



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**«Η τεχνολογία του Blockchain και η προσπάθεια σύγκλισής
της με το Γενικό Κανονισμό Προστασίας Προσωπικών
Δεδομένων»**

Διπλωματική Εργασία

του

Θωμά Λάππα

(Αριθμός Μητρώου icsd518010)

Επιβλέπων Καθηγητής: Γεώργιος Κορμέντζας

Ιούλιος 2021

Ευχαριστίες

Η συγκεκριμένη διπλωματική εργασία πέρασε από αρκετά στάδια, ενδεχομένως περισσότερα και από τα μέχρι τώρα lock down που έχουμε υποστεί ως ελληνική κοινωνία εξαιτίας της πανδημίας. Παρ' όλες τις δυσκολίες που προέκυψαν, εν τέλει κατάφερα να φέρω εις πέρας και αυτό το εγχείρημα.

Ξεκινώντας, θα ήθελα να ευχαριστήσω τον καθηγητή μου, Δρ. Γεώργιο Κορμεντζά, ο οποίος με καθοδήγησε σχετικά με την εύρεση της θεματολογίας. Οι συμβουλές του και τα σχόλιά του συνέβαλαν στη σωστή διεκπεραίωση αυτής της διπλωματικής εργασίας.

Ειδικές ευχαριστίες θα ήθελα να δώσω στους καθηγητές μου από το πτυχίο των Οικονομικών μου σπουδών, Δρ. Νίκο Θεοχαράκη, Δρ. Θανάση Μανιάτη και Δρ. Εμμανουήλ Κουντούρη. Τόσο οι ακαδημαϊκές τους διαλέξεις όσο και οι περαιτέρω συζητήσεις τους, έδρασαν καθοριστικά στη διαμόρφωση της προσωπικότητάς μου.

Επίσης, τις θερμές μου ευχαριστίες και τις καλύτερες ευχές στους ακαδημαϊκούς μου φίλους από το Ηνωμένο Βασίλειο (Δρ. Γιάννη Βαϊλάκη, Δρ. Δήμο Ανδρονούδη, Δρ. Νικόλαο Βλάσση). Πραγματικά έχω επιθυμήσει τις όμορφες συζητήσεις και τις στιγμές που ζήσαμε μαζί.

Αν και μεγαλύτεροι σε ηλικία πια, η παρέα του μεταπτυχιακού θύμιζε, τρόπον τινά, τις παλιές φοιτητικές μου στιγμές πριν αρκετά χρόνια. Όλα τα παιδιά στο μεταπτυχιακό ήταν εξαιρετικά. Ειδικότερα όμως θα ήθελα να ευχαριστήσω το Δήμητρη Α. και τον Πέτρο Π., μιας και συνεργαστήκαμε σε αρκετές εργασίες και στις εξεταστικές του τμήματος.

Επιπροσθέτως, θα ήθελα να ευχαριστήσω όλο το εκπαιδευτικό προσωπικό και τους διδάσκοντες του τμήματος Φωτογραφίας και Οπτικοακουστικών Τεχνών του Πανεπιστημίου Δυτικής Αττικής. Τον τελευταίο χρόνο, η παρακολούθηση των διαλέξεων και των εργαστηρίων ανέπτυξε την αισθητική μου ως ανθρώπου, ενώ ταυτόχρονα με βοήθησε να ξεπεράσω πολλές από τις δυσκολίες που δημιουργήθηκαν εξαιτίας του κορωνοϊού.

Κλείνοντας, θα ήθελα να ευχαριστήσω την αξιαγάπητη οικογένεια μου, η οποία εξακολουθεί να με στηρίζει σε ό,τι επιλέγω να κάνω στη ζωή μου. Στον πατέρα μου, τη μητέρα μου, την αδερφή μου και όλη την υπόλοιπη οικογένεια. Παρ' όλη την παραξενιά και την γκρίνια μου, αυτοί βρίσκονται πάντα εκεί να με υποστηρίζουν. Ιδιαίτερες ευχαριστίες θα ήθελα να δώσω στη Θεοδώρα, η οποία με βοήθησε και με στήριξε κατά τη διάρκεια όλης της συγγραφής καθώς και στον παλιό μου φίλο Μάκη Πέτσα για την γλωσσική επιμέλεια του τελικού μου κειμένου.

Η σελίδα είναι σκόπιμα κενή

Πίνακας Περιεχομένων

Εισαγωγή	10
Μέρος 1^ο: Η Τεχνολογία του Blockchain	12
1.1 Οι Τεχνολογίες Κατανεμημένου Λογισμικού	12
1.2 Τύποι DLTs	13
1.3 Η Τεχνολογία του Blockchain.....	14
1.4 Τα δομικά συστατικά στοιχεία	15
1.5 Η Διαδικασία Δημιουργίας Ενός Μπλοκ	16
1.6 Βασικές Ιδιότητες ενός Blockchain.....	17
1.7 Ταξινόμηση των Blockchain	18
1.8 Μηχανισμοί Συναίνεσης (Consensus Mechanisms)	19
1.9 Χρησιμοποιούμενες Τεχνικές Κρυπτογράφησης	23
1.10 Έξυπνα Συμβόλαια (Smart Contracts)	26
Μέρος 2^ο : Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων	28
2.1 Εισαγωγή – Συνοπτική Ιστορική Αναδρομή	28
2.2 Αντίστοιχοι Κανονισμοί εκτός Ευρώπης	29
2.3 Βασικές Οντότητες - Υπό Χρήση Έννοιες του ΓΚΠΔ.....	30
2.4 Οι Βασικές Αρχές του GDPR.....	32
2.5 Τα δικαιώματα του υποκειμένου των προσωπικών δεδομένων	34
Μέρος 3^ο : Ενοποιώντας την τεχνολογία του Blockchain με τον ΓΚΠΔ	36
3.1 Εισαγωγή	36
3.2 Τα προβλήματα που δημιουργούνται	36
3.3 Προτεινόμενες Τεχνικές Λύσεις.....	37
Μέρος 4^ο: Μία Τεχνολογία Σύγκλισης του ΓΚΠΔ με την Τεχνολογία του Blockchain	40
4.1 Εισαγωγή	40
4.2 Ιδιωτικό Blockchain - Live Contracts (1ο Επίπεδο).....	40
Μέθοδοι Απεικόνισης των Δεδομένων - Πληροφοριών	41
Ο Εκτεταμένος Μηχανισμός Πεπερασμένων Καταστάσεων	42
Τα Συστατικά Στοιχεία του Μοντέλου	42
Η ροή δημιουργίας ενός Live Contract	44
Ιδιωτικότητα του Δικτύου και Συμβατότητα με τον ΓΚΠΔ	46
4.3 Δημόσιο Blockchain - Global Blockchain (2ο Επίπεδο).....	48
«Αγκιστρώνοντας» τις Συναρτήσεις Κατακερματισμού	48
Χρησιμοποιούμενος Μηχανισμός Συναίνεσης.....	49
Συντελεστές Προσδιορισμού	49

Διπλωματική Εργασία: «Η τεχνολογία του Blockchain και η προσπάθεια
συμμόρφωσης της με τον ΓΚΠΔ»

Τα Μπλοκ Σύνοψης.....	50
Το συνολικό μέγεθος ενός blockchain	52
4.4 Τα συστατικά μέρη ενός Κόμβου.....	53
(LTO Network, 2021).....	53
Μέρος 5ο: Πρακτικές Εφαρμογές	55
5.1 Από το θεωρητικό μοντέλο στην πρακτική εφαρμογή.....	55
5.2 Πρακτικές Εφαρμογές Του Δικτύου (<i>LTO Netwrok - Use Cases</i>).....	56
<i>A. Proofi</i>	56
<i>B. Waste Transport</i>	57
<i>C. SignRequest</i>	58
<i>D. Capptions</i>	59
<i>E. Artwork Authenticity on Blockchain</i>	60
Άλλες Περιπτώσεις Εφαρμογής	61
Μέρος 6^ο: Επίλογος - Συμπεράσματα.....	62
Χρησιμοποιούμενη Βιβλιογραφία	64
Συμπληρωματική Βιβλιογραφία	67

Λίστες Σχημάτων – Πινάκων – Διαγραμμάτων (Σελίδες)

Λίστα Σχημάτων

Σχήμα 1: Η Δομή Ενός Μπλοκ	15
Σχήμα 2 : Διαδικασία Δημιουργίας και Προσθήκης ενός Μπλοκ στην Αλυσίδα	17
Σχήμα 3: Η Δομή ενός Merkle Tree.....	25
Σχήμα 4: Ο Εκτεταμένος Μηχανισμός Πεπερασμένων Καταστάσεων	42
Σχήμα 5: Τα Συστατικά Στοιχεία ενός Live Contract	46
Σχήμα 6: Τα Δομικά Συστατικά ενός Κόμβου στο Δίκτυο LTO.....	54

Λίστα Συγκριτικών Πινάκων

Πίνακας 1 : Ταξινόμηση Μεταξύ των Blockchain	19
Πίνακας 2 : Σύγκριση των Μηχανισμών Συναίνεσης	23

Λίστα Διαγραμμάτων

Διάγραμμα 1: Η Ροή Proof of Work.....	21
Διάγραμμα 2: Η Ροή Proof of Stake.....	22
Διάγραμμα 3: Οι Βασικές Αρχές του ΓΚΠΔ	33

Λίστα Εικόνων

Εικόνα 1 : Η Διαδικασία της Ασύμμετρης Κρυπτογράφησης.....	26
Εικόνα 2: Οι οντότητες του GDPR.....	31
Εικόνα 3: Τρόπος λειτουργίας Proofi	57

Ακρωνύμια	
API	Application Programming Interface
CalOPPA	California Online Privacy Protection Act
DAG	Direct Acyclic Graph
DLT	Decentralized Ledger Technologies
EHS	Environmental, Health & Safety Reports
EFSM	Extended Finite State Machine
FSM	Finite State Machine
GDPR	General Data Protection Regulation
ID	Identification
IPP	Information Party Principles
JSON	Javascript Object Notation
LGPD	Lei Geral de Proteção de Dados
LPoS	Leased Proof Of Stake
pBFT	Practical Byzantine Fault Tolerance
PDF	Portable Document Format
PIPEDA	Personal Information Protection and Electronic Documents Act
PoI	Proof of Importance
POPI	Protection of Personal Information Act
PoS	Proof of Stake
PoW	Proof of Work
RabbitMQ	Rabbit Message-Queueing
SHA	Secure Hash Algorithm
SSL EV	Secure Sockets Layer Extended Validation
YAML	YAML Ain't Markup Language
ΓΚΠΔ ή ΓΚΠΠΔ	Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων
Αναλογία M.M.	Αναλογία Μερισματικών Μονάδων
E.E.	Ευρωπαϊκή Ένωση

Περίληψη

Η συγκεκριμένη διπλωματική εργασία, πραγματεύεται τη διερεύνηση του κατά πόσον η τεχνολογία του blockchain μπορεί να συμμορφωθεί με το κανονιστικό πλαίσιο που θέτει ο ΓΚΠΔ. Η ανάλυσή μας ξεκινάει με την εισαγωγή των αναγκαίων όρων και εννοιών, με τους οποίους ενδύεται η τεχνολογία του blockchain. Στη συνέχεια, εκθέτει τις απαραίτητες έννοιες και τους κανονισμούς που αφορούν στον GDPR. Η επόμενη ενότητα μας βρίσκει να εξετάζουμε τα προβλήματα που δημιουργούνται κατόπιν της προσπάθειας σύζευξης των δύο αυτών εννοιών, ενώ θα αναφερθούμε στις τεχνικές λύσεις που έχουν προταθεί για τη διευθέτηση των προβλημάτων. Ακολούθως, παρουσιάζεται η πρόταση μίας συγκεκριμένης τεχνολογίας υλοποίησης, η οποία φαίνεται να υπερπηδά τα προβλήματα που δημιουργούνται. Επιπροσθέτως, γίνεται αναλυτική αναφορά τόσο στη δημιουργία του θεωρητικού μοντέλου όσο και στην αρχιτεκτονική του δικτύου LTO. Στο πέμπτο μέρος, έχοντας καθορίσει το θεωρητικό πλαίσιο και την αρχιτεκτονική του δικτύου που επιλύει τη σύγκρουση μεταξύ του blockchain και του ΓΚΠΔ, θα υπάρξει μία συνοπτική παρουσίαση διαφόρων πρακτικών εφαρμογών οι οποίες υλοποιούνται το τελευταίο χρονικό διάστημα. Στο τελευταίο μέρος, θα συνοψίσουμε την ανάλυσή μας, προσπαθώντας να απαντήσουμε το αρχικό ερώτημα της συγκεκριμένης διπλωματικής -ήτοι, αν η τεχνολογία του blockchain συμμορφώνεται με τις επιταγές του GDPR- ενώ θα εξεταστούν και πιθανές προοπτικές περαιτέρω ανάπτυξης του μοντέλου.

Αν και, εν πρώτοις, το εύρος της διπλωματικής φαίνεται να μην είναι και τόσο μεγάλο, η συγκεκριμένη προσπάθεια αποδεικνύει ακριβώς το αντίθετο -υπάρχει μία δυναμική, η οποία ακόμη δεν έχει κάνει την εμφάνισή της στο ευρύτερο κοινό.

Λέξεις Κλειδιά: *Blockchain, GDPR, ΓΚΠΔ, Αποκεντρωμένες Βάσεις Διαχείρισης, Μηχανισμός Συναίνεσης, Κατανεμημένο Καθολικό, Αποκεντρωμένη Τεχνολογία, Κόμβος, Ομότιμοι Χρήστες, Συνάρτηση Σύνοψης, Αλγόριθμος, Δένδρα Merkle, Ασύμμετρη Κρυπτογράφηση, Έξυπνα Συμβόλαια, Υπεύθυνος Επεξεργασίας, Εκτελών την Επεξεργασία, Υποκείμενο Δεδομένων, Επεξεργασία, Ψευδωνυμοποίηση, Ανωνυμοποίηση, Συγκατάθεση, Διαφάνεια, Ακρίβεια, Ελαχιστοποίηση, Ακεραιότητα, Φορητότητα, Διόρθωση, Αγκίστρωση, Ζωντανά Συμβόλαια, δίκτυο LTO, Μηχανισμός Πεπερασμένων Καταστάσεων, Ροές Εργασιών*

Abstract

In the current dissertation thesis, we will try to answer if blockchain technology can be compliant with the General Data Protection Regulation. Our analysis, begins with the essential elements and definitions needed to understand blockchain technology. Up next, we introduce GDPR semantics and definitions. Going forward, we will try to combine the above two elements and analyse the conflicts that are created by this unification. Additionally, we indicate the proposed technical solutions which provide us with satisfactory results and resolve these disputes. In part four, we will present our theoretical model looking into the LTO network architecture and its entities which deliver our desired outcomes. In the next part, we will focus on some practical implementations and applications which rely on LTO network and at the same time are GDPR compliant. Finally, in part six we will summarize our findings and draw our final conclusions.

While a quick look denotes that the specific research range is quite limited, this dissertation proves the exact opposite. There is a potential that has been not exposed to the public yet.

Keywords: *Blockchain, GDPR, DLT, Consensus Mechanisms, Distributed Ledger, Decntralized Technology, Nodes, Peer-to-Peer Netwrok, Hash, Algorithm, Merkle Trees, Asymmetric Cryptography, Smart Contracts, Data Controller, Data Processor, Pseudonymisation, Anonymization, Consent, Transparency, Accuracy, Minimization, Integrity, Portability, Correction, Anchoring, Live Contracts, LTO Network, Finite State Machine, Workflow*

Εισαγωγή

Έχουν περάσει αισίως περίπου 13 χρόνια από τη δημιουργία και παρουσίαση του πρώτου κρυπτονομίσματος. Αν και αρχικά δεν υπήρξε ιδιαίτερο ενδιαφέρον για τη συγκεκριμένη τεχνολογία, την τελευταία πενταετία ισχύει ακριβώς το αντίθετο.

Όπως συμβαίνει και με τους υπόλοιπους φυσικούς πόρους, το εύρος του κάθε κρυπτονομίσματος είναι πεπερασμένο. Παρ' όλα αυτά, η ζήτηση στη συγκεκριμένη αγορά παραμένει διαρκώς αυξητική. Μέχρι τη στιγμή που γράφονται αυτές οι γραμμές, η συγκεκριμένη αγορά ξεπερνά τα 4000 κρυπτονομίσματα. Πολλοί επίδοξοι «επενδυτές» καθημερινά ψάχνουν να ανακαλύψουν το νέο El Dorado, που θα τους αποφέρει το εύκολο και γρήγορο κέρδος, γεμίζοντάς τους τις τσέπες με χρήματα.

Εκτός όμως από το οικονομοτεχνικό κομμάτι, με το οποίο ασχολείται η πλειοψηφία του κόσμου, υπάρχει και ένα ακόμη πιο ουσιαστικό, αυτό της τεχνολογίας στην οποία στηρίζεται όλο το παραπάνω εγχείρημα. Ευρισκόμενοι στο πρώτο μισό του 21^{ου} αιώνα, η τεχνολογία του blockchain ήρθε να προστεθεί σε εκείνες της τεχνολογικές επαναστάσεις, οι οποίες από ό,τι φαίνεται θα συμβάλουν στη ριζική αλλαγή της καθημερινότητας που γνωρίζουμε μέχρι σήμερα. Η βασική αλλαγή που προσφέρει η συγκεκριμένη τεχνολογία έναντι άλλων έγκειται στο γεγονός του «εκδημοκρατισμού» των υφιστάμενων διαδικασιών. Η αποκεντροποίηση των κατανεμημένων καθολικών και των πληροφοριών έρχεται να καταργήσει την κεντρική διαχείριση των δεδομένων, δίνοντας την εξουσία στους ίδιους τους χρήστες της κάθε βάσης δεδομένων (είτε πρόκειται για νόμισμα είτε για οτιδήποτε άλλο). Η συγκεκριμένη τακτική έχει ως αποτέλεσμα την ενίσχυση της εμπιστοσύνης των χρηστών στις ακολουθούμενες διαδικασίες. Η αδιαφάνεια και η κεντρική διαχείριση αντικαθίσταται από τη διαφάνεια και τη διάχυση των πληροφοριών. Ο κάθε χρήστης που συμμετέχει στο δίκτυο μπορεί να έχει πρόσβαση στα δεδομένα του, ενώ οι εκτελούμενες ενέργειες είναι συνήθως μη αναστρέψιμες.

Οι αλλαγές στις υφιστάμενες δομές όλων των κλάδων οι οποίοι μέχρι πρότινος χαρακτηρίζονταν από ανελαστικότητα έχουν ήδη αρχίσει να κάνουν την εμφάνισή τους. Από τις πιο απλές διαδικασίες (π.χ. επικαιροποίηση και πιστοποίηση προσωπικών στοιχείων, χρηματοπιστωτικές συναλλαγές, αγορά εργασίας, διαχείριση εφοδιαστικής αλυσίδας κ.ά.) μέχρι και τις πιο περίπλοκες και δύσκολες με τα προσωπικά δεδομένα να είναι ευαίσθητα (εκλογική διαδικασία, υγειονομικές υπηρεσίες, ενεργειακή διαχείριση κ.ά.), η αλλαγή έχει ήδη ξεκινήσει να συντελείται.

Η πανδημία του κορωνοϊού έδρασε ως ο επιπλέον αναγκαίος καταλύτης που επιτάχυνε αυτή τη διαδικασία του ψηφιακού «κοινωνικού» μετασχηματισμού. Μέχρι την στιγμή που γράφονται οι συγκεκριμένες γραμμές, ακόμη δεν έχει καταλαγιάσει «η σκόννη της πανδημίας του COVID», με το φόβο και την αβεβαιότητα να εξακολουθούν να κυριαρχούν στη συνείδηση του κόσμου. Αξίες και αντιλήψεις που μέχρι πρότινος υπήρχαν έρχονται σε αμφισβήτηση και επαναδιαπραγμάτευση, ενώ πολλά ερωτήματα συνεχίζουν να παραμένουν αναπάντητα. Η παραγωγική διαδικασία σε παγκόσμιο επίπεδο έχει υποστεί καίρια πλήγματα, ενώ κανένας δεν γνωρίζει προς ποια κατεύθυνση θα εξελιχθούν τα πράγματα. Ωστόσο, είναι σίγουρο ότι οι ιστορικοί του

μέλλοντος θα μνημονεύουν και θα μελετούν τη συγκεκριμένη χρονική περίοδο τα χρόνια που έπονται.

Ένα σημαντικό συστατικό στοιχείο, στο οποίο παραλείψαμε να αναφερθούμε προηγούμενως στην ανάλυσή μας, είναι τα δεδομένα αυτά καθεαυτά. Με βάση πρόσφατες μελέτες, η αξία των δεδομένων είναι μεγαλύτερη από ποτέ. Σύμφωνα με μετρήσεις τις Ευρωπαϊκής Ένωσης, για το 2020 η χρηματική αποτύπωση μίας μόνο κατηγορίας δεδομένων (από τις πολλές), ήτοι των προσωπικών δεδομένων, θα ξεπεράσει το ένα τρις Euro (Rea & Sutton, 2019). Ως επακόλουθο, σε ένα διαρκώς μεταβαλλόμενο περιβάλλον, όπου τα δεδομένα από τη δημιουργία ως και τη διαχείρισή τους γνωρίζουν μία συνεχή εξέλιξη, όλο και περισσότεροι είναι εκείνοι που προσπαθούν να βρουν τρόπους αξιοποίησής τους μέσω της αξίας που αυτά εμπεριέχουν.

Η εφαρμογή του ΓΚΠΔ το Μάιο του 2018 έφερε σημαντικές ανακατατάξεις στον τρόπο προσέγγισης της διαχείρισης των προσωπικών δεδομένων, προσθέτοντας πολλές δυσκολίες που μέχρι πρότινος δεν υπήρχαν. Η άρση και αλλαγή του ασαφούς και θολού προγενέστερου νομοθετικού πλαισίου αντικαταστάθηκε από τη σαφήνεια, με απώτερο στόχο την «ενδυνάμωση θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, καθώς και την ομοιομορφία του νομικού πλαισίου σε όλα τα κράτη-μέλη» της Ε.Ε. (Σφακιανάκης - Μακρυπούλιας, 2021).

Με βάση τα παραπάνω, θα λέγαμε ότι η προσπάθεια συμμόρφωσης της πολλά υποσχόμενης τεχνολογίας του blockchain με το ΓΚΠΔ μοιάζει να αποτελεί νομοτέλεια. Η μόνη μεταβλητή που παραμένει άλυτη στη συγκεκριμένη συνάρτηση είναι ο χρόνος υλοποίησης. Η τεχνολογία της αλυσίδας των μπλοκ ήρθε για να μείνει. Στα μέρη που θα ακολουθήσουν, εμείς θα επιχειρήσουμε να διερευνήσουμε εάν η τεχνολογία του blockchain καταφέρνει να λειτουργήσει υπό το αυστηρό κανονιστικό πλαίσιο του Κανονισμού.

Μέρος Ι': Η Τεχνολογία του Blockchain

1.1 Οι Τεχνολογίες Κατανεμημένου Λογισμικού

(DLT's - Decentralized Ledger Technologies)

Οι τεχνολογίες κατανεμημένου λογισμικού αποτελούν ένα πρωτόκολλο που επιτρέπει την καταγραφή, το διαμοιρασμό και το συγχρονισμό μίας αποκεντρωμένης ψηφιακής βάσης δεδομένων ή (και) πληροφοριών, την οποία διαχειρίζονται ομότιμα οι χρήστες ενός υπολογιστικού δικτύου. Ο κάθε χρήστης που συμμετέχει στον κόμβο διατηρεί ένα αντίγραφο του καθολικού, ενώ κάθε αλλαγή ή τροποποίησή του γίνεται ορατή σε όλους τους συμμετέχοντες, μέσα σε σύντομο χρονικό διάστημα (δευτερόλεπτα ή λεπτά), διατηρώντας την εμπιστοσύνη για τη σωστή λειτουργία του δικτύου.

Η έννοια του «**αποκεντρωμένου**» (*decentralized*) έρχεται να συγκριθεί με αυτή της **κεντρικής διαχείρισης** (*centralized*), η οποία αποτελεί και τη διαδεδομένη χρησιμοποιούμενη μέθοδο. Θα λέγαμε, λοιπόν, ότι στην «**κεντροποιημένη**» διαχείριση, μία οντότητα (π.χ. οργανισμός, εταιρία) διατηρεί τον πλήρη έλεγχο στο δίκτυό της, με την πρόσβαση στις πληροφορίες να πραγματοποιείται μέσω ενός κεντρικού κόμβου. Υιοθετώντας την αποκεντρωμένη διαχείριση, τα δεδομένα επικαιροποιούνται άμεσα, με την ενημέρωση να πραγματοποιείται σε όλους τους κόμβους που συμμετέχουν.

Η συγκεκριμένη τεχνολογία παρέχει το πλεονέκτημα κατάργησης των «ενδιάμεσων» συμβαλλόμενων, δηλαδή των «**μεσαζόντων**» (*intermediaries*). Έτσι, μειώνεται το εκάστοτε δυνητικό κόστος, ενώ ταυτόχρονα αυξάνεται η ταχύτητα της συναλλαγής και η υπολογιστή ισχύς του δικτύου.

Επίσης, κατά πολλούς θεωρείται μία πολύ πιο **διαφανής διαδικασία** (*transparency*) εν συγκρίσει με τις προγενέστερες, διότι όλες οι πληροφορίες διαμοιράζονται εντός του δικτύου με τον κάθε χρήστη να διατηρεί ένα αντίγραφο του **καθολικού** (*ledger*). Ένα ακόμη πλεονέκτημα της συγκεκριμένης τεχνολογίας αποτελεί η μείωση της **λειτουργικής αναποτελεσματικότητας**, δηλαδή του χρόνου απόκρισης μίας συναλλαγής, μέσω της συνεχούς και αδιάλειπτης αυτόματης λειτουργίας του συστήματος, καθώς παρέχει στους χρήστες της τη δυνατότητα άμεσης τροποποίησης του κατανεμημένου καθολικού.

Ανάλογα με την περίπτωση και τους στόχους που θέλει κάποιος να εκπληρώσει, το κατανεμημένο καθολικό διακρίνεται σε **δημόσιο ή ιδιωτικό** (*public / private*) με **ελεύθερη ή αδειοδοτούμενη πρόσβαση στο δίκτυο** (*permissioned / permissionless*). Για παράδειγμα, σε μία βάση η οποία περιέχει τα ιατρικά δεδομένα ασθενών, τα οποία είναι ευαίσθητα και απαιτούν ιδιαίτερο χειρισμό, προτιμάται η χρησιμοποίηση ενός ιδιωτικού DLT με χορήγηση άδειας για τους χρήστες του. Από την άλλη μεριά, για την πραγματοποίηση μίας εκλογικής διαδικασίας, προτιμάται η χρησιμοποίηση μίας δημόσιας ανοικτής βάσης δεδομένων χωρίς άδεια πρόσβασης στο εκλογικό αποτέλεσμα, ενισχύοντας έτσι την ακεραιότητα και την εμπιστοσύνη του εκλογικού σώματος.

Για τη δημιουργία και επικύρωση των νέων στοιχείων που προστίθενται στη βάση δεδομένων, γίνεται χρήση διαφορετικών κρυπτογραφικών μηχανισμών

επικύρωσης, οι οποίοι ονομάζονται **μηχανισμοί συναίνεσης**. Επίσης, με στόχο την ορθή επαλήθευση του προστιθέμενου στοιχείου στο καθολικό, γίνεται χρήση **ψηφιακής υπογραφής**, η οποία λειτουργεί ως επιβεβαίωση - «χρονosφραγίδα» αυτών των νέων δεδομένων που προστίθενται στην αλυσίδα.

1.2 Τύποι DLTs

Υπάρχουν διάφοροι τύποι τεχνολογίας κατανεμημένου καθολικού (DLTs) (Green, 2019). Ενδεικτικά, θα μπορούσαμε να αναφερθούμε σε μερικούς από αυτούς:

1. **Blockchain**: Αποτελεί το πιο γνωστό είδος τεχνολογίας κατανεμημένου λογισμικού. Οι συναλλαγές που πραγματοποιούνται διατηρούνται στο καθολικό ως μία μορφή αλυσίδας στο εκάστοτε μπλοκ. Η ομαδοποίησή τους πραγματοποιείται σε μπλοκ δεδομένων και η διατήρησή τους μεταξύ των ομότιμων κόμβων του. Για την επιβεβαίωσή τους στην αλυσίδα γίνεται χρήση αλγορίθμων ασύμμετρης κρυπτογραφίας, με τη δημιουργία τους να προκύπτει από τη χρήση διαφόρων μηχανισμών συναίνεσης μεταξύ των κόμβων του (π.χ. *Proof of Work*, *Proof of Stake*, *Proof of Importance*). Περισσότερες λεπτομέρειες θα δούμε στη συνέχεια της ανάλυσής μας.

2. **Direct Acyclic Graph (D.A.G.)**: Κάθε συναλλαγή αποθηκεύεται σε παράλληλη τυπολογική σειρά μέσα στο καθολικό. Σε αντίθεση με την τεχνολογία του blockchain, δεν υπάρχουν ξεχωριστά μπλοκ αλλά ένα ενιαίο. Αποτελεί μία ακολουθία όπου κάθε συναλλαγή προκύπτει από την επόμενη ακολουθία (*Sequence*). Ο χρόνος επικύρωσης των συναλλαγών είναι αντιστρόφως ανάλογος με τους χρήστες του δικτύου: Όσο περισσότεροι χρήστες χρησιμοποιούν το δίκτυο τόσο λιγότερος χρόνος χρειάζεται για την επικύρωση, παρέχοντας την επιλογή απεριόριστης επεκτασιμότητας των πληροφοριών (*Scalability*). Οι ψηφιακές υπογραφές που χρησιμοποιούνται είναι μίας χρήσης, ενισχύοντας την ασφάλεια του δικτύου (*Quantum Resistant*).

3. **Hashgraph**: Υπάρχει η δυνατότητα πολλαπλές συναλλαγές να αποθηκευτούν στο καθολικό της ίδιας χρονosφραγίδας (*timestamp*). Κάθε καταχώρηση στο καθολικό χαρακτηρίζεται ως «συμβάν» (*event*), ενώ όλες οι συναλλαγές διατηρούνται και αποθηκεύονται σε παράλληλη δομή. Η πραγματοποίηση της μετάδοσης και του συγχρονισμού των πληροφοριών πραγματοποιείται με τυχαίο τρόπο μεταξύ των κόμβων, έως ότου έχουν ενημερωθεί όλα τα μέλη του. Η διαδικασία αυτή ονομάζεται «gossip to gossip».

Διατηρώντας αντίγραφο του hashgraph, οι χρήστες έχουν τη δυνατότητα πρόβλεψης των υπολοίπων κόμβων σε μία ενδεχόμενη ψηφοφορία. Η διαδικασία αυτή ονομάζεται εικονική ψηφοφορία (*Virtual Voting*).

4. **Holochain**: Αποτελεί μία από τις πιο πρόσφατες τεχνολογίες αποκεντρωμένου λογισμικού. Στο συγκεκριμένο τύπο DLT, δε χρησιμοποιείται κάποιος μηχανισμός συναίνεσης μεταξύ των κόμβων. Η επικύρωση μπορεί να πραγματοποιηθεί εξατομικευμένα από τον κάθε κόμβο ξεχωριστά, οδηγώντας τον στη διατήρηση του δικού του (μοναδικού) καθολικού. Η μέθοδος αυτή αλλάζει τη δομή διαχείρισης των δεδομένων από δεδομενο-κεντρική (*data-centric structure*), σε

πρακτορο-κεντρική (*agent-centric structure*), καθιστώντας πιο αποτελεσματική και την όλη ενεργειακή διαχείριση του δικτύου.

5. **Tempo (Radix)**: Κάθε κόμβος του δικτύου διατηρεί ένα μέρος του συνολικού «παγκόσμιου καθολικού». Μεταξύ των κόμβων υπάρχει η δυνατότητα ανταλλαγής και συγχρονισμού των διαφορετικών μερών των πληροφοριών που κατέχουν. Η διαδικασία αυτή ονομάζεται «λογικά ρολόγια» (*Logical Clocks*). Αντίθετα, στα υπόλοιπα DLTs χρησιμοποιείται η μέθοδος της χρονοσφραγίδας (*timestamp*), όπου για τη συναίνεση μίας συναλλαγής το σύστημα «θυμάται» τη σειρά με την οποία πραγματοποιήθηκαν οι συναλλαγές.

1.3 Η Τεχνολογία του Blockchain

Όπως είδαμε και παραπάνω εν συντομία, η τεχνολογία του blockchain αποτελεί μία υποκατηγορία προερχόμενη από την τεχνολογία του κατακευκτισμένου καθολικού. Αποτελεί «μία χρονολογική ακολουθία αμετάβλητων αρχείων δεδομένων, τα οποία διαχειρίζεται ένα αποκεντρωμένο σύμπλεγμα (*cluster*) υπολογιστών, ενώ ακολουθούνται συγκεκριμένοι κανόνες κρυπτογράφησης» (Rosic, 2020). Επίσης, πρόκειται για «έναν συνδυασμό προϋπαρχόντων μηχανισμών, όπως το κατακευκτισμένο καθολικό, η ασύμμετρη κρυπτογράφηση και τα δέντρα Merkle, οι οποίοι συνδυάστηκαν με στόχο τη χρησιμοποίησή τους στην υλοποίηση Bitcoin το 2009» (Finck, 2018) (Nakamoto, 2008). Με άλλα λόγια, θα λέγαμε ότι το blockchain είναι μία «ειδική» κατηγορία δεδομένων, η οποία διαφοροποιείται από την παραδοσιακή βάση δεδομένων στον τρόπο με τον οποίο αποθηκεύει τα δεδομένα, ομαδοποιώντας τα σε μπλοκ και συνδέοντάς τα με συγκεκριμένη χρονολογική σειρά.

Στις παραδοσιακές βάσεις δεδομένων, οι χρήστες μπορούν να πραγματοποιήσουν 4 ενέργειες για τη διαχείρισή τους (*Create, Read, Update, Delete* → Δημιουργία, Ανάγνωση, Ενημέρωση, Διαγραφή), μην έχοντας δυνατότητα προβολής του ιστορικού των ενεργειών τροποποίησης που έχουν πραγματοποιήσει σε αυτή. Από τη στιγμή που υπάρχει η επιλογή της μεταβολής ή της διαγραφής των πληροφοριών της βάσης, χωρίς όμως να αντικατοπτρίζεται το ιστορικό των ενεργειών της, προκύπτει ζήτημα διαφάνειας και εμπιστοσύνης στη διαδικασία που ακολουθείται.

Αντίθετα με τις παραδοσιακές βάσεις, η τεχνολογία του blockchain είναι σχεδιασμένη με τέτοιον τρόπο ώστε να επιτρέπει μόνο την προσθήκη νέων στοιχείων χωρίς τη δυνατότητα τροποποίησής τους. Έτσι, το ιστορικό της βάσης παραμένει ορατό και αμετάβλητο για όλους τους χρήστες του, με την αποθήκευση των δεδομένων να πραγματοποιείται με τέτοιο τρόπο ώστε να διασφαλίζεται η ακεραιότητα του δικτύου και να επαληθεύεται εύκολα από τους χρήστες του. Οι όποιες ενημερώσεις κρίνονται απαραίτητες, μπορούν να πραγματοποιηθούν μόνο με την προσθήκη νέων μπλοκ στον υπάρχον δίκτυο.

1.4 Τα δομικά συστατικά στοιχεία (Zheng, Xie, Dai, Chen, & Wang, June 2017)

Κάθε μπλοκ αποτελείται από την **Κεφαλίδα** (*Block Header*) και το **Σώμα** (*Block Body*).

Πιο συγκεκριμένα, κάθε **κεφαλίδα** περιέχει τα εξής συστατικά στοιχεία:

1. Την **έκδοση του Block** (*Block Version*): Δείχνει ποιος αριθμός έκδοσης πρωτοκόλλου ακολουθείται για κάθε μπλοκ. Έχει μέγεθος 4 bytes.

2. Τη **ρίζα ενός δένδρου Merkle** (*Previous Tree - Root Hash*): Περιέχει την αξία των συναρτήσεων κατακερματισμού της ρίζας του δένδρου Merkle που περιέχεται στο συγκεκριμένο μπλοκ.

3. **Χρονοσφραγίδα** (*timestamp*): Τη χρονική στιγμή, με την τρέχουσα ένδειξη να είναι υπό την μορφή ωρών, λεπτών και δευτερολέπτων (με αρχική ημερομηνία την 1η Ιανουαρίου 1970).

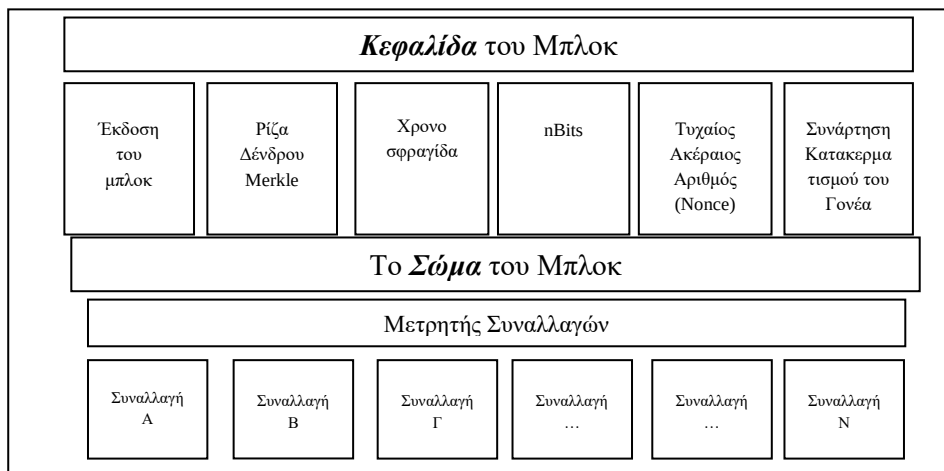
4. **nBits**: Το ανώτερο όριο bit στο οποίο μπορεί να φτάσει μία έγκυρη συνάρτηση κατακερματισμού.

5. **Nonce**: Αποτελεί έναν τυχαίο θετικό ακέραιο αριθμό με μέγεθος 4-bit. Θα μπορούσαμε να τον χαρακτηρίσουμε ως έναν μετρητή, ο οποίος βοηθάει στην εκτέλεση του μηχανισμού συναίνεσης στον αλγόριθμο συναίνεσης.

6. **Συνάρτηση κατακερματισμού του γονέα** (*Parent block hash*): Αποτελεί μία συνάρτηση κατακερματισμού, η οποία συνδέεται με το αμέσως προηγούμενο μπλοκ. Είναι της μορφής των 256-bit.

Το κάθε **σώμα του μπλοκ** αποτελείται από έναν **μετρητή συναλλαγών** (*transaction counter*) και τις **συναλλαγές** (*transactions*). Ο μέγιστος αριθμός των συναλλαγών που μπορεί να έχει το κάθε μπλοκ εξαρτάται από το μέγεθος και τον όγκο πληροφοριών της κάθε συναλλαγής, καθώς και από το μέγεθος του ίδιου του μπλοκ. Για την επικύρωση της κάθε συναλλαγής γίνεται χρήση της μεθόδου της ασύμμετρης κρυπτογράφησης, ενώ παράλληλα για την επικύρωση χρησιμοποιούνται οι ψηφιακές υπογραφές.

Σχηματικά, τα παραπάνω θα μπορούσαν να αναπαρασταθούν με το ακόλουθο σχήμα:



Σχήμα 1: Η Δομή Ενός Μπλοκ (Zheng, Xie, Dai, Chen, & Wang, June 2017)

1.5 Η διαδικασία δημιουργίας ενός Μπλοκ

Για να δημιουργηθεί και να προστεθεί ένα επιπλέον μπλοκ στην υπάρχουσα αλυσίδα, ακολουθείται η εξής διαδικασία¹:

1. Το αίτημα για συναλλαγή: Αρχή της διαδικασίας αποτελεί η δημιουργία αιτήματος συναλλαγής το οποίο αφορά κάποια δεδομένα ή πληροφορίες, τις οποίες ένας χρήστης θέλει να διαβιβάσει μέσω του δικτύου στο οποίο συμμετέχει σε κάποιον άλλο χρήστη του.

2. Η δημιουργία του μπλοκ: Για να προχωρήσει η συναλλαγή, απαιτείται η δημιουργία ενός καινούργιου μπλοκ, το οποίο θα περιέχει τις πληροφορίες ή τα δεδομένα στα οποία θα πραγματοποιηθεί η συναλλαγή.

3. Η γνωστοποίηση του μπλοκ: Το νέο μπλοκ γνωστοποιείται στους υπόλοιπους κόμβους που συμμετέχουν στο δίκτυο.

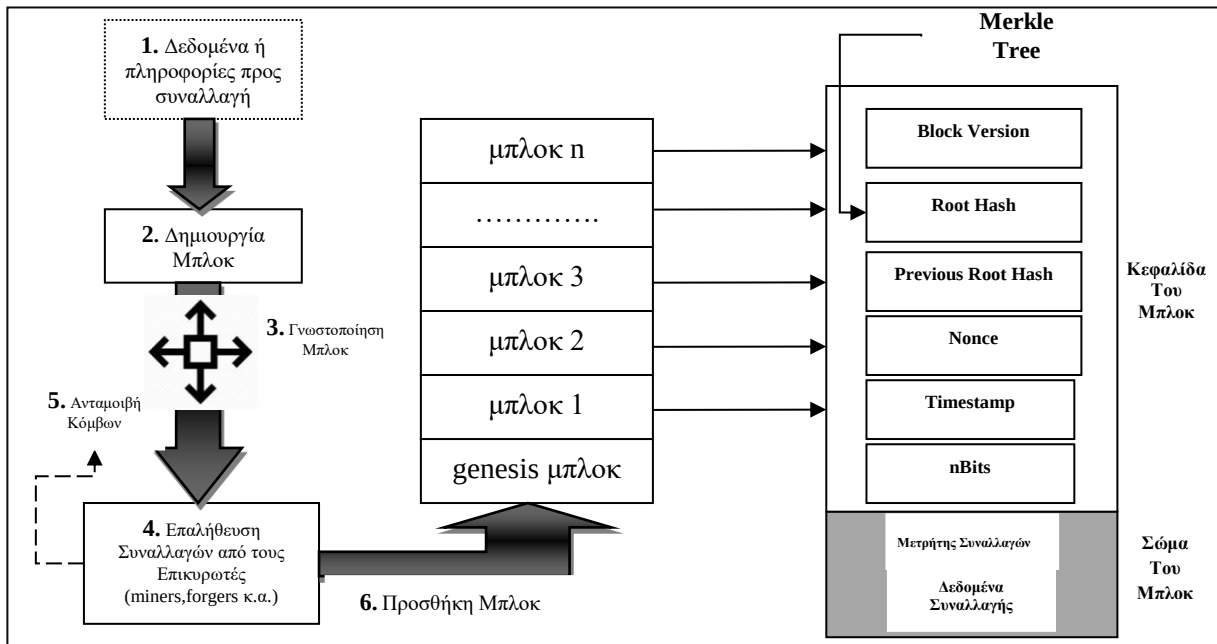
4. Η επικύρωση της συναλλαγής : Οι κόμβοι προχωρούν σε επικύρωση της συναλλαγής των δεδομένων του νέου μπλοκ. Η συμφωνία της επικύρωσης γίνεται με τη χρήση μηχανισμών συναίνεσης (θα τους δούμε πιο αναλυτικά σε επόμενο μέρος της ανάλυσής μας). Στην περίπτωση που πραγματοποιούνται πολλές συναλλαγές ταυτόχρονα, αυτές πρώτα ταξινομούνται με τη σωστή χρονική σειρά, αυτή με την οποία δημιουργήθηκαν, και στη συνέχεια ξεκινάει η διαδικασία επικύρωσής τους.

5. Η ανταμοιβή: Παράλληλα με την επικύρωση της συναλλαγής, οι κόμβοι οι οποίοι βοήθησαν στην δημιουργία του νέου εγκεκριμένου μπλοκ, λαμβάνουν ως ανταμοιβή ένα ποσό (συνήθως προκαθορισμένο), το οποίο διαμοιράζεται ανάλογα με το ποσοστό συνεισφοράς τους στην διαδικασία δημιουργίας του. Για παράδειγμα, στο Bitcoin οι δημιουργοί ενός νέου μπλοκ (*miners*) λαμβάνουν 6.25 BTC για την δημιουργία κάθε νέου μπλοκ (Φεβρουάριος 2021).

6. Η προσθήκη του καινούργιου μπλοκ: Το νέο μπλοκ προστίθεται στην υπάρχουσα αλυσίδα με τους κόμβους να ανανεώνουν (άμεσα) το καθολικό τους προσθέτοντάς το στην αλυσίδα τους. Με την επιβεβαίωση της ορθής διαδικασίας, πραγματοποιείται η ομαδοποίηση των μπλοκ με την αντίστοιχη χρονολογική σειρά.

¹ Εξάιρεση αποτελεί η δημιουργία του πρώτου μπλοκ της αλυσίδας, το οποίο ονομάζεται το μπλοκ της γένεσης (“genesis block” ή “Block 0”). Αποτελεί τη βάση για την αρχή της δημιουργίας της αλυσίδας των συναλλαγών στο δίκτυο.

Ακολουθεί μία σχηματική αναπαράσταση, στην οποία περιγράφεται η διαδικασία της δημιουργίας και προσθήκης ενός νέου μπλοκ στο blockchain:



Σχήμα 2 : Διαδικασία Δημιουργίας και Προσθήκης ενός Μπλοκ στην Αλυσίδα

1.6 Βασικές Ιδιότητες ενός Blockchain

(Ehmke, Blum, & Gruhn, 2019) (Zheng, Xie, Dai, Chen, & Wang, June 2017) (Finck, 2018)

Όπως αναφέρθηκε και σε προηγούμενο μέρος της ανάλυσής μας, η τεχνολογία του blockchain αποτελεί μία υποκατηγορία των αποκεντρωμένων τεχνολογιών κατακεντρωμένου λογισμικού. Από τη δημοσιοποίηση του Bitcoin έχουν ήδη παρέλθει 10 και πλέον χρόνια, καθιστώντας ενδεχομένως ανώριμες τις συνθήκες για τον σαφή ορισμό και την «οριστικοποίηση» της χρησιμοποιούμενης ορολογίας και των ιδιοτήτων που εσωκλείονται στην συγκεκριμένη τεχνολογία. Πολλοί συγγραφείς χρησιμοποιούν διαφορετικές λέξεις για να περιγράψουν τις ίδιες ιδιότητες που χαρακτηρίζουν ένα blockchain. Παρ' όλη, λοιπόν, την ενδεχόμενη ασάφεια, εμείς θα επιχειρήσουμε να τις δούμε παρακάτω.

Έτσι, οι βασικές ιδιότητες ενός blockchain θα μπορούσαν να συνοψιστούν στις εξής:

1. Αμεταβλητότητα (Immutability): Από τη στιγμή που θα υπάρξει συμφωνία μεταξύ των κόμβων και το νέο μπλοκ θα προστεθεί στο υπάρχον καθολικό του δικτύου, δεν υπάρχει δυνατότητα οποιασδήποτε τροποποίησης ή μεταβολής των δεδομένων του. Με τον τρόπο αυτό, οι συμφωνημένες πληροφορίες διαμοιράζονται στους κόμβους που συμμετέχουν, χωρίς καμία πιθανότητα μελλοντικής αλλαγής, διασφαλίζοντας έτσι την ακεραιότητα του δικτύου.

2. Μη αναστρεψιμότητα (Irreversible): Όπως αναφέρθηκε και παραπάνω, από τη στιγμή που θα προστεθεί ένα μπλοκ στο καθολικό του δικτύου, δεν υπάρχει η επιλογή της αντιστροφής αυτής της ενέργειας από τους χρήστες του.

3. Κατανεμημένο Καθολικό (Distributed Ledger): Τα δεδομένα και οι πληροφορίες της αλυσίδας θα πρέπει να είναι διαμοιρασμένα μέσω αντιγράφων τους σε όλους τους συμμετέχοντες του δικτύου.

4. Αποκεντρωμένη Τεχνολογία (Decentralized Technology): Στην υπάρχουσα βιβλιογραφία -πολλές φορές λανθασμένα- ταυτίζονται οι έννοιες του «κατανεμημένου» (*distributed*) και του «αποκεντρωμένου» (*decentralized*) καθολικού. Η ανάγκη της «αποκέντρωσης» δεδομένων ή πληροφοριών προέκυψε από την κακή διαχείρισή τους μέσω της συγκέντρωσης και του ελέγχου τους από όλο και λιγότερους κόμβους. Παράλληλα, από πολλούς τέθηκαν ζητήματα σχετικά με το κατά πόσο η χρήση τους είναι ελεύθερη. Αυτή ακριβώς την ανάγκη ήρθε να καλύψει η τεχνολογία του blockchain, στην οποία καταργείται η κεντρική διαχείριση των δεδομένων.

5. Ανθεκτικότητα (Resilient): Η αποκεντρωμένη λειτουργία των κόμβων τους επιτρέπει να δρουν ως ξεχωριστά μεμονωμένα δίκτυα, διευκολύνοντας την εύρυθμη συνέχιση της λειτουργίας του δικτύου, ακόμη και σε ενδεχόμενα σφάλματα ή προβλήματα μερικών εξ αυτών (των κόμβων). Αντιθέτως, στα δίκτυα υπό κεντρική διαχείριση κάτι τέτοιο δεν μπορεί να συμβεί και, συνεπώς, οδηγείται σε αποτυχία όλο το δίκτυο.

Κατά πολλούς, ακόμη δύο όροι προστίθενται στις ιδιότητες ενός blockchain: η **ανωνυμία** (*anonymity*) και η **διαφάνεια** (*transparency*).

Για την περίπτωση της **ανωνυμίας** και το κατά πόσον αποτελεί ιδιότητα της τεχνολογίας του blockchain, η λανθασμένη προσέγγιση ξεκίνησε από το γεγονός ότι, ενώ ο S. Nakamoto στο *White Paper* μιλούσε για τη διαδικασία της ψευδωνυμοποίησης (*pseudonymity*), πολλοί θεώρησαν εσφαλμένα ότι μιλούσε για τη διαδικασία της ανωνυμοποίησης.

Στην περίπτωση της εξέτασης της διαφάνειας ως επιπλέον ιδιότητας, θα λέγαμε ότι αυτή ήδη εμπεριέχεται, υπό μία έννοια, σε αρκετές από τις προαναφερθείσες ιδιότητες (1,3 και 4). Συνεπώς, θα αποτελούσε πλεονασμό η εκ νέου αναφορά σε μία ταυτόσημη έννοια, η οποία ήδη υπάρχει.

1.7 Ταξινόμηση των Blockchain

Τα Blockchain διαχωρίζονται ανάλογα με τη χρήση τους και τα πεδία εφαρμογής στις εξής κατηγορίες:

1. Δημόσιο Blockchain (Public Blockchain): Η συμμετοχή είναι ελεύθερη με τον κάθε χρήστη να έχει πρόσβαση στις πληροφορίες όλου του κόμβου καθώς και να συμμετέχει ενεργά στη διαμόρφωση και τη λήψη των αποφάσεων μέσω των αντίστοιχων μηχανισμών συναίνεσης. Εξαιτίας της πλήρους αποκεντρωμένης φύσης της βάσης δεδομένων, η λειτουργία του θεωρείται ασφαλής, με μία πιθανή τροποποίησή τους να μοιάζει σχεδόν αδύνατη. Ο μεγάλος αριθμός των κόμβων έχει ως αποτέλεσμα η μετάδοση των πληροφοριών να καθυστερεί περισσότερο και έτσι η αποτελεσματικότητα και η απόκριση του δικτύου κινείται σε χαμηλά (μη ικανοποιητικά πολλές φορές) επίπεδα.

2. Ιδιωτικό Blockchain (Private Blockchain): Ο έλεγχος του blockchain βρίσκεται συγκεντρωμένος στα χέρια ενός ατόμου (π.χ. ενός οργανισμού ή μίας ομάδας

χρηστών), με την πρόσβαση στα δεδομένα να απαιτεί έγκριση από κάποιον/ους «διαχειριστή» τους. Ο αριθμός των συμμετεχόντων στο δίκτυο μειώνεται δραστικά σε σύγκριση με την περίπτωση του δημόσιου blockchain. Το γεγονός αυτό καθιστά περισσότερο πιθανή μία ενδεχόμενη τροποποίηση των δεδομένων τους. Στα θετικά στοιχεία είναι ότι ο μικρός αριθμός των κόμβων του καθιστά αποτελεσματικότερη τη λειτουργία του δικτύου, με πολύ ταχύτερη απόκριση σε τροποποιήσεις και αλλαγές του καθολικού στα δεδομένα του.

3. Υβριδικό Blockchain (Hybrid / Consortium Blockchain): Το υβριδικό blockchain αποτελεί έναν συνδυασμό του δημοσίου και του ιδιωτικού blockchain. Παρά το γεγονός ότι η πρόσβαση στη βάση δεδομένων είναι συνήθως ελεγχόμενη, εξακολουθεί να διατηρεί τα βασικά πλεονεκτήματα που υπάρχουν στη δημόσια αλυσίδα (ακεραιότητα, διαφάνεια, ασφάλεια). Η αρχιτεκτονική του συγκεκριμένου μοντέλου προσαρμόζεται ανάλογα με τις απαιτήσεις και τα αποτελέσματα τα οποία θέλει να πετύχει. Οι κόμβοι του μπορούν να αποφασίσουν ποιες συναλλαγές θα είναι ορατές στους χρήστες τους, προσθαφαιρώντας παράλληλα τον αριθμό των συμμετεχόντων. Θα μπορούσαμε να πούμε να πούμε ότι στο υβριδικό blockchain συνδυάζονται τα καλύτερα στοιχεία του ιδιωτικού και του δημόσιου blockchain.

Τα παραπάνω θα μπορούσαν να συνοψιστούν στο εξής συγκεντρωτικό πίνακα:

	Δημόσιο Blockchain	Ιδιωτικό Blockchain	Υβριδικό Blockchain
Διαδικασία Συναίνεσης	Από όλους τους συμμετέχοντες στην διαδικασία της εξόρυξης (miners)	Μία οντότητα (π.χ. ένας οργανισμός)	Επιλεγμένος - προκαθορισμένος αριθμός κόμβων
Αριθμός Κόμβων	Μεγάλος	Μικρός	Μικρός
Δυνατότητα Προσθήκης Δεδομένων	Ναι ή Με εξουσιοδότηση	Προκαθορισμένη	Προκαθορισμένη
Ανάγνωση Δεδομένων	Ελεύθερη Για Όλους	Ελεύθερη ή περιορισμένη	Ελεύθερη ή περιορισμένη
Αποτελεσματικότητα Δικτύου	Χαμηλή	Υψηλή	Υψηλή
Κεντρική Διαχείριση	Όχι (θεωρητικά)	Ναι	Μερική (ελεγχόμενη)
Ασφάλεια Δικτύου	Σχεδόν Αδύνατο Να Παραβιαστεί	Μπορεί Να Παραβιαστεί	Μπορεί Να Παραβιαστεί
Τρόπος Συναίνεσης	Χωρίς Άδεια Πρόσβασης	Με Άδεια Πρόσβασης	Με Άδεια Πρόσβασης
Εμπιστοσύνη Μεταξύ Των Χρηστών	Όχι	Ναι	Ναι
Μηχανισμός Παροχής Κινήτρων	Ναι	Όχι / Ενδεχομένως	Όχι / Ενδεχομένως

Πίνακας 1 : Ταξινόμηση Μεταξύ των Blockchain (Shahaab, Lidgely, Hewage, & Khan, 2019)

1.8 Μηχανισμοί Συναίνεσης (Consensus Mechanisms)

Σε ένα αποκεντρωμένο περιβάλλον, όπου οι μεσάζοντες έχουν καταργηθεί, η συναίνεση μεταξύ των κόμβων αποτελεί το στοιχείο εκείνο με το οποίο μπορεί να διασφαλιστεί η επικύρωση των συναλλαγών εντός του δικτύου. Για παράδειγμα, στην περίπτωση των χρηματοπιστωτικών συναλλαγών, η διαδικασία αυτή κρίνεται απαραίτητη γιατί πρέπει να αποφευχθεί το λεγόμενο «διπλό ξόδεμα» των δεδομένων

τα οποία θα εγγραφούν στο καθολικό του κόμβου, αποτελώντας τη βάση των συναλλαγών.

Ανάλογα με την περίπτωση, υπάρχουν μηχανισμοί συναίνεσης οι οποίοι ταιριάζουν περισσότερο εν συγκρίσει με άλλους. Η απόφαση της χρησιμοποίησης ενός συγκεκριμένου μηχανισμού επηρεάζει τις λειτουργίες του κόμβου (π.χ. ταχύτητα, ασφάλεια, αποτελεσματικότητα κ.ά.). Η ειδοποιός διαφορά ανάμεσα στους διαφορετικούς μηχανισμούς συναίνεσης είναι ο τρόπος με τον οποίο αναθέτουν και ανταμείβουν τις συναλλαγές που πραγματοποιούνται.

Τα τελευταία χρόνια έχουν προστεθεί αρκετοί νέοι μηχανισμοί συναίνεσης, με τον αριθμό τους μέχρι στιγμής να έχει φτάσει σε αρκετές δεκάδες (Shahaab, Lidgley, Hewage, & Khan, 2019). Εμείς θα αναφερθούμε στους πιο σημαντικούς από αυτούς:

- **Proof of Work (PoW)** (Bach, Mihaljevic, & Zagar, 2018): Αποτελεί τον πιο διαδεδομένο μηχανισμό συναίνεσης, ο οποίος χρησιμοποιήθηκε επιτυχώς τόσο στο Bitcoin όσο και στο Ethereum. Βασίζεται στην υπολογιστική ισχύ των χρηστών, οι οποίοι αποκαλούνται «μεταλλωρύχοι» (*miners*), προσπαθώντας να λύσουν μία αλγοριθμική συνάρτηση υπό την ονομασία συνάρτηση κατακερματισμού (*hash function*). Ο κάθε «miner» στο δίκτυο προσπαθεί να υπολογίσει τη συνάρτηση κατακερματισμού της Κεφαλίδας του μπλοκ (αναφερθήκαμε και σε προηγούμενο μέρος της ανάλυσης).

Τα τρία βασικά συστατικά που απαιτούνται για την εύρεση της συνάρτησης είναι τα εξής:

- α. ένας τυχαίος ακέραιος αριθμός (*nonce*), διαφορετικός κάθε φορά,
- β. τα δεδομένα της συναλλαγής,
- γ. μία συνάρτηση κατακερματισμού (συνδέεται και με τα προηγούμενα block)

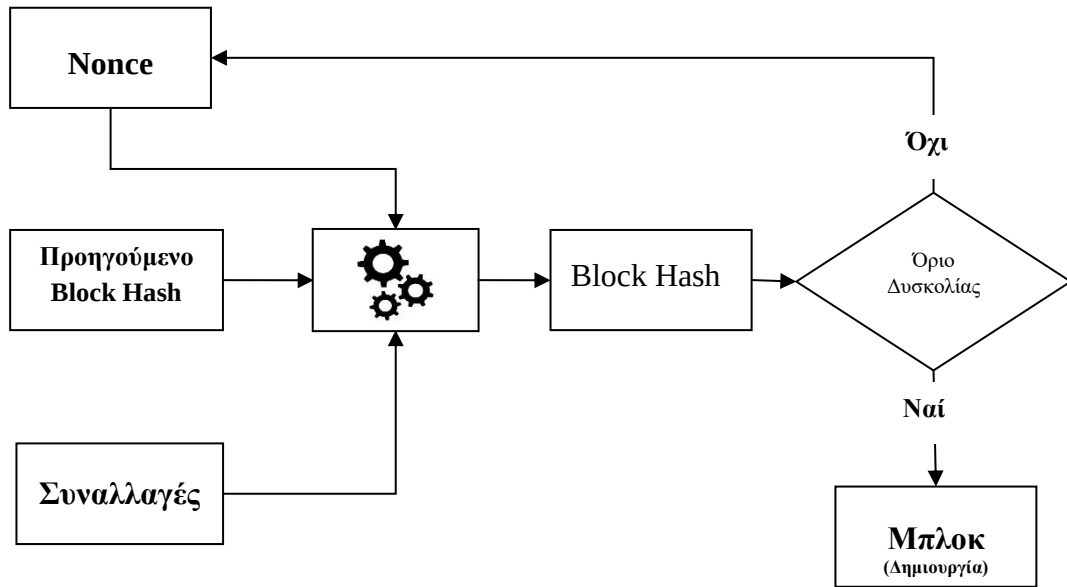
Αυτά τα τρία στοιχεία συνδυάζονται συνεχώς, με τον τυχαίο αριθμό να μεταβάλλεται μέχρις ότου η αξία της συνάρτησης κατακερματισμού που θα παραχθεί να είναι ίση ή μικρότερη από τη «στοχευμένη αξία» (*target value*)². Όταν, λοιπόν, ένας miner φτάσει στη «στοχευμένη αξία» της συνάρτησης κατακερματισμού, θα αναμεταδώσει το μπλοκ στους υπολοίπους, οι οποίοι με τη σειρά τους θα πρέπει να συμφωνήσουν για την «ορθότητά» της. Σε περίπτωση που εγκριθεί η εγκυρότητα του κόμβου, οι υπόλοιποι miners θα προσθέσουν το νέο μπλοκ και στις δικές τους αλυσίδες.

Θα πρέπει να σημειωθεί ότι στην περίπτωση των αποκεντρωμένων δικτύων, επειδή η αναζήτηση της λύσης πραγματοποιείται την ίδια στιγμή από πολλούς κόμβους - miners, είναι δυνατόν να παραχθούν περισσότεροι του ενός τυχαίοι αριθμοί (*nonce*). Ωστόσο, είναι εξαιρετικά απίθανο δύο (ή και περισσότερα) διαφορετικά παρακλάδια του κόμβου να παραχθούν ταυτόχρονα. Για το μηχανισμό συναίνεσης του PoW, έγκυρη θεωρείται η αλυσίδα που αποτελείται από τα περισσότερα μέρη - κλαδιά.

Ένα απλό παράδειγμα με το οποίο θα μπορούσε να γίνει κατανοητή η διαδικασία που περιγράφηκε προηγουμένως αποτελεί η εύρεση του κωδικού μίας κλειδαριάς. Όσο δύσκολη διαδικασία είναι η εύρεση του συνδυασμού - κωδικού της,

² Στην συγκεκριμένη περίπτωση, η «στοχευμένη αξία» (*target value*) είναι ένας αλγόριθμος SHA-256 με πολλά μηδενικά και τη δυσκολία ο στόχος να προσαρμόζεται κάθε 2016 μπλοκ. Για την περίπτωση του Blockchain, στόχος είναι η δημιουργία του κάθε μπλοκ να πραγματοποιείται κάθε 10 λεπτά.

τόσο εύκολη γίνεται η επιβεβαίωση του κωδικού από τη στιγμή που θα βρεθεί.

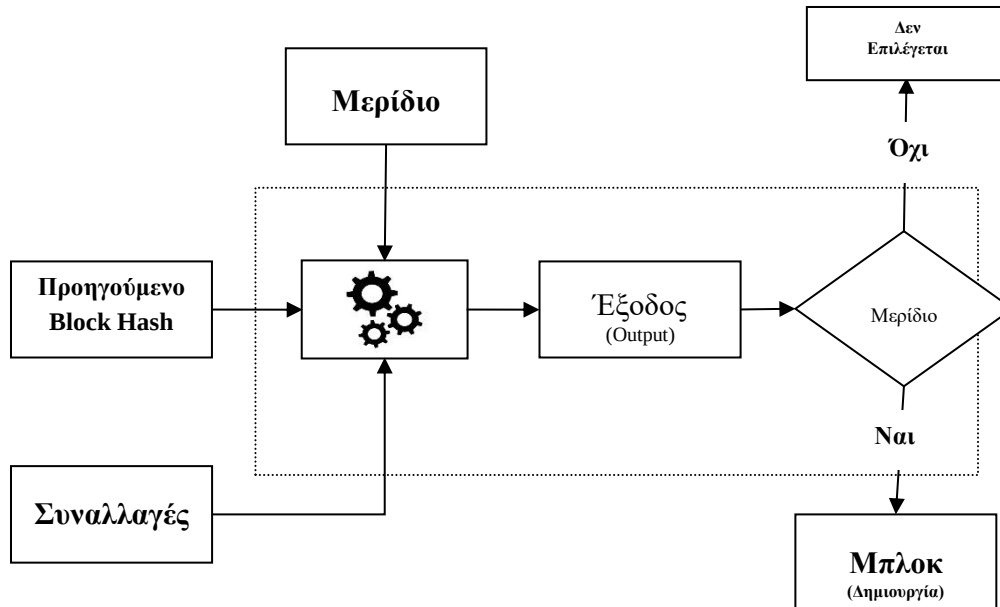


Διάγραμμα 1: η Ποί Proof of Work
(Natoli, Gramoli, & Esteves-Verissimo, August 2019)

- **Proof of Stake (PoS):** Για την περίπτωση του Proof of Stake, οι miners αντικαθίστανται από τους «επικυρωτές» (*validators*), ενώ η διαδικασία δημιουργίας του νέου μπλοκ ονομάζεται «σφυρηλάτηση» (*forging*). Η ανάγκη δημιουργίας του προέκυψε ύστερα από την προσπάθεια περιορισμού της χρησιμοποιούμενης ενέργειας κατά τη δημιουργία ενός μπλοκ στο Proof Of Work.

Εφόσον ένας χρήστης επιθυμεί να συμμετάσχει στη διαδικασία επιλογής του νέου μπλοκ, θα πρέπει να καταθέσει μία «εγγύηση», η οποία αποθηκεύεται σε μία κοινόχρηστη «δεξαμενή» (*pool*) και ονομάζεται ποντάρισμα (*staking*). Εν συνεχεία, ένας αλγόριθμος αναθέτει τυχαία (*pseudo randomly*) τη δημιουργία του επόμενου μπλοκ σε έναν «επικυρωτή» με το χρονικό διάστημα ανάθεσης να είναι εξ αρχής προκαθορισμένο. Το συγκεκριμένο μπλοκ θα πρέπει να συνδέεται με ένα προηγούμενο μπλοκ, το οποίο συνήθως είναι αυτό που έχει τη μεγαλύτερη αλυσίδα. Με την πάροδο του χρόνου τα μπλοκ συγκλίνουν και προστίθενται σε μία ενιαία ακολουθία η οποία αυξάνεται. Το τελευταίο βήμα, αποτελεί η επιβεβαίωση της συναλλαγής από τους υπόλοιπους «επικυρωτές» του κόμβου. Με την ολοκλήρωση της επιβεβαίωσης, τους επιστρέφεται η εγγύηση που είχαν καταθέσει στην αρχή της διαδικασίας συν την ανταμοιβή τους από τη δημιουργία του νέου μπλοκ.

Για την περίπτωση κατά την οποία άποιος «επικυρωτής» δράσει κακόβουλα στη δημιουργία του νέου μπλοκ επικυρώνοντας «δόλιες» συναλλαγές (*fraudulent*), αυτομάτως χάνει το μερίδιο που έχει καταθέσει ως αρχική εγγύηση καθώς και το δικαίωμά του για δημιουργία των μελλοντικών μπλοκ. Με τον τρόπο αυτό επιχειρείται να διασφαλιστεί η φερεγγυότητα της ορθής λειτουργίας του συγκεκριμένου μηχανισμού.



Διάγραμμα 2: η Ποί Proof of Stake
(Natoli, Gramoli, & Esteves-Verissimo, August 2019)

- **Practical Byzantine Fault Tolerance (pBFT)** (Sukhwani, Martinez, Chang, & Trivedi, September 2017): Πρόκειται για ένα permissioned blockchain, στο οποίο όλοι οι κόμβοι «γνωρίζονται» μεταξύ τους. Κάθε κόμβος που συμμετέχει αποτελεί έναν «ομότιμο επικυρωτή» (validating peer) και ένας εξ αυτών επιλέγεται ως ο **αρχηγός** τους (leader node).

Λαμβάνει ως βασική υπόθεση την ύπαρξη «ανεξάρτητων» κακόβουλων κόμβων, οι οποίοι δεν μπορούν να είναι ίσοι ή να ξεπερνούν το 1/3 του συνολικού αριθμού των κόμβων που υπάρχουν στο δίκτυο. Όσο αυξάνεται ο αριθμός των κόμβων που συμμετέχουν τόσο μικρότερη είναι η πιθανότητα να πλησιάσουν το όριο των κακόβουλων κόμβων, με τον αλγόριθμο του δικτύου να δείχνει λειτουργικός και αποτελεσματικός.

Η δημιουργία ενός μπλοκ πραγματοποιείται ανά «γύρο» (round) και ολοκληρώνεται ύστερα από την υλοποίηση ενός πρωτοκόλλου τριών φάσεων: της **προετοιμασίας**, της **ετοιμασίας** και της **δέσμευσης** (pre-prepared, prepared, commit). Η διαδικασία ξεκινάει με τους πελάτες που επιθυμούν να πραγματοποιήσουν μία συναλλαγή να την αιτούνται μέσω του «ομότιμου επικυρωτή» τους. Εν συνεχεία, ο επικυρωτής πληροφορεί τους υπόλοιπους «συναδέλφους» του, αφού έχει διασφαλίσει την ορθότητα της συναλλαγής. Ύστερα από μερικά δευτερόλεπτα (το οποίο ονομάζεται **διάλλειμα παρτίδας** - batch timeout) ή μετά από έναν ορισμένο αριθμό συναλλαγών που εκκρεμούν (ονομάζεται **μέγεθος παρτίδας** - batch size), ο **αρχηγός** (leader) δημιουργεί το νέο μπλοκ με τις συναλλαγές που εκκρεμούν, τηρώντας τη σειρά τους μέσω της χρονοσφραγίδας που έχουν. Στη συνέχεια, αναμεταδίδει στους υπόλοιπους «επικυρωτές» το υποψήφιο μπλοκ με σκοπό να λάβει τη συναίνεσή τους. Εφόσον τα 2/3 του συνολικού αριθμού των κόμβων (ή και παραπάνω) συμφωνήσουν, κάθε

«ομότιμος επικυρωτής» εκτελεί όλες τις εκκρεμείς συναλλαγές, προσθέτοντάς τις στο ιδιωτικό τους καθολικό ως το επόμενο μπλοκ του δικτύου.

Ακολουθεί ένας συγκριτικός πίνακας των χρησιμοποιούμενων μηχανισμών συναίνεσης:

Ιδιότητα	PoW	PoS	pBFT
Πρόσβαση Κόμβων	Ελεύθερη	Ελεύθερη	Με Άδεια
Εξοικονόμηση Ενέργειας	Όχι	Μερική	Ναι
Επιτρεπόμενο Όριο Δύναμης του Αντιπάλου	Μικρότερο του 25% της υπολογιστικής ισχύος του κόμβου	Λιγότερο από του 51% επί του συνολικού μεριδίου του κόμβου	Λιγότερο από το 33% ύπαρξης κακόβουλων κόμβων
Παράδειγμα	Bitcoin	Peercoin	Hyperledger Fabric

Πίνακας 2 : Σύγκριση των Μηχανισμών Συναίνεσης (Zheng, Xie, Dai, Chen, & Wang, June 2017)

- **Leased Proof Of Stake (LPoS)** (Shahaab, Lidgey, Hewage, & Khan, 2019): Αποτελεί έναν πιο εκτεταμένο μηχανισμό συναίνεσης από αυτόν του PoS, δίνοντας στους χρήστες την δυνατότητα «μίσθωσης» (lease) μεριδίων άλλων χρηστών. Όπως και στο συμβατικό PoS, η επιλογή για τη δημιουργία του επόμενου μπλοκ γίνεται μέσω αλγοριθμικής τυχαίας επιλογής, με τις πιθανότητες να αυξάνονται όσο αυξάνεται το μερίδιο που κατέχει ο κάθε χρήστης. Η αύξηση των πιθανοτήτων εδράζεται στη δυνατότητα χρησιμοποίησης μεριδίου μέσω της μίσθωσης από άλλους κόμβους του δικτύου. Έτσι, εντείνεται ο ανταγωνισμός μεταξύ των κόμβων, αυξάνοντας τις πιθανότητες συμμετοχής από περισσότερους ενδιαφερόμενους και ελαχιστοποιώντας το ενδεχόμενο διαχείρισης ολόκληρου του δικτύου από μία μόνο ομάδα χρηστών. Οι ανταμοιβές που προκύπτουν από τη δημιουργία του μπλοκ διαμοιράζονται μεταξύ των «εκμισθωτών» και των «μισθωτών» του κόμβου.

- **Proof of Importance (PoI)** (Natoli, Gramoli, & Esteves-Verissimo, August 2019): Όπως και προηγουμένως με το LPoS, ο μηχανισμός του PoI αποτελεί μία παραλλαγή του PoS. Για κάθε χρήστη υπάρχει ένας δείκτης σημαντικότητας (importance). Αυτός επηρεάζεται τόσο από το μερίδιο που διατηρεί ο χρήστης στο δίκτυο όσο και από τη δράση του εντός του δικτύου (ενεργή ή παθητική). Η διαδικασία δημιουργίας ενός μπλοκ ονομάζεται «μάζεμα - συγκομιδή» (harvesting), με την επιλογή του κόμβου να γίνεται υπό την προϋπόθεση να πληρούνται οι ελάχιστες απαιτήσεις του μεριδίου, ενώ ταυτόχρονα διατηρείται μία ικανοποιητική «ενεργός» θέση του κόμβου εντός του δικτύου.

1.9 Χρησιμοποιούμενες Τεχνικές Κρυπτογράφησης

A. Συναρτήσεις Σύνοψης ή Συναρτήσεις Κατακερματισμού (hash functions): Αποτελούν μαθηματικές συναρτήσεις οι οποίες έχουν σταθερό μέγεθος χαρακτήρων.

Μπορούν να δεχτούν ως είσοδο τυχαία δεδομένα χωρίς κάποιο προκαθορισμένο αριθμό ή μέγεθος χαρακτήρων, παράγοντας ως έξοδο ένα ακέραιο αριθμό με σταθερό μέγεθος (μεταξύ 32bit και 256bit). Για κάθε είσοδο χαρακτήρων υπάρχει και ένα μοναδιαίο αποτέλεσμα, που σημαίνει διαφορετική συνάρτηση κατακερματισμού.

Είναι μονόπλευρες συναρτήσεις (*one way functions*), με τον υπολογισμό και τη δημιουργία τους να αποτελεί αρκετά εύκολη διαδικασία. Ωστόσο, η αντιστροφή της συνάρτησης και ο επανυπολογισμός των δεδομένων της καθίσταται πρακτικά αδύνατος. Ως καλύτερη επιλογή προκρίνεται μόνο η τυχαία αναζήτηση των δεδομένων εισόδου (*preimage resistance*).

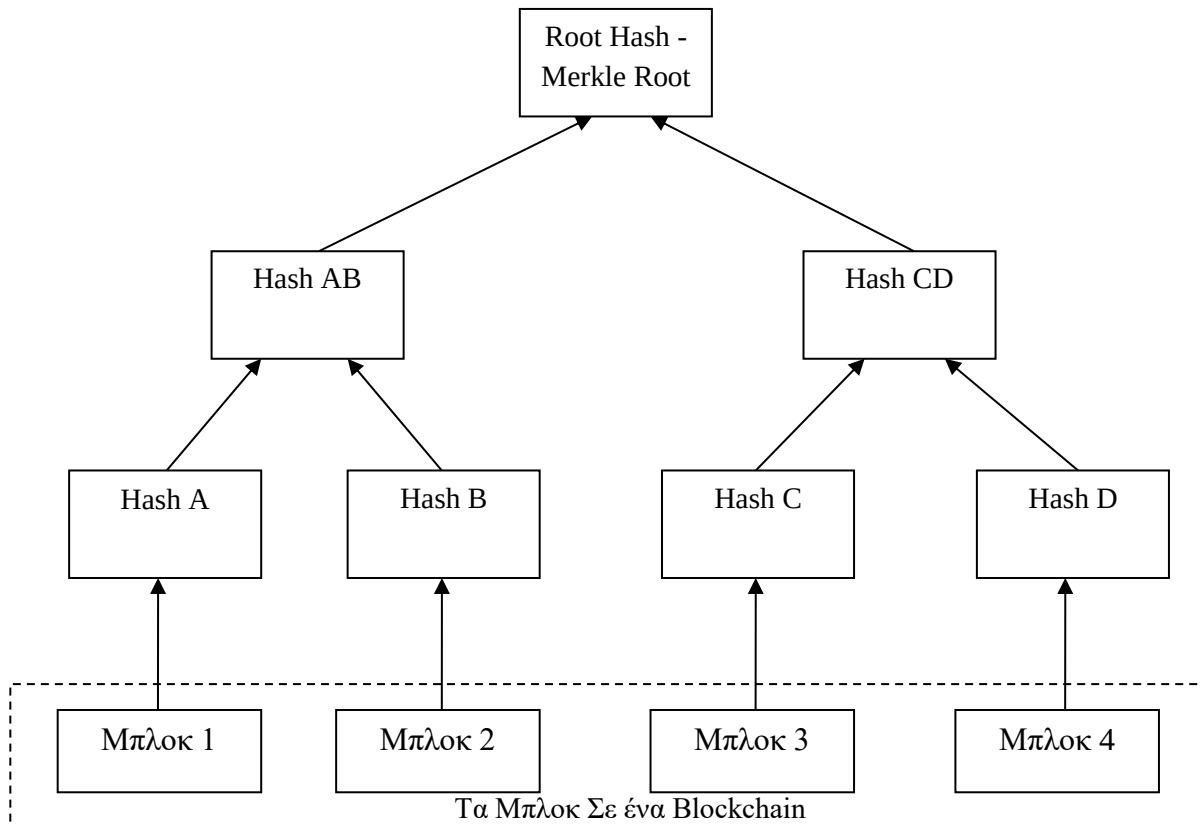
Όπως αναφέραμε και παραπάνω, για κάθε διαφορετική είσοδο υπάρχει και ανάλογη έξοδος δεδομένων, που σημαίνει **διαφορετική συνάρτηση κατακερματισμού** (*collision resistance*). Σε δεδομένα τα οποία διαφέρουν έστω και κατά ένα bit, δημιουργούνται συναρτήσεις κατακερματισμού οι οποίες διαφέρουν, κατά μέσο όρο, κατά τα μισά bits. Έτσι, αποτρέπεται η εξεύρεση των δεδομένων εισόδου μέσω της συνάρτησης κατακερματισμού (**αναρρίχηση στον λόφο - hill climbing**).

Καθίσταται σχεδόν **αδύνατη η εύρεση της ίδιας συνάρτησης κατακερματισμού** με είσοδο από δύο διαφορετικές ομάδες δεδομένων (*2nd preimage resistance*).

B. Δένδρα Merkle (Merkle Tree ή Hash Tree) (Lee & Park, March 2020): Στη συγκεκριμένη μέθοδο, τα δεδομένα χωρίζονται σε δυαδικά δένδρα, στα οποία αναπαράγονται υπολογισμοί περιέχοντες συναρτήσεις κατακερματισμού, μέχρις ότου προκύψει μία μοναδική συνάρτηση, η οποία ονομάζεται ρίζα Merkle.

Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για επαλήθευση και επιβεβαίωση της ακεραιότητας μεγάλου όγκου δεδομένων. Έτσι, όταν υπάρχει μεγάλο όγκος δεδομένων, αυτά μπορούν να διαχωριστούν σε επιμέρους μικρότερα μπλοκ με συγκεκριμένο μέγεθος και να τοποθετηθούν σε αντίστοιχα δυαδικά φύλλα. Εάν προκύψει ανάγκη για μετάδοση ή ανταλλαγή των δεδομένων σε άλλο κόμβο, η ρίζα Merkle εξάγεται ύστερα από την αναμετάδοση των δεδομένων. Στη συνέχεια, η ακεραιότητά τους μπορεί να επιβεβαιωθεί με τη σύγκριση των δύο αξιών. Σε περίπτωση λάθους, έστω και εάν αυτό είναι πολύ μικρό (π.χ. της τάξεως του 1byte), υπάρχει η δυνατότητα άμεσης εύρεσης του μέσω της σύγκρισης των δύο δένδρων. Έτσι, η διόρθωση καθίσταται αποτελεσματικότερη, αφού επικαιροποιούνται μόνο τα σημεία για τα οποία προέκυψαν λάθη.

Σχηματικά ένα **δένδρο Merkle** έχει την εξής μορφή:



Σχήμα 3: Η Δομή ενός Merkle Tree (Gangmax Blog, 2019)

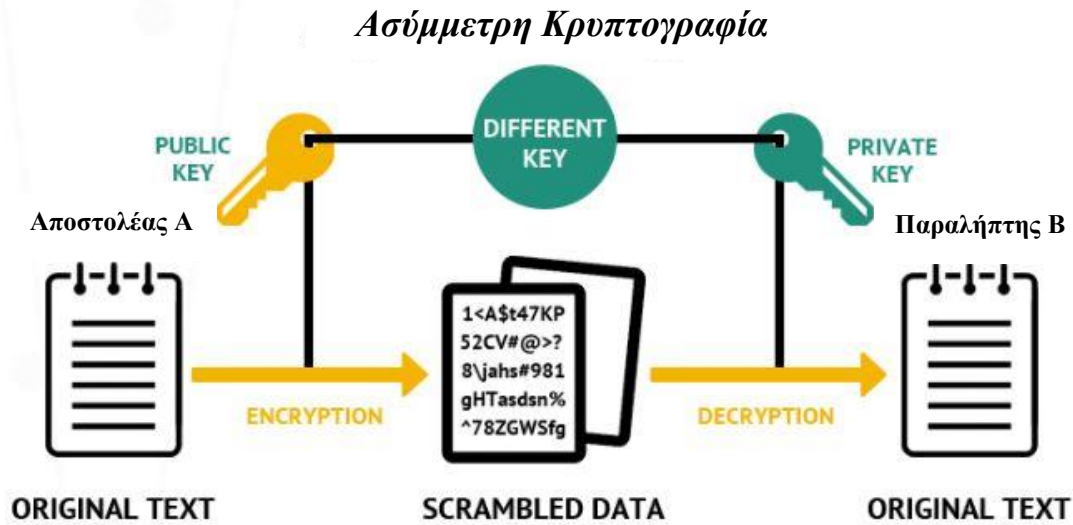
Γ. Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημόσιου Κλειδιού (*asymmetric cryptography*): Βασίζεται στη λογική σύμφωνα με την οποία κάθε χρήστης κατέχει δύο είδη κλειδιών: (α) ένα δημόσιο κλειδί (*public key*), το οποίο γνωστοποιείται σε κάθε ενδιαφερόμενο και (β) ένα ιδιωτικό κλειδί (*private key*), το οποίο είναι κρυφό και γνωρίζει μόνο ο κάτοχός του. Η συσχέτιση μεταξύ των δύο κλειδιών πραγματοποιείται μέσω μονόδρομων συναρτήσεων (*one-way functions – hash functions*).

Για παράδειγμα, ας υποθέσουμε ότι ένας αποστολέας Α επιθυμεί να αποστείλει ένα μήνυμα στον παραλήπτη Β. Έτσι έχουμε:

1. Τα δεδομένα προς αποστολή κρυπτογραφούνται από τον αποστολέα Α με το δημόσιο κλειδί του παραλήπτη και δημιουργείται το κρυπτογραφημένο προς αποστολή μήνυμα.

2. Αποστέλλονται τα δεδομένα στον παραλήπτη Β, ο οποίος τα αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί και εφαρμόζοντας μία αντίστροφη συνάρτηση, η οποία τα ξεκλειδώνει με τη χρήση του κλειδιού.

Σχηματικά, η παραπάνω διαδικασία θα μπορούσε να συνοψιστεί με το εξής σχήμα:



Εικόνα 1 : η Διαδικασία της Ασύμμετρης Κρυπτογράφησης (SSL Shop, 2021)

1.10 Έξυπνα Συμβόλαια (Smart Contracts)

Ο όρος «έξυπνα συμβόλαια» (*smart contracts*) πρωτοεμφανίστηκε τη δεκαετία του 1990 από τον N. Szabo, ο οποίος τα όρισε ως «ένα προκαθορισμένο σύνολο υποσχέσεων σε ψηφιακή μορφή, στο οποίο υπάρχουν πρωτόκολλα όπου εκτελούνται οι δεσμεύσεις από τα συμβαλλόμενα μέρη» (Szabo, 1996). Ένα ενδεικτικό παράδειγμα κατανόησης της λειτουργίας τους αποτελούν τα μηχανήματα αυτόματης πώλησης, τα οποία δέχονται κέρματα ως είσοδο και μέσω του απλού μηχανισμού τους αποδίδουν το επιλεγμένο προϊόν και τα ρέστα ως έξοδο, λαμβάνοντας υπόψη την τιμή του καθενός.

Κατά τον ίδιο, η λειτουργικότητα των *smart contracts* μέσω της εφαρμογής των πρωτοκόλλων κρυπτογράφησης ήταν πολύ καλύτερη εν συγκρίσει με αυτή των παραδοσιακών συμβολαίων σε έντυπη μορφή. Ωστόσο, χρειάστηκε να περάσουν αρκετά χρόνια μέχρι η ιδέα του να γίνει πραγματικότητα και να υλοποιηθεί, με την εμφάνισή τους στις τεχνολογίες κατακεντρωμένου λογισμικού (DLT).

Στην περίπτωση των DLT, τα *smart contracts* «ορίζονται ως τα υπολογιστικά πρωτόκολλα που διευκολύνουν, επαληθεύουν και επιβεβαιώνουν τα ψηφιακά συμβόλαια που υπογράφηκαν μεταξύ δύο ή περισσότερων μερών» (Wang, et al., November 2019).

Η εφαρμογή και υλοποίησή τους στο υπολογιστικό περιβάλλον ενός blockchain παράγει συγκεκριμένα χαρακτηριστικά, τα οποία θα μπορούσαν να συνοψιστούν στα εξής: 1. Είναι ανθεκτικά στις παραβιάσεις (*tamper resistant*). Η εφαρμογή και η επιβεβαίωση του έξυπνου συμβολαίου πραγματοποιείται εντός του blockchain. 2. Η εκτέλεση και η εφαρμογή τους δε χρειάζεται την ύπαρξη μεσαζόντων (*intermediaries*), τελώντας υπό κεντρική διαχείριση. Αντιθέτως μάλιστα, επιτελείται μέσω αποκεντρωμένων και ανώνυμων υπολογιστών κόμβων (αυτονομία - *autonomy*). 3. Όταν πληρούνται οι προκαθορισμένες συνθήκες του συμβολαίου, ενεργοποιείται ο

μηχανισμός των «ψηφιακών αξιών» που εσωκλείονται σε αυτές. Τέτοιο παράδειγμα αποτελεί η μεταφορά κρυπτονομίσματος μεταξύ δύο χρηστών.

Η πρώτη εφαρμογή των smart contract υλοποιήθηκε στο Bitcoin με απλοποιημένη φιλοσοφία, εξαιτίας των περιορισμών στην γλώσσα προγραμματισμού του. Το Ethereum αποτέλεσε την πρώτη δημόσια πλατφόρμα blockchain, η οποία με τη βοήθεια της εικονικής μηχανής που διαθέτει (E.V.M. = Ethereum Virtual Machine) υποστηρίζει πιο «προχωρημένες» μορφές smart contracts. Κάθε κόμβος του δικτύου εκτελεί μία εφαρμογή EVM, όπου με τη σειρά τους εκτελούνται οι προκαθορισμένες εντολές.

Σε αρκετές γλώσσες προγραμματισμού χρησιμοποιούνται τα smart contract (π.χ. Solidity). Το κωδικοποιημένο «έξυπνο συμβόλαιο» μετατρέπεται στην εικονική μηχανή, ενώ στη συνέχεια αξιοποιείται από το blockchain για την εκτέλεση των προκαθορισμένων ενεργειών εντός του δικτύου. Αυτή τη στιγμή, το Ethereum αποτελεί την δημοφιλέστερη πλατφόρμα για την πρακτική υλοποίηση των smart contract. Η χρησιμοποίησή του συντελείται σε ένα ευρύ φάσμα αποκεντρωμένων εφαρμογών (*Decentralized Applications*), όπως για παράδειγμα πλατφόρμες ψηφοφορίας - εκλογών, εφαρμογές διαχείρισης πνευματικών δικαιωμάτων, πλατφόρμες τυχερών παιχνιδιών κ.ά.

Παρά το γεγονός ότι τα **smart contracts** έχουν εξελιχθεί κατά πολύ τα τελευταία χρόνια, υπάρχουν ακόμη πολλά άλματα ζητήματα και προκλήσεις. Ένα πολύ γνωστό συμβάν είναι αυτό που έγινε τον Ιούνιο του 2016, όταν μέσω ενός ιού που «εισχώρησε» στα smart contract του Ethereum (ενός εγχειρήματος υπό την ονομασία Decentralized Autonomous Organization³ που λειτουργούσε τον Απρίλιο του ίδιου έτους), υπεξαيرέθηκαν περισσότερο από 50 εκατομμύρια δολάρια σε αξιακή μορφή Ether (11,5 εκατομμύρια δολάρια εκείνη την περίοδο). Τα χρήματα μεταφέρθηκαν σε ένα παρόμοιο DAO, το οποίο ήταν παρεμφερές, έχοντας την ίδια δομή, με το αυθεντικό. Ως λύση, επιλέχθηκε να εφαρμοστεί η πολιτική του «σκληρού πιρουνιού» (*hard fork*), με τα χρήματα να επιστρέφονται στους κατόχους τους. Παρ' όλα αυτά, για πολλούς αυτή η παρεμβολή αποτέλεσε σαφή παραβίαση των ίδιων των βασικών αρχών της φιλοσοφίας του blockchain, με την **αμεταβλητότητα** (*immutability*) να μην τηρείται και να παραβιάζεται. Ως αποτέλεσμα του όλου ζητήματος που προέκυψε, συντελέστηκε η «διάσπαση» και η δημιουργία δύο διαφορετικών κρυπτονομισμάτων, του Ethereum και του Ethereum Classic.

Παρ' όλες τις μερικές αδυναμίες και αστοχίες, η συνεχόμενη ανάπτυξη της τεχνολογίας του Blockchain έχει ανοίξει διάπλατα το δρόμο για την ανάγκη αξιοποίησης των smart contract. Η επίτευξη της αυτόνομης και αποτελεσματικής λειτουργίας χωρίς μεσάζοντες και η οικοδόμηση εμπιστοσύνης σε ένα μη έμπιστο περιβάλλον αφήνει πολλές υποσχέσεις για το μέλλον. Ο μετασχηματισμός σε τομείς όπως η υγεία, τα χρηματοοικονομικά, το Διαδίκτυο των Πραγμάτων καθώς και άλλους θα πρέπει να θεωρείται σίγουρος και δεδομένος.

³ Το "The Decentralized Autonomous Organization" δημιουργήθηκε τον Απρίλιο του 2016 από μια Γερμανική start-up. Χρησιμοποιούσε Ethereum Blockchain, ενώ είχε ως στόχο τη δημιουργία μίας εταιρίας επιχειρηματικών κεφαλαίων που θα λειτουργούσε αποκλειστικά μέσω των smart contract, χωρίς καμία ανθρώπινη παρέμβαση.

Μέρος 2^ο : Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

2.1 Εισαγωγή – Σύντοπτική Ιστορική Αναδρομή

Η 25η Μαΐου 2018 αποτέλεσε την ημερομηνία εφαρμογής του GDPR (General Data Protection Regulation) για όλα τα κράτη μέλη της ΕΕ. Ο ερχομός του αντικατέστησε την υπ' αριθμόν 95/46/EΚ Κοινοτική Οδηγία, η οποία μέχρι τότε εφαρμόζοταν, επιχειρώντας να προστατεύσει δεδομένα προσωπικού χαρακτήρα εντός των ευρωπαϊκών χωρών. Η ψήφιση της συγκεκριμένης ντιρεκτίβας είχε γίνει το 1995.

Ο νέος **Κανονισμός** λαμβάνει υπ' όψιν του τις βασικές αρχές της προηγούμενης Κοινοτικής Οδηγίας, κάνοντας πιο συγκεκριμένες τις απαιτήσεις για την προστασία των προσωπικών δεδομένων των φυσικών προσώπων, έχοντας ένα ευρύτερο φάσμα επιβολής, ενώ σε περιπτώσεις μη συμμόρφωσης, εφαρμόζονται πολύ αυστηρότερες κυρώσεις για τους παραβάτες του (πρόστιμα). Με τον τρόπο αυτό, τα φυσικά πρόσωπα αποκτούν περισσότερο έλεγχο στον τρόπο επεξεργασίας και διακίνησης των προσωπικών τους δεδομένων από τον εκάστοτε Οργανισμό ή Φορέα, ενώ διατηρούν το δικαίωμα προσφυγής, σε περίπτωση που θεωρούν ότι υπάρχει κάποιου είδους παραβίαση των δικαιωμάτων τους -τα οποία επίσης ρητώς απαριθμούνται στον εν λόγω Κανονισμό.

Ως θεσμικοί θεματοφύλακες για την ορθή εφαρμογή των συγκεκριμένων κανονισμών, ορίζονται οι **υπεύθυνοι επεξεργασίας** και οι **εκτελούντες την επεξεργασία** των δεδομένων. Αξίζει να αναφερθεί ότι, εν συγκρίσει με τα προηγούμενα χρόνια, ο GDPR ξεκαθάρισε και απλοποίησε το ρυθμιστικό περιβάλλον με το οποίο πλέον συμπλέει και το νομικό πλαίσιο προστασίας των δεδομένων και των πληροφοριών των φυσικών προσώπων.

Η επιλογή εφαρμογής του Κανονισμού έναντι των προγενέστερων Κοινοτικών Οδηγιών από μέρους των κρατών-μελών κάθε άλλο παρά τυχαία θα μπορούσε να θεωρηθεί, επικυρώνοντας τη σημασία που διαδραματίζουν τα προσωπικά δεδομένα στη σημερινή εποχή. Ο ΓΚΠΔ, εφαρμόστηκε από όλα τα κράτη-μέλη της ΕΕ χωρίς κάποια επιπλέον επικαιροποίηση ή ανάγκη ψήφισης ξεχωριστών νόμων ανά κράτος. Άλλωστε, ο ΓΚΠΔ, εισήχθη στις εθνικές έννομες τάξεις ως Κανονισμός Αμέσου Εφαρμογής, χωρίς να απαιτείται κάποιο πρόσθετο εθνικό νομοθέτημα για να τεθεί σε ισχύ -με εξαίρεση, βέβαια, τους εθνικούς νόμους που έπονται του GDPR και που αποκλειστικό σκοπό είχαν την ενσωμάτωσή τους με τυπικό και επίσημο τρόπο στην εθνική νομοθεσία των κρατών.

Η ψήφιση και εφαρμογή του Κανονισμού αποτέλεσαν απλώς την επιβεβαίωση μιας μακρόχρονης διαδικασίας των τελευταίων σαράντα και πλέον ετών, η οποία προκύπτει από τη διαχείριση των προσωπικών δεδομένων. Προς την κατεύθυνση αυτή συνέβαλαν καταλυτικά η τεχνολογική ανάπτυξη και η ραγδαία εξάρτηση των ανθρώπων από τους υπολογιστικούς πόρους, συνδέοντας την καθημερινότητά τους ολόένα και περισσότερο με αυτούς.

Το 1970 αποτέλεσε τη χρονιά κατά την οποία η Γερμανία, και συγκεκριμένα το ομοσπονδιακό κρατίδιο του Έσσεν, συνέταξε τον πρώτο νόμο για τα προσωπικά

δεδομένα (θεωρείται ως ο πρώτος νόμος στον κόσμο που εισήγαγε την έννοια των προσωπικών δεδομένων).

Τον Ιανουάριο του 1981 συντάχθηκε και υπογράφηκε η συνθήκη για την προστασία των προσωπικών δεδομένων με ημερομηνία εφαρμογής την 1η Οκτωβρίου 1985. Για την επικύρωση της συμφώνησαν όλα τα τότε μέλη του συμβουλίου της Ευρώπης εκτός της Τουρκίας.

Τον Οκτώβριο του 1995 κρίθηκε αναγκαία η δημιουργία μίας νομοθεσίας, η οποία, σεβόμενη τις θεμελιώδεις αρχές της ελευθερίας και της ιδιωτικότητας, θα συνέβαλλε στην οικονομική και κοινωνική πρόοδο των ατόμων υπερασπιζόμενη τα δικαιώματά τους. Η οδηγία τέθηκε σε ισχύ από το Δεκέμβριο του ίδιου έτους, με τα κράτη-μέλη της ΕΕ να λαμβάνουν χρονικό περιθώριο τριών ετών για την ψήφιση και εφαρμογή του (Οκτώβριος 1998).

Τα χρόνια που ακολούθησαν, υπήρξε ένας εκτεταμένος διάλογος εντός των κόλπων της ΕΕ, ενώ παράλληλα επιχειρήθηκε η διερεύνηση των νέων προκλήσεων που αντιμετώπιζε η καθημερινότητα των πολιτών. Προς αυτή την κατεύθυνση έδρασε καταλυτικά η σύγκλιση των πληροφοριακών και επικοινωνιακών συστημάτων με τη δημιουργία ενός ενιαίου αλληλένδετου παγκοσμιοποιημένου ιστού.

Από το Μάρτιο του 2012 που ξεκίνησε η συζήτηση περί τροποποίησης της Κοινοτικής Οδηγίας, χρειάστηκαν κάτι περισσότερο από τέσσερα χρόνια (Μάιος 2016) μέχρι την οριστικοποίησή της στα κράτη-μέλη της ΕΕ καθώς και στο ευρύτερο κοινό.

2.2 Αντίστοιχοι Κανονισμοί εκτός Ευρώπης (Simmons, 2021) (Lubowicka, 2021)

Ο *Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων* αποτελεί ένα ακόμη εγχείρημα για την προστασία των πληροφοριών των φυσικών προσώπων, προσπαθώντας να «θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας τους στην ίδια την επιχείρηση» (Ομάδα Εργασίας ΣΕΒ, 2018). Κοιτώντας στον παγκόσμιο χάρτη, μπορούμε να βρούμε αρκετά αντίστοιχα παραδείγματα.

Εν συνεχεία, ακολουθούν μερικές ενδεικτικές περιπτώσεις με τις χώρες και τις αντίστοιχες ονομασίες των νόμων:

- **Αυστραλία - The Privacy Act:** Για πρώτη φορά εφαρμόστηκε το 1988. Έκτοτε έχουν πραγματοποιηθεί αρκετές τροποποιήσεις του. Οι κρατικοί φορείς, οι συνεργαζόμενες με το δημόσιο τομέα επιχειρήσεις και οι πάροχοι υπηρεσιών υγείας υποχρεούνται να εφαρμόσουν τις Αρχές Ιδιωτικότητας (*Information Privacy Principles - IPPs*) για τους Αυστραλούς πολίτες σε περιπτώσεις συλλογής και επεξεργασίας των δεδομένων τους.

- **ΗΠΑ (Καλιφόρνια) - California Online Privacy Protection Act (CalOPPA):** Αποτέλεσε την πρώτη πράξη νομοθετικού περιεχομένου στις Ηνωμένες Πολιτείες, υποχρεώνοντας τις ιστοσελίδες σε δημοσιοποίηση των πολιτικών απορρήτου που αφορούν στη διαχείριση και χρησιμοποίηση των προσωπικών δεδομένων των φυσικών προσώπων (2004).

- **Καναδάς - Personal Information Protection and Electronic Documents Act (PIPEDA):** Το συγκεκριμένο νομοθέτημα υποχρεώνει τις επιχειρήσεις που χρησιμοποιούν (ή λαμβάνουν υπόψη) τα δεδομένα των φυσικών προσώπων για

εμπορικές δραστηριότητες, να τους έχουν προηγουμένως ενημερώσει, λαμβάνοντας την αντίστοιχη συγκατάθεση για οποιαδήποτε περαιτέρω επεξεργασία τους.

- **Νότια Αφρική - Protection of Personal Information Act (POPI)**: Ήρθε σε εφαρμογή το 2014, έχοντας νομοθετική ισχύ για όλους τους εγχώριους Οργανισμούς. Θέτει κανόνες λογοδοσίας για την επεξεργασία των προσωπικών δεδομένων (data accountability), αξιώνοντας τη συναίνεση των χρηστών σε περιπτώσεις απευθείας επικοινωνίας για εμπορικούς σκοπούς μέσω στρατηγικών μάρκετινγκ.

- **Σενεγάλη - Data Protection Act**: Υπήρξε η πρώτη αφρικανική χώρα όπου θεσπίστηκε νομοθεσία για την προστασία των προσωπικών δεδομένων (2008) για τις επιχειρήσεις που διατηρούν τα μέσα επεξεργασίας εντός της χώρας. Το πεδίο εφαρμογής της είναι λιγότερο αυστηρό εν συγκρίσει με τον ΓΚΠΔ, με την ισχύ του να αφορά στα προσωπικά δεδομένα που ανταλλάσσονται μεταξύ τρίτων.

- **Βραζιλία - Lei Geral de Proteção de Dados (LGPD)**: Αποτελεί μία από τις πιο πρόσφατες νομοθεσίες που σχετίζονται με την προστασία των προσωπικών δεδομένων, έχοντας ως καταληκτική ημερομηνία εφαρμογής την 18η Σεπτεμβρίου του 2020. Αποτελεί την αντιπρόταση της Βραζιλίας σε σχέση με το ΓΚΠΔ, έχοντας ως στόχο τη δημιουργία ενός νομικού πλαισίου για την επεξεργασία των προσωπικών δεδομένων στον ιδιωτικό και τον δημόσιο τομέα (Iubenda, 2020). Παρ' όλες τις ομοιότητες με τον Ευρωπαϊκό Κανονισμό, υπάρχουν και αρκετές διαφορές, με αρχή τις 10 προκαθορισμένες νομικές βάσεις υπό τις οποίες μπορεί να ξεκινήσει μία επεξεργασία στα προσωπικά δεδομένα των φυσικών προσώπων. Αν και δημιουργήθηκε αργότερα από το ΓΚΠΔ, οι ποινές που προβλέπονται σε περίπτωση παραβίασης (ή μη συμμόρφωσης) είναι πολύ λιγότερο αυστηρές για τους παραβάτες του.

- **Ινδία - Personal Data Protection Bill**: Ύστερα από την επίσημη αναγνώριση της ιδιωτικότητας ως θεμελιώδους ανθρωπίνου δικαιώματος από το Ανώτατο Δικαστήριο της Χώρας (2017), δημιουργήθηκε και ο πρώτος νόμος για την προστασία των προσωπικών δεδομένων (2019). Το νομοθέτημα θέτει συγκεκριμένα πρότυπα για την προστασία των προσωπικών δεδομένων και των πληροφοριών, με ετήσιους υποχρεωτικούς ελέγχους που σχετίζονται με τη διαχείριση και την αποθήκευσή τους.

2.3 Βασικές Οντότητες - Υπό Χρήση Έννοιες του ΓΚΠΔ (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

Πριν προχωρήσουμε στην παρουσίαση των οντοτήτων που αλληλεπιδρούν στο ΓΚΠΔ, είναι σημαντικό να ορίσουμε την έννοια των προσωπικών δεδομένων. Τα **Προσωπικά Δεδομένα** νοούνται ως οι πληροφορίες εκείνες μέσω των οποίων μπορεί να πραγματοποιηθεί η ταυτοποίηση - αναγνώριση ενός φυσικού προσώπου. Εκτός από τις άμεσες πληροφορίες (π.χ. όνομα, επίθετο, ΑΦΜ, αριθμός κοινωνικής ασφάλισης, Ηλικία, Αριθμός Ταυτότητας, χρώμα δέρματος, ηλικία) υπάρχουν και έμμεσες, μέσω των οποίων θα μπορούσε να πραγματοποιηθεί η ταυτοποίηση ενός φυσικού προσώπου (π.χ. πολιτικές πεποιθήσεις, θρησκευτικές πεποιθήσεις, υγεία κ.ά.).

Η επεξεργασία των προσωπικών δεδομένων πραγματοποιείται μέσω της επεξεργασίας τους από μία οντότητα (νομικό ή φυσικό πρόσωπο), με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων, με την εφαρμογή διάφορων τεχνικών (π.χ. διαβίβαση, ανταλλαγή, αποθήκευση, συλλογή, τροποποίηση, εξαγωγή κ.ά.)

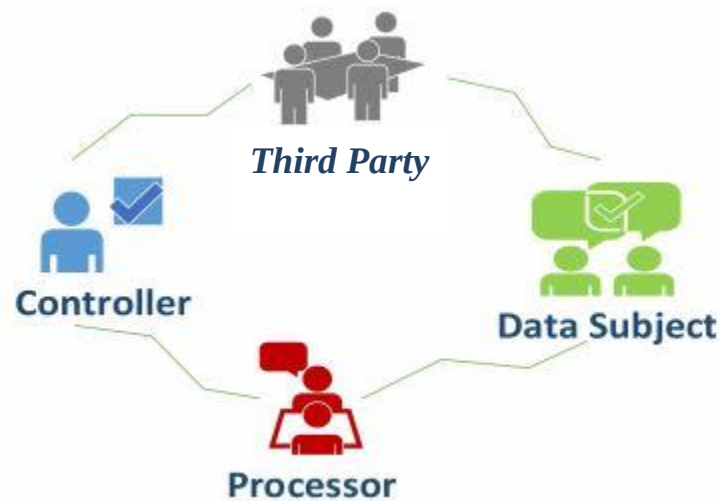
Οι **οντότητες** που αλληλεπιδρούν στον ΓΚΠΔ, είναι οι ακόλουθες:

- Το **Υποκείμενο των Δεδομένων (Data Subject)**: Αποτελεί κάθε φυσικό πρόσωπο μέσω του οποίου η χρήση των προσωπικών δεδομένων μπορεί να γνωστοποιήσει την ταυτότητά του (είτε έμμεσα είτε άμεσα).

- Ο **Υπεύθυνος Επεξεργασίας (Data Controller)**: Αποτελεί οποιοδήποτε φυσικό ή νομικό πρόσωπο το οποίο καθορίζει «τους σκοπούς και τον τρόπο επεξεργασίας» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016) των προσωπικών δεδομένων των υποκειμένων.

- Ο **Εκτελών την Επεξεργασία (Data Processor)**: Πρόκειται για το φυσικό ή νομικό πρόσωπο το οποίο επεξεργάζεται εκ μέρους του **υπευθύνου επεξεργασίας** τα δεδομένα προσωπικού χαρακτήρα.

- **Τρίτος (Third Party)**: Οποιαδήποτε οντότητα (φυσική ή νομική), πλην των τριών προαναφερθέντων, που έχει εγκριθεί να προχωρά σε επεξεργασία των προσωπικών δεδομένων, τελώντας υπό την εποπτεία του υπευθύνου ή του εκτελούντος την επεξεργασία.



Εικόνα 2: Οι οντότητες του GDPR
(Georgiou & Lambrinoudakis, 2020)

Ακολουθούν οι ορισμοί μερικών όρων οι οποίοι θα χρησιμοποιηθούν στη συνέχεια της ανάλυσης μας.

- **Επεξεργασία (processing)**: Οποιαδήποτε ενέργεια σχετίζεται με τη χρησιμοποίηση *προσωπικών δεδομένων*, είτε προκύπτει μέσω αυτοματοποιημένων μεθόδων είτε όχι.

- **Περιορισμός της Επεξεργασίας (restriction of processing)**: Νοείται «η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

- **Κατάρτιση Προφίλ (profiling)**: Είναι η κάθε είδους αυτοματοποιημένη διαδικασία αξιολόγησης των προσωπικών δεδομένων των φυσικών προσώπων με σκοπό τη δημιουργία προβλέψεων που σχετίζονται με αυτά.

- **Ψευδωνυμοποίηση (pseudonymisation)**: Αποτελεί μία τεχνική με βάση την οποία τα προσωπικά δεδομένα των φυσικών προσώπων «καμουφλάρονται» με τέτοιο

τρόπο ώστε «να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016). Να σημειωθεί το γεγονός ότι οι συμπληρωματικές πληροφορίες βρίσκονται φυλαγμένες σε ξεχωριστό μέρος, ενώ είναι διαρθρωμένες με τέτοιο τρόπο (τεχνικό ή οργανωτικό) ώστε να διαφυλάσσεται η μη δυνατότητα συγκεκριμένης ταυτοποίησης.

- **Ανωνυμοποίηση (anonymization)** (Lyons , Courcelas, & Timsit, October 2018): Αποτελεί τη διαδικασία με την οποία αφαιρούνται όλα τα προσωπικά δεδομένα (είτε πρόκειται για άμεσες είτε για έμμεσες πληροφορίες) που μπορούν να οδηγήσουν σε συσχέτιση με το αντίστοιχο φυσικό πρόσωπο. Σε αντίθεση με την ψευδωνυμοποίηση, όπου τα αναγνωριστικά στοιχεία αλλάζουν με τέτοιο τρόπο ώστε να προκύπτει αναγνώριση του αρχικού υποκειμένου με τη βοήθεια και τη χρήση επιπλέον πληροφοριών, η συγκεκριμένη τεχνική καθιστά αδύνατη οποιαδήποτε προσπάθεια ταυτοποίησης και προσδιορισμού του υποκειμένου στο οποίο ανήκουν τα συγκεκριμένα δεδομένα.

- **Σύστημα αρχειοθέτησης (filing system)**: Αποτελεί το χώρο όπου βρίσκονται αποθηκευμένα τα προσωπικά δεδομένα χωρίς να τα επηρεάζει ο τρόπος αποθήκευσής τους (π.χ. αποκεντρωμένα, κατακεντρωμένα, κεντριοποιημένα κ.ά.).

- **Συγκατάθεση (consent)** (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Αναφέρεται στην κάθε είδους ελεύθερη, ρητή και συγκεκριμένη δήλωση επιθυμίας εκ μέρους του υποκειμένου των δεδομένων που δίνει τη συγκατάθεσή του για την επεξεργασία τους (γραπτώς ή προφορικώς).

2.4 Οι Βασικές Αρχές του GDPR (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016)

1. **Νομιμότητα, αντικειμενικότητα και διαφάνεια (Lawfulness, fairness and transparency)** (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Ο εκτελών την επεξεργασία των δεδομένων θα πρέπει να τα επεξεργάζεται με τρόπο σύννομο και διαφανή. Έτσι γίνονται ξεκάθαρες οι βασικές αρχές οι οποίες θα πρέπει να τηρούνται».

2. **Περιορισμός του σκοπού (Purpose Limitation)** (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016) : «Τα προσωπικά δεδομένα θα πρέπει να συλλέγονται για ‘‘συγκεκριμένους, ρητούς και νόμιμους σκοπούς’’ χωρίς κάποια περαιτέρω ενέργεια. Εξαιρούνται ζητήματα τα οποία αφορούν το δημόσιο συμφέρον, την επιστημονική ή ιστορική έρευνα καθώς και στατιστικοί σκοποί».

3. **Ελαχιστοποίηση των δεδομένων (Data Minimization)** (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Τα δεδομένα θα πρέπει να επικεντρώνονται σε εκείνα τα οποία είναι τα αναγκαία προς επεξεργασία και μόνο. Με τον τρόπο αυτό καθορίζεται ένα πιο συγκεκριμένο πλαίσιο το οποίο εφαρμόζεται στην πράξη». Για παράδειγμα θα ήταν παράνομο σε μία παραγγελία πίτσας να ζητηθεί από το «υποκείμενο» να δηλώσει την οικογενειακή του κατάσταση (Lyons , Courcelas, & Timsit, October 2018).

4. Ακρίβεια των δεδομένων (Accuracy) (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Τα προσωπικά δεδομένα των χρηστών (*data subjects*) θα πρέπει να είναι ενημερωμένα και ορθά. Όπου διαπιστώνεται λάθος, ο εκτελών την επεξεργασία τους θα πρέπει να προχωράει είτε σε επικαιροποίηση και διόρθωσή τους είτε σε άμεση διαγραφή τους». Με τον τρόπο αυτό επιτυγχάνεται η ορθότητα και εγκυρότητα των προσωπικών δεδομένων των χρηστών καθ' όλη τη διάρκεια χρησιμοποίησής τους.

5. Αποθηκευτικός Περιορισμός των δεδομένων (Storage Limitation) (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Η διατήρηση των προσωπικών δεδομένων των υποκείμενων θα πρέπει να περιορίζεται μόνο «για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016). Εξαιρέση αποτελεί η διατήρηση δεδομένων που αφορούν το δημόσιο συμφέρον, την επιστημονική ή την ιστορική έρευνα ή άλλους ιστορικούς σκοπούς.

6. Ακεραιότητα και εμπιστευτικότητα (Integrity and Confidentiality) (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Τα προσωπικά δεδομένα θα πρέπει να γίνονται αντικείμενο επεξεργασίας με τρόπο που να θεωρείται ασφαλής, αποφεύγοντας οποιαδήποτε παραποίηση τους». Οι υπεύθυνοι επεξεργασίας θα πρέπει να προστατεύουν να προσωπικά δεδομένα από οποιοδήποτε είδος αλλοίωσης, φθοράς ή απώλειάς τους.

Εν συνεχεία, ακολουθεί μία διαγραμματική απεικόνιση των Βασικών Αρχών του ΓΚΠΔ:



Διάγραμμα 3: οι Βασικές Αρχές του ΓΚΠΔ
(PECB -General Data Protection Regulation, 2017)

Εκτός από τις προαναφερθείσες αρχές από τις οποίες διέπονται τα προσωπικά δεδομένα, έχουμε και την **αρχή της λογοδοσίας (accountability)**, για την οποία ο

υπεύθυνος επεξεργασίας ορίζεται ως το άτομο που «φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016) με τις βασικές αρχές του ΓΚΠΔ.

2.5 Τα δικαιώματα του υποκειμένου των προσωπικών δεδομένων

1. Το δικαίωμα της ενημέρωσης (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Σχετίζεται με την αρχή της διαφάνειας των δεδομένων καθώς και τη σύννομη και θεμιτή επεξεργασία τους. Η συλλογή των προσωπικών δεδομένων μπορεί να πραγματοποιηθεί από το ίδιο το υποκείμενο αλλά και από άλλους (π.χ. ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία τους). Στην περίπτωση αυτή, το υποκείμενο δικαιούται τόσο να ενημερωθεί για τους λόγους της επεξεργασίας τους όσο και να λάβει οποιεσδήποτε περαιτέρω σχετικές πληροφορίες .

2. Το δικαίωμα πρόσβασης (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Τα υποκείμενα επεξεργασίας των δεδομένων έχουν το δικαίωμα να λάβουν επιβεβαίωση για την ενδεχομένη (ή μη) επεξεργασία των πληροφοριών τους». Σε περίπτωση επεξεργασίας των δεδομένων τους, τα υποκείμενα διατηρούν το δικαίωμα της πρόσβασης ως προς τον τρόπο διαχείρισής τους από τους υπευθύνους επεξεργασίας.

3. Το δικαίωμα στη «διόρθωση δεδομένων» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Παρέχεται η δυνατότητα άμεσης διόρθωσης λανθασμένων δεδομένων και πληροφοριών καθώς και συμπληρωματικής προσθήκης για άλλα δεδομένα τα οποία είτε έχουν παραληφθεί είτε δε δόθηκαν προηγουμένως κατά την εισαγωγή τους.

4. Το «δικαίωμα στη λήθη» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Το υποκείμενο επεξεργασίας των δεδομένων του δικαιούται να αιτηθεί την οριστική διαγραφή όλων των δεδομένων που συνδέονται με αυτό, για λόγους οι οποίοι σχετίζονται με τον **Κανονισμό**. Υπάρχουν, ωστόσο, και κάποιοι περιορισμοί του δικαιώματος στη λήθη, όπως είναι η εξυπηρέτηση του δημοσίου συμφέροντος, επιστημονικοί σκοποί ή νομικές αξιώσεις.

5. Το δικαίωμα στον «περιορισμό της επεξεργασίας» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Το υποκείμενο της επεξεργασίας των δεδομένων του μπορεί να αιτηθεί τον περιορισμό της επεξεργασίας αυτής εφόσον ισχύει ένας από τους προκαθορισμένους λόγους του **Κανονισμού** (π.χ. αμφισβήτηση της ακρίβειας των δεδομένων, η επεξεργασία των δεδομένων είναι παράνομη, το υποκείμενο των δεδομένων φέρει αντίρρηση σχετικά με την επεξεργασία τους)

6. Το δικαίωμα της «φορητότητας των δεδομένων» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Το υποκείμενο της επεξεργασίας των δεδομένων του έχει τη δυνατότητα λήψης των προσωπικών του πληροφοριών τα οποία έχει επεξεργαστεί ο υπεύθυνος επεξεργασίας, διαβιβάζοντάς τα σε άλλον υπεύθυνο επεξεργασίας ή όπου αλλού αυτό επιθυμεί.

7. Το δικαίωμα της «αντίρρησης – εναντίωσης» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): Το υποκείμενο της επεξεργασίας των

δεδομένων του έχει το δικαίωμα να αντιτάσσεται «ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

8. Το δικαίωμα αντίρρησης σε περιπτώσεις «αυτοματοποιημένης διαδικασίας για την κατάρτιση προφίλ χρήστη (profiling)» (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016): «Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας» των προσωπικών του δεδομένων (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Μέρος 3^ο: Ενοποιώντας την τεχνολογία του Blockchain με τον ΓΚΠΔ

3.1 Εισαγωγή

Στα προηγούμενα δύο μέρη της ανάλυσής μας επιχειρήσαμε να διερευνήσουμε όσο το δυνατόν πιο διεξοδικά και εμπεριστατωμένα τις έννοιες της τεχνολογίας του blockchain καθώς και αυτές που αφορούν το ΓΚΠΔ. Με τον τρόπο αυτό, ξεκαθαρίστηκαν τα επιμέρους στοιχεία, βοηθώντας μας να προχωρήσουμε στο αμέσως επόμενο στάδιο της ανάλυσης. Σ' αυτό, θα επιχειρήσουμε να διερευνήσουμε κατά πόσον κρίνεται επιτυχημένη μία σύγκλιση μεταξύ των δύο εννοιών, καθώς καθεμία επιτελεί το ρόλο της και αλληλεπιδρούν, με απώτερο στόχο τη συμμόρφωση του ΓΚΠΔ στην τεχνολογία του Blockchain.

Παρ' όλες τις όποιες διαφορές μεταξύ των δύο εννοιών, θα λέγαμε ότι «δεν υπάρχει τεχνολογία η οποία συγκλίνει με την περίπτωση του ΓΚΠΔ. Υπάρχουν μόνο περιπτώσεις και εφαρμογές που συμμορφώνονται με το ΓΚΠΔ» (Lyons , Courcelas, & Timsit, October 2018).

3.2 Τα προβλήματα που δημιουργούνται

Τα **προβλήματα** τα οποία ανακύπτουν μεταξύ του GDPR και του Blockchain θα μπορούσαν να συνοψιστούν στα εξής:

- Στο ΓΚΠΔ υποχρεωτικά θα πρέπει να υπάρχει ένα πρόσωπο (φυσικό ή νομικό), το οποίο είναι υπεύθυνο και υπόλογο για τη διαχείριση των προσωπικών δεδομένων των φυσικών προσώπων. Με βάση τον Κανονισμό, ανεξαρτήτως εάν πρόκειται για τον υπεύθυνο επεξεργασίας ή για τον εκτελούντα την επεξεργασία, πάντα υπάρχει κάποιος στον οποίο τα φυσικά πρόσωπα μπορούν να απευθυνθούν με σκοπό την επιβολή της κείμενης νομοθεσίας ασκώντας τα έννομα δικαιώματά τους για την ορθή εφαρμογή του. Από την άλλη μεριά, όπως είδαμε, η τεχνολογία του Blockchain βασίζεται στην αρχή της αποκέντρωσης, αντικαθιστώντας την κεντρική διαχείριση ενός κόμβου από πολλούς (όμορους) αποκεντρωμένους κόμβους. Η εφαρμογή αυτής της αποκεντρωμένης λογικής καθιστά δύσκολη (έως αδύνατη) την πρακτική εφαρμογή της **«αρχής της λογοδοσίας»** στην οποία στηρίζεται ο ΓΚΠΔ. Εξίσου προβληματική καθίσταται και μία λύση οριζόντιου διαμοιρασμού (συν)ευθύνης για όλους τους (ομότιμους) κόμβους που συμμετέχουν στο δίκτυο. Έτσι, προκύπτει το **πρώτο εμπόδιο** για τη σύγκλιση του Blockchain με το ΓΚΠΔ, το οποίο μπορεί να περιγραφεί ως ο σαφής προσδιορισμός του ατόμου εκείνου που είναι υπεύθυνο για την επεξεργασία των προσωπικών δεδομένων των χρηστών εντός του δικτύου.

- Ένα **δεύτερο εμπόδιο** σχετίζεται με τα άρθρα 16 και 17 του ΓΚΠΔ. Όπως είδαμε και στο δεύτερο μέρος της ανάλυσής μας, σ' αυτά δίνεται η δυνατότητα διόρθωσης ή διαγραφής των προσωπικών δεδομένων των υποκειμένων. Για τις περιπτώσεις κατά τις οποίες τα φυσικά πρόσωπα το επιθυμούν, μπορούν να αιτηθούν την άμεση διόρθωση ή την οριστική διαγραφή ενός μέρους ή όλων των δεδομένων με τα οποία εκείνα συνδέονται ή σχετίζονται. Ωστόσο, στην περίπτωση της τεχνολογίας του Blockchain, κάτι τέτοιο δεν μπορεί να εφαρμοστεί. Όπως αναφέρθηκε και στο

πρώτο μέρος της ανάλυσης, στις τεχνολογίες αποκεντρωμένου λογισμικού οι νέες πληροφορίες ομαδοποιούνται σε μπλοκ, τα οποία εν συνεχεία (μόνο) προστίθενται σε εκείνα που ήδη υπάρχουν (append-only), χωρίς να δίνεται η δυνατότητα διαγραφής ή τροποποίησής τους. Στην περίπτωση κατά την οποία θα προέκυπτε θέμα διόρθωσης ή διαγραφής τους, θα προέκυπτε και αντίστοιχο ζήτημα ακεραιότητας των δεδομένων, το οποίο με τη σειρά του θα έθετε ζήτημα αξιοπιστίας και ακεραιότητας του ίδιου του δικτύου. Έτσι, η δυνατότητα τροποποίησης ή μεταβολής οποιασδήποτε πληροφορίας ολοκληρώνεται πριν από την συμφωνία μεταξύ των κόμβων του δικτύου για την προσθήκη του μπλοκ στην αλυσίδα του δικτύου.

- Ένα **τρίτο εμπόδιο** για τη σύγκλιση μεταξύ του ΓΚΠΔ και της τεχνολογίας του Blockchain, αποτελεί το κατά πόσον τα δεδομένα που αποθηκεύονται εντός της αλυσίδας μπορούν να θεωρούνται προσωπικά ή όχι.

3.3 Προτεινόμενες Τεχνικές Λύσεις

Στη συγκεκριμένη τεχνολογία, υπάρχουν οι εξής τρεις μέθοδοι αποθήκευσης των δεδομένων: η απλή μορφή κειμένου, η κρυπτογραφημένη μορφή και η αποθήκευση μέσω συναρτήσεων κατακερματισμού (Finck, 2018). Η αποθήκευση των προσωπικών δεδομένων σε απλή μορφή κειμένου αντίκειται στις αρχές του Κανονισμού και συνεπώς εξαιρείται οποιασδήποτε περαιτέρω ανάλυσης. Για την περίπτωση της κρυπτογράφησης των δεδομένων, θα μπορούσαμε να πούμε ότι η χρήση των σωστών κλειδιών οδηγεί σε αποκρυπτογράφησή τους και, συνεπώς, δε θα λέγαμε ότι βάσει του Κανονισμού αποτελεί μία σωστή τεχνική ανωνυμοποίησής τους, αλλά περισσότερο πρόκειται για μία τεχνική ψεύδωνυμοποίησης, στην οποία το υποκείμενο δεδομένων μπορεί (έμμεσα) να αναγνωρισθεί. Το ίδιο ισχύει και για την τρίτη μέθοδο αποθήκευσης μέσω των συναρτήσεων κατακερματισμού (hash functions), η οποία λογίζεται και αυτή ως τεχνική ψεύδωνυμοποίησης των δεδομένων, δίνοντας τη δυνατότητα σύνδεσης του υποκειμένου των δεδομένων με τα χρησιμοποιούμενα δεδομένα.

Μία λύση η οποία φαίνεται να επιλύει τα προβλήματα που αναφέρθηκαν παραπάνω είναι η μέθοδος βάσει της οποίας τα προσωπικά δεδομένα που περιέχουν τα αναγνωριστικά στοιχεία (*Personal Identifiable Information*) αποθηκεύονται εκτός αλυσίδας του blockchain και μέσω μίας συνάρτησης κατακερματισμού συνδέονται στο κατακερματισμένο καθολικό. Αν και στην πράξη τα δεδομένα παραμένουν προσωπικά, καθίσταται ευκολότερο να συγκλίνουν με τις προδιαγραφές ασφαλείας του ΓΚΠΔ, περιορίζοντας την αποθήκευση των στοιχείων εντός της αλυσίδας και παρέχοντας πρόσβαση σε χωριστή βάση εκτός της αλυσίδας.

Εφαρμόζοντας την παραπάνω προσέγγιση, «επανενεργοποιείται» η δυνατότητα επιτυχούς διόρθωσης ή διαγραφής των προσωπικών δεδομένων, όπως προβλέπεται στα άρθρα 16 και 17 του ΓΚΠΔ. Παρ' όλα αυτά, μία ενδεχόμενη διαγραφή των προσωπικών δεδομένων εκτός της αλυσίδας θα αφήσει τη συνάρτηση κατακερματισμού, που τα συνδέει εντός, κενή. Έτσι, τίθεται το ζήτημα κατά πόσον η συγκεκριμένη συνάρτηση κατακερματισμού εμπίπτει στην σφαίρα των προσωπικών δεδομένων. Όπως πολύ ορθά προτείνεται σε διάφορες μελέτες, θεμιτό θα ήταν να

δοθούν οδηγίες και περαιτέρω διευκρινίσεις επ' αυτού του ζητήματος (European Parliamentary Research Service, July 2019).

Με βάση τις εκάστοτε κανονιστικές οδηγίες από τις ρυθμιστικές αρχές καθώς και τον τρόπο εφαρμογής τους, έχουν προταθεί διάφορες τεχνικές οι οποίες επιχειρούν να επιλύσουν τα προβλήματα που αναφέραμε προηγουμένως. Τέτοιες είναι οι αποδείξεις μηδενικής γνώσης (Zero Knowledge Proofs), οι κρυφές διευθύνσεις (Stealth Addresses), η ομομορφική κρυπτογράφηση (Homomorphic Encryption), οι κυκλικές υπογραφές (Ring Signatures), οι προσθήκες «θορύβου» (The Addition Of Noise), οι καμουφλαρισμένες συναρτήσεις κατακερματισμού (Chameleon Hashes), καθώς και οι τεχνικές «κλαδέματος» των hash (*Pruning*) (European Parliamentary Research Service, July 2019).

Ακολουθεί μία συνοπτική αναφορά των υπό εξέλιξη προτεινόμενων τεχνικών λύσεων (European Parliamentary Research Service, July 2019):

- **Αποδείξεις μηδενικής γνώσης (Zero Knowledge Proofs):** Παρέχεται πρόσβαση στα προσωπικά στοιχεία μέσω μίας απάντησης σωστού / λάθους, χωρίς να δίνονται οποιεσδήποτε περαιτέρω πληροφορίες. Για παράδειγμα, θα δοθεί απάντηση στην ερώτηση εάν κάποιος είναι άνδρας ή έχει ηλικία άνω των 18 χωρίς να δίνεται κάποια επιπλέον πληροφορία. Με τον τρόπο αυτό αποκαλύπτεται μόνο η πραγματοποίηση μίας ενέργειας, χωρίς να γνωστοποιούνται παραπάνω στοιχεία. Έτσι, επιτυγχάνεται η **ελαχιστοποίηση των δεδομένων** που απαιτούνται για την επιτυχή ολοκλήρωση μίας συναλλαγής.

- **Κρυφές διευθύνσεις (Stealth Addresses):** Αποτελεί μία τεχνική με την οποία επιχειρείται να αποκρυφτεί η ταυτότητα του παραλήπτη σε ένα δημόσιο blockchain, μέσω της χρησιμοποίησης συναρτήσεων κατακερματισμού μίας χρήσης που πραγματοποιείται εντός του δικτύου. Αποτέλεσε μία πρόταση του P. Todd το 2014, βάσει της οποίας οι «ιδιωτικές διευθύνσεις» μίας χρήσης προκύπτουν μέσω του πρωτοκόλλου Diffie-Hellman, με τη χρησιμοποίηση των ελλειπτικών καμπυλών.

- **Ομομορφική Κρυπτογράφηση (Homomorphic Encryption):** Με τη μέθοδο αυτή, επιτρέπεται η επεξεργασία κρυπτογραφημένων δεδομένων σε οποιοδήποτε περιβάλλον (αξιόπιστο ή μη). Όπως και στις άλλες μορφές κρυπτογράφησης (π.χ. ασύμμετρη κρυπτογραφία), υπάρχει ένα (μοναδικό) ιδιωτικό κλειδί μέσω του οποίου αποκρυπτογραφούνται τα δεδομένα και φανερώνεται η αρχική τους μορφή. Η διαφορά του συγκεκριμένου τρόπου κρυπτογράφησης έγκειται στη δυνατότητα εκτέλεσης υπολογισμών και λειτουργιών στα κρυπτογραφημένα δεδομένα από εξουσιοδοτημένους χρήστες με τη χρήση ενός αλγεβρικού υπολογιστικού συστήματος. Όπως φανερώνει και ο μαθηματικός ορισμός, το «ομομορφικό» περιγράφει την τροποποίηση μίας ομάδας δεδομένων (πρώτη ομάδα) εντός μίας άλλης (δεύτερη ομάδα), ενώ παράλληλα οι σχέσεις μεταξύ των δύο αυτών συνόλων δεδομένων συνεχίζονται και ισχύουν.

- **Κυκλικές Υπογραφές (Ring Signatures):** Πρόκειται για μία ομάδα χρηστών που ενώνονται με σκοπό να «μπερδέψουν» την περαιτέρω αναγνώριση ενός συγκεκριμένου κλειδιού από τα μέλη του, η οποία θα οδηγήσει με τη σειρά της σε αποκρυπτογράφηση των δεδομένων. Η αναγνώριση μίας συναλλαγής που ξεκίνησε

από έναν συγκεκριμένο χρήστη της ομάδας καθίσταται σχεδόν αδύνατη, αφού υπάρχουν πολλά ιδιωτικά κλειδιά χωρίς να υπάρχει σαφής τρόπος καθορισμού του συγκεκριμένου κλειδιού με το οποίο πραγματοποιήθηκε η συγκεκριμένη συναλλαγή.

-Προσθήκες «θορύβου» (*The addition of data noise*): Όπως και με τις κυκλικές υπογραφές, στη μέθοδο αυτή πραγματοποιείται ομαδοποίηση αρκετών συναλλαγών με τέτοιο τρόπο ώστε καθίσταται αδύνατη η αναγνώριση τόσο των αποστολέων όσο και των παραληπτών των συναλλαγών αυτών. Αξίζει να αναφερθεί ότι η συγκεκριμένη τεχνική έχει αναγνωριστεί από την Ευρωπαϊκή Επιτροπή Προστασίας Ιδιωτικότητας και Προσωπικών ως μία επιτυχημένη τεχνική ανωνυμοποίησης των προσωπικών δεδομένων, που συμβαδίζει με το ΓΚΠΔ Δεδομένων (Article 29 - Data Protection Working Party, 2014).

-Καμουφλαρισμένες Συναρτήσεις Κατακερματισμού και τα Προσαρμοσμένα Blockchain (*Chameleon hashes and editable hashes*) (Lumb, Treat, & Jelf, 2016): Έχουν προταθεί ως μέθοδοι εφαρμογής στα μπλοκ στα οποία απαιτείται μία τροποποίηση ή αλλαγή των πληροφοριών του. Η συγκεκριμένη τεχνική δίνει τη δυνατότητα επεξεργασίας ενός μπλοκ της αλυσίδας, μέσω της χρησιμοποίησης μίας «καμουφλαρισμένης» συνάρτησης κατακερματισμού, η οποία μπορεί να παραγάγει νέους συμβατούς αλγόριθμους χρησιμοποιώντας ιδιωτικά κλειδιά. Μετά την ολοκλήρωση της αλλαγής στο συγκεκριμένο μπλοκ, το αρχικό μη τροποποιημένο blockchain παραμένει ακέραιο χωρίς να χρειάζεται κάποια εφαρμογή πολιτικής «σκληρού πιρουνιού» (“hard fork”) ή εκ νέου δημιουργία των επόμενων μπλοκ της αλυσίδας. Θα πρέπει να επισημανθεί ότι η συγκεκριμένη τεχνική είναι συμβατή μόνο σε blockchain όπου απαιτείται πρόσβαση στους χρήστες του (permissioned blockchain), με το μοντέλο διακυβέρνησης και τους κανόνες να είναι προσυμφωνημένοι και ελεγχόμενοι από τα συμβαλλόμενα μέρη. Έτσι, διασφαλίζεται η ακεραιότητα της συγκεκριμένης αλυσίδας.

-Τεχνικές Κλαδέματος σε Συναρτήσεις Κατακερματισμού (*Hash Pruning Techniques*): Σε πολλές περιπτώσεις, ο περιορισμός του διαθέσιμου αποθηκευτικού χώρου καθώς και άλλοι τεχνικοί περιορισμοί (π.χ. η διαθέσιμη ταχύτητα στο διαδίκτυο) αποτρέπουν πολλούς από το να συμμετάσχουν στην όλη διαδικασία ως κόμβοι διαμοιρασμού του δικτύου. Για το λόγο αυτό, δημιουργήθηκαν οι «κλαδεμένοι» κόμβοι (pruned nodes), όπου διατηρούνται μόνο οι σημαντικές πληροφορίες της αλυσίδας των μπλοκ που απαιτούνται για την επαλήθευση των διαδικασιών. Εφαρμόζοντας αυτή τη μέθοδο, πληρούνται η *αρχή της ελαχιστοποίησης των δεδομένων* καθώς και οι περιορισμοί του διαθέσιμου αποθηκευτικού χώρου.

Μέρος 4^ο: Μία Τεχνολογία Σύγκλισης του ΓΚΠΔ με την Τεχνολογία του Blockchain

(LTO Network, September 2018) (The Team of LTO Network, November 2018)

4.1 Εισαγωγή

Μέχρι τώρα στην ανάλυσή μας, είδαμε τα μέρη από τα οποία αποτελείται τόσο η τεχνολογία του Blockchain όσο και ο ΓΚΠΔ. Επίσης, προσπαθήσαμε να ορίσουμε τις διάφορες χρησιμοποιούμενες ορολογίες από τις οποίες αποτελείται το καθένα από αυτά. Στο τρίτο μέρος της ανάλυσης, εστιάσαμε στις δυσκολίες που προκύπτουν όταν επιχειρούμε να συνδέσουμε τους δύο αυτούς όρους, με στόχο μία αποτελεσματική συνεργασία. Επίσης, αναφερθήκαμε στις διάφορες τεχνικές λύσεις οι οποίες προσπαθούν να διορθώσουν αυτά τα προβλήματα.

Έχοντας οικοδομήσει το θεωρητικό πλαίσιο, το οποίο μας βοηθάει να ξεκαθαρίσουμε το τοπίο, ήρθε η στιγμή της προσπάθειας εφαρμογής μίας τεχνολογίας στην οποία είναι δυνατή μία σύγκλιση μεταξύ του ΓΚΠΔ και της τεχνολογίας του blockchain.

Αυτή η λύση προκρίνεται μέσω της τεχνολογίας του δικτύου LTO. Πιο συγκεκριμένα, η τεχνολογία αυτή πετυχαίνει τη συνεργασία μεταξύ δύο ή περισσότερων συμβαλλόμενων μερών με αντικρουόμενα συμφέροντα, χωρίς την ανάγκη των μεσαζόντων ή την αναγκαστική ύπαρξη μεταξύ τους εμπιστοσύνης. Η σύγκλιση με τον Κανονισμό πραγματοποιείται μέσω της χρησιμοποίησης ενός υβριδικού blockchain. Στο ένα επίπεδο ανταλλάσσονται τα δεδομένα και οι πληροφορίες μεταξύ των χρηστών του (ιδιωτικό blockchain - 1ο επίπεδο), ενώ στο άλλο επικυρώνονται οι συναλλαγές μέσω των μηχανισμών συναίνεσης (δημόσιο blockchain - 2ο επίπεδο).

Για την κατασκευή του (θεωρητικού) μοντέλου του δικτύου LTO, θα ακολουθήσουν τα εξής τρία μέρη: Α. Το επίπεδο του **ιδιωτικού blockchain**, στο οποίο πραγματοποιούνται όλες οι συναλλαγές των δεδομένων και των πληροφοριών μεταξύ των κόμβων. Β. Το επίπεδο του **δημόσιου blockchain**, όπου επικαιροποιούνται οι συναλλαγές μέσω της τεχνικής της «αγκίστωσης» (“anchoring”). Στο μοντέλο μας, το δημόσιο blockchain ονομάζεται «παγκόσμιο blockchain» (“global blockchain”). Γ. Τα μέρη τα οποία συνθέτουν έναν κόμβο του δικτύου LTO, συνδυάζοντας τα δύο προηγούμενα επίπεδα του blockchain, καθώς και διάφορες πρόσθετες υπηρεσίες που συμβάλλουν στην ορθή λειτουργία της πλατφόρμας -του δικτύου μας.

4.2 Ιδιωτικό Blockchain - Live Contracts (1ο Επίπεδο)

Στο συγκεκριμένο μοντέλο γίνεται χρήση των Live Contracts έναντι αυτών των Smart Contracts. Ο σκοπός της δημιουργίας τους είναι παρόμοιος με εκείνον των «έξυπνων συμβολαίων», καθορίζοντας και δείχνοντας το σκεπτικό που θα πρέπει να ακολουθείται σε ένα τέτοιο μοντέλο. Παρ’ όλα αυτά, υπάρχουν και σημαντικές διαφορές μεταξύ των δύο αυτών εννοιών. Από τη μία έχουμε τα smart contracts, τα οποία περιγράφονται ως «κουτιά» σε καθένα από τα οποία εμπεριέχεται αξία. Στα Live

Contracts δε θα μπορούσαμε να ισχυριστούμε κάτι τέτοιο. Θα λέγαμε ότι μοιάζουν περισσότερο με τα παραδοσιακά έντυπα συμβόλαια, στα οποία περιγράφεται το κανονιστικό πλαίσιο αλληλεπίδρασης δύο ή περισσότερων αντισυμβαλλόμενων μερών.

Ο ορισμός των Live Contracts έρχεται να ταιριάζει με εκείνο των Ρικαρντιανών Συμβολαίων (*Ricardian Contracts*), αποτελώντας μία μορφή η οποία είναι κατανοητή και μπορεί να διαβαστεί τόσο από τους ανθρώπους όσο και από τους υπολογιστές. Τα βασικά τους χαρακτηριστικά μπορούν να συνοψιστούν στα εξής (Geroni, 2020): **α. Σαφήνεια** -οι όροι της συμφωνίας είναι διατυπωμένοι υπό τη μορφή νομικού εγγράφου. **β. Συμβατότητα** -υποστηρίζουν εφαρμογές οι οποίες χρησιμοποιούν την τεχνολογία του blockchain. **γ. Εγκυρότητα** -αποτελούν μία συμφωνία με δεσμευτικό νομικό χαρακτήρα. **δ. Ευελιξία** -έχουν την δυνατότητα να συνδυάζουν δύο ή και περισσότερες επιλογές (π.χ. Smart Contract και Live Contract) **ε. Αναγνωσιμότητα** -με την έννοια ότι μπορούν να διαβαστούν τόσο από τους ανθρώπους (χωρίς να χρειάζονται κάποιες εξειδικευμένες γνώσεις) όσο και από τους υπολογιστές .

Μία άλλη βασική ιδιότητα των Live Contracts αποτελεί η ομοιομορφία μεταξύ των εγγράφων σε φυσική μορφή και του εκάστοτε υπολογιστικού προγραμματιστικού περιβάλλοντος. Υπάρχει δηλαδή ένας ενιαίος τρόπος εμφάνισης, σύνταξης και επικαιροποίησης του εκάστοτε κειμένου χωρίς να χρειάζεται κάποια επιπλέον ενέργεια κωδικοποίησης της συμφωνίας και υπογραφής μεταξύ των αντισυμβαλλόμενων μερών.

Η εκτέλεση των εργασιών στη συγκεκριμένη πλατφόρμα διαμορφώνει ένα εύκολο επαληθεύσιμο ιστορικό ενεργειών, περιορίζοντας το ενδεχόμενο πρόβλημα της ασύμμετρης πληροφόρησης και διευκολύνοντας την επίλυση μίας ενδεχόμενης διαφωνίας ή διαμάχης.

Μέθοδοι Απεικόνισης των Δεδομένων - Πληροφοριών

Σε αντίθεση με τα Smart Contracts, όπου το user interface είναι κατασκευασμένο και γραμμένο σε γλώσσα προγραμματισμού, στα Live Contracts δεν υπάρχει κάποιος πρόσθετος μηχανισμός μετασχηματισμού των δεδομένων προς εισαγωγή. Το user interface σχηματίζεται από τα δεδομένα και τις πληροφορίες που παρέχονται από το ίδιο το κείμενο. Έτσι, κάθε ροή εργασίας μπορεί να εκτελεστεί ψηφιακά στην πλατφόρμα του LTO χωρίς την ανάγκη μετασχηματισμού της στο user interface.

Για να γίνουν κατανοητά τα Live Contracts, τόσο από τους ανθρώπους όσο και από τους υπολογιστές, πραγματοποιείται σχηματική απεικόνιση μέσω **διαγραμμάτων ροής** (flowcharts), όπου οι ενέργειες είναι **προκαθορισμένες** (deterministic state logic).

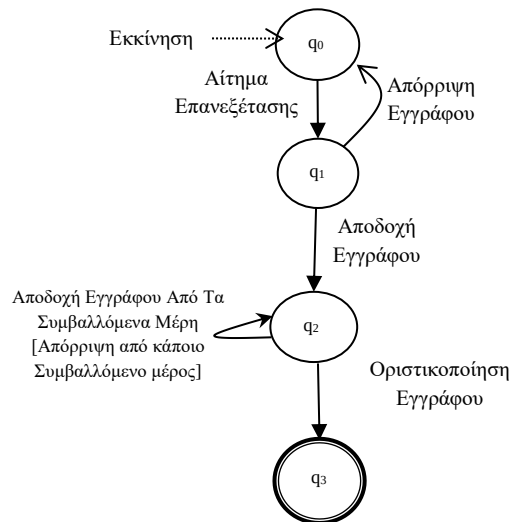
Υπάρχουν διάφορες μέθοδοι με τις οποίες μπορεί κάποιος να αναπαραστήσει τις πραγματοποιούμενες **ροές εργασιών** (workflows). Μία από αυτές αποτελεί ο **Μηχανισμός Πεπερασμένων Καταστάσεων** (Finite State Machine). Ένα αρνητικό του συγκεκριμένου μηχανισμού είναι η μη δυνατότητα εκτέλεσης πολλαπλών ταυτόχρονων εργασιών. Μια προτεινόμενη επίλυση του συγκεκριμένου προβλήματος αποτελεί το σπάσιμο του σε επιμέρους **υπό-εργασίες** (sub-processes) επιτρέποντας τη δυνατότητα εκτέλεσης ταυτόχρονων διαδικασιών σε ένα Live Contract.

Άλλες μέθοδοι είναι: **1. Τα Petri Nets** -αποτελούν και αυτά γραφικές αναπαραστάσεις, στις οποίες υπάρχει η δυνατότητα εκτέλεσης πολλαπλών ταυτόχρονων εργασιών. **2. Η Επιχειρηματική Επεξεργασία και Μοντελοποιημένη Σημειολογία (Business Processing and Modeling Notation)** -δεν αποτελεί κατάλληλη μέθοδο για την εφαρμογή του σε ένα δίκτυο blockchain. Μία προτεινόμενη λύση αποτελεί η μετατροπή του συγκεκριμένου μοντέλου σε Petri net, το οποίο με τη σειρά του μετασχηματίζεται σε έξυπνο συμβόλαιο. **3. Η Μεθοδολογία Σχεδιασμού και Μηχανικής Οργανισμών (D.E.M.O. - Design and Engineering Methodology for Organizations)** -βασίζεται στις «επικοινωνιακές δράσεις», στις οποίες οι ροές εργασίας ομαδοποιούνται σε γενικευμένες για κάθε μεμονωμένη συναλλαγή που εκτελείται.

Ο Εκτεταμένος Μηχανισμός Πεπερασμένων Καταστάσεων

Στην περίπτωση του Μηχανισμού Πεπερασμένων Καταστάσεων, επειδή ο αριθμός των καταστάσεων και των μεταβάσεων αυξάνεται με εκθετικό τρόπο καθώς προχωρούν οι νέες ενέργειες, επιλέγεται η χρήση του **Εκτεταμένου Μηχανισμού Πεπερασμένων Καταστάσεων (E.F.S.M. - Extended Finite State Machine)**. Σ' αυτόν, γίνονται αποδεκτές οι υπό συνθήκη - επιλεκτικές μεταβάσεις καταστάσεων.

Σχηματικά, μία ροή εργασίας θα μπορούσε να αναπαρασταθεί ως εξής:



Σχήμα 4: Ο Εκτεταμένος Μηχανισμός
Πεπερασμένων Καταστάσεων
(LTO Network, September 2018)

Τα Συστατικά Στοιχεία του Μοντέλου

Μία **ροή εργασίας** ορίζεται ως ένα **σενάριο**, το οποίο αποτελεί το σύνολο των πιθανών **ενεργειών** που μπορούν να υλοποιηθούν σε μία ροή εργασίας (π.χ. αναθεώρηση εγγράφου, αποστολή ή απάντηση αιτήματος HTTP, συμπλήρωση μίας ηλεκτρονικής φόρμας). Το κάθε Live Contract θα πρέπει να περιέχει τουλάχιστον ένα **σενάριο** στο οποίο περιγράφονται οι εκάστοτε διαδικασίες.

Το κάθε **σενάριο** με τη σειρά του αποτελείται από: Τις **φάσεις** (q_x με αρχική φάση την q_0 - states), τις **ενέργειες** (s_x - actions), τις **μεταβατικές καταστάσεις** (δ - transition functions), τις ομάδες των ατόμων που συμμετέχουν σε κάθε εκτελούμενη

ενέργεια ($\bar{I}$ - actors), τα διαθέσιμα **πάγια** σε κάθε διαδικασία ($\bar{A}$ - assets) και τα αντίστοιχα σύνολά τους για το κάθε συστατικό στοιχείο.

Οι **φάσεις** (states) αποτελούνται από μία **σύντομη ονομασία - τίτλο** της εκάστοτε φάσης, ένα **σύνολο συναλλαγών** με τις μεταβάσεις, μία **αναλυτική περιγραφή** των φάσεων και τις **αναλυτικές οδηγίες** για τις συγκεκριμένες ομάδες που συμμετέχουν στη διαδικασία.

Η **αμεταβλητότητα των δεδομένων και των πληροφοριών** (immutability) διασφαλίζεται μέσω της δημιουργίας ενός νέου αντικειμένου δεδομένων για την περίπτωση κατά την οποία πραγματοποιείται τροποποίηση του παλιού αντικειμένου με ταυτόχρονη αντικατάστασή του από το νέο τροποποιημένο. Για την υποστήριξη των ψηφιακών ροών εργασίας και των προτύπων που θα πρέπει να δημιουργηθούν στα Live Contracts, προτείνεται η χρησιμοποίηση της μορφοποίησης των ανοικτών εγγράφων (Open Document Format).

Η **ταυτότητα** (identity) ορίζεται ως το άτομο (φυσικό ή όχι) ή ο οργανισμός που δημιουργεί τα Live Contracts. Περιέχει τις απαιτούμενες πληροφορίες ώστε να αναγνωρίζεται ο καθένας που συμμετέχει στη διαδικασία (αναγνωριστικό, αναγνωριστικό κόμβου, επιμέρους πληροφορίες, κλειδιά υπογραφής, κλειδιά κρυπτογράφησης).

Η **προσθήκη νέων οντοτήτων** (π.χ. φυσικά πρόσωπα, ομάδα χρηστών, οργανισμός) θα πρέπει να είναι προκαθορισμένη από το εκτελούμενο σενάριο, καθορίζοντας τις ενέργειες για οποιαδήποτε νέα προσθήκη. Στην περίπτωση κατά την οποία τα δημόσια κλειδιά είναι γνωστοποιημένα, η νέα οντότητα μπορεί να προστεθεί απευθείας. Σε αντίθετη περίπτωση, θα πρέπει να υπάρξει πρόσκληση, η οποία μπορεί να πραγματοποιηθεί μέσω ενός ασφαλούς διαύλου επικοινωνίας. Η διαδικασία πρόσκλησης πραγματοποιείται με τη δημιουργία ενός κλειδιού μίας χρήσης, το οποίο αποστέλλεται στην νέα οντότητα. Αφού γίνει αποδεκτή η πρόσκληση, η νέα οντότητα θα πρέπει να ορίσει νέο κλειδί χρήστη και νέο κλειδί συστήματος (user & system keys). Πριν τη συμμετοχή του νέου χρήστη στις ενέργειες του κόμβου, ενδέχεται να απαιτηθεί πρόσθετη ταυτοποίηση (απλή ή σύνθετη). Τέλος, το σύστημα επιτρέπει την ενημέρωση των πληροφοριών των χρηστών εκτός από την αλλαγή του αναγνωριστικού τους.

Εκτός από τα σενάρια, υπάρχουν και άλλοι τύποι δεδομένων τα οποία μπορούν να ενσωματωθούν στην διαδικασία ή να συσχετιστούν και να αποθηκευτούν μεμονωμένα. Αυτοί οι τύποι ονομάζονται **αντικείμενα δεδομένων** (data-objects).

Οι **ενέργειες** (actions) που πραγματοποιούνται από τους χρήστες των κόμβων χωρίζονται σε **χειροκίνητες** (manual actions), στις οποίες η ανθρώπινη παρέμβαση είναι απαραίτητη για την εκτέλεση τους, και σε **συστημικές** (system actions), οι οποίες μπορούν να εκτελεστούν αυτόματα από το ίδιο το σύστημα. Οι χειροκίνητες ενέργειες θα πρέπει να υπογράφονται από τους εκτελούντες την ενέργεια πριν από την επικύρωσή τους στο δίκτυο, ενώ παρέχεται ενημέρωση σχετικά με τις επιλογές υλοποίησής τους σε κάθε στάδιο. Από την άλλη μεριά, οι αυτοματοποιημένες (συστημικές) μεταβάσεις, υπογράφονται αυτόματα από τον κόμβο χωρίς να χρειάζεται κάποια ανθρώπινη συμμετοχή, οδηγώντας σε δύο τελικές καταστάσεις: μία της επιτυχούς υλοποίησης και μία δεύτερη με την ένδειξη σφάλματος.

Είναι προφανές ότι ένα **σενάριο** δεν μπορεί να προβλέψει εκ των προτέρων όλες τις πιθανές μεταβάσεις που μπορούν να υπάρξουν στο μοντέλο που δημιουργήθηκε. Για το λόγο αυτό, χρησιμοποιούνται τρία είδη **προσαρμοσμένων ροών εργασίας** (*adaptive workflows*) μέσω των οποίων βελτιστοποιείται το ίδιο το σύστημα. Αυτά είναι: **i. Τα σχόλια** (*comments*), τα οποία δεν προκαλούν οποιαδήποτε αλλαγή κατάστασης στο μοντέλο μας, αλλά βοηθούν να βελτιωθεί η διαδικασία υπογραμμίζοντας πιθανές υπαρκτές παραλείψεις ή προβλήματα. Όλα τα σχόλια και οι παρατηρήσεις βρίσκονται εντός της αλυσίδας, βοηθώντας τους κόμβους να ανατρέξουν στο τι έχει ειπωθεί σε παλιότερα σχόλια. Μπορούν να έχουν τη μορφή κειμένου, εικόνων ή εγγράφων. **ii. Οι ροές απόκλισης** (*deviation*), οι οποίες μπορούν να πραγματοποιηθούν από οποιονδήποτε κόμβο μέσα στο δίκτυο, προτείνοντας μία εναλλακτική ροή υλοποίησης του σεναρίου, υπό την προϋπόθεση ότι ξεκινούν και καταλήγουν σε μία από τις προκαθορισμένες υπάρχουσες καταστάσεις του σεναρίου. Για την υιοθέτησή τους θα πρέπει να υπάρξει καθολική συμφωνία από όλα τα συμβαλλόμενα μέρη του κόμβου. Η χρήση τους μπορεί να πραγματοποιηθεί σε περιπτώσεις ασυμφωνίας, στην οποία ένας κόμβος αμφισβητεί την ορθότητα μίας προηγούμενης κατάστασης, προτείνοντας μία διόρθωσή του. **iii. Η ενημέρωση σεναρίου** (*scenario update*), η οποία μπορεί να προκύψει ύστερα από κάποια αλλαγή στις υπάρχουσες συνθήκες (π.χ. μία νέα συμφωνία πραγματοποιείται ή ένας νέος νόμος ψηφίζεται).

Σε ένα σύστημα με κεντρική διαχείριση, ο κεντρικός διαχειριστής του ορίζεται ως ο θεματοφύλακας για την ακεραιότητα των δεδομένων. Τα συμβαλλόμενα μέρη είναι υποχρεωμένα να τον εμπιστευτούν, εφόσον επιθυμούν να συνεχίσουν να χρησιμοποιούν το δίκτυο. Στην περίπτωση όμως της αποκεντρωμένης διαχείρισης, η εξουσία της διαχείρισης των δεδομένων και η ευθύνη διασφάλισης της ακεραιότητάς τους διαμοιράζεται ισάξια μεταξύ των κόμβων. Προκειμένου να προσδιοριστεί η *τρέχουσα κατάσταση στον Μηχανισμό του EFSM*, θα πρέπει να καθοριστεί μία συγκεκριμένη διαδικασία με την οποία προσδιορίζεται η **χρονολογική σειρά των απαντήσεων των συμβάντων** (*events*) μέσω των οποίων δημιουργούνται οι επόμενες **φάσεις** (*states*).

Η ροή δημιουργίας ενός Live Contract (LTO Network, 2019)

Για τη δημιουργία ενός Live Contract στο δίκτυο του LTO, απαιτείται η δημιουργία ενός πλήρους κόμβου. Σε κάθε κόμβο θα πρέπει να υπάρχει τουλάχιστον ένα σενάριο όπου περιγράφονται οι διαδικασίες που πραγματοποιούνται. Η γλώσσα προγραμματισμού που χρησιμοποιείται είναι η JSON ή η YMAL.

Οι **Actors**⁴ (φυσικά πρόσωπα ή οργανισμοί) αποτελούν τις ομάδες εκείνες που συμμετέχουν στη διαδικασία. Στο σενάριο θα πρέπει να προσδιορίζεται ποιοι actors μπορούν να συμμετέχουν σ' αυτό. Συνήθως, για κάθε σενάριο υπάρχουν τουλάχιστον δύο ή περισσότεροι **actors**, με τον έναν από αυτούς να ξεκινάει τη διαδικασία και να

⁴ Αποτελούν τη γενικευμένη κατηγορία των χρηστών π.χ. «φοιτητής», «προγραμματιστής», «διαχειριστής» σε αντίθεση με την έννοια της «ταυτότητας», με την οποία καθορίζεται ο συγκεκριμένος χρήστης π.χ. «John Doe», «Adobe Organization» κ.ά.

λογίζεται ως «εκκινήτης» της (*initiator*). Οι *ενέργειες* (*actions*) οι οποίες μπορεί να υλοποιήσει ένας actor πρέπει είναι προκαθορισμένες μέσω των υπαρχουσών φάσεων.

Η διαδικασία των *φάσεων* (*states*) ξεκινάει από την αρχική φάση, ενώ σταδιακά μεταβαίνει και στις επόμενες, μέχρις ότου η διαδικασία ολοκληρωθεί φτάνοντας στην επιτυχή ολοκλήρωση της κατάστασης.

Για να διασφαλιστεί η ορθή λειτουργία του Live Contract δημιουργούνται και εκτελούνται κάποια διαγνωστικά τεστ στον πλήρη κόμβο του δικτύου (με τη χρήση Gherkin syntax). Για να λειτουργήσει επιτυχώς ένας τέτοιος μηχανισμός, η *χρονολογική σειρά των συμβάντων* (*event chain*) ακολουθείται όπως στα *ιδιωτικά blockchain*. Οι κόμβοι ενημερώνονται μόνο στις περιπτώσεις όπου συμμετέχουν στη ροή των συμβάντων. Σε αντίθετη περίπτωση, αποθηκεύουν μόνο τις αλλαγές και τις τροποποιήσεις, ενημερώνοντας αντίστοιχα το καθολικό τους χωρίς κάποια περαιτέρω εμπλοκή στην διαδικασία. Τα βήματα που ακολουθούνται είναι τα εξής:

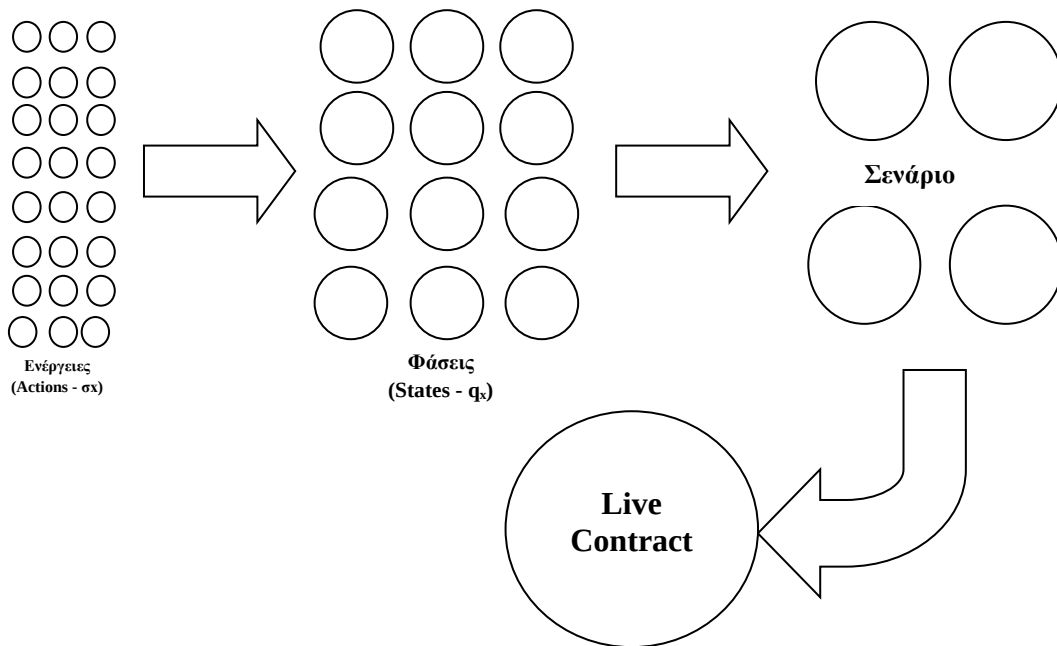
- Κάθε απάντηση ομαδοποιείται σε ένα *συμβάν* (*event*), το οποίο μπορεί να θεωρηθεί ως ένα μπλοκ.

- Η ακολουθία των συμβάντων (*event chain*) σχηματίζει μία συνάρτηση κατακερματισμού, η οποία κοινοποιείται μεταξύ των κόμβων. Ο μηχανισμός συναίνεσης διασφαλίζει την ορθή χρονολογική παράθεση των γεγονότων εντός του δικτύου.

Ένα πρόσθετο στοιχείο διασφάλισης της ακεραιότητας των συμβάντων αποτελεί η ψηφιακή υπογραφή πριν την επικύρωσή τους στον κόμβο, μέσω *ασύμμετρης κρυπτογράφησης*. Στο συγκεκριμένο μοντέλο, χρησιμοποιείται η *καμπύλη Edwards - ED25519* ως ο αλγόριθμος για τις ψηφιακές κρυπτογραφικές υπογραφές, συνδυάζοντας τη γρήγορη επαλήθευση με τη διατήρηση των απαιτήσεων ασφαλείας.

Η χρησιμοποίηση της *ψηφιακής υπογραφής* μαζί με τη *συνάρτηση κατακερματισμού* του προηγούμενου συμβάντος (της μορφής SHA-2 στα 256bit) στο κάθε μπλοκ της αλυσίδας δημιουργεί ένα ιστορικό συναρτήσεων κατακερματισμού, εκ των οποίων διασφαλίζεται η ορθή παράθεση των συμβάντων (*events*), οδηγώντας στην τρέχουσα φάση (*state*).

Ακολουθεί μία σχηματική αναπαράσταση **των στοιχείων που συνθέτουν ένα Live Contract** :



Σχήμα 5: Τα Συστατικά Στοιχεία ενός Live Contract

Όπως αναφέρθηκε και προηγουμένως, το δίκτυο LTO αποτελεί έναν αποκεντρωμένο μηχανισμό διαχείρισης δεδομένων μέσω της χρήσης της τεχνολογίας blockchain, στο οποίο ο καθένας μπορεί να συμμετάσχει ως ομότιμος κόμβος του. Τα δεδομένα που προσθέτει τα γνωστοποιεί στους υπόλοιπους κόμβους, οι οποίοι ύστερα από τον αντίστοιχο έλεγχο τα προσθέτουν (ή τα απορρίπτουν) στα δικά τους καθολικά. Αυτό σημαίνει ότι υπάρχει η πιθανότητα ενός **μεταβατικού διαστήματος** μεταξύ των κόμβων του δικτύου, στο οποίο ακόμη δεν έχει ξεκαθαριστεί ποιο συμβάν προηγείται έναντι των υπολοίπων. Για το λόγο αυτό, χρησιμοποιούνται οι μηχανισμοί συναίνεσης. Παρ' όλα αυτά, επειδή στο συγκεκριμένο μοντέλο ο αριθμός των κόμβων είναι περιορισμένος για κάθε συμβάν, λειτουργώντας υπό τη σκέπη του *private blockchain*, η πιθανότητα σύγκρουσης (*conflict*) και διαφωνίας μεταξύ δύο ή περισσότερων κόμβων είναι πάρα πολύ μικρή και συνεπώς δε λαμβάνεται υπόψη. Αυτό θα αλλάξει μόνο σε περίπτωση στην οποία παρατηρηθεί αυξημένος αριθμός χρηστών σε κάποιο συμβάν. Στην περίπτωση της σύγκρουσης, εφαρμόζονται συγκεκριμένοι κανόνες βαρύτητας για τη λήψη της απόφασης της προτεραιότητας των συμβάντων (προτεραιότητα συμβάντος, προτεραιότητα actor, χρονολογική σειρά του «anchoring»).

Ιδιωτικότητα του Δικτύου και Συμβατότητα με τον ΓΚΠΔ

Όπως είδαμε, το 1ο επίπεδο του δικτύου LTO έχει κατασκευαστεί με τη φιλοσοφία ενός ιδιωτικού blockchain, με σκοπό η γνωστοποίηση των δεδομένων και

των πληροφοριών να γίνεται μόνο στους κόμβους που συμμετέχουν στο δίκτυο. Στην αντίπερα όχθη, βρίσκονται τα δημόσια blockchain, για τα οποία η «ψευδωνυμοποίηση» ενέχει πολλές πιθανότητες αναγνώρισης της ταυτότητας του χρήστη, αποκαλύπτοντας τις πληροφορίες που περικλείονται εντός του. Τα «ειδικά» *ιδιωτικά blockchain* (*ad hoc private blockchain*) προκρίνουν την τυχαία συνεργασία μεταξύ των συμβαλλόμενων μερών, χωρίς την ανάγκη κάποιας περαιτέρω έγκρισης ή ευρύτερης δημοσιοποίησης των πληροφοριών τους. Σημαντικό, επίσης, είναι το γεγονός ότι, αφού ολοκληρωθεί ο κύκλος ζωής της χρησιμοποίησής τους, τα συγκεκριμένα blockchain μπορούν να διαγραφούν πλήρως.

Η σύνδεση των χρηστών στο δίκτυο πραγματοποιείται μέσω του εγκεκριμένου κόμβου, όπου ο καθένας τους διατηρεί έναν δικό του *ιδιωτικό αποθηκευτικό χώρο* (*private storage service*), αποθηκεύοντας τις πληροφορίες που επιθυμεί. Ο έλεγχος των δεδομένων γίνεται από τους ιδίους, λειτουργώντας όπως η υπηρεσία του Dropbox, με τη δυνατότητα διαγραφής τους όποτε αυτοί το θελήσουν. Ο διαμοιρασμός των πληροφοριών δεν πραγματοποιείται χωρίς την εκ των προτέρων συμφωνία και ρητή έγκριση από τον ίδιο το χρήστη και ιδιοκτήτη των δεδομένων.

Όταν μία *ενέργεια* (*action*) έχει ως αποτέλεσμα το διαμοιρασμό δεδομένων, δημιουργείται στην αλυσίδα μία συνάρτηση κατακερματισμού μίας χρήσης, που περιέχει τα προς ανταλλαγή δεδομένα μαζί με μία χρονοσφραγίδα και κάποια τυχαία δεδομένα. Εάν ένας χρήστης γνωστοποιήσει την πρόθεσή του για την πραγματοποίηση μίας ενέργειας για την οποία απαιτείται ανταλλαγή τους, δημιουργείται αίτημα από το συμβεβλημένο του κόμβο στο δίκτυο. Στη συνέχεια, ο κόμβος όπου βρίσκονται τα δεδομένα, θα προχωρήσει σε έλεγχο της ορθότητας του αιτήματος της ενέργειας και θα πραγματοποιήσει το διαμοιρασμό τους -εφόσον οι υπόλοιποι κόμβοι του δικτύου αποφανθούν θετικά.

Όπως είδαμε στο 3ο μέρος της ανάλυσής μας, εφαρμόζοντας το ΓΚΠΔ ο καθορισμός του υπευθύνου επεξεργασίας των προσωπικών δεδομένων καθίσταται δύσκολος έως αδύνατος, ενώ ταυτόχρονα υπάρχει πρόβλημα στη διαγραφή και τροποποίησή τους, επηρεάζοντας την αμετάβλητη φύση του blockchain. Στο συγκεκριμένο μοντέλο, ο κόμβος που επιλέγεται να διαμοιράζει τα δεδομένα στο δίκτυο θεωρείται ότι είναι ο Υπεύθυνος Επεξεργασίας (Data Controller), ενώ όλοι οι υπόλοιποι κόμβοι που αλληλεπιδρούν θεωρούνται ως οι Εκτελούντες την Επεξεργασία (Data Processors). Τα όποια αιτήματα ανταλλαγής πληροφοριών λειτουργούν όπως ακριβώς οι τυπικές συμφωνίες δεδομένων, στις οποίες καθορίζεται ο σκοπός και η χρονική στιγμή της επεξεργασίας τους. Η μέθοδος αυτή καθιστά συμβατή την τεχνολογία του blockchain με τα αυστηρά προαιπατούμενα που θέτει ο ΓΚΠΔ.

Η συγκεκριμένη πλατφόρμα υποστηρίζει τη χρησιμοποίηση των *αποδείξεων μηδενικής γνώσης* (*zero knowledge proofs*), μέσω της διάδρασης μεταξύ των χρηστών. Δύο συμβαλλόμενα μέρη, ο *επαληθευτής* (*prover*) και ο *επικυρωτής* (*verifier*), ανταλλάσσουν μηνύματα με στόχο ο μὲν επαληθευτής να πείσει τον επικυρωτή ότι είναι φερέγγυος, ο δε επικυρωτής να αποκαλύψει τον ανέντιμο επαληθευτή.

4.3 Δημόσιο Blockchain - Global Blockchain (2ο Επίπεδο)

Στη συγκεκριμένη πλατφόρμα, το 2ο επίπεδο του δημόσιου blockchain, ονομάζεται «**Παγκόσμιο**» **Blockchain** (“*Global Blockchain*”), στο οποίο δεν απαιτείται **άδεια πρόσβασης** (*permissionless*). Η δημιουργία του έχει ως στόχο την επιβεβαίωση των δεδομένων και των πληροφοριών των κόμβων, επαληθεύοντας τα Live Contracts και τα **συμβάντα** (*events*) -τα προσωπικά δεδομένα που υλοποιούνται στο 1ο επίπεδο της ιδιωτικής αλυσίδας.

Γίνεται χρήση του **Nxt Blockchain** (Jelurida, 2020), το οποίο αποτελεί μία πλατφόρμα ανοικτού κώδικα, με το **Proof of Stake (PoS)** να είναι ο εφαρμοζόμενος μηχανισμός συναίνεσης. Ένα σημαντικό πλεονέκτημα που πηγάζει από τη χρησιμοποίηση του Nxt είναι ότι μειώνει το συνολικό μέγεθος της αλυσίδας, βελτιώνοντας την αποτελεσματικότητα και παρέχοντας εναλλακτικούς τρόπους για τις «**συμβαιολογραφικές**» **συναλλαγές** (*Notary Transactions*).

«**Αγκιστρώνοντας**» τις **Συναρτήσεις Κατακερματισμού**

Οι παραγόμενες συναρτήσεις κατακερματισμού επικαιροποιούνται στη δημόσια αλυσίδα με τη διαδικασία της «**αγκίστρωσης**» (*anchoring*). Τα δεδομένα εισόδου προκύπτουν από τις παραγόμενες συναρτήσεις κατακερματισμού και αποθηκεύονται εντός της αλυσίδας, με στόχο την αποτροπή οποιασδήποτε τροποποίησης. Έτσι, διασφαλίζεται η γνησιότητά τους, διατηρώντας παράλληλα τις ιδιότητες της ακεραιότητας και αναλλοίωτης φύσης τους.

Στο συγκεκριμένο δίκτυο επιλέγεται η αποκεντρωμένη διαχείριση της «αγκίστρωσης» με τον κάθε κόμβο να μπορεί να δει άμεσα όλες τις πραγματοποιούμενες συναλλαγές (σε χρονικό διάστημα 3 δευτερολέπτων) κάνοντας χρήση του **πρωτοκόλλου NG**, το οποίο βοηθάει στον περιορισμό των προβλημάτων της **επεκτασιμότητας** (*scalability*). Για τους κόμβους, δεν κρίνεται αναγκαία η κεντρική διαχείριση, αφού παρέχεται η δυνατότητα εντοπισμού του **anchoring**, επί του συνολικού αριθμού είτε των συναρτήσεων κατακερματισμού του κόμβου είτε μόνο αυτών που πραγματοποίησαν οι ίδιοι.

Κάθε συμβάν που πραγματοποιείται στην ιδιωτική αλυσίδα του δικτύου (1ο επίπεδο) «αγκιστρώνεται» στο «παγκόσμιο» blockchain, το οποίο αποτελεί και το αποδεικτικό επικύρωσης των δεδομένων. Υπολογίζεται ότι περίπου το 99,8% των συναλλαγών που πραγματοποιούνται στο συγκεκριμένο επίπεδο του δικτύου αποτελούν οι συναλλαγές επικύρωσης - «αγκίστρωσης». Μία ομαδοποίησή τους θα πετύχει τη μείωση του απαιτούμενου αποθηκευτικού χώρου που χρησιμοποιείται στην αλυσίδα.

Με τη δημιουργία ενός νέου μπλοκ από τις πραγματοποιούμενες συναλλαγές, ο κόμβος παράγει ένα νέο δένδρο Merkle με χρονολογική σειρά. Στο blockchain προστίθεται μόνο η ρίζα του δένδρου, ενώ το Merkle Tree προστίθεται και σε κάθε κόμβο που συμμετέχει στο δίκτυο.

Όλοι οι κόμβοι έχουν την δυνατότητα αναζήτησης των συναρτήσεων κατακερματισμού του δικτύου. Ωστόσο, επειδή τίθεται ως βασικός στόχος η εξοικονόμηση του αποθηκευτικού χώρου, οι κόμβοι επιλέγουν να αποθηκεύσουν μόνο

τις δικές τους διαδρομές «αγκίστρωσης» των δένδρων Merkle. Έτσι, προστίθεται μία δεύτερη απόδειξη επιβεβαίωσης, η οποία μπορεί να αποθηκευτεί μαζί με τα αρχικά τους δεδομένα.

Χρησιμοποιούμενος Μηχανισμός Συναίνεσης

Όπως αναφέρθηκε προηγουμένως, το «παγκόσμιο» blockchain λειτουργεί όπως ένα δημόσιο blockchain, στο οποίο ένας κόμβος του δικτύου επιλέγεται ως «δημιουργός» (*generator*) για την επικύρωση των συναλλαγών και την εν τέλει δημιουργία του επόμενου μπλοκ της αλυσίδας. Ο **μηχανισμός συναίνεσης** που χρησιμοποιείται για τον καθορισμό του (επόμενου) «δημιουργού» του μπλοκ είναι ο ***Leased Proof of Importance***, ο οποίος αποτελεί έναν συνδυασμό του μεριδίου (*token*) που κατέχει ο συγκεκριμένος κόμβος στο δίκτυο, όπως γίνεται στο ***Proof of Stake***, συνυπολογίζοντας την ενεργή (ή παθητική) δραστηριότητά του, όπως γίνεται στο ***Proof of Importance*** (αναφερθήκαμε στο 1^ο μέρος). Για τους μη ενεργούς κόμβους του δικτύου, παρέχεται η δυνατότητα «μίσθωσης» τους (*Leased*) σε άλλους ενδιαφερόμενους, αυξάνοντας την πιθανότητα επιλογής τους ως «δημιουργών» του. Σε περίπτωση επιτυχούς επιλογής του συγκεκριμένου κόμβου ως *generator*, οι ανταμοιβές που προβλέπονται διαμοιράζονται αναλογικά μεταξύ μισθωτών και εκμισθωτών.

Για να αποφευχθεί η μαζική «μίσθωση» των κόμβων, τίθεται περιορισμός για τη διαχείριση των «μισθωμένων» **μεριδίων**, με τον κάθε μισθωτή να επιτρέπεται να κατέχει μέχρι το 10% επί του συνολικού μεριδίου.

Συντελεστές Προσδιορισμού

Ο υπολογισμός του ποσοστού χρήσης του δικτύου, από τον οποίο προκύπτει η πιθανότητα «δημιουργίας» του επόμενου μπλοκ, ονομάζεται «**Αναλογία Μερισματικών Μονάδων**» (*ST ratio*). Αποτελεί ένα κλάσμα με αριθμητή το ποσοστό του μεριδίου του κόμβου επί των συνολικών μεριδίων επί τοις εκατό (*staked tokens as % of total*) και παρονομαστή τις συνεισφορές των συναλλαγών στο δίκτυο επί τοις εκατό (*Contributed transactions as % of total*).

Έτσι προκύπτει ο εξής μαθηματικός τύπος (LTO Network, September 2018):

$$\text{Αναλογία } M.M. = \frac{\text{ποσοστό του μεριδίου του κόμβου επί των συνολικών μεριδίων \%}}{\text{συνεισφορές των συναλλαγών στο δίκτυο \%}} \quad (1)$$

Ο συντελεστής της αναλογίας των Μερισματικών Μονάδων επηρεάζει τον **Τυχαίο Παράγοντα** (*Raffle Factor - r*), ο οποίος αποτελεί τη μαθηματική εξίσωση που προσδιορίζει την πιθανότητα επιλογής ενός κόμβου για τη δημιουργία του επόμενου μπλοκ του δικτύου, με επιτρεπόμενο εύρος τιμών μεταξύ του 1.0 (ελάχιστο) και του 1.5 (μέγιστο). Όσο πιο σταθμισμένη είναι η αναλογία των M.M. προσεγγίζοντας την τιμή του 1.0 τόσο μεγαλύτερη είναι η τιμή του τυχαίου παράγοντα, με μέγιστη αυτή του 1.5.

Η μαθηματική εξίσωση η οποία αναπαριστά τον **Τυχαίο Παράγοντα** είναι η εξής (LTO Network, September 2018):

$$\text{Τυχαίος Παράγοντας } (r) = 1 + (0.5 \times e^{-0.5 \times (\text{Αναλογία } M.M. - 1)^2}) \quad (2)$$

Στηριζόμενοι στις εξισώσεις (1) και (2), προκύπτει η εξίσωση που αναπαριστά την **πιθανότητα (P) επιλογής του κόμβου** ως του επόμενου «δημιουργού» του:

$$P = S \times r \quad (3)$$

Όπου: $S \rightarrow$ μερίδιο του κόμβου στο δίκτυο.

Κατά τον υπολογισμό του P , το μερίδιο S θα πρέπει να παραμένει σταθερό για να αποφευχθεί το ενδεχόμενο κατάχρησης.

$r \rightarrow$ Τυχαίος Παράγοντας

Ο προσδιορισμός του κόμβου που κρίνεται κατάλληλος για τη δημιουργία του επόμενου μπλοκ γίνεται μέσω του αλγορίθμου **Fair Proof of Stake**, που έχει δημιουργηθεί από την πλατφόρμα του **Waves**.

Το **πιστοποιητικό συναλλαγών (certificate)** επιτρέπει σε έναν κόμβο τη μεταβίβαση δεδομένων σε έναν άλλο, χρησιμοποιώντας μόνο τη διεύθυνσή του. Σε αντίθεση με τα μερίδια, τόσο η έγκριση όσο και η ανάκληση του λογαριασμού ενός χρήστη βρίσκεται υπό τον έλεγχο του εκδότη του πιστοποιητικού. Χωρίς να είναι προαπαιτούμενο, προτείνεται η αποδοχή από την παραλήπτη πριν την παρουσίασή τους σε άλλους.

Ενώ η δημόσια διεύθυνση στην οποία χρησιμοποιείται η μέθοδος της ασύμμετρης κρυπτογράφησης με δημόσιο κλειδί αποτελεί ένα τρόπο επαλήθευσης της ταυτότητας του κόμβου, δεν παρέχεται κάποια λύση σχετικά με την έγκριση και εξουσιοδότηση του κόμβου στο δίκτυο. Τα **πιστοποιητικά** των διαφορετικών **identity** μπορούν να συνεισφέρουν σ' αυτό το κομμάτι παρέχοντας μία λύση. Έτσι, προκύπτει μία σύνδεση μεταξύ δύο διαφορετικών **identity**, στην οποία εμφανίζεται μόνο η επιβεβαίωση της μεταξύ τους συσχέτισης, χωρίς την αποκάλυψη οποιασδήποτε άλλης πληροφορίας. Με τον τρόπο αυτό επιτυγχάνεται η εξ αποστάσεως συνεργασία μεταξύ των **identities**, απομακρύνοντας την ανάγκη μίας δια ζώσης μεταξύ τους συνάντησης.

Για την πραγματοποίηση οποιασδήποτε συναλλαγής, το σύστημα απαιτεί την εισαγωγή των προσωπικών κωδικών, αποτελούμενων από το ιδιωτικό κλειδί του χρήστη. Η πλατφόρμα του Waves (Waves, 2021) εισάγει τους **«έξυπνους λογαριασμούς» (smart accounts)**, επιτρέποντας την εξατομίκευσή τους ανά χρήστη. Για να πραγματοποιηθεί η προσαρμογή στις απαιτήσεις του κάθε χρήστη, δημιουργείται ένα **σενάριο σε μη προγραμματιστική μορφή (Non Turing Scenario)**, το οποίο επιβεβαιώνει ή απορρίπτει αποκλειστικά τη συναλλαγή για τον συγκεκριμένο λογαριασμό, δίχως τη δυνατότητα πραγματοποίησης άλλων συναλλαγών.

Τα Μπλοκ Σύνοψης

Όπως αναφέρθηκε και προηγουμένως, καθώς προχωράει ο χρόνος, η αλυσίδα του blockchain επεκτείνεται, με το μέγεθός της να θέτει συγκεκριμένες απαιτήσεις και περιορισμούς στον εξοπλισμό για τη διατήρηση ενός πλήρους αντιγράφου της. Έτσι, το μεγάλο μέγεθος του blockchain αποτελεί εμπόδιο για την είσοδο στο δίκτυο νέων κόμβων, μιας και χρειάζεται η εκ νέου αντιγραφή ολόκληρης της αλυσίδας του. Προκειμένου να υπάρξει επίλυση στα ζητήματα του αποθηκευτικού χώρου της αλυσίδας μέσω της σταδιακής ανάπτυξής τους, εισάγεται ένας δεύτερος τύπος μπλοκ,

τα οποία ονομάζονται **Μπλοκ Σύνοψης** (*summary blocks*). Ανά ημέρα στο δίκτυο δημιουργείται ένα μπλοκ σύνοψης.

Μία υπόθεση που γίνεται είναι ότι καθημερινά η μέγιστη επεκτασιμότητα του δικτύου μπορεί να υποστηρίξει μέχρι 50 εκατομμύρια συναλλαγές. Ο αριθμός αυτός είναι περίπου πέντε φορές μεγαλύτερος από τις αναμενόμενες απαιτήσεις του δικτύου.

Το μέγεθος των **key μπλοκ** (*keyblock size*) αποτελεί το άθροισμα των **δεδομένων του μπλοκ** (*block data*) και των **δεδομένων της συναλλαγής** (*transaction data*). Μαθηματικά αυτό λαμβάνει την εξής μορφή (LTO Network, September 2018):

$$\text{Μέγεθος key Μπλοκ} = d + t \quad (4)$$

Όπου $d \rightarrow$ δεδομένα του μπλοκ,

$t \rightarrow$ δεδομένα της συναλλαγής.

Για να προκύψει η παραπάνω εξίσωση, λαμβάνονται υπόψη οι εξής **υποθέσεις**:

- Το 99,98% των πραγματοποιούμενων συναλλαγών το αποτελούν οι συναλλαγές «αγκίστρωσης».

- Το εναπομείναν 0,02%, το αποτελούν οι συναλλαγές πιστοποιητικών.

- Οποιαδήποτε άλλη πραγματοποιούμενη συναλλαγή θεωρείται μη σχετική και μπορεί να αγνοηθεί.

- Όλες οι συναλλαγές διαμοιράζονται ομοιόμορφα μεταξύ των μπλοκ.

- Κατά προσέγγιση, ανά λεπτό παράγεται ένα **keyblock**.

- 1440 **key μπλοκ** (*key blocks*) δημιουργούνται ανά ημέρα ($24 \times 60 = 1440$).

Στηριζόμενοι στις παραπάνω υποθέσεις, και με το μέγεθος των δεδομένων ενός μπλοκ να ορίζεται στα 277 bytes, το μέγεθος των δεδομένων μίας συναλλαγής μπορεί να υπολογιστεί από τον εξής μαθηματικό τύπο (LTO Network, September 2018):

$$\text{Μέγεθος Δεδομένων Συναλλαγής} = n \times (0.9998 \times a + 0.0002 \times c) \quad (5)$$

Όπου: $a \rightarrow$ μέγεθος συναλλαγών «αγκίστρωσης»,

$c \rightarrow$ μέγεθος πιστοποιητικού συναλλαγών,

$n \rightarrow$ πλήθος συναλλαγών ανά μπλοκ.

Έτσι, το συνολικό μέγεθος του κάθε **μπλοκ** (*key block*) είναι της τάξεως των **3.8 MB**.

Εάν προχωρήσουμε τους υπολογισμούς στη συνολική ημερήσια και ετήσια ανάπτυξη του κόμβου, θα διακρίνουμε ότι, εφόσον θέλουμε ο συγχρονισμός του δικτύου να είναι ταχύτατος (π.χ. να απαιτούνται λιγότερο από 20 λεπτά για την ανάκτηση των δεδομένων ενός έτους), ο κόμβος θα πρέπει να μπορεί να επεξεργάζεται περίπου ένα μπλοκ σύνοψης ανά 3 δευτερόλεπτα. Για να συμπεστούν όσο περισσότερο γίνεται τα δεδομένα του μπλοκ, διατηρώντας μόνο τα στοιχεία που κρίνονται απαραίτητα, εφαρμόζεται η μέθοδος του «διαχωρισμένου μάρτυρα» (*segregated witness*) για τα μπλοκ σύνοψης. Τα δεδομένα του μπλοκ χωρίζονται σε δεδομένα που είναι προς επεξεργασία και σε αυτά τα οποία χρησιμοποιούνται για την επαλήθευση της συναλλαγής εντός του μπλοκ, τα οποία ονομάζονται **«δεδομένα μαρτυρίας»** (*witness data*). Τα δεδομένα αυτά παραλείπονται από τους κόμβους που

πραγματοποιούν τις συναλλαγές τους χωρίς τις επικυρώσεις υπογραφής, βασιζόμενοι στην υπόθεση της **οριστικότητας**⁵ (finality).

Έτσι, το μέγεθος των **μπλοκ σύνοψης** προκύπτει από τον εξής τύπο:

$$\text{Μέγεθος Μπλοκ Σύνοψης (ή περίληψη συναλλαγής)} = p \times e \quad (6)$$

Όπου: $p \rightarrow$ πλήθος συμμετεχόντων για τα τελευταία 1500 μπλοκ,

$e \rightarrow$ μέγεθος αλλαγής υπολοίπου μίας εισαγωγής σύνοψης.

Για τον υπολογισμό του προσδοκώμενου μεγέθους ενός μπλοκ σύνοψης λαμβάνονται υπόψη οι ακόλουθες **βασικές υποθέσεις**:

- Ο συνολικός αριθμός των συμμετεχόντων είναι 200.000 (το μέγιστο).
- Καθημερινά δημιουργείται ένα μπλοκ σύνοψης.
- Η αλλαγή του μεγέθους αποτελεί το μόνο σημαντικό μέρος που λαμβάνεται υπόψη στο μπλοκ σύνοψης.

Το συνολικό μέγεθος ενός blockchain

Το συνολικό μέγεθος του blockchain διαχωρίζεται μεταξύ των εξής δύο μερών: Ενός **σταθερού μέρους** και ενός **μεταβλητού**, το οποίο επεκτείνεται με την πάροδο του χρόνου. Το **στατικό μέρος** περιλαμβάνει τα τελευταία 1000 key μπλοκ, όπου περιλαμβάνονται τα συνημμένα δεδομένα.

$$\text{Σταθερό Μέρος} = n \times k \quad (7)$$

Όπου: $n \rightarrow$ όγκος key μπλοκ, που αποθηκεύονται μαζί με τα δεδομένα συναλλαγής,

$k \rightarrow$ μέγεθος key μπλοκ.

Αξιοποιώντας την εξίσωση (7), μπορούμε να προχωρήσουμε σε υπολογισμό του σταθερού μέρους του μπλοκ, για το οποίο εξαιτίας της υπόθεσης πλήρους αποθήκευσης των τελευταίων 1000 μπλοκ δεν μπορούν να υπάρξουν μεγάλες αποκλίσεις, ήτοι ότι είναι ίσο με 11,3GB.

Το **μεταβλητό μέρος** αποτελείται από τα **μπλοκ σύνοψης** και ό,τι έχει απομείνει από τα key μπλοκ, αφού αφαιρεθούν τα δεδομένα συναλλαγής (transaction data).

Έτσι, προκύπτει η εξής μαθηματική εξίσωση:

$$\text{Μεταβλητό μέρος} = n \times k + m \times s \quad (8)$$

Όπου: $n \rightarrow$ πλήθος,

$m \rightarrow$ ετήσιο πλήθος μπλοκ σύνοψης,

$k \rightarrow$ μέγεθος key μπλοκ χωρίς τα δεδομένα συναλλαγής,

$s \rightarrow$ μέγεθος μπλοκ σύνοψης.

Ακολουθώντας τις **βασικές υποθέσεις** που προαναφέρθηκαν, το αποτέλεσμα ανάπτυξης της αλυσίδας σε ετήσια βάση είναι κατά προσέγγιση ίσο με 3.7GB.

Ενοποιώντας τις εξισώσεις (7) και (8), προκύπτει το συνολικό μέγεθος της αλυσίδας του μπλοκ, δηλαδή:

$$\text{Συνολικό μέγεθος του Μπλοκ} = \text{Σταθερό Μέρος} + \text{Μεταβλητό Μέρος} \quad (9)$$

⁵ Η οριστικότητα – αμεταβλητότητα, αναφέρεται στην παραδοχή ότι δεν υπάρχει καμία δυνατότητα τροποποίησης του μπλοκ.

4.4 Τα συστατικά μέρη ενός Κόμβου

(LTO Network, 2021)

Όπως είδαμε αναλυτικά και στα προηγούμενα δύο μέρη, το δίκτυο LTO επιτρέπει μεταξύ δύο ή περισσότερων μερών, το διαμοιρασμό δεδομένων και πληροφοριών, ενώ παράλληλα είναι σύγγραμμο με τον ΓΚΠΔ. Η ανταλλαγή των δεδομένων γίνεται χωρίς την απαίτηση ενός κεντρικού διαχειριστή ή κάποιου διαμεσολαβητή, αλλά μεταξύ των (ομότιμων) κόμβων του δικτύου. Για να επιτύχουν την ευρεία αποδοχή δημιουργίας του επόμενου κόμβου στο δίκτυο, τα συμβαλλόμενα μέρη αξιοποιούν το δημόσιο blockchain. Αυτό γίνεται μέσω της «αγκίστρωσης» των συναρτήσεων κατακερματισμού των ιδιωτικών συμβάντων - πληροφοριών. Το μέγεθος των μπλοκ είναι προκαθορισμένο στη δημόσια αλυσίδα, καθώς και η χρονολογική τους ακολουθία. Αυτή ακριβώς η χρονολογική ακολουθία είναι που προσφέρει την αλληλουχία των πληροφοριών που χρησιμοποιούνται για να επιτευχθεί η επιδιωκόμενη συναίνεση στο κομμάτι της ιδιωτικής αλυσίδας.

Συνοψίζοντας, θα λέγαμε ότι το LTO αποτελεί μία μορφή υβριδικού blockchain, όπου τα ιδιωτικά δεδομένα και πληροφορίες κοινοποιούνται με δημόσια συναίνεση.

Τα μέρη από τα οποία αποτελείται ένας κόμβος του δικτύου είναι τα εξής:

- **Πύλη Διεπαφής Προγραμματισμού Εφαρμογών (API gateway)**: Είναι ένας διακομιστής (HTTP) διαμεσολάβησης, που «φιλτράρει» τα αιτήματα και τα προωθεί στους κατάλληλους αιτούντες του δικτύου.

- **Υπηρεσία Ιδιωτικών Συμβάντων (Event Chain Service)**: Ένα κόμβος διατηρεί πολλά ιδιωτικά blockchain εντός του, τα οποία είναι διαχωρισμένα μεταξύ τους. Αυτό επιτυγχάνεται μέσω της χρησιμοποίησης της αρχιτεκτονικής του μοτίβου των μικροπηρεσιών (*microservices architecture pattern*), με την κάθε υπηρεσία να επηρεάζει ελάχιστα τη λειτουργία του κόμβου. Με τη μέθοδο αυτή είναι εύκολη η προσθήκη (ή αφαίρεση) και διαμόρφωση μίας υπηρεσίας στο πεδίο της εφαρμογής του κόμβου.

- **Επιπλέον Πρόσθετες Υπηρεσίες (Additional Services)**: Υπάρχει η δυνατότητα προσθήκης επιπλέον πρόσθετων υπηρεσιών με σκοπό την εκτέλεση αποκεντρωμένων εφαρμογών. Οι ροές εργασιών εκτελούνται μέσω του εκτεταμένου μηχανισμού πεπερασμένων καταστάσεων. Μέσω της επιτήρησης της κατανομής των δεδομένων μεταξύ των χρηστών του δικτύου, επιτυγχάνεται η σύγκλιση με το ΓΚΠΔ.

- **Υπηρεσίες Εναλλαγής (Queueer)**: Χρησιμοποιείται το πρωτόκολλο RabbitMQ⁶ για την ορθή ταξινόμηση των συμβάντων στους υπόλοιπους κόμβους.

- **Υπηρεσίες Αποστολής (Dispatcher)**: Αναλύει το περιεχόμενο των μηνυμάτων, αφού πρώτα έχουν ταξινομηθεί με τη σωστή χρονολογική σειρά, και εν συνεχεία τα προωθεί στην κατάλληλη υπηρεσία μέσα στον κόμβο.

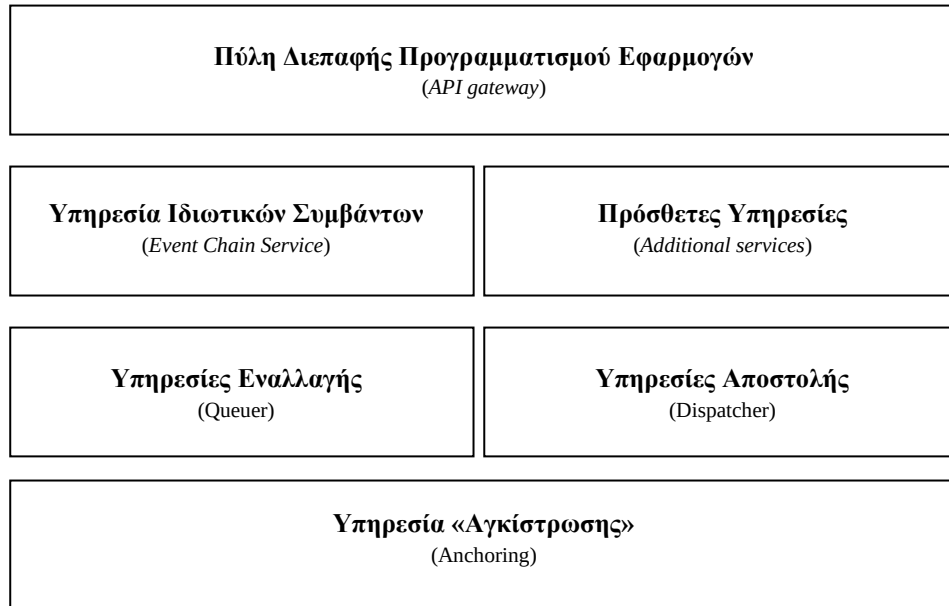
- **Υπηρεσία «Αγκίστρωσης» (Anchoring)**: Διασύνδεει την πλατφόρμα του LTO με το δημόσιο blockchain του δικτύου, το οποίο και είναι υπεύθυνο για την ακεραιότητα των δεδομένων, των πληροφοριών και των συμβάντων μέσω της

⁶ Η RabbitMQ, αποτελεί ένα λογισμικό ανταλλαγής μηνυμάτων ανοιχτού κώδικα στην οποία εφαρμόζονται διάφορα πρωτόκολλα.

Διπλωματική Εργασία: «Η τεχνολογία του Blockchain και η προσπάθεια
συμμόρφωσης της με τον ΓΚΠΔ»

«αγκίστρωσής» τους. Όπως αναφέρθηκε και σε προηγούμενο μέρος της ανάλυσής μας, ο χρησιμοποιούμενος αλγόριθμος για τις συναρτήσεις κατακερματισμού είναι ο SHA-2, ενώ για την ψηφιακή υπογραφή γίνεται χρήση της καμπύλης ED25519. Η χρήση του πρωτοκόλλου NG πετυχαίνει την άμεση επιβεβαίωση των συναλλαγών (συνήθως εντός 3 δευτερολέπτων), με την αξιοποίηση του δημοσίου blockchain ως αποθετηρίου των συναρτήσεων κατακερματισμού των δεδομένων.

Μία σχηματική αναπαράσταση των 6 στοιχείων που αναφέρθηκαν είναι η εξής:



Σχήμα 6: Τα δομικά συστατικά
ενός κόμβου στο δίκτυο LTO
(LTO Network, 2021)

Μέρος 5ο: Πρακτικές Εφαρμογές

(Binance, 2020) (Deep Analysis , 2020) (LetsFlow, 2021) (The team of LTO Network, 2018) (LTO Network, 2020)

5.1 Από το θεωρητικό μοντέλο στην πρακτική εφαρμογή

Στο προηγούμενο μέρος της ανάλυσής μας είδαμε το θεωρητικό σκέλος της δημιουργίας και οικοδόμησης του δικτύου LTO. Όπως προαναφέρθηκε, το LTO αποτελεί ένα υβριδικό blockchain, στο οποίο διασφαλίζεται η σωστή διαχείριση, επιβεβαίωση και ανταλλαγή πληροφοριών και δεδομένων μεταξύ των χρηστών του. Ο συνδυασμός των δύο επίπεδων *blockchain* (ιδιωτικών – δημοσίων *blockchain*), χρησιμοποιώντας ως μηχανισμό συναίνεσης το *Leased Proof of Stake*, συντελεί στη συμμόρφωση του δικτύου με το ΓΚΠΔ.

Το επίπεδο του ιδιωτικού *blockchain* ικανοποιεί τις απαιτήσεις των οργανισμών και των επιχειρήσεων, παρέχοντας τα κατάλληλα εργαλεία πρακτικής εφαρμογής τους. Από την άλλη μεριά, το δημόσιο «ελεύθερο» (permissionless) επίπεδο του blockchain εγγυάται μία αποκεντρωμένη προσέγγιση, στην οποία τα δεδομένα και οι πληροφορίες του ιδιωτικού επιπέδου διατηρούν την ακεραιότητα και ασφάλειά τους.

Η δημιουργία των *Live Contracts*, παρόμοια με αυτή των *Smart Contracts*, έχει ως βασικό στόχο τη βελτιστοποίηση των ροών εργασίας (*workflows*), που εκτελούνται μεταξύ των κόμβων του δικτύου.

Το στοιχείο, όμως, που διαφοροποιεί τη συγκεκριμένη αρχιτεκτονική blockchain από τα υπόλοιπα και τις αντίστοιχες πλατφόρμες εφαρμογής που ανήκουν στην ίδια ομάδα (*Enterprise Blockchain Applications*) είναι το γεγονός ότι τα κρυπτογραφικά *token* του δικτύου διαδραματίζουν κομβικό ρόλο τόσο σε τεχνικό, ως προς τον τρόπο λειτουργίας τους, όσο και σε αξιακό επίπεδο, ως προς τον τρόπο δημιουργίας της αξίας. Η προσέγγιση αυτή είναι ασυνήθιστη, καθώς τα περισσότερα εταιρικά *blockchain* προσπαθούν να είναι αποστασιοποιημένα από τον κόσμο της κρυπτογραφίας.

Η αξιοποίηση της κρυπτογράφησης πραγματοποιείται με τους ακόλουθους τρόπους:

- Η πληρωμή των λειτουργιών του δικτύου απαιτεί τη χρησιμοποίηση *token*. Υπάρχει ένα *token* και τρεις ανταλλάξιμοι εναλλακτικοί τύποι *token* (BEP2, ERC20 και BEP20).
- Μέσω του συγκεκριμένου μηχανισμού συναίνεσης (*LPoS*), υπάρχει ανταμοιβή στις περιπτώσεις των χρηστών και των οργανισμών που λαμβάνουν μέρος στη διαδικασία της επικύρωσης των κόμβων του δικτύου, είτε πρόκειται για φιλοξενία είτε για ενεργό συμμετοχή.
- Έχει καθοριστεί συγκεκριμένη μέθοδος, στην οποία καθορίζεται η προσφορά, η ροή και η διαχείριση των *token*, ενώ ξεκαθαρίζονται τα κίνητρα για τους συμμετέχοντες στη διαδικασία.

5.2 Πρακτικές Εφαρμογές Του Δικτύου (*LTO Netwrok - Use Cases*)

A. Proofi (Proofi, 2020)

Η συγκεκριμένη διεπαφή προγραμματισμού εφαρμογών (A.P.I.), δημιουργήθηκε με βάση τις αρχές που διέπουν το δίκτυο LTO. Πιο συγκεκριμένα, αποτελεί ένα εργαλείο στο οποίο μπορούν να δημιουργηθούν έγγραφα και προσχέδια εγγράφων τα οποία «αγκιστρώνονται» στο δημόσιο blockchain. Για τη δημιουργία των εγγράφων υπάρχει η δυνατότητα συλλογής δεδομένων από διάφορες εφαρμογές (π.χ. Gmail, Microsoft Outlook, Telegram, WhatsApp, Paypal, Dropbox, Salesforce κ.α.).

Η δημιουργία του προέκυψε από την ανάγκη επίλυσης του προβλήματος της παραποίησης της (ηλεκτρονικής) ταυτότητας των φυσικών προσώπων. Με την ηλεκτρονική υπογραφή της κάθε πραγματοποιούμενης ηλεκτρονικής συναλλαγής, επιτυγχάνεται η διατήρηση της ασφάλειας και της προστασίας των προσωπικών δεδομένων των χρηστών. Θα πρέπει να τονιστεί ότι η πλατφόρμα είναι σχεδιασμένη να πληροί τους κανονισμούς και το πλαίσιο του ΓΚΠΔ.

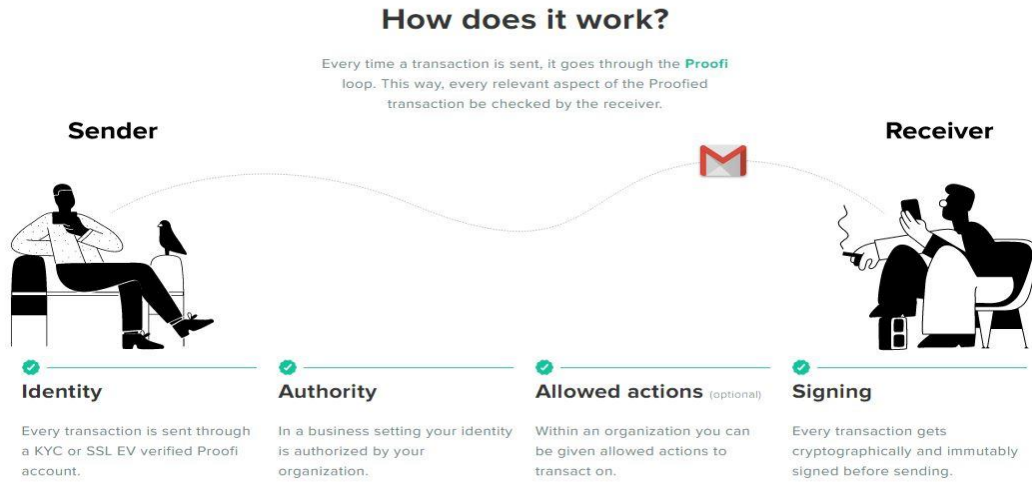
Τρόπος Λειτουργίας

Μεταξύ του αποστολέα και του παραλήπτη, κάθε συναλλαγή περνά από το «φίλτρο» του *Proofi*. Έτσι τεκμηριώνεται η πιστότητα – γνησιότητα και των δύο μερών. Η μεθοδολογία που ακολουθείται στη συγκεκριμένη πλατφόρμα, συνοψίζεται στα εξής βήματα:

- Ταυτότητα (*Identity*): Η ολοκλήρωση της κάθε συναλλαγής πραγματοποιείται μέσω της πρότερης επεξεργασίας της στο Proofi -φιλτραρίσματος. Η πιστοποίηση της συναλλαγής, γίνεται με τη χρησιμοποίηση των *Secure Sockets Layer Extended Validation (SSL EV) Certificate*.
- Εξουσιοδότηση (*Authority*): Η έγκριση και εξουσιοδότηση του κάθε χρήστη γίνεται από τον ίδιο τον οργανισμό.
- Επιτρεπόμενες Ενέργειες (Προαιρετική Επιλογή – *Allowed Actions*): Δίνεται η δυνατότητα καθορισμού συγκεκριμένων ακολουθούμενων ενεργειών, εντός των ορίων του οργανισμού.
- Υπογραφή (*Signature*): Πριν την αποστολή του εγγράφου, κάθε πραγματοποιούμενη συναλλαγή λαμβάνει μία κρυπτογραφημένη και μη αναστρέψιμη (*immutable*) υπογραφή με τα στοιχεία του κάθε αποστολέα.

Διπλωματική Εργασία: «Η τεχνολογία του Blockchain και η προσπάθεια συμμόρφωσης της με τον ΓΚΠΔ»

Η παραπάνω διαδικασία θα μπορούσε να συνοψιστεί με την παρακάτω εικόνα:



Εικόνα 3: Τρόπος λειτουργίας Proofi (Proofi, 2020)

Έτσι, διασφαλίζεται η πιστότητα των πληροφοριών των χρηστών. Είτε πρόκειται για μεμονωμένους χρήστες είτε για εταιρικούς, επιτυγχάνεται η σωστή και πιστή ανταλλαγή δεδομένων μεταξύ των χρηστών (δύο ή περισσότερων).

B. Waste Transport (LTO Network, 2020)

Πρόκειται για μία συνεργασία του Ολλανδικού Υπουργείου Υποδομών και Διαχείρισης Υδάτινων Πόρων με τους εμπλεκόμενους φορείς διαχείρισης απορριμάτων. Με την υιοθέτηση αυτής της μεθόδου, το Υπουργείο κατάφερε να εξοικονομήσει περισσότερα από 7 εκ. ευρώ.

Μέχρι πρότινος, υπήρχαν αρκετά προβλήματα τα οποία θα έπρεπε να ξεπεραστούν. Αυτά θα μπορούσαν να συνοψιστούν στα εξής:

- Μεγάλος αριθμός εμπλεκόμενων με δυσκολία μεταξύ τους (αποτελεσματικού) συντονισμού.
- Το κανονιστικό πλαίσιο καθορίζεται από την Ε.Ε., η οποία θεωρείται η ανώτερη εποπτεύουσα αρχή των **σχετιζομένων** διαδικασιών για τη διαχείριση των απορριμάτων (π.χ. αδειοδοτήσεις διαχείρισης, γνωστοποιήσεις μεταφορών απορριμάτων κ.ά.).
- Η διαχείριση των πολλαπλών διαδικασιών πραγματοποιούνταν συνήθως χειρόγραφα, με γραπτά έντυπα σε πολλές γλώσσες. Για παράδειγμα, στο Βέλγιο το φαξ εξακολουθούσε να χρησιμοποιείται σε αρκετές διαδικασίες.

Τρόπος Λειτουργίας

Η υιοθέτηση του δικτύου LTO, διευκόλυνε την όλη κατάσταση, καταφέροντας να εξαλείψει τις υπάρχουσες εγγενείς αδυναμίες. Πιο συγκεκριμένα, κατάφερε να επιλύσει τα παραπάνω ζητήματα με τους ακόλουθους τρόπους:

- Αυτοματοποίησε τους ελέγχους, τις εγκρίσεις και εκδόσεις των απαραίτητων αδειών στα αιτήματα μεταφοράς. Η κοινοποίηση των απαιτούμενων δεδομένων πραγματοποιείται απευθείας από τους άμεσα ενδιαφερομένους, χωρίς την ανάγκη οποιασδήποτε διαμεσολάβησης.
- Απλοποίησε τις διαδικασίες και ελαχιστοποίησε τις απαραίτητες προς χρήση πληροφορίες. Οι μεταφορείς μπορούν να κάνουν χρήση των κινητών τους τηλεφώνων ή άλλων συσκευών, προσκομίζοντας τα απαιτούμενα έγγραφα σε περίπτωση ελέγχου. Από την άλλη, ο ελεγκτής μπορεί να επιβεβαιώσει την ορθότητά τους μέσω της απευθείας πρόσβασής του στο δίκτυο του LTO.
- Η ψηφιοποίηση των δεδομένων και των πρωτοκόλλων από το χαρτί στα *Live Contracts* συνέβαλε στην απευθείας επικοινωνία και το διαμοιρασμό των πληροφοριών και των συστημικών ειδοποιήσεων σε πραγματικό χρόνο.

Εφαρμόζοντας την παραπάνω διαδικασία, όλα τα μέρη βγήκαν κερδισμένα. Εκτός από την εξοικονόμηση οικονομικών πόρων, όλες οι διαδικασίες επιταχύνθηκαν, ενώ ταυτόχρονα πληρούται η συμμόρφωση με το ΓΚΠΔ. Πιο συγκεκριμένα, κάθε εμπλεκόμενο μέρος «υπογράφει» για τη συμμετοχή του στη διαδικασία (είτε πρόκειται για την προσθήκη νέου εγγράφου είτε για τη συμμετοχή σε ένα από τα ακολουθούμενα προκαθορισμένα βήματα). Ύστερα από την υλοποίηση προκαθορισμένων βημάτων ή με το πέρας μίας προκαθορισμένης χρονικής ακολουθίας μέσω των *Live Contracts*, πραγματοποιείται διαγραφή των δεδομένων και των προσωπικών πληροφοριών που είχαν εισαχθεί στο δίκτυο. Έτσι διασφαλίζεται η συμμόρφωση με τον GDPR.

C. SignRequest (LTO Network , 2020) (SignRequest, 2021)

Όπως και στην περίπτωση του *Proofi*, η εφαρμογή έχει ως στόχο τη δημιουργία ψηφιακών εγγράφων των οποίων δεν υπάρχει η δυνατότητα παραποίησης, καθώς φέρουν την αντίστοιχη χρονοσφραγίδα (*timestamp*) κατά τη δημιουργία τους.

Το ζήτημα που υπήρχε ήταν ότι τα ηλεκτρονικά έγγραφα μπορούσαν να παραποιηθούν. Αυτό το κενό ήρθε να καλύψει η εφαρμογή του SignRequest. Πιο συγκεκριμένα, υπήρχαν τα εξής ζητήματα:

-Απόδειξη δημιουργίας εγγράφου: Σε περίπτωση που υπήρχε κάποια διχογνωμία σχετικά με την ημέρα και την ώρα δημιουργίας ενός εγγράφου, αναζητούνταν ένας αξιόπιστος τρόπος επιβεβαίωσης.

-Αυθεντικότητα Εγγράφου: Σε ενδεχόμενο διαφωνίας σχετικά με την συμφωνημένη έκδοση και υπογραφή ενός εγγράφου, θεμιτό θα ήταν οι αντισυμβαλλόμενοι να έχουν τη δυνατότητα επιβεβαίωσής του πρωτότυπου.

-Επαλήθευση εγγράφου: Κατά την υπογραφή ενός εγγράφου, συνήθως υπάρχουν αρκετά μέρη που εμπλέκονται. Σκόπιμο θα ήταν να υπάρχει ένα μηχανισμός ο οποίος διασφαλίζει την αναγκαία εμπιστοσύνη σχετικά με τη γνησιότητα του εγγράφου, ενώ παράλληλα παρέχεται η δυνατότητα αυτόνομης επιβεβαίωσής του.

Τρόπος Λειτουργίας

Η χρησιμοποίηση του δικτύου LTO έδωσε τις απαιτούμενες λύσεις στα παραπάνω προβλήματα. Η δημιουργούμενη συνάρτηση κατακερματισμού από το αρχικό έγγραφο κατάφερε επιτυχώς να λειτουργήσει ως το «δακτυλικό αποτύπωμα» που έλειπε μέχρι πρότινος. Η συνάρτηση hash αποθηκεύεται εντός του δικτύου LTO. Ο κάθε ενδιαφερομένος ο οποίος έχει πρόσβαση στα δεδομένα μπορεί να επιβεβαιώσει τη γνησιότητα του εγγράφου, συγκρίνοντας το hash που έχει στα χέρια έναντι αυτού που είναι αποθηκευμένο στο σύστημα. Εκτός βέβαια του hash, υπάρχει και η αντίστοιχη χρονοσφραγίδα (timestamp) του εγγράφου. Έτσι, τα έγγραφα γίνονται εύκολα επαληθεύσιμα, ενώ παράλληλα είναι αυτονομημένα. Ένα ακόμη σημαντικό στοιχείο αποτελεί το γεγονός ότι, χρησιμοποιώντας την τεχνολογία του *blockchain*, καταργήθηκαν οι μεσάζοντες. Ο κάθε συμβαλλόμενος έχει απευθείας πρόσβαση στο δίκτυο χωρίς την αναγκαιότητα να βασίζεται σε τρίτους.

D. Carptions (Carptions, 2021) (LTO Network, 2021)

Πρόκειται για μία εφαρμογή η οποία έχει ως στόχο τη διασφάλιση της ορθότητας και ακεραιότητας εταιρικών αναφορών επιθεώρησης (*Environmental, Health & Safety Reports – E.H.S.*) και των αντίστοιχων δεδομένων καταχώρησης που σχετίζονται με αυτές (προσωπικά ή μη).

Με τη συγκεκριμένη εφαρμογή γίνεται προσπάθεια να επιλυθούν τα εξής ζητήματα:

- *Δυνατότητα παραποίησης των εγγράφων*: Η αλλοίωση των γραπτών αναφορών και λιστών γίνεται ευκολότερα, αφού δεν υπάρχει κάποιος μηχανισμός που να διασφαλίζει τη μη τροποποίησή τους. Επίσης, χωρίς τον καθορισμό κάποιας μεθόδου περαιτέρω ελέγχου, η δημιουργία ενός εγγράφου (π.χ. PDF) ή η ψηφιακή λήψη μίας εικόνας στη διάρκεια μίας επιθεώρησης δεν καθίστανται ικανοποιητικά στοιχεία για την ακεραιότητα των πληροφοριών που περιέχονται στις αναφορές.

- *Τροποποίηση των δεδομένων*: Είναι σύνηθες η αποθήκευση των δεδομένων και των πληροφοριών να πραγματοποιείται σε κεντρικούς διακομιστές (server). Το γεγονός αυτό αποκαλύπτει την αδυναμία που υπάρχει στη ροή των ακολουθούμενων διαδικασιών με την πιθανότητα αλλοίωσης των συγκεκριμένων δεδομένων.

- *Ανταλλαγή των πληροφοριών και πρόσβαση σ' αυτές*: Κατά τη διάρκεια των επιθεωρήσεων, τα δεδομένα θα πρέπει να κοινοποιούνται τόσο σε εργαζομένους εντός της εταιρίας όσο και εκτός της. Όσο πιο «απομακρυσμένη» είναι η επικοινωνία μεταξύ των εμπλεκόμενων μερών τόσο πιο δύσκολος καθίσταται ο διαμοιρασμός των πληροφοριών εντός του συγκεκριμένου δικτύου.

Η πρόταση του Carptions, έδωσε τις απαιτούμενες λύσεις στα προβλήματα που αναφέραμε παραπάνω. Πιο συγκεκριμένα:

- Πέτυχε την *ακεραιότητα* και *διασφάλισε την αμεταβλητότητα των δεδομένων και των πληροφοριών (capturing immutable evidence)*. Οι συσκευές που χρησιμοποιούνται για τη λήψη των απαιτούμενων δεδομένων είναι πιστοποιημένες, με την καθεμία να περιέχει ένα αναγνωριστικό αριθμό (ID). Μέσω αυτού, υπογράφεται η κάθε

καταχώρηση δεδομένων, ενώ δημιουργείται και η αντίστοιχη αναφορά. Έτσι προκύπτει μία μη τροποποιήσιμη αναφορά.

- Οι αναφορές υλοποιούνται σε πραγματικό χρόνο και είναι συμμορφούμενες με τις απαιτήσεις και τις προδιαγραφές (*real time compliance reporting*). Για τις περιπτώσεις των επιχειρήσεων που δουλεύουν με επικίνδυνα προϊόντα ή τα επεξεργάζονται σε επικίνδυνα περιβάλλοντα, η επίδειξη συμμόρφωσης καθίσταται σημαντική. Ο συνδυασμός της εφαρμογής του Carptions με την αρχιτεκτονική του δικτύου LTO, δίνει τη δυνατότητα όλες οι αναφορές και οι καίριες διαδικασίες της επιχείρησης να παράγονται σε πραγματικό χρόνο.

- Ο διαμοιρασμός πληροφοριών έγινε αποτελεσματικός (*effective data sharing*). Όπως αναφέρθηκε και παραπάνω, η εφαρμογή στηρίζεται στην αρχιτεκτονική του δικτύου LTO. Μέσω αυτού επιτυγχάνεται και ο διαμοιρασμός των πληροφοριών της κάθε σχετιζόμενης ομάδας. Η (επανα)χρησιμοποίηση των πληροφοριών καθώς και η αυτοματοποίηση των διαδικασιών είχε θετικά αποτελέσματα για όλους τους συμμετέχοντες.

Η υιοθέτηση και χρησιμοποίηση της συγκεκριμένης εφαρμογής, στηριζόμενης στο δίκτυο LTO, κατάφερε να προσφέρει λύσεις και να παραγάγει τις απαιτούμενες απαντήσεις στα προβλήματα που υπήρχαν στο συγκεκριμένο τομέα. Με τον τρόπο αυτό, επιλύθηκαν τα τρία προβλήματα (*αυτοματοποίηση διαδικασιών, αποτροπή παραποίησης δεδομένων, διαμοιρασμός δεδομένων*), ενώ ταυτόχρονα εξοικονομήθηκαν πόροι.

E. Artwork Authenticity on Blockchain (LTO Network , 2021)

Μεγάλη πρόκληση αποτελεί η διασφάλιση της γνησιότητας των έργων τέχνης ανεξαρτήτως της εποχής κατά την οποία αυτά δημιουργήθηκαν. Βασική επιδίωξη του κάθε αγοραστή ήταν πάντοτε η απόκτηση της γνήσιας δημιουργίας και όχι μίας πιστής απομίμησης ή αντιγραφής ενός έργου τέχνης. Σε αρκετές περιπτώσεις, έχει παρατηρηθεί ότι τα παρεχόμενα πιστοποιητικά γνησιότητας είχαν παραποιηθεί. Οι νέες τεχνολογίες ενίσχυσαν ακόμη περισσότερο τη δυνατότητα πλαστογράφησης τους. Βέβαια, από τη μεριά του αγοραστή, υπήρχε η επιδίωξη εξεύρεσης μίας μεθόδου η οποία θα επικύρωνε την αυθεντικότητα του κάθε έργου τέχνης.

Μία προτεινόμενη λύση στο συγκεκριμένο πρόβλημα ήρθε να δώσει η συνεργασία της V-ID με τριάντα και πλέον επιχειρήσεις, στα πλαίσια της οποίας χρησιμοποιείται μία πλατφόρμα πιστοποίησης έργων τέχνης στηριζόμενη στο δίκτυο LTO. Η συγκεκριμένη μέθοδος είχε ως αποτέλεσμα την κατάργηση της ανάγκης ύπαρξης μεσαζόντων για την επιβεβαίωση της γνησιότητας του έργου. Με την πλατφόρμα βασισμένη σε ανοικτά πρότυπα, κάθε ενδιαφερόμενος μπορεί να επιβεβαιώσει τη γνησιότητα του, μέσω της μοναδιαίας χρονοσφραγίδας για το κάθε πιστοποιητικό γνησιότητας. Στο καθένα από αυτά, περιέχονται δύο στοιχεία: η συνάρτηση κατακερματισμού του πιστοποιητικού (*hash certificate*) και η χρονοσφραγίδα (*timestamp*).

Εύκολα, λοιπόν, γίνεται αντιληπτή η σημασία της δημιουργίας ενός αποδεικτικού για το κάθε έργο τέχνης, ανεξαρτήτως εάν πρόκειται για τη δημιουργία ενός έργου κάποιου ανωνύμου καλλιτέχνη ή για έναν πίνακα του Ρέμπραντ. Το πιστοποιητικό

αντιπροσωπεύει το (ψηφιακό) «δακτυλικό αποτύπωμα», καθώς για κάθε νέο έργο τέχνης δημιουργείται μία καινούργια συνάρτηση κατακερματισμού. Η αποθήκευση της συνάρτησης γίνεται ταυτόχρονα σε όλα τα συστήματα τα οποία είναι συνδεδεμένα στην αλυσίδα του *blockchain*. Έτσι, σε περίπτωση που κάποιος έχει στην κατοχή του ένα πιστοποιητικό, μπορεί να το διασταυρώσει συγκρίνοντάς το με αυτό που υπάρχει ήδη εντός του *blockchain*.

Ως συνέπεια, η πρότερη κατάσταση χειροκίνητης εισαγωγής των δεδομένων στο σύστημα με τη λήψη e-mail, φαξ ή γραπτών επιστολών αποτελεί παρελθόν. Εφαρμόζοντας της τεχνολογία του LTO, η συλλογή και συμπλήρωση των αναγκών πληροφοριών στο σύστημα γίνεται μεθοδικά και δομημένα για όλους τους συμμετέχοντες. Η συγκεκριμένη μέθοδος είχε ως αποτέλεσμα μία πιο σωστή διαχείριση, μειώνοντας τις απαιτούμενες ενέργειες και το απαιτούμενο κόστος λειτουργίας των συγκεκριμένων υπηρεσιών (περίπου κατά 30%). Ένα ακόμη θετικό στοιχείο αποτελεί η ευελιξία και προσαρμοστικότητα της συγκεκριμένης πλατφόρμας. Η χρήση του δικτύου δεν απαιτεί την αλλαγή των υποδομών στο *hardware* των επιχειρήσεων, αλλά μπορεί να ενσωματωθεί σ' αυτά. Η εφαρμογή του δικτύου είναι πολύ απλοποιημένη, με τις εργασίες να διεκπεραιώνονται όπως και στην πρότερη κατάσταση. Για οποιονδήποτε κλάδο, η δυνατότητα επίδειξης συμμόρφωσης αποτελεί σημαντικό πλεονέκτημα. Η χρησιμοποίηση της «ανοιχτής πλατφόρμας» έδωσε την δυνατότητα καταγραφής όλων των δεδομένων για κάθε βήμα, παρέχοντας την απαιτούμενη επαλήθευση και συμμόρφωση με τους ισχύοντες κανόνες και αναφορές σε όλους τους ενδιαφερόμενους ανεξαρτήτως σχέσης τους με αυτή.

Άλλες Περιπτώσεις Εφαρμογής (Binance, 2020)

Οι παραπάνω πρακτικές εφαρμογές του δικτύου του LTO αποτελούν μία συνοπτική παρουσίαση μερικών μόνο περιπτώσεων, στις οποίες έχει εφαρμοστεί επιτυχώς η συγκεκριμένη τεχνολογία. Υπάρχουν ακόμη πολλοί τομείς στους οποίους η τεχνολογία είτε έχει ήδη εκτελεστεί είτε σχεδιάζεται άμεσα στο εγγύς μέλλον. Ενδεικτικά, μερικά ακόμη παραδείγματα είναι η αγορά των διαμαντιών (*Diamond Traceability*), η ψηφιοποίηση μετοχικών μεριδίων επιχειρήσεων (*Digital Share Registry*) και οι συμφωνίες μίσθωσης ή αγοραπωλησίας ακινήτων (*Lease Agreements*)

Επιπρόσθετως, αξίζει να αναφέρουμε ότι τα τελευταία δύο χρόνια έχουν υπάρξει και αρκετές ακόμη εμπορικές συνεργασίες με συγκεκριμένες επιχειρήσεις και διεθνείς οργανισμούς (π.χ. η IBM, η ISO, η BP, η Bosch και η Airbus).

Μέρος 6^ο: Επίλογος - Συμπεράσματα

Στην ανάλυσή μας, είδαμε μία προτεινόμενη πρακτική λύση, η οποία απαντά στο πρόβλημα του συγκερασμού μεταξύ της τεχνολογίας του blockchain και του ΓΚΠΔ. Το δίκτυο LTO, με την υβριδική του προσέγγιση, παρουσιάζει μία μέθοδο κατά την οποία η συνεργασία τους καταφέρνει να είναι αποτελεσματική.

Ο διαχωρισμός της ανταλλαγής των δεδομένων και της συναίνεσης μεταξύ των κόμβων του δημιουργεί δύο επίπεδα: ένα δημόσιο επίπεδο επικύρωσης των πληροφοριών και ένα προσαρμοσμένο ιδιωτικό επίπεδο. Απώτερος στόχος είναι η δημιουργία πρακτικών λύσεων που μπορούν εύκολα να ενσωματωθούν σε υφιστάμενα εταιρικά συστήματα και υπολογιστικά περιβάλλοντα, ενώ πληρούνται οι επιταγές του ΓΚΠΔ.

Με τα *Live Contracts*, οι χρήστες μπορούν να πραγματοποιούν το διαμοιρασμό των δεδομένων τους χωρίς να προαπαιτείται η ύπαρξη της μεταξύ τους εμπιστοσύνης. Η κατάργηση της εξάρτησης των εμπλεκόμενων μερών από τον ανθρώπινο παράγοντα, επιτρέπει στους συμμετέχοντες να επικεντρωθούν στη βελτίωση της αποτελεσματικότητας, της διαφάνειας και της ασφάλειας των ενεργειών τους.

Εντός του δικτύου, καλύπτεται ολόκληρο το φάσμα των απαιτούμενων ενεργειών για την ανταλλαγή πληροφοριών: η διευκόλυνση ελέγχου ολόκληρης της διαδικασίας από τους συμμετέχοντες (κόμβους), ο αποτελεσματικός διαμοιρασμός των δεδομένων μεταξύ των εμπλεκόμενων, καθώς και η διάσφαλιση κοινοποίησης των πληροφοριών τους σε τρίτους.

Στόχο της ομάδας διαχείρισης του δικτύου αποτελεί η προσέλκυση περισσότερων συναλλαγών και επικυρωτών εντός του, διευρύνοντας το εύρος των παρεχομένων προτάσεων εφαρμογής. Το υφιστάμενο πεδίο συνεχώς διευρύνεται, αυξάνοντας τον αριθμό των εμπλεκόμενων.

Συνοψίζοντας, είδαμε τη δημιουργία μίας ολοκληρωμένης πρότασης, που συνδυάζει την τεχνολογία του blockchain με τον GDPR. Αφού πρώτα χτίσαμε το αναγκαίο θεωρητικό μοντέλο, προχωρήσαμε σε μερικές πρακτικές εφαρμογές υλοποίησής του.

Οι προοπτικές διάδοσης και ανάπτυξης είναι πολλά υποσχόμενες. Η απότομη απόκτηση δημοσιότητας της αγοράς κρυπτονομισμάτων έχει στρέψει το ενδιαφέρον προς την κατεύθυνση της τεχνολογίας του Blockchain. Το δίκτυο του LTO στοχεύει σε επιχειρήσεις, οργανισμούς και κράτη που επιθυμούν τη συμμόρφωσή τους με το ΓΚΠΔ. «Στο τεχνολογικό κομμάτι είμαστε ακόμη πίσω εξαιτίας της έλλειψης προγραμματιστών για το περιβάλλον του Blockchain» (Zaki, 2019). Ωστόσο, τα πρώτα αναγκαία βήματα εξέλιξης έχουν ήδη αναδυθεί. Η ενασχόληση των κρατών και των

Διπλωματική Εργασία: «Η τεχνολογία του Blockchain και η προσπάθεια
συμμόρφωσης της με τον ΓΚΠΔ»

επιχειρήσεων με το συγκεκριμένο κλάδο αποδεικνύει ότι το τρένο έχει ήδη μπει σε
τροχιά -περιμένει να το συναντήσουμε στη επόμενη γωνία του δρόμου.

Χρησιμοποιούμενη Βιβλιογραφία

- Article 29 - Data Protection Working Party (2014, 05). Ανάκτηση από Europa EU: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
- Bach, L., Mihaljevic, B. & Zagar, M. (2018), *Comparative Analysis of Blockchain Consensus Algorithms. 41st International Convention on Information and Communication Technology*. IEEE. doi:10.23919/MIPRO.2018.8400278.
- Binance (2020, February), *Binance Research - LTO Network*. Ανάκτηση από Research Binance: <https://research.binance.com/en/projects/lto-network>.
- Capptions (2021), *Capptions -EHS Your Way*. Ανάκτηση από Capptions: <https://www.capptions.com/>.
- Deep Analysis, (2020), *Deep Analysis - LTO Network*. doi:<https://www.deep-analysis.net/vendor-vignette/lto-network/>.
- Ehmke, C., Blum, F. & Gruhn, V. (2019), *Properties of Decentralized Consensus Technology - Why not every Blockchain is a Blockchain*. doi:10.13140/RG.2.2.35506.45765.
- European Parliamentary Research Service (July 2019), *Can distributed ledgers be squared with European data protection law? Panel for the Future of Science and Technology* (σ. page 44). Scientific Foresight Unit (STOA). doi:[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).
- Finck, M. (2018), *Blockchain and Data Protection in the European Union. European Data Protection Law Review, Volume 4*(Issue 1), Pages 17 - 35. doi:https://edpl.lexxion.eu/data/article/12327/pdf/edpl_2018_01-007.pdf.
- Gangmax Blog (2019, Kanuary), *What is Merkle DAG*. Ανάκτηση από <https://gangmax.me/blog/2019/01/03/what-is-merkle-dag/>.
- Georgiou, D. & Lambrinoudakis, C. (2020, December), *Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)*. doi:file:///C:/Users/user/Downloads/information-11-00586-v2.pdf.
- Geroni, D. (2020, December), *What Are Ricardian Contracts? A Comprehensive Guide*. Ανάκτηση από 101 Blockchains: <https://101blockchains.com/ricardian-contracts/#prettyPhoto>.
- Green, T. (2019, March), *Different Types Of DLTs And How They Work*. Ανάκτηση από https://medium.com/@support_61820/different-types-of-dlts-and-how-they-work-cfd4eb218431.
- iubenda (2020), *What is LGPD and how do you become compliant?* doi:<https://www.iubenda.com/en/help/26706-lgpd-guide>.
- Jelurida. (2020), *What is Nxt?* Ανάκτηση από Jelurida: <https://www.jelurida.com/nxt/what-is-nxt>.
- Lee, D. & Park, N. (March 2020), *Blockchain based privacy preserving multimedia*. doi:<https://doi.org/10.1007/s11042-020-08776-y>.
- LetsFlow (2021), *LetsFlow · the workflow engine developers love. (LTO)* Ανάκτηση από LetsFlow: <https://www.letsflow.io/>.
- LTO Network (2020), *LTO Network - Use Cases - Digital signatures on blockchain*. Ανάκτηση από <https://ltonetwork.com/use-cases/digital-signatures-on-blockchain/>.

- LTO Network (2021), *LTO Network - Use Cases - Artwork authenticity on blockchain*. Ανάκτηση από LTO Network: <https://ltonetwork.com/use-cases/artwork-authenticity-on-blockchain/>.
- LTO Network (2019), *The basics - Setup a node and run your first Live Contract*. Ανάκτηση από LTO Network: <https://docs.ltonetwork.com/tutorials/live-contracts/the-basics>.
- LTO Network (2020), *LTO Network - Use Cases*. (LTO Network) doi:<https://ltonetwork.com/use-cases/>.
- LTO Network (2020), *LTO Network - Use Cases - Waste Transport on blockchain*. Ανάκτηση από <https://ltonetwork.com/use-cases/waste-transport-on-blockchain/>.
- LTO Network (2021), *Inside an LTO Node - Select any component to learn more about our setup*. Ανάκτηση από LTO Network: <https://www.ltonetwork.com/tech/>.
- LTO Network (2021), *LTO Network - Use Cases - Inspection reports on blockchain*. Ανάκτηση από LTO Network: <https://ltonetwork.com/use-cases/inspection-reports-on-blockchain/>.
- LTO Network, (September 2018), *Blockchain for Decentralized Workflows*. LTO Network. doi:<https://ltonetwork.com/documents/LTO%20Network%20-%20Technical%20Paper.pdf>.
- Lubowicka, K. (2021, March), *6 New Privacy Laws Around The Globe You Should Pay Attention To*. Ανάκτηση από PIWIK Pro: <https://piwik.pro/blog/privacy-laws-around-globe/>.
- Lumb, R., Treat, D. & Jelf, O. (2016), *Editing The Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world*. Accenture. doi:https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf.
- Lyons , T., Courcelas, L. & Timsit, K. (October 2018), *Blockchain and The GDPR*. The European Union Blockchain Observatory and Forum. doi:https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.
- Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. Technical Report., doi:<https://bitcoin.org/bitcoin.pdf>.
- Natoli, C., Gramoli, J. & Esteves-Verissimo, P. (August 2019), *Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure*. Cornell University. doi:1908.08316v1.
- PECB -General Data Protection Regulation (2017, November), *Data Protection Principles*. Ανάκτηση από PECB: <https://pecb.com/whitepaper/general-data-protection-regulation-gdpr>.
- Proofi (2020), *Proofi - How does it Work*. Ανάκτηση από <https://www.proofi.com/>.
- Rea, N. & Sutton , A. (2019), *Putting a value on data*. PricewaterhouseCoopers LLP. doi:<https://www.pwc.co.uk/data-analytics/documents/putting-value-on-data.pdf>.
- Rosic, A. (2020, November), *What is Blockchain Technology? A Step-by-Step Guide For Beginners*. doi:<https://blockgeeks.com/guides/what-is-blockchain-technology/>.
- Shahaab, A., Lidgley, B., Hewage, C. & Khan, I. (2019), *Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review*. IEEE Access. doi:10.1109/ACCESS.2019.2904181.
- SignRequest (2021), *SognRequest - how it works*. Ανάκτηση από SingRequest: <https://signrequest.com/en/how-it-works>.

- Simmons, D. (2021, January), *12 Countries with GDPR-like Data Privacy Laws*. (Comforte Blog) doi:<https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws>.
- SSL Shop (2021, January), *Symmetric VS Asymmetric Encryption – Which is Morer Secure?* Ανάκτηση από SSL Shop: <https://www.cheapsslshop.com/blog/symmetric-vs-asymmetric-encryption-whats-the-difference/>.
- Sukhwani, H., Martinez, J., Chang, X. & Trivedi, K. (September 2017), Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). *36th Symposium on Reliable Distributed Systems*,. IEEE.
- Szabo, N. (1996), *Smart Contracts: Building Blocks for Digital Markets*. Ανάκτηση από https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/L_OTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
- The team of LTO Network (2018), *LTO Network - Token Economy*. LTO. doi:<https://ltonetwork.com/documents/LTO%20Network%20-%20Token%20Economy.pdf>.
- The Team of LTO Netwrok (November 2018), *LTO Network - Token Economy*. LTO Netwrok. doi:<https://ltonetwork.com/documents/LTO%20Network%20-%20Token%20Economy.pdf>.
- Wang , S., Ouyang, L., Yuan, Y., Ni, X., Han, X. & Wang, F. (November 2019), Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems*, 49(11). doi:10.1109/TSMC.2019.2895123.
- Waves (2021), *Waves - About Us*. Ανάκτηση από Waves: <https://www.waves.com/about-us>
- Zaki , I. (2019, January), *Blockchain Adoption Could Be Closer Than We Think*. Ανάκτηση από Hackernoon: <https://hackernoon.com/blockchain-adoption-could-be-closer-than-we-think-e68bebaebca4>.
- Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (June 2017), An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *6th IEEE International Congress on Big Data*. doi:10.1109/BigDataCongress.2017.85.
- Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2016), *Κανονισμός (ΕΕ) 2016/679 Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων - ΓΚΠΠΔ*. Βρυξέλλες: Επίσημη Σελίδα της Ευρωπαϊκής Ένωσης. doi:<https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=HR>.
- Ομάδα Εργασίας ΣΕΒ (2018), *Ο νέος Γενικός Κανονισμός για την Προσταία Δεδομένων (GDPR): Εφαρμογή και προκλήσεις για τις επιχειρήσεις στην εποχή της ψηφιοποίησης*. Αθήνα: ΣΕΒ. Ανάκτηση από https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf.
- Σφακιανάκης - Μακρυπούλιας (2021), *GDPR - Εισαγωγή στο νέο Γενικό Κανονισμό Προστασίας Δεδομένων*. Ανάκτηση από GDPR gr: <https://www.gdprgreece.com/>.

Συμπληρωματική Βιβλιογραφία

[1] Nam, Y., Shin, E., Lee, S., Jung, S., Bae, Y., Kim, J., “*Global - scale GDPR Compliant Data Sharing System*”, IEEE, International Conference on Electronics, Information, and Communication (ICEIC), January 2020, Barcelona.

DOI : [10.1109/ICEIC49074.2020.9051171](https://doi.org/10.1109/ICEIC49074.2020.9051171)

[2] Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M., “*Privacy Issues and Data Protection in Big Data: A Cases Study Analysis under GDPR*”, Cornell University, Proceedings of the 2018 IEEE International Conference on Big Data, 2018.

DOI : <https://arxiv.org/pdf/1811.08531.pdf>

[3] Al-Zaben, N., Onik Md, M.H., Yang, J., Lee, N., Kim, C., “*General Data Protection Regulation Complied Blockchain Architecture for Personal Identifiable Information Management*”, IEEE, IEEE Transaction On Information Forensics And Security, October 2019.

DOI : <https://arxiv.org/pdf/1904.03038.pdf>

[4] Truong, N. B. , Sun, K., Guo, Y., “*Blockchain - based Personal Data Management: From Fiction to Solution*”, IEEE 18th International Symposium on Network Computing and Applications (NCA), September 2019.

DOI : [10.1109/NCA.2019.8935049](https://doi.org/10.1109/NCA.2019.8935049)

[5] Ji, Y., Bae, S., Shin, Yongtae, “*A Personal Information Management Using Blockchain*”, IEEE, 2019 International Conference on Information Networking (ICOIN), January 2019.

DOI : [10.1109/ICOIN.2019.8718144](https://doi.org/10.1109/ICOIN.2019.8718144)

[6] Markovikj, D., Gievska, S., Kosinski, M., Stillwell, D., “*Mining Facebook Data for Predictive Personality Modeling*”, Proceedings Of AAAI International Conference on Weblogs and Social Media (ICWSM), January 2013.

DOI : [file:///C:/Users/user/Downloads/6179-30320-1-PB.pdf](https://arxiv.org/pdf/1301.3816v1.pdf)

[7] Greenwald, G., MacAskill, E., “*NSA Prism program taps into user data of Apple, Google and others*”, The Guardian, January 2013.

DOI:<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data#:~:text=7%20years%20old-,NSA%20Prism%20program%20taps%20in%20to,of%20Apple%2C%20Google%20and%20others&text=The%20National%20Security%20Agency%20has,document%20obtained%20by%20the%20Guardian.>

[8] Lee, N, Yang, J., Onik MD, M.H., Kim, C., “*Modifiable Public Blockchains Truncated Hashing and Sidechains*”, IEEE Access (Volume: 7), November 2019.

DOI : [10.1109/ACCESS.2019.2956628](https://doi.org/10.1109/ACCESS.2019.2956628)

[9] Nget, R., Cao, Y., Yoshikawa, M., ‘‘How to Balance Privacy and Money through Pricing Mechanism in Personal Data Market’’, 40th International ACM SIGIR Conference on Research and Development in Information Retrieval eCom, August 2017.

DOI : http://ceur-ws.org/Vol-2311/paper_15.pdf

[10] Weber, T., Prinz, W., ‘‘Trading User Data: A Blockchain Based Approach’’, 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 547-554, 2019.

DOI : <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8939246>

[11] Viseu, A. Clement, A., Aspinall, J., ‘‘Situating Privacy Online - Complex Perceptions and everyday practices’’, Information, Communication & Society, 7:1, 92-114, February 2007.

DOI: [10.1080/1369118042000208924](https://doi.org/10.1080/1369118042000208924)

[12] Zyskind, G., Nathan, O., Pentland, A., ‘‘Enigma: Decentralized Computation Platform with Guaranteed Privacy’’, Cornell University, January 2015.

DOI: <https://arxiv.org/pdf/1506.03471.pdf>

[13] Mansour, E., Smbra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., Aboulmaga, A., Berners-Lee, T., ‘‘A Demonstration of the Solid Platform for Social Web Applications’’, WWW '16, April 2016.

DOI: <http://dx.doi.org/10.1145/2872518.2890529>

[14] Simply Explained , "IPFS: Interplanetary file storage!", YouTube, May 2018.

DOI: <https://www.youtube.com/watch?v=5Uj6uR3fp-U>

[15] Coelho, F., Younes, G., ‘‘The GDPR-Blockchain paradox: a work around’’, 1st workshop on GDPR compliant systems, co-located with 19th ACM International Middleware Conference, December 2018, Rennes, France.

DOI:https://www.researchgate.net/publication/329656420_The_GDPR-Blockchain_paradox_a_work_around

[16] Chowdhury, M. J. M., Ferdous Md., Sadek, Biswas, K., Chowdhury, N., Kayes, A.S.M., Alazab, M., Watters, P., ‘‘A Comparative Analysis of Distributed Ledger Technology Platforms’’, IEEE Access (Volume: 7), November 2019.

DOI: [10.1109/ACCESS.2019.2953729](https://doi.org/10.1109/ACCESS.2019.2953729)

[17] Zyskind, G., Nathan, O., Pentland, A., ‘‘Decentralizing Privacy: Using Blockchain to Protect Personal Data’’, IEEE Security and Privacy Workshops, May 2015.

DOI: [10.1109/SPW.2015.27](https://doi.org/10.1109/SPW.2015.27)

[18] Chowdhury, M. J. M., Colman, A. , Kabir, M. A., Han, J., Sarda, P., “*Blockchain as a Notarization Service for Data Sharing With Personal Data Store*”, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, August 2018.

DOI: [10.1109/TrustCom/BigDataSE.2018.00183](https://doi.org/10.1109/TrustCom/BigDataSE.2018.00183)

[19] Alessi, M., Camillò, A., Giangreco, E., Matera, M., Pino, S., Storeli, D., “*Make users own their data: a decentralized personal data store prototype based on Ethereum and IPFS*”, 3rd International Conference on Smart and Sustainable Technologies (SpliTech), June 2018.

DOI: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8448350>

[20] Buterin, V., “*Privacy on the Blockchain*”, *Ethereum Blog*.

DOI: <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/>

[21] Buterin, V., “*Ethereum White Paper: A next generation smart contract & decentralized application platform*”, Ethereum Wiki Github.

DOI:https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[22] Tapscott, D., Tapscott, A., “*How the Tech Behind Bitcoin Will Change Your Life*”, Time, May 2016.

DOI:https://d3c33hcgiewv3.cloudfront.net/Xz6zYEQUEemo6BKcywtCxcg_2ed55dce51e04cf0869b64bf3cb7740e_Tapscott--Tapscott-2016-How-the-Tech-Behind-Bitcoin-Will-Change-Your-Life_Time.pdf?Expires=1595894400&Signature=P1fKqJ3rQwDxF4KAKxkQ9jBaVDfhSCxhlc4Rn6N2t77nMjjqjw14bcvLH5o8ffQRk-aBg3oBiA1A~wwsy16BqIZ1Xlz1jq~1YG~DCyfVSfK4qvQNo-GNNM1rN~upTvIGIIDuH~JvLpwmRNphtw5f0HoujKKOVaT3XtNrVSMOpI_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A

[23] Jobs, J., “*A Brief History on the Origins Of Blockchain*”, Medium.com, February 2016.

DOI: <https://medium.com/@jmrjobs/a-brief-history-on-the-origins-of-blockchain-6210ce345a21>

[24] Szabo, N., “*The God Protocols*”, Satoshi Nakamoto Institute, 1997.

DOI: <https://nakamotoinstitute.org/the-god-protocols/>

[25] MIT Technology Editors, “Explainer: What is a blockchain?”, MIT Technology Review Article, April 2018.

DOI: <https://www.technologyreview.com/2018/04/23/143477/explainer-what-is-a-blockchain/>

[26] Banerjee, A., Dr. Joshi, K. P., “Link Before You Share: Managing Privacy Policies through Blockchain”, 4th International Workshop on Privacy and Security of Big Data in conjunction with 2017 IEEE International Conference on Big Data, December 2017.

DOI: <https://arxiv.org/ftp/arxiv/papers/1710/1710.05363.pdf>

[27] Mahindrakar, A., Joshi, K. P., “Automating GDPR Compliance using Policy Integrated Blockchain”, 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), May 2020.

DOI: [10.1109/BigDataSecurity-HPSC-IDS49724.2020.00026](https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00026)

[28] Rieger, A., Guggenmos, F., Locki, J., Fridgen, G., Urbach, N., “*Building a Blockchain Application that Complies with the EU General Data Protection Regulation*”, MIS Quartely Executive, pp 263-279, December 2019.

DOI: [10.17705/2msqe.00020](https://doi.org/10.17705/2msqe.00020)

[29] Hassan, F., Ali, A., Rahouti, M., Latif, S., Kanhere, S., Singh, J., Al-Fuqaha, A., Janjua, U., Mian, A. N., Qadir, J., Crowcroft, J., “*Blockchain and the Future of the Internet: A Comprehensive Review*”, Cornell University, November 13th 2020 (2nd version).

DOI: <https://arxiv.org/pdf/1904.00733.pdf>

[30] Online Course on EDX platform, Linux Foundation X: LFS170x, Blockchain: “*Understanding Its Uses and Implications*”.

DOI: <https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS170x+1T2020/course/>

[31] Commission Nationale Informatique et Libertés (CNIL), “*Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*”, November 2018.

DOI: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>

[32] GoCryptowise, Penglund, “*Blockchain and GDPR are struggling to co-exist*”, June 2020.

DOI: <https://gocryptowise.com/blog/blockchain-and-gdpr-are-struggling-to-co-exist/>

[33] Menezes, N., “*How Troubled Can the Relation between Blockchain and GDPR Be?*”, *btcmanager.com*, December 2018.

DOI: <https://btcmanager.com/how-troubled-can-the-relation-between-blockchain-and-gdpr-be/>

[34] CryptoNinjas.net, “*2 Dutch blockchain firms present unique GDPR compliance tool for business and government*”, April 2019.

DOI: <https://www.cryptoninjas.net/2019/04/04/2-dutch-blockchain-firms-present-unique-gdpr-compliance-tool-for-business-and-government/>

[35] Stein, B., Kuznecov, K., Sangseop, L., Müller, “*A public blockchain solution permitting secure storage and deletion of private data*”, August 2018.

DOI: https://lition.io/docs/Lition_TechnicalWhitePaper.pdf

[36] LTO.network, “*Blockchain for Decentralized Workflows*”, Technical Report, September 2018.

DOI: <https://legalthings.github.io/livecontracts.io/documents/LTO%20Network%20-%20Technical%20Paper.pdf>

[37] Lyons, T., Ludovic, C., Timsit, K., “*Legal and regulatory framework of blockchains and smart contracts*”, The European Union Blockchain Observatory and Forum, Thematic Report, September 2019.

DOI: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

[38] Konashevych, O., Poblet, M., “*Blockchain Anchoring of Public Registries: Options and Challenges*”, Proceedings of the 12th International Conference on Theory and Practice of Electronic, Conference Paper, April 2019.

DOI: <https://dl.acm.org/doi/10.1145/3326365.3326406>

[39] International Telecommunication Union (ITU), “*Distributed ledger technology overview, concepts, ecosystem*”, Telecommunication Standardization Sector Of ITU, Technical Report, August 2019.

DOI: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf>

[40] European Parliamentary Research Service, “*Can distributed ledgers be squared with European data protection law?*”, Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA), PE 634.445 July 2019.

DOI: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

[41] Lubowicka, K., “*6 New Privacy Laws Around The Globe You Should Pay Attention To*”, Piwik Pro blog, Data Privacy and Security, March 2021.

DOI: <https://piwik.pro/blog/privacy-laws-around-globe/>