διαπιστώθηκε ότι τα όρια επέκτασης μιας τεχνολογίας τέτοιας εμβέλειας εξαρτώνται σημαντικά από τον βαθμό υιοθέτησής τους από κρατικούς φορείς, κεντρικές αρχές και κυβερνήσεις, αλλά κυρίως από την υποστήριξη των πολιτών και την προθυμία τους να συμμετέχουν και να ανταπεξέλθουν, παρόλες τις δυσκολίες που ενδεχομένως θα αντιμετωπίσουν, στα νέα δεδομένα. Η παρούσα εργασία με μια ανασκόπηση των δυνατοτήτων που τα δίκτυα blockchain υπόσχονται να προσφέρουν, ευελπιστούμε να αποτελέσει έναν οδηγό για την βελτίωση της αποδοτικότητας των φορέων του Δημοσίου, εφόσον επιλέξουν να εκμεταλλευτούν τα πλεονεκτήματά της. Η τεχνολογία blockchain προσφέρει συνεχώς νέες προοπτικές. Με αφορμή την εν λόγω διπλωματική εργασία, παρατίθενται προτάσεις για μελλοντική έρευνα και την ενδεχόμενη δημιουργία μιας πιλοτικής εφαρμογής, ώστε να διερευνηθούν περαιτέρω οι προοπτικές υιοθέτησης μιας τέτοιας τεχνολογίας.

- **Κατανεμημένη δικαιοδοσία αποκεντρωμένης διακυβέρνησης**

Η απουσία νομικής υποδομής με σημείο αναφοράς τις συναλλαγές κρυπτογράφησης αποτελεί τροχοπέδη και το Κράτος οφείλει να μεριμνήσει σε αυτό. Τα επιμέρους χαρακτηριστικά των τεχνολογιών που βασίζονται σε υποδομή blockchain, όπως η ανωνυμία, η ψευδωνυμία, η αυτόματη εκτέλεση κλπ. δεν δύναται να αποτελέσουν νομική βάση σύμφωνα με την ισχύουσα νομοθεσία **[9].** Αυτό σημαίνει ότι δεν μπορεί να εφαρμοσθεί σε κώδικα μια παραδοσιακή έκβαση επίλυσης διαφορών, παρά μόνο εάν συνταχθούν ρήτρες επίλυσης. Συνεπώς θα πρέπει να εξεταστούν τέτοια θέματα εξαρχής από τους νομοθέτες και να δημιουργηθεί ένα νέο ρυθμιστικό καθεστώς.

Το γεγονός αυτό ενδεχομένως να αποτελέσει την επόμενη θεσμική καινοτομία, λαμβάνοντας υπόψη ότι οι νέοι τύποι νομικών διαφορών θα μπορούσαν να είναι ακόμη και διασυνοριακοί με αποτέλεσμα να υπόκεινται σε πολλές δικαιοδοσίες. Μια αναπτυσσόμενη διαδικτυακή υπηρεσία λοιπόν, την οποία θα ονομάσουμε ως κατανεμημένη δικαιοδοσία, θα είναι το επόμενο είδος αποκεντρωμένης διακυβέρνησης βασισμένο σε τεχνολογία blockchain.

Έχει ήδη αναπτυχθεί η ενσωμάτωση ενός μηχανισμού επίλυσης διαφορών στο ίδιο το έξυπνο συμβόλαιο, που οδηγεί στην επιβολή αποφάσεων μέσω κώδικα (Mattereum),[37] **[9]** καθώς και η μέθοδος της λογικής του χρησμού μέσω της πλατφόρμας LTO[38] **[9].** Υπάρχει μια αποκεντρωμένη υπηρεσία ψηφιακής διαμεσολάβησης, η λεγόμενη «επιτροπή κριτών», με επικεφαλής έναν δικαστή ή έναν διαιτητή από μια ομάδα εμπειρογνωμόνων. Όταν ανακύπτει διαφορά, οι δυνητικοί ένορκοι ή δικαστές επιλέγονται τυχαία και ανώνυμα και ανεξάρτητα εξετάζουν τα σχετικά αποδεικτικά στοιχεία. Ο κάθε δικαστής εκδίδει μια απόφαση κρυπτογραφημένη και όλες μαζί

[37]Το Matereum υποστηρίζει ένα αποκεντρωμένο σύστημα εμπορικού δικαίου, το Έξυπνο Μητρώο Ιδιοκτησίας, το οποίο εκτελείται μέσω αυτοματοποιημένων έξυπνων συμβάσεων που διασφαλίζουν τα δικαιώματα ιδιοκτησίας, καθώς και την επίλυση διαφορών μέσω της εφαρμογής.

[38] Το δίκτυο LTO είναι μια ολλανδική πλατφόρμα που κυκλοφόρησε το 2014. Η πλατφόρμα LTO δημιουργεί ένα Ricardian σε ένα ιδιωτικό blockchain

συγκεντρώνονται για να σχηματιστεί απόφαση πλειοψηφίας. Με αυτό τον τρόπο συνεχίζεται η εμπιστοσύνη και η αμεροληψία στα πρωτόκολλα blockchain με την εφαρμογή Jury online[39], **[9]** μια ανθρώπινη και μηχανική εξειδίκευση για τη διαιτησία των αναδυόμενων διαφορών. Η εναλλακτική επιλογή είναι προτιμηθεί η επίλυση των διαφορών εκτός της αλυσίδας του δικτύου μέσω διαπραγμάτευσης ή με την παρέμβαση ενός εξουσιοδοτούμενου τρίτου μέρους, εφόσον τα μέρη εισαγάγουν σε μια έξυπνη σύμβαση, ότι θα προτιμήσουν μη δεσμευτικούς μηχανισμούς επίλυσης διαφορών, εάν αυτές προκύψουν. Συνεπώς υπάρχουν δύο (2) διακριτές προσεγγίσεις επίλυσης διαφορών στο οικοσύστημα blockchain. Η αυτόνομη υπηρεσία και οι ενσωματωμένοι μηχανισμοί επίλυσης διαφορών, που θα κωδικοποιούνται στις συμβάσεις. Είναι μια εξαίσια ευκαιρία για μελλοντική έρευνα που θα συγκρίνει τις εναλλακτικές λύσεις.

- **Σύγκλιση Blockchain και τεχνητής νοημοσύνης – Ευφυϊα Blockchain**

Ο τεράστιος όγκος, η ετερογένεια, η ψευδοανωνυμοποίηση και κρυπτογράφηση των δεδομένων του blockchain, αποτελεί και μειονέκτημα. Η σύγκλιση των τεχνολογιών τεχνητής νοημοσύνης και blockchain, θα έδινε τις δυνατότητες να ξεπεραστούν αυτοί οι περιορισμοί του, μετά από την ανάλυση των δεδομένων του, για τον εντοπισμό πιθανών ευάλωτων κωδικών προγραμμάτων σε έξυπνα συμβόλαια, τα οποία ευνοούν κακόβουλες δραστηριότητες. Η μηχανική μάθηση με τις πολλαπλές προσεγγίσεις της, δίνει επιπλέον τη δυνατότητα να εποπτεύονται τα δεδομένα blockchain, συσχετίζοντας διαφορετικούς λογαριασμούς. Γι' αυτό, στο μέλλον, η τεχνητή νοημοσύνη αναμένεται να ενσωματωθεί στο αποκεντρωμένο σύστημα blockchain.

[39] Πλατφόρμα που συνδυάζει την ανθρώπινη και τη μηχανική εξειδίκευση για τη διαιτησία αναδυόμενων διαφορών.

Εικόνα 53: Ευφυΐα blockchain [49]

Βιβλιογραφία

[1] J. Rothfeder and Jeffrey, 1992. *Privacy for sale: how computerization has made everyone's private life an open secret*. **Simon & Schuster.**

[2] Nitin Gaur, Luc Dersosiers, Petr Novothy, Venkatraman Ramakrishna, Antony O'Dowd, Dr. Salman A. Baset, Anthony O'Dowd, 2018. *Hands On Blockchain with Hyperledger Fabric. Building decentralized applications with Hyperledger Fabric and Composer*. BIRMINGHAM – MUMBAI. **Packt Publishing**

[3] Jenny Alexandra Triana Casallas, Juan Manuel Cueva Lovelle, José Ignacio Rodríguez Molano, 2020. Smart Contracts with Blockchain in the Public Sector. *International Journal of Interactive Multimedia and Artificial Intelligence* (In Press) : 10. **E-journal.** https://www.ijimai.org/journal/sites/default/files/2020-08/ijimai_6_3_8.pdf

[4] Krawczyk, H.,& Rabin, T.,1998. Chameleon Hashing and Signatures. *International Conference on Financial Cryptography and Data Security.* **E-journal**. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.50.3262&rep=rep1&type=pdf.

[5] Pauline Debono., 2019. Transforming Public Procurement Contracts Into Smart Contracts. *International Journal of Information Technology Project Management*. **E-journal.** 10 (2). pp 16-28. https://www.igi-global.com/gateway/article/224928. Accessed 30 June 2020.

[6] William Metcalfe, 2020. Ethereum, Smart Contracts, Dapps. *Springer*. **E-journal**. In book: Blockchain and Crypt Currency. Pp 77 - 93. Available at: https://link.springer.com/chapter/10.1007%2F978-981-15-3376-1_5.Accessed 30 June 2020

[7] Κωνσταντίνος Λογαράς, 2018. Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της. *Ναυτεμπορική.* **Ηλεκτρονική Εφημερίδα**. Διαθέσιμο στη διεύθυνση: https://www.naftemporiki.gr/story/1363055/i-texnologia-blockchain-oi-efarmoges-tis-kai-oi-nomikes-ptuxes-tis. Πρόσβαση 29 Σεπτεμβρίου 2020

[8] Νικόλαος Ι. Θεοδωράκης, Γεώργιος Μ. Καλογεράκης, 2019. Blockchain : Εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. *Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας.(ΔΙΜΕΕ*) **Ηλεκτρονικό περιοδικό**. Κεφ.1 σελ. 3-24. Διαθέσιμο στην διεύθυνση : https://www.academia.edu.gr. Πρόσβαση 29 Σεπτεμβρίου 2020

[9] Darcy W E Allen, Aaron M Lane, Marta Poblet, 2020. *The Governance of Blockchain Dispute Resolution.* **Pdf**. Available at : https://www.researchgate.net/publication/340827439_The_Governance_of_Blockchain_DisputeResolution_-_Harvard_Negotiation_Law_Review_Vol_25. Accessed 29 September 2020

[10] Georgios Dimitropoulos, 2020. *The law of Blockchain*. **Pdf.** Available at : https://www.researchgate.net/publication/339998624_THE_LAW_OF_BLOCKCHAIN. Accessed 29 September 2020.

[11] Janes Hazard, Helena Haapi, 2017. *Wise Contracts: Smart Contracts that Work for People and Machines.* **Pdf.** Available at : https://www.researchgate.net/publication/314263820_Wise_Contracts_Smart_Contracts_that_Work_for_People_and_Machines. Accessed 29 September 2020.

[12] Kevin Werbach and Nicolas Cornell, 2017. *Contracts ex Machina*. **Pdf.** Available at: https://www.researchgate.net/publication/321265778_Contracts_Ex_Machina. Accessed 29 September 2020

[13] Zibin Zheng, Shaoan Xie, Hong -Ning Dai, Xiangping Chen.,2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*. **E-journal** 14 (4). pp 352-375. https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647

[14] Maher Alharby, Amjad Aldweesh, Aad Van Moorsel, 2019. *Blockchain-based Smart Contracts : A Systematic Mapping Study of Academic Research (2018).***Pdf**. Available at: https://www.researchgate.net/publication/333748177_Blockchain-based_Smart_Contracts_A_Systematic_Mapping_Study_of_Academic_Research_2018/link/5d021f11a6fdccd13096b161/download. Accessed 29 September 2020

[15] Nawari, Shriraam Ravindran, 2019. *Blockchain technology and BIM process: review and potential applications*. **Pdf.** Available at : https://www.researchgate.net/publication/333369406_Blockchain_technology_and_BIM_process_review_and_potential_applications F) Blockchain technology and BIM process: review and potential applications (researchgate.net). Accessed 17 October 2020

[16] Paul Davis, 2009. *BUYING INNOVATION to SMART Procurement and SME Access to Public Contracts.* **Pdf.** Available at : https://www.researchgate.net/publication/263238508_BUYING_INNOVATION_to_SMART_Procurement_and_SME_Access_to_Public_Contracts. Accessed 29 September 2020

[17] Release Master, June 2018. *Hyperledger- fabricdocs Documentation*. **Pdf**. Available at : Available at : https://hyperledger-fabric.readthedocs.io/_/downloads/en/release-2.0/pdf /. Accessed 29 September 2020

[18] Stavros Kitsakis, 2018. *Τεχνητή νοημοσύνη και συμβατική διαδικασία (Artificial Intelligence and contract law. An introduction).* **Pdf.** Available at : https://www.researchgate.net/publication/326711736_Technete_noemosyne_kai_symbatikedia dikasia_Artificial_Intelligence_and_contract_law_An_introduction) Τεχνητή νοημοσύνη και συμβατική διαδικασία (Artificial Intelligence and contract law. An introduction) (researchgate.net). Accessed 29 September 2020

[19] Steven Wright, 2019. *Tech and Legal Challenges for healthcare blockchains and Smart Contract.* **Pdf.** Available at : https://www.researchgate.net/publication/336114081_TECH_LEGAL_CHALLENGES_FOR _HEALTHCARE_BLOCKCHAINS_SMART_CONTRACTS. Accessed 29 September 2020.

[20] Yining Hu, Madhusanka Liyanage, Ahsan Manzoor, Kanchana Thilakarathna, Guillaume Jourjon, Aruna Seneviratne, 2019. *Blockchain - based Smart Contracts - Applications and Challenges*. **Pdf.** Available at.: https://www.researchgate.net/publication/328230865_Blockchain-based_Smart_Contracts_-Applications_and_Challenges Accessed 29 September 2020

[21] Zibin Zheng, Hong-Ning Dai, 2019. *Blochchain Intelligence : When Blockchain Meets Artificial Intelligence.* **Pdf**. Available at: https://www.researchgate.net/publication/337944266_Blockchain_Intelligence_When_Blockc hain_Meets_Artificial_Intelligence. Accessed 29 September 2020

[22] Αικατερίνη Μπουτακίδου, 2019. *Υλοποίηση και Εφαρμογές του Blockchain*. **Πτυχιακή εργασία**. Πανεπιστήμιο Ιωαννίνων. Σχολή Πληροφορικής και Επικοινωνιών.

[23] Αποστολόπουλος Αλέξανδρος, 2018. *Μελέτη της τεχνολογίας Blockchain και των εφαρμογών της στις ψηφιακές συναλλαγές*. **Τελική εργασία**. ΚΕ Εκπαιδευτική Σειρά. ΕΚΔΔΑ. Τμήμα Εξειδίκευσης : Ψηφιακή Πολιτική.

[24] Βασίλειος Χαντζιάρας, 2019. Επισκόπηση των δυνατοτήτων τεχνολογίας blockchain και εφαρμογές state of art στην υγεία και άλλους κλάδους. **Διπλωματική εργασία.** Διαπανεπιστημιακό Πρόγραμμα Μεταπτυχιακών Σπουδών : Τεχνο - οικονομικά Συστήματα.

[25] Γιαννακού Μαρία – Αγγελική, 2019. *Η τεχνολογία BC για την εξυπηρέτηση των πολιτών. Πρωτόκολλο Blockchain : Κρυπτονομίσματα και Ηλεκτρονική Ταυτοποίηση.* **Πτυχιακή εργασία** *ΕΚΠΑ*. Σχολή Οικονομικών και Πολιτικών Επιστημών.

[26] Δέδε Δήμητρα, Παπαδημήτρη Μαρία – Ελένη, Παπαδόπουλος Δημήτριος, Τσολάτη Παναγιώτα, 2014. *Γνωρίσματα και αδυναμίες της Δημόσιας Γραφειοκρατίας και του Δημοσίου Management.* **Διπλωματική εργασία**. Μεταπτυχιακό πρόγραμμα σπουδών : Κράτος και Δημόσια Διοίκηση. ΕΚΠΑ, Σχολή Νομικών και Πολιτικών Επιστημών. Τμήμα Πολιτικής Επιστήμης και Δημόσιας Διοίκησης

[27] Ιωάννης Μαυρουδής, 2019. *Τεχνολογία Blockchain και θέματα συμμόρφωσης με τον ΓΚΠΔ*. Διπλωματική εργασία. Μεταπτυχιακό Πρόγραμμα Σπουδών στα Πληροφοριακά Συστήματα. Ελληνικό Ανοικτό Πανεπιστήμιο. Σχολή Θετικών Επιστημών και Τεχνολογίας.

[28] Μπισδούνη Αριστέα, 2019. *Blockchain και Έξυπνα Συμβόλαια. Εφαρμογές και Προεκτάσεις*. **Πτυχιακή εργασία**. Πανεπιστήμιο Ιωαννίνων. Σχολή Οικονομίας και Διοικητικών Επιστημών

[29] Νάκου Χριστίνα, 2019. *Αξιοποίηση τεχνολογίας blockchain σε εφαρμογές κρίσιμης αποστολής : Μια μελέτη στο οικοσύστημα Hyperledger Using BC Technologies in mission – critical applications : a case study, based on Hyperledger ecosystem*. **Διπλωματική εργασία**. Εθνικό Μετσόβιο Πολυτεχνείο. Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών.

[30] Μπεκρή Ελένη, 2020. *Σύγκριση τεχνολογιών κατανεμημένης εγγραφής Blockchain*. **Διπλωματική εργασία**. Εθνικό Μετσόβιο Πολυτεχνείο. Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών.

[31] Ντόα Γεωργία, 2017. *Blockchain και η εφαρμογή του IoT*. **Διπλωματική εργασία**. Μεταπτυχιακό πρόγραμμα Ψηφιακής επικοινωνίας και Δίκτυα. Πανεπιστήμιο Πειραιώς.

[32] Πανταζή Ιωάννα, 2018. *Η ηλεκτρονική διακυβέρνηση ως παράγοντας μεταρρύθμισης της Δημόσιας Διοίκησης σε Ευρώπη και Ελλάδα. Εφαρμογές – Προοπτικές – Δυσκολίες στην τοπική Αυτοδιοίκηση.* **Διπλωματική εργασία**. Μεταπτυχιακό πρόγραμμα σπουδών Ευρωπαϊκή Ολοκλήρωση και Διακυβέρνηση. Πανεπιστήμιο Μακεδονίας.

[33] Ραψομανίκης Ερμανός, 2019. *Η συμβολή της τεχνολογίας blockchain στην Κυβερνοασφάλεια του IoT*. **Διπλωματική εργασία**. Πανεπιστήμιο Πατρών, Πολυτεχνική Σχολή, Τμήμα Μηχανικών Υπολογιστών και Πληροφορικής.

[34] Σαραφίδης Λεωνίδας, 2019. *Ψηφιακό νόμισμα, Τεχνολογία Blockchain, Τράπεζες*. Ελληνικό Ανοικτό Πανεπιστήμιο. Σχολή Κοινωνικών Επιστημών. **Διπλωματική εργασία**. Μεταπτυχιακό Πρόγραμμα Σπουδών στην Τραπεζική.

[35] Τζώρτζης Παναγιώτης, 2020. *Μελέτη επίδοσης του Blockchain Συστήματος στο Hyperledger Fabric*. **Διπλωματική εργασία**. Εθνικό Μετσόβιο Πολυτεχνείο. Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών.

[36] Adil Haris, 2019. *Smart Contracts – A Simple Yet Comprehensive Explanation in Pictures*. **Online**. Available at : https://adilharis.medium.com/smart-contracts-a-simple-yet-comprehensive-explanation-in-pictures-bc21c7ab89b6. Accessed 29 September 2020.

[37] Aeron Benchmarking, 2020. *AERON Blockchain for Aviation Safety*. **Online**. Available at: https://i.aeron.aero/storage/AeronWhitepaper.pdf . Accessed 29 September 2020

[38] Arnold Daniels, 2018. *The rise of private permissionless blockchains – part 1*. **Online**. Available at : https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be. Accessed 29 September 2020.

[39] Blackrypto society, 2019. *SMART VS. RICARDIAN CONTRACTS: WHAT'S THE DIFFERENCE ?* **Online**. Available at: https://blackrypto.org/blogs/crypto-education/smart-vs-ricardian-contracts-what-s-the-difference. Accessed 29 September 2020.

[40] Buterin, V., 2015. *A Next-Generation Smart Contract and Decentralized Application Platform*. **Online**. Available at : https://ethereum.org/en/whitepaper/.Accessed 29 September 2020.

[41] Computerworld, 2018. *IBM sees blockchain as ready for government use*. **Online**. Available at : https://medium.com/hellenic-blockchain-hub-el/blockchain-for-digital-government-report-774d57ca112a. Accessed 29 September 2020.

[42] DocuSign, 2020. *Understanding digital signatures*. **Online**. Available at : https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq. Accessed 29 September 2020.

[43] Friebe, T., 2017. *Bitcoin, Ethereum, and Hyperledger Fabric — which one wins?* **Online.** Available at : https://medium.com/blockchainspace/3-comparison-of-bitcoin-ethereum-and-hyperledger-fabric-cd48810e590c. Accessed 29 September 2020.

[44] Hewlett Packard Enterprise, 2018. *Should you move to blockchain ? Follow a systematic approach to making your decision*. **Online**. Available at : https://community.hpe.com/t5/Servers-Systems-The-Right/Should-you-move-to_blockchain-Follow-a-systematic-approach-to/ba-p/7004262#.YfA1BupByM9. Accessed 29 September 2020.

[45] Hyperledger Foundation, 2020. *Case Studies. Browse various use cases powered by Hyperledger technologies*. **Online**. Available at : https://www.hyperledger.org/learn/case-studies. Accessed 30 June 2020

[46] Hyperledger Foundation, 2020. *White Papers. Read popular white papers created by the Hyperledger community.* **Online**. Available at: https://www.hyperledger.org/learn/white-papers. Accessed 30 June 2020

[47] IBM Blockchain Blog, 2020, *What are smart contracts on blockchain*. **Online.** Available at**:** https://www.ibm.com/topics/smart-contracts. Accessed 30 June 2020

[48] IBM Blockchain Blog, 2020. *What is Hyperledger Fabric?* **Online.** Available at : https://www.ibm.com/topics/hyperledger . Accessed 30 June 2020

[49] Leandro Nascimento, 2018. *Blockchain is a nutshell*. **Online**. Available at : https://blogs.sap.com/2018/03/06/blockchain-in-a-nutshell/. Accessed 29 September 2020.

[50] Nakamoto S, 2008. *Bitcoin: A Peer-to-Peer Electronic cash system.* ***Online.*** Available at : https://bitcoin.org/bitcoin.pdf Accessed 29 September 2020.

[51] Paul, M.S, 2017. *Hyperledger - When to use the Blockchain Technology*. **Online.** Available at : https://medium.com/swlh/hyperledger-chapter-3-when-to-use-the-blockchaintechnology-a5c414221bdf . Accessed 29 September 2020.

[52] Rosic, A., 2017. *What Is Hyperledger? The Most Comprehensive Step-by-Step Guide!* **Online.** Available at: https://blockgeeks.com/guides/hyperledger/ Accessed 29 September 2020.

[53] Wikimedia Commons, 2015. *File : Hash Tree. Svg*. **Online**. Available at : https://commons.wikimedia.org/w/index.php?curid=18157888. Accessed 29 September 2020.

[54] Hellenic Blockchain Hub, *Τι Είναι Η Τεχνολογία Blockchain ?* **Διαδίκτυο** https://www.blockchain.org.gr/home/mathe/. Πρόσβαση 29 Σεπτεμβρίου 2020

[55] KGLawFirm, 2018. *Blockchain & Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR).* Διαθέσιμο στη διεύθυνση: https://kglawfirm.gr/wp-content/pdfs/5c1384df40b59.pdf Πρόσβαση 29 Σεπτεμβρίου 2020

[56] Lawspot, 2018. *Εννοϊκές ρυθμίσεις για blockchain και DLT ζητά το Ευρωκοινοβούλιο (Ψήφισμα).* **Διαδίκτυο**. https://www.lawspot.gr/nomika-nea/eynoikes-rythmiseis-gia-blockchain-kai-dlt-zita-eyrokoinovoylio-psifisma. Πρόσβαση 29 Σεπτεμβρίου 2020

[57] RSM Greece, 2018. *Blockchain: Η τεχνολογία που η δυναμική της δε μπορεί να αγνοηθεί.* **Διαδίκτυο.** Διαθέσιμο στη διεύθυνση : https://www.rsm.global/greece/news/blockchain-i-tehnologia-poy-i-dynamiki-tis-de-mporei-na-agnoithei. Πρόσβαση 29 Σεπτεμβρίου 2020

[58] Ευρωπαϊκό Κοινοβούλιο, 2018. *Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 13ης Δεκεμβρίου 2018 σχετικά με την τεχνολογία blockchain: μια μακρόπνοη εμπορική πολιτική (2018/2085(INI))*. **Διαδίκτυο.** https://www.europarl.europa.eu/doceo/document/TA-8-2018-0528_EL.html . Πρόσβαση 29 Σεπτεμβρίου 2020

[59] Κωνσταντίνος Λογαράς, 2018. *Η Τεχνολογία Blockchain, οι εφαρμογές και οι νομικές πτυχές της.* **Διαδίκτυο.** Διαθέσιμο στη διεύθυνση : https://www.lawspot.gr/nomika-nea/h-tehnologia-blockchain-oi-efarmoges-kai-oi-nomikes-ptyhes-tis. Πρόσβαση 29 Σεπτεμβρίου 2020

[60] Παρατηρητήριο Ψηφιακού Μετασχηματισμού, 2020. *Ψηφιακή και τεχνολογική ωριμότητα οικονομίας και επιχειρήσεων*. Διαθέσιμο στη διεύθυνση: https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/technology/gr_SEV_Deloitte_Digital_Maturity_Report_2020_noexp.pdf. Πρόσβαση 29 Σεπτεμβρίου 2020

[61] Υπουργείο Ψηφιακής Πολιτικής, 2018. *Υπογραφή της Διυπουργικής Διακήρυξης χωρών της Ν. Ευρώπης για τις Τεχνολογίες Κατανεμημένου Καθολικού (blockchain)* .**Διαδίκτυο**. Διαθέσιμο στη διεύθυνση : http://mindigital.gr/index.php/41-ggpsp/media/3259-blockchain-4-2018. Πρόσβαση 29 Σεπτεμβρίου 2020

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα πτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.