ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

BLOCKCHAIN, SMART (LEGAL) CONTRACTS & ΗΛΕΚΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ
(Πρόταση: BIG DATA ANALYTICS)

Διπλωματική Εργασία της
Νικολέττας Γεωργακοπούλου

Θεσσαλονίκη, Ιούνιος 2023

BLOCKCHAIN, SMART (LEGAL) CONTRACTS & ΗΛΕΚΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ
(Πρόταση: BIG DATA ANALYTICS)

Νικολέττα Γεωργακοπούλου

Πτυχίο Νομικής Σχολής, Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές:

Ψάννης Κωνσταντίνος
Μυλώση Μαρία

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την …ημ/νια……

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
Ψάννης Κωνσταντίνος	Μυλώση Μαρία	Βλαχοπούλου Μαρία

Νικολέττα Γεωργακοπούλου

Περίληψη

Η δημιουργία του Blockchain και η ταχύτατη ανάπτυξη του καθώς και η επέκταση του σε πληθώρα εφαρμογών εγείρει το ενδιαφέρον τόσο των ιδιωτών όσο και των επιχειρήσεων για την αξιοποίηση του ως ένα πολύτιμο εργαλείο. Παράλληλα, τα οφέλη της εν λόγω τεχνολογίας, ήτοι αποκέντρωση, ταχύτητα, ασφάλεια και χαμηλό κόστος συναλλαγών αποτελούν ισχυρά κίνητρα για την διερεύνηση των δυνατοτήτων που προσφέρονται. Πιο συγκεκριμένα, οι έξυπνες συμβάσεις και ιδίως τα έξυπνα νομικά συμβόλαια, ως μια εφαρμογή του Blockchain (πιο συγκεκριμένα Ethereum), έχουν προκαλέσει έντονο ενδιαφέρον τόσο στους συναλλασσόμενους όσο και στην επιστημονική κοινότητα. Με τις έξυπνες νομικές συμβάσεις διευκολύνεται και επιταχύνεται η σύναψη συμβάσεων και η δέσμευση των μερών, με αποτέλεσμα να ενισχύεται η οικονομία και η ανάπτυξη. Περαιτέρω δε, φυσικά και νομικά πρόσωπα από όλον τον κόσμο μπορούν να συνάψουν μία δεσμευτική σύμβαση χωρίς τις χρονοβόρες και δαπανηρές ενέργειες των Αρχών έκαστης χώρας. Ωστόσο, ανακύπτουν ποικίλα ερωτήματα αναφορικά με την επίλυση οιονεί διαφορών από έξυπνα νομικά συμβόλαια κατά την εφαρμογή αυτών σε συγκεκριμένους τομείς του δικαίου. Προβληματισμοί εγείρονται αναφορικά με τα προσωπικά δεδομένα, τον ΓΚΠΔ και τις έξυπνες νομικές συμβάσεις. Επιπρόσθετα, τα έξυπνα νομικά συμβόλαια εξετάζονται σε συνδυασμό με την ηλεκτρονική υπογραφή, μελετώντας τη δεσμευτικότητα που προκύπτει από την εφαρμογή της. Επιπλέον, γίνεται μνεία και στην τεχνολογία των Big Data Analytics καθώς και στον τρόπο εκμετάλλευσής τους προκειμένου να δημιουργηθεί μια πλούσια νομική βιβλιοθήκη προς αξιοποίηση από τις έξυπνες νομικές συμβάσεις.

Στην παρούσα εργασία, πραγματοποιείται μία ανάλυση των τεχνολογιών Blockchain, Smart (Legal) Contracts, Ηλεκτρονικής Υπογραφής καθώς και Big Data Analytics, με σκοπό την συνδυαστική και βέλτιστη εφαρμογή όλων αυτών. Στο πλαίσιο αυτό, καταβάλλεται μια προσπάθεια εξεύρεσης τόσο των πλεονεκτημάτων όσο και των μειονεκτημάτων των παραπάνω τεχνολογιών, προτείνοντας μελλοντικές ενέργειες για την άμβλυνση των τελευταίων, ει δυνατόν. Τα ζητήματα αυτά μελετώνται και αξιολογούνται σε θεωρητικό επίπεδο μέσω της ανασκόπησης βιβλιογραφίας (άρθρα και case studies) σε διεθνή κλίμακα.

Λέξεις-Κλειδιά:

Τεχνολογίες Blockchain, Τεχνολογίες Κατανεμημένου Καθολικού, Εφαρμογές, Smart Legal Contracts, Έξυπνες Συμβάσεις, Ηλεκτρονική Υπογραφή, Κρυπτογραφία, Προσωπικά Δεδομένα, ΓΚΠΔ, Big Data Analytics

Abstract

The rapid development of Blockchain technology and its expansion into a multitude of applications has raised the interest of both individuals and businesses to use it as a valuable tool. At the same time, the benefits of this technology, namely decentralization, speed, security and low transaction costs are strong incentives to explore the possibilities offered. More specifically, smart contracts and in particular smart legal contracts, as an application of Blockchain (Ethereum), have generated strong interest among both traders and the scientific community. Smart legal contracts facilitate and accelerate the contracting and engagement of parties, thus boosting the economy and growth. Furthermore, natural and legal persons from all over the world can enter into a binding contract without the time-consuming and costly actions of the authorities of each country. However, various questions arise regarding the resolution of quasi-disputes in smart legal contracts, when applied to specific areas of law. Concerns are raised regarding personal data, GDPR and smart legal contracts. In addition, smart legal contracts are examined in conjunction with electronic signatures, studying the binding nature of their application. As well, mention is made of Big Data Analytics technology and how to exploit it in order to create a rich legal library to be used by smart legal contracts.

In the present study, an analysis of the technologies Blockchain, Smart (Legal) Contracts, Electronic Signature as well as Big Data Analytics is carried out with a view to the combined and optimal implementation of all these. In this regard, an effort is made to find both the advantages and disadvantages of the above technologies, proposing future actions to mitigate the latter, if possible. These issues are studied and evaluated at a theoretical level through a review of literature (articles and case studies) on an international scale.

Keywords:

Blockchain technologies, Distributed Ledger Technology, Applications, Smart Legal Contracts, Smart Contracts, Electronic Signature, Cryptography, Personal Data, GDPR, Big Data Analytics.

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τη Διευθύντρια του Μεταπτυχιακού προγράμματος «Δίκαιο και Πληροφορική» αλλά και όλους τους καθηγητές μας για τις πολύτιμες γνώσεις που μας προσέφεραν καθ' όλη τη διάρκεια του προγράμματος.

Ιδιαιτέρως, θα ήθελα να ευχαριστήσω τους επιβλέποντες Καθηγητές μου, κυρίους Ψάννη Κωνσταντίνο και Μυλώση Μαρία, για την πολύτιμη καθοδήγηση και βοήθεια που μου παρείχαν κατά τη συγγραφή της εργασίας μου.

Τέλος, αφιερώνω αυτή την εργασία στην οικογένεια μου και στους φίλους μου για την αμέριστη στήριξη και εμψύχωση τους καθ΄όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

Περιεχόμενα

1. Εισαγωγή

Η χρήση τεχνολογιών Blockchain και ιδίως Smart Legal Contracts φαντάζει τουλάχιστον γοητευτική λόγω όλων αυτών που υπόσχεται καθώς και της νεωτερικότητας που φέρει. Ωστόσο, παρά το γεγονός ότι είναι πολλά υποσχόμενη, δεν είναι λίγοι οι προβληματισμοί που γεννώνται τόσο σε πρακτικό όσο και σε δογματικό επίπεδο. Ένα μείζον ζήτημα, είναι αυτό της δικαιοδοσίας, δεδομένου ότι ενδεχομένως έκαστο μέρος να υπόκειται σε διαφορετικούς νόμους αναλόγως το κράτος. Ένα ακόμη ζήτημα εξαιρετικής σημασίας και σπουδαιότητας ανακύπτει σχετικά με την προστασία των προσωπικών δεδομένων, την απόδοση των ρόλων-ευθυνών σε περίπτωση διαρροής των προσωπικών δεδομένων καθώς και την ασφάλεια τόσο εξ ορισμού όσο και κατά τον σχεδιασμό. Περαιτέρω, ένα αλγοριθμικό σύστημα είναι μεν αδιάβλητο – αν και υπάρχουν έντονες αμφιβολίες ως προς αυτό[1]- θέτει όμως και σοβαρούς περιορισμούς στην ελευθερία και αυτονομία των χρηστών.

Επιπρόσθετα, η Ηλεκτρονική Υπογραφή και ο Κανονισμός eIDAS αποτελούν καινοτομίες που διευκολύνουν την συναλλακτική ροή, καλλιεργούν την εμπιστοσύνη στις συναλλαγές εξ αποστάσεως και μειώνουν το κόστος των συναλλαγών στην Ενιαία Ευρωπαϊκή Αγορά. Ωστόσο, πρόβλημα γεννάται από τη μη αναγνώριση της ηλεκτρονικής αναγνώρισης από όλα τα κράτη μέλη της ΕΕ.

Τέλος, τα Big Data Analytics καθώς και η αξιοποίηση αυτών υπόσχονται σημαντική βελτίωση στην παραγωγή των έξυπνων νομικών συμβάσεων καθώς και στην ανάπτυξη των συμβατικών σχέσεων, δεδομένου ότι μέσω των Big Data θα μπορεί να αποτυπωθεί κάθε έκφανση της βούλησης των μερών. Βεβαίως, και σε αυτό το ζήτημα ανακύπτουν ερωτήματα και προβληματισμοί, οι οποίοι θα αναλυθούν στη σχετική ενότητα.

[1] Επηρεασμός των αλγορίθμων. Δεν αφορά την παρούσα εργασία. Πρόκειται για το φαινόμενο που ο αλγόριθμος εκπαιδεύεται σύμφωνα με τα δεδομένα που λαμβάνει. Κατά συνέπεια, ο αλγόριθμος γίνεται αντικειμενικός σε μεγαλύτερο ποσοστό εάν δέχεται δεδομένα από πολλές πηγές και πολλούς ανθρώπους.

2. Blockchain

Προτού γίνει μία ιστορική αναδρομή για την τεχνολογία Blockchain, σε αυτό το σημείο θα δοθεί ένας σύντομος και απλός ορισμός προκειμένου ο εκάστοτε αναγνώστης να έχει μια βασική ιδέα για αυτό που θα ακολουθήσει.

Blockchain είναι μια ηλεκτρονική βάση δεδομένων καταγραφής κάθε είδους συναλλαγών, της οποίας αντίγραφο έχουν όλοι οι χρήστες. Πρόκειται για μια αποκεντρωμένη βάση δεδομένων, της οποίας αντίγραφο έχουν όλα τα μέλη της κοινότητας. Ειδικότερα, είναι μια αλυσίδα (chain) από ψηφιακά blocks (block) που περιέχουν δεδομένα. Τα blocks αυτά με τα πολλά δεδομένα - συναλλαγές συνδέονται με ενα hash μεταξύ τους σε μία γονεϊκή σχέση, κάτι που υπόσχεται την αδιαβλητότητα (όπως θα εξηγηθεί παρακάτω)[2]. Ο ορισμός καθώς και τα είδη, τα εργαλεία και οι εφαρμογές της τεχνολογίας Blockchain θα αναλυθούν εκτενώς ακολούθως.

2.1.1. Ιστορία του Blockchain

Η ιδέα της τεχνολογίας του Blockchain αποδίδεται στον Satoshi Nakamoto. Στην πραγματικότητα όμως πρόκειται για μια ιδέα που χρονολογείται στο 1982 και εκφράστηκε από τον David Chaum[3], στη διατριβή του με τίτλο «Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups» . Ο Chaum - έχοντας θέσει τα θεμέλια με το έργο του- ίδρυσε μια εταιρεία με την ονομασία DigiCash το 1989. Το 1995, η εταιρεία εισήγαγε ένα κρυπτονόμισμα που ονομαζόταν eCash[4]. Ο D.Chaum υποσχόταν πώς η DigiCash θα προσέφερε πολλά από τα χαρακτηριστικά των σύγχρονων κρυπτονομισμάτων, όπως : ασφάλεια και ανωνυμία, καθώς ούτε η Κυβέρνηση δεν θα μπορούσε να αποκρυπτογραφήσει τις eCash συναλλαγές. Παρότι επρόκειτο για μια σπουδαία και καινοτόμα ιδέα, ο Chaum δεν μπόρεσε να πείσει τις Τράπεζες να υποστηρίξουν την ιδέα αυτή και ελλείψει της υποδομής του διαδικτύου των ομότιμων δικτύων (peer - to- peer networks), το σχέδιο ναυάγησε και η εταιρεία κήρυξε πτώχευση το 1998.

[2] Stéphane Blemus, “Law and Blockchain: a legal perspective on current regulatory trends worldwide”, 2017, SSRN

[3] https://en.wikipedia.org/wiki/David_Chaum

[4] https://www.investopedia.com/terms/e/ecash.asp

Στην συνέχεια, το 1991 οι Stuart Haber και W. Scott Stornetta[5] περιέγραψαν για πρώτη φορά μια κρυπτογραφική αλυσίδα από blocks. Σκοπός τους ήταν να εξασφαλίσουν πως τα ψηφιακά αρχεία θα φέρουν μια συγκεκριμένη ημερομηνία καθώς και ότι δεν θα μπορεί να τροποποιηθεί το περιεχόμενο τους.

Όμως, η πρώτη πρακτική εφαρμογή της τεχνολογίας Blockchain γίνεται με το Bitcoin- και το λεγόμενο genesis block ή άλλως block 0- το 2009 και οφείλεται στον Satoshi Nakamoto[6]. Η τεχνολογία που πρότεινε ο Nakamoto είναι ίδια με αυτή που είχε προταθεί από τον Chaum, με την μόνη ουσιαστική διαφορά αυτή του μηχανισμού συναίνεσης proof-of-work του Bitcoin για την επικύρωση των blocks δεδομένων και την εξόρυξη νομισμάτων. Ο Satoshi Nakamoto είναι αγνώστου ταυτότητας και κανείς μέχρι και σήμερα δεν έχει καταφέρει να τον "αποκρυπτογραφήσει" παρά τις συνεχείς προσπάθειες. Το 2008 κυκλοφόρησε την Λευκή Βίβλο (The Bitcoin White Paper) [7] , μια μελέτη για το Bitcoin, ενώ στις 3 Ιανουαρίου 2009 δημιούργησε και το πρώτο Block των 50 Bitcoin. Ο Nakomoto έμεινε ενεργός στην ανάπτυξη του κρυπτονομίσματος έως τον Δεκέμβριο του 2010 [8].

Επιλογικά, η ιδέα του Bitcoin θα είχε την ίδια δυσάρεστη μοίρα με την DigiCash. Χρειάστηκαν περισσότερα από δύο χρόνια για να φτάσει το Bitcoin στη συμβολική αξία του ενός δολαρίου ΗΠΑ. Ήταν μόλις το 2017 που η αξία του Bitcoin έφτασε τα 1.000 δολάρια. Έκτοτε, η αξία του νομίσματος έχει διατηρήσει τη χαρακτηριστική του αστάθεια, αλλά παράλληλα έχει έντονα ανοδική τάση.

2.1.2. Τεχνολογία DLT (Distributed Ledger Technology - Τεχνολογία Κατανεμημένου Καθολικού)- Η βάση του Blockchain

Η τεχνολογία DLT χρησιμοποιείται για την επικύρωση της κυριότητας είτε χρήματος είτε περιουσιακών αγαθών. Χαρακτηριστικό παράδειγμα για την επεξήγηση αυτής της τεχνολογίας αποτελεί ο τρόπος που διενεργούνται οι τραπεζικές συναλλαγές. Για την διενέργεια μιας απλής μεταφοράς χρημάτων από ένα τραπεζικό λογαριασμό σε έναν άλλο, χρησιμοποιούνται κεντρικές

[5] Haber S., Stornetta W.S., "How to time-stamp a digital document" , 1991, SpringerLink

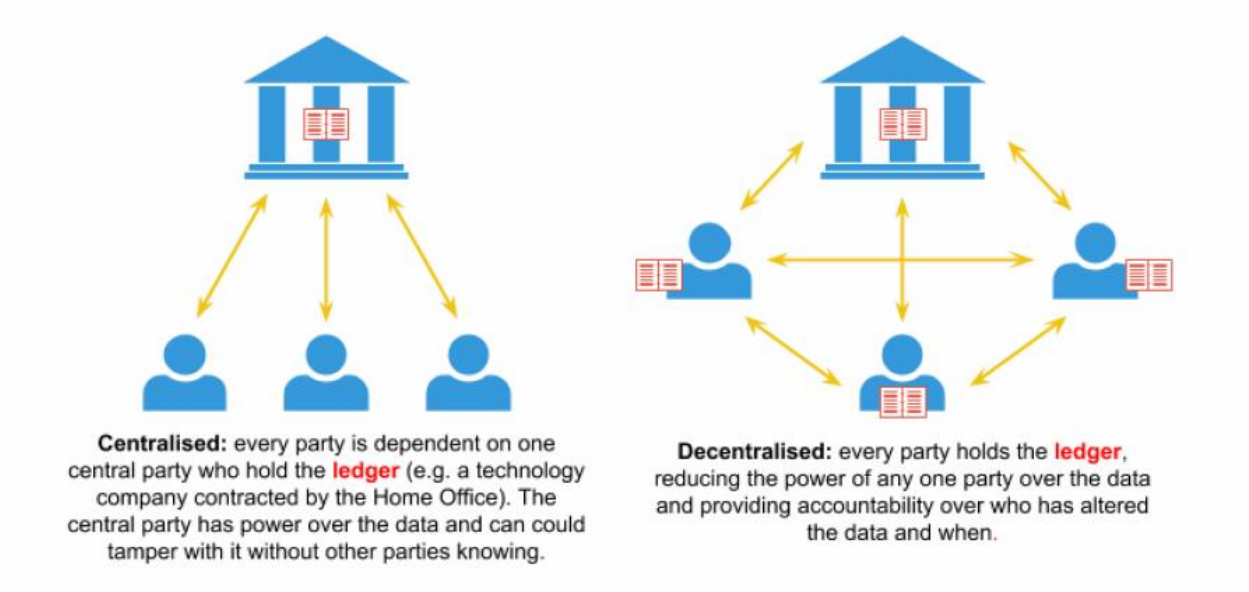
[6] Szczerbowski, Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017, SSRN

[7] Nakamoto S, " Bitcoin: A Peer - to - Peer Electronic Cash System"

[8] Wallace, Benjamin , «The Rise and Fall of Bitcoin». , 2011, Wired **19**

βάσεις δεδομένων, οι οποίες διαχειρίζονται από κεντρικές τράπεζες και ορισμένα τμήματα αυτών. Πιο συγκεκριμένα, η τράπεζα καταγράφει τις συναλλαγές σε τοπικές βάσεις δεδομένων, οι οποίες επικαιροποιούνται μετά την ολοκλήρωση έκαστης συναλλαγής και ενημερώνεται το κεντρικό σύστημα.

Αντίθετα, το DLT[9] είναι μία βάση δεδομένων για συναλλαγές, η διεκπεραίωση και ολοκλήρωση των οποίων διαμοιράζεται σε όλο το δίκτυο και δεν αποθηκεύεται σε μία κεντρική τοποθεσία.



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

2.2. Ορισμός και Χαρακτηριστικά του Blockchain

Όπως προαναφέρθηκε, το Blockchain είναι μια τεχνολογία διασύνδεσης βάσεων δεδομένων και η διασύνδεση αυτή είναι γνωστή ως DLT - Distributed Ledger Technology (Τεχνολογία Κατανεμημένου Καθολικού) [10]. Ειδικότερα, τα αρχεία μιας κοινής βάσης δεδομένων αποθηκεύονται σε έναν κεντρικό διακομιστή στον οποίο έχουν πρόσβαση όλοι οι χρήστες, ενώ

[9] Bashir I., "Mastering Blockchain: Distributed Ledger Technology, decentralization, and smart contracts explained", 2018

[10] G. Callsen, "FinTech, DLT and regulation", 2017, International Capital Market Association (ICMA).

αντίθετα τα αρχεία ενός blockchain αποθηκεύονται στους υπολογιστές των χρηστών σε όλο τον κόσμο. Αυτό καθιστά το Blockchain μια κατανεμημένη βάση δεδομένων με αρχιτεκτονική peer-to-peer (ομότιμη)[11]. Οι όροι "κατανεμημένη" και "ομότιμη" σημαίνουν αντιστοίχως ότι τα δεδομένα αποθηκεύονται σε πολλές τοποθεσίες και ότι δεν υπάρχει κεντρική υποδομή που να έχει ένα πρωτότυπο αρχείο των δεδομένων και παράλληλα δεν μπορεί να ελεγχθεί ενιαία από καμία Αρχή. Πρόκειται λοιπόν για ένα αρχείο συναλλαγών που διαφέρει πολύ από το παραδοσιακό έγχαρτο και υπόσχεται ασφάλεια των συναλλαγών, λόγω των χαρακτηριστικών του που θα αναλυθούν παρακάτω.

Η τεχνολογία Blockchain κατ΄ουσίαν είναι ένα αποκεντρωμένο ψηφιακό μητρώο συναλλαγών (κάθε είδους: οικονομικών, λογιστικών, νομικών, εμπορικών, έξυπνων συμβολαίων κλπ), στην οποία δεν παρεμβάλλονται ενδιάμεσοι τρίτοι, μειώνοντας έτσι το κόστος των συναλλαγών. Επομένως, παρατηρείται ότι δημιουργείται μια αδιάκοπη αλυσίδα καταχωρήσεων, οι οποίες τεκμηριώνονται από μια συνάρτηση κατακερματισμού (Hash Function)[12] και μια χρονοσφραγίδα (Timestamp)[13] και σε αυτά αποτυπώνονται τα δεδομένα της συναλλαγής. Κάθε επόμενο block εμπεριέχει στην ταυτότητα του και στοιχεία από το προηγούμενο.

---

[11] Wikpedia: Ένα δίκτυο υπολογιστών **peer-to-peer** (ή **P2P,** *ελληνικά:* ομότιμο δίκτυο) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

[12] **Συνάρτηση κατακερματισμού** είναι οποιαδήποτε συνάρτηση που μπορεί να χρησιμοποιηθεί για τη χαρτογράφηση δεδομένων αυθαίρετου μεγέθους σε τιμές σταθερού μεγέθους, αν και υπάρχουν ορισμένες συναρτήσεις κατακερματισμού που υποστηρίζουν έξοδο μεταβλητού μήκους. Οι τιμές που επιστρέφονται από μια συνάρτηση κατακερματισμού ονομάζονται *τιμές κατακερματισμού* , *κωδικοί κατακερματισμού* , *αναλύσεις* ή απλώς *κατακερματισμοί* .

[13] Η **χρονική σήμανση** είναι μια ακολουθία χαρακτήρων ή κωδικοποιημένων πληροφοριών που προσδιορίζουν πότε συνέβη ένα συγκεκριμένο συμβάν, συνήθως δίνοντας ημερομηνία και ώρα της ημέρας, μερικές φορές με ακρίβεια σε ένα μικρό κλάσμα του δευτερολέπτου.

Το Blockchain αποδίδεται στα ελληνικά με τους όρους αλυσίδα μπλοκ [14],συστοιχία κόμβων [15] , αλυσίδα συστοιχιών[16], αλυσίδα κατανεμημένης εγγραφής [17]. Ως τεχνολογία DLT (Distributed Ledger Technology - Τεχνολογία κατανεμημένου καθολικού) έχει το πλεονέκτημα ότι είναι δημόσια και είναι σχεδόν αδύνατο να τροποποιηθεί ως προς το ιστορικό της [18] και τις καταγραφές της[19]. Πιο συγκεκριμένα με το DLT μπορεί να δημιουργηθεί μια βάση κατανεμημένη, αποκεντρωμένη, διαμοιρασμένη που είναι προσβάσιμη από ένα δίκτυο υπολογιστών, το οποίο αλληλοεπιδρά και συνδέεται σε μια ομότιμη βάση, έτσι ώστε οι συμμετέχοντες στο δίκτυο να μπορούν να μοιράζονται και να διατηρούν πανομοιότυπες, κρυπτογραφικά ασφαλείς και αμετάβλητες εγγραφές με αποκεντρωμένο τρόπο. Η ιδέα για αυτή την τεχνολογία συνίστατο στη δημιουργία ενός αποκεντρωμένου συστήματος, δηλαδή ενός δικτύου χωρίς την ύπαρξη κάποιας κεντρικής αρχής (peer to peer network- P2P), χωρίς την διαμεσολάβηση κάποιου τρίτου για την ολοκλήρωση της συναλλαγής.

Ένα από τα βασικά χαρακτηριστικά του είναι ότι το κατανεμημένο λογιστικό βιβλίο συντηρείται από τους συμμετέχοντες και όχι από έναν κεντρικό διαχειριστή βάσης δεδομένων ή ένα μέροςΓια το λόγο αυτό χαρακτηρίζεται ως αποκεντρωμένο σύστημα. Επιπλέον, κάθε συμμετέχων του δικτύου μπορεί να έχει ένα πανομοιότυπο αντίγραφο του κατανεμημένου λογιστικού βιβλίου. Με τη συνδυαστική χρήση ενός μηχανισμού συναίνεσης καθώς και της κρυπτογράφησης, οποιαδήποτε προσθήκη στη βάση δεδομένων, όπως πχ μια νέα συναλλαγή, ομαδοποιούνται και επικυρώνονται από ένα δίκτυο συμμετεχόντων, που ονομάζονται κόμβοι (nodes).

[14]«ΦΕΚ. Τεύχος Β’ 1756/22.05.2017». Εφημερίδα της Κυβερνήσεως: 17803, 17805, 17807 κ.ε.. 22 Μαΐου 2017.

[15] «Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές;», Ευρωπαϊκή Κεντρική Τράπεζα, 19 Απριλίου 2017

[16] Σταμπέρνας, Σωτήριος, «Τεχνολογίες αλυσίδας συστοιχιών και έξυπνα συμβόλαια στο πλαίσιο του Διαδικτύου των Πραγμάτων», 2018, Πανεπιστήμιο Πειραιώς (μεταπτυχιακή διατριβή)

[17] Παπαδημόπουλος Ιωάννης, « Η δογματική ένταξη των smart contracts στο δίκαιο των συμβάσεων», ΧρΙΔ 2020.471.

[18] «Blockchain Enhances Privacy, Security and Conveyance of Data», 2016, CIENTIFIC AMERICAN.

[19] Ομοίως.

Πιο αναλυτικά, το Blockchain έχει τα εξής χαρακτηριστικά[20] [21] [22], με τα οποία ανακτάται η χαμένη εμπιστοσύνη στις συναλλαγές:

1. Αποκεντρωμένο: όπως προαναφέρθηκε, δεν υπάρχει κάποια κεντρική Αρχή ή ενδιάμεσος τρίτος για την επικύρωση ή ολοκλήρωση των συναλλαγών. Αυτό πλέον γίνεται με κρυπτογραφικούς αλγορίθμους και τη συμμετοχή ολόκληρου του δικτύου.
2. Ασφαλές: Αυτό επιτυγχάνεται με τη χρήση ασύμμετρης κρυπτογραφίας (δημόσιο - ιδιωτικό κλειδί)[23] και την χρήση ψηφιακών υπογραφών.
3. Αυτοματοποιημένο: Όταν πληρωθούν οι όροι και οι προϋποθέσεις που το δομούν, το έξυπνο συμβόλαιο αυτοεκτελείται.
4. Σταθερό: Έκαστο block - που περιέχει ποικίλες συναλλαγές- βρίσκεται σε άμεση σύνδεση με το προηγούμενο.
5. Έμπιστο: Τα μέρη συναλλάσσονται χωρίς την παρέμβαση κάποιου αξιόπιστου τρίτου αλλά βασιζόμενα στο ίδιο το δίκτυο και την υποστήριξη των άλλων κόμβων.
6. Ακέραιο: Υπάρχει η δυνατότητα χρήσης ψευδωνύμων, υποστηρίζοντας κατά αυτόν τον τρόπο το δικαίωμα στην ανωνυμία.
7. Διαφάνεια: Κάθε κόμβος έχει αντίγραφο όλων των συναλλαγών και ανά πάσα στιγμή γίνεται μέρος αυτών.
8. Χαμηλό κόστος: Η απουσία ενδιάμεσων τρίτων συνεπάγεται και μείωση συναλλακτικού κόστους
9. Δυνατότητα Ιχνηλάτησης: Δεδομένης της δημόσιας καταγραφής του ιστορικού των συναλλαγών καθώς και του αντιγράφου που έχει κάθε κόμβος, καθίσταται δυνατό να εντοπιστεί η προέλευση κάθε συναλλαγής.

[20] Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, Anoud Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends", 2021, SpringerLink

[21] https://data-flair.training/blogs/features-of-blockchain/

[22] Rashideh W., "Blockchain technology framework: Current and future perspectives for the turism industry", 2020

[23] Ασύμμετρη Κρυπτογράφηση ή Κρυπτογράφηση Δημοσίου Κλειδιού περιλαμβάνει τους κρυπτογραφικούς αλγόριθμους στους οποίους χρησιμοποιείται ένα κλειδί για κρυπτογράφηση και ένα διαφορετικό κλειδί για την αποκρυπτογράφηση των δεδομένων. Αναλύεται εκτενώς παρακάτω, στο κυρίως κείμενο της εργασίας.

2.2.1. Επίπεδα του Blockchain

Οι απόψεις διίστανται αναφορικά με τα επίπεδα σχεδίασης του Blockchain, ωστόσο το επικρατέστερο μοντέλο είναι το ακόλουθο[24]:

1. Application Layer : Γίνεται η κωδικοποίηση των επιθυμητών λειτουργιών για την δημιουργία εφαρμογών για τον τελικό χρήστη.
2. Execution Layer : Εδώ, εκτελούνται οι εντολές - όπως δίδονται από το application layer- σε όλους τους κόμβους του δικτύου. Οι εντολές μπορεί να είναι είτε απλές (πχ μεταφορά χρημάτων) είτε σύνθετες (πχ εκτέλεση smart contracts). Ανεξαρτήτως του είδους των συναλλαγών , όλοι οι κόμβοι πρέπει να εκτελέσουν το πρόγραμμα προκειμένου να εκτελεστεί σωστά η εντολή. Οι απλές εντολές που τρέχουν συνήθως στο Bitcoin δεν είναι Turing Complete (Non Turing Complete). Αντίθετα, πιο σύνθετες εντολές εκτελούνται σε Turing Complete[25] blockchain όπως το Ethereum και το Hyperledger.
3. Semantic Layer : Η εκτέλεση των εντολών του execution layer, επικυρώνεται σε αυτό εδώ το επίπεδο. Σε αυτό το επίπεδο λοιπόν ελέγχεται εάν κάποιος έχει κάνει μια νόμιμη συναλλαγή ή εάν γίνεται απόπειρα double-spending (διπλή-δαπάνη). Επιπρόσθετα, σε αυτό το επίπεδο, καθορίζεται η σειρά των blocks και ο τρόπος σύνδεσης τους, δηλαδή η αποτύπωση του hash του προηγούμενου block μέχρι το αρχικό block (block 0).
4. Propagation Layer : Η peer-to-peer επικοινωνία μεταξύ των κόμβων λαμβάνει χώρα σε αυτό το επίπεδο. Με αυτό τον τρόπο συνομιλούν και συγχρονίζονται βάσει της τρέχουσας κατάστασης του δικτύου. Επομένως, όταν ένας κόμβος προτείνει ένα έγκυρο block, αυτό αναμεταδίδεται στο δίκτυο με σκοπό οι υπόλοιποι κόμβοι να επιβεβαιώσουν και να συνεχίσουν την αλυσίδα. Κατά αυτόν τον τρόπο,

[24] Niranjanamurthy M., Nithya B., Jagannatha S., "Analysis of Blockchain Technology: pros, cons and SWOT". 2019, Springer

[25] Wikipedia: Στη θεωρία υπολογισιμότητας , ένα σύστημα κανόνων χειρισμού δεδομένων (όπως το σύνολο εντολών ενός υπολογιστή , μια γλώσσα προγραμματισμού) λέγεται ότι είναι πλήρες ή υπολογιστικά καθολικό εάν μπορεί να χρησιμοποιηθεί για την προσομοίωση οποιασδήποτε μηχανής Turing (επινοήθηκε από τον Άγγλο μαθηματικό και επιστήμονα υπολογιστών Άλαν Τούρινγκ). Αυτό σημαίνει ότι αυτό το σύστημα είναι σε θέση να αναγνωρίσει ή να αποφασίσει άλλα σύνολα κανόνων χειρισμού δεδομένων. Η πληρότητα Turing χρησιμοποιείται ως τρόπος έκφρασης της ισχύος ενός τέτοιου συνόλου κανόνων χειρισμού δεδομένων, που δεν αρκείται στην απλή εκτέλεση συγκεκριμένων πράξεων/εντολών.

εξασφαλίζεται και η σταθερότητα του δικτύου (ένα από τα βασικά χαρακτηριστικά του blockchain όπως αναφέρθηκε και ως άνω).

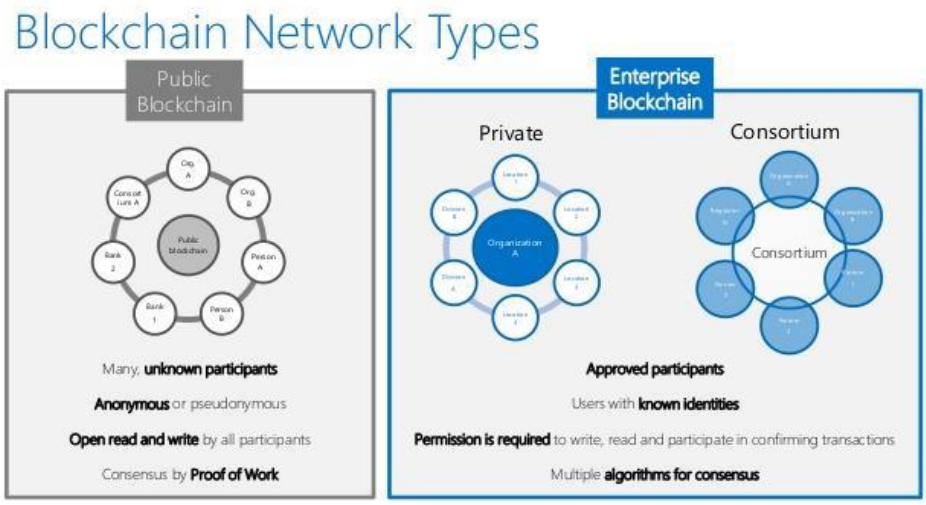
5. Consensus Layer: Οι μηχανισμοί συναίνεσης που τρέχουν σε αυτό το επίπεδο αποτελούν τη βάση των συστημάτων blockchain. Απώτερος στόχος είναι η επίτευξη συναίνεσης - πλήρους συμφωνίας μεταξύ των κόμβων ολόκληρου του δικτύου, ώστε να εξασφαλιστεί η σταθερότητα του καθολικού. Επιπλέον, η ασφάλεια των συναλλαγών επιτυγχάνεται σε αυτό το επίπεδο. Στο Bitcoin και στο Ethereum (που θα μας απασχολήσει παρακάτω), η συναίνεση επιτυγχάνεται μέσω των αλγορίθμων Proof of Work και Proof of Stake αντιστοίχως. (αναλύεται πιο κάτω).

2.2.2. Είδη Blockchain

1. Δημόσιο δίκτυο blockchain (public blockchain): είναι κατανεμημένα λογιστικά βιβλία όπου ο καθένας μπορεί να συμμετέχει μέσω της διαδικασίας συναίνεσης (Proof of Work)και να αλληλεπιδρά χωρίς περιορισμούς πρόσβασης [26]. Επομένως, η πλατφόρμα επιτρέπει σε κάθε χρήστη να συμμετάσχει, έχοντας το δικαίωμα της δημιουργίας νέου block στην αλυσίδα, καθώς και το δικαίωμα πρόσβαση στις ήδη πραγματοποιημένες συναλλαγές.
2. Ιδιωτικό δίκτυο blockchain (private blockchain): Πρόκειται για ένα εν μέρει αποκεντρωμένο δίκτυο, στο οποίο συμμετέχουν μόνο εξουσιοδοτημένοι χρήστες, απολώντας το δικαίωμα στην ανωνυμία. Οι συμμετέχοντες είναι μέρος ενός ενιαίου οργανισμού και το οποίο θα μπορούσε να εφαρμοστεί για σκοπούς ελέγχου και εσωτερικής διαχείρισης. Τα δίκτυα αυτά χρησιμοποιούνται κυρίως από ομίλους επιχειρήσεων, προκειμένου να διακινούν και να διατηρούν σημαντικές πληροφορίες.
3. Ημι-ιδιωτικό δικτυο blockchain (consortium blockchain): Αποτελείται από μία ελεγχόμενη ομάδα χρηστών, οι οποίοι έχουν πλήρη πρόσβαση στα δεδομένα. Το ημι-ιδιωτικό διαφέρει από το αμιγώς ιδιωτικό στο ότι υφίσταται ένα δημόσιο

[26] Buterin V. , "On Public and Private Blockchains", Ethereum Blog, 7 August 2015; Guegan D. , "Public Blockchain versus Private Blockchain", Docu-ments de travail du Centre d'Economie de la Sorbonne, 2017.

κομμάτι διαθέσιμο σε όλους με κάποιους περιορισμούς, οι οποίοι τίθενται από την ελεγχόμενη ομάδα χρηστών. Πρόκειται λοιπόν για ένα υβριδικό μοντέλο κατά το οποίο επιτρέπεται η ελεγχόμενη πρόσβαση και σε άλλους χρήστες. Επομένως. είναι κατανεμημένα ledgers όπου η "διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων." [27] [28] Το σύστημα αυτό συνήθως επιλέγεται από Τραπεζικά Ιδρύματα.



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

2.3. Πώς λειτουργεί το Blockchain (consesus + mining);

Τα blocks δημιουργούνται από μια σειρά από κατανεμημένες εγγραφές, που απεικονίζουν συναλλαγές και περιλαμβάνουν δεδομένα. Έκαστη συναλλαγή φέρει ένα συγκεκριμένο κωδικό χρήστη ή ένα ψευδώνυμο. Τα blocks συνδέονται μεταξύ τους με κρυπτογραφικούς

[27] Ομοίως

[28] Blemus Stéphane, “Law and Blockchain: a legal perspective on current regulatory trends worldwide”, 2017

κατακερματισμούς (cryptographic hashes) και κάθε block περιέχει τον κρυπτογραφικό κατακερματισμό του προηγούμενου (hash)[29] [30].

Πιο αναλυτικά, σε πρώτο επίπεδο ζητάει κάποιος να γίνει μια συναλλαγή (μεταφορά χρημάτων, έξυπνο συμβόλαιο, αγορά αγαθού). Στη συνέχεια δημιουργείται ένα προσωρινό block που αντιπροσωπεύει αυτή τη συναλλαγή. Το block αυτό στέλνεται σε οποιοδήποτε κόμβο (node) προκειμένου να τύχει επιβεβαίωσης από τα υπόλοιπα μέλη. Οι κόμβοι μιας αλυσίδας blocks είναι οι ενδιαφερόμενοι φορείς του δικτύου και οι συσκευές τους είναι εξουσιοδοτημένες να παρακολουθούν το κατανεμημένο βιβλίο (Ledger [31]) και να χρησιμεύουν ως κόμβοι επικοινωνίας για διάφορες εργασίες του δικτύου. Η πρωταρχική εργασία ενός κόμβου Blockchain είναι να επιβεβαιώνει τη νομιμότητα κάθε επόμενης παρτίδας συναλλαγών του δικτύου, γνωστής ως block.

Η ομάδα ή ο ανθρωπος που θα αναλάβει να ελέγξει τη συναλλαγή πραγματοποιώντας και λύνοντας κάποιες αλγοριθμικές εξισώσεις ονομάζεται miner [32]. Όταν ο miner λύσει τον αλγοριθμικό γρίφο - εξίσωση, η συναλλαγή θεωρείται έγκυρη και το block προστίθεται στην αλυσίδα. Για την επίλυση της εξίσωσης αυτής, δίδεται μια αμοιβή προκειμένου ο miner να έχει κίνητρο να επιλύσει την εξίσωση αλλά και να καλύψει τους πόρους και την ενέργεια που κατανάλωσε. [33]

[29] Πιο συγκεκριμένα κάθε μπλοκ κατά τη δημιουργία του αποκτά μια ταυτότητα- ήτοι μια συμβολοσειρά από γράμματα και νούμερα- μέρος της οποίας παίρνει και το επόμενο μπλοκ, προκειμένου να συνδεθούν αυτά τα δύο μπλοκ. Θα μπορούσε να το παραλληλίσει κανείς με τον τυπικό τρόπο που ένα παιδί αποκτά επίθετο από έναν από τους δύο γονείς.

[30] Yaga D., Mell P., Roby N., Scarfone K., "Blockchain Technology Overview", 2019, Computer Science

[31] Ledger: Το λογιστικό βιβλίο είναι ένα ψηφιακό ή φυσικό αρχείο καταγραφής που καταγράφει τις συναλλαγές που σχετίζονται με ένα χρηματοπιστωτικό σύστημα. Τα δίκτυα blockchain είναι ένας τύπος αποκεντρωμένου συστήματος λογιστικών βιβλίων που έχει σχεδιαστεί για την ασφαλή αποθήκευση δεδομένων. Αναλύεται παρακάτω στο κυρίως κείμενο της εργασίας.

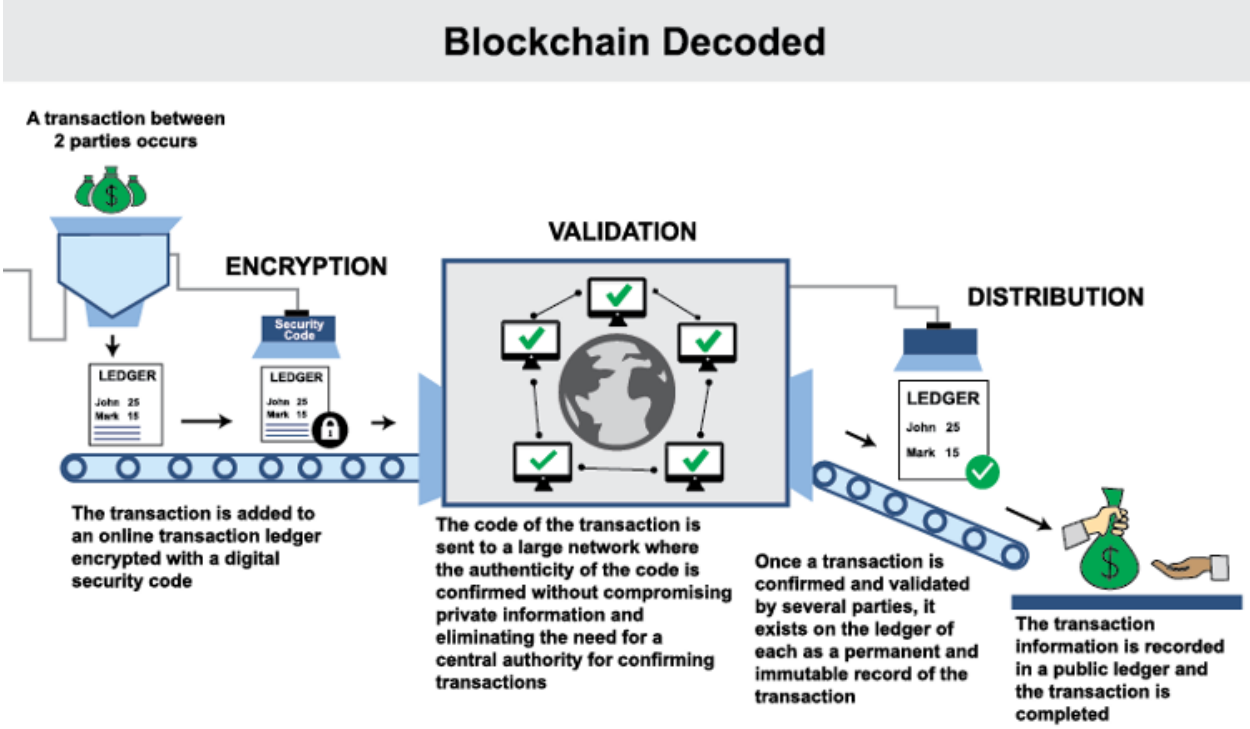
[32] Singhal, B., Dhameja, G., Panda, P.S., "How Blockchain Works. In: Beginning Blockchain. ", 2018,Apress, Berkeley

[33] Σε αυτό το σημείο, αξίζει να σημειωθεί πώς στο δίκτυο Blockchain απαιτείται ενέργεια ίση με όση χρειάζεται μια ολόκληρη πόλη για την κάλυψη όλων των αναγκών της.

Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

Ειδικότερα, ως προς τη συναλλαγή ακολουθείται μια διαδικασία κρυπτογράφησης που εγγυάται την ασφάλεια και το αμετάβλητο των συναλλαγών. Πιο συγκεκριμένα, η συναλλαγή αυτή κωδικοποιείται και κρυπτογραφείται με ένα κλειδί "ασφαλείας". Με αυτόν τον τρόπο, το κείμενο μετατρέπεται σε μια σειρά από νούμερα, σύμβολα και γράμματα δημιουργώντας μια ακατάληπτη φράση. Ο κώδικας της συναλλαγής αποστέλλεται σε ένα δίκτυο κόμβων προκειμένου να επιβεβαιωθεί η εγκυρότητα της χωρίς να γίνεται γνωστό το περιεχόμενο αυτής, λόγω της προγενέστερης/προηγούμενης κρυπτογράφησης. Επομένως, πιστοποιείται η εγκυρότητα της συναλλαγής χωρίς να αποκαλυφθεί σε τρίτο μέρος το περιεχόμενο της εν λόγω συναλλαγής. Στη συνέχεια, η πιστοποιημένη και έγκυρη συναλλαγή πλέον καταγράφεται σε ένα μόνιμο αρχείο, κατανεμημένο βιβλίο, γνωστό ως Ledger. Ως ledger καλείται το δημόσιο λογιστικό βιβλίο, στο οποίο καταγράφονται όλες οι συνετελεσμένες συναλλαγές, με αποτέλεσμα το σύνολο των blocks να δημιουργεί το καθολικό. Εν συνεχεία, το καθολικό αποθηκεύεται σε ένα κατανεμημένο σύστημα (Distributed System). Η αξία αυτού έγκειται στο ότι πλέον δεν εμπλέκεται τρίτο μέρος -μια κεντρική Αρχή-ως αξιόπιστος ενδιάμεσος για την ολοκλήρωση της συναλλαγής, αλλά ένα ολόκληρο δίκτυο κόμβων, μηχανισμοί συναίνεσης και κρυπτογραφικοί αλγόριθμοι[34].

[34] Primavera De Filippi, Aaron Wright, " Blockchain and the Law- The Rule of Code", Harvard University Press, 2018, σελ 13-19 και 22-31



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

2.3.1. Consensus (Proof of Work & Proof of Stake)

Ο miner καλείται να λύσει ένα κρυπτογραφικό αλγόριθμο προκειμένου να επικυρωθεί η συναλλαγή, να δημιουργηθεί το block και να ενταχθεί στην αλυσίδα. Οι υπολογισμοί που καλείται να κάνει ο miner για την επίλυση του κρυπτογραφικού γρίφου εξαρτώνται από το πρωτόκολλο συναίνεσης. Η αξία των μηχανισμών consensus αναδεικνύεται με την παρεμπόδιση και αντιμετώπιση των κακόβουλων κόμβων, που θα προσπαθήσουν να επικυρώσουν μη έγκυρες συναλλαγές. Οι μηχανισμοί συναίνεσης αποτελούν μια δικλείδα ασφαλείας ως προς την επιβεβαίωση ως έγκυρης εκάστοτε συναλλαγής, αφού μέσω αυτών οι κόμβοι ελέγχουν και επιβεβαιώνουν ένα block που έχει προταθεί ως έγκυρο από άλλο κόμβο, δεδομένου ότι έχουν ήδη ένα αντίγραφο του καθολικού. Όταν υπάρξει η συναίνεση, το block προστίθεται στην αλυσίδα.

Κατά αυτόν τον τρόπο το σύστημα παραμένει αδιάβλητο, ιδίως από αυτού του είδους τις επιθέσεις. Οι δύο επικρατέστεροι μηχανισμοί συναίνεσης είναι το Proof of Work και Proof of Stake και επιλέγονται ανάλογα με τις ανάγκες του συστήματος.

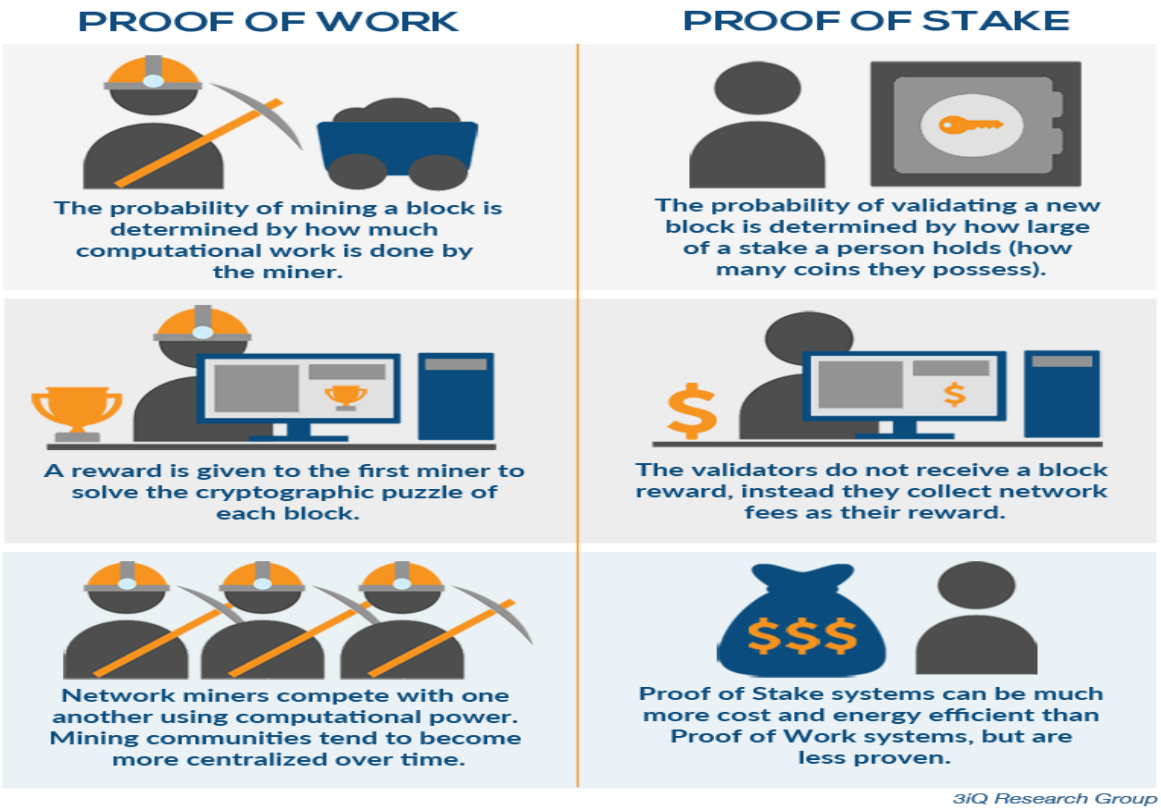
2.3.1.α. Proof of Work (PoW) - Απόδειξη Εργασίας

Το PoW ως αλγόριθμος λειτουργεί βάσει συγκεκριμένης ποσότητας υπολογιστικής εργασίας, το mining (εξόρυξη), προτού ένας κόμβος προτείνει ένα blocks συναλλαγών σε ολόκληρο το δίκτυο. Το PoW είναι ένα κομμάτι δεδομένων που παράγεται δύσκολα, εξαιτίας της μεγάλης υπολογιστικής ισχύος και του χρόνου που απαιτούνται, παρ΄ όλα αυτά μπορεί να επιβεβαιωθεί σχετικά εύκολα. Περαιτέρω, αυτό που καθιστά αξιόπιστο και ασφαλή τον αλγόριθμο PoW είναι ότι κάθε φορά προσαρμόζεται στο επίπεδο της δυσκολίας της εκάστοτε εργασίας, ώστε ο ρυθμός παραγωγής των blocks να ελέγχεται και να παραμένει σταθερός (δημιουργία νέου block περίπου ανά 10 λεπτά). Επιπροσθέτως, εάν πολλοί κόμβοι προσπαθούν να επιλύσουν έναν κρυπτογραφικό αλγόριθμο , καθίσταται δυσχερές να εντοπιστεί ποιος το επέλυσε πρώτος. Αξίζει να σημειωθεί, πως στα δημόσια blockchain είναι δύσκολο να εντοπιστεί η ταυτότητα ενός κόμβου - δεδομένης της πλήρους ανωνυμίας- όπως επίσης και των πολλαπλών ταυτοτήτων που μπορεί να διατηρεί ένας κόμβος. Σε αυτό το σημείο επισημαίνεται πως πρέπει να επιβραβεύονται οι κόμβοι που παρά την υπολογιστική τους δύναμη, δρουν τίμια αποφεύγοντας δόλιες ενέργειες, παρακωλύοντας το σύστημα.

2.3.1.β. Proof of Stake (PoS)

Ο εν λόγω αλγόριθμος συναίνεσης βασίζεται στην επικύρωση blocks συναλλαγών και όχι στο mining (εξόρυξη). Αυτός ο μηχανισμός συναίνεσης εξασφαλίζει τέλη συναλλαγών για τους validators (επικυρωτές) και όχι επιβράβευση στους miners για την παραγωγή νέων νομισμάτων. Στο παρόν σύστημα, οι validators δεσμεύουν εκ των προτέρων το μερίδιο τους προκειμένου να μπορέσουν να συμμετάσχουν στην επικύρωση συναλλαγών. Όσο μεγαλύτερο είναι το μερίδιο που θα δοθεί στον επικυρωτή, τόσο μεγαλύτερη η πιθανότητα να επικυρώσει ένα νέο block συναλλαγών. Το PoS χρησιμοποιείται ως μηχανισμός συναίνεσης στο Ethereum, και το

προδεσμεύμενο μερίδιο ρυθμίζεται με το Gas[35]. Τα πλεονεκτήματα των PoS έναντι των PoW είναι η εγγύηση μεγαλύτερης ασφάλειας έναντι των επιθέσεων καθώς και οι λιγότερες απαιτήσεις ηλεκτρικής ενέργειας. Αυτό οφείλεται στο Gas, το οποίο δίδεται σε συγκεκριμένη ποσότητα για την διενέργεια συγκεκριμένων πράξεων, με αποτέλεσμα να μην γίνεται σπατάλη ενέργειας ή προσπάθεια από κακόβουλους χρήστες να δημιουργήσουν κενά για να τα εκμεταλλευτούν και να μην ολοκληρωθεί η συναλλαγή. Σε κάθε περίπτωση το Gas και η λειτουργία του επεξηγείται παρακάτω, στην Ενότητα Ethereum.



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

[35] Στην αλυσίδα μπλοκ Ethereum, απαιτούνται ethers (ETH) για να πληρωθούν τα τέλη αερίου. Το Gas είναι η μονάδα μέτρησης για το πόση υπολογιστική εργασία απαιτείται για τη διεκπεραίωση συναλλαγών και έξυπνων συμβάσεων στο Ethereum.

2.4. Κρυπτογράφηση και Κατακερματισμός

Η τεχνολογία Blockchain είναι άμεσα συνυφασμένη με την ασύμμετρη κρυπτογραφία (ιδιωτικό και δημόσιο κλειδί) κι αυτός είναι ένας ακόμη λόγος που υπόσχεται ασφαλείς συναλλαγές. Περαιτέρω δε, η χρήση δημοσίων και ιδιωτικών κλειδιών αποτελεί μέσο πιστοποίησης της γνησιότητας της εκάστοτε συναλλαγής. Κάθε χρήστης έχει ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό) προκειμένου να μπορεί να μεταφέρει το μήνυμά του στο δίκτυο ασφαλώς.

Η κρυπτογραφία είναι ένας τρόπος εξασφάλισης και σεβασμού των τριών βασικών αρχών που διακατέχουν το blockchain: εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Confidentiality, Integrity, Availability- C.I.A) [36]. Ο συνδυασμός δε αυτών των τριών αρχών καθιστά το blockchain ως μια από τις καλύτερες τεχνολογίες. Η Αρχή της Εμπιστευτικότητας εξασφαλίζει την ανταλλαγή των πληροφοριών μεταξύ των σωστών μερών καθώς και ότι ο διαμοιρασμός των πληροφοριών γίνεται αποκλειστικά με τη συναίνεση των συμμετεχόντων (πχ οικονομικά δεδομένα, ιατρικές εξετάσεις) καθώς αποτελεί μέσο πρόληψης από μη εξουσιοδοτημένη πρόσβαση και ανάγνωση αυτών των πληροφοριών. Η Αρχή της Ακεραιότητας διασφαλίζει ότι τα δεδομένα δεν μπορούν να τροποποιηθούν από μη εξουσιοδοτημένο χρήστη και χωρίς να καταγραφεί στο αρχείο η εν λόγω τροποποίηση. Με αυτή την Αρχή αποτρέπεται η μη εξουσιοδοτημένη μεταβολή οποιασδήποτε μορφής: διαγραφή, επεξεργασία, δημιουργία. Η Αρχή της Διαθεσιμότητας εγγυάται ότι έκαστος εξουσιοδοτημένος χρήστης έχει στη διάθεση του τα δεδομένα αυτά όποτε τα χρειαστεί.

Η διαδικασία της κρυπτογραφίας αποτελείται από δύο διεργασίες: την κρυπτογράφηση και την αποκρυπτογράφηση. Η κρυπτογράφηση (encryption) είναι η διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατάληπτη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου, έτσι ώστε να μην είναι αναγνώσιμο από τρίτα μέρη, αλλά παρά μόνο από τον νόμιμο παραλήπτη. Η αποκρυπτογράφηση (decryption) είναι η διεργασία ανάκτησης του αρχικού μηνύματος (αναγνώσιμη μορφή) από μία ακατανόητη έκδοσή του που είχε παραχθεί μετά την κρυπτογράφηση. Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνονται με τη χρήση ενός κρυπτογραφικού αλγορίθμου και ενός κλειδιού κρυπτογράφησης. Η ανθεκτικότητα μιας κρυπτογράφησης εξαρτάται περισσότερο από το μέγεθος των κλειδιών που

[36] https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

χρησιμοποιούνται παρά από τους αλγορίθμους. [37] Υπάρχουν δύο συστήματα κρυπτογραφίας: η συμμετρική και η ασύμμετρη κρυπτογραφία, στην οποία βασίζεται και το blockchain.

Η ασύμμετρη κρυπτογραφία - γνωστή και ως κρυπτογραφία δημόσιου κλειδιού- είναι μια καινοτόμα μέθοδος που χρησιμοποιεί δύο κλειδιά και λύνει το πρόβλημα του διαμοιρασμού κλειδιών που είχε ανακύψει με την συμμετρική κρυπτογραφία. Θεμελιώδης ιδέα είναι ότι ο αποστολέας και ο παραλήπτης διαθέτουν διαφορετικά κλειδιά για την ανταλλαγή του μηνύματος (και όχι ένα κοινό κλειδί όπως συμβαίνει στην συμμετρική κρυπτογραφία). Συγκεκριμένα, κάθε χρήστης διαθέτει ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού (public - private key). Το δημόσιο κλειδί ανακοινώνεται σε όλο το δίκτυο ή σε όποιον επιθυμεί να επικοινωνήσει με τον χρήστη. Περαιτέρω, υπάρχουν ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers), οι οποίοι βοηθούν στην αναζήτηση ή κοινοποίηση ενός δημοσίου κλειδιού. Σε περιβάλλον blockchain, τα δημόσια κλειδιά αποτελούν τα αναγνωριστικά που αναφέρονται στην αιτιολογική σκέψη 30 του ΓΚΠΔ [38]. Αντίθετα, το ιδιωτικό πρέπει να φυλάσσεται με άκρα μυστικότητα διότι αυτό ξεκλειδώνει το μήνυμα και το αποκρυπτογραφεί. Ειδικότερα, κάθε χρήστης έχει ένα δημόσιο κλειδί (αποτελείται από μια ακαθόριστη ακολουθία γραμμάτων και αριθμών που αντιπροσωπεύει τον χρήστη), το οποίο εξομοιούται με λογαριασμό, τα στοιχεία του οποίου μοιράζεται με άλλους για να είναι δυνατή η πραγματοποίηση συναλλαγών. Επιπρόσθετα, κάθε χρήστης έχει και ένα προσωπικό ιδιωτικό κλειδί, (επίσης μια ακαθόριστη συμβολοσειρά γραμμάτων και αριθμών), το οποίο λογίζεται ως κωδικός πρόσβασης (ο οποίος δεν πρέπει να μοιραστεί ποτέ σε άλλους χρήστες)[39]. Επί παραδείγματι, η διαδικασία ανταλλαγής κλειδιών και επιβεβαίωσης είναι η εξής: ο Παραλήπτης (Π) γνωρίζει το δημόσιο κλειδί του Αποστολέα (Α). Ο Α, κάνοντας χρήση του

---

[37] Μαυρίδης Ι., Πάγκαλος Γ., "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", σελ. 187, 2002 , Εκδ ΑΝΙΚΟΥΛΑ

[38] Αιτ. Σκέψη 30 ΓΚΠΔ Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων.

Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους.

[39] Bikramaditya S. Gautam D., Priyansu Sekhar P., " Beginning Blockchain: A Beginners Guide to Building Blockchain Solutions", 2018, Apress

ιδιωτικού κλειδιού του, στέλνει ένα κρυπτογραφημένο - υπογεγραμμένο μήνυμα στον Π. Ο Π λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Α.

Αυτά τα δύο κλειδιά - δημόσιο και ιδιωτικό- συνδέονται με μία μαθηματική σχέση, η οποία μειώνει τις πιθανότητες να παραλάβει το μήνυμα κάποιος κακόβουλος τρίτος - μη εξουσιοδοτημένος. Πιο συγκεκριμένα, το ιδιωτικό κλειδί αποκρυπτογραφεί δεδομένα που έχουν κρυπτογραφηθεί μέσω του δημόσιου κλειδιού. Η επιτυχία της μαθηματικής αυτής σχέσης έγκειται στο ότι δεν μπορεί να διαβαστεί με αντίστροφη πορεία και κατά αυτόν τον τρόπο να αποκαλυφθεί το ιδιωτικό κλειδί του χρήστη.

Κατακερματισμός

Ο όρος συνάρτηση κατακερματισμού (hash function) υποδηλώνει ένα μετασχηματισμό που παίρνει σαν είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h περιορισμένου μήκους που καλείται hash value, δηλαδή είναι h = H(m).

Η ακολουθία χαρακτήρων (hash values) "καλύπτει" συνοπτικά το μήνυμα, γι αυτό καλείται και Σύνοψη Μηνύματος (Message Digests). Η συνάρτηση κατακερματισμού h μετατρέπει ένα μήνυμα αυθαίρετου μεγέθους, σε σταθερό μέγεθος, μη προδίδοντας ούτε το περιεχόμενο ούτε το μέγεθος του μηνύματος.

Ειδικότερα, το μήνυμα τεμαχίζεται σε blocks[40] σταθερού μήκους και το τελευταίο block συμπληρώνεται ώστε να γίνει ίδιο μέγεθος με τα προηγούμενα. Έπειτα σε κάθε block εκτελείται μια συνάρτηση συμπίεσης, ώστε να επιτευχθεί το μικρότερο δυνατό μέγεθος. Στη συνέχεια, ακολουθεί η συνάρτηση κατακερματισμού (hash function), η οποία προκύπτει με την επανειλημμένη εφαρμογή της συνάρτησης συμπίεσης που εφαρμόζεται σε κάθε τμήμα του block -μηνύματος μέχρι ολόκληρο το μήνυμα να υποστεί επεξεργασία.

Εν συνεχεία, ο χρήστης που παραλαμβάνει ένα μήνυμα, μπορεί να ελέγξει εάν υπήρξε κάποια αλλοίωση, εάν δώσει την ίδια συνάρτηση σαν όρισμα και οι συμβολοσειρές (message digest) ταυτίζονται. Προκειμένου να θεωρηθεί μια συνάρτηση κατακερματισμού αποδεκτή για χρήση στην κρυπτογραφία πρέπει να πληροί τις εξής απαιτήσεις: i) ασχέτως μεγέθους του κειμένου εισόδου, η έξοδος πρέπει να έχει συγκεκριμένο μήκος, ii) το hash value να μπορεί να

[40] Διαφορετικά block από αυτά που αναφέρονται στο blockchain. Πρόκειται για μικρά μέρη στα οποία «σπάει» ένα μήνυμα προκειμένου να μεταφερθεί και όταν φτάσει στον παραλήπτη να ενωθεί, προκειμένου να επανέλθει στην αρχική μορφή.

υπολογίζεται για οποιοδήποτε κείμενο, iii) η ίδια είσοδος με την ίδια συνάρτηση κατακερματισμού να παράγουν την ίδια τιμή σε κάθε επανάληψη, iv) να είναι αδύνατη η αντιστροφή της τιμής hash προκειμένου να διαβαστεί το μήνυμα και v) οποιαδήποτε αλλαγή στο μήνυμα πρέπει να επηρεάζει την συνάρτηση της εξόδου - το αποτύπωμα (hash)[41].

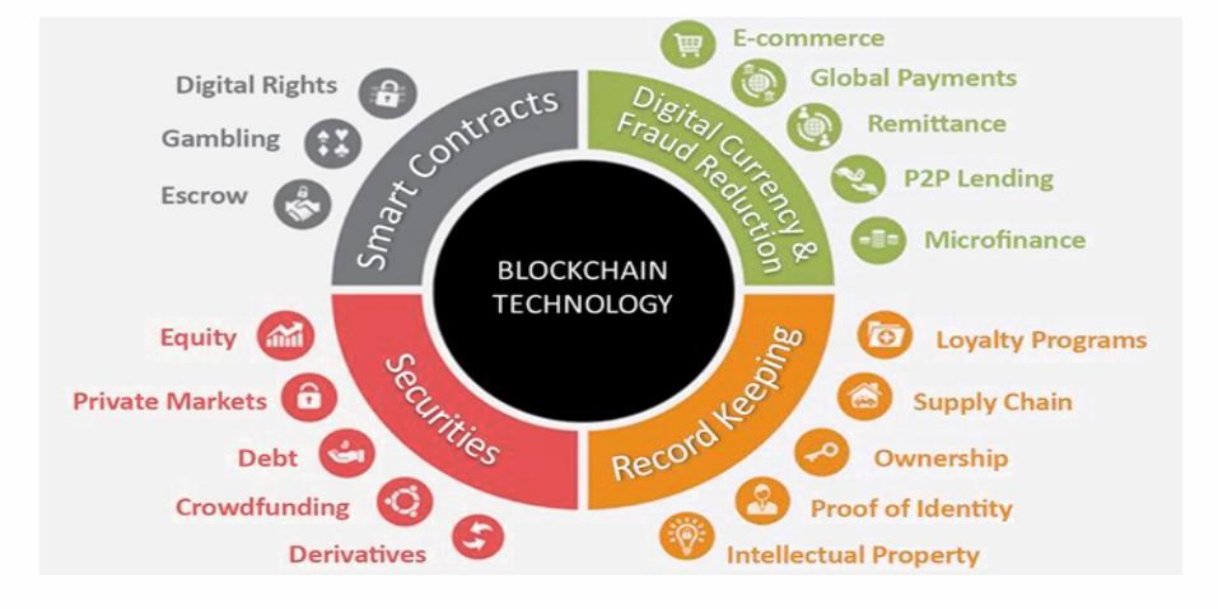
Η προηγούμενη ανάλυση αφορά την τυπική διαδικασία κατακερματισμού. Ωστόσο, υπάρχει και μία βελτιωμένη έκδοση που υπόσχεται μεγαλύτερη ασφάλεια. Πρόκειται για τον "κατακερματισμό χαμαιλέοντα"[42], ο οποίος επαναδημιουργεί αλγορίθμους μέσω της χρήσης ενός ασφαλούς ιδιωτικού κλειδιού. Το εν λόγω κλειδί ξεκλειδώνει ένα εικονικό λουκέτο στην αλυσίδα που συνδέει κάθε μπλοκ. Με τη μέθοδο αυτή επιτρέπεται η τροποποίηση ή η διαγραφή δεδομένων, αφήνοντας ίχνος της κάθε ενέργειας, ώστε να λαμβάνουν γνώση οι συμμετέχοντες για κάθε πράξη[43].

[41] Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, "Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions", 2018, Apress

[42] Khalili et al., "Chameleon hashing, Efficient chameleon hash functions in the enhanced collision resistant model" https://www.sciencedirect.com/science/article/abs/pii/S002002551930831X?via%-3Dihub

[43] Κανέλλος Λ., "Smart Contracts, Νομικές Προκλήσεις και επιχειρηματικές προοπτικές", , σελ 217, 2022, Νομική Βιβλιοθήκη

2.5. Εφαρμογές Blockchain

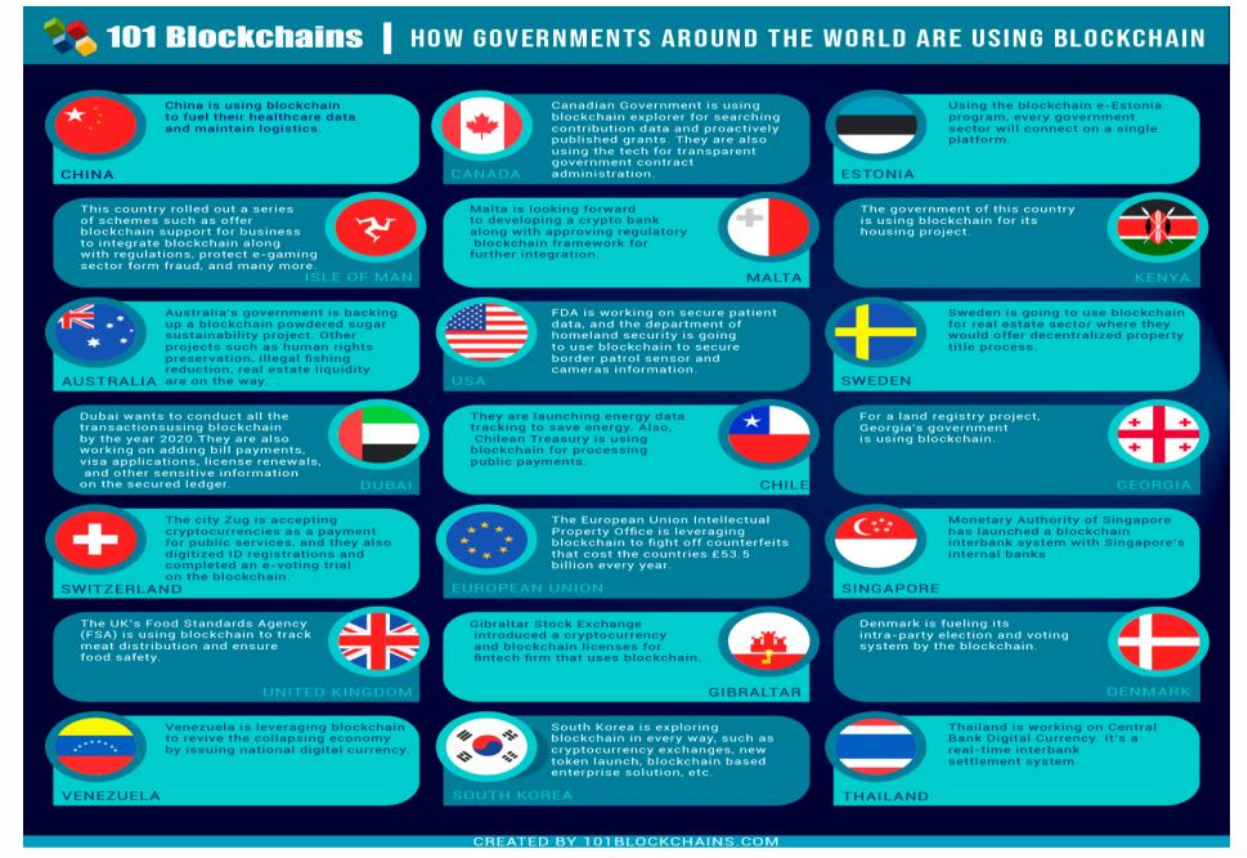


Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

Στην παρούσα ενότητα και πριν αναλύσουμε το θέμα της παρούσας εργασίας σε βάθος, αξίζει να καταγράψουμε τις εφαρμογές blockchain που χρησιμοποιούνται σήμερα και ενδεχομένως μερικές ιδεατές ή και αναγκαίες για το μέλλον. Σε πολλές χώρες[44], χρησιμοποιείται ήδη το blockchain ποικιλοτρόπως, εμπνέοντας και τις λοιπές να υιοθετήσουν το παράδειγμά τους. Μερικά παραδείγματα εξ αυτών αποτελεί η Κίνα που χρησιμοποιεί blockchain εφαρμογές τόσο στο σύστημα Υγείας όσο και σε υπηρεσίες logistics. Στις ΗΠΑ γίνεται χρήση blockchain εφαρμογών από τον FDA (Food and Drug Administration) καθώς και από το Υπουργείο Δημόσιας Τάξης. Περαιτέρω, η Ελβετία - η οποία πρωτοπόρησε σε αυτόν τον τομέα- δέχεται τα bitcoins και άλλα κρυπτονομίσματα ως μέσο πληρωμής σε δημόσιες υπηρεσίες και έχει πάνω από εξακόσιες (600) εταιρείες. Αντιστοίχως, η Βενεζουέλα και η Ταϊλάνδη χρησιμοποιούν κρυπτονομίσματα ως παράλληλο ψηφιακό νόμισμα. Επίσης, η Σιγκαπούρη χρησιμοποιεί εφαρμογές blockchain για ανταλλαγή νομισμάτων με την Κεντρική Τράπεζα. Το Ηνωμένο Βασίλειο ελέγχει την πορεία και την κατάσταση των τροφίμων (ημερομηνία παραγωγής, υλικά, διαδρομή που ακολούθησαν, πόσο καιρό έμειναν στα ράφια) και κατ΄αυτόν τον τρόπο μπορεί να εξασφαλίσει την ασφάλεια των

[44] https://irishtechnews.ie/global-blockchain-adoption-which-countries-are-leading-the-charge/

τροφίμων (πχ του κρέατος). Στην Δανία, υλοποιείται πιλοτικά σύστημα ψηφοφορίας βασισμένο σε blockchain. Στον Καναδά, γίνεται έλεγχος της Δημόσιας Διοίκησης με εφαρμογές και συστήματα blockchain. Επιπρόσθετα, οι εν λόγω εφαρμογές χρησιμοποιούνται και για την διαχείριση ακινήτων, όπως στη Σουηδία που το χρησιμοποιεί στο real estate αλλά και στην Κένυα και τη Μαλαισία υπάρχουν εφαρμογές που ρυθμίζουν ζητήματα στέγασης και εκμίσθωσης. Η Κορέα εισάγει και προωθεί στην αγορά τα crypto tokens. Στην Ελλάδα, η εταιρεία Mytilineos[45] διασφαλίζει μια συνεργασία με την Αυστραλία υπογράφοντας νέα σύμβαση εξαγοράς ενέργειας μέσω blockchain. Η Σύμβαση υπεγράφη στην πλατφόρμα της WePower, μιας από τις μεγαλύτερες διεθνώς πλατφόρμες αγοράς και εμπορίας ενέργειας που στηρίζεται στην τεχνολογία blockchain.



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

[45] https://www.mytilineos.gr/news/press-releases/mytilineos-is-securing-a-new-ppa-in-australia-through-the-blockchain-technology/

Υπό το φως του πρόσφατου νόμου 4622/2022 (ΦΕΚ Α’ 133/07.08.2019) με τον οποίο γίνονται τα πρώτα βήματα στην Ελλάδα για την αναγνώριση της τεχνολογίας αυτής αλλά και της ένταξης της στην καθημερινότητα μας σε πληθώρα δραστηριοτήτων και ενεργειών, θα κατηγοριοποιήσουμε τις εφαρμογές σε δύο κατηγορίες: εφαρμογές δημοσίου τομέα και εφαρμογές ιδιωτικού τομέα. Σε αυτό το σημείο, δέον να υπογραμμισθεί ότι τα ποικίλα νομικά ζητήματα που τίθενται - όπως θα εκτεθούν στις έξυπνες συμβάσεις- ποικίλουν σε μεγάλο βαθμό, αναλόγως του πλαισίου εφαρμογής τους καθώς και τον τύπο δικτύου στο οποίο έχουν δομηθεί (ανοικτά-κλειστά- κοινοπρακτικά). Οι οιονεί ευθύνες που θα αποδοθούν είναι ανάλογες και συναρτώνται με τα προαναφερθέντα.

Οι εφαρμογές δημοσίου τομέα συνεχώς και τάχιστα εδραιώνονται στην Ευρώπη και πλέον κερδίζουν έδαφος και στην Ελλάδα. Οι περισσότερες ιδέες που έχουν υλοποιηθεί αφορούν την τήρηση αρχείων και δημοσίων μητρώων, όπως **φορολογικά, ληξιαρχικά, κτηματολογικά και εμπορικά μητρώα**. Εφαρμογές blockchain ωστόσο υπάρχουν και στην **δικαιοσύνη, στην ηλεκτρονική διακυβέρνηση**, **την εκλογική διαδικασία** καθώς και στην **εκπαίδευση** και στην **υγεία**. Επιπρόσθετα, με μεγάλη ταχύτητα δημιουργούνται εφαρμογές blockchain και στον ιδιωτικό τομέα. Εφαρμογές για ψηφιακή αναπαράσταση της αξίας είτε για την επένδυση σε κάποιο ακίνητο (φυσικό ή εικονικό) είτε σε μορφή ηλεκτρονικού χρήματος είτε για την αγορά υπηρεσιών (utility tokens), εφαρμογές για μη ανταλλάξιμα ψηφιακά πιστοποιητικά ιδιοκτησίας (Non-Fungible Tokens - NFTs) για την αγορά συλλεκτικών αντικειμένων, συνήθως έργων τέχνης . Επιπλέον υπάρχουν εφαρμογές κατανεμημένου καθολικού για αγορά ενέργειας, για συμβολαιογραφικές υπηρεσίες, για την ιχνηλάτηση εφοδιαστικής αλυσίδας για τις εργασιακές σχέσεις καθώς και για ασφαλιστικές υπηρεσίες. Παρακάτω, γίνεται πιο εκτενής αναφορά στις εφαρμογές με νομικό χαρακτήρα:

2.5.1. Φορολογικό και Κτηματολογικό Μητρώο

Χαρακτηριστικό είναι το παράδειγμα της Σουηδίας , η οποία χρησιμοποιεί εφαρμογές blockchain τόσο για κτηματολογικά μητρώα όσο και για φορολογικά. Πιο συγκεκριμένα, υπάρχει μια πιλοτική πλατφόρμα στην οποία καταχωρούνται τα ιδιοκτησιακά δικαιώματα των πολιτών επί

ακίνητης περιουσίας καθώς και πιθανά εμπράγματα βάρη αυτών. Η διαδικασία της καταχώρησης των ακινήτων στο κτηματολογικό μητρώο γίνονται με χρονολογική σειρά και πιστοποιούνται τη διαδικασία της χρονοσφράγισης (timestamp) με αποτέλεσμα να αποφεύγονται λάθη και παραποιήσεις [46]. Επιπλέον, η Σουηδία έχει δημιουργήσει μια πιλοτική εφαρμογή για την ψηφιοποίηση των αποδείξεων, του φόρου εισοδήματος καθώς και των τελωνειακών δασμών. Περαιτέρω, αξίζει να αναφερθούν και μεμονωμένα παραδείγματα χωρών που χρησιμοποιούν το blockchain με διαφορετικό τρόπο για την τήρηση αντίστοιχων μητρώων, προκειμένου να αποτυπωθεί η ευρεία και ποικιλόμορφη χρήση τους. Για φορολογικούς σκοπούς, η Φινλανδία χρησιμοποιεί blockchain εφαρμογές προκειμένου η φορολογική διοίκηση να συνεργάζεται με τις Τράπεζες για την παρακολούθηση και είσπραξη φόρων στις συναλλαγές ακινήτων [47].

Όσον αφορά τα φορολογικά μητρώα, καταβάλλονται συνεχείς προσπάθειες με κατεύθυνση τη δημιουργία ενός ενιαίου ψηφιακού μητρώου τιμολογίων με σκοπό την αντιμετώπιση της φοροδιαφυγής [48] καθώς και την αντιμετώπιση του μείζονος προβλήματος του ξεπλύματος μαύρου χρήματος (money laundering- AML νομοθεσία), παρά το ότι η τεχνολογία blockchain έχει κατηγορηθεί ως μέσο για ξέπλυμα μαύρου χρήματος [49]. Πιο συγκεκριμένα, η Ευρώπη αποσκοπεί στην αυτόματη είσπραξη φόρου και ΦΠΑ με την χρήση των έξυπνων συμβολαίων. Ωστόσο, το ενδιαφέρον για τις φορολογικές και κτηματολογικές εφαρμογές blockchain δεν περιορίζεται σε ευρωπαϊκά σύνορα αλλά εξαπλώνεται σε παγκόσμιο επίπεδο. Η Ομοσπονδιακή Φορολογική Διοίκηση της Βραζιλίας ενσωμάτωσε τα γενικά εμπορικά και φορολογικά μητρώα σε υποδομή blockchain, διασυνδέοντας κατά αυτόν τον τρόπο τα τελωνεία των χωρών της κοινής αγοράς, υπακούοντας στις επιταγές της Συνθήκης Mercosur [50] [51].

Όσον αφορά στα κτηματολογικά μητρώα, το παράδειγμα της Σουηδίας ακολουθούν πολλές χώρες, όπως η Ινδία, η Ελβετία, το Λουξεμβούργο, η Γεωργία, η Εσθονία και η Μάλτα [52].

---

[46] https://blog.chain.link/blockchain-technology-real-estate/

[47] https://www.unlock-bc.com/news/2020-03-16/finlands-housing-market-now-securely-on-the-blockchain/

[48] https://news.bloombergtax.com/daily-tax-report-international/eu-inches-toward-blockchain-in-fight-against-vat-fraud-1

[49] Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business - https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital

[50] https://en.wikipedia.org/wiki/Mercosur

[51] Blockchain in Tax Administrations - https://www.ciat.org/blockchain-in-tax-administrations/?lang=en

[52] https://www.blockchain-council.org/blockchain/blockchain-land-registries-across-the-globe/

Σε αυτό το σημείο ωστόσο, οφείλουμε να επισημάνουμε ότι σε όλες αυτές τις χώρες η εφαρμογή είναι πιλοτική και δεν πρόκειται για κανονική και πλήρη χρήση εξαιτίας των ζητημάτων που ανακύπτουν. Η εν λόγω τεχνολογία είναι σε εμβρυακό στάδιο και τα ζητήματα ασφαλείας που τίθενται είναι πολλά και δυσεπίλυτα σε ορισμένες περιπτώσεις (πχ μια κακόβουλη καταγραφή στο αρχείο μπορεί να δώσει ή να στερήσει ένα εμπράγματο δικαίωμα επί ακινήτου). Περαιτέρω δε, η τεχνολογία δεν υποστηρίζει ακόμα όλες τις απαραίτητες διορθωτικές ενέργειες που μπορούν και απαιτούνται να γίνουν στον φυσικό κόσμο. Για τον λόγο αυτό, οι εφαρμογές αυτές δεν μπορούν να αντικαταστήσουν - προς το παρόν τουλάχιστον- τα κτηματολογικά γραφεία καθώς και τα "έγγραφα" που εκδίδονται δεν μπορούν να εξομοιωθούν με συμβολαιογραφικά (και την ισχύ που φέρουν αυτά). Αξίζει ωστόσο, στο πλαίσιο αυτό, να καταγραφεί μια ευχή του νομικού κόσμου για τη δημιουργία μίας ενιαίας και ασφαλούς κτηματολογικής βάσης, η οποία θα αναγνωρισθεί νομοθετικά και θα μετατρέψει όλες τις παραδοσιακές συναλλαγές σε ψηφιακές, προσδίδοντας βεβαίως το αίσθημα ασφάλειας για την ταυτότητα και ό,τι άλλο χαρακτηρίζει ένα ακίνητο. Οι χρονοβόρες και πολυδάπανες γραφειοκρατικές διαδικασίες θα εκλείψουν αφού η εκάστοτε μεταβίβαση ακινήτου (με ό,τι απαιτεί αυτή) θα γίνεται σε μία ενιαία βάση blockchain. Περαιτέρω δε, η ένταξη αυτών των μηχανισμών στις προαναφερθείσες διαδικασίες δεν καταργεί και δεν ακυρώνει την εργασία των έμπειρων νομικών και συμβολαιογράφων, αλλά αντιθέτως την ενισχύει διότι χωρίς την σύμπραξή τους το σύστημα δεν θα μπορέσει να δημιουργηθεί το αντίστοιχο-ψηφιακό πλέον-συμβόλαιο.

2.5.2. Δικαιοσύνη

Όπως έχει προαναφερθεί, η τεχνολογία blockchain παρέχει εγγυήσεις ασφάλειας ως προς την αδιαβλητότητα, την ακεραιότητα και την εμπιστευτικότητα. Τα χαρακτηριστικά αυτά μπορούν να το καταστήσουν ένα πολύτιμο εργαλείο για τους νομικούς για την θεμελίωση και προάσπιση της δικαιοσύνης. Η ανάγκη για ανάπτυξη ενός τέτοιου συστήματος που θα διασφαλίζει τα έγγραφα και τις νομικές πράξεις πλέον καθίσταται αδήριτη. Ο νομικός κόσμος, σε διεθνές επίπεδο, αποζητά αυτό το σύστημα και η προσοχή είναι στραμμένη στις χώρες που έχουν κάνει τα πρώτα βήματα σε αυτόν τον τομέα. Πιο συγκεκριμένα. η Γαλλία, (η οποία αναγνώρισε την αποδεικτική αξία των αρχείων blockchain που αφορούν σε ψηφιακά δικαιώματα

χρηματοοικονομικών προϊόντων και παραγώγων), η Ιταλία και το Ηνωμένο Βασίλειο[53] αποδέχονται το blockchain ως μέσο απόδειξης.

Η Ευρωπαϊκή Επιτροπή, το 2020, διεξήγαγε μια μελέτη στην οποία παρουσιάστηκαν πληθώρα δυνητικών εφαρμογών κατανεμημένου καθολικού για τον κλάδο της Δικαιοσύνης όπως ταυτοποίηση υπόπτων, ασφαλής ανταλλαγή εγγράφων μεταξύ διωκτικών αρχών, υπουργείων και δικαστηρίων, ψηφιοποίηση δικαστικών αποφάσεων (και ανάγνωση αυτών από μηχανές) [54]. Παράλληλα, σε διεθνές επίπεδο αναπτύσσονται συνεχώς εφαρμογές DLT κυρίως για την ποινική διαδικασία στην Κίνα και στις ΗΠΑ, όπου τα προβλήματα απάτης και διαφθοράς είναι πιο μεγάλα.

Όμως, οι δικαστηριακές εφαρμογές blockchain δεν περιορίζονται στην ποινική διαδικασία αλλά χρησιμοποιούνται και στην πολιτική διαδικασία. Τα δικαστήρια του Διεθνούς Χρηματοοικονομικού Κέντρου στο Ντουμπάι, με τη χρήση blockchain επαληθεύουν δικαστικά έγγραφα σε πραγματικό χρόνο, επιβάλλοντας ταυτόχρονα διασυνοριακά τον νόμο[55]. Επίσης, στην πόλη Hangzou, τα κινέζικα δικαστήρια χρησιμοποιούν τεχνολογίες blockchain για την επίλυση διαφορών ηλεκτρονικού εμπορίου [56]. Περαιτέρω δε, υπάρχει και μια πλατφόρμα εκτέλεσης των δικαστικών αποφάσεων που σχετίζονται με τις οφειλές από κρυπτονομίσματα μέσω των έξυπνων συμβολαίων [57]

[53] Blockchain & Cryptocurrency Laws and Regulations | United Kingdom | GLI - https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/united-kingdom

[54] Study on the use of innovative technologies in the justice field https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1/language-en/format-PDF/source-279592216

[55] Courts and Smart Dubai to launch world's first "Court of the Blockchain" https://www.engage.hoganlovells.com/knowledgeservices/news/difc-courts-and-smart-dubai-to-launch-worlds-first-court-of-the-blockchain

[56] Vivien Chan , Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb

[57] Zhen Er Low, Execution of Judgements on the Blockchain- A Practical Legal Commentary, 2021 https://jolt.law.harvard.edu./digest/execution-of-judgements-on-the-blockchain-a-practical-legal-commentary

2.5.3. Ηλεκτρονική Διακυβέρνηση

Η τεχνολογία DLT (blockchain) δίνει τη δυνατότητα δημιουργίας ασφαλών αρχείων κυβερνητικών υπηρεσιών καθώς και ψηφιακών διαπιστευτηρίων πολιτών. Η Ευρωπαϊκή Ένωση έχει σχέδιο εφαρμογής μια τεχνολογίας για τα βιογραφικά Europass καθώς και τα ψηφιακά διαπιστευτήρια , προκειμένου να ενισχύσει και να διασφαλίσει την εγκυρότητα των προσόντων και άλλων μαθησιακών επιτευγμάτων σε όλη την Ευρώπη [58]. Παράλληλα, η Εσθονία φέρει την παγκόσμια πρωτιά στη δημιουργία ενός κυρίαρχου και πανίσχυρου διαπιστευτηρίου ταυτότητας που υποστηρίζεται από την κυβέρνηση μέσω του KSI blockchain[59]. Με την εφαρμογή αυτή η κυβέρνηση διαχειρίζεται πληθώρα και ποικίλα έγγραφα των πολιτών της όπως : διπλώματα οδήγησης, διαβατήρια, πιστοποιητικά διαφόρων κατηγοριών καθώς και τραπεζικά αρχεία και δεδομένα υγείας.

2.5.4. Ηλεκτρονική Ψηφοφορία

Η χρήση εφαρμογών blockchain στις ηλεκτρονικές ψηφοφορίες μπορεί να αποδειχθεί καλύτερη και ασφαλέστερη παρέχοντας πληθώρα δυνατοτήτων όπως ελεγχόμενος τρόπος πρόσβασης στο σύστημα, καταγραφή ψήφων, οριστική καταγραφή ψήφων στο βιβλίο ψηφοφορίας, σεβασμός ανωνυμίας εκλογέα και αποτροπή νοθείας. Ωστόσο, για να είναι εφαρμόσιμο ένα τέτοιο εργαλείο σε πραγματικές συνθήκες θα πρέπει να τεθούν κάποια κριτήρια και περιορισμοί. Πιο συγκεκριμένα, κάθε ανάλογη εφαρμογή πρέπει να πληροί τις προϋποθέσεις της ισχύουσας εκλογικής νομοθεσίας όπως : α) επιλεξιμότητα και έλεγχος, ώστε να ψηφίζει μία φορά έκαστος εκλογέας στους καταλόγους που είναι εγγεγραμμένος, β) μυστικότητα, γ) αυστηρότητα, ώστε τα άκυρα ψηφοδέλτια να αναγνωρίζονται και να μην λαμβάνονται υπόψη με αυτόματο τρόπο, δ) πληρότητα, ώστε όλα τα έγκυρα ψηφοδέλτια να καταχωρίζονται και καταμετρώνται σωστά. Στο πλαίσιο αυτό, έχουν δημιουργηθεί αρκετές εφαρμογές για την διεξαγωγή ηλεκτρονικών ψηφοφοριών, σε εταιρικό, τοπικό, περιφερειακό ή ακόμα και εθνικό επίπεδο [60]. Εφαρμογές blockchain για ηλεκτρονική ψηφοφορία χρησιμοποιήθηκαν και στέφθηκαν με απόλυτη επιτυχία σε τοπικό επίπεδο (Μάλτα, Ισπανία,Ολλανδία), σε περιφερειακό επίπεδο

[58] Απόφαση Europass (ΕΕ) 2018/646, άρθρο 4 παρ 6

[59] https://www.dhs.gov/science-and-technology/blockchain-portfolio

[60] Uzma Jafar,Mohd Juzaiddin Ab Aziz andZarina Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges” https://www.mdpi.com/1424-8220/21/17/5874

στην Ουκρανία[61] και στις εθνικές εκλογές του 2018 στην Σιέρρα Λεόνε[62]. Αξιοσημείωτο είναι δε πως καινοτόμες ψηφιακές λύσεις βασισμένες σε τεχνολογία blockchain στις δημόσιες υπηρεσίες, στο πλαίσιο του ευρωπαϊκού έργου TOKEN εφαρμόζονται και στην Ελλάδα για δημοψηφίσματα στους Δήμους Κατερίνης και Παύλου Μελά[63].

2.5.5. Προστασία Πνευματικών Δικαιωμάτων

Το blockchain μπορεί επίσης να συμβάλει στην αποτελεσματική διαχείριση και προστασία των δικαιωμάτων διανοητικής ιδιοκτησίας. Σε αυτά συμπεριλαμβάνονται η αδειοδότηση χρήσης πνευματικών έργων καθώς και η εκμετάλλευση ψηφιακού έργου[64]. Πιο συγκεκριμένα, η διαδικασία καταχώρησης και προστασίας είναι η εξής: η καταχώριση γίνεται σε μια βάση δεδομένων, τηρώντας την Αρχή της Χρονικής Προτεραιότητας και διασφαλίζοντας την ασφάλεια των έργων με κρυπτογραφικό τρόπο. Ενδεικτικά, τα έργα που μπορούν να προστατευτούν με αυτό τον τρόπο είναι εφευρέσεις, εμπορικά σήματα, πνευματικά έργα[65], υποδείγματα και σχέδια κατοχυρώνοντας και εξασφαλίζοντας το δικαίωμα εμπορικής εκμετάλλευσης στους δικαιούχους στα προϊόντα της διάνοιας τους. Περαιτέρω δε, η κατοχύρωση των δικαιωμάτων τους με τεχνολογία blockchain και η παράλληλη χρήση ψηφιακών διακριτικών θα έθετε ένα όριο στην οικονομική ανασφάλεια και ανισορροπία, διευκολύνοντας την κατανομή των αμοιβών μεταξύ δικαιούχων και χρηστών, περιορίζοντας τη δράση των οργανισμών συλλογικής διαχείρισης[66]. Περαιτέρω δε, εικάζεται πως η τεχνολογία blockchain θα αποτελέσει σημαντικό και καθοριστικό φραγμό στην ελεύθερη κυκλοφορία προϊόντων απομίμησης που κατακλύζουν την αγορά, αφού στα γνήσια έργα θα δίδεται ένα μοναδικό ψηφιακό αναγνωριστικό από τις αστυνομικές και τελωνειακές αρχές.

---

[61] Σύστημα Ηλεκτρονικής Ψηφοφορίας e-Vox, το οποίο βασίζεται στα "colored coins"

[62] Raul Zambrano, Andrew Young, and Stefaan Verhulst, "Seeking Ways to Prevent Electoral Fraud using Blockchain in Sierra Leone" https://blockchan.ge/blockchange-election-monitoring.pdf

[63] https://www.fortunegreece.com/article/efarmoges-blockchain-gia-proti-fora-ston-dimo-katerinis/

[64] Οδηγία DSM (2019/790)

[65] Balázs Bodó, Daniel Gervais, João Pedro Quintais, "Blockchain and smart contracts: the missing link in copyright licensing? " International Journal of Law and Information Technology, Volume 26, Issue 4, Winter 2018, Pages 311–336, https://doi.org/10.1093/ijlit/eay014

[66] Παπαδοπούλου Α., "Blockchain: Η τεχνολογία που υπόσχεται «ψηφιακή ασφάλεια» - Πιθανές εφαρμογές και συνέπειες για το δίκαιο πνευματικής ιδιοκτησίας και ιδίως στο ζήτημα της ψηφιακής ανάλωσης" σ. 211, 2018, ΕπισκΕΔ

Ένα ακόμη πλεονέκτημα αυτής της τεχνολογίας αποτελεί η χρονοσήμανση (timestamping) των έργων, ανάλογο της εφαρμογής WIPO Proof (της Διεθνούς Οργάνωσης Προστασίας Πνευματικής Ιδιοκτησίας)[67]. Η εγγραφή δεδομένων δημιουργίας πνευματικών έργων σε τεχνολογία DLT και η ταυτόχρονη χρονοσήμανση αυτών θα γίνεται με τη χρήση tokens (κουπόνια). Ωστόσο, η συγκεκριμένη πρόταση παρότι εγγυάται ασφάλεια και το αδιάβλητο της διαδικασίας, δεν μπορεί να εγγυηθεί ότι όποιος καταχωρεί ένα έργο σε πρότερο χρόνο είναι και ο πραγματικός δημιουργός του, και όχι ένας άρτιος τεχνικά λογοκλόπος που κινείται δολίως υφαρπάζοντας την δουλεία και τη δημιουργία του αληθινού δημιουργού.

Συνοπτικά, η πρόταση αυτή αποτελεί έναν εναλλακτικό τρόπο κατάθεσης του έργου σε έναν συμβολαιογράφο, προς κατοχύρωση και εξασφάλιση του βέβαιου της χρονολογίας και κατάκτησης δικαιωμάτων σε οιονεί δικαστικές διαμάχες. Αντίστοιχες προσπάθειες, έχουν γίνει στο παρελθόν από φωτογράφους και δημιουργούς εικόνας, οι οποίες απέβησαν άκαρπες [68].

2.5.6. Συμβολαιογραφικές Υπηρεσίες

Ο συμβολαιογράφος αποκτά ένα νέο σύμμαχο και εξαιρετικό συνεργάτη για την ταχύτερη και ασφαλέστερη διεκπεραίωση της δουλειάς του. Οι πάροχοι εφαρμογών απομακρυσμένης συμβολαιογραφικής επικύρωσης επιτρέπουν στους συμβολαιογράφους που συμμετέχουν στο δίκτυο blockchain να παράσχουν επαναστατικές υπηρεσίες δημιουργίας και επικύρωσης εγγράφων. Πάροχοι όπως DIGIT, 4Eire, Acronis, που δημιουργούν αυτές τις εφαρμογές , χρησιμοποιούν μια διεπαφή χρήστη (API) και ένα έξυπνο συμβόλαιο αποθηκευμένο στο ίδιο blockchain που χειρίζεται ο χρήστης, προκειμένου να αλληλεπιδρούν ακώλυτα. Πρόκειται για εφαρμογές smart notarization [69].

Η διαδικασία εκκινεί θέτοντας μια συμβολαιογραφική υπογραφή σε οποιοδήποτε ψηφιακό περιεχόμενο συμβολαιογραφικής φύσης[70] (μαρτυρική κατάθεση, ψηφιακή διαθήκη, κατάθεσης

---

[67] Rose A., "Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights" https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html

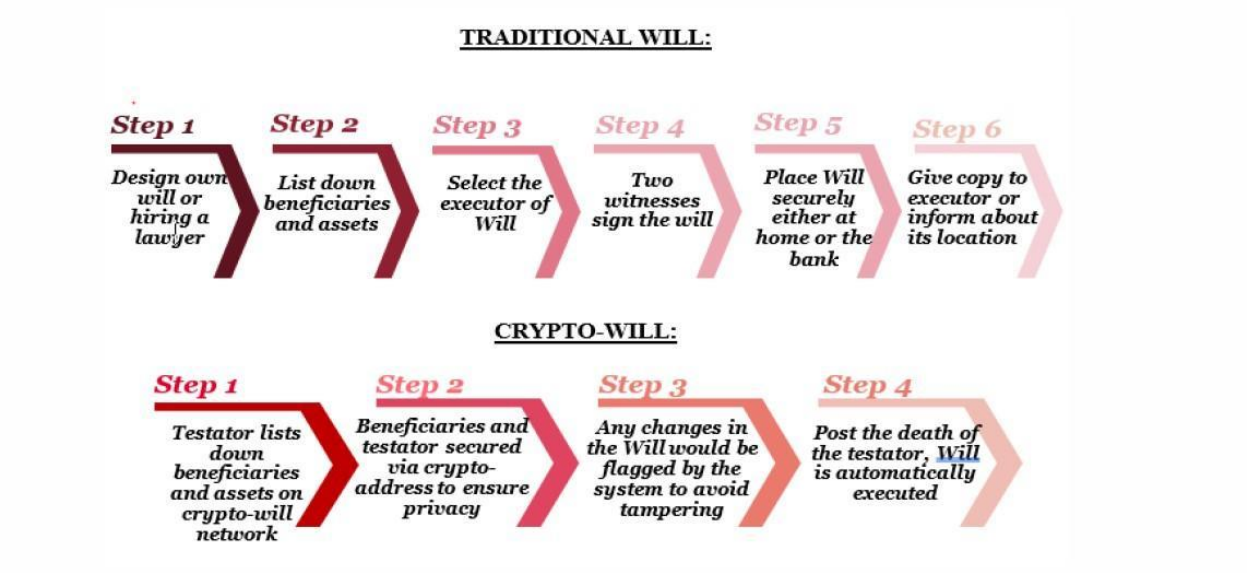
[68] https://en.wikipedia.org/wiki/KodakCoin

[69] About Blockchain Based Notary Proof Of Concept https://joinup.ec.europa.eu/collection/blockchain-egov-services/solution/blockchain-based-notary-proof-concept/about#:~:text=DIGIT%20has%20developed%20a%20Blockchain,a%20distributed%20and%20decentralized%20ledger.

[70] Blockchain Use Case for Notary https://4irelabs.com/cases/notarization-in-blockchain/#:~:text=Notarization%20is%20an%20official%20fraud,cannot%20be%20edited%20or%20deleted.

πνευματικού έργου και συμβόλαιο αγοραπωλησίας ακινήτου) με την παράλληλη δημιουργία μιας μοναδικής συνάρτησης κατακερματισμού (SHA 256). Κατ΄ουσίαν, ο εκάστοτε πελάτης θα επιλέγει ένα μοναδικό αρχείο για χρονοσήμανση σε μια συγκεκριμένη και προκαθορισμένη αλυσίδα blocks. Εν συνεχεία, έπεται η μόνιμη αποθήκευση και η χρονοσήμανση του κατακερματισμένου -πλέον-αρχείου στην εκάστοτε και επιλεχθείσα πλατφόρμα DLT. Στο επόμενο στάδιο, ο server (διακομιστής) του συμβολαιογράφου συνδέει το αρχείο με την επιλεγείσα συγκεκριμένη χρονοσήμανση. Έπειτα, ο server με αυτοματοποιημένο τρόπο υποβάλλει ερώτημα στο blockchain, ώστε να ελεγθεί εάν ο συγκεκριμένος κατακερματισμός είναι ήδη καταχωρημένος. Σε περίπτωση καταφατικής απάντησης, εκκινεί πλήρως η διαδικασία, ώστε ο server του συμβολαιογράφου να επιτρέψει την τοποθέτηση χρονοσφραγίδας. Δέον να επισημανθεί ότι κατά αυτόν τον τρόπο (κατακερματισμός SHA 256) δεν αποκαλύπτεται το περιεχόμενο του εγγράφου και η διεύθυνση του έξυπνου συμβολαίου (που φέρει το εν λόγω έγγραφο) δεν μπορεί να οδηγήσει σε αντίστροφη κρυπτογράφηση και να αποκαλύψει το περιεχόμενο.

Επομένως, με την μέθοδο αυτή διασφαλίζεται η ακέραιη και ασφαλής καταχώρηση των δεδομένων που περιλαμβάνονται στα ψηφιακά αρχεία προς οποιαδήποτε συμβολαιογραφική ενέργεια



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

3. Ethereum

Το Ethereum είναι μια πλατφόρμα λογισμικού (Software Platform), η οποία βασίζεται στην τεχνολογία του Blockchain. Πιο συγκεκριμένα, πρόκειται για μια DIY Platform (Do it yourself) με την οποία καθίσταται εφικτή η χρήση αποκεντρωμένων προγραμμάτων (Decentralized Apps). Κάθε χρήστης μπορεί να δημιουργήσει τη δική του αποκεντρωμένη εφαρμογή (Dapp) χρησιμοποιώντας τα Έξυπνα Συμβόλαια (Smart Contracts) αξιοποιώντας την τεχνολογία Blockchain με όλες τις δυνατότητες που προσφέρει το Ethereum.

Το Ethereum έχει ως στόχο να αποκεντρώσει τις υπηρεσίες που προσφέρονται στο internet. Μέχρι και σήμερα, το internet μεσολαβεί στην επικοινωνία ή στην παροχή υπηρεσιών δίνοντας βήμα και συνδέοντας όλο τον κόσμο. Το Ethereum υπόσχεται πώς θα χρησιμοποιεί το internet αλλά δεν θα χρειάζεται όλους αυτούς τους μεσάζοντες αλλά κάθε επικοινωνία, δραστηριότητα, ή υπηρεσία θα παρέχεται – ανταλλάσσεται μεταξύ των χρηστών, χωρίς τη μεσολάβηση κάποιας πλατφόρμας.

Σε αυτό το σημείο και πριν την λεπτομερή ανάπτυξη τους, θα γίνει μια σύντομη αναφορά σε βασικούς όρους για το Ethereum. Η δημιουργία εφαρμογών και έξυπνων συμβολαίων στο Ethereum γίνεται με τη γλώσσα προγραμματισμού Solidity. Περαιτέρω, το δίκτυο τροφοδοτείται και λειτουργεί με τη χρήση του κρυπτονομίσματος Ether, το οποίο δίνεται ως κίνητρο στους χρήστες προκειμένου να χρησιμοποιούν το πρωτόκολλο αυτό στους υπολογιστές τους.

3.1. Ιστορικά για το Ethereum

Το 2013, ο Vitalik Buterin, ερευνητής και προγραμματιστής κρυπτονομισμάτων πρότεινε το Ethereum. Το 2014, δημοσιεύτηκε το Yellow Paper του Ethereum από τον Dr. Gavin Wood[71], στο οποίο περιγράφονται οι τεχνικές λεπτομέρειες του. Εν συνεχεία, τον Ιούλιο του ίδιου έτους, η ανάπτυξη χρηματοδοτήθηκε από μια διαδικτυακή χρηματοδότηση (crowdsale). Το σύστημα

[71] Gavin Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger” Berlin Version. 2022

δημιουργήθηκε στις 30 Ιουλίου 2015, με 11.9 εκατομμύρια «προεξορυγμένα» κέρματα για το crowdsale [72].

Το όνομα Ethereum είναι αποτέλεσμα διαδικτυακής περιήγησης σχετικά με τα στοιχεία και την επιστημονική φαντασία. Ο Buterin, βρίσκοντας το όνομα Ethereum , έγραψε: *«αμέσως κατάλαβα ότι μου άρεσε περισσότερο από όλες τις άλλες εναλλακτικές λύσεις που είχα δει. Υποθέτω ότι ήταν το γεγονός που ακουγόταν ωραίο και είχε τη λέξη "ether" (αιθέρας), που αναφέρεται στο υποθετικό αόρατο μέσο που διαπερνά το σύμπαν και επιτρέπει στο φως για να ταξιδεύει.»* [73]

3.2. Τι είναι - Πώς λειτουργεί

Το Ethereum είναι δημόσια πλατφόρμα blockchain ανοιχτού κώδικα που βασίζεται στην κατανεμημένη υπολογιστική αλλά και λειτουργικό σύστημα που διαθέτει τη λειτουργικότητα έξυπνης σύμβασης (scripting) [74]. Εκτελείται σε ένα δίκτυο υπολογιστών και διασφαλίζει ότι τα δεδομένα και τα μικρά προγράμματα υπολογιστών, γνωστά ως smart contracts (έξυπνα συμβόλαια), μεταδίδονται και αντιγράφονται σε όλους τους υπολογιστές του δικτύου, χωρίς ένα κεντρικό συντονιστή. Με αυτό τον τρόπο επεκτείνει τις εφαρμογές του blockchain, επικυρώνοντας, αποθηκεύοντας και αντιγράφοντας δεδομένα συναλλαγών σε πολλούς υπολογιστές σε όλο τον κόσμο. Η ιδέα και δομή του Ethereum αποσκοπεί στη δημιουργία ενός παγκόσμιου ηλεκτρονικού υπολογιστή, ο οποίος θα είναι αυτάρκης, αποκεντρωμένος και απαλλαγμένος από κάθε είδους λογοκρισία και έλεγχο.

Το Ethereum παρέχει μια αποκεντρωμένη εικονική μηχανή, την Εικονική Μηχανή του Ethereum (Ethereum Virtual Machine - EVM)[75], η οποία μπορεί να εκτελέσει σενάρια χρησιμοποιώντας διεθνές δίκτυο δημόσιων κόμβων. Χαρακτηρίζεται ως Turing Complete πρόγραμμα (εν αντιθέσει με το bitcoin, το οποίο είναι Turing Incomplete), διότι μπορεί να προσαρμοστεί, ώστε να προσομοιώνει την λογική οποιουδήποτε αλγορίθμου, και δεν περιορίζεται

[72] Wikipedia - https://el.wikipedia.org/wiki/Ethereum#cite_note-4

[73] Buterin Vitalik, «So where did the name Ethereum come from?» , 2014

[74] https://www.coindesk.com/markets/2016/06/24/coindesks-ethereum-research-report-now-available/

[75] https://ethereum.org/en/developers/docs/evm/

στην εκτέλεση απλών και προκαθορισμένων εντολών[76]. Η ιδιότητα αυτή του Ethereum το διαφοροποιεί από το Bitcoin στο ότι το Ethereum εκτός από την διανεμημένη αποθήκευση δεδομένων, διενεργεί και την υπολογιστική διαδικασία.

Το Ethereum δομείται σε δημόσιο δίκτυο και καθένας μπορεί να το κατεβάσει ή να συνδεθεί σε αυτό προκειμένου να δημιουργήσει συναλλαγές ή έξυπνα συμβόλαια, να επικυρώσει, να κάνει minining. Περαιτέρω , ως τεχνολογία blockchain , αποτελείται από blocks δεδομένων , τα οποία μπορεί να είναι είτε συναλλαγές είτε έξυπνα συμβόλαια. Τα blocks δημιουργούνται ή εξορύσσονται και διανέμεται αντίγραφο αυτών των συναλλαγών προς επικύρωση από τους υπόλοιπους χρήστες.

Παρότι το Ethereum χρησιμοποιεί και βασίζεται στην τεχνολογία blockchain, παρουσιάζει διαφορές με το Bitcoin. Διαθέτει ένα επίπεδο αφαίρεσης στο οποίο οι συναλλαγές διαφόρων εφαρμογών εφαρμόζονται και τρέχουν στον κώδικα του προγράμματος, το οποίο τρέχει σε όλους τους κόμβους. Όλες αυτές οι διεργασίες , γίνονται με ίδιους πόρους, δηλαδή πόρους του συστήματος. Πιο συγκεκριμένα, οι miners παράγουν Ethers, ώστε το δίκτυο να παραμένει αυτάρκες. Σε αυτό συμβάλλει και ο μηχανισμός τιμολόγησης εσωτερικών συναλλαγών "Gas" που χρησιμοποιείται για να μειώσει τις ανεπιθύμητες συναλλαγές (spam) και να κατανείμει τους πόρους του δικτύου.

Αναφορικά με το Gas και την λειτουργία του, μπορούμε να παραλληλίσουμε με ένα αυτοκίνητο και τα καύσιμα. Πιο συγκεκριμένα, κάθε γραμμή κώδικα που εκτελείται από το δίκτυο απαιτεί συγκεκριμένη ποσότητα Gas. Εάν το Gas εξαντληθεί, τότε σταματάει να εκτελείται ο κώδικας. Η χρησιμότητα και ο τρόπος λειτουργίας του θα αναλυθούν περαιτέρω στην ενότητα Smart Contract.

Το κατανεμημένο καθολικό του Ethereum αποτελείται από αντικείμενα, τους "λογαριασμούς", οι οποίοι αλληλοεπιδρούν μεταξύ τους μέσω μηνυμάτων. Υπάρχουν δύο είδη λογαριασμών: α) ο Externally Owned Account (EOA, ή εξωτερικοί λογαριασμοί) και β) ο Contract Account (άλλως, Λογαριασμός Σύμβασης), ο οποίος σχετίζεται και εξαρτάται από κώδικα [77].

Ειδικότερα, ο EOA έχει μια Ethereum διεύθυνση που ελέγχεται από ιδιωτικό κλειδί και δεν σχετίζεται με κανενός είδος κώδικα. Ο χρήστης μπορεί να ανοίξει πολλούς EOAs χωρίς

[76] Zhang Weijia, Anand Tej, Blockchain and Ethereum Smart Contract Solution Development: Dapp Programming with Solidity, 2022, Scopus

[77] Alharby M., Van Moorsel A., "Blockchain -based smart contracts: A systematic mapping study, 2019

κανένα πρόβλημα. Ο λογαριασμός αυτός μπορεί να δέχεται Ether. Η ιδιαιτερότητα των EOAs είναι ότι μπορούν να δημιουργούν συμβάσεις και ταυτόχρονα να τις ενεργοποιούν. Η δεύτερη κατηγορία λογαριασμών, οι Contract Accounts αυτοελέγχονται , δηλαδή ελέγχονται από δικό τους κώδικα, που περιγράφεται και εκτελείται από την αρχή στα έξυπνα συμβόλαια τους, με την ενσωμάτωση προκαθορισμένων ενεργοποιητών (predefined triggers)[78]. Κάθε συμβόλαιο έχει τον δικό του λογαριασμό, ο οποίος σχετίζεται με μία μοναδική διεύθυνση Ethereum, ωστόσο οι Λογαριασμοί Συμβάσεων δεν έχουν ένα ιδιωτικό κλειδί για να ελέγχονται και να προστατεύονται. Σε κάθε περίπτωση, ο Λογαριασμός Σύμβασης, ομοίως με τον EOA, λαμβάνει Ether και εάν του ζητηθεί, αποστέλλει Ether ή ενεργοποιεί νέους λογαριασμούς (contract accounts). Δέον να λεχθεί, ότι οι λογαριασμοί αυτοί δεν μπορούν να τροποποιηθούν από την στιγμή της ενεργοποίησης και της κοινοποίησης τους στο δίκτυο. Για τον λόγο αυτό, χρήστης- κάτοχος πρέπει να είναι πολύ προσεκτικός στη συγγραφή του κώδικα για το τι θα ορίσει ως ενεργοποιητές και με ποιους όρους θα τρέξει/εκτελεστεί ο λογαριασμός (δηλαδή στο ότι θα ορίσει για έκαστο trigger) [79] [80].

Όπως προαναφέρθηκε, στο Ethereum υπάρχει η δυνατότητα αλληλεπίδρασης των λογαριασμών μέσω μηνυμάτων. Πρόκειται για μηνύματα που περικλείονται μέσα στις συναλλαγές, οι οποίες πληρώνονται με Ether. Επομένως, ενώ το bitcoin χρησιμοποιείται μόνο για τη μεταφορά αξίας ("χρημάτων"), το Ethereum μπορεί να χρησιμοποιηθεί και με άλλους τρόπους, όπως: μεταφορά αξίας (πρόκειται για την πιο απλή συναλλαγή), δημιουργία και ενεργοποίηση ενός έξυπνου συμβολαίου. Η δημιουργία ενός νέου συμβολαίου γίνεται αποστέλλοντας μία νέα συναλλαγή που εσωκλείει τον κώδικα του συμβολαίου. Η ενεργοποίηση του συμβολαίου γίνεται με την αποστολή χρημάτων σε έναν Initial Coin Offering (ICO) λογαριασμό (ICO's contract account address), ο οποίος στη συνέχει επιστρέφει tokens, ως επιβεβαίωση της ενεργοποίησης του συμβολαίου.

[78] Kasireddy Preethi, "How does Ethereum work, anyway?", 2017

[79] Zheng Z., Xie S., Dai H., Chen X., Weng J., Imran M., "An overview on smart contracts: Challenges, advances and platforms". 2020, Science Direct

[80] Bartoletti M., Pompianu L., " An empirical analysis of smart contracts: platforms, applications, and design patterns", 2017, ResearchGate

3.3. Smart Contracts

Η ιστορία των ψηφιακών συμβάσεων (digital contracts) αρχίζει να γράφεται το 1948, όταν η Σοβιετική Ένωση απέκοψε κάθε δίοδο (οδική και σιδηροδρομική) στη δυτική Γερμανία και σε μεγάλο μέρος του Βερολίνου [81]. Η πράξη αυτή πυροδότησε την αντίδραση των ΗΠΑ και λοιπών συμμάχων της Γερμανίας, δημιουργώντας και εκμεταλλευόμενοι την Αερογέφυρα του Βερολίνου, προμηθεύοντας την διηρημένη χώρα με πάνω από 2 εκατομμύρια τόνους τρόφιμα και κάθε είδους άλλες προμήθειες. Στο πλαίσιο αυτό και με σκοπό τον έλεγχο των αποστολών, ο αρχιλοχίας του αμερικανικού στρατού Edward Guilbert , δημιούργησε και οργάνωσε ένα σύστημα δηλώσεων των αποστολών το οποίο μπορούσε να μεταδίδεται με τέλεξ, ραδιο-τηλετυπία και τηλέφωνο (telex, radio-teletype, or telephone)[82]. Όμως, ο τρόπος αυτός δεν αποδείχθηκε ασφαλής, διότι οι καταγραφές από την αερογέφυρα διέρρευσαν στον ιδιωτικό τομέα, μετά την σύγκρουση με την Σοβιετική Ένωση. Με αφορμή την εν λόγω διαρροή, το 1965, ο Guilbert που εργαζόταν στην DuPoint, ανακάλυψε ένα σύστημα ηλεκτρονικής ανταλλαγής δεδομένων, γνωστό και ως EDI (Electronic Data Interchange) αναπτύσσοντας ένα τυποποιημένο σύνολο ηλεκτρονικών μηνυμάτων μεταξύ της DuPont και ενός εκ των μεταφορέων της Chemical Lehman Tank Lines για την αποστολή πληροφοριών έκαστου φορτίου[83]. Η DuPoint κατάφερε με αυτήν την εφεύρεση να στέλνει υπερατλαντικά ναυτιλιακά δηλωτικά ως μηνύματα telex, τα οποία στη συνέχεια μπορούσε να τα μετατρέπει σε χάρτινες ταινίες, ώστε να μπορούν να εισαχθούν στους υπολογιστές της εταιρείας. Τις επόμενες δεκαετίες, η εφεύρεση του Guilbert -τα συστήματα EDI - άρχισε να εφαρμόζεται και σε άλλες εταιρείες, μετατρέποντας τις έγχαρτες συμφωνίες και εντολές επιβεβαίωσης σε ψηφιακές αναπαραστάσεις.

Σήμερα, τα συστήματα EDI έχουν υιοθετηθεί ευρέως από τις επιχειρήσεις, ιδίως για τη διαχείριση και τον έλεγχο πολύπλοκων προμηθευτικών αλυσίδων. Μεγάλες βιομηχανίες (ενδεικτικά: τροφίμων, αυτοκινήτων, ναυτιλίας) στηρίζουν την ανταλλαγή ηλεκτρονικών εντολών αγοράς, τιμολογίων, φορτωτικών, δεδομένων για τα αποθέματα στα συστήματα EDI, ώστε να εξασφαλιστεί η επιχειρησιακή συνέχεια, να εξαλειφθούν χρονοβόρες γραφειοκρατικές διαδικασίες και παράλληλα να μειωθεί το εργατικό κόστος κάθε συναλλαγής. Ωστόσο, οφείλουμε

[81] https://www.defense.gov/News/Feature-Stories/story/Article/3072635/the-berlin-airlift-what-it-was-its-importance-in-the-cold-war/
[82] https://edilibrary.wordpress.com/2016/08/29/father-of-edi-army-master-sargent-edward-a-guilbert/
[83] https://www.edistaffing.com/blog/2015/11/06/electronic-data-interchange-edi-trivia/

να επισημάνουμε ότι τα συστήματα EDI έχουν κάποιους περιορισμούς. Οι ηλεκτρονικές συμβάσεις EDI επαναδιατυπώνουν σε ηλεκτρονική μορφή υφιστάμενους όρους και προϋποθέσεις, αλλάζοντας σε μικρό βαθμό τον τρόπο σύναψης και εκτέλεσης των εμπορικών υποχρεώσεων.

Ο όρος "smart contract" πρωτοεμφανίστηκε τη δεκαετία του 1990 (δηλαδή σχεδόν 20 χρόνια πριν την εμφάνιση του bitcoin) στο άρθρο "Formalizing and Securing Relationships on Public Networks,". Το "smart contract" αποδίδεται στα ελληνικά ως "έξυπνη σύμβαση" ή "έξυπνο συμβόλαιο" και δεν σχετίζεται αμιγώς με την νομική επιστήμη. Ο Nick Szabo, κρυπτογράφος με επιστημονική κατάρτιση στους υπολογιστές και τα νομικά, δημιούργησε αυτόν τον όρο το 1994 [84]. Ο εν λόγω όρος περιγράφει "ένα κωδικοποιημένο υπολογιστικό πρωτόκολλο συναλλαγών, που εκτελεί τους όρους μιας σύμβασης, χωρίς την ύπαρξη κάποιου ενδιάμεσου τρίτου (πχ δικηγόρου, τράπεζας)." Σύμφωνα με τον Szabo, σκοπός ενός smart contract είναι μεταξύ άλλων και η ελαχιστοποίηση των περιστατικών απάτης και αθέτησης των συμβατικών όρων, καθώς επίσης και η μείωση του συναλλακτικού κόστους[85]. Μια από τις πρώτες και πιο διάσημες εφαρμογές που λειτουργεί με τη λογική ενός smart contract θεωρείται ο αυτόματος πωλητής, ο οποίος όμως απέχει πολύ από τις δυνατότητες που έχει σήμερα ένα έξυπνο συμβόλαιο.

Η δημοσίευση του Szabo πυροδότησε το ενδιαφέρον της επιστημονικής κοινότητας και πλήθος ερευνητών, όπως ο Mark Miller, ο Chip Morningstar, και ο Bill Frantz έκαναν προσπάθειες μοντελοποίησης συμβολαίων για δικαιώματα προαίρεσης[86] χρησιμοποιώντας μια αντικειμενοστραφή γλώσσα προγραμματισμού. Περί τα τέλη της δεκαετίας του 1990, τις έρευνες

---

[84] Szczerbowski Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017.

[85] Szabo Nick, "Smart Contracts. Unpublished manuscript", 1994

[86] Το δικαίωμα προαίρεσης συνιστά περιουσιακό και διαπλαστικό δικαίωμα, που λειτουργεί ως εξής: Ο μέτοχος ή τρίτος υπέρ του οποίου το σχετικό δικαίωμα μπορεί, κατ΄αποτέλεσμα, να προβεί, μόνος αυτός, σε αγορά ή πώληση μετοχών.
https://koumentakislaw.gr/arthra/dikaioma-proairesis-sth-metabibash-metohon/#:~:text=%CE%A4%CE%BF%20%CE%B4%CE%B9%CE%BA%CE%B1%CE%AF%CF%89%CE%BC%CE%B1%20%CF%80%CF%81%CE%BF%CE%B1%CE%AF%CF%81%CE%B5%CF%83%CE%B7%CF%82%20%CF%83%CF%85%CE%BD%CE%B9%CF%83%CF%84%CE%AC%2C%20%CE%BA%CE%B1%CF%84,%CF%83%CE%B5%20%CE%B1%CF%80%CF%8C%CE%BA%CF%84%CE%B7%CF%83%CE%B7%20%CE%AE%20%CE%BC%CE%B5%CF%84%CE%B1%CE%B2%CE%AF%CE%B2%CE%B1%CF%83%CE%AE%20%CF%84%CE%BF%CF%85%CF%82.

αυτές διαδέχτηκαν, η Microsoft και οι ερευνητές του Πανεπιστημίου της Γλασκώβης που πειραματίζονταν με τη δημιουργία και την χρήση μηχανογραφημένων χρηματοοικονομικών συμβολαίων. Λίγα χρόνια αργότερα, το 2004, ο χρηματοοικονομικός κρυπτογράφος Ian Grigg εισήγαγε και περιέγραψε ένα συμβόλαιο το οποίο θα διαβάζεται και από μηχανές και από ανθρώπους, το Ricardian Contract (στα ελληνικά αναφέρεται και ως Ρικαρδιανό). Στη συνέχεια, το 2012, ο Harry Surden, καθηγητής νομικής στο Πανεπιστήμιο του Κολοράντο, μελέτησε πώς η αναπαράσταση των συμβατικών υποχρεώσεων, υπό τη μορφή δεδομένων, θα μπορούσε να οδηγήσει στη δημιουργία "υπολογίσιμων" συμβατικών όρων[87].

Ειδικότερα, ένα smart contract είναι ένας υπολογιστικός κώδικας που αποτυπώνει μια ψηφιακή σύμβαση, η οποία δεν εκφράζεται γραπτώς σε ανθρώπινη γλώσσα, εκτελείται σε ένα κατανεμημένο, αποκεντρωμένο, κοινόχρηστο και αναπαραγόμενο λογιστικό βιβλίο (blockchain) και πιστοποιείται με τη χρήση ηλεκτρονικών υπογραφών και κρυπτογραφικών κλειδιών [88]. Ως σύμβαση, δεν νοείται μόνο ένα νομικό κείμενο, αλλά μια συμφωνία μεταξύ δύο ή και περισσοτέρων μερών. Αυτός ο υπολογιστικός κώδικας που περιγράφει τους όρους της συμφωνίας εκτελείται σε περιβάλλον blockchain και όταν πληρωθούν όλοι οι όροι (τα ifs), τότε εκτελείται η εκάστοτε σύμβαση ("τρέχουν" τα then) [89]. Επομένως, βάσει αυτών, μπορεί να εκτελεστεί μια υπηρεσία ή εργασία, σύμφωνα με τα όσα ορίζει ο χρήστης. Ένα έξυπνο συμβόλαιο, ως Turing Complete εφαρμογή, μπορεί να εκτελεί πολύπλοκες συναλλαγές , όπως να εκτελεί υπολογισμούς, να αποθηκεύει πληροφορίες και να στέλνει αυτόματα- με την πλήρωση κάποιων όρων- χρήματα σε άλλους λογαριασμούς. [90] [91] Όπως έχει περιγραφεί: " *μπορούν να εκφράσουν κάθε πιθανό αλγόριθμο, ή με άλλα λόγια μπορούν να προσομοιώσουν τη λειτουργία ενός αφηρημένου καθολικού υπολογιστή*" [92] .

---

[87] https://scholar.law.colorado.edu/faculty-articles/148/

[88] Szczerbowski Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017.

[89] Szabo N., "Formalizing and Securing Relationships on Public Networks", 1997.

[90] AlharbyM, Aldweesh A, van Moorsel A, "Blockchain-based smart contracts: A systematic mapping study of academic research", 2018.

[91] Bashir I., "Mastering Blockchain: Distributed Ledger Technology, decentralization, and smart contracts explained", 2018

[92] Liberti, L. & Marinelli F.. "Mathematical programming: Turing completeness and applications

Τα smart contracts διακρίνονται σε δύο είδη, τα ντετερμινιστικά και μη. Όσον αφορά την εκτέλεση των πρώτων, δεν απαιτείται η άντληση πληροφοριών από κάποιον εξωγενή παράγοντα, ενώ αντίθετα, για την εκτέλεση των μη ντετερμινιστικών smart contracts απαιτείται η παροχή πληροφοριών από τρίτους[93].

Η ολοκλήρωση ενός smart contract απαιτεί κάποιους πόρους προκειμένου να μπορέσει να εκτελεστεί. Μέρος των πόρων αυτών αφορά και την αμοιβή των miners (validators) που θα κάνουν την απαιτούμενη εργασία. Στο Ethereum η διαδικασία αυτή γίνεται με το Gas, μια διαδικασία διαφορετική από αυτή του Bitcoin. Ειδικότερα, για να τρέξει κάθε γραμμή κώδικα απαιτείται να έχει ορισθεί το Gas, κάτι που πρέπει να υπολογιστεί προσεκτικά, διότι δεν υπάρχει δυνατότητα ανεφοδιασμού όταν αρχίσει να εκτελείται η σύμβαση. Εάν το Gas για έκαστο συμβόλαιο είτε δεν έχει υπολογιστεί σωστά είτε έχει γραφτεί λάθος, αυτό θα σταματήσει να εκτελείται με ό,τι συνεπάγεται αυτό. Με αυτόν τον τρόπο παρακινούνται οι προγραμματιστές των smart contracts να διατηρούν τον κώδικα λιτό και - ει δυνατόν- βελτιστοποιημένο, δεδομένου ότι το Gas κοστίζει. Το Gas που δαπανάται, χρησιμοποιείται ως αμοιβή των miners (validators), οι οποίοι επενδύουν υπολογιστική ισχύ προκειμένου να ενημερώσουν το Ledger των συναλλαγών του Ethereum, αντιστοίχως με ό,τι συμβαίνει με το Bitcoin. Δέον να διευκρινιστεί , ότι το Gas δεν είναι κάτι που αποκτάται, αλλά είναι μία μονάδα λογαριασμού, με την οποία μπορεί να καταμετρηθεί η εργασία που απαιτείται για την εκτέλεση μιας γραμμής κώδικα, αντιστοίχως με τις ώρες εργασίας στον πραγματικό κόσμο. Το Gas πληρώνεται σε Ether. Εκ του γεγονότος αυτού, ανακύπτει το ερώτημα γιατί δεν αρκεί το Ether αλλά απαιτείται ένα επιπρόσθετο νόμισμα. Η απάντηση σε αυτό είναι ότι η τιμή του Ether μεταβάλλεται συνεχώς, γεγονός που θα δημιουργούσε ανασφάλεια και συνεχείς ανατιμολογήσεις έκαστου smart contract, εξαιτίας της κυμαινόμενης συναλλαγματικής ισοτιμίας. Με το Gas, η εκτέλεση το ίδιου συμβολαίου κάθε φορά, θα αποφέρει πάντα ένα σταθερό ποσό Gas προς πληρωμή. Επιπλέον, σε ότι αφορά τον υπολογισμό της ενέργειας και του Gas που απαιτείται για να εκτελεστεί κάθε γραμμή κώδικα, υπάρχουν προκαθορισμένες ποσότητες για κάθε ενέργεια που πρέπει να εκτελεστεί στον εκάστοτε κώδικα.

Περαιτέρω, με το Gas παρέχεται μια δικλείδα ασφαλείας του κεφαλαίου. Όταν ο χρήστης στείλει μια συναλλαγή σε Ether, πρέπει επίσης να καθορίσει ένα όριο Gas, δηλαδή πόσο Gas είναι

---

to software analysis" , 2014

[93] Samuel Zaruba Smith, Andy Garcia, "Blockchain Smart Contracts,: Introduction for Accounting and Auditing Professionals", 2022, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/blockchain-smart-contracts-part-1

διατεθειμένος να χρησιμοποιήσει για την εκτέλεση των γραμμών του κώδικά του. Αυτό γίνεται για να τον προστατεύσει από την εξάντληση των κεφαλαίων του σε περίπτωση που ο κώδικάς του έχει κάποιο σφάλμα και εκτελείται ατελείωτα (loops) ή αναποτελεσματικά. Επομένως, και επειδή δεν υπάρχει η δυνατότητα ανατροφοδότησης (refueling), ο χρήστης πληρώνει εκ των προτέρων ολόκληρο το ποσό, προκειμένου να εξασφαλιστεί η εκτέλεση του. Σε περίπτωση που έχει υπολογιστεί μεγαλύτερη αξία από αυτή που πραγματικά χρειάζεται, το πλεόνασμα επιστρέφεται στον χρήστη. Ωστόσο, εάν ένα smart contract δεν μπορέσει να εκτελεστεί εξ ολοκλήρου -ελλείψει Gas- θα σταματήσει η εκτέλεση του και δεν θα επιστραφεί το Gas που χρησιμοποιήθηκε (παρότι δεν ολοκληρώθηκε η εκτέλεση του έξυπνου συμβολαίου). Αυτό μπορεί να συμβεί αν, επί παραδείγματι, το συμβόλαιο πρέπει να εκτελέσει κάποια επαναλαμβανόμενη λειτουργία (loop), η οποία συνεχίζει να καταναλώνει Gas με αποτέλεσμα να εξαντλείται. Περαιτέρω δε, εάν στην απαιτούμενη τιμή του Gas δεν προστεθούν και επιπλέον μονάδες για την εκτέλεση του κώδικα, κανένας miner (validator) δεν θα αναλάβει τη συναλλαγή. Εάν αντίθετα, υπολογιστούν αρκετές μονάδες Gas αλλά πληρωθούν πολύ λίγα για κάθε μονάδα, ενδεχομένως να χρειαστεί πολύς χρόνος για να περάσει η συναλλαγή, αφού οι miners θα δώσουν προτεραιότητα σε συναλλαγές με υψηλότερες πληρωμές.

3.3.1. Εκτέλεση Smart Contract (Oracles)

Οι έξυπνες συμβάσεις ως αυτοεκτελούμενες ¨μελετούν¨ και διαβάζουν κάποιους όρους προκειμένου όταν πληρωθούν να εκτελεστούν. Στις αυτόνομες συμβάσεις, οι ενσωματωμένοι όροι που κωδικοποιούνται και αποτυπώνονται σε αντίστοιχη γλώσσα προγραμματισμού τερματίζονται πιο δύσκολα σε σχέση με εκείνους που αποτυπώνονται σε φυσική γλώσσα σε μια "παραδοσιακή" νομική συμφωνία, δεδομένου ότι κανένα μέρος δεν ελέγχει την αλυσίδα block. Σε αυτό διαφαίνεται ένας πιθανός κίνδυνος να μην σταματήσει η εκτέλεση μιας έξυπνης σύμβασης αφού ενεργοποιηθεί από τα σχετικά μέρη (με τον τρόπο που περιεγράφη ως άνω).

Με την εκκίνηση της διαδικασίας της ενεργοποίησης του έξυπνου συμβολαίου, εκτελούνται οι ενσωματωμένοι όροι και δεν σταματά η εκτέλεση τους (loop), εάν τα μέρη δεν έχουν προβλέψει γι αυτό. Περαιτέρω δε, το πλεονέκτημα των έξυπνων συμβάσεων είναι η δυνατότητα αναπροσαρμογής στις παρούσες συνθήκες κάθε φόρα με την ενσωμάτωση μιας ενδιάμεσης-αξιόπιστης πηγής τρίτου μέρους- που συνήθους ονομάζεται oracle. Oracle, σημαίνει χρησμός/μαντείο και πράττει αυτό που περιγράφεται από την ερμηνεία του ονόματος, δηλαδή

αποθηκεύει και μεταδίδει πληροφορίες από το εξωτερικό περιβάλλον, οι οποίες επηρεάζουν το εκάστοτε έξυπνο συμβόλαιο. Τα oracles μπορεί να είναι προγράμματα και σπανιότερα κάποιο φυσικό πρόσωπο, που αντλούν πληροφορίες και δεδομένα από το εξωτερικό περιβάλλον προκειμένου να αναπροσαρμοστεί η έξυπνη σύμβαση σύμφωνα με τα προβλεφθέντα[94]. Για παράδειγμα, τα oracles ελέγχουν -ενδεικτικά-τις τιμές της αγοράς, την εξωτερική θερμοκρασία ή την πιθανότητα βροχής μέσω αισθητήρων ή οτιδήποτε άλλο κρίνεται ουσιώδες για την εκτέλεση έκαστου έξυπνου συμβολαίου, προκειμένου να αλληλεπιδρούν με πρόσωπα του πραγματικού κόσμου και ενδεχομένως να αντιδρούν σε εξωτερικά γεγονότα. Τα oracles έχουν χαρακτηριστεί ως πάροχοι πληροφοριών λόγω του ότι χρησιμοποιούνται για την βεβαίωση γεγονότων του εξωτερικού περιβάλλοντος[95].

Περαιτέρω, τα oracles αναγνωρίζουν δεδομένα από ιδιωτικά συστήματα επίλυσης διαφορών ή συστήματα διαιτησίας[96]. Δέον να λεχθεί ότι τα oracles είναι ικανά να μεταφέρουν και ερμηνεύσουν γνώσεις των ανθρώπων, ώστε να προσαρμοστεί αναλόγως η έξυπνη σύμβαση. Επιπροσθέτως, η όποια μεταβολή αναγνωρίζεται από τα oracles σε σχεδόν πραγματικό χρόνο, με αποτέλεσμα η "προσαρμογή" των smart contracts να είναι τάχιστη και τα μέρη να προχωρούν στις απαραίτητες αλλαγές (όπως για παράδειγμα αλλαγή υποχρεώσεων και δικαιωμάτων, τροποποίηση ροής πληρωμών). Περαιτέρω δε, πρέπει να επισημανθεί ότι τα oracles έχουν τη δυνατότητα να επικαιροποιούν ή να προσδιορίζουν τις συνθήκες προκειμένου να προσαρμόσουν τις υποχρεώσεις έκαστου μέρου σύμφωνα με τη βούληση και την κρίση των μερών. Κατά αυτόν τον τρόπο, τα μέρη αποκτούν μεγαλύτερη εμπιστοσύνη στο σύστημα και στην αντικειμενική εκτέλεση της σύμβασης, διότι βασίζονται και εμπιστεύονται τον ντετερμινιστικό[97] τρόπο εκτέλεσης των έξυπνων συμβολαίων για κάθε αντικειμενικό όρο που μπορεί εύκολα να μεταφραστεί σε κώδικα. Επιπρόσθετα, μπορεί να δημιουργηθούν oracles βασισμένα σε ανθρώπους και όχι σε εξωτερικές

---

[94] Beniiche Abdeljalil. "A Study of Blockchain Oracles", 2020

[95] Primavera De Filippi, Aaron Wright, "Blockchain and the Law", p.73-75, 2018, Harvard University Press

[96] Ortolani P., "Self- Enforcing Online Dispute Resolution: Lesson from Bitcoin", 2016, Oxford Journal

[97] Η αιτιοκρατία (ντετερμινισμός) (determinism) είναι η φιλοσοφική τάση που επηρέασε ιδιαιτέρως την επιστημονική σκέψη από την αρχαιότητα μέχρι και σήμερα. Αποδέχεται την ύπαρξη της αιτιότητας, την καθολική αιτιώδη και νομοτελειακή συνάφεια όλων των φαινομένων. Πρόκειται λοιπόν γιαι την φιλοσοφική πίστη ότι κάθε γεγονός ή δράση είναι το αναπόφευκτο αποτέλεσμα προηγούμενων γεγονότων και δράσεων. Έτσι τουλάχιστον κατ' αρχήν κάθε γεγονός ή δράση μπορεί να προβλεφθεί πλήρως εκ
των προτέρων ή αναδρομικά.

πηγές, τα οποία θα αξιολογούν όρους και συμφωνίες που δεν μπορούν να κωδικοποιηθούν εύκολα, ώστε να εκτελεστούν από το έξυπνο συμβόλαιο κι αυτό γιατί ο όρος ενδέχεται να είναι είτε υποκειμενικός είτε διφορούμενος και να χρήζει ερμηνείας με συνθήκες πραγματικού κόσμου.

Σύμφωνα με τα προλεχθέντα, προκύπτει ότι τα έξυπνα συμβόλαια πρέπει να συνδεθούν με ορισμένα oracles, ώστε να ενημερωθούν για την οποιαδήποτε αλλαγή και να εκτελεστούν αναλόγως. Τα έξυπνα συμβόλαια, ως προγράμματα που φέρουν ορισμένους όρους εκτελούνται με την πιστοποίηση αυτών. Γεγονότα όπως η παρέλευση της δήλης ημέρας, η πλήρωση μια αίρεσης, ο θάνατος του κληρονομουμένου, η ματαίωση πτήσης, η μεταβολή της θερμοκρασίας σε ορισμένο τόπο ή μηχάνημα, οι τιμές του χρηματιστηρίου καθώς και όποια άλλη σημαντική παράμετρος για το συμβόλαιο, μπορεί να ερμηνευθεί από τα oracles, ώστε εάν οι χρήστες την αξιολογήσουν ως αληθή και ακριβή, να ενημερωθεί στη συνέχεια το έξυπνο συμβόλαιο. Δέον να επισημανθεί ότι απαιτείται η συναίνεση όλων των χρηστών για την εγκυρότητα της πληροφορίας των oracles. Ωστόσο, γεννάται ο προβληματισμός περί παρέμβασης τρίτου μέρους-ακόμα και αξιόπιστου- διότι αλλοιώνεται η δομή το blockchain. Το ισχυρό πλεονέκτημα του blockchain είναι ότι είναι απαλλαγμένο από οποιαδήποτε Αρχή ή κάποια κεντρικά ελεγχόμενη πηγή. Όμως, ο τρόπος λειτουργίας των oracles απαιτούν την παρέμβαση ενός τρίτου μέρους, είτε της Κεντρικής Τράπεζας, είτε της Εθνικής Μετεωρολογικής Υπηρεσίας, είτε του εκάστοτε Υπουργείου. Επιπρόσθετα, εάν για την διατήρηση της ταυτότητας του blockchain ως κατανεμημένου λογιστικού ελεγχόμενο από τους χρήστες , οι πληροφορίες προέρχονται από πολλές ετερογενείς και αποκεντρωμένες πηγές, θα ανακύψει σοβαρό πρόβλημα αξιοπιστίας καθώς και σύγκρουση των χρηστών κάτι που θα δυσχεράνει την εκτέλεση της σύμβασης αλλά θα κλονίσει και την εμπιστοσύνη των μερών. Για το πρόβλημα αυτό έχει προταθεί η δημιουργία ενός αποκεντρωμένου συστήματος εμπιστοσύνης για τον συνεχή έλεγχο των oracles. Πρόκειται για ομάδες προγραμματιστών, μηχανικών λογισμικού καθώς και εμπορικές εταιρείες oracles, οι οποίοι ακολουθούν το σκεπτικό και τη δομή του blockchain, αναπτύσσοντας αποκεντρωμένους ιδιωτικούς οργανισμούς για την παροχή όλων των εξωτερικών πληροφοριών[98]. Εταιρίες όπως οι Oracle Cloud, Chainlink, Augur και Reality Keys συγκεντρώνουν, αντιπαραβάλλουν και αφομοιώνουν εξωτερικές πληροφορίες από πολλές και ποικίλες πηγές του εξωτερικού κόσμου. Η συλλογή των πληροφοριών θα γίνεται από αισθητήρες (θερμοκρασία, υγρασία κ.α.), ανιχνευτές,

[98] https://cryptoslate.com/cryptos/oracle/

συσκευές IoT που διασυνδέονται με τον εξωτερικό κόσμο και λαμβάνουν πληθώρα ερεθισμάτων, παρόχους πληροφοριών και webAPI (διεπαφές ιστού). Ωστόσο και σε αυτή την πρόταση, το πρόβλημα δεν επιλύεται, διότι οι εταιρείες που παρέχουν την περιγραφείσα υπηρεσία ενδέχεται να προβούν σε δόλιες ενέργειες ή να επιδείξουν μεροληψία υπέρ ενός συγκεκριμένου μέρους. Επομένως, η ανησυχία περί αντικειμενικότητας και ουδετερότητας των oracles παραμένει, κάτι το οποίο υπονομεύει την ανάπτυξη και επέκταση των έξυπνων νομικών συμβάσεων και την ένταξη τους σε πολλές συναλλαγές.

3.3.2. Χαρακτηριστικά, δομή και λειτουργία ενός smart contract

Ένα έξυπνο συμβόλαιο, όπως έχει προαναφερθεί, είναι αυτο-επαληθεύσιμο, αυτο-εκτελούμενο και ανθεκτικό σε παραβιάσεις. Χαρακτηρίζεται δε από i) ακρίβεια, ii) αυτονομία, iii) ασφάλεια, iv) οικονομία και v) εμπιστοσύνη, λόγω του συγκερασμού όλων αυτών, η εφαρμογή αυτή θεωρήθηκε "έξυπνη" . Πιο αναλυτικά[99]:

I. ακρίβεια: Η αυτόματη σύνταξη των υπολογιστικών κωδίκων ξεπερνά και αντιμετωπίζει την όποια ανακρίβεια.
II. αυτονομία: Η σύμβαση εκτελείται από το ίδιο το δίκτυο και τους ενδιαφερόμενους χρήστες και δεν απαιτείται η επέμβαση αξιόπιστων τρίτων.
III. ασφάλεια: Κάθε κόμβος του blockchain αποκτά αντίγραφο των συναλλαγών και των δεδομένων.
IV. οικονομία: Ελλείψει των αξιόπιστων τρίτων, το συναλλακτικό κόστος μειώνεται σημαντικά.
V. εμπιστοσύνη: Τα δεδομένα και οι συναλλαγές κρυπτογραφούνται, με αποτέλεσμα οι πιθανότητες απώλειας και παραβίασης να μειώνονται σημαντικά.

Τα δομικά στοιχεία ενός smart contract είναι τα ακόλουθα[100]:

[99] Shubhani Aggarwal, Neeraj Kumar, "Blockchain 2.0: Smart Contracts", 2020
[100] Mohanta B. K., Panda S. S, Jena D., "An overview of smart contract and use cases in blockchain technology", 2018

I. Address (διεύθυνση)[101], η οποία είναι ένα κράμα από την διεύθυνση του αποστολέα και από τη διεύθυνση του παραλήπτη της εκάστοτε συναλλαγής
II. Value (αξία), αποτελεί το αντικείμενο της εκάστοτε συναλλαγής (δηλαδή την αξία που μεταφέρεται κάθε φορά)
III. State (κατάσταση), σε αυτή διαφαίνονται τα δεδομένα που διαμορφώνουν εκάστοτε έξυπνο συμβόλαιο
IV. Variables (μεταβλητές), απεικονίζει τις μεταβλητές των ως άνω στοιχείων ενός smart contract και αποτυπώνονται στην αντίστοιχη γλώσσα προγραμματισμού.

Η δημιουργία και η λειτουργία ενός smart contract[102]:

Σε πρώτο επίπεδο, λαμβάνουν χώρα οι διαπραγματεύσεις μεταξύ των μερών αναφορικά με τις υποχρεώσεις, τους περιορισμούς και τα δικαιώματα που θα απορρέουν από την έξυπνη σύμβαση. Επομένως, πρόκειται για τη μεταφορά μιας συμφωνίας σε υπολογιστικό κώδικα. Πιο συγκεκριμένα, οι τυχόν ρήτρες, οι όροι και κάθε άλλο δομικό στοιχείο μεταφράζονται σε κώδικα ανάλογα με τις απαιτήσεις κάθε γλώσσας προγραμματισμού. Κατ΄ουσίαν πρόκειται για ένα σύνολο "if…then", το οποίο μεταφράζεται αναλόγως.

Λαμβάνοντας υπ΄οψιν ότι σε ένα έξυπνο συμβόλαιο μπορούν να αποθηκευτούν περιουσιακά στοιχεία σε ψηφιακή μορφή, τα μέρη επιλέγουν ποια στοιχεία θα αποτελέσουν αντικείμενο της επικείμενης σύμβασης. Σε αυτό το στάδιο, ακολουθεί ο έλεγχος εγκυρότητας προκειμένου να αποθηκευτεί στο blockchain, εάν και εφόσον εγκριθεί. Αξιοσημείωτο είναι πώς τα περιουσιακά στοιχεία παραμένουν ασφαλή, δεδομένου ότι μέχρι την ολοκλήρωση της σύμβασης, παραμένουν κλειδωμένα.

Στο τρίτο στάδιο, λαμβάνει χώρα η εκτέλεση του smart contract. Εάν συντρέξει έστω και ένας όρος από τους περιγραφόμενους στην σύμβαση, θα ενεργοποιηθεί η διαδικασία για την πλήρη εκτέλεση του. Εφόσον λοιπόν, έχει διενεργηθεί ο αυτόματος έλεγχος των προϋποθέσεων και των συμβατικών όρων, το smart contract εκτελείται αυτόματα και κατά συνέπεια επικυρώνεται και ενημερώνεται η κατάσταση των μερών.

[101] Jakub J. Szczerbowski, "Place of smart contracts in civil law. A few comments on form and interpretation", 2018, SSRN
[102] Smith S. S., "Blockchain, Smart Contracts and Financial Audit Implications", 2020

Στο τέταρτο και τελευταίο στάδιο, ολοκληρώνεται η έξυπνη σύμβαση και αποθηκεύεται σε περιβάλλον blockchain. Κατά συνέπεια, τα ψηφιακά περιουσιακά στοιχεία ξεκλειδώνουν και διανέμονται αναλόγως στα μέρη. Πλέον, και μετά τη διανομή των περιουσιακών στοιχείων, η συναλλαγή θεωρείται ολοκληρωμένη και μη αναστρέψιμη[103].

3.4. Smart Legal Contracts

Ένα έξυπνο συμβόλαιο είναι ένας υπολογιστικός κώδικας που λειτουργεί ως μέρος μιας αλυσίδας block και μπορεί να εκτελέσει τους όρους ενός συμβολαίου ή μιας συμφωνίας όταν πληρούνται προκαθορισμένες προϋποθέσεις. Μια έξυπνη σύμβαση μπορεί να αποτελεί μέρος μιας δεσμευτικής νομικής σύμβασης. Μπορεί επίσης να μην έχει καμία σχέση με ένα τέτοιο συμβόλαιο. Δέον να κριθεί εάν ένα έξυπνο συμβόλαιο προσιδιάζει στον αυστηρό και τεχνικό ορισμό ενός νομικού συμβολαίου. Μέχρι σήμερα, έχει επικρατήσει η χρήση του smart contract ως συμφωνία και όχι ως δέσμευση στον νομικό κόσμο. Ωστόσο, η ταχεία εξοικείωση της κοινωνίας καθώς και η πολλά υποσχόμενη εν λόγω τεχνολογία, τείνει να οδηγήσει στην δημιουργία εφαρμογών και με νομική χροιά.

Σύμφωνα, με τα προλεχθέντα οι έξυπνες συμβάσεις μπορούν να αποτελέσουν τη βάση για μια συμφωνία που γίνεται μεταξύ μερών που ενδέχεται να είναι άγνωστα μεταξύ τους και η οποία εκτελείται μόνο με τους κωδικοποιημένους όρους. Ο κώδικας ενός smart contract μπορεί να περιέχει τόσες προϋποθέσεις όσες είναι απαραίτητες για την εκτέλεση και ολοκλήρωση μια συγκεκριμένης συναλλαγής. Έτσι, μπορεί να σχεδιαστεί ένα έξυπνο συμβόλαιο ομοίωμα νομικού συμβολαίου, στο οποίο , το ανώνυμο άτομο Α μπορεί να καταθέσει κρυπτονόμισμα στο πορτοφόλι του ανώνυμου ατόμου Β ως πληρωμή μιας υπηρεσίας ή ενός αγαθού. Σε αυτή την περίπτωση, το έξυπνο συμβόλαιο εκτελεί τη συναλλαγή εφόσον πληρούνται όλοι οι όροι της συμφωνίας. Εάν δεν πληρούνται, ο κώδικας του προγράμματος τερματίζει τη συναλλαγή, με τις συνέπειες που αναφέρθηκαν σε προηγούμενη ενότητα (βλ. Gas).

[103] Zheng Z., Xie S., Dai H., Chen X., Weng J., Imran M., "An overview on smart contracts: Challenges, advances and platforms". 2020, Science Direct

Επομένως, δυνητικά, ένα έξυπνο νομικό συμβόλαιο θα μπορούσε να ικανοποιεί όλες τις νομικές απαιτήσεις για μια δεσμευτική νομική συμφωνία - σύμβαση. Στη Μεγάλη Βρετανία, η Νομική Επιτροπή[104] διεξήγαγε μια εκτενή μελέτη για την τεχνολογία blockchain και για τον τρόπο με τον οποίο θα πρέπει να την αντιμετωπίσουν οι εκάστοτε εθνικοί νόμοι. Μεταξύ άλλων ευρημάτων, στην έκθεση[105] καταγράφεται ότι μια έξυπνη νομική σύμβαση μπορεί να εμφανιστεί με τρεις μορφές: πρώτον, "μπορεί να έχει τη μορφή μιας συμφωνίας σε φυσική γλώσσα με αυτοματοποιημένη εκτέλεση μέσω κώδικα. Δεύτερον, μια έξυπνη νομική σύμβαση μπορεί να είναι γραμμένη αποκλειστικά σε κώδικα (και να εκτελείται από αυτόν). Τρίτον, και μεταξύ αυτών των δύο μορφών, μια έξυπνη νομική σύμβαση μπορεί να λάβει τη μορφή μιας υβριδικής σύμβασης, όπου ορισμένες συμβατικές υποχρεώσεις περιέχονται σε όρους φυσικής γλώσσας και άλλες καταγράφονται σε κώδικα".

Οι έξυπνες νομικές συμβάσεις αποτελούν μια από τις πρώτες σημαντικές εξελίξεις, με τις οποίες οι παραδοσιακές συμβάσεις θα μπορούσαν να αυτοματοποιηθούν ψηφιακά, δίνοντας τη δυνατότητα στους χρήστες να εγγυηθούν ένα άμεσο αποτέλεσμα με ελάχιστη ανθρώπινη συμβολή. Στο πλαίσιο αυτό και σε μία συνεχή προσπάθεια του νομικού κόσμου να προσαρμοστεί και να ακολουθήσει τις τεχνολογικές εξελίξεις, γίνονται συνεχώς έρευνες και μελέτες για το πώς τα smart contracts θα αποκτήσουν και νομικό χαρακτήρα. Χαρακτηριστικό παράδειγμα, η Νομική Επιτροπή της Μεγάλης Βρετανίας δημοσίευσε την εκτενή έκθεσή της, Smart Legal Contracts [106]: Advice to Government, η οποία καλύπτει τις βασικές αρχές της τεχνολογίας και διερευνά τον τρόπο με τον οποίο χρησιμοποιούνται οι έξυπνες νομικές συμβάσεις. Η έκθεση – όπως προαναφέρθηκε- χρησιμεύει επίσης ως ένα καλό εισαγωγικό σημείωμα σχετικά με τις τεχνολογίες blockchain και τα κατανεμημένα βιβλία. Στις Ηνωμένες Πολιτείες, δύο μεγάλες νομικές ενώσεις, η Επιτροπή Ενιαίου Δικαίου (The Uniform Law Commission) και το Αμερικανικό Ινστιτούτο Δικαίου (The American Law Institute), συγκρότησαν μια επιτροπή για τη μελέτη του Ενιαίου Εμπορικού Κώδικα και των Τεχνολογιών Κατανεμημένων Βιβλίων. Η Επιτροπή Ενιαίου

[104] We published our advice to Government on 25 November 2021, concluding that the current legal framework in England and Wales is clearly able to facilitate and support the use of smart legal contracts. https://www.lawcom.gov.uk/project/smart-contracts/

[105] https://www.lawcom.gov.uk/project/smart-contracts/ /// https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final.pdf

[106] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf

Εμπορικού Κώδικα και Αναδυόμενων Τεχνολογιών (The Uniform Commercial Code and Emerging Technologies Committee)[107] επεξεργάζεται τη δική της έκθεση σχετικά με την εναρμόνιση του Νόμου και αυτής της νέας τεχνολογίας.

Κρίνεται σκόπιμο, πριν την νομική ανάλυση αυτής της πολλά υποσχόμενης τεχνολογίας των smart legal contracts, να γίνει μνεία στα πλεονεκτήματα και τα μειονεκτήματα τους. Οι έξυπνες νομικές συμβάσεις υπόσχονται: 1) ταχύτητα και αποτελεσματικότητα στην εκτέλεση της σύμβασης. Με την πλήρωση μιας προϋπόθεσης, οι όροι της σύμβασης θα εκτελούνται αμελλητί, χωρίς αναμονή και καθυστέρηση για την αναγκαία παρέμβαση τρίτου μέρους. Με την απομάκρυνση από την παραδοσιακή διαδικασία σύναψης συμβάσεων και την επιλογή μιας πιο αποτελεσματικής ροής εργασιών (όπως οι έξυπνες συμβάσεις) οι νομικοί-δικηγόροι αλλά και οι πολίτες μπορούν να εξοικονομήσουν πολύτιμο χρόνο και πόρους που μπορούν να επενδύσουν αλλού. Περαιτέρω, η τεχνολογία αυτή μπορεί να εγγυηθεί: 2) μεγάλη ακρίβεια, κάτι που την καθιστά αξιόπιστη. Δεδομένου ότι οι έξυπνες συμβάσεις απαιτούν υψηλό βαθμό λεπτομέρειας στο πλαίσιο της κωδικοποίησης των συμβολαίων τους, οι όροι και οι προϋποθέσεις τους θα πρέπει φυσικά να καταγράφονται με ρητό και περιεκτικό τρόπο. Αυτό οφείλεται στο γεγονός ότι ακόμη και η παραμικρή παράλειψη μπορεί να οδηγήσει σε μια κακώς εκτελούμενη σύμβαση ή σε μια σύμβαση που δεν εκτελείται καθόλου. Ωστόσο, από την άλλη πλευρά, τυχόν παραλείψεις ή λάθη μπορεί να είναι δυνητικά καταστροφικά, καθώς τυχόν ατυχίες ή αστοχίες θα μπορούσαν να οδηγήσουν σε δαπανηρά σφάλματα στις συναλλαγές. Επιπλέον, 3) και καθοριστικό πλεονέκτημα των έξυπνων συμβάσεων αποτελεί η ασφάλεια. Πιο συγκεκριμένα, τα αρχεία των συναλλαγών είναι κρυπτογραφημένα, γεγονός που καθιστά απίστευτα δύσκολη την παραβίαση/παραποίηση και τη χειραγώγησή τους[108].

Ωστόσο, δεν θα μπορούσαν να λείπουν τα μειονεκτήματα από τις έξυπνες συμβάσεις. Στην πραγματικότητα, υπάρχουν πολλά προβλήματα που δημιουργεί η συγκεκριμένη τεχνολογία στον νομικό κόσμο.

Πρώτον, η τεχνολογία τους είναι λιγότερο προσιτή για τα συμβαλλόμενα μέρη. Πιο συγκεκριμένα, οι έξυπνες νομικές συμβάσεις έγιναν δημοφιλείς για τα χαρακτηριστικά τους που αποτρέπουν την παραποίηση, αυξάνουν τη διαφάνεια και προστατεύουν τις συναλλαγές και τους

[107] https://www.jdsupra.com/legalnews/the-ucc-and-emerging-technologies-8250345/

[108] Kosba A., Miller A., Shi E., Wen Z., Papamanthoy C., "Hawk: The Blockchain Model of Cryptography and Privacy Preserving Smart Contracts", 2016, IEEE

συναλλασσόμενους από την απάτη. Ωστόσο, με τον τρόπο αυτό, οι έξυπνες συμβάσεις μπορούν να στερήσουν την πιο ανθρώπινη πτυχή των συμβάσεων που είναι κύριο γνώρισμα μιας κοινωνίας αλλά και ένας βασικός λόγος για τις νομικές διαφορές που ανακύπτουν μεταξύ των μερών της. Εν τοις πράγμασι, ο αλγόριθμος δεν μπορεί να αντιληφθεί την ανθρώπινη φύση και την αλληλεπίδραση της κοινωνίας κατά συνέπεια ενδεχομένως να μην μπορεί να επιλύσει τις ανθρώπινες νομικές διαφορές. Όμως, από την άλλη πλευρά, τα νομικά έγγραφα πολλές φορές είναι δυσνόητα για τα μέρη κατά συνέπεια η ενσωμάτωση ψηφιακών μέσων, όπως οι οπτικές διεπαφές, στις έξυπνες συμβάσεις και η παράλληλη αφαίρεση της νομικής διαλέκτου, ενδεχομένως να καθιστούσαν τις συμβάσεις επιτυχημένες και πιο κατανοητές. Ωστόσο, τα έξυπνα συμβόλαια φαίνεται να υιοθετούν μια εντελώς διαφορετική προσέγγιση στον σχεδιασμό των συμβάσεων, καθώς οι χρήστες των συμβάσεων θα πρέπει πλέον να κατανοούν γλώσσες προγραμματισμού για να κατανοήσουν και να έχουν πρόσβαση στις συμβάσεις, κάτι που ανατρέπει το επιχείρημα περί ευχρηστίας των έξυπνων συμβάσεων.

Ένα δεύτερο μειονέκτημα είναι ότι οι έξυπνες συμβάσεις δεν έχουν την ευελιξία που απαιτεί μια κοινωνία, δεν υπάρχουν περιθώρια για ασάφειες, για αλλαγές, πολλώ δε μάλλον για λάθη. Δεν προσφέρεται η δυνατότητα διαπραγματεύσεων, κάτι που είναι απαραίτητο στη διαμόρφωση μιας νομικής σχέσης ή επίλυση μιας νομικής διαφοράς. Η έλλειψη ευελιξίας καθιστά τα έξυπνα συμβόλαια αρκετά “αποσυνδεδεμένα” από τον πραγματικό κόσμο και τα εξωτερικά γεγονότα, παρά τον μεγάλο αντίκτυπο που μπορούν να έχουν στην διαμόρφωση των σχέσεων και των συναλλαγών.

Τρίτον, τα λάθη μπορεί να αποδειχθούν δαπανηρά. Ο νομικός κόσμος γνωρίζει ήδη αρκετούς από τους κινδύνους που συνδέονται με μια κακογραμμένη και κακοδιατυπωμένη σύμβαση. Από τα κενά που υπάρχουν μέχρι την ανεπαρκή νομική προστασία, κάθε λάθος στο πλαίσιο της διαδικασίας σύνταξης της σύμβασης μπορεί να αποδειχθεί δαπανηρό για την όποια συναλλαγή μεταξύ των μερών. Δυστυχώς, οι έξυπνες συμβάσεις επιτείνουν αυτό το πρόβλημα λόγω του αμετάβλητου χαρακτήρα τους, γεγονός που καθιστά το όποιο λάθος μόνιμο και πιθανόν ανεπίλυτο.

Σε αυτό το σημείο, ενδιαφέρον παρουσιάζει ότι οι έξυπνες συμβάσεις μοιάζουν περισσότερο με επιχειρηματικούς κανόνες παρά με συμβατικές νομικές συμβάσεις. Αυτό οφείλεται στο γεγονός ότι σε βασικό επίπεδο, οι έξυπνες συμβάσεις αυτοματοποιούν τις επιχειρηματικές συναλλαγές και δεν επενδύουν χρόνο στη συζήτηση των ρόλων, των καθηκόντων

και των ευθυνών κάθε μέρους, καθώς και της ευθύνης που αναλαμβάνουν σε περίπτωση που δεν τις εκπληρώσουν.

Στο ίδιο πλαίσιο, μια έξυπνη νομική σύμβαση εκτελεί αυτόματα τους επιχειρηματικούς κανόνες, σε αντίθεση με τις παραδοσιακές συμβάσεις που περιλαμβάνουν περίπλοκες και λεπτομερείς ρήτρες που προσφέρουν προστασία σε περίπτωση που προκύψουν πολύπλοκα νομικά ζητήματα. Οι έξυπνες συμβάσεις επικεντρώνονται αποκλειστικά στην επίτευξη απλών αποτελεσμάτων, ενώ άλλες συμβάσεις σχεδιάζονται για να προσφέρουν καθοδήγηση σε περίπτωση που αυτά τα αποτελέσματα δεν καρποφορήσουν. Παρ΄όλα αυτά, η ομάδα εργασίας για ζητήματα Νομικής Πληροφορικής της Κυβέρνησης του Ηνωμένου Βασιλείου (The LawTech Delivery Panel Legal) θεωρεί πώς « ένα έξυπνο συμβόλαιο (που χαρακτηρίζεται από την αυτοματοποίηση) είναι ικανό να έχει συμβατική ισχύ, ακόμη και εάν οι προϋποθέσεις για να έχει εκτελεστότητα θα εξαρτηθούν σε μία δεδομένη στιγμή από τα λόγια και τη συμπεριφορά των μερών [109].»

3.4.1. Έλεγχος πλήρωσης κριτηρίων νομικής σύμβασης

Σε αυτό το σημείο χρήζει περαιτέρω διερεύνησης η νομική φύση των έξυπνων συμβολαίων. Στις προηγούμενες ενότητες αναφέρθηκε και ως "σύμβαση¨, οπότε σε αυτό το σημείο οφείλουμε να εξετάσουμε, εάν πρόκειται για σύμβαση με τη νομική έννοια ή εάν πρόκειται για ένα νέο νομικό μόρφωμα.

Με γνώμονα τον ορισμό της σύμβασης, θα γίνει μια προσπάθεια προσέγγισης των ποικίλων ερωτημάτων που προβληματίζουν τον νομικό κόσμο. Ο όρος "σύμβαση" φέρει πολλές σημασίες. Ενδέχεται να αφορά στην πράξη σύναψης μιας συμφωνίας, η οποία συνεπάγεται την αμοιβαία δέσμευση των συμβαλλομένων μερών. Επίσης, ενδέχεται να αναφέρεται στο κείμενο-περιεχόμενο μιας συμφωνίας , από το οποίο απορρέουν υποχρεώσεις και δικαιώματα για τα μέρη. Τέλος, ως σύμβαση μπορεί να νοηθεί το έγγραφο μιας συμφωνίας, στο οποίο αποτυπώνονται οι

[109] https://lawtechuk.io/insights/cryptoasset-and-smart-contract-statement

όροι αυτής. [110] Ωστόσο, στον νομικό κόσμο, η έννοια της σύμβασης έχει πιο αυστηρά όρια και είναι πιο σαφής. Σύμφωνα με τον νομικό ορισμό, "σύμβαση είναι η συμφωνία μεταξύ των μερών (δύο ή περισσότερων), η οποία δημιουργεί αντίστοιχες δεσμεύσεις στα συμβαλλόμενα μέρη." Ειδικότερα, πρόκειται για μια δικαιοπραξία , απόρροια της σύμπτωσης βουλήσεων δύο ή περισσότερων προσώπων (φυσικών ή νομικών) αναφορικά με το επιδιωκόμενο αποτέλεσμα [111]. Οι συμβάσεις διακρίνονται σε ετεροβαρείς και αμφοτεροβαρείς, ωστόσο στην παρούσα εργασία θα εξετάσουμε τις αμφοτεροβαρείς, διότι μόνο από αυτές-κατά το σύνηθες- μπορεί να προκύψει η όποια νομική διαμάχη.

Σε κάθε δικαιοπραξία, εν προκειμένω στη σύμβαση, απαραίτητο στοιχείο αποτελεί η σύμπτωση δύο ή περισσότερων δηλώσεων βουλήσεως. Η δήλωση βούλησης πρέπει να είναι απευθυντέα (ΑΚ 167), προκειμένου να συναφθεί μια σύμβαση. Σύμφωνα με τα όσα ορίζει το ΑΚ 167, δεν αρκεί η εξωτερίκευση της δικαιοπρακτικής βούλησης, αλλά απαιτείται επιπροσθέτως να περιέλθει στην σφαίρα επιρροής και του άλλου μέρους, προκειμένου να λάβει γνώση. Επιπλέον, σύμφωνα με την Αρχή του Ατύπου των Δικαιοπραξιών , ο τύπος δεν είναι απαραίτητο στοιχείο μιας σύμβασης και μπορεί να καθοριστεί ελεύθερα από τα μέρη, ελλείψει κάποιου κανόνα αναγκαστικού δικαίου (ΑΚ 158 επ.) [112]. Η διαδικασία αυτή μετουσιώνεται στο σχήμα της "πρότασης - αποδοχής" (ΑΚ 185 επ.), και νοείται ως " η μονομερής δήλωση βούλησης, η οποία απευθύνεται προς ένα πρόσωπο (φυσικό ή νομικό) με σκοπό τη σύναψη σύμβασης". Η πρόταση-προσφορά πρέπει να είναι πλήρης και ορισμένη κατά περιεχόμενο και να απευθύνεται σε πρόσωπο ορισμένο ή έστω οριστό [113]. Επομένως, υπάρχει η ευχέρεια να απευθύνεται σε πρόσωπο αόριστο, με μόνη επιφύλαξη ότι θα μπορεί να προσδιοριστεί κατά το χρόνο της αποδοχής. Ως αποδοχή νοείται η μονομερής δήλωση βουλήσεως του αποδέκτη της εκάστοτε πρότασης, μέσω της οποίας εκφράζεται η συναίνεση- συγκατάθεση με την πρόταση και κατά συνέπεια με τη σύναψη της εκάστοτε σύμβασης. Σε αυτό το σημείο, αξίζει να επισημανθεί πώς η πρόταση αυτή καθ΄αυτή δεν παράγει το επιδιωκόμενο αποτέλεσμα, αλλά μόνο σε συνάρτηση με την αποδοχή.

---

[110] Lauslahti K. , Mattila J., Seppala T., "Smart contacts - How will blockchain technology affect contractual practices?"

[111] Παπαστερίου Δ., Κλαβανίδου Δ., "Δίκαιο της Δικαιοπραξίας" 2008

[112] Γεωργιάδης Α, Γενικές Αρχές Αστικού Δικαίου, 2019

[113] Παπαστερίου Δ., Κλαβανίδου Δ., "Δίκαιο της Δικαιοπραξίας" 2008

Έπειτα από μία σύντομη αναφορά κάποιων χαρακτηριστικών μιας νομικής σύμβασης, θα γίνει μια απόπειρα ένταξης των έξυπνων συμβάσεων στον νομικό κόσμο, προκειμένου να διαπιστωθεί, εάν μπορούν να χαρακτηριστούν συμβάσεις υπό το πρίσμα του δικαίου ή όχι, καθώς και ποια προβλήματα ενδεχομένως ανακύπτουν από τον χαρακτηρισμό αυτό.

Ξεκινώντας από την κατάρτιση μιας έξυπνης σύμβασης οφείλουμε να εξετάσουμε την ύπαρξη της ικανότητας δικαίου, δηλαδή οι εκάστοτε δηλώσεις βουλήσεως να αντιστοιχίζονται με ένα πρόσωπο. Στις έξυπνες συμβάσεις αυτό γίνεται με την αντιστοίχιση ενός λογαριασμού χρήστη με ένα πρόσωπο. Επομένως, δεδομένου ότι ο λογαριασμός χρήστη αντιστοιχεί σε ένα ορισμένο πρόσωπο, τότε πληρούται η προϋπόθεση ύπαρξης ικανότητας δικαίου και μπορεί να γίνει λόγος για σύμβαση, σύμφωνα με τις γενικές αρχές αστικού δικαίου.

Προβληματισμός γεννάται σε αυτό το σημείο για το εάν η τεχνολογία blockchain, μέσω της οποίας δημιουργούνται οι έξυπνες συμβάσεις, διαχειρίζεται από φυσικά πρόσωπα ή από αλγορίθμους. Εάν υπάρχει η πιθανότητα, τα έξυπνα συμβόλαια να μην συνάπτονται μεταξύ φυσικών προσώπων, ανακύπτει ζήτημα περί ικανότητας δικαίου. Για παράδειγμα, σε περίπτωση αμφισβήτησης ικανότητας δικαιοπραξίας, θα ανακύψει ζήτημα κατά την αποδεικτική διαδικασία στο πλαίσιο διερεύνησης και αναζήτησης της ταυτότητας του προσώπου, κι αυτό γιατί η ανωνυμία και ψευδωνυμοποίηση στα έξυπνα συμβόλαια δυσχεραίνει την ταυτοποίηση των χρηστών, παρά την μοναδική χρήση των κρυπτογραφικών - ταυτοποιητικών κλειδιών. Συνεχίζοντας, ακολουθεί η εξέταση του σχήματος πρότασης - αποδοχής, το οποίο φαίνεται να ακολουθείται και στα έξυπνα συμβόλαια. Ειδικότερα, το ένα μέρος εκφράζει τη βούλησή του για κατάρτιση σύμβασης δημιουργώντας μια έξυπνη σύμβαση και μεταφορτώνοντας την σε ένα δίκτυο blockchain, και σε συνέχεια αυτών το άλλο μέρος εκφράζει τη βούλησή του για αποδοχή της πρότασης και κατ΄επέκταση σύναψη της σύμβασης με την υπογραφή της μέσω των αντιστοίχων κρυπτογραφικών κλειδιών καθώς και την κατάθεση των αντίστοιχων περιουσιακών στοιχείων στο blockchain προκειμένου να ολοκληρωθεί η σύμβαση. Παρατηρείται λοιπόν, πως υπάρχει μια αντιστοιχία και αναλογία στο σύστημα πρότασης- αποδοχής στον πραγματικό αλλά και στον blockchain κόσμο. Ωστόσο, παρά την αναλογία αυτή, εντοπίζεται μια διαφορά ως προς τον χρόνο περιέλευσης της δήλωσης βούλησης στον αντισυμβαλλόμενο συγκριτικά με τον παραδοσιακό τρόπο σύναψης συμβάσεων. Εν προκειμένω, αναφορικά με τον χρόνο σύναψης των έξυπνων

συμβάσεων δεν υπάρχει κάποιος περιορισμός εξαιτίας των αυτοματοποιημένων διαδικασιών. Ωστόσο, διαφαίνεται πώς δεν υπάρχει ρητή διατύπωση αποδοχής, γεγονός που οδηγεί σε σιωπηρώς καταρτιζόμενες συμβάσεις. Όμως, ειδικότερα και σε ό,τι αφορά τον χρόνο, ενδιαφέρον παρουσιάζει η διερεύνηση του πότε και εάν υπάρχει σύμπτωση των δηλώσεων βουλήσεως των αντισυμβαλλομένων. Το ζήτημα αυτό επιλύεται με την χρήση των κρυπτογραφικών κλειδιών, τα οποία μαρτυρούν τον χρόνο πρόθεσης των μερών να συμβληθούν, θέτοντας την υπογραφή τους στο έξυπνο συμβόλαιο. Εν αντιθέσει με τον χρόνο, δυσκολία έως και αδυναμία απόδειξης προκύπτει ως προς την πρόθεση τους να δεσμευτούν με ορισμένες συμβατικές ρήτρες που καθορίζονται μονομερώς και ex ante από το μέρος που δημιουργεί το έξυπνο συμβόλαιο [114]. Κατά αναλογία, η "υποχρεωτική" αυτή προσχώρηση σε κάποιους όρους του έξυπνου συμβολαίου, θα μπορούσε με τον τρόπο που αντιμετωπίζονται οι ΓΟΣ στη σύναψη συμβάσεων στον φυσικό κόσμο. Λαμβάνοντας υπ΄όψιν όλα τα ως άνω, μπορούν να χαρακτηριστούν οι έξυπνες συμβάσεις ως συμβόλαια.

Όσον αφορά τον τύπο, όπως προαναφέρθηκε, αυτός δεν αποτελεί υποχρεωτικό συστατικό στοιχείο μιας σύμβασης εκτός εάν αυτό απαιτείται ρητά από το νόμο. Περαιτέρω δε, κανόνα αποτελεί η ελεύθερη διαμόρφωση του τύπου από τα μέρη, εφόσον αυτό δεν απαιτείται από ρητή διάταξη νόμου αναγκαστικού δικαίου. Επομένως, στις περιπτώσεις που ο Έλληνας νομοθέτης απαιτεί έγγραφο τύπο για την εγκυρότητα μιας σύμβασης, τότε αυτή δεν θα μπορούσε να θεωρηθεί έγκυρη με τη μορφή μιας έξυπνης σύμβασης. Παρά ταύτα, δεδομένου ότι στην Ελλάδα ισχύει το Άτυπο των Δικαιοπραξιών, και η φύση των έξυπνων συμβάσεων προσιδιάζει στις σιωπηρώς καταρτιζόμενες συμβάσεις, θεωρητικά θα μπορούσαν να εφαρμοστούν για την πώληση κινητών πραγμάτων με όλες τις δέουσες συνέπειες, δηλαδή να θεωρούνται έγκυρες και να δεσμεύουν τα μέρη.

Ωστόσο, γεννάται ο προβληματισμός εάν πράγματι μια έξυπνη σύμβαση που υπογράφεται με κρυπτογραφικά κλειδιά μπορεί να θεωρείται έγκυρη και ισάξια με τις συμβάσεις στον φυσικό κόσμο. Η εξέλιξη της τεχνολογίας καθώς και οι ποικίλοι τρόποι συναλλαγών καλλιεργούν το έδαφος και για την αποδοχή των έξυπνων νομικών συμβάσεων. Χαρακτηριστικό παράδειγμα αποτελεί η ψηφιακή υπογραφή (η οποία θα αναλυθεί σε επόμενη ενότητα) και η αναγνώριση της

[114] Werbach K., Cornell N., "Contracts ex machina", 2017

ως αξιόπιστη και έγκυρη για την ολοκλήρωση ηλεκτρονικών συναλλαγών. Στο πλαίσιο αυτό προτείνεται η αναλογική προσέγγιση των κρυπτογραφικών κλειδιών με την ψηφιακή υπογραφή.

Ένα ακόμη ζήτημα, άμεσα συνυφασμένο με τις συμβάσεις και την ανθρώπινη φύση που τις διέπει είναι αυτό της τροποποίησης ή της ακύρωσης. Ο παραδοσιακός τρόπος σύναψης συμβάσεων επιτρέπει στα μέρη να προβλέψουν αυτές τις περιπτώσεις ή ακόμα και εάν δεν έχουν προβλεφθεί, δίνεται η δυνατότητα σε ορισμένες περιπτώσεις με διαμεσολάβηση να επιλυθεί το εν λόγω ζήτημα με τις αντίστοιχες συνέπειες. Τα μέρη ενδέχεται να διαπιστώσουν ότι η αρχική συμφωνία δεν τα εξυπηρετεί και να συναποφασίσουν να την τροποποιήσουν, λαμβάνοντας υπ΄όψιν τα νέα δεδομένα. Σε περίπτωση λοιπόν κοινής βούλησης των αντισυμβαλλομένων για τροποποίηση της σύμβασης, ο νόμος παρέχει ορισμένες δυνατότητες προς αυτήν την κατεύθυνση. Αντιστοίχως, ο νόμος προβλέπει και περιπτώσεις ακύρωσης, προκειμένου να διαφυλάξει και να προστατεύσει το θιγόμενο μέρος. Χαρακτηριστικό παράδειγμα ακύρωσης αποτελεί το τρίπτυχο πλάνη-απάτη-απειλή (ΑΚ 140 επ) [115], το οποίο διόλου σπάνιο είναι. Η τροποποίηση και η ακύρωση λοιπόν, είναι εφικτές στα παραδοσιακά συμβόλαια, παρότι κάποιες φορές μπορεί να πρόκειται για δύσκολη διαδικασία. Οι επιλογές αυτές μοιάζουν ανέφικτες στα έξυπνα συμβόλαια λόγω, ακριβώς αυτών που υπόσχονται ως πλεονεκτήματα, ήτοι της αδιάβλητης και της μόνιμης καταγραφής. Η μόνη δυνατότητα που υπάρχει σήμερα, είναι η δημιουργία ενός νέου έξυπνου συμβολαίου, φαινομενικά τροποποιητικού, διότι δεν θα καταργεί καθώς ούτε θα απενεργοποιεί το ήδη αναρτημένο αρχικό έξυπνο συμβόλαιο.

Επομένως, όπως διαφαίνεται από τα παραπάνω, τα έξυπνα συμβόλαια ενώ δεν είναι ανεκτικά σε αοριστίες και πιθανόν προβαίνουν σε πολλές προβλέψεις, από την άλλη, περιορίζουν τα μέρη στερώντας τους την δυνατότητα υπαναχώρησης, ακύρωσης ή και τροποποίησης λόγω απρόοπτης μεταβολής συνθηκών (ΑΚ 388 επ). Περαιτέρω δε, δεν νοείται η επιδίκαση αποζημίωσης, εάν αυτό δεν έχει προβλεφθεί σαφώς και ρητώς από την σύνταξη του αρχικού έξυπνου συμβολαίου.

Ωστόσο, σε καμμία περίπτωση, δεν θα επιτρεπόταν, η αρχιτεκτονική του blockchain και κατ΄επέκταση των smart contracts να σταθεί τροχοπέδη στην ροή των συναλλαγών. Για τον λόγο αυτό, δίνονται ορισμένες δυνατότητες για τον χειρισμό και την αντιμετώπιση των προαναφερθέντων συμβάντων στα έξυπνα συμβόλαια. Αρχικά, τα μέρη μπορούν να εντάξουν

[115] Γεωργιάδης Α., Γενικές Αρχές Αστικού Δικαίου, 2019

στον κώδικα του συμβολαίου μια διαδικασία πληρωμής αποζημίωσης σε περίπτωση αποτυχίας της εκάστοτε έξυπνης σύμβασης καθώς και τη δυνατότητα επιστροφής χρημάτων, αναλόγως το συμβάν και τις απαιτήσεις των περιστάσεων. Έπειτα, στις περιπτώσεις που δεν είναι εφικτό να συμπεριληφθούν στον κώδικα και κυρίως να προβλεφθούν όλες οι περιπτώσεις που απαιτούν τροποποίηση ή ακύρωση της σύμβασης, τότε τα μέρη μπορούν να ακολουθήσουν την δικαστική οδό για την επίλυση της όποιας διαφοράς ανακύπτει. Βέβαια, και σε αυτή την εναλλακτική υπάρχουν δυσκολίες, όπως ο εντοπισμός των μερών, η απόδειξη ύπαρξης ή μη βούλησης καθώς και ζητήματα δικαιοδοσίας, εάν δεν έχουν ρυθμιστεί από τα μέρη.

Συμπερασματικά και αναλογιζόμενοι τα ως άνω (ικανότητα δικαίου, σχήμα πρότασης-αποδοχής, δυνατότητα τροποποίησης και ακύρωσης), παρά τα προβλήματα που εξετέθησαν, οι έξυπνες συμβάσεις πληρούν τις απαιτήσεις που θέτει ο Αστικός Κώδικας, προκειμένου να θεωρηθούν νομικές συμβάσεις, αντίστοιχες με αυτές που υπάρχουν στον φυσικό κόσμο. Ωστόσο, καθίσταται εύληπτο το γεγονός πως οι έξυπνες συμβάσεις είναι τεχνολογικά και νομικά ανώριμες ακόμα, δεδομένου ότι δεν μπορούν να ανταποκριθούν επαρκώς σε μια πολύπλοκη σχέση καθώς και δεν μπορούν και να ικανοποιήσουν θεμελιώδεις αρχές του αστικού δικαίου.

3.4.2. Είδη Smart Legal Contracts

Ο εφευρέτης του Ethereum, Vitalik Buterin, ανέφερε το 2018 στο Twitter, ότι ο όρος Smart Contract δημιούργησε διεθνώς σύγχυση με την νομική ορολογία και γι αυτό το λόγο θα προτιμούσε να μην χρησιμοποιήσει την ορολογία του Szabo, αλλά αντί αυτού να είχε χρησιμοποιήσει τον «αδιάφορο» τεχνικό όρο “Persistent Scripts” (επίμονα σενάρια)[116]. Για τον λόγο αυτό και για την καλύτερη θεώρηση και κατανόηση του ζητήματος, λαμβάνοντας ως κριτήριο την έκφραση των συμβατικών όρων σε φυσική γλώσσα καθώς και υπολογιστικό κώδικα, τα έξυπνα συμβόλαια κατανέμονται σε τρεις επιμέρους κατηγορίες[117]:

[116] https://twitter.com/VitalikButerin/status/1051160932699770882

[117] Smart Legal Contracts: Summary - Law Commission United Kingdom

3.4.3.Α. Νομική Σύμβαση με εξωτερικό κώδικα

Πρόκειται για μια κατηγορία που περιλαμβάνει τις τυπικές νομικές συμβάσεις, οι οποίες καταγράφονται και μεταφράζονται σε κώδικα μόνο στο τελικό στάδιο της εκτέλεσης. Πιο συγκεκριμένα, η διατύπωση των όρων γίνεται σε φυσική νομική γλώσσα, ενώ η εκτέλεση αυτών συμβαίνει σε προγραμματιστικό πλαίσιο και γλώσσα κώδικα. Εν προκειμένω, ο κώδικας κατέχει ένα επικουρικό ρόλο στο στάδιο που εκτελείται η σύμβαση, χωρίς να μεταβάλει ή να διεισδύει στις νομικές συμφωνίες. Οι εν λόγω συμφωνίες βασίζονται στο εμπορικό, αστικό ή διοικητικό δίκαιο και φέρουν όλα αυτά τα στοιχεία που καθιστούν μια συμφωνία νομικά δεσμευτική. Σε αυτές τις συμβάσεις περιέχονται συμβατικές ρήτρες περί δικαιωμάτων και υποχρεώσεων, υπαναχώρησης, ανωτέρας βίας, εγγυήσεων. Παράδειγμα μια σύμβασης αυτού του είδους αποτελεί ένας δημόσιος μειοδοτικός διαγωνισμός, για τον οποίο αποθηκεύονται σε μια πλατφόρμα blockchain το είδος, η ποσότητα, η υπηρεσία, οι τιμές, τα κριτήρια επιλογής προμηθειών, ο τρόπος υποβολής ενστάσεων καθώς και οποιοδήποτε άλλο στοιχείο κρίνεται απαραίτητο για την σύναψη της σύμβασης. Η αξιολόγηση των προσφορών καθώς και των συνοδευτικών εγγράφων και προσφορών γίνεται από μια επιτροπή που συστήνεται έπειτα από καθορισμένη και διαφανή διαδικασία για τον εκάστοτε και τρέχοντα διαγωνισμό. Σε επόμενο στάδιο, και εφόσον πληρούνται οι προϋποθέσεις, η επιτροπή θα βαθμολογεί τον κάθε φάκελο βάσει ορισμένων κριτηρίων και με προκαθορισμένους συντελεστές, ώστε να επιτυγχάνεται ακρίβεια και ίση μεταχείριση και διαχείριση των φακέλων. Εν συνεχεία, ο υπολογισμός και η τελική κατάταξη θα γίνεται από τον κώδικα, ο οποίος και θα ανακηρύσσει τον μειοδότη.

Το παρόν μόρφωμα θα μπορούσε να χρησιμοποιηθεί και σε άλλου είδους συμβάσεις, όπως συμβάσεις δανείου, πρόσληψης σε εργασία και ενοικίασης ακινήτου, διότι ο κώδικας αναλαμβάνει μόνο το τελευταίο στάδιο και εφόσον στα προηγούμενα υπάρχει έντονο το στοιχείο της παραδοσιακής νομικής πρακτικής. Για τον λόγο αυτό, δεν γεννάται πρόβλημα ερμηνείας και απόδοσης ρόλων στον υπολογιστή και τον κώδικα.

3.4.3.Β. Υβριδική νομική σύμβαση με εσωτερικό κώδικα

Σε αυτή την κατηγορία ανήκουν οι συμβάσεις που οι όροι τους έχουν συνταχθεί κατά ένα μέρος σε φυσική νομική γλώσσα και κατά ένα άλλο μέρος σε κώδικα. Επομένως, γίνεται λόγος

για μεικτές συμβάσεις, οι οποίες χαρακτηρίζονται ως υβριδικές έξυπνες συμβάσεις[118]. Χαρακτηριστικό παράδειγμα αυτού του είδους της σύμβασης αποτελούν τα RICARDIAN Contracts (Ρικαρδιανά Συμβόλαια όπως λέγονται στα ελληνικά), τα οποία αναπτύχθηκαν για χρηματοοικονομικές συναλλαγές [119]. Σε νομική φυσική γλώσσα καταγράφονται το αντικείμενο της σύμβασης, οι τιμές, ο χρόνος παράδοσης- και κάθε τι άλλο που ορίζεται από το δίκαιο ως βασικό χαρακτηριστικό της εκάστοτε σύμβασης. Σε γλώσσα κώδικα καταγράφονται το ύψος και ο αριθμός τυχόν δόσεων, το κυμαινόμενο επιτόκιο, τα ποσοστά των εκπτώσεων επί του όγκου των αγορών και κάθε τι άλλο που δεν αποτελεί θεμέλιο γνώρισμα μιας σύμβασης κατά τον νόμο, αλλά αποτελεί επιπρόσθετη συμφωνία των μερών.

Η παρούσα σύμβαση διαφέρει από την προαναφερθείσα (ενότητα Α- Νομική Σύμβαση με εξωτερικό κώδικα) στο ότι στην υβριδική σύμβαση η νομική σύμβαση εσωκλείει και εμπεριέχει το λογισμικό και τον κώδικα που περιγράφουν τους λοιπούς όρους για να ολοκληρωθεί η σύμβαση, οι οποίοι είναι αμοιβαία δεσμευτικοί. Οι εν λόγω όροι, λόγω της ισότητας τους με τους αμιγώς νομικούς καθώς και λόγω της ανάγκης προς ενσωμάτωση ως κώδικας στο νομικό κείμενο, ονομάζονται "εσωτερικοί".

3.4.3.Γ. Έξυπνη Σύμβαση χωρίς συμβατικό κείμενο- Code is Law

Στην παρούσα κατηγορία εντάσσονται οι έξυπνες συμβάσεις που είναι αμιγώς τεχνικές και δεν έχουν καθόλου νομικό κείμενο. Πρόκειται για συμβάσεις με ένα πεπερασμένο σύνολο τεχνικών οδηγιών σε γλώσσα προγραμματισμού αναγνώσιμη από το Ethereum (Solidity- γλώσσα προγραμματισμού). Η Solidity εμπεριέχει περί τις 150 εντολές[120] προσαρμοσμένες και κατάλληλες για τα έξυπνα συμβόλαια. Πρόκειται για μια γλώσσα προγραμματισμού που ως θεμέλιο χρησιμοποίησε την Javascript και μεταγλωτίζεται σε byte προκειμένου να είναι κατανοητή από την EVM[121]. Η Solidity προσφέρεται ως γλώσσα για την υποστήριξη και την εκτέλεση διαφόρων ειδών έξυπνων συμβάσεων, μερικές εκ των οποίων ενδέχεται να είναι

[118] Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP,An Introduction to Smart Contracts and Their Potential and Inherent Limitations 2018 https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

[119] Geroni D., "What Are Ricardian Contracts? A Comprehensive Guide", 2021 https://101blockchains.com/ricardian-contracts/

[120] https://docs.soliditylang.org/en/v0.8.13/solidity-by-example.html#blind-auction

[121] Solidity: El lenguaje de programación de los Contratos Inteligentes - Cardaniers https://cardaniers.com/solidity/

αδιάφορες για το δίκαιο (ηλεκτρονική ψηφοφορία, μίσθωση ακινήτου, έξυπνα δίκτυα διαχείρισης κυκλοφορίας, έξυπνα δίκτυα φροντίδας καλλιεργήσιμων χωραφιών).

Η κατηγορία αυτή, εκ πρώτης μοιάζει αδιάφορη για το δίκαιο και τον νόμο, ωστόσο η εκτέλεση του τεχνικού κώδικα ενδέχεται να βασίζεται σε μία νομική συμφωνία και να αυτοματοποιεί την εκτέλεση της (πχ μίσθωση ακινήτου με συμφωνία μεταφοράς ποσού στο πορτοφόλι του εκμισθωτή). Η εκτέλεση του κώδικα αυτού ενδέχεται να έχει ως έρεισμα την εκάστοτε νομική συμφωνία, η οποία μπορεί να αποδειχθεί με μάρτυρες και έγγραφα. Το μόρφωμα αυτό μπορεί να εφαρμοστεί σε κάθε είδος σύμβασης (δωρεά, δάνειο, διανομή κερδών μεταξύ εταίρων μιας εμπορικής εταιρείας, καταβολή μισθώματος για την βραχυπρόθεσμη ή μακροπρόθεσμη εκμίσθωση ακινήτου ή οχήματος). Ωστόσο, στο συγκεκριμένο μόρφωμα σύμβασης ενδέχεται να μην υπάρχει κάποιο γραπτό νομικά δεσμευτικό έγγραφο, κάτι που σε περίπτωση αντιπαράθεσης, θα δυσχεράνει το έργο του δικαστή. Η απουσία νομικής έγγραφης συμφωνίας δημιουργεί ασάφειες και οδηγεί σε αοριστία και κατ΄επέκταση σε αδυναμία γραμματικής, ιστορικής, τελολογικής ερμηνείας. Περαιτέρω δε, η απουσία ή αδυναμία σύνδεσης των έξυπνων συμβάσεων με αλγορίθμους μηχανικής μάθησης (ML-Machine Learning) καθώς και συστήματα Τεχνητής Νοημοσύνης (AI- Artificial Intelligence) δυσχεραίνει την έρευνα για το μερίδιο ευθύνης εκάστου μέρους, προκειμένου να προβεί σε απόδοση ευθυνών και επιβολή καταβολής αντίστοιχης (της ευθύνης) αποζημίωσης.

Επομένως, το εν λόγω μόρφωμα σύμβασης (δηλαδή η νομική συμφωνία εκφρασμένη αποκλειστικά σε κώδικα) με τις παρούσες συνθήκες, γεννά πολλά ερμηνευτικά προβλήματα, τα οποία στο μέλλον με την προσθήκη και την ανάμειξη των τεχνολογιών της Μηχανικής Μάθησης (ML), της Τεχνητής Νοημοσύνης (AI) και των Δεδομένων Μεγάλης Κλίμακας (Big Data) θα μειωθούν σημαντικά ή ακόμα και θα εξαλειφθούν.

3.5. Smart Legal Contracts και Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ ή General Data Protection Regulation GDPR 2016/679) κατέστη δεσμευτικός τον Μάιο του 2018 [122]. Νομοθετικό έρεισμα αποτελεί η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Ο στόχος του ΓΚΠΔ είναι ουσιαστικά διττός. Αφενός, επιδιώκει να διευκολύνει την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των διαφόρων χωρών και μελών της ΕΕ. Αφετέρου, θεσπίζει ένα πλαίσιο προστασίας των θεμελιωδών δικαιωμάτων, με βάση το δικαίωμα στην προστασία των δεδομένων του άρθρου 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων.

Ο ΓΚΠΔ και οι έξυπνες νομικές συμβάσεις βρίσκονται αντιμέτωπες αμφότερες με ζητήματα που σχετίζονται με την προστασία των δεδομένων και την ιδιωτική ζωή, αλλά υπό διαφορετικό πρίσμα.

Ο ΓΚΠΔ είναι ένας κανονισμός που ορίζει συγκεκριμένους κανόνες και απαιτήσεις για τους οργανισμούς καθώς και για κάθε πρόσωπο (φυσικό ή νομικό) που χειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ. Σκοπός του ΓΚΠΔ είναι να προσφέρει μεγαλύτερη ασφάλεια στα υποκείμενα των δεδομένων για την προστασία και τον έλεγχο της ιδιωτικής τους σφαίρας. Παρέχει στα άτομα μεγαλύτερο έλεγχο των προσωπικών τους δεδομένων και θέτει ορισμένες προϋποθέσεις προκειμένου έκαστο ενδιαφερόμενο μέρος να προβεί σε συλλογή και επεξεργασία προσωπικών δεδομένων. Περαιτέρω δε, πέρα από τις υποχρεώσεις και τους περιορισμούς που θέτει στους υπεύθυνους την επεξεργασία και στους εκτελούντες την επεξεργασία, παρέχει στα υποκείμενα των δεδομένων (φυσικά πρόσωπα μόνο) ορισμένα δικαιώματα προς διασφάλιση και προάσπιση των προσωπικών τους δεδομένων και εν γένει της ιδιωτικής τους σφαίρας (ο ΓΚΠΔ παρέχει: το δικαίωμα ενημέρωσης και διαφάνειας (12-14 ΓΚΠΔ), δικαίωμα πρόσβασης (15 ΓΚΠΔ), διόρθωσης (16 ΓΚΠΔ), διαγραφής (17 ΓΚΠΔ), το δικαίωμα περιορισμού της επεξεργασίας (18 ΓΚΠΔ), το δικαίωμα στη φορητότητα των δεδομένων (20 ΓΚΠΔ), το δικαίωμα

[122] https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpikon_dedomenon
Ειδικότερα, ο ΓΚΠΔ τέθηκε σε εφαρμογή από τις 25-5-2018, σύμφωνα με το άρθρο 99 παρ. 2 αυτού. Σύμφωνα με το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), ο ΓΚΠΔ έχει άμεση εφαρμογή σε όλα τα κράτη μέλη, τα οποία υποχρεούνται να λάβουν τα αναγκαία μέτρα για την προσαρμογή της εθνικής νομοθεσίας τους.
Με τον ν. 4624/2019 (ΦΕΚ Α΄137), ορίζονται μέτρα εφαρμογής του ΓΚΠΔ και ενσωματώνεται στην εθνική νομοθεσία η Οδηγία (ΕΕ) 2016/680. Ο ν. 2472/1997 καταργήθηκε, εκτός των διατάξεων που αναφέρονται ρητά στο άρθρο 84 του ν. 4624/2019.

εναντίωσης (21 ΓΚΠΔ), δικαίωμα στη μη αυτοματοποιημένη ατομική λήψη αποφάσεων - κατάρτιση προφίλ (22 ΓΚΠΔ) των προσωπικών τους δεδομένων)

Οι έξυπνες νομικές συμβάσεις, από την άλλη πλευρά, είναι αυτοεκτελούμενες συμβάσεις που είναι γραμμένες σε κώδικα και συχνά συνδέονται με την τεχνολογία blockchain. Αυτοματοποιούν την εκτέλεση μιας σύμβασης βάσει προκαθορισμένων κανόνων και προϋποθέσεων και μπορούν να χρησιμοποιηθούν σε διάφορους κλάδους, όπως η χρηματοδότηση, η ακίνητη περιουσία, η διαχείριση της εφοδιαστικής αλυσίδας καθώς και ποικίλες άλλες ενέργειες και πράξεις που διενεργούν οι πολίτες (πχ μίσθωση ακινήτου, μίσθωση αυτοκινήτου).

Η σχέση μεταξύ του ΓΚΠΔ, της προστασίας της ιδιωτικής ζωής και των έξυπνων νομικών συμβάσεων δομείται στο ότι οι έξυπνες συμβάσεις ενδεχομένως να μπορούν να χρησιμοποιηθούν ως μέσο για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ, δημιουργώντας ένα αυτοματοποιημένο, απαραβίαστο και διαφανές αρχείο των δραστηριοτήτων επεξεργασίας δεδομένων. Επιπρόσθετα, στις έξυπνες νομικές συμβάσεις (ή ακόμα και τις τεχνολογικές συμβάσεις με νομικές πτυχές) αναγράφονται προσωπικά δεδομένα των εμπλεκόμενων μερών και ταυτόχρονα δημιουργείται μέρος της ταυτότητάς τους (στοιχεία ταυτότητας, λόγος συναλλαγής, αιτία αντιδικίας). Επομένως, η καινοτομία καθώς και όλα τα οφέλη των έξυπνων συμβάσεων δεν αναιρούν την ανάγκη συμμόρφωσης με τον ΓΚΠΔ ή άλλους σχετικούς νόμους περί προστασίας της ιδιωτικής ζωής. Σημειώνεται δε, πως εξακολουθεί να είναι ευθύνη των οργανισμών που χρησιμοποιούν έξυπνες συμβάσεις να διασφαλίζουν ότι συμμορφώνονται με όλους τους ισχύοντες κανονισμούς. Επιπλέον, οι έξυπνες συμβάσεις μπορούν να χρησιμοποιηθούν για την προστασία της ιδιωτικής ζωής, επιτρέποντας στα μέρη να συνάπτουν συμφωνίες και να διενεργούν συναλλαγές χωρίς να αποκαλύπτουν πληροφορίες ταυτοποίησης.

Για το λόγο αυτό, στην συγκεκριμένη ενότητα θα προσπαθήσουμε να θίξουμε τα διάφορα ζητήματα και σημεία τόσο σύγκρουσης όσο και σύγκλισης των έξυπνων νομικών συμβάσεων και του ΓΚΠΔ.

3.5.1. Ιδιωτική Ζωή και Προσωπικά Δεδομένα

Σύμφωνα με τα ανωτέρω και εξετάζοντας το ζήτημα ειδικότερα, το δικαίωμα στην ιδιωτική ζωή προστατεύεται με πληθώρα νομοθετημάτων διεθνώς (άρθρο 9 § 1 του ελληνικού Συντάγματος, στο άρθρο 8§1 της ΕΣΔΑ). Ωστόσο, οφείλουμε να επισημάνουμε η προστασία της ιδιωτικής ζωής δεν ταυτίζεται με την προστασία των προσωπικών δεδομένων, παρά το γεγονός

ότι αναδεικνύει μια πολύ σημαντική πτυχή της ιδιωτικότητας του ατόμου, την πληροφοριακή ιδιωτικότητα. Πρόκειται για μια θέση που έχει υιοθετηθεί από το ΔΕΚ στην υπόθεση Österreichischer Rundfunk[123] και η οποία ανάγει την προστασία των προσωπικών δεδομένων σε δικαίωμα του ατόμου. Πιο συγκεκριμένα ανάγεται στον έλεγχο των πληροφοριών που αφορούν πτυχές της ιδιωτικής και προσωπικής του ζωής, με την έννοια ενός πεδίου προστατευμένου από τις παρεμβάσεις του κράτους, της κοινωνίας και λοιπών φυσικών προσώπων. Η ιδιωτική ζωή είναι μια πολυσύνθετη έννοια που δεν μπορεί να περιοριστεί στο πλαίσιο ενός ορισμού, αν και τα όρια της, τα χαρακτηριστικά της καθώς και η έκταση της είναι διακριτά αλλά και συνεχώς προσαρμόσιμα και διευρυμένα, προς προάσπιση του ατόμου. Σύμφωνα με τον Koops[124], υπάρχουν ενδεχομένως εννέα "ιδανικοί τύποι ιδιωτικότητας": σωματική, διανοητική, χωροταξική, του αποφασίζειν, επικοινωνιακή, συνειρμική, ιδιοκτησιακή, συμπεριφορική και πληροφοριακή ιδιωτικότητα. Η τελευταία συνδέεται με το νομοθετικό πλαίσιο για τα προσωπικά δεδομένα και τα όσα ορίζονται και προστατεύονται από τον ΓΚΠΔ.

Σε αυτό το σημείο και δεδομένου του αντικειμένου αυτής της εργασίας, αξίζει να επισημανθεί ότι η IP Address (Internet Protocol) [125] είναι προσωπικό δεδομένο διότι μπορεί να οδηγήσει έμμεσα στην ταυτοποίηση του φυσικού προσώπου. Πιο συγκεκριμένα, στην υπόθεση Patrick Breyer κατά της Ομοσπονδιακής Δημοκρατίας της Γερμανίας (C-582/14), ο Γενικός Εισαγγελέας θεωρεί ότι οι δυναμικές διευθύνσεις IP εντάσσονται στον όρο «προσωπικά δεδομένα» του άρθρου 2, στοιχείο α της Οδηγίας 95/46/ΕΚ, εφόσον ο πάροχος πρόσβασης (ISP) κατέχει πρόσθετες πληροφορίες που επιτρέπουν την εξακρίβωση της ταυτότητας ενός ατόμου. *«Η δυναμική διεύθυνση IP πρέπει να χαρακτηρισθεί, ως προς τον φορέα παροχής υπηρεσιών διαδικτύου, δεδομένο προσωπικού χαρακτήρα λαμβανομένης υπόψη της υπάρξεως τρίτου (του φορέα παροχής προσβάσεως στο διαδίκτυο) στον οποίο μπορεί εύλογα αυτός να απευθυνθεί για να*

---

[123] Συλλογή Νομολογίας – Δικαστήριο Ευρωπαϊκής Ένωσης (ΔΕΕ) - 2001-2018
"Σεβασμός της Ιδιωτικής και Οικογενειακής Ζωής (Άρθρο 7 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης) & Προστασία Προσωπικών Δεδομένων (Άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης)"
https://www.homodigitalis.gr/wp-content/uploads/2018/08/%CE%94%CE%95%CE%95%CE%9D%CE%BF%CE%BC%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1-2001-2018.pdf

[124] Koops BJ and others, " A Typology of Privacy", 2018, Science Direct

[125] Μια IP διεύθυνση είναι μοναδική για κάθε συσκευή συνδεδεμένη στο διαδίκτυο ή σε κάποιο τοπικό δίκτυο. Πρόκειται για ένα "Πρωτόκολλο Διαδικτύου", το οποίο είναι σύνολο των κανόνων που διέπουν τη μορφή των δεδομένων που αποστέλλονται μέσω του διαδικτύου ή του τοπικού δικτύου.

εξασφαλίσει άλλα πρόσθετα δεδομένα τα οποία, σε συνδυασμό με τη διεύθυνση IP, συμβάλλουν την εξακρίβωση της ταυτότητας ενός χρήστη». Την άποψη αυτή ενστερνίζεται και η Ομάδα Εργασίας του άρθρου 29 [126].

Στο πλαίσιο αυτό και δεδομένης της μεγάλης αξίας της ιδιωτικής ζωής, τα προσωπικά δεδομένα, ως έκφανση αυτής, χρήζουν προστασίας και λεπτομερούς μελέτης υπό το φως των τεχνολογικών εξελίξεων και ιδίως των έξυπνων νομικών συμβάσεων. Η κρυπτογραφία καθώς και η δομή του blockchain σε ένα πρώτο επίπεδο υπόσχονται την ασφάλεια των δεδομένων.

Ζητήματα όπως η κρυπτογράφηση και η ασφάλεια των δεδομένων καθώς και το εάν η τήρηση των Αρχών του ΓΚΠΔ είναι εφικτή σε περιβάλλον blockchain, θα αναλυθεί παρακάτω λαμβάνοντας υπ΄όψιν και εξετάζοντας το ζήτημα σύμφωνα με τα όσα ορίζονται από τον ΓΚΠΔ για την ασφάλεια δεδομένων κατά τη σχεδίαση αλλά την ασφάλεια δεδομένων εξ ορισμού (Privacy By Design and Privacy By Default).

3.5.2. Privacy by Design and Privacy by Default

Το ζήτημα της προστασίας των δεδομένων διαδραματίζει σπουδαίο ρόλο στο πλαίσιο των έξυπνων συμβάσεων και ιδιαίτερα εάν πρόκειται για νομικές συμβάσεις, στις οποίες διακυβεύονται πληθώρα προσωπικών δεδομένων. Πιο συγκεκριμένα, σύμφωνα με τον ΓΚΠΔ, υποχρέωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία δεδομένων, αποτελεί η εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων προς διασφάλιση επιπέδου ασφαλείας ανάλογου του κινδύνου.

Οι επόμενες ενότητες σχετικές με τον ΓΚΠΔ θα εξεταστούν υπό το πρίσμα της Προστασίας των Δεδομένων τόσο από το Σχεδιασμό όσο και Εξ Ορισμού. Για το λόγο αυτό και πριν αναπτυχθεί αναλυτικά το σκεπτικό σε κάθε υπο-ενότητα, θα δοθεί ένας ορισμός και μια προσέγγιση των εννοιών αυτών τόσο στη θεωρία όσο και στην πράξη προκειμένου να γίνει ανάλογη προσέγγιση των κατωτέρω. Η προστασία των δεδομένων μπορεί να θεωρηθεί ότι σχετίζεται με έναν συγκεκριμένο τύπο ιδιωτικότητας: την πληροφοριακή ιδιωτικότητα. Αυτό συμβαίνει διότι, ενώ το δικαίωμα στην ιδιωτική ζωή αφορά και τους εννέα τύπους (όπως προαναφέρθηκαν) [127] , η προστασία των δεδομένων αφορά κυρίως τη διασφάλιση της νόμιμης

[126] https://ec.europa.eu/newsroom/article29/items

[127] Bert Jaap Koops and others " A typology of Privacy", 2018, Science Direct

επεξεργασίας των δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων (ΓΚΠΔ αρθρο 1 παρ 1).

Σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας των Δεδομένων (ΕΣΠΔ) και τις Κατευθυντήριες Γραμμές 4/2019 για το άρθρο 25 του ΓΚΠΔ, *"η τήρηση των απαιτήσεων της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού διαδραματίζει καθοριστικό ρόλο στην προαγωγή της προστασίας της ιδιωτικής ζωής και των δεδομένων στην κοινωνία. Επιβάλλεται επομένως οι υπεύθυνοι επεξεργασίας να λάβουν σοβαρά υπόψη τους αυτήν την ευθύνη και να εφαρμόσουν τις υποχρεώσεις τους σε σχέση με τον ΓΚΠΔ κατά τον σχεδιασμό των πράξεων επεξεργασίας."* Στο κείμενο αυτό (Κατευθυντήριες Γραμμές 04/2019), το ΕΣΠΔ υπογραμμίζει την ανάγκη για εφαρμογή των κατάλληλων μέτρων και την εφαρμογή των απαραίτητων εγγυήσεων προκειμένου να λειτουργήσει ομαλά και αποτελεσματικά ο μηχανισμός διασφάλισης και προστασίας των δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ήδη από τον σχεδιασμό.

Οι δύο έννοιες του άρθρου 25 ΓΚΠΔ είναι αλληλοσυμπληρούμενες καθώς ερμηνευτικά καλύπτουν όλα τα στάδια στο πλαίσιο σύναψης μιας νομικής σύμβασης. Περαιτέρω, πρόκειται για δύο όρους που "αλληλοενισχύονται" δεδομένου ότι τα υποκείμενα των δεδομένων προστατεύονται τόσο εξ ορισμού όσο και κατά τον σχεδιασμό έκαστης έξυπνης νομικής σύμβασης.

By Design

Πιο συγκεκριμένα, στο άρθρο 25 παρ. 1 ΓΚΠΔ ("Προστασία των δεδομένων ήδη από τον σχεδιασμό") απαιτείται από τον Υπεύθυνο Επεξεργασίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα καθώς και να παρέχει τις κατάλληλες εγγυήσεις προς διασφάλιση αυτών. Σε αυτό το σημείο γεννώνται πληθώρα ερωτημάτων όπως: ποιος είναι υπεύθυνος επεξεργασίας σε ένα blockchain δίκτυο στο οποίο δημιουργούνται οι έξυπνες νομικές συμβάσεις, πώς ορίζεται ο όρος "κατάλληλα" και ποιος αξιολογεί τα τεχνικά μέτρα αυτά; Ο όρος "κατάλληλα" είναι άμεσα συνδεδεμένος με την αποτελεσματικότητα, εφόσον και εάν με τα μέτρα αυτά επιτυγχάνεται ο επιδιωκόμενος σκοπός, ήτοι η προστασία των δεδομένων. Η αποτελεσματικότητα αυτών κρίνεται από το εάν εφαρμόζονται τα κατάλληλα ανά περίπτωση μέτρα και από το εάν ο Υπεύθυνος Επεξεργασίας μπορεί να αποδείξει την τήρηση αυτών καθώς και τον σεβασμό προς τις Αρχές του ΓΚΠΔ. Ενδεικτικά, ως κατάλληλα τεχνικά και οργανωτικά μέτρα προτείνονται η ψευδωνυμοποίηση (όπως ορίζεται στο άρθρο 4 παρ 5 ΓΚΠΔ), η κρυπτογράφηση, η παροχή πληροφοριών για την αποθήκευση των δεδομένων, η χρήση μέσων για την ανίχνευση κακόβουλου

λογισμικού. Τα μέτρα αυτά καθώς και πλήθος άλλων που κρίνονται απαραίτητα ad hoc, πρέπει να εφαρμόζονται τη στιγμή του προσδιορισμού των μέσων επεξεργασίας.

Η εύρεση και ο ορισμός του συγκεκριμένου χρόνου είναι μια απαιτητική εργασία στον φυσικό κόσμο, πολλώ δε μάλλον σε περιβάλλον blockchain, διότι οι έννοιες του φυσικού κόσμου (χρόνος, επεξεργασία, τεχνικά μέσα) αποκτούν άλλη σημασία, η οποία μάλιστα είναι προς διερεύνηση. Ειδικότερα, σύμφωνα με τον ΓΚΠΔ και το ΕΣΠΔ η στιγμή του καθορισμού των μέσων επεξεργασίας από τον Υπεύθυνο Επεξεργασίας είναι η δέουσα προς εφαρμογή της ασφάλειας των δεδομένων. Πρόκειται δηλαδή για το χρονικό διάστημα κατά το οποίο ο Υπεύθυνος Επεξεργασίας αποφασίζει τον τρόπο και τους μηχανισμούς της επεξεργασίας. Σε αυτό το σημείο ανακύπτουν τα εξής ζητήματα: α) ποιος είναι υπεύθυνος επεξεργασίας και τι ευθύνες φέρει σε ένα blockchain δίκτυο και ειδικότερα σε μία έξυπνη νομική σύμβαση; , β) ποιος είναι ο ορισμός της "επεξεργασίας" στο δίκτυο blockchain; και γ) υπάρχει εκτελών την επεξεργασία στο blockchain για τον οποίο φέρει ευθύνη ο υπεύθυνος επεξεργασίας;

By Default

Εν συνεχεία στο άρθρο 25 παρ 2 ΓΚΠΔ ("Προστασία δεδομένων εξ ορισμού") χρήζει ερμηνείας ο όρος "εξ ορισμού". Σύμφωνα με τις κατευθυντήριες γραμμές[128] ο όρος αναφέρεται "*στην προϋπάρχουσα ή προεπιλεγμένη τιμή μιας διαμορφώσιμης ρύθμισης που αντιστοιχεί σε μια εφαρμογή λογισμικού, ένα πρόγραμμα ηλεκτρονικού υπολογιστή ή συσκευή. Οι εν λόγω ρυθμίσεις ονομάζονται επίσης «προκαθορισμένες ρυθμίσεις» ή «εργοστασιακές προκαθορισμένες ρυθμίσεις», ειδικά για τις ηλεκτρονικές συσκευές."*. Κατά συνέπεια, προκύπτει ότι κατά την επεξεργασία των προσωπικών δεδομένων πρέπει να έχει γίνει η ανάλογη παραμετροποίηση των τιμών προκειμένου να είναι ελεγχόμενα τόσο η ποσότητα και ο τρόπος συλλογής όσο και η έκταση επεξεργασίας, το διάστημα αποθήκευσης και η προσβασιμότητα σε αυτά. Σε αυτό το σημείο, γεννάται το ερώτημα κατά πόσο είναι εφικτά και εάν η ίδια η δομή του blockchain επιτρέπει αυτού του είδους την παραμετροποίηση ώστε έκαστη εφαρμογή του να συμβαδίζει με τις απαιτήσεις του ΓΚΠΔ. Επιπλέον, και σε αυτό το στάδιο, ο υπεύθυνος επεξεργασίας οφείλει να λογοδοτεί για την εφαρμογή και την αποτελεσματικότητα των ρυθμίσεων και παραμετροποιήσεων που έχουν γίνει προκειμένου να επεξεργάζονται αυστηρά τα απολύτως αναγκαία προσωπικά δεδομένα για την επίτευξη του επιδιωκόμενου σκοπού. Επομένως, γεννώνται ερωτήματα αντίστοιχα με αυτά που

[128] Κατευθυντήριες Γραμμές 04/2019 του ΕΣΠΔ για το άρθρο 25 ΓΚΠΔ

ανέκυψαν κατά την ανάλυση του 25 παρ 1 ΓΚΠΔ, για το ποιος είναι ο υπεύθυνος επεξεργασίας και πού λογοδοτεί καθώς και για τις ευθύνες που φέρει, εάν φέρει. Τα ερωτήματα αυτά θα προσεγγιστούν ειδικώς και αναλόγως στις αντίστοιχες ενότητες. Ωστόσο, πριν την εκ του σύνεγγυς μελέτη των ζητημάτων αυτών, θα γίνει μια σύντομη αναφορά για τη σχέση και την σύνδεση του άρθρου 25 ΓΚΠΔ με το blockchain.

Σύμφωνα με τα προλεχθέντα, συνάγεται πως το blockchain ή άλλως οι αλυσίδες μπλοκ συνιστούν μια κατηγορία τεχνολογίας. Πρόκειται για μια τεχνολογία που συνεχώς εξελίσσεται και βελτιώνεται διατηρώντας ωστόσο τον πυρήνα σταθερό. Η τεχνολογία DLT αναφέρεται σε πολλές και ποικίλες μορφές κατανεμημένων βάσεων δεδομένων, οι οποίες διαφοροποιούνται τόσο σε τεχνικό όσο και διοικητικό επίπεδο, με αποτέλεσμα να καθίστανται ιδιαιτέρως πολύπλοκες. Απόρροια της διαφοροποίησης και της πολυπλοκότητας αυτής είναι η απουσία κοινής αξιολόγησης και όμοιου χειρισμού ως προς τον ΓΚΠΔ, ώστε η σχέση των κατανεμημένων βιβλίων και του ΓΚΠΔ να κρίνεται ξεχωριστά και μεμονωμένα. Ειδικότερα, απαιτείται λεπτομερής μελέτη και ανάλυση εκάστης εφαρμογής προκειμένου να μελετηθεί επισταμένα ο συγκεκριμένος τεχνικός σχεδιασμός και η συγκεκριμένη διοικητική δομή καθώς και οι ρυθμίσεις διακυβέρνησης της σχετικής περίπτωσης χρήσης blockchain. Κατά συνέπεια, θα ήταν άτοπη μια γενικευμένη αξιολόγηση και κριτική των αλυσίδων μπλοκ ως εναρμονισμένες ή μη με τον ΓΚΠΔ. Εν προκειμένω λοιπόν, έκαστη εφαρμογή DLT πρέπει να αξιολογείται εξατομικευμένα βάσει των δικών της χαρακτηριστικών προκειμένου να κριθεί η συμβατότητά της ή μη με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων. Σε αυτό το σημείο και βάσει των ανωτέρω συνάγεται ότι η αξιολόγηση των ιδιωτικών και αδειοδοτημένων αλυσίδων (Private) ως προς την εναρμόνιση με τον Κανονισμό της ΕΕ για την προστασία των δεδομένων καθίσταται σαφώς ευκολότερη και ακριβέστερη έναντι των δημοσίων μη αδειοδοτημένων δικτύων (permissionless). Αυτό οφείλεται στη φύση και τη δομή των ιδιωτικών δικτύων και το γεγονός ότι οι συμμετέχοντες γνωρίζονται και συνήθως αποδίδουν ρόλους μεταξύ τους, ορίζοντας το είδος της συμβατικής τους σχέσης, επιτρέποντας ταυτόχρονα τον κατάλληλο καταμερισμό της ευθύνης. Περαιτέρω δε, όπως αναφέρθηκε και στην αντίστοιχη ενότητα, στα ιδιωτικά δίκτυα γίνεται έλεγχος του περιεχομένου καθώς και των προσώπων και των φορέων που έχουν πρόσβαση σε αυτά, κάτι το οποίο είναι αδύνατο τεχνολογικά να συμβεί στα δημόσια δίκτυα. Τούτο λεχθέντος,

επισημαίνεται ότι η CNIL (Commission Nationale de l'Informatique et des Libertés)[129] αναφέρει ότι η μεταφορά δεδομένων σε μια δημόσια αλυσίδα μπλοκ μπορεί να είναι ιδιαίτερα προβληματική, δεδομένου ότι οι miners (ανθρακωρύχοι) ενδέχεται να επικυρώνουν συναλλαγές εκτός της ΕΟΧ[130]. Για το λόγο αυτό προτείνει στις περιπτώσεις που τα προσωπικά δεδομένα που δεν μπορούν να αποθηκευτούν εκτός αλυσίδας, να εξετάζονται λύσεις όπως ο κατακερματισμός και η κρυπτογράφηση.

3.5.3. Απόδοση Ρόλων και Ευθυνών του ΓΚΠΔ στις έξυπνες νομικές συμβάσεις

Σύμφωνα με τα όσα αναπτύχθηκαν στην προηγούμενη ενότητα, στο πλαίσιο συμμόρφωσης με τις απαιτήσεις του ΓΚΠΔ για την προστασία της ιδιωτικής ζωής μέσω του σχεδιασμού (by default) και την ελαχιστοποίηση των δεδομένων (data minimization), οι υπεύθυνοι επεξεργασίας οφείλουν να ελέγξουν εάν το blockchain και ειδικότερα έκαστη εφαρμογή αυτού μπορούν να διαμορφωθούν με τρόπο σύννομο και παράλληλο προς τις απαιτήσεις του ευρωπαϊκού κανονισμού. Ο ΓΚΠΔ αναθέτει υποχρεώσεις και επιρρίπτει ευθύνες σε ορισμένα πρόσωπα τα οποία φέρουν κάποιο συγκεκριμένο ρόλο, όπως περιγράφεται από τον Κανονισμό. Έκαστος ρόλος αποδίδεται υπό προϋποθέσεις και φέρει συγκεκριμένες υποχρεώσεις και τις ανάλογες ευθύνες. Στον πραγματικό κόσμο, η ανάθεση των ρόλων και η ανάληψη των ευθυνών είναι μια εφικτή και εφαρμοστέα διαδικασία. Σε περιβάλλον blockchain η διαδικασία αυτή καθίσταται δύσκολη λόγω της δομής και της τεχνολογίας του.

Περαιτέρω δε, οι έξυπνες συμβάσεις, ως πλήρως αυτοματοποιημένο πρωτόκολλο συναλλαγών που εκτελούνται και αποθηκεύονται στο blockchain, πρέπει να εξεταστεί σε επίπεδο διάκρισης και απόδοσης ρόλων σε κάθε κόμβο. Σε κάποιους κόμβους εκχωρούνται πλήρη δικαιώματα τόσο συναλλασσόμενου όσο και επικυρωτή συναλλαγών (full nodes). Σε άλλους

[129] Η Εθνική Επιτροπή Υπολογιστών και Ελευθεριών (CNIL) είναι μια ανεξάρτητη γαλλική διοικητική αρχή και συγκεκριμένα η Γαλλική Αρχή Προστασίας Δεδομένων . Η CNIL είναι υπεύθυνη να διασφαλίζει ότι η τεχνολογία της πληροφορίας βρίσκεται στην υπηρεσία των πολιτών και ότι δεν παραβιάζει την ανθρώπινη ταυτότητα, τα ανθρώπινα δικαιώματα , την ιδιωτική ζωή , τις ατομικές ελευθερίες ή το δημόσιο.

[130] Ο Ευρωπαϊκός Οικονομικός Χώρος (ΕΟΧ) συγκεντρώνει τα κράτη μέλη της ΕΕ και τα τρία κράτη ΕΟΧ / ΕΖΕΣ (Ισλανδία, Λιχτενστάιν και Νορβηγία) σε μια εσωτερική αγορά που διέπεται από τους ίδιους βασικούς κανόνες. Αυτοί οι κανόνες αποσκοπούν στην ελεύθερη κυκλοφορία αγαθών, υπηρεσιών, κεφαλαίου και προσώπων στον ΕΟΧ σε ένα περιβάλλον ανοιχτό και ανταγωνιστικό. Η συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο τέθηκε σε ισχύ την 1η Ιανουαρίου 1994.

χρήστες χορηγούνται ορισμένα δικαιώματα και κυρίως τα δικαιώματα κατόχου αντιγράφου της βάσης στερώντας το δικαίωμα επεξεργασίας (light node). Δέον να επισημανθεί ότι τα προσωπικά δεδομένα των χρηστών που συλλέγονται προκειμένου να μπορέσει να λειτουργήσει ομαλά το δίκτυο blockchain είναι : δημόσια κρυπτογραφικά κλειδιά, cookies, ηλεκτρονικές διευθύνσεις, αναγνωριστικά συσκευών πλοήγησης, ιστορικό αγορών και μεταδεδομένα κρυπτοσυναλλαγών.

Από τα ανωτέρω γεννάται προβληματισμός για το εάν και σε ποιο βαθμό τα έξυπνα συμβόλαια συμβαδίζουν με τον Κανονισμό προστασίας δεδομένων προσωπικού χαρακτήρα[131]. Περαιτέρω, φαίνεται πως τα ζητήματα που εγείρονται αναφορικά με τη προστασία της ασφάλειας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων, ρυθμίζονται και οριοθετούνται τόσο από τον υπεύθυνο επεξεργασίας όσο και από τον εκτελούντα την επεξεργασία. Για το λόγο αυτό, παρακάτω γίνεται μια ανάλυση εκάστου ρόλου αναφορικά με το blockchain και τα smart contracts. Πρόκειται για μια δύσκολη διεργασία[132], αφού έκαστος ρόλος φέρει αντίστοιχες ευθύνες και υποχρεώσεις. Σύμφωνα δε, με την CNIL και την Έκθεση της[133], που εστιάζει στο blockchain και όχι στην ευρύτερη τεχνολογία κατανεμημένου καθολικού (DLT), η απόδοση και κατανομή των ρόλων γίνεται με αυστηρό και ανάλογο της τεχνολογίας τρόπο.

3.5.3.Α. Υπεύθυνος Επεξεργασίας

Σύμφωνα με τον ΓΚΠΔ, ο Υπεύθυνος Επεξεργασίας καθορίζει το σκοπό και τα μέσα επεξεργασίας, είτε αυτοβούλως είτε σε συνεργασία (από κοινού) με ένα έναν ή περισσότερους υπεύθυνους επεξεργασίας κατόπιν γραπτής συμφωνίας. Σε ορισμένες περιπτώσεις, η εν λόγω εργασία μπορεί να ανατεθεί σε έναν ή περισσότερους εκτελούντες την επεξεργασία με υπεργολαβία. Ωστόσο, στα δίκτυα blockchain η απουσία ενός κεντρικού υπεύθυνου επεξεργασίας, ο οποίος θα αναλάμβανε την οργάνωση αλλά και την ευθύνη σε περιπτώσεις

[131] European Parliament, "Blockchain and the General Data Protection Regulation can distributed ledgers be squared with European data protection law?", 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/ERPS_STU(2019)634445_EN.pdf

[132] Czarnecki J., "Who is the data controller in a blockchain?", 2018 https://newtech.law/en/author/jacek-czarnecki/

[133] Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?, 2018 https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

παραβιάσεων, δημιουργεί εμπόδια στην κατανομή των ρόλων παρά τις απόπειρες απόδοσης και κατανομής αυτών.

Πιο συγκεκριμένα, ως Υπεύθυνος επεξεργασίας δεδομένων (controller) νοείται νομικό ή φυσικό πρόσωπο που έχει το δικαίωμα να γράφει σε μια αλυσίδα μπλοκ και να δημιουργεί μια συναλλαγή που υποβάλλεται για επικύρωση (σημειώνεται στην αναφορά της CNIL ως «συμμετέχων»). Επομένως, μπορεί να θεωρηθεί υπεύθυνος επεξεργασίας δεδομένων, ο συμμετέχων που καταγράφει προσωπικά δεδομένα σε blockchain και (i) είναι φυσικό πρόσωπο που ασκεί επαγγελματική ή εμπορική δραστηριότητα ή (ii) είναι εταιρική οντότητα. Όμως, ο χρήστης που απλώς αποθηκεύει τη βάση δεδομένων στον υπολογιστή του και δεν πραγματοποιεί άλλη επεξεργασία, δεν θεωρείται υπεύθυνος επεξεργασίας. Αντιθέτως, για παράδειγμα, εάν μια τράπεζα εισάγει δεδομένα πελατών σε μια αλυσίδα μπλοκ, η τράπεζα θα θεωρείται υπεύθυνος επεξεργασίας δεδομένων. Ένα ακόμα παράδειγμα, όπως περιγράφεται από την CNIL, υπευθύνου επεξεργασίας αποτελεί αυτό του Γάλλου συμβολαιογράφου , που ως δημόσιος υπάλληλος με μονοπώλιο στην πώληση ακινήτων, καταχωρεί τίτλο ιδιοκτησίας πελάτη σε blockchain[134]. Επομένως, υπεύθυνοι επεξεργασίας μπορούν να είναι φυσικά ή νομικά πρόσωπα που έχουν δυνατότητα καταχώρισης προσωπικών δεδομένων των πελατών τους στο δίκτυο blockchain[135].

Εν συνεχεία, προσπαθεί να περιορίσει τις περιπτώσεις, στις οποίες υπάρχουν από κοινού υπεύθυνοι επεξεργασίας καθώς και να οριοθετήσει τις συνθήκες κατά τις οποίες μπορούν αναλαμβάνουν τον συγκεκριμένο ρόλο. Στην περίπτωση που υπάρχουν περισσότεροι του ενός υπεύθυνοι επεξεργασίας, η CNIL συνιστά να **μην** ορίζονται Από Κοινού Υπεύθυνοι Επεξεργασίας (joint controller) και τα συμμετέχοντα μέρη να ορίζουν έναν υπεύθυνο επεξεργασίας, προκειμένου να αποφευχθεί η σύγχυση που μπορεί να επέλθει κατά την απόδοση ευθυνών, κατά το άρθρο 26 ΓΚΠΔ. Πιο συγκεκριμένα, το άρθρο 26 ΓΚΠΔ κάνει λόγο για κοινή ευθύνη των από κοινού υπεύθυνων επεξεργασίας σε ό,τι αφορά την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων καθώς και τις αντίστοιχες ευθύνες που φέρουν τόσο στο στάδιο της συμμόρφωσης όσο και σε περίπτωση οποιαδήποτε παραβίασης του Κανονισμού. Σε αυτό το σημείο, αξίζει να σημειωθεί πως αυτό έχει ιδιαίτερη αξία στο blockchain διότι η ανωνυμία καθώς και η ευκολία

[134] Daoui Sonia, Fleinert-Jensen Thomas, Lempérière Marc, " GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions", 2019

[135] CNIL, Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

δημιουργίας λογαριασμού μπορεί να αποτελέσει ευκαιρία για αποποίηση ή και μετάθεση αυτών σε περίπτωση κάποιας παραβίασης (data breach) σχετικής με τον ΓΚΠΔ.

Μετά την προσέγγιση των δύο βασικότερων ρόλων του ΓΚΠΔ, η CNIL περιγράφει και αποδίδει ρόλους σε δύο πρωταγωνιστές του blockchain: στους προγραμματιστές των έξυπνων συμβολαίων καθώς και στους miners. Ωστόσο, αποπειράται να χαρακτηρίσει και το ρόλο των κόμβων που συμμετέχουν στη διαδικασία επικύρωσης της συναλλαγής.

3.5.3.Β. Εκτελών την Επεξεργασία

Υπό το φως της ως άνω ανάλυσης για τον Υπεύθυνο Επεξεργασίας, δέον να σημειωθούν κάποιοι προβληματισμοί και για τον εκτελούντα την επεξεργασία. Ο συγκεκριμένος ρόλος θα μπορούσε να αποδοθεί σε α) βασικούς προγραμματιστές (core developers) και β) σε εταιρείες παραγωγής έξυπνων συμβολαίων[136]. Αυτές οι δύο κατηγορίες κατέχουν σημαντικό ρόλο στο δίκτυο, δεδομένου ότι ελέγχουν το λογισμικό διαχείρισης.

α) Σε αυτό το σημείο, αξίζει να επισημανθεί πώς όταν οι προγραμματιστές αναβαθμίζουν το λογισμικό ή δημιουργούν προτυποποιημένα έξυπνα συμβόλαια, τα διαχέουν στο δίκτυο και στους κόμβους, χωρίς να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα αυτών. Επιπλέον, στο βαθμό που δεν αναλαμβάνουν υποχρεώσεις επικυρωτή συναλλαγών, και ταυτόχρονα δεν συνδέονται συμβατικά με τα λοιπά μέρη, η δραστηριότητα τους δεν γεννά προβληματισμούς ως προς τον ΓΚΠΔ. Περαιτέρω δε, όταν οι προγραμματιστές παρέχουν τυποποιημένα συμβόλαια (smart contract as a service) και τα μέρη αναλαμβάνουν την προσαρμογή στις ανάγκες τους, δεν μπορεί να αποδοθεί ρόλος στους προγραμματιστές[137]. Εκ των ανωτέρω, συνάγεται ότι δεν μπορούν να χαρακτηριστούν εκτελούντες την επεξεργασία.

β) Αναφορικά με την κατηγορία των εταιρειών παραγωγής έξυπνων συμβολαίων, τα πράγματα διαφοροποιούνται. Οι εν λόγω εταιρείες αναλαμβάνουν να υλοποιήσουν τη βούληση των μερών, μέσω των έξυπνων συμβάσεων, στις οποίες τα μέρη προσδιορίζουν το σκοπό

---

[136] Κανέλλος Λ., "Smart Contracts, Νομικές Προκλήσεις και επιχειρηματικές προοπτικές", σελ 211, 2022, Νομική Βιβλιοθήκη

[137] Σύμφωνα με την CNIL, σε ό,τι αφορά τα έξυπνα συμβόλαια, ο προγραμματιστής μπορεί να είναι απλός πάροχος λύσεων. Όταν όμως, ο εν λόγω προγραμματιστής αναλαμβάνει ενεργό δράση στον καθορισμό του σκοπού επεξεργασίας, τότε ενδέχεται να χαρακτηριστεί είτε υπεύθυνος είτε εκτελών την επεξεργασία, αναλόγως και άλλων περιστάσεων που λαμβάνονται υπόψη για τον χαρακτηρισμό.

επεξεργασίας. Επομένως, η δράση των εταιρειών προσιδιάζει σε αυτή των εκτελούντων την επεξεργασία. Η απόδοση αυτού του ρόλου συνεπάγεται και συμμόρφωση προς τις επιταγές του ΓΚΠΔ. Δέον να επισημανθεί, ότι οι εταιρείες αυτές οφείλουν να συμμορφωθούν προκειμένου να αποφευχθούν περιστατικά διαρροής προσωπικών δεδομένων, ένεκα κενών ασφαλείας και προγραμματιστικών σφαλμάτων[138]. Προς επίρρωση αυτού, μια μελέτη που διεξήχθη το 2016 κατέδειξε ότι σχεδόν το 50% των έξυπνων συμβάσεων στο Ethereum είχαν προγραμματιστικά λάθη (στα 19.336 έξυπνα συμβόλαια, τα 8.883 είχαν κενά ασφαλείας)[139] .

3.5.3.Γ. Προγραμματιστής Έξυπνων Συμβολαίων

Ο προγραμματιστής των έξυπνων συμβολαίων εξομοιούται με τον υπεύθυνο επεξεργασίας δεδομένων, εάν στο συγκεκριμένο έξυπνο συμβόλαιο γίνεται με όποιο τρόπο (δημιουργία, καταχώρηση, αντιγραφή) επεξεργασία προσωπικών δεδομένων. Επί παραδείγματι, ο προγραμματιστής λογισμικού που προσφέρει ένα έξυπνο συμβόλαιο σε ασφαλιστικές εταιρείες που θα αποζημιώνει αυτόματα τους επιβάτες αεροπορικών εταιρειών, εάν μια πτήση καθυστερήσει (σύμφωνα με τα ασφαλιστήρια συμβόλαια ταξιδιωτικής ασφάλισης), θεωρείται υπεύθυνος επεξεργασίας και φέρει τις ευθύνες και τις υποχρεώσεις που επιβάλλει ο ΓΚΠΔ[140]. Ωστόσο, στο ίδιο παράδειγμα, σύμφωνα με την CNIL, ο προγραμματιστής μπορεί να είναι εκτελών την επεξεργασία, εάν ακολουθεί τους κανόνες και τις οδηγίες του υπεύθυνου επεξεργασίας. Στην περίπτωση αυτή, ο υπεύθυνος και ο εκτελών την επεξεργασία πρέπει να υπογράψουν μια σύμβαση, οι διατάξεις της οποίας θα αποσκοπούν στην προστασία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όπως το αντικείμενο και η διάρκεια της επεξεργασίας, η φύση και ο σκοπός της επεξεργασίας και ο τύπος των δεδομένων προσωπικού χαρακτήρα. Στην σύμβαση πρέπει επίσης να αναγράφεται ρητώς ότι ο εκτελών την επεξεργασία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο κατόπιν τεκμηριωμένων οδηγιών του υπευθύνου επεξεργασίας. Σε αυτό το σημείο, πρέπει να επισημανθεί πως η σύναψη της εν λόγω

[138] Cheong, Ben Chester and Kishen, Harry, Legal Risks Beneath Blockchain enabled Smart Contracts, 2021 https://ssrn.com/abstract=3772066

[139] ο.π.

[140] Παράδειγμα της CNIL στην έκθεση - Premiers éléments d'analyse de la CNIL BLOCKCHAIN

σύμβασης δεν αποτελεί μείζον ζήτημα στις ιδιωτικές αλυσίδες μπλοκ (private blockchain) όσο στις δημόσιες και μη αδειοδοτημένες (public, permissionless). Αυτό συμβαίνει γιατί σε μία δημόσια αλυσίδα ο κόμβος που θα επικυρώσει (miner), απλώς θα εγκαταστήσει ένα κομμάτι λογισμικού και θα κατεβάσει ένα πλήρες αντίγραφο της αλυσίδας μπλοκ. Επομένως, οι πιθανότητες είναι ότι δεν θα συναφθεί ποτέ καμία συμφωνία με τους χρήστες του δικτύου, κι αυτό εγείρει προβλήματα συμμόρφωσης με τον ΓΚΠΔ.

3.5.3.Δ. Miner

Όσον αφορά στον κόμβο επικύρωσης μιας συναλλαγής (miner), έχει επικρατήσει το εξής σκεπτικό. Ειδικότερα, υπεύθυνος επεξεργασίας μπορεί να θεωρηθεί και ο miner καθώς εκτελεί τις οδηγίες του προγραμματιστή του λογισμικού κατά την επαλήθευση μιας συναλλαγής ως προς το εάν πληροί συγκεκριμένα τεχνικά κριτήρια, κατά συνέπεια ελέγχει υπό διαφορετικό πρίσμα την αλυσίδα και εξ αυτού δεν θεωρείται εκτελών την επεξεργασία. Ωστόσο, παρά την πρώτη αυτή προσέγγιση, η CNIL αναγνωρίζει τα πιθανά κωλύματα που ενδέχεται να εμφανιστούν εάν ένας miner λάβει ρόλο υπευθύνου επεξεργασίας σε ένα δημόσιο blockchain, διότι ανακύπτουν πρακτικές δυσκολίες ως προς την υπογραφή (με όποιο τρόπο) συμφωνίας με τον εκάστοτε υπεύθυνο επεξεργασίας. Περαιτέρω, προς επίρρωση της άποψης ότι οι miners δεν μπορούν να αναλάβουν ρόλο υπευθύνου επεξεργασίας, η CNIL επισημαίνει ότι επικυρώνουν τις συναλλαγές χωρίς να καθορίζουν το σκοπό και τα μέσα επεξεργασίας.

3.5.3.Ε. Nodes (Κόμβοι)

Η CNIL προσπαθεί να αποδώσει ρόλο και στους συμμετέχοντες κόμβους του δικτύου. Οι κόμβοι -ως σπουδαίο μέρος της αλυσίδας μπλοκ- παρότι το έργο τους είναι όμοιο με των miners, δεν είναι υπεύθυνοι επεξεργασίας, διότι δεν καθορίζουν τον σκοπό και τα μέσα επεξεργασίας[141] καθώς και δεν αναλαμβάνουν ενεργό ρόλο στην ολοκλήρωση της συναλλαγής. Οι κόμβοι μπορούν να χαρακτηριστούν ως εκτελούντες την επεξεργασία δεδομένων "σε ορισμένες περιπτώσεις", κατά τις οποίες επεξεργάζονται προσωπικά δεδομένα για λογαριασμό των

[141] DiMatteo L., Cannarsa M., Poncibo C., “Smart Contracts and Contract Law”, in The Cambridge Handbook of Smart Contracts, 2020, Cambridge University

υπευθύνων επεξεργασίας. Κατά την εκτέλεση του πρωτοκόλλου, οι κόμβοι επικύρωσης (miners) θεωρούνται ως εντολοδόχοι των χρηστών του δικτύου. Κατά συνέπεια, οι χρήστες του δικτύου (κόμβοι) θα πρέπει να συνάψουν συμφωνία τόσο με τους προγραμματιστές έξυπνων συμβολαίων όσο και με τους κόμβους επικύρωσης[142] . Η εν λόγω συμφωνία μεταξύ του υπεύθυνου επεξεργασίας δεδομένων και του εκτελούντος την επεξεργασία δεδομένων αποτελεί απαίτηση του ΓΚΠΔ. Παρ΄όλα αυτά, οι κόμβοι συνήθως είναι άγνωστοι μεταξύ τους κάτι που καθιστά δύσκολη την σύναψη σύμβαση μεταξύ τους.

Αντίθετη άποψη επί του ρόλου των κόμβων έχουν διατυπώσει οι Martini και Weinzierl, κατά τους οποίους κάθε κόμβος που ξεκινά μια συναλλαγή (και κατά συνέπεια διανέμονται πληροφορίες σε όλους τους άλλους κόμβους) ή που αποθηκεύει μια συναλλαγή στο δικό του αντίγραφο της βάσης δεδομένων θεωρείται υπεύθυνος επεξεργασίας, δεδομένου ότι κατά αυτόν τον τρόπο επιδιώκει τη συμμετοχή του στο δίκτυο . Επομένως, με την τακτική αυτή ο κόμβος καταχωρεί και αποθηκεύει δεδομένα και εν συνεχεία μπορεί να τα χρησιμοποιήσει ελεύθερα.

Περαιτέρω, έχει υποστηριχθεί ότι οι κόμβοι μπορούν να εκληφθούν ως από κοινού υπεύθυνοι επεξεργασίας, λαμβάνοντας υπόψη ότι "*έχουν την ίδια επιρροή και ελευθερία να επιλέξουν (ή να ξεκινήσουν) ένα συγκεκριμένο δίκτυο blockchain - και μπορούν, για παράδειγμα με την απαραίτητη πλειοψηφία από ένα fork[143], να αλλάξουν τους κανόνες",* γεγονός που μαρτυρά τον από κοινού έλεγχο[144].

3.5.4. Θεμελιώδεις Αρχές ΓΚΠΔ, Δικαιώματα των Υποκειμένων των Δεδομένων και έξυπνα νομικά συμβόλαια

Το νομικό πλαίσιο δημιουργεί μια σειρά από υποχρεώσεις που βαρύνουν τους υπευθύνους επεξεργασίας δεδομένων, οι οποίοι -όπως προαναφέρθηκε- είναι οι οντότητες που καθορίζουν τα μέσα και τους σκοπούς της επεξεργασίας των δεδομένων. Αποδίδει επίσης μια σειρά δικαιωμάτων

---

[142] Daoui Sonia, Fleinert-Jensen Thomas, Lempérière Marc, " GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions", 2019

[143] Σχετίζεται με το γεγονός ότι διαφορετικά μέρη πρέπει να χρησιμοποιούν κοινούς κανόνες για να διατηρήσουν το ιστορικό του blockchain. Όταν τα μέρη δεν συμφωνούν, μπορεί να προκύψουν εναλλακτικές αλυσίδες.

[144] Wirth C and Kolain M (2018), 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' in Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design , https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf

στα υποκείμενα των δεδομένων, ήτοι τα φυσικά πρόσωπα στα οποία αναφέρονται τα δεδομένα προσωπικού χαρακτήρα και με αυτά μπορούν να προστατευτούν ή να εναντιωθούν έναντι έκαστης παράβασης.

Παρά το γεγονός ότι σε ένα πρώτο επίπεδο η σχέση ΓΚΠΔ και έξυπνων νομικών συμβάσεων ομοιάζει αλληλοσυμπληρούμενη/εξαρτώμενη, μελετώντας πιο προσεκτικά το ζήτημα γεννώνται ορισμένοι προβληματισμοί, αναφορικά με την τήρηση των Αρχών του ΓΚΠΔ αλλά και τον σεβασμό των δικαιωμάτων των υποκειμένων.

3.5.4.Α. Δικαίωμα Διαγραφής (στη Λήθη)

Χαρακτηριστικό παράδειγμα αποτελεί το δικαίωμα διαγραφής (άρθρο 17 ΓΚΠΔ), σύμφωνα με το οποίο κάτω από ορισμένες προϋποθέσεις το υποκείμενο των δεδομένων μπορεί να ζητήσει τη διαγραφή των συλλεγμένων προσωπικών του δεδομένων. Τα έξυπνα (νομικά) συμβόλαια - όπως έχει αναφερθεί σε αρκετά σημεία- υπόσχονται αδιαβλητότητα και αδυναμία παρέμβασης στο περιεχόμενο και αδυναμία διαγραφής αυτού. Επομένως, το πλεονέκτημα αυτό των έξυπνων συμβολαίων , μετατρέπεται και αντιμετωπίζεται ως εμπόδιο, εξεταζόμενο υπό το φως του ΓΚΠΔ. Η CNIL αναγνωρίζει ότι είναι τεχνικά αδύνατη η συμμόρφωση με ένα αίτημα διαγραφής όταν τα προσωπικά δεδομένα είναι καταχωρημένα στο blockchain, ωστόσο, θεωρεί ότι υπάρχουν τεχνικά μέσα που πλησιάζουν στη διαγραφή των προσωπικών δεδομένων. Αυτό συμβαίνει όταν τα δεδομένα καταχωρούνται στο blockchain με κατακερματισμό ή οποιαδήποτε κρυπτογράφηση τελευταίας τεχνολογίας. Εάν, για παράδειγμα, διαγραφεί το ιδιωτικό κλειδί, στην πράξη δεν υπάρχει κίνδυνος σχετικά με την εμπιστευτικότητα των προσωπικών δεδομένων. Σε κάθε περίπτωση, η CNIL διατηρεί επιφυλάξεις για το κατά πόσον τέτοια μέσα μπορούν να θεωρηθούν ισοδύναμα με δικαίωμα διαγραφής και για το λόγο αυτό προτείνει την αποφυγή της απευθείας αποθήκευσης προσωπικών δεδομένων και χωρίς κρυπτογράφηση σε αλυσίδες μπλοκ.

Ειδικότερα, η Αρχή της Προστασίας των Δεδομένων από τον Σχεδιασμό (Privacy by Design) δημιουργεί την υποχρέωση για ασφαλή καταγραφή των προσωπικών δεδομένων που δεν προστατεύονται με κάποιο τεχνικό μέτρο σε κάποια άλλη βάση δεδομένων, για παράδειγμα σε βάση δεδομένων των ίδιων των χρηστών του δικτύου κι αυτό γιατί σε αυτές υπάρχει η δυνατότητα διαγραφής σύμφωνα με τον ΓΚΠΔ. Ωστόσο, στην αλυσίδα μπλοκ για την ορθή και ομαλή λειτουργία της και την εκτέλεση κάθε συναλλαγής, θα καταγράφεται ένα δεδομένο ή κάποιος

μοναδικός αριθμός, ο οποίος θα υποδεικνύει σε ποια βάση δεδομένων είναι αποθηκευμένα τα συγκεκριμένα προσωπικά δεδομένα εκάστης συναλλαγής.

3.5.4.Β. Αρχή Ελαχιστοποίησης των Δεδομένων και Αρχή Περιορισμού του Σκοπού

Στις κατευθυντήριες γραμμές της CNIL εξετάζεται με ποιο τρόπο ταυτοποιούνται οι χρήστες και οι κόμβοι στις αλυσίδες μπλοκ, ήτοι πώς γίνεται στην ουσία ο συνδυασμός του δημόσιου και του ιδιωτικού κλειδιού (εμπιστευτικό κλειδί) και εάν μπορεί να οδηγήσει σε αποκάλυψη της ταυτότητας. Το δημόσιο κλειδί του χρήστη είναι ορατό καθώς πρόκειται για τεχνική απαίτηση των συστημάτων για να επιτευχθεί η ανταλλαγή μηνύματος. Για το λόγο αυτό η CNIL αξιολογεί ότι πρόκειται για τη μέγιστη δυνατή ελαχιστοποίηση των δεδομένων που συλλέγονται για ταυτοποίηση του χρήστη. Γενικότερα όμως, όλες οι πληροφορίες που καταχωρίζονται στην αλυσίδα μπλοκ, ακόμη και οι κρυπτογραφημένες, θα πρέπει να διατηρούνται στο ελάχιστο.

3.5.4.Γ. Δικαίωμα στη Λήθη και Αρχή του Περιορισμού του Σκοπού

Παρά ταύτα, θα μπορούσε να γίνει μια άλλη ανάλυση που βασίζεται σε μια προσεκτική ανάγνωση του άρθρου 17 του ΓΚΠΔ σχετικά με τη συμφιλίωση του δικαιώματος διαγραφής με την αλυσίδα μπλοκ και σχετίζεται άμεσα με την Αρχή του Περιορισμού του Σκοπού. Το δικαίωμα στη λήθη υφίσταται πράγματι μόνο σε έξι περιοριστικώς καθορισμένες περιπτώσεις, εκ των οποίων οι πέντε δεν βρίσκουν εφαρμογή για τις περισσότερες ενέργειες και συναλλαγές στο blockchain:

(i) προσφορές υπηρεσιών της κοινωνίας της πληροφορίας προς παιδιά κάτω των 16 ετών- (ii) υποχρέωση διαγραφής των δεδομένων σύμφωνα με την ισχύουσα εθνική νομοθεσία- (iii) παράνομη επεξεργασία των δεδομένων- (iv) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία των δεδομένων, η οποία στηρίζεται νομικά στο γεγονός ότι η εν λόγω επεξεργασία ήταν αναγκαία για την άσκηση αποστολής δημόσιας υπηρεσίας ή για τα έννομα συμφέροντα του υπεύθυνου επεξεργασίας- (v) επεξεργασία δεδομένων βάσει συγκατάθεσης.

Κατ' αρχήν, η επεξεργασία δεδομένων για υπηρεσίες και εφαρμογές blockchain ερείδεται στο ότι η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί κατόπιν αιτήματός του. Ως εκ τούτου, η μόνη αιτιολόγηση για αίτημα διαγραφής των δεδομένων από μια αλυσίδα μπλοκ θα προκύψει όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα ενόψει του σκοπού για τον οποίο συνελέχθησαν.

Επομένως, από την ως άνω ανάλυση συνάγεται ότι, όταν ένα φυσικό πρόσωπο αποφασίζει να συμμετάσχει στην αλυσίδα μπλοκ, ως υποκείμενο των δεδομένων γνωρίζει και σιωπηρά συναινεί στην υποβολή των προσωπικών δεδομένων του προς επεξεργασία για όσο διάστημα απαιτείται προκειμένου να εκτελεστεί έκαστη συναλλαγή στην συγκεκριμένη αλυσίδα μπλοκ.

Σημειωτέον δε, πώς ο χρόνος επεξεργασίας και τήρησης αυτών δεν νοείται ακαθόριστος και ατέρμονος. Πρόβλημα ανακύπτει αναφορικά με το ζήτημα περιορισμού του χρόνου επεξεργασίας και αποθήκευσης κι αυτό διότι ανάγεται στην μελλοντική φθορά και καταστροφή των συστημάτων που αποθηκεύονται αυτές οι πληροφορίες και όχι σε κάποια τεχνολογική υποδομή ή διαδικασία που να επιτρέπει τη διαγραφή σε προβλεπόμενο και προκαθορισμένο χρόνο.

Κατά συνέπεια, το blockchain διατηρεί τα δεδομένα προσωπικού χαρακτήρα για όλη τη διάρκεια τους καθώς και μέχρι την φθορά ή καταστροφή και του τελευταίου διακομιστή (server) στον οποίο αποθηκεύεται μέρος έκαστης αλυσίδας που είναι απαραίτητο για την επεξεργασία δεδομένων και την εκτέλεση της συναλλαγής. Ως εκ τούτου, το δικαίωμα στην λήθη δεν μπορεί να τηρηθεί και για το λόγο αυτό , απαιτείται η ενίσχυση των τεχνικών μέτρων και δη της κρυπτογραφίας καθώς και η τήρηση των λοιπών Αρχών του ΓΚΠΔ προκειμένου να ενημερώνονται τα μέρη για το χρόνο διατήρησης καθώς και τον τρόπο επεξεργασίας των δεδομένων τους (Αρχή Διαφάνειας και Δικαίωμα στην Ενημέρωση).

3.5.4.Δ. Αρχή Διαφάνειας και Δικαίωμα Ενημέρωσης

Ο ΓΚΠΔ σε κάθε περίπτωση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, παρέχει το δικαίωμα ενημέρωσης των υποκειμένων τους και επιβάλλει την υποχρέωση προς τούτο στους υπευθύνους επεξεργασίας. Στην περίπτωση του blockchain, η υποχρέωση προς ενημέρωση (Δικαίωμα Ενημέρωσης) είναι σαφώς μεγαλύτερη λόγω των λοιπών προσκομμάτων προς

ενάσκηση βασικών δικαιωμάτων (Δικαίωμα διαγραφής/λήθης και Δικαίωμα διόρθωσης). Πιο συγκεκριμένα, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται τόσο εκ των προτέρων- σε στάδιο που δεν έχουν συμβληθεί ακόμα- όσο και εκ των υστέρων, ότι τα δεδομένα τους θα διατηρηθούν μέχρι την καταστροφή και του τελευταίου διακομιστή, στον οποίο είναι αποθηκευμένο και τρέχει το blockchain.

3.5.4.Ε. Δικαίωμα ανθρώπινης παρέμβασης ως προτεινόμενη εναλλακτική λύση ενόψει της απουσίας των Δικαιωμάτων Διαγραφής και Διόρθωσης

Οι έξυπνες συμβάσεις, ως ένα είδος αυτοματοποιημένης επεξεργασίας, χρησιμοποιούνται ευρέως στο blockchain. Η χρήση έξυπνων συμβάσεων καλύπτεται από τον ΓΚΠΔ, ο οποίος, κατ' εξαίρεση,, επιτρέπει την αυτοματοποιημένη επεξεργασία, εφόσον είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας. Η CNIL, παρέχοντας ορισμένες εγγυήσεις, αναγνωρίζει τον συγκεκριμένο τύπο αυτοματοποιημένης επεξεργασίας δεδομένων, ως μέσο σύναψης σύμβασης.

Σύμφωνα με τις κατευθυντήριες γραμμές, η δυνατότητα ανθρώπινης παρέμβασης πρέπει να δίνεται σε κάθε χρήστη του δικτύου, ως εναλλακτική επιλογή για την επίλυση προβλημάτων. Πιο συγκεκριμένα και ενόψει της αμφισβήτησης των αυτοματοποιημένων αποφάσεων, ο χρήστης πρέπει να έχει τη δυνατότητα ανθρώπινης παρέμβασης ακόμα και μετά την εκτέλεση και την καταχώρηση της έξυπνης σύμβασης στο δίκτυο blockchain.

Η συγκεκριμένη άποψη της CNIL συμβαδίζει με τις επιταγές του ΓΚΠΔ, ο οποίος παρέχει στα υποκείμενα των δεδομένων το δικαίωμα να μην υπόκεινται σε απόφαση που βασίζεται μόνο σε αυτοματοποιημένη επεξεργασία. Ο εν λόγω περιορισμός αποκτά ιδιαίτερη σημασία σε περιβάλλον blockchain.

3.5.4.ΣΤ. Μεταφορά δεδομένων εκτός ΕΟΧ

Η CNIL μελετά το θέμα του blockchain και σε επίπεδο μεταφοράς των δεδομένων μεταξύ των κρατών, δεδομένου ότι οι συμμετέχοντες ενδέχεται να βρίσκονται εκτός Ευρωπαϊκού

Οικονομικού Χώρου (ΕΟΧ). Επομένως, γεννάται το ζήτημα της μεταφοράς δεδομένων προσωπικού χαρακτήρα σε χώρες, όπου η προστασία ενδεχομένως είναι λιγότερο αυστηρή. Δέον να διευκρινιστεί ότι η συγκεκριμένη προβληματική δεν αφορά χώρες εντός ΕΕ ή εδάφη για τα οποία η Ευρωπαϊκή Επιτροπή έχει αποφασίσει ότι διασφαλίζει επαρκές επίπεδο προστασίας.

Οι χώρες που βρίσκονται εντός ΕΟΧ (Ισλανδία, Νορβηγία και Λιχνενστάιν) αλλά και οι χώρες που είναι εξοπλισμένες με Απόφαση Επάρκειας, δεν χρειάζονται ειδική άδεια για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα.Οι χώρες που καλύπτονται με Απόφαση Επάρκειας και κατά συνέπεια υπόκεινται σε καθεστώς ΓΚΠΔ είναι το Ηνωμένο Βασίλειο (μέχρι και τις 27/06/2025)[145], ο Καναδάς, οι ΗΠΑ (μόνο στο πλαίσιο του Privacy Shield), η Νήσος Μαν, η Νέα Ζηλανδία, το Ισραήλ η Αργεντινή, η Ελβετία, το Τζέρσεϊ, η Ανδόρα, οι Νήσοι Φερόε, η Ιαπωνία και η Ουρουγουάη [146]. Δέον να διευκρινιστεί ότι πλειονότητα αυτών των χωρών είναι πολύ μικρές και ότι η ασπίδα προστασίας της ιδιωτικής ζωής (Privacy Shield), η οποία επιτρέπει τις διαβιβάσεις προς αμερικανικές εταιρείες που έχουν (αυτο)πιστοποιηθεί βάσει αυτής, υπόκειται σε πολύ σοβαρή νομική αμφισβήτηση -μετά την απόφαση του Irish Commercial High Court να υποβάλει στο Δικαστήριο της Ευρωπαϊκής Ένωσης προδικαστικό ερώτημα σχετικά με τη νομιμότητα αυτής της απόφασης επάρκειας [147].

Ωστόσο, ελλείψει Απόφασης Επάρκειας, ο ΓΚΠΔ προτείνει εναλλακτικές λύσεις για την επίτευξη επαρκούς προστασίας και συμφιλίωσης με τον Ευρωπαϊκό Κανονισμό. Αξίζει να σημειωθεί όμως, πώς ακόμα και αυτές οι λύσεις δεν μπορούν να εφαρμοστούν σε κάθε εφαρμογή blockchain, αλλά σε κάθε περίπτωση μπορούν να ενσωματωθούν σε μία έξυπνη νομική σύμβαση. Μία προτεινόμενη λύση είναι η ύπαρξη δεσμευτικών εταιρικών κανόνων, οι οποίοι καταγράφονται από κάθε εταιρεία και καθορίζουν, μεταξύ άλλων, και ζητήματα διαβιβάσεων δεδομένων καθώς και την υποχρέωση για τήρηση και εφαρμογή των γενικών αρχών προστασίας δεδομένων. Εναλλακτικά, προτείνεται η χρήση των τυποποιημένων συμβατικών ρητρών περί προστασίας δεδομένων κατόπιν εγκρίσεως της Ευρωπαϊκής Επιτροπής. Πρόκειται για προειλημμένες ρήτρες που μπορούν να διευκολύνουν τα μέρη κατά τη δημιουργία μίας έξυπνης νομικής σύμβασης.

---

[145]Επίσημη Εφημερίδα της ΕΕ- L360_Οκτώβριος 2021 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2021:360:FULL&from=EN

[146] https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/apofaseis_eparkeias

[147] Απόφαση Schrems II - C-311/2018

Σε κάθε περίπτωση η CNIL διευκρινίζει ότι η προστασία αυτή μπορεί να αποδειχθεί επαρκής για ένα δίκτυο blockchain και ειδικότερα για τις έξυπνες νομικές συμβάσεις. Ωστόσο, διατηρεί επιφυλάξεις για την εφαρμογή αυτών στις δημόσιες, χωρίς άδεια αλυσίδες μπλοκ, καθώς μπορεί να είναι δύσκολο για τους χρήστες του δικτύου να ελέγξουν πού βρίσκονται οι κόμβοι.

Συμπερασματικά:

Στο πλαίσιο αυτό και μετά την προηγειθείσα ανάλυση, δέον να εξεταστούν οι έξυπνες νομικές συμβάσεις, υπό το πρίσμα της προστασίας των δεδομένων τόσο από το σχεδιασμό όσο και εξ ορισμού (privacy by design and by default), διότι είναι σημαντικά τα πιθανά προβλήματα που μπορεί να προκύψουν. Παρακάτω αναφέρονται συνοπτικά ορισμένα εξ αυτών:

1) Έλλειψη διαφάνειας: Οι έξυπνες συμβάσεις εκτελούνται συχνά αυτόματα, χωρίς ανθρώπινη παρέμβαση, γεγονός που μπορεί να δυσχεράνει την κατανόηση του τρόπου με τον οποίο χρησιμοποιούνται και επεξεργάζονται τα προσωπικά τους δεδομένα.

2) Περιορισμένος έλεγχος των προσωπικών δεδομένων: Οι έξυπνες συμβάσεις μπορούν να εκτελούνται αυτόματα με βάση προκαθορισμένους κανόνες και προϋποθέσεις, γεγονός που μπορεί να περιορίσει τη δυνατότητα των ατόμων να ελέγχουν τον τρόπο χρήσης και κοινοποίησης των προσωπικών τους δεδομένων.

3) Μη τήρηση της Αρχής της Ελαχιστοποίησης των δεδομένων: Οι έξυπνες συμβάσεις μπορούν να συλλέγουν και να επεξεργάζονται αυτόματα μεγάλες ποσότητες δεδομένων, οι οποίες ενδέχεται να μην είναι απαραίτητες για τη συγκεκριμένη σύμβαση ή συναλλαγή και να αυξάνουν τον κίνδυνο παραβίασης δεδομένων.

4) Περιορισμένα δικαιώματα πρόσβασης και διόρθωσης: Οι έξυπνες συμβάσεις ενδέχεται να μην παρέχουν στα άτομα εύκολη πρόσβαση στα προσωπικά τους δεδομένα ή τη δυνατότητα διόρθωσης σφαλμάτων ή ανακριβειών στα δεδομένα.

5) Διατήρηση δεδομένων: Οι έξυπνες συμβάσεις ενδέχεται να διατηρούν δεδομένα για μεγαλύτερα χρονικά διαστήματα από τα αναγκαία, γεγονός που μπορεί να αυξήσει τον κίνδυνο

παραβίασης δεδομένων και να καταστήσει δυσκολότερη την άσκηση του δικαιώματος των ατόμων να ξεχαστούν (δικαίωμα στη λήθη).

Είναι σημαντικό να σημειωθεί ότι για τα ανωτέρω προβλήματα αναζητούνται λύσεις προκειμένου να μετριαστούν -ωστόσο σύμφωνα με τα σημερινά τεχνολογικά δεδομένα δεν μπορούν να εξαλειφθούν. Απόρροια της αδυναμίας των έξυπνων νομικών συμβάσεων για συμμόρφωση με τα όσα επιτάσσει το άρθρο 25 ΓΚΠΔ (privacy by design and by default) είναι και η αδυναμία διενέργειας εκτίμησης αντικτύπου (Data Protection Impact Assessment - DPIA), της εφαρμογής και χρήσης κατάλληλων τεχνικών και οργανωτικών μέτρων για την προστασία των προσωπικών δεδομένων και την εφαρμογή μηχανισμών για τον έλεγχο και την πρόσβαση των ατόμων στα προσωπικά τους δεδομένα.

3.5.5. Κρυπτογραφία και Προσωπικά Δεδομένα

Τα προσωπικά δεδομένα των υποκειμένων προστατεύονται και διασφαλίζονται τόσο μέσω των νομοθετημάτων για τα ανθρώπινα δικαιώματα όσο και μέσω του ΓΚΠΔ αλλά και νομοθετημάτων σχετικά με την ασφάλεια στον κυβερνοχώρο [148](στα οποίους περιλαμβάνονται οι νόμοι για την ασφάλεια των πληροφοριών και την προστασία των δεδομένων). Οι νόμοι περί ασφάλειας στον κυβερνοχώρο εστιάζουν στην τεχνική πλευρά, ιδίως στην ασφάλεια της τεχνολογίας και των δεδομένων που εμπλέκονται στην κρυπτογράφηση. Οι εν λόγω νόμοι είναι εξαιρετικά σημαντικοί επειδή απαιτούν ή συνιστούν τη χρήση της κρυπτογράφησης με σκοπό τη διασφάλιση[149]: α) της νόμιμης επεξεργασίας προσωπικών δεδομένων (προστασία δεδομένων) και β) της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των δεδομένων (ασφάλεια πληροφοριών-γνωστή και ως C.I.A: Confidentiality – Integrity - Availability). Περαιτέρω, στο

[148] 1. Νόμος 3917/2011 - Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.

2. Νόμος 3471/2006 - Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών

3. Οδηγία NIS2
4. Ο κανονισμός του ENISA είναι ο Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ της 17ης Απριλίου 2019 (Νόμος για την ασφάλεια στον κυβερνοχώρο)

[149] Michael Anthony C. Dizon, Peter John Upson, " Laws of encryption: An emerging legal framework", 2021

πλαίσιο της γενικής νομικής υποχρέωσης για την προστασία της ασφάλειας της επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθώς και της τήρησης του C.I.A. (ΓΚΠΔ άρθρο34 παρ. 3 περ. α, εξηγείται στο προοίμιο του ΓΚΠΔ: *"Προκειμένου να διατηρηθεί η ασφάλεια και να αποτραπεί η επεξεργασία κατά παράβαση του παρόντος κανονισμού , ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα πρέπει να αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και να εφαρμόζει μέτρα για τον μετριασμό των εν λόγω κινδύνων, όπως η κρυπτογράφηση . Τα εν λόγω μέτρα θα πρέπει να εξασφαλίζουν κατάλληλο επίπεδο ασφάλειας, συμπεριλαμβανομένης της εμπιστευτικότητας, λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας και το κόστος εφαρμογής σε σχέση με τους κινδύνους και τη φύση των προς προστασία δεδομένων προσωπικού χαρακτήρα"* (ΓΚΠΔ αιτιολογική σκέψη 83). Ο Κανονισμός απαιτεί συγκεκριμένα από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να "εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο με τον κίνδυνο, συμπεριλαμβανομένων, μεταξύ άλλων, κατά περίπτωση την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα"(ΓΚΠΔ αρ. 32 παρ. 1 περ. α).

Σε αυτό το σημείο, πρέπει να επισημανθεί ότι η εφαρμογή κρυπτογράφησης στα δεδομένα προσωπικού χαρακτήρα μπορεί να απαλλάξει τον υπεύθυνο επεξεργασίας από την υποχρέωση ενημέρωσης του υποκειμένου των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα (ΓΚΠΔ αρ. 34 παρ. 3 περ. α). Αυτοί οι κανόνες σχετικά με τη χρήση της κρυπτογράφησης συνάδουν με την έκτη αρχή της προστασίας των δεδομένων, την Αρχή της Εμπιστευτικότητας. Σύμφωνα με αυτήν την Αρχή απαιτείται τα δεδομένα προσωπικού χαρακτήρα να υποβάλλονται σε επεξεργασία "κατά τρόπο που να διασφαλίζει την κατάλληλη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημία, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων " (ΓΚΠΔ αρ. 5 παρ.1 περ. στ).

Από την ως άνω ανάλυση, ανακύπτει το ερώτημα εάν η κρυπτογραφία εντάσσεται και ρυθμίζεται από νόμους καθώς και εάν αυτό θα αποτελούσε τροχοπέδη στην ανάπτυξη της τεχνολογίας blockchain καθώς και της διασφάλισης της εγγυώμενης ασφάλειας. Η κρυπτογραφία αποτελεί ήδη αντικείμενο υφιστάμενων νομοθετημάτων και εξ αυτού γεννάται το ερώτημα πώς η κρυπτογραφία ελέγχεται και ρυθμίζεται από το νόμο. Πρόκειται για ένα εύλογο ερώτημα, διότι η νομοθεσία ενδεχομένως να επηρεάσει αποφασιστικά τρεις βασικούς πυλώνες της

κρυπτογραφίας: α) την τεχνολογία τόσο της ίδιας της κρυπτογραφίας όσο και άλλων που σχετίζονται με αυτή, β) τα μέρη της κρυπτογραφημένης συναλλαγής ή επικοινωνίας καθώς και γ) τα κρυπτογραφημένα δεδομένα έκαστης επικοινωνίας. Ενδεικτικά, οι κυβερνητικές προτάσεις για υποχρεωτικές εναλλακτικές αποκάλυψης τους μηνύματος (backdoors-δυνατότητα αναστροφής του κλειδάριθμου με σκοπό να οδηγήσει στην αποκάλυψη των εμπλεκομένων μερών και των δεδομένων επικοινωνίας) στην κρυπτογράφηση θα ήταν αντίθετες με το νομικό πλαίσιο και τις υποσχέσεις της κρυπτογράφησης. Πιο συγκεκριμένα, η ενεργοποίηση αυτών των εναλλακτικών, θέτει σε κίνδυνο την ασφάλεια των δεδομένων των ατόμων καθώς και υποσκάπτει τις νομικές αρχές και υποχρεώσεις περί ασφάλειας των πληροφοριών και προστασίας των δεδομένων.

Το ζήτημα αυτό προκύπτει από το γεγονός και την τεχνολογική δυνατότητα αποκρυπτογράφησης των δεδομένων από τον εκάστοτε κάτοχο του κλειδιού. Η προβληματική σχετίζεται με τη σχέση δημόσιου-ιδιωτικού κλειδιού καθώς και σχέση που τα συνδέει. Όπως αναλύθηκε στην σχετική ενότητα, τα δημόσια κλειδιά αποκρύπτουν την ταυτότητα του φυσικού προσώπου (των οποίων τα προσωπικά δεδομένα προστατεύονται) εκτός εάν συνδέονται με πρόσθετα αναγνωριστικά στοιχεία. Δέον να διευκρινιστεί πως η χρήση DLT εφαρμογών από εταιρείες ή νομικά πρόσωπα (πχ Χρηματοπιστωτικά Ιδρύματα) δεν υπόκειται σε προστασία από τον ΓΚΠΔ, εάν πρόκειται για ενέργειες που δεν αφορούν φυσικά πρόσωπα. Επί παραδείγματι, εάν οι τράπεζες χρησιμοποιούν το blockchain για τον ημερήσιο διακανονισμό των διατραπεζικών συναλλαγών για τους δικούς τους λογαριασμούς, τότε τα δημόσια κλειδιά είναι συνδεδεμένα με τα νομικά πρόσωπα και δεν χρήζουν προστασίας από τον ΓΚΠΔ[150].

Πιο συγκεκριμένα, τα κρυπτογραφημένα δεδομένα μπορούν να οδηγήσουν μέσω αποκρυπτογράφησης σε κάθε υποκείμενο των δεδομένων αυτών [151]. Κατά συνέπεια, τα δεδομένα αυτά παραμένουν προσωπικά για τον εκάστοτε κάτοχο του κλειδιού, αφού έχει τη δυνατότητα να προβεί σε ταυτοποίηση αυτών. Δέον να υπογραμμιστεί ότι η ομάδα εργασίας του άρθρου 29 τόνισε στη γνωμοδότησή της σχετικά με το cloud computing, ότι *"αν και η κρυπτογράφηση μπορεί να συμβάλει σημαντικά στην εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, εάν εφαρμοστεί σωστά", δεν "καθιστά τα δεδομένα προσωπικού χαρακτήρα αμετάκλητα ανώνυμα"* [152].

[150] Bacon J et al, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers', 2018

[151] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20

[152] Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN

Ο προβληματισμός αυτός γεννάται λόγω του ότι το δημόσιο κλειδί, εάν αντιστοιχηθεί και με άλλες πληροφορίες, πιθανόν να οδηγήσει στην ταυτοποίηση του προσώπου, με αποτέλεσμα να γίνεται λόγος για ψευδωνυμοποίηση (άρθρο 4 παρ 5 ΓΚΠΔ). Ειδικότερα, πληροφορίες όπως όνομα, διεύθυνση IP[153], κινήσεις λογαριασμού[154] μπορούν να οδηγήσουν εμμέσως σε ταυτοποίηση. Συνεπώς, διαφαίνεται μια αναλογία μεταξύ δημοσίων κλειδιών και άλλων μεθόδων ψευδωνυμοποίησης όπως τα μοναδικά αναγνωριστικά των cookies, τα οποία θεωρούνται προσωπικά δεδομένα[155].

Για το συγκεκριμένο θέμα, η ομάδα εργασίας του άρθρου 29 έχει υποστηρίξει ότι η ψευδωνυμοποίηση είναι *"η διαδικασία απόκρυψης των ταυτοτήτων"*, η οποία είναι ανάλογη με τα δημόσια κλειδιά, με τη διαφορά της μη αναστρεψιμότητας[156] . Κατά συνέπεια, τα δημόσια κλειδιά μπορούν να οδηγήσουν σε ταυτοποίηση ενός συγκεκριμένου φυσικού προσώπου που φέρει μια διεύθυνση blockchain. Επιπρόσθετα, αναφέρεται ότι έχουν καταγραφεί περιπτώσεις στις οποίες τα υποκείμενα των δεδομένων συνδέθηκαν με δημόσια κλειδιά και προκειμένου να λάβουν παρανόμως κεφάλαια, οικειοθελώς αποκάλυψαν το δημόσιο κλειδί τους ή περιπτώσεις κατά τις οποίες τα ανταλλακτήρια[157], προκειμένου να αντιμετωπίσουν την νομιμοποίηση εσόδων που παρανόμως αποκτήθηκαν, συλλέγουν πρόσθετες πληροφορίες, όπως απαιτείται από αντίστοιχες κανονιστικές ρυθμίσεις[158]. Επομένως, προς επίρρωση της άποψης ότι τα δημόσια κλειδιά αποτελούν προσωπικά δεδομένα, οι Berberich και Steiner υπογραμμίζουν ότι " *αν και τα προσωπικά δεδομένα περιλαμβάνουν μόνο αριθμούς ταυτότητας αναφοράς, τα εν λόγω*

[153] Biryukov A et al (2014), 'Deanonymisation of Clients in Bitcoin P2P Network' https://arxiv.org/abs/1405.7418.

[154] In Jehovan Todistajat, the ECJ provided a broad interpretation of the terminology of the 'filing system' covers 'a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to fall within that concept, it is not necessary that they include data sheets, specific lists or other search methods'). Case C-25/17 Jehovan Todistajat [2018] EU:C:2018:551, para 62

[155] Zuiderveen Borgesius F., "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", 2016, 32 Computer Law & Security Review 256, 260.

[156] Article 29 Working Party, Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN, 18

[157] Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' 25 Richmond Journal of Law and Technology 1, 61.

[158] Philipps Erb K., "IRS Tries Again To Make Coinbase Turn Over Customer Account Data", 2017 https://www.forbes.com/sites/kellyphillipserb/2017/03/20/irs-tries-again-to-make-coinbase-turn-over-customeraccount-data/#1841d9e5175e .

αναγνωριστικά στοιχεία είναι συνήθως μοναδικά για ένα συγκεκριμένο πρόσωπο. Ενώ σε όλες αυτές τις περιπτώσεις που απαιτούνται πρόσθετες πληροφορίες για την απόδοση πληροφορίες στο υποκείμενο των δεδομένων, οι πληροφορίες αυτές θα είναι απλώς ψευδωνυμοποιημένες και θα θεωρούνται προσωπικές πληροφορίες" [159]. Την συγκεκριμένη άποψη ενστερνίζονται τόσο η CNIL [160] όσο και το Παρατηρητήριο και το Φόρουμ της ΕΕ για την τεχνολογία blockchain [161], αναδεικνύοντας τους κινδύνους της συνδεσιμότητας.

3.5.5.1. Τεχνολογική λύση στα προσωπικά δεδομένα κρυπτογραφία και κατακερματισμός

Μετά την ως άνω ανάλυση προκύπτει ότι η κρυπτογράφηση παράγει ψευδώνυμα, όχι όμως ανώνυμα δεδομένα. Περαιτέρω, ο κίνδυνος αντιστροφής είναι εγγενής με την τεχνολογία της κρυπτογραφίας, ωστόσο αυτό δεν ισχύει για τον κατακερματισμό. Αντίστοιχος κίνδυνος όμως υπάρχει και για την τεχνολογία κατακερματισμού και ειδικότερα *"εάν το εύρος των τιμών εισόδου της συνάρτησης κατακερματισμού είναι γνωστό, μπορούν να αναπαραχθούν μέσω της συνάρτησης κατακερματισμού προκειμένου να να προκύψει η σωστή τιμή για μια συγκεκριμένη εγγραφή"* [162]. Επομένως, συνάγεται ότι αν και οι συναρτήσεις κατακερματισμού μειώνουν σε σημαντικό βαθμό *"τη δυνατότητα σύνδεσης ενός συνόλου δεδομένων με την αρχική ταυτότητα του υποκειμένου των δεδομένων- ως εκ τούτου, είναι ένα χρήσιμο μέτρο ασφαλείας αλλά όχι μια μέθοδος ανωνυμοποίησης"*[163].

Σε κάθε περίπτωση, είναι σημαντικό να εξετάζεται έκαστη χρήση blockchain, αναφορικά με την αποθήκευση δεδομένων στην ίδια αλυσίδα. Το ζήτημα αποκτά ιδιαίτερη σημασία σε συνάρτηση με τα έξυπνα νομικά συμβόλαια και τα προσωπικά δεδομένα που απαιτούνται για την

[159] Berberich M and Steiner M., "Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?", 2016, European Data Protection Law Review 422.

[160] Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data https://www.cnil.fr/en/blockchain-and-gdpr-solutionsresponsible-use-blockchain-context-personal-data

[161] Report of the European Blockchain Observatory and Forum (16 October 2018) Blockchain and the GDPR 20 https://www.eublockchainforum.eu/reports

[162] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20.

[163] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20

εκτέλεση και την δεσμευτικότητα τους. Εν αρχή, ένα νομικό συμβόλαιο εμπεριέχει πολλά προσωπικά δεδομένα και συνήθως προσωπικά δεδομένα ειδικών κατηγοριών που χρήζουν αυξημένης προστασίας και εγγυήσεων. Σε εφαρμογές, όπως αυτή, που απαιτούνται πολλά προσωπικά δεδομένα, προτείνεται λύση συνδυαστική της κρυπτογραφίας και του κατακερματισμού. Τα εν λόγω δεδομένα μπορούν να αποθηκεύονται κρυπτογραφημένα σε μία βάση δεδομένων εκτός αλυσίδας και εν συνεχεία να συνδέονται με το κατανεμημένο βιβλίο μέσω ενός κατακερματισμού, του hash-pointer[164]. Στην περίπτωση αυτή, αξιοποιούνται τα πλεονεκτήματα τόσο της κρυπτογραφίας όσο και του κατακερματισμού σε ό,τι αφορά την ασφάλεια των προσωπικών δεδομένων και επιτυγχάνεται η δέουσα συμμόρφωση με τον ΓΚΠΔ.

.

3.6. Smart Legal Contracts και Νομικά Ζητήματα

Η εγκυρότητα και ισχύς μιας νομικής σύμβασης συνήθως κρίνεται από το εκάστοτε εφαρμοστέο δίκαιο. Επομένως, η εγγραφή δεδομένων στην αλυσίδα μπλοκ δεν πρέπει να επηρεάζει την νομική υπόσταση έκαστης δικαιοπραξίας. Αντιστοίχως, η καινοτομία των έξυπνων νομικών συμβάσεων δεν μπορεί να υπονομεύσει ούτε να στερήσει τα δικαιώματα των συμβαλλομένων, όπως αυτά έχουν καθιερωθεί από το παραδοσιακό δίκαιο και εφαρμόζονται στις συμβάσεις στον φυσικό κόσμο. Ενδεικτικά, μερικά δικαιώματα των μερών είναι η συμβατική ελευθερία, το δικαίωμα επιλογής συμβαλλομένου, το δικαίωμα προσχώρησης, τροποποίησης, υπαναχώρησης και καταγγελίας. Το ζήτημα αυτό πρέπει να αντιμετωπιστεί σφαιρικά, δεδομένου ότι οι έξυπνες συμβάσεις ενδέχεται να συνάπτονται εκτός blockchain και εν συνεχεία να αποτυπώνονται απλώς σε μια αλυσίδα και να εκτελούνται με τη χρήση αντίστοιχου λογισμικού[165]. Ένα ακόμα ενδιαφέρον ζήτημα που ανακύπτει λόγω της δομής της τεχνολογίας και του παγκόσμιου χαρακτήρα του DLT, ανάγεται στη διεθνή δικαιοδοσία καθώς και το ποιο είναι θα το εφαρμοστέο δίκαιο σε κάθε συναλλαγή ή σύμβαση μέσω της αποκεντρωμένης τεχνολογικής υποδομής.

[164] Berberich M and Steiner M (2016), 'Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?' 2 European Data Protection Law Review 422, 425 and Finck M., "Blockchains and Data Protection in the European Union", 2018, 4 European Data Protection Law Review 17.

[165] Woebbeking M., "The Impact of Smart COntracts on Traditional Concepts of Contract Law", 2019

3.6.1.Εφαρμοστέο Ευρωπαϊκό Δίκαιο

Στην Ευρωπαϊκή Ένωση δεν υπάρχει ενιαίο νομοθετικό πλαίσιο και για τα 27 κράτη μέλη. Απόρροια αυτού, είναι η εγκυρότητα έκαστης έξυπνης νομικής σύμβασης να κρίνεται υπό το φως της εκάστοτε εθνικής νομοθεσίας καθώς και πλήθος ειδικότερων ρυθμίσεων περί ηλεκτρονικού εμπορίου, προστασίας του καταναλωτή, χρηματοοικονομικών συναλλαγών και ό,τι άλλο κρίνεται απαραίτητο για την εκάστοτε σύμβαση.

Ωστόσο, η κατάργηση των συνόρων και η διασπορά των χρηστών παγκοσμίως σε συνδυασμό με την ανωνυμία καθώς και την ευκολία και την ταχύτητα σύναψης ποικίλων έξυπνων συμβολαίων, γεννά μεγάλα και δυσεπίλυτα προβλήματα αναφορικά με τη δωσιδικία και την αρμοδιότητα των δικαστηρίων. Ωστόσο, η εφαρμογή ήδη υφιστάμενων ευρωπαϊκών νομοθετημάτων κατάλληλων για τα έξυπνα συμβόλαια καθώς και η ευρωπαϊκή νομοθεσία για τις συμβατικές και εξωσυμβατικές ενοχές, σε συνδυασμό με την υπό ψήφιση Ευρωπαϊκή Πράξη για τα Δεδομένα, θα προσέφερε ασφάλεια σε όσους προβληματίζονται για το εάν θα δεσμευτούν συμβατικά με ένα έξυπνο νομικό συμβόλαιο.

3.6.1.Α. Συμβατικές Ενοχές-Κανονισμός "Ρώμη Ι"

Ο Κανονισμός υπ΄αριθμ. 593/2008 του Ευρωπαϊκού Κοινοβουλίου (ΕΚ) και του Συμβουλίου της 17ης Ιουνίου 2008 (¨Ρώμη Ι¨) ρυθμίζει ζητήματα που άπτονται των συμβατικών σχέσεων στον ευρωπαϊκό χώρο. Σκοπός είναι "η διατήρηση και η ανάπτυξη ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης" [166]. Με έρεισμα αυτό η Ευρωπαϊκή Κοινότητα θεσπίζει μέτρα συνεργασίας των δικαστικών αρχών για τις αστικές υποθέσεις προκειμένου να εξασφαλιστεί η ομαλή λειτουργία της εσωτερικής αγοράς.

Ειδικότερα, τα άρθρα 3 και 4 του ΕΚ Ρώμη Ι παρέχουν την ελευθερία στα μέρη να επιλέξουν το εφαρμοστέο δίκαιο. Σε περίπτωση που δεν συμφωνηθεί ρητά αυτό στην έξυπνη σύμβαση, ο εν λόγω Κανονισμός έχει μια σειρά ρυθμίσεων, ώστε να καλύπτεται κάθε είδους σύμβαση (αγορά-πώληση αγαθών υπηρεσιών, σύμβαση χρηματοπιστωτικών μέσων, σύμβαση ασφάλισης κλπ).

[166] Κανονισμός Ρώμη Ι

Κατά κανόνα, θεωρείται ως εφαρμοστέο δίκαιο της χώρας, στην οποία ο πωλητής ή πάροχος των υπηρεσιών έχει τη συνήθη διαμονή του ή το δίκαιο της χώρας που βρίσκεται το πωλούμενο ή μίσθιο ακίνητο[167].

3.6.1.Β. Εξωσυμβατικές Ενοχές-Κανονισμός "Ρώμη ΙΙ"

Αντιστοίχως, έχει θεσμοθετηθεί ένα πλαίσιο και για τις εξωσυμβατικές ενοχές. Ο Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Ιουλίου, υπ΄αριθμ. 864/2007 ("Ρώμη ΙΙ") ρυθμίζει ζητήματα αδικαιολόγητου πλουτισμού, αδικοπραξιών, διοίκησης αλλοτρίων και αθέμιτου ανταγωνισμού.

Στον Κανονισμό αυτό, βασικός κανόνας περί εφαρμοστέου δικαίου, εισάγεται στο άρθρο 4, κατά το οποίο εφαρμόζεται το δίκαιο της χώρας στην οποία επήλθε ζημία, ανεξάρτητα από την χώρα στην οποία έλαβε χώρα το ζημιογόνο γεγονός.

Κατά συνέπεια, οι διαφορές που προκύπτουν από έξυπνες συμβάσεις, συναπτόμενες μεταξύ ευρωπαίων χρηστών, μπορούν να προσεγγιστούν και να επιλυθούν με τους Κανονισμούς Ρώμη Ι & ΙΙ, που δημιουργούν ένα πλαίσιο προσαρμογής και αντίδρασης ανάλογα με τη φύση της εκάστοτε σύμβασης. Ωστόσο, κάτι τέτοιο δεν μπορεί να εφαρμοστεί για συμβάσεις με διεθνή χαρακτήρα, ελλείψει διεθνών ενιαίων νομοθετημάτων, ώστε να υπάρξει αναλογική εάν όχι παράλληλη εφαρμογή αυτών.

3.6.1.Γ. Ευρωπαϊκή Πράξη για τα Δεδομένα

Το Ευρωπαϊκό Κοινοβούλιο ακολουθώντας τις τεχνολογικές εξελίξεις εξέδωσε το Ψήφισμα της 3ης Οκτωβρίου 2018 σχετικά με τις τεχνολογίες DLT (κατανεμημένου καθολικού) και το σύστημα blockchain. Εν συνεχεία, η Ευρωπαϊκή Επιτροπή ανέλαβε την ευθύνη της διεξαγωγής μιας εμπεριστατωμένης αξιολόγησης των νομικών συνεπειών από τη χρήση αυτών των τεχνολογιών καθώς και την εφαρμογή των έξυπνων συμβάσεων.

Πιο συγκεκριμένα, η Ευρωπαϊκή Επιτροπή δεσμεύτηκε ως προς την εναρμόνιση και την πιστοποίηση των τεχνολογιών αυτών καθώς και τη δημιουργία κατάλληλων κανόνων δίκαιης χρήσης και πρόσβασης στα δεδομένα. Πρόκειται για την Πράξη για τα Δεδομένα [168] [169], στην

[167] Κανονισμός Ρώμη Ι, άρθρα 5-8

[168] https://ec.europa.eu/commission/presscorner/detail/el/ip_22_1113

[169] Πρόταση: ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

οποία περιλαμβάνονται ρυθμίσεις για την προώθηση της διαλειτουργικότητας των έξυπνων συμβολαίων μεταξύ επιχειρήσεων και φυσικών προσώπων (άρθρο 30 "Βασικές απαιτήσεις σχετικά με τις έξυπνες συμβάσεις για την κοινοχρησία δεδομένων")[170].

Περαιτέρω, η συγκεκριμένη Πρόταση Κανονισμού προβλέπει ανάλογες υποχρεώσεις προς συμμόρφωση των παρόχων έξυπνων νομικών συμβάσεων, έχοντας υπ΄όψιν τον Κανονισμό 1025/2012 περί ευρωπαϊκής τυποποίησης[171]. Σε περίπτωση πλημμελούς συμμόρφωσης των προμηθευτών έξυπνων συμβάσεων, στοιχειοθετείται δικαίωμα καταγγελίας και αποζημίωσης υπερ των πελατών, στο αντίστοιχο εθνικό δίκαιο των κρατών μελών.

3.6.2. Ελληνική Νομοθεσία

Ο πρόσφατος νόμος 4961/2022 (ΦΕΚ Α 46, 27/07/2022)[172] για τις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών και την ηλεκτρονική διακυβέρνηση περιέχει καινοτόμες ρυθμίσεις. Το εν λόγω νομοθέτημα περιέχει μεταξύ άλλων ρυθμιστικές διατάξεις για τις τεχνολογίες κατανεμημένου καθολικού (ΤΚΚ) και τα έξυπνα συμβόλαια, την τεχνητή νοημοσύνη καθώς και το διαδίκτυο των πραγμάτων.

Στην εισηγητική έκθεση του συγκεκριμένου νόμου προσδιορίζονται i) οι προϋποθέσεις εγκυρότητας εγγραφής μιας συναλλαγής σε μια εφαρμογή blockchain και εν γένει σε ένα δίκτυο DLT, ii) προϋποθέσεις κατάρτισης, κύρους και απόδειξης των έξυπνων νομικών συμβάσεων, με ανάλογη εφαρμογή των διατάξεων του Αστικού Κώδικα και της Πολιτικής Δικονομίας . Περαιτέρω δε, σύμφωνα με τον ΑΚ , το blockchain μπορεί -με τις κατάλληλες νομοθετικές ρυθμίσεις-να αποτελέσει σύννομη υποδομή για τη σύναψη έξυπνων συμβολαίων.

Στο άρθρο 31 δίνεται ο ορισμός του έξυπνου συμβολαίου σε μία προσπάθεια αναγνώρισης της αλγοριθμικής σύναψης συμβάσεων σε υποδομή DLT. Πρόκειται για μία έκφανση της συμβατικής ελευθερίας (ΑΚ 361) καθώς και του άτυπου των δικαιοπραξιών (ΑΚ 158),

---

για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους (Πράξη για τα δεδομένα)
https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0068

[170] https://www.europarl.europa.eu/doceo/document/A-9-2023-0031_EL.html

[171] ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) αριθ. 1025/2012 Του Ευρωπαϊκου Κοινοβουλίου Και Του Συμβουλίου της 25ης Οκτωβρίου 2012
https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32012R1025

[172] https://www.ey.com/el_gr/tax/tax-alerts/l-4961-2022-the-greek-legal-framework-on-emerging-technologies

εκφράζοντας ποικιλοτρόπως το δικαίωμα στην ιδιωτική αυτονομία, στην ελεύθερη ανάπτυξη της προσωπικότητας, στην οικονομική ελευθερία, που έχουν κατοχυρωθεί συνταγματικά.

3.6.3. Δικαιοδοσία των Έξυπνων Συμβάσεων

Η επίλυση των διαφορών που ανακύπτουν από τις έξυπνες νομικές συμβάσεις μπορεί να γίνει είτε εξωδικαστικά είτε δικαστηριακά. Σε κάθε περίπτωση, υπάρχουν πλεονεκτήματα και μειονεκτήματα τα οποία συνυπολογίζονται ανάλογα τη φύση της διαφοράς.

Εξωδικαστική επίλυση-Διαιτησία

Η διαιτησία, ως μέσο επίλυσης διαφορών από έξυπνες νομικές συμβάσεις, παρουσιάζει αρκετά πλεονεκτήματα, όσον αφορά την ταχύτητα, το κόστος και την αποτελεσματικότητα. Ειδικότερα, τα πλεονεκτήματα αυτά αποκτούν μεγαλύτερη αξία σε συνάρτηση με τις ιδιαιτερότητες του blockchain (διασυνοριακός χαρακτήρας, ανωνυμία διαδίκων, εφαρμοστέο δίκαιο). Πλέον, πολλές συμβάσεις στο Meta Universe ενσωματώνουν ρήτρες διαιτησίας (Axie Infinity, Decentraland, Somnium)[173].

Δικαστική Επίλυση Διαφορών

Αντίθετα με την διαιτησία, η δικαστική οδός είναι χρονοβόρα και δαπανηρή. Όσον αφορά την ερμηνεία των συμβάσεων, ενδεχομένως να διαφέρει τόσο ανάλογα τη φύση της (νομική, τεχνική, μεικτή) όσο και από την εμπειρία του κρίνοντος δικαστή σε αυτά τα ζητήματα. Μέχρι σήμερα, δεν υπάρχει νομολογία, πέραν ελαχίστων εξαιρέσεων για ζητήματα πνευματικής ιδιοκτησίας. Για το λόγο αυτό, η ανάλυση που ακολουθεί βασίζεται σε άρθρα και πιθανές προβλέψεις.

Βασικό ζήτημα για την δικαστική επίλυση αποτελεί η ερμηνεία της εκάστοτε σύμβασης. Ενδεχομένως, τα περισσότερα και δυσχερέστερα προβλήματα να ανακύψουν στις μεικτές συμβάσεις, ήτοι σε αυτές που συνδυάζουν κώδικα και νόμο. Οι εν λόγω συμβάσεις πέρα από την δυσκολία ανάγνωσης και κατανόησης τους λόγω του ότι είναι γραμμένες σε κώδικα, πιθανόν να είναι και δυσερμήνευτες ως προς την πραγματική βούληση των μερών. Στις παραδοσιακές

[173] Κανέλλος Λ.,"Smart Contracts: Νομικές Προκλήσεις και επιχειρηματικές προοπτικές", 2022, Νομική Βιβλιοθήκη

συμβάσεις, εάν δεν προκύπτει από το συμβατικό κείμενο η βούληση των μερών, συνάγεται από εξωτερικούς παράγοντες και από ερμηνευτικούς κανόνες των δικαιοπραξιών (ΑΚ 173, 200). Στις μεικτές συμβάσεις, αυτή η προσέγγιση είναι σχεδόν αδύνατη, λόγω της αιτιοκρατικής δομής των προγραμμάτων υπολογιστή, ήτοι η εισαγωγή παρόμοιων δεδομένων εξάγει παρόμοια αποτελέσματα, που βασίζονται σε εντολές γλώσσας προγραμματισμού. Απόρροια αυτού είναι η αδυναμία ερμηνείας ή αναζήτησης νοήματος και εφαρμοστέου δικαίου[174].

Περαιτέρω δε, σε ένα πρωτόκολλο λογισμικού δεν μπορεί να γίνει συστηματική, γραμματική ή τελολογική ερμηνεία, δεδομένης της έλλειψης ενιαίων νομοθετημάτων, ώστε να γίνει ανάλογη υπαγωγή. Αντιστοίχως, δυσκολία ανακύπτει και ως προς την κατανομή της ευθύνης (ενδοσυμβατική ευθύνη) στις περιπτώσεις πλημμελούς εκπλήρωσης των υποχρεώσεων.

Σε αυτό το σημείο, δέον να επισημανθεί πώς το προτέρημα της μη τροποποίησης των συμβάσεων μπορεί να αποτελέσει τροχοπέδη στη νομική έκβαση και αξιολόγηση δεδομένου ότι δεν θα μπορούν να προσαρμοστεί η σύμβαση σε μία πιθανή μεταβολή συνθηκών ή γεγονότα ανωτέρας βίας ή οτιδήποτε άλλο που θα οδηγούσε σε τροποποίηση ή αναστολή της σύμβασης.

4. Ηλεκτρονική Υπογραφή

Η ηλεκτρονική υπογραφή είναι απόρροια της εξέλιξης της τεχνολογίας και των συναλλακτικών αναγκών. Πρόκειται για ένα μέσο ηλεκτρονικής ταυτοποίησης προκειμένου να διασφαλιστεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές. Επιπλέον, αποτελεί το μέσο αποδοχής του περιεχομένου των ψηφιακών εγγράφων, μέσω των οποίων δημιουργούνται ψηφιακές συμβατικές σχέσεις εξ αποστάσεως.

Η έννοια της ψηφιακής υπογραφής εκφράστηκε πρώτη φορά το 1976 από τους Whitfield Diffie και Martin Hellman, περιγράφοντας την ως σχέδιο ψηφιακής απεικόνισης, υποθέτοντας ότι πρόκειται για σχήματα που βασίζονται σε συναρτήσεις μετατροπών μονής κατεύθυνσης[175], θέτοντας κατά αυτόν τον τρόπο τα θεμέλια της συμμετρικής κρυπτογραφίας. Μετέπειτα ακολούθησαν οι Ronald Rivest, Adi Shamir, Len Adleman, οι οποίοι εφηύραν τον αλγόριθμο

[174] Di Angelo M., "Smart Contracts in view of Civil Code", 2019

[175] Πρόκειται για τη Συμμετρική Κρυπτογραφία. Ειδικότερα: https://www.techtarget.com/searchsecurity/definition/Diffie-Hellman-key-exchange#:~:text=Diffie%2DHellman%20key%20exchange%20is,encrypt%20and%20decrypt%20their%20messages.

RSA, ο οποίος χρησιμοποιήθηκε για την παραγωγή των πρώτων ψηφιακών υπογραφών. Οι υπογραφές αυτές χαρακτηρίστηκαν ως "απλές υπογραφές RSA" [176] λόγω της πρωτόγονης δομής τους καθώς και του χαμηλού επιπέδου ασφάλειας που παρέχουν[177]. Σε αυτό το σημείο αξίζει να σημειωθεί πώς το πρώτο λογισμικό ψηφιακής υπογραφής κυκλοφόρησε το 1989 και ήταν το Lotus Notes 1.0[178] [179], που βασίζεται στον αλγόριθμο RSA[180]. Εν συνεχεία, το σύστημα RSA διαδέχθηκαν πολλά συστήματα ψηφιακής υπογραφής, όπως οι υπογραφές Lamport, τα δέντρα Merkle (hash tree που λειτουργούν ως υπογραφές) και οι υπογραφές Rabin. Το 1995, οι Shafi Goldwasser, Silvio Micali και Ronald Rivest, περιγράφοντας ένα ιεραρχικό μοντέλο επίθεσης για τα σχήματα υπογραφής[181], δημιούργησαν ένα αυστηρό πλαίσιο ασφάλειας των συστημάτων ψηφιακής υπογραφής[182], το οποίο στη συνέχεια αποτέλεσε το θεμέλιο λίθο και για τα λοιπά συστήματα ψηφιακής υπογραφής.

Σύμφωνα με τη θεωρία, η ηλεκτρονική υπογραφή αποτελεί μέθοδο τεκμηρίωσης και εφαρμόζεται σε συγκεκριμένες μηχανικές απεικονίσεις προκειμένου να διασφαλίσει, κατά πρώτον την γνησιότητα και την ακρίβεια της δήλωσης βουλήσεως και σε συνέχεια αυτού την ταυτότητα του προσώπου που προβαίνει στην συγκεκριμένη δήλωση [183]. Από την άποψη αυτή, συνάγεται πως κατ΄ουσίαν πρόκειται για μία "κατ΄ευφημισμό" υπογραφή, καθώς αποκρυσταλλώνεται μια διαδικασία τεκμηρίωσης. Επομένως, υπάρχουν πολλές μορφές ηλεκτρονικής υπογραφής μέσω της οποίας κάποιος είτε δεσμεύεται ως προς το περιεχόμενο είτε

---

[176] Δέον να διευκρινιστεί ότι: Ο αλγόριθμος RSA μπορεί να κάνει και τα τρία: Κρυπτογράφηση, ανταλλαγή κλειδιών και υπογραφές. Ο αλγόριθμος Diffie-Hellman (DH) μπορεί να χρησιμοποιηθεί μόνο ως ανταλλαγή κλειδιών. Ο αλγόριθμος ψηφιακής υπογραφής (DSA) μπορεί να χρησιμοποιηθεί μόνο για υπογραφές.

[177] https://www.rapid7.com/blog/post/2017/08/28/rsa-rivest-shamir-and-adleman/

[178] https://www.stellarinfo.com/blog/complete-history-ibm-lotus-notes-hcl-notes/

[179]https://www.slideshare.net/edbrill/lotusphere-2010-an-oral-history-of-ibm-lotus-notes-first-20-years/4-Lotus_Notes_10_1989_of

[180] Lincoln A., "Electronic signature laws and the need for uniformity in the global market, 2004

[181] Goldwasser S., Micali S., Rivest R. L., " A digital signature scheme secure against adaptive chosen-message attacks", 1995

[182] Το GMR υποσχόταν αναγνώριση και αποκλεισμό της πλαστογραφίας έναντι επιλεγμένων μηνυμάτων. Πιο συγκεκριμένα η ασφάλεια του συστήματος σχετίζεται με τη δυσκολία παραγοντοποίησης πολύ μεγάλων αριθμών. Όμως, σε αντίθεση με τον RSA, ο GMR είναι ασφαλής έναντι των επιθέσεων προσαρμοστικής επιλογής μηνύματος, που είναι ο αποδεκτός σήμερα ορισμός ασφάλειας για τα συστήματα υπογραφών - ακόμη και όταν ένας επιτιθέμενος λαμβάνει υπογραφές για μηνύματα της επιλογής του, αυτό δεν του επιτρέπει να πλαστογραφήσει μια υπογραφή για ένα μόνο πρόσθετο μήνυμα.

[183] Καράκωστας Ι., "Δίκαιο και Ίντερνετ, Νομικά Ζητήματα του Διαδικτύου", σελ 137, 2009

επιβεβαιώνει την ταυτότητα του. Σε αυτό το σημείο, δέον να επισημανθεί πώς μέσω αυτής της μη περιοριστικής προσέγγισης συνδυάζεται τόσο η τεχνική ουδετερότητα και προσαρμοστικότητα απέναντι σε μελλοντικές προκλήσεις όσο και η τήρηση των ήδη υφιστάμενων μορφών υπογραφής.

4.1. Είδη Ηλεκτρονικής Υπογραφής

Ο Κανονισμός eIDAS (EU Regulation 910/2014) στο άρθρο 3, περιγράφει τρεις τύπους ηλεκτρονικών υπογραφών[184] : i) την απλή ηλεκτρονική υπογραφή[185], ii) την προηγμένη ηλεκτρονική υπογραφή[186] και iii) την εγκεκριμένη ηλεκτρονική υπογραφή[187]. Σύμφωνα με τα άρθρα 3 παρ. 12 και 25 παρ. 2 του Κανονισμού, η εγκεκριμένη ηλεκτρονική υπογραφή *«δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής» και « έχει νομική ισχύ ισοδύναμη με την ιδιόχειρη.».* Σε αυτό το σημείο διαφαίνεται ότι ο Ευρωπαίος νομοθέτης περιόρισε ex lege σε αυστηρά μια κατηγορία ηλεκτρονικής υπογραφής την ισχύ της ιδιόχειρης, εξισώνοντας αυτές τις δύο - εγκεκριμένη και ιδιόχειρη- υποστηρίζοντας την έκδοση ψηφιακών πιστοποιητικών σκληρής αποθήκευσης[188].

---

[184] Ως ηλεκτρονική υπογραφή ορίζεται το ηλεκτρονικό σύμβολο ή η διαδικασία που επισυνάπτεται ή συνδέεται λογικά με ένα συμβόλαιο ή αρχείο και εκτελείται ή υιοθετείται από ένα άτομο που έχει πρόθεση να υπογράψει το αρχείο.

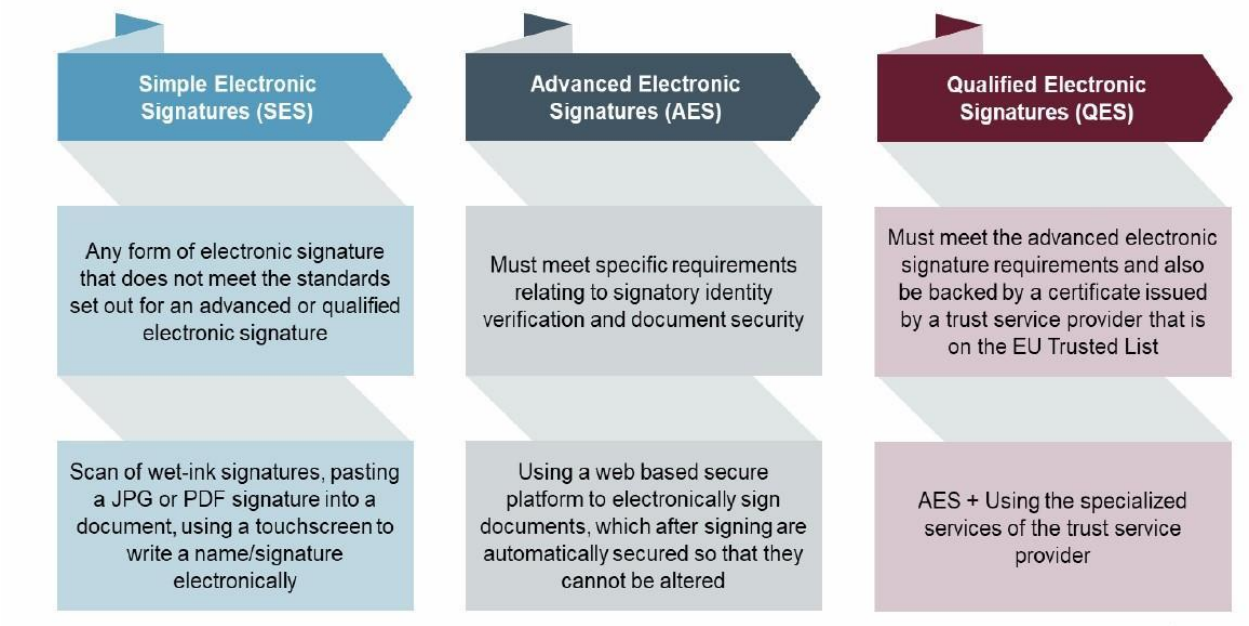
[185] eIDAS άρθρο 3 εδ 10: απλές ηλεκτρονικές υπογραφές είναι δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον γράφοντα για να υπογράψει.

[186] eIDAS άρθρο 3 εδ 11: προηγμένες ηλεκτρονικές υπογραφές είναι δεδομένα που συνδέονται με απλό τρόπο με τον υπογράφοντα, βάσει δεδομένων υπογραφής που τελούν υπό τον αποκλειστικό του έλεγχο, υποστηρίζονται δε από ένα ψηφιακό πιστοποιητικό.

[187] eIDAS άρθρο 25 παρ 2: εγκεκριμένες ηλεκτρονικές υπογραφές είναι ισοδύναμες με χειρόγραφες. Έκαστη τέτοια υπογραφή δημιουργείται από μία εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής, παρέχει σύνδεση με μοναδικό τρόπο με τον υπογράφοντα, βάσει δεδομένων υπογραφής υπό τον αποκλειστικό του έλεγχο, η οποία βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής.

[188] Ζέκος Γ.,"Διαδίκτυο & Τεχνητή Νοημοσύνη στο Ελληνικό Δίκαιο", 2022 (σλ 155)

Ειδικότερα, από τον συνδυασμό των διατάξεων του Κανονισμού eIDAS και του άρθρου 2 του ν.4727/2020[189] προκύπτει ότι η εγκεκριμένη ηλεκτρονική υπογραφή είναι ένα κρυπτογραφημένο σύνολο αριθμών και χαρακτήρων που δημιουργείται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης συνδέοντας με μοναδικό τρόπο την υπογραφή με το πρόσωπο που υπογράφει. Η εν λόγω υπογραφή χρησιμοποιεί εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής, το οποίο εκδίδεται από τον εθνικά αναγνωρισμένο εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), η οποία είναι εγγεγραμμένη στην Λίστα Εμπιστοσύνης της Ευρωπαϊκής Ένωσης[190].



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

[189] Ο νόμος 4727/2020 ενσωμάτωσε τον Κανονισμό eIDAS και κατήργησε το ΠΔ 150/2001

[190] https://www.eett.gr/parochoi/ilektronikes-epikoinonies/ypiresies-empistosynis/genikes-plirofories/katalogos-empisteysis-egkekrimenon-parochon-ypiresion-empistosynis-trusted-list/

4.2. Τύπος και (Ηλεκτρονική) Υπογραφή

Το δίκαιο των συμβάσεων διέπεται από μια θεμελιώδη αρχή, την Αρχή του Ατύπου των Δικαιοπραξιών (ΑΚ 158). Η εν λόγω Αρχή εκφράζει ότι δεν απαιτείται κατ΄ αρχήν η τήρηση τύπου ως συστατικού στοιχείου μιας σύμβασης για την εγκυρότητα αυτής, αλλά απαιτείται μόνο όταν το ορίζει ο νόμος. Στις περιπτώσεις αυτές, κατά τις οποίες η τήρηση του τύπου αποτελεί απαραίτητο στοιχείο για την κατάρτιση μιας δικαιοπραξίας, γίνεται λόγος για "συστατικό τύπο".

Ο συστατικός τύπος, με τον οποίο καλύπτεται η απαίτηση του νόμου για εξωτερίκευση των δηλώσεων βουλήσεως για την εγκυρότητα μιας δικαιοπραξίας[191], χωρίζεται σε τρεις κατηγορίες: i) ιδιωτικό έγγραφο (ΑΚ 849)[192]. ii) συμβολαιογραφικό έγγραφο (ΑΚ 1033) και iii) δήλωση ενώπιον της Αρχής (ΑΚ 1505). Στο πλαίσιο της παρούσας εργασίας, δεν θα εξετάσουμε την τρίτη κατηγορία (¨δήλωση ενώπιον της Αρχής¨) αλλά θα γίνει μνεία μόνο στις δύο πρώτες, σε συνάρτηση με τις έξυπνες συμβάσεις. Το ιδιωτικό έγγραφο θα εξεταστεί λεπτομερώς κατωτέρω, ωστόσο για το συμβολαιογραφικό έγγραφο αρκεί να υπογραμμισθεί ότι με τα σημερινά νομοθετικά δεδομένα δεν μπορεί να καταρτιστεί ηλεκτρονικά δικαιοπραξία[193].

4.3. Ηλεκτρονικά Έγγραφα και Υπογραφή αυτών - Έξυπνες Συμβάσεις

Οι έξυπνες συμβάσεις πραγματώνονται στο διαδίκτυο μέσω υπολογιστικού συστήματος[194] και εξ αυτού του λόγου μπορούν να θεωρηθούν ηλεκτρονικά έγγραφα που ρυθμίζονται από τον Κανονισμό eIDAS[195]. Ειδικότερα, στο άρθρο 3 περίπτωση 35 του eIDAS δίνεται ο ορισμός του ηλεκτρονικού εγγράφου *"οποιοδήποτε περιεχόμενο έχει αποθηκευτεί σε ηλεκτρονική μορφή και ειδικότερα ως κείμενο ή με ηχητική, οπτική ή οπτικοακουστική εγγραφή"*. Για το λόγο αυτό, θα εξετάσουμε το ιδιωτικό έγγραφο και το συμβολαιογραφικό έγγραφο στο πλαίσιο τήρησης του

---

[191] Γεωργιάδης Α., "Γενικές Αρχές Αστικού Δικαίου", 2019

[192] Παραδείγματα ιδιωτικών εγγράφων: α) βιβλία που οι έμποροι και επαγγελματίες τηρούν κατά τον εμπορικό νόμο ή άλλες διατάξεις, β) και γ) φωτογραφίες ή κινηματογραφικές αναπαραστάσεις, φωνοληψίες και κάθε άλλη μηχανικη απεικόνιση (ΚΠολΔ 444)

[193] Σπυριδάκης Ι., "Γενικές Αρχές Αστικού Δικαίου", σελ 929, 2022.

[194] Παπαδημόπουλος Ι., "Η δογματική ένταξη των smart contracts στο δίκαιο των συμβάσεων", σελ 469, 2020, ΧρΙΔ

[195] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910

νόμιμου συστατικού τύπου κατά την κατάρτιση μιας έξυπνης σύμβασης και ειδικότερα σε ό,τι αφορά στην υπογραφή αυτών.

Ιδιωτικό Έγγραφο

Ειδικότερα, το ιδιωτικό έγγραφο φέρει την μορφή γραπτού κειμένου και κατά τις συναλλακτικές αντιλήψεις λογίζεται ως έγγραφο που εκφράζει τη δήλωση βουλήσεως του συμβαλλομένου. Αυτό κρίνεται και επικυρώνεται, εάν το έγγραφο φέρει την ιδιόχειρη υπογραφή του εκδότη (ΑΚ 160 παρ 1), *ήτοι του προσώπου που προβαίνει στη δήλωση βουλήσεως που περιέχει το έγγραφο*[196] . Αντίστοιχη περίπτωση των ιδιωτικών εγγράφων αποτελούν τα ηλεκτρονικά έγγραφα, που η υπογραφή θεωρείται απαραίτητο στοιχείο εγκυρότητας και γνησιότητας αυτών. Στο πλαίσιο αυτό, αναπτύχθηκε η ηλεκτρονική υπογραφή προκειμένου να διαπιστώνεται η εγκυρότητα και να αποφεύγεται οποιαδήποτε αλλοίωση του περιεχομένου. Ειδικότερα, η εγκεκριμένη ηλεκτρονική υπογραφή εξομοιούται με την ιδιόχειρη. Πιο συγκεκριμένα, όπως ορίζει το άρθρο 15 παρ 2 εδ 1 *"Στην περίπτωση του 160 ΑΚ και του άρθρου 443 ΚΠολΔ απαιτείται εγκεκριμένη ηλεκτρονική υπογραφή ή εγκεκριμένη ηλεκτρονική σφραγίδα."*. Ωστόσο, ενδέχεται να ανακύψουν ζητήματα αποδεικτικής ισχύς.

Πιο συγκεκριμένα, η νομικής ισχύς και το παραδεκτό της ηλεκτρονικής υπογραφής, δεν μπορούν να απορριφθούν λόγω της ηλεκτρονικής μορφής ή εξαιτίας των ελλείψεων των στοιχείων της εγκεκριμένης υπογραφής (άρθρο 25 του eIDAS). Εξ αυτού προκύπτει ότι οι έξυπνες συμβάσεις που είναι υπογεγραμμένες με απλή ή προηγμένη ηλεκτρονική υπογραφή, εκτιμώνται ελεύθερα από το δικαστήριο. Προς επίρρωση αυτού, παρατίθεται και το αντίστοιχο άρθρο 15 παρ 2 εδ 2 του ν. 4727/2020, σύμφωνα με το οποίο *"Ηλεκτρονικά έγγραφα με απλή ή προηγμένη ηλεκτρονική υπογραφή εκτιμώνται ελεύθερα ως νόμιμα αποδεικτικά μέσα κατά τις ισχύουσες δικονομικές διατάξεις."*.

Από τα ανωτέρω, γεννάται το ερώτημα, εάν οι έξυπνες συμβάσεις μπορούν να υπογραφούν με εγκεκριμένη ηλεκτρονική υπογραφή προκειμένου να έχουν την αυξημένη αποδεικτική ισχύ της ιδιόχειρης υπογραφής. Η απάντηση ποικίλει ανάλογα με τον τύπο εκάστου blockchain. Πιο συγκεκριμένα, στα ανοικτά δίκτυα, καλύπτονται σωρευτικά τα τρία εκ των τεσσάρων κριτηρίων της υπογραφής, ήτοι i) η μοναδική δημιουργία από ειδική συσκευή, ii) η προαναφερθείσα συσκευή βρίσκεται στην κατοχή του υπογράφοντος και iii) γίνεται αποκλειστική και μοναδική

[196] Γεωργιάδης Α., "Γενικές Αρχές Αστικού Δικαίου", 2019

σύνδεση του περιεχομένου με τον υπογράφοντα. Ωστόσο, η μη συνδρομή του τέταρτου κριτηρίου, ήτοι η έλλειψη ενός κεντρικού διαχειριστή που θα ελέγχει την πηγή του εκάστοτε ψηφιακού πιστοποιητικού από κάποιον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης της ΕΕ[197], με αποτέλεσμα να καθίσταται αδύνατη η πιστοποίηση της ταυτότητας του υπογράφοντος στις έξυπνες συμβάσεις[198].

Επομένως, η ηλεκτρονική υπογραφή αποτελεί ένα μέσο τεκμηρίωσης με ηλεκτρονικό τρόπο κατά τον οποίο χρησιμοποιούνται συγκεκριμένες μηχανικές απεικονίσεις (εγγραφές δεδομένων σε μαγνητικά μέσα Η/Υ), προκειμένου να διασφαλιστεί η γνησιότητα της δήλωσης βουλήσεως καθώς και η ταυτότητα του προσώπου που την εκφράζει[199]. Ωστόσο, αναφορικά με τα έξυπνα συμβόλαια, πρέπει να γίνει η εξής διάκριση: έξυπνες συμβάσεις συναπτόμενες σε ανοιχτό και σε ιδιωτικό ή κοινοπρακτικό δίκτυο blockchain. Στα ανοιχτά δίκτυα blockchain δεν είναι εφικτό να τεθεί εγκεκριμένη εφαρμογή. Αντίθετα, στα ιδιωτικά ή κοινοπρατικά δίκτυα, πληρούται το τέταρτο κριτήριο (ήτοι της πιστοποίησης της ταυτότητας του υπογράφοντος), επειδή υπάρχει δυνατότητα να ελεγχθεί η προέλευση του ψηφιακού πιστοποιητικού. Πιο συγκριμένα, στα ιδιωτικά δίκτυα πχ τραπεζών ή οργανισμών καθίσταται εφικτή η πιστοποίηση της σχέσης μεταξύ υπογράφοντος και υπογραφής[200] και για το λόγο αυτό, μπορεί να τεθεί εγκεκριμένη ηλεκτρονική υπογραφή στα έξυπνα συμβόλαια.

4.4. Κρυπτογραφία και Ηλεκτρονική Υπογραφή

Έκαστο μέρος μιας έξυπνης σύμβασης κατέχει ένα ζεύγος κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί είναι γνωστό σε όλους προκειμένου να εκκινήσει η διαδικασία των διαπραγματεύσεων. Αντιθέτως, το ιδιωτικό κλειδί -ως μυστικό κλειδί- χρησιμοποιείται για την υπογραφή έκαστης σύμβασης και την ολοκλήρωση έκαστης συναλλαγής. Επομένως, κρίνεται σκόπιμο να εξεταστεί εάν η χρήση του κρυπτογραφικού κλειδιού σε ένα έξυπνο συμβόλαιο μπορεί να εξομοιωθεί με τις ηλεκτρονικές υπογραφές του eIDAS.

---

[197] Παράρτημα ΙΙ Κανονισμού eIDAS

[198] Κανέλλος Λ., "Smart Contracts: Νομικές Προκλήσεις και επιχειρηματικές προοπτικές", σελ 155-157, 2022, Νομική Βιβλιοθήκη,

[199] Παπαστερίου Δ., Κλαβανίδου Δ., "Δίκαιο της δικαιοπραξίας", 2008

[200] The European Union Blockchain Observatory And Forum - Blockchain and digital Identity https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Σε ένα δίκτυο blockchain οι λογαριασμοί ανταλλάσσουν μεταξύ τους δεδομένα σε ηλεκτρονική μορφή προκειμένου να επιτευχθεί μια συναλλαγή. Αντιστοίχως, όταν τα μέρη συνάπτουν νομικά δεσμευτικές συμβάσεις σε περιβάλλον blockchain, η πρόταση του ενός μέρους εκφράζεται μέσω της μεταφόρτωσης του έξυπνου συμβολαίου στην αλυσίδα των blocks και η αποδοχή επιτυγχάνεται με την αποστολή μιας συναλλαγής στον λογαριασμό του έξυπνου συμβολαίου. Επομένως, προκύπτει ότι ο κώδικας της έξυπνης σύμβασης προστίθεται στο blockchain και αντιστοιχίζεται με την διεύθυνση ενός λογαριασμού. Εξετάζοντας τα προαναφερθέντα, συνάγεται ότι το ιδιωτικό κλειδί του προτείνοντος συνδέεται με κάποιες συναλλαγές και εγκρίνονται οι πληροφορίες που περιλαμβάνονται στα τελευταία δεδομένα. Οι εν λόγω συναλλαγές υπογράφονται με ιδιωτικά κλειδιά αξιοποιώντας υποδομή δημοσίων κλειδιών. Επομένως. οι υπογραφές αυτές μπορούν να εξομοιωθούν με απλές ηλεκτρονικές υπογραφές.

Ωστόσο, προκειμένου οι ηλεκτρονικές υπογραφές να θεωρηθούν εγκεκριμένες, σύμφωνα με τα όσα ορίζει ο eIDAS, απαιτείται η χρήση μιας εγκεκριμένης συσκευής δημιουργίας υπογραφών και ένα εγκεκριμένο πιστοποιητικό. Επομένως. προκειμένου να εξομοιωθούν τα κρυπτογραφικά κλειδιά με εγκεκριμένες υπογραφές απαιτούνται σωρευτικά τα εξής: α) το ‘πορτοφόλι” των κλειδιών κρυπτογράφησης-αποκρυπτογράφησης να διασφαλίζει την εμπιστευτικότητα και την ασφάλεια των δεδομένων για την δημιουργία της υπογραφής και β) να δημιουργηθεί ένα πιστοποιητικό που θα πληροί όλες τις απαιτήσεις του eIDAS, ήτοι την έκδοση από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, ο οποίος θα ελέγχει την σύνδεση μεταξύ της ταυτότητας έκαστου χρήστη καθώς και των κλειδιών που χρησιμοποιεί.

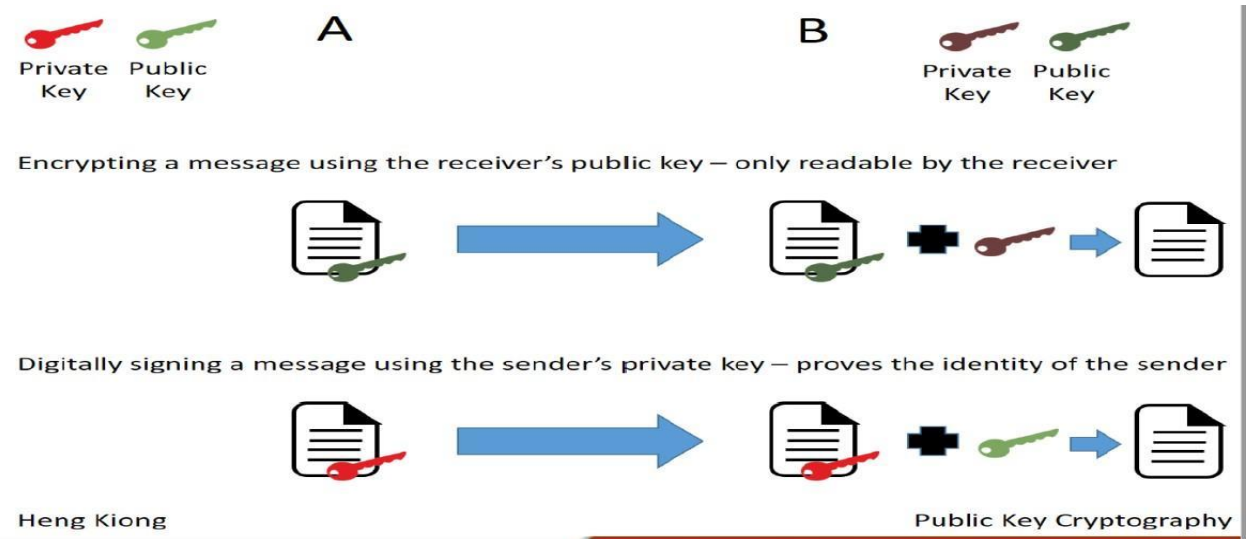
Από τα προαναφερθέντα συνάγεται το συμπέρασμα, ότι η απουσία παρόχου εμπιστοσύνης στο δίκτυο blockchain συνιστά τροχοπέδη[201] στην ανάπτυξη των έξυπνων νομικών συμβάσεων. Πιο συγκεκριμένα, μια κεντρική αρχή ελέγχου και ταυτοποίησης των υπογραφών και των μερών που τις φέρουν, θα αντίκειτο στη βασική αρχή του blockchain, το οποίο χαρακτηρίζεται ως αποκεντρωμένο σύστημα, βασιζόμενο αποκλειστικά στους χρήστες του. Επομένως, λαμβάνοντας υπόψη τα ως άνω, παρατηρούμε ότι το συγκεκριμένο πρόβλημα είναι σχεδόν αδύνατο να ξεπεραστεί, με αποτέλεσμα να δημιουργείται μερική συμβατότητα μεταξύ της τεχνολογίας DLT και του eIDAS. Πιο συγκεκριμένα, το blockchain είναι συμβατό με απλές και προηγμένες υπογραφές αλλά μέχρι σήμερα όχι τις εγκεκριμένες. Ωστόσο, έχει υποστηριχθεί και η αντίθετη

[201] Κανέλλος Λ., Κωνσταντινίδης Ο., “Εφαρμογές blockchain στη Νομική Πρακτική”, Διαδικτυακό Σεμινάριο της Νομικής Βιβλιοθήκης, https://www.nb.org/efarmoges-blockchain-sti-nomiki-praktiki.html

άποψη από τον Κανέλλο Λ., σύμφωνα με τον οποίο *"το εμπόδιο αυτό δεν είναι ανυπέρβλητο καθώς…το λογισμικό θα μπορούσε να βεβαιώνει ότι το ψηφιακό πιστοποιητικό προέρχεται από ένα πιστοποιημένο πάροχο, ώστε να εξομειώσει την υπογραφή του χρήστη με ιδιόχειρη".*

Συνοψίζοντας τα όσα αναφέρθηκαν σε αυτή την ενότητα, προκύπτει ότι η τεχνολογία των έξυπνων συμβάσεων δεν πληροί όλες τις προϋποθέσεις προκειμένου να τεθεί εγκεκριμένη υπογραφή, η οποία εξομοιούται με την ιδιόχειρη και θα καθιστούσε το έξυπνο νομικό συμβόλαιο, ιδιωτικό έγγραφο. Πιο συγκεκριμένα, εφόσον το ηλεκτρονικό έγγραφο δεν φέρει ιδιόχειρη υπογραφή, δεν λογίζεται και δεν εξισώνεται με ιδιωτικό έγγραφο. Ωστόσο, προκειμένου να ξεπεραστούν τα κωλύματα που γεννώνται από την κατάσταση αυτή, τα μέρη μπορούν να συμφωνήσουν στις ηλεκτρονικές συμβάσεις, ότι ένα ηλεκτρονικό έγγραφο εξισώνεται με "έγγραφο" στις μεταξύ τους σχέσεις. Στο ίδιο πλαίσιο, τα μέρη παραιτούνται αμοιβαίως από το την ένσταση ακυρότητας ελλείψει τύπου[202], κάτι που θα μπορούσε αντιστοίχως να εφαρμοστεί και στα έξυπνα συμβόλαια. Σε κάθε περίπτωση, επισημαίνεται πως τα έξυπνα συμβόλαια που δεν φέρουν ιδιόχειρη υπογραφή , αν και ελλείψει του συστατικού τύπου δεν εξομοιώνονται με ιδιωτικά έγγραφα, δεν ισχύει το ίδιο και ως προς την αποδεικτική τους δύναμη. Τα εν λόγω έγγραφα μπορούν να ληφθούν υπ΄οψιν από το δικαστήριο και να εξεταστούν ως ιδιωτικά. Προς επίρρωση αυτού, το άρθρο 51 του ν. 4961/2022 ορίζει πως "ένα έξυπνο συμβόλαιο αποτελεί έγγραφο κατά την έννοια του άρθρου 339 Κώδικα Πολιτικής Δικονομίας (ΚΠολΔ)" και παράλληλα δέχεται την εφαρμογή των άρθρων 432-465 ΚΠολΔ, τα οποία εξετάζουν τη χρήση του εγγράφου ως αποδεικτικό μέσο.

[202] Γεωργιάδης Α., "Γενικές Αρχές Αστικού Δικαίου", 2012, Π.Ν. Σάκκουλας, Αθήνα



Νομική Βιβλιοθήκη Webinar Εφαρμογές Blockchain στη Νομική Πρακτική, 2021
Λ. Κανέλλος
Ο. Κωνσταντινίδης

5. Big Data Analytics και Smart Legal Contracts

5.1. Τι είναι τα Big Data

Κάθε οργανισμός και κάθε υπηρεσία είναι πλέον μάρτυρες/αποδέκτες και διαχειριστές ενός τεράστιου όγκου δεδομένων και πληροφοριών. Πρόκειται για το φαινόμενο των Big Data, δηλαδή ενός μη μετρήσιμου και συνεχώς αυξανόμενου όγκου πληροφοριών και δεδομένων, δομημένων και μη. Τα δεδομένα αυτά μπορούν να αναλυθούν και να επεξεργαστούν κατά τρόπο με τον οποίο θα προκύπτουν νέες και σαφείς πληροφορίες, προκειμένου οργανισμοί και εταιρείες να τις αξιοποιούν στο έπακρο. Η έκρηξη αυτή των μαζικών δεδομένων μπορεί να αναλυθεί σε όγκο (δηλαδή σε bytes δεδομένων), σε ταχύτητα (δηλαδή στην ταχύτητα δημιουργίας δεδομένων) καθώς και την ποικιλία αυτών (δηλαδή ποικιλομορφία των δεδομένων).

Όταν συλλεχθούν όλα αυτά τα δεδομένα , πρέπει να αξιοποιηθούν με ενδελεχή ανάλυση αυτών. Η διαδικασία της ανάλυσης και εξαγωγής πληροφοριών είναι αντικείμενο του κλάδου των Big Data Analytics. Με τη χρήση συγκεκριμένων μεθοδολογικών και ερευνητικών τεχνικών αναλύονται οι συλλεχθείσες πληροφορίες προκειμένου να προκύψουν νέες αξιοποιήσιμες πληροφορίες και να βελτιωθεί η λήψη αποφάσεων σε ένα δεδομένο πλαίσιο. Εν προκειμένω, το πλαίσιο μπορεί να είναι οι έξυπνες νομικές συμβάσεις και ό,τι αφορά σε αυτές.

Αρχικά, συλλέγονται-χωρίς συγκεκριμένο σκοπό- τα διάφορα δεδομένα -δομημένα ή μη- και εκ των υστέρων ακολουθεί η εξαγωγή κάποιου νοήματος χωρίς ωστόσο να υπάρχει κάποια εγγενής σύνδεση των δεδομένων αυτών. Εν συνεχεία, τα δεδομένα αποθηκεύονται και ομαδοποιούνται με άλλα δεδομένα, προκειμένου μελλοντικά να μπορεί να αξιοποιηθεί έστω και μέρος αυτών. Ο μηχανισμός συλλογής και ανάλυσης (Big Data Analytics) διαρθρώνεται ως εξής: συλλογή, προετοιμασία, κωδικοποίηση/εισαγωγή, επεξεργασία, ερμηνεία/χρήση και αποθήκευση. Επιπλέον, τα ενδιαφερόμενα μέρη είναι εξίσου πολλά και ποικίλα: τα ίδια τα υποκείμενα των δεδομένων, οι δημιουργοί δεδομένων, οι τελικοί χρήστες και όλα αυτά τα μέρη σε κάθε πιθανό συνδυασμό.

Αξίζει να σημειωθεί ότι τα Big Data (ή μεγάλα δεδομένα όπως αναφέρονται καταχρηστικά στα ελληνικά) είναι μια πιο σύνθετη διαδικασία από την απλή συλλογή και διαχείριση πολλών πληροφοριών. Συγκεκριμένα, η IBM [203], το 2018, περιέγραψε τα Big Data με τα τέσσερα V

[203] IBM, " The four Vs of big data",2018 http://www.ibmbigdatahub.com/infographic/four-vs-big-data

(volume-velocity-variety-validity) [204] . Ωστόσο, υποστηρίζεται ότι υπάρχει και πέμπτο V[205], αυτό του value ήτοι της αξίας. Ειδικότερα:

- Volume (όγκος) : το τεράστιο μέγεθος των πληροφοριών που συλλέγονται
- Velocity (ταχύτητα) : πόσο γρήγορα παράγονται και πόσο διατηρούνται τα δεδομένα αυτά
- Variety (ποικιλία) : ο αριθμός των τύπων και των πηγών των δεδομένων
- Validity ή Veracity (αξιοπιστία) : η αξιοπιστία των δεδομένων που συλλέγονται και αναλύονται καθώς και η ποιότητα και η ακρίβεια αυτών
- Value (αξία)[206]: το οικονομικό όφελος των εταιρειών και των οργανισμών που τα αξιοποιούν. Ειδικότερα, αναφέρεται στην ανακάλυψη πληροφοριών και την αναγνώριση προτύπων που οδηγούν σε πιο αποτελεσματικές λειτουργίες, ισχυρότερες σχέσεις με τους πελάτες και άλλα σαφή και μετρήσιμα επιχειρηματικά οφέλη.

Τα χαρακτηριστικά αυτά σε συνδυασμό με την επιστήμη των Big Data Analytics μπορεί να ωφελήσει σε πολύ μεγάλο βαθμό κάθε κλάδο.

Είδη των Big Data και αξιοποίηση αυτών

Σε αυτό το σημείο, δέον γίνει μια ανάλυση των τύπων των Big Data, από την επεξεργασία των οποίων μπορούν να προκύψουν πολύ χρήσιμες πληροφορίες. Πιο συγκεκριμένα, υπάρχουν 5 είδη ανάλυσης των Big Data : Περιγραφικό, Διαγνωστικό, Προγνωστικό, Κανονιστικό και Γνωσιακό[207]. Κάθε φορά και ανάλογα την πληροφορία που αναζητείται γίνεται η κατάλληλη επεξεργασία, ώστε να δοθεί η κατάλληλη και ορθή απάντηση, σε ζητήματα από το τι συμβαίνει στην επιχείρησή τους έως και λύσεις ή προτάσεις για βελτίωση της πορεία δράσης προκειμένου να παρακαμφθούν ή να εξαλειφθούν μελλοντικά επιχειρηματικά ζητήματα.

Η περιγραφική (descriptive) ανάλυση χρησιμοποιείται σε περιπτώσεις που απαιτείται ανάλυση ή περιγραφή ένα ζήτημα προκειμένου να δοθεί απάντηση. Πιο συγκεκριμένα, σε ανοιχτές ερωτήσεις με τις οποίες ζητείται η περιγραφή μιας κατάστασης ή ενός γεγονότος, θα

---

[204] Nersessian D., "The law and ethics of big data analytics: A new role for international human rights in the search for global standards", 2018

[205] https://www.techtarget.com/searchdatamanagement/definition/5-Vs-of-big-data

[206] https://www.teradata.com/Glossary/What-are-the-5-V-s-of-Big-Data

[207] 5 Types of analytics: Prescriptive, Predictive, Diagnostic, Descriptive and Cognitive Analytics https://www.weirdgeek.com/2018/11/types-of-analytics/?amp

χρησιμοποιηθεί αυτή η μέθοδος. Για παράδειγμα σε μια ανοιχτή ερώτηση "τι συμβαίνει στην επιχείρησή μου;", θα αναλυθούν δεδομένα σε πραγματικό χρόνο χρησιμοποιώντας εργαλεία οπτικοποίησης[208], προκειμένου να μάθουμε από προηγούμενες συμπεριφορές και να μπορέσουμε να σκιαγραφήσουμε το πώς θα επηρεάσουν μελλοντικά οι προηγούμενες αντιδράσεις. Ωστόσο, παρότι μπορεί να δίνεται μια εικόνα για την πορεία της επιχείρησης, δεν μπορεί να εντοπίσει την αιτία της εν λόγω κατάστασης. Για το λόγο αυτό, γίνεται συνδυασμός κι άλλων ειδών ανάλυσης προκειμένου το αποτέλεσμα να είναι πλήρες.

Εν συνεχεία, εφόσον αποκτηθεί η πληροφορία για το τι συμβαίνει, συνήθως αναζητάται η αιτία. Σε τέτοιου είδους ερώτηση, απάντηση θα δοθεί μέσω της διαγνωστικής (diagnostic) ανάλυσης των δεδομένων. Για παράδειγμα σε ένα ερώτημα "Γιατί;" , πρέπει να συλλεχθούν και να επεξεργαστούν με συγκεκριμένο τρόπο οι πληροφορίες, ώστε να δοθεί μια απάντηση.

Σε αυτό το σημείο, θα γίνει αναφορά στην προγνωστική (predictive) ανάλυση των δεδομένων, διότι προκύπτουν από τον συνδυασμό και τον συγκερασμό των προγνωστικών και των διαγνωστικών δεδομένων. Ειδικότερα, η ανάλυση αυτή χρησιμοποιείται για την εύρεση απαντήσεων στο ερώτημα "τι είναι πιθανό να συμβεί στο μέλλον βάσει προηγούμενων τάσεων και μοτίβων" . Στη συγκεκριμένη ανάλυση, χρησιμοποιούνται διάφοροι αλγόριθμοι στατιστικής και μηχανικής μάθησης (ML) προκειμένου να συναχθούν συμπεράσματα και να δοθούν απαντήσεις που αφορούν το μέλλον. Δέον να επισημανθεί, πως πρόκειται για εκτιμήσεις και όχι σαφείς απαντήσεις με απόλυτη ακρίβεια, δεδομένου ότι πρόκειται για εικασίες και λαμβάνοντας υπόψη ότι θα λείπουν κάποια στοιχεία.

Στη συνέχεια, το κανονιστικό (prescriptive) μοντέλο ανάλυσης λαμβάνει τις απαντήσεις από το περιγραφικό, το διαγνωστικό και το προγνωστικό μοντέλο - που προηγήθηκαν - και αναλύοντας τα, προσδιορίζει ποια είναι η βέλτιστη πορεία ή διαδικασία που πρέπει να ακολουθηθεί προκειμένου να μην επαναληφθούν ή να εξαλειφθούν τα προβλήματα του παρελθόντος. Ένα παράδειγμα εφαρμογής που χρησιμοποιεί αυτό το μοντέλο ανάλυσης των δεδομένων είναι οι Χάρτες της Google, οι οποίοι προτείνουν την καλύτερη διαδρομή λαμβάνοντας υπόψη την απόσταση, την κίνηση και την ταχύτητα.

Το γνωσιακό (cognitive) μοντέλο ανάπτυξης συνδυάζει μια σειρά από ευφυείς τεχνολογίες όπως η τεχνητή νοημοσύνη (AI), οι αλγόριθμοι μηχανικής μάθησης (ML), η βαθιά μάθηση (DL)

[208] για παράδειγμα τα εργαλεία Google Analytics

για την εφαρμογή της ανθρώπινης νοημοσύνης για την εκτέλεση συγκεκριμένων εργασιών . Πιο συγκεκριμένα, αυτό το μοντέλο ανάλυσης των δεδομένων είναι εμπνευσμένο από τον τρόπο που ο ανθρώπινος εγκέφαλος επεξεργάζεται τις πληροφορίες, κωδικοποιεί ένστικτα, αποκτά εμπειρία στη μάθηση, εξάγει συμπεράσματα, κατανοεί λέξεις, κείμενο αλλά και το πλαίσιο αυτών. Η τεχνολογία αυτή αναπτύσσεται και εξελίσσεται με τη συνεχή αλληλεπίδραση με τον άνθρωπο.

5.2. Big Data and GDPR

Τα μεγάλα δεδομένα χαρακτηρίζονται από μαζική συλλογή μεγάλων και πολύπλοκων συνόλων δεδομένων, τα οποία δεν μπορούν να αποθηκευτούν και να επεξεργαστούν με τα παραδοσιακά μέσα που διαθέτει στην κατοχή του ο μέσος χρήστης (πχ usb stick, εξωτερικός σκληρός δίσκος, ηλεκτρονικός υπολογιστής). Τα Big Data απαιτούν υψηλή υπολογιστική ισχύ και αποθήκευση καθώς και χρήση κατανεμημένων δικτύων και υπολογιστικής νέφους (Cloud systems). Η ανάλυση των δεδομένων αυτών ανάγεται σε ανάλυση αόρατων μοτίβων δεδομένων από μεγαλύτερες κατηγορίες δεδομένων. Παραμένει άγνωστη η συσχέτιση αυτών και ο αλγόριθμος βάσει του οποίου αλληλεπιδρούν και διαμοιράζονται.

Το μέγεθος των δεδομένων που παράγονται και διαχέονται από τις τις δημόσιες υπηρεσίες, πολυάριθμους βιομηχανικούς και μη κερδοσκοπικούς τομείς, τις επιχειρήσεις και την επιστημονική έρευνα έχει αυξηθεί υπέρμετρα . Κάθε μέρα παράγονται περίπου 2,5 quintillion[209] bytes δεδομένων, με το 90% αυτών των δεδομένων που προκύπτουν στον κόσμο να είναι αδόμητα, ήτοι ακατέργαστα. Οι καθιερωμένες τεχνολογίες επεξεργασίας δεδομένων, όπως για παράδειγμα οι βάσεις δεδομένων και οι αποθήκες δεδομένων, καθίστανται ανεπαρκείς δεδομένης της ποσότητας δεδομένων που δημιουργούνται καθημερινά. Ο τεράστιος όγκος δεδομένων πρέπει να αναλύεται με επαναληπτικό, αλλά και διαχρονικό τρόπο. Στη σημερινή εποχή, υπάρχει πρόβλημα αποθήκευσης του τεράστιου όγκου δεδομένων για μεγάλους οργανισμούς, οι οποίοι λειτουργούν σε παγκόσμιο επίπεδο. Έτσι, οι οργανισμοί αυτοί έχουν στραφεί στην αποθήκευση στο Νέφος

[209] Ισούται ένα πεντάκις εκατομμύριο

(Cloud), το οποίο έχει εξαιρετικές ιδιότητες για την αποθήκευση και τη μεταφορά των δεδομένων[210] [211].

Η αποθήκευση αυτών των δεδομένων στο Νέφος (Cloud) εξαρτάται αποκλειστικά και πλήρως από μεγάλους παρόχους αποθήκευσης. Οι εν λόγω πάροχοι αποθήκευσης ενεργούν ως αξιόπιστα τρίτα μέρη, τα οποία διενεργούν συναλλαγές για την αποθήκευση, την λήψη και την αποστολή έκαστης πληροφορίας από διάφορες πηγές. Οι πληροφορίες που συνθέτουν τα Big Data αντλούνται από μέσα κοινωνικής δικτύωσης, διάφορα ιδρύματα, φορείς υγειονομικής περίθαλψης. Το παρόν μοντέλο συλλογής και επεξεργασίας πληροφοριών γεννά ποικίλα ζητήματα όπως η διαθεσιμότητα των δεδομένων, το υψηλό λειτουργικό κόστος καθώς και η ασφάλεια των δεδομένων, η οποία βρίσκεται σε άμεση συνάρτηση με την ιδιωτική ζωή και την ασφάλεια αυτής, και απαιτούν ιδιαίτερη προσοχή ιδίως συναρτώμενα με τα μεγάλα δεδομένα[212]. Ένα ακόμη στοιχείο που γεννά προβληματισμούς είναι ότι έκαστη αλυσίδα μπλοκ - με όλες τις πληροφορίες που φέρει- αναπαράγεται σε πολλούς κόμβους, και για αυτό απαιτείται μεγάλος αποθηκευτικός χωρίς να εξυπηρετείται άμεσος σκοπός, ιδίως στις περιπτώσεις που ο χρήστης δεν απαιτείται να δει κάθε αρχείο που είναι αποθηκευμένο στα blocks.

Η σχέση των Big Data και του ΓΚΠΔ είναι νεφελώδης, διότι οι απαιτήσεις του Κανονισμού έρχονται σε αντίθεση με την τεχνολογική υποδομή και τον τρόπο που λειτουργούν και συλλέγονται τα big data. Πιο συγκεκριμένα, ο ΓΚΠΔ θέτει αυστηρά όρια και συγκεκριμένους κανόνες για τη διαβίβαση των δεδομένων σε τρίτες χώρες. Αντίθετα, όλη η δομή και η τεχνολογία των Big Data στηρίζεται στην ελεύθερη και άνευ συνόρων ανταλλαγή ποικίλων δεδομένων. Από την άλλη πλευρά, ο ΓΚΠΔ έχει επεκτείνει το πεδίο προστασίας του (εξωεδαφική προστασία) όχι μόνο στους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία που είναι εγκατεστημένοι στην ΕΕ, αλλά και σε αυτούς που είναι εγκατεστημένοι εκτός ΕΕ αλλά διαχειρίζονται δεδομένα προσωπικού χαρακτήρα ευρωπαίων πολιτών [213]. Περαιτέρω δε, ο ΓΚΠΔ απαιτεί τη χορήγηση συγκατάθεσης(σαφής, ρητή και αδιαμφισβήτητη) προκειμένου να γίνει κάποια πράξη επεξεργασίας δεδομένων, με απώτερο σκοπό τον περιορισμό και την οριοθέτηση

[210] Young M., "Blockchains: The great chain of being sure about things". The Economist. , 2015. Archived from the original on 3 July 2016

[211] Morris, David Z. (15 May 2016). "Leaderless, Blockchain Based Venture Capital Fund Raises $100 Million, And Counting". 2016

[212] Vaghela A., Suthar A., " A Review of Big Data Analysis Using Smart Contracts", UGC Care Group I Listed Journal, 2020

[213] Marcelo Corrales, Mark Fenwick, Helena Haapio , " Legal Tech, Smart Contracts and Blockchain", 2019, Springer

των φορέων που συλλέγουν δεδομένα. Ωστόσο, κάτι τέτοιο ως ένα βαθμό είναι ανέφικτο με τα big data, διότι τα δεδομένα και οι πληροφορίες δεν μπορούν να ελεγχθούν απόλυτα. Πιο συγκεκριμένα, εάν όχι ολόκληρη, ένα μεγάλο μέρος έκαστης πηγής πληροφοριών καθίσταται εκτός ανθρώπινου ελέγχου και περιορισμού, με αποτέλεσμα πολλά δεδομένα να αποτελούν στοιχεία των big data. Επιπρόσθετα, δύο απαιτήσεις του ΓΚΠΔ που θα μπορούσαν πιθανόν να περιορίσει την διακίνηση των τεράστιων όγκων πληροφοριών, είναι το δικαίωμα πρόσβασης και το δικαίωμα διαγραφής. Το υποκείμενο των δεδομένων μπορεί να ζητήσει πρόσβαση και έλεγχο των δεδομένων του, για το πού είναι αποθηκευμένα καθώς και τον λόγο και το είδος των πληροφοριών που επεξεργάζονται.

Αναφορικά με την αποθήκευση και τη διαχείριση των δεδομένων, φαίνεται να δίνεται λύση με το πρωτόκολλο IPFS (Inter Planetary File System), του οποίου δημιουργός είναι ο Juan Benet [214] [215]. Το εν λόγω πρωτόκολλο έχει σχεδιαστεί για την αποθήκευση μεγάλων δεδομένων σε μια ομότιμη κατανεμημένη βάση αποθήκευσης αρχείων με δυνατότητα διεύθυνσης περιεχομένου. Επιπλέον δίνεται η δυνατότητα οι δομές αρχείων στο IPFS να συνδέονται μεταξύ τους χρησιμοποιώντας συνδέσμους Merkle και κάθε αρχείο μπορεί να βρεθεί χρησιμοποιώντας ένα αποκεντρωμένο σύστημα ονοματοδοσίας, το οποίο δίνει ονόματα αναγνώσιμα από τον άνθρωπο. Το παρόν προτεινόμενο πρωτόκολλο[216] προσπαθεί να συγκεράσει τα μεγάλα δεδομένα, τις αλυσίδες μπλοκ καθώς και την κρυπτογράφηση, για να δημιουργήσει ένα ασφαλές, απαραβίαστο μοντέλο τήρησης αρχείων ακαδημαϊκής έρευνας με μεθόδους ελέγχου πρόσβασης. Επιπλέον, με το πρωτόκολλο αυτό διασφαλίζεται η ιδιωτικότητα των δεδομένων, ενισχύοντας την ιδιότητα της αμετάβλητης αλυσίδας μπλοκ (blockchain) με την αποθήκευση τους σε κατανεμημένο παγκόσμιο δίκτυο. Αυτό μπορεί να υλοποιηθεί με τη χρήση έξυπνων συμβολαίων και μέχρι και σήμερα βρίσκεται σε δοκιμαστικό στάδιο. Οι πληροφορίες μεταδεδομένων προέλευσης των εγγράφων που είναι αποθηκευμένα στο IPFS μεταφορτώνονται περαιτέρω στην αλυσίδα μπλοκ προκειμένου να διασφαλιστεί η ακεραιότητα των πληροφοριών. Ο βασικός

[214] J. Benet, "IPFS - Content addressed, versioned, p2p file system (draft 3)," https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs. draft3.pdf, 2014

[215] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven , "Bitcoin and ".cryptocurrency technologies: a comprehensive introduction.", 2016, Princeton: Princeton University Press

[216] Vaghela A., Suthar A., "A Review Of Big Data Analysis Using Smart Contract" , UGC Care Group I Listed Journal, 2020

δημιουργός του εγγράφου μπορεί να διασφαλίσει ότι στα έγγραφα αυτά έχουν πρόσβαση και τα τροποποιούν μόνο οι προβλεπόμενοι χρήστες, στους οποίους επιτρέπεται η πρόσβαση. Με αυτό τον τρόπο, εξασφαλίζεται η διαβαθμισμένη πρόσβαση σε κάθε κόμβο με τη χρήση ασύμμετρων κλειδιών κρυπτογραφίας.

5.3. Big Data and Smart Legal Contracts -Πρόταση

Η αξιοποίηση των προαναφερθέντων μεθόδων ανάλυσης των Μεγάλων Δεδομένων σε συνδυασμό με τα έξυπνα συμβόλαια υπόσχεται να φέρει μεγάλες αλλαγές. Πράγματι, η αποτελεσματική διαχείριση αυτών των δεδομένων μπορεί να αλλάξει ριζικά τον τρόπο που συναλλασσόμαστε σε κάθε επίπεδο. Για το λόγο αυτό, θα εξετάσουμε το φαινόμενο των Big Data και υπό το πρίσμα των Smart Legal Contracts, προκειμένου να ανακαλύψουμε νέες πτυχές και να ερευνήσουμε πώς θα μπορούσαν να αξιοποιηθούν. Περαιτέρω δε, η συνεχώς αυξανόμενη χρήση έξυπνων συσκευών (IoT) καθώς και η χρήση smartphones και φορητών υπολογιστών συμβάλλει στην εκθετική αύξηση των δεδομένων με αποτέλεσμα να πολλαπλασιάζεται και ο όγκος των πληροφοριών που μπορούν να εξαχθούν.

Μετά την ανάλυση τόσο των Smart Contracts και ιδίως της νομικής πτυχής τους καθώς και την συνοπτική έρευνα και παρουσίαση των Big Data, με την παρούσα εργασία και λαμβάνοντας υπόψη τα όσα άρθρα έχουν μελετηθεί, προτείνεται μια συνδυαστική εφαρμογή και λύση. Με κάθε επιφύλαξη και στο μέτρο των μελετώμενων άρθρων, προτείνεται ως κάτι νέο, τα Smart Legal Contracts να χρησιμοποιούν Big Data προκειμένου να διαμορφωθεί μια σύμβαση που να καλύπτει σε μεγάλο ποσοστό τις ανάγκες εκάστου μέρους καθώς και να ταιριάζει στην εκάστοτε περίοδο. Επιπρόσθετα, στο πλαίσιο αυτό, θα υπάρξει ένα ενιαίο νομοθέτημα για όλα τα Κράτη, το οποίο θα είναι αποτέλεσμα διαβουλεύσεων των περισσότερων, εάν όχι όλων των συμβαλλομένων Κρατών. Το νομοθέτημα αυτό θα ρυθμίζει τις σχέσεις των μερών στα Smart Legal Contracts καθώς και περιπτώσεις ανώμαλης εξέλιξης τόσο σε περιβάλλον blockchain όσο και στο φυσικό κόσμο. Επιπλέον, θα συσταθεί μια Αρχή με εκπροσώπους από κάθε ήπειρο, η οποία σε εξαιρετικές περιπτώσεις θα επιλαμβάνεται ρόλο Δικαστηρίου.

Ειδικότερα, προτείνεται τα έξυπνα νομικά συμβόλαια να δημιουργούνται σε πρώτο στάδιο από ανθρώπους και εν συνεχεία να εμπλουτίζονται και να αλληλεπιδρούν με την "δεξαμενή" (pool) των πληροφοριών που έχουν συλλεχθεί για ποικίλους σκοπούς και όχι αυστηρά και μόνο στο πλαίσιο έξυπνων συμβάσεων. Με τον τρόπο αυτό, οι έξυπνες συμβάσεις είτε θα εμπλουτίζονται είτε θα βελτιώνονται. Όταν η δεξαμενή με τα μεγάλα δεδομένα έχει αρκετές και ποικίλες πληροφορίες, μαθαίνοντας με τις ανάλογες τεχνολογίες, πιθανόν να μπορεί να συντάξει εξ ολοκλήρου ένα έξυπνο νομικό συμβόλαιο κατάλληλο για τις ανάγκες των μερών. Επιπρόσθετα, μέσω των μεγάλων δεδομένων θα συλλέγονται και θα αναδιαμορφώνονται συνεχώς νέα πρότυπα, υποδείγματα συμβάσεων, ώστε κάθε φορά να επιλέγεται το πιο κατάλληλο και εξειδικευμένο για κάθε περίπτωση.

Εν συνεχεία, με την πάροδο του χρόνου και την συλλογή και αξιολόγηση μεγάλου δείγματος έξυπνων συμβάσεων, καθώς και την γνωμοδότηση ανθρώπων με εμπειρία σε αυτό το χώρο, θα δημιουργηθεί ένα ενιαίο νομοθέτημα για το Blockchain και τα Smart Contracts, στο οποίο δεν θα τίθεται χωρικοί περιορισμοί. Το εν λόγω νομοθέτημα θα ρυθμίζει σε κάθε στάδιο την εξέλιξη και τη σύναψη έκαστης σύμβασης, εξειδικεύοντας σε ορισμένες περιπτώσεις. Υπογραμμίζεται πως με το νομοθέτημα αυτό δεν θα υψώνονται εμπόδια τοπικής αρμοδιότητας, ισχύς του νόμου ή παρέμβασης των αντίστοιχων Αρχών. Το συγκεκριμένο νομοθέτημα θα υπερισχύει των εθνικών νόμων σε ό,τι αφορά ζητήματα blockchain και smart legal contracts. Κατ΄εξαίρεση, και σε αυστηρά ειδικές περιπτώσεις που αφορούν την ιδιωτικότητα, την ελευθερία του ατόμου σε κάθε έκφανση, την ασφάλεια και τη σωματική ακεραιότητα, θα γίνεται στάθμιση με υπερεθνικά νομοθετήματα, τα οποία σε κάθε περίπτωση θα έχουν ληφθεί υπ΄όψιν κατά τη σύνταξη του παγκόσμιου νομοθετήματος για Blockchain και Smart Legal Contracts.

Σε αυτό το σημείο, δέον να σχολιαστεί πώς ένα νομοθέτημα που θα ρυθμίζει το blockchain είναι αντίθετο με την αποκεντρωμένη δομή του. Για το λόγο αυτό, τονίζεται πως το νομοθέτημα θα ρυθμίζει αυστηρά τη σχέση των μερών από μία έξυπνη σύμβαση, ιδίως όταν τα μέρη προσφεύγουν σε αυτή τη λύση, χωρίς να επηρεάζεται το υπόλοιπο οικοδόμημα. Το νομοθέτημα αυτό θα ρυθμίζει και θα επιλύει τα προβλήματα εκ των υστέρων. δεν θα θέτει κανόνες και περιορισμούς σε προσυμβατικό στάδιο ή κατά τη σύναψη της σύμβασης. Επομένως, τα μέρη θα έχουν απόλυτη ελευθερία να ρυθμίσουν τη συμβατική σχέση σε οποιοδήποτε επίπεδο χωρίς νομικά εμπόδια και προσκόμματα.

Συμπεράσματα

Μετά την μελέτη και σύντομη ανάλυση τόσων ιδιαίτερων τεχνολογιών και ζητημάτων, μπορούμε να οδηγηθούμε σε κάποια συμπεράσματα. Από τα προαναφερθέντα προκύπτει ότι η Τεχνολογία Κατανεμημένου Καθολικού και κατ΄επέκταση το Blockchain και το Ethereum ανοίγουν νέους διάπλατους δρόμους για οικονομική και νομική ανάπτυξη. Η δημιουργία και η σταδιακή αφομοίωση των έξυπνων νομικών συμβάσεων φαντάζει συναρπαστική δεδομένου ότι δεν γνωρίζει εδαφικά και νομικά σύνορα. Το πλήθος των συναλλαγών θα εκτοξευθεί και το κόστος τους θα μειωθεί σημαντικά, δεδομένης της απουσίας ενδιάμεσων τρίτων που πιστοποιούν και ελέγχουν τις συμβάσεις και τις λοιπές διαδικασίες.

Εν τούτοις, δεν είναι λίγα τα ερωτήματα και οι προβληματισμοί που εγείρονται. Πιο συγκεκριμένα, ζητήματα δικαιοδοσίας και εφαρμογής νόμου σε περίπτωση νομικής διαμάχης ή ανώμαλης εξέλιξης απασχολούν την νομική κοινότητα. Κρίσιμα θέματα προκύπτουν και από την εξέταση των έξυπνων νομικών συμβάσεων υπό το πρίσμα του ΓΚΠΔ και της προστασίας των προσωπικών δεδομένων. Επιπρόσθετα, οι προγραμματιστές αγωνίζονται διαρκώς για την ενίσχυση των συστημάτων ασφαλείας καθώς και την ενδυνάμωση και βελτίωση των γλωσσών προγραμματισμού. Παράλληλα, η κρυπτογραφία και η ηλεκτρονική υπογραφή αποτελούν μέσα για τη διασφάλιση της ασφάλειας και της πιστοποίησης του υπογράφοντος την σύμβαση ή την συναλλαγή.

Οι έξυπνες νομικές συμβάσεις με τη χρήση κρυπτογραφικών κλειδιών καθώς και της κατάλληλης ηλεκτρονικής υπογραφής μπορούν να εξομοιωθούν τουλάχιστον με ηλεκτρονικά έγγραφα. Σε ορισμένες περιπτώσεις, μπορούν να χαρακτηριστούν ηλεκτρονικές συμβάσεις, εφόσον φέρουν τα χαρακτηριστικά μιας παραδοσιακής σύμβασης, τηρώντας την Αρχή του Ατύπου των Δικαιοπραξιών καθώς και το σχήμα πρότασης-αποδοχής. Σε κάθε περίπτωση, τα έξυπνα νομικά συμβόλαια δεν αντικαθιστούν τα παραδοσιακά καθώς και δεν μειώνουν το έργο δικηγόρων και συμβολαιογράφων. Η χρήση των έξυπνων νομικών συμβάσεων περιορίζεται σε απλές και λειτουργικές συναλλαγές, αλλά ταυτόχρονα αποκτά και το ρόλο εργαλείου για τους νομικούς.

Επίσης, η χρήση των Big Data μπορεί να οδηγήσει στην ταχύτερη ανάπτυξη των έξυπνων συμβάσεων, δεδομένου ότι θα συλλέγονται ποικίλα πρότυπα συμβάσεων καθώς και

νομοθετημάτων σε μια δεξαμενή, προκειμένου κάθε φορά οι έξυπνες νομικές συμβάσεις να διαμορφώνονται με τον βέλτιστο τρόπο για κάθε περίσταση.

Εν κατακλείδι, λαμβάνοντας υπόψη την τεχνολογική εξέλιξη και τις συνεχώς αυξανόμενες απαιτήσεις, προτείνεται η δημιουργία ενός ενιαίου νομοθετικού πλαισίου – σε παγκόσμιο επίπεδο- καθώς και η σύσταση μιας κοινής Επιτροπής ελέγχου σε περιπτώσεις που υπάρχουν αντιρρήσεις ως προς κάποιο έξυπνο νομικό συμβόλαιο. Δέον να διευκρινιστεί πώς η εν λόγω Επιτροπή δεν θα μπορεί να παρεμβαίνει εκ των προτέρων, διότι κάτι τέτοιο θα αντίκειτο στην ιδέα που πρεσβεύει το Blockchain. Αυτή η ιδέα- πρόταση εκφράζεται με κάθε επιφύλαξη και στο πλαίσιο μελέτης ενός πεπερασμένου αριθμού άρθρων και μελετών.

Βιβλιογραφία

Βιβλία

- Primavera De Filippi, Aaron Wright, " Blockchain and the Law- The Rule of Code", 2018, Harvard University Press
- Γεωργιάδης Α., "Γενικές Αρχές Αστικού Δικαίου", 2019, Π.Ν. Σάκκουλας
- Ζέκος Γ.,"Διαδίκτυο & Τεχνητή Νοημοσύνη στο Ελληνικό Δίκαιο", 2022 , Σάκκουλας
- Θεοδωράκης Ν., Καλογεράκης Γ., " Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα.", ΔiΜΕΕ 1/2019
- Ιγγλεζάκης Ι., Δίκαιο και Πληροφορική, 2021, Σάκκουλας
- Κανέλλος Λ., "Smart Contracts, Νομικές Προκλήσεις και επιχειρηματικές προοπτικές", 2022, Νομική Βιβλιοθήκη
- Καράκωστας Ι., "Δίκαιο και Ίντερνετ, Νομικά Ζητήματα του Διαδικτύου", 2009 , Π.Ν. Σάκκουλας
- Μαυρίδης Ι., Πάγκαλος Γ., "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", 2002, ΑΝΙΚΟΥΛΑ
- Σπυριδάκης Ι., "Γενικές Αρχές Αστικού Δικαίου" , 2022, Σάκκουλας
- Παπαδημόπουλος Ι., "Η δογματική ένταξη των smart contracts στο δίκαιο των συμβάσεων", 2020, ΧρΙΔ
- Παπαθανασίου Βαϊα, "Μη εναλλάξιμα κρυπτοπαραστατικά- Non- Fungible Tokens, Νομικά ζητήματα και προτάσεις ", 2022, Νομική Βιβλιοθήκη
- Παπαστερίου Δ., Κλαβανίδου Δ., "Δίκαιο της Δικαιοπραξίας" 2008

Σεμινάρια

- Κανέλλος Λ., Κωνσταντινίδης Ο., "Εφαρμογές blockchain στη Νομική Πρακτική", Διαδικτυακό Σεμινάριο της Νομικής Βιβλιοθήκης, https://www.nb.org/efarmoges-blockchain-sti-nomiki-praktiki.html .
- Κανέλλος Λ., "Έξυπνα Συμβόλαια (Smart Contracts) - Σύγχρονες Προκλήσεις & η εφαρμογή τους στη νομική πράξη", Διαδικτυακό Σεμινάριο της Νομικής Βιβλιοθήκης , https://www.nb.org/exipna-symbolaia-smart-contracts.html
- Λογαράς Κ., "Blockchain - Distributed Ledger Technology (DLT): Νομικές Προεκτάσεις ", Διαδικτυακό Σεμινάριο της Νομικής Βιβλιοθήκης, https://www.nb.org/blockchain-distributed-ledger-technology-dlt.html

Άρθρα

- Alharby M., Van Moorsel A., "Blockchain -based smart contracts: A systematic mapping study, 2019

- AlharbyM, Aldweesh A, van Moorsel A, "Blockchain-based smart contracts: A systematic mapping study of academic research", 2018.
- Bacon J et al (2018), 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' 25 Richmond Journal of Law and Technology 1, 61.
- Bal?zs Bod?, Daniel Gervais, Jo?o Pedro Quintais, "Blockchain and smart contracts: the missing link in copyright licensing? " International Journal of Law and Information Technology, Volume 26, Issue 4, Winter 2018, https://doi.org/10.1093/ijlit/eay014
- Bartoletti M., Pompianu L., " An empirical analysis of smart contracts: platforms, applications, and design patterns", 2017, ResearchGate
- Bashir I., "Mastering Blockchain: Distributed Ledger Technology, decentralization, and smart contracts explained", 2018
- Bashir I., "Mastering Blockchain: Distributed Ledger Technology, decentralization, and smart contracts explained", 2018
- Bikramaditya S. Gautam D., Priyansu Sekhar P., " Beginning Blockchain: A Beginners Guide to Building Blockchain Solutions", 2018, Apress
- Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, "Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions", 2018, Apress
- Blemus St?phane, "Law and Blockchain: a legal perspective on current regulatory trends worldwide", 2017
- Blockchain Enhances Privacy, Security and Conveyance of Data, 2016, CIENTIFIC AMERICAN
- Blockchain Enhances Privacy, Security and Conveyance of Data, 2016, CIENTIFIC AMERICAN
- Buterin V. , "On Public and Private Blockchains", Ethereum Blog, 7 August 2015; Guegan D. , "Public Blockchain versus Private Blockchain", Docu-ments de travail du Centre d'Economie de la Sorbonne, 2017
- Di Angelo M., "Smart Contracts in view of Civil Code", 2019
- G. Callsen, "FinTech, DLT and regulation", 2017, International Capital Market Association (ICMA).
- Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger" Berlin Version. 2022
- Goldwasser S., Micali S., Rivest R. L., " A digital signature scheme secure against adaptive chosen-message attacks", 1995
- Haber S., Stornetta W.S., "How to time-stamp a digital document" , 1991, SpringerLink
- J. Benet, "IPFS - Content addressed, versioned, p2p file system (draft 3)," https://ipfs.io/ipfs/ QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs. draft3.pdf, 2014
- Jakub J. Szczerbowski, "Place of smart contracts in civil law. A few comments on form and interpretation", 2018, SSRN
- Kasireddy Preethi, "How does Ethereum work, anyway?", 2017
- Khalili et al., "Chameleon hashing, Efficient chameleon hash functions in the enhanced collision resistant model" , 2019, Science Direct
- Liberti, L. & Marinelli F.. "Mathematical programming: Turing completeness and applications
- Lincoln A., "Electronic signature laws and the need for uniformity in the global market, 2004
- Marcelo Corrales, Mark Fenwick, Helena Haapio , " Legal Tech, Smart Contracts and Blockchain", 2019, Springer
- Michael Anthony C. Dizon, Peter John Upson, " Laws of encryption: An emerging legal framework", 2021

- Mohanta B. K., Panda S. S, Jena D., "An overview of smart contract and use cases in blockchain technology", 2018
- Morris, David Z. (15 May 2016). "Leaderless, Blockchain Based Venture Capital Fund Raises $100 Million, And Counting". 2016
- Nakamoto S, " Bitcoin: A Peer - to - Peer Electronic Cash System"
- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven , "Bitcoin and ".cryptocurrency technologies: a comprehensive introduction.", 2016, Princeton: Princeton University Press
- Nersessian D., "The law and ethics of big data analytics: A new role for international human rights in the search for global standards", 2018
- Niranjanamurthy M., Nithya B., Jagannatha S., "Analysis of Blockchain Technology: pros, cons and SWOT". 2019, Springer
- Rashideh W., "Blockchain technology framework: Current and future perspectives for the turism industry", 2020
- Samuel Zaruba Smith, Andy Garcia, "Blockchain Smart Contracts,: Introduction for Accounting and Auditing Professionals", 2022, ISACA
- Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, Anoud Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends", 2021, SpringerLink
- Shubhani Aggarwal, Neeraj Kumar, "Blockchain 2.0: Smart Contracts", 2020
- Singhal, B., Dhameja, G., Panda, P.S., "How Blockchain Works. In: Beginning Blockchain. ", 2018,Apress
- Smith S. S., "Blockchain, Smart Contracts and Financial Audit Implications", 2020
- Stephane Blemus, "Law and Blockchain: a legal perspective on current regulatory trends worldwide", 2017, SSRN
- Szabo N., "Formalizing and Securing Relationships on Public Networks", 1997.
- Szabo Nick, "Smart Contracts. Unpublished manuscript", 1994
- Szczerbowski Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017.
- Szczerbowski Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017.
- Szczerbowski, Jakub J., "Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation", 2017, SSRN
- to software analysis" , 2014
- Vaghela A., Suthar A., "A Review Of Big Data Analysis Using Smart Contract" , UGC Care Group I Listed Journal, 2020
- Vaghela A., Suthar A., " A Review of Big Data Analysis Using Smart Contracts", UGC Care Group I Listed Journal, 2020
- Wallace, Benjamin , "The Rise and Fall of Bitcoin". , 2011, Wired 19
- Woebbeking M., "The Impact of Smart Contracts on Traditional Concepts of Contract Law", 2019
- Yaga D., Mell P., Roby N., Scarfone K., "Blockchain Technology Overview", 2019, Computer Science
- Young M., "Blockchains: The great chain of being sure about things". The Economist. , 2015. Archived from the original on 3 July 2016
- Zhang Weijia, Anand Tej, Blockchain and Ethereum Smart Contract Solution Development: Dapp Programming with Solidity, 2022, Scopus
- Zhen Er Low, "Execution of Judgements on the Blockchain- A Practical Legal Commentary", 2021

- Zheng Z., Xie S., Dai H., Chen X., Weng J., Imran M., "An overview on smart contracts: Challenges, advances and platforms". 2020, Science Direct
- Zheng Z., Xie S., Dai H., Chen X., Weng J., Imran M., "An overview on smart contracts: Challenges, advances and platforms". 2020, Science Direct
- Παπαδημόπουλος Ιωάννης, " Η δογματική ένταξη των smart contracts στο δίκαιο των συμβάσεων", ΧρΙΔ 2020.471.
- Παπαδοπούλου Α., "Blockchain: Η τεχνολογία που υπόσχεται "ψηφιακή ασφάλεια" - Πιθανές εφαρμογές και συνέπειες για το δίκαιο πνευματικής ιδιοκτησίας και ιδίως στο ζήτημα της ψηφιακής ανάλωσης",2018, ΕπισκΕΔ
- Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές;, Ευρωπαϊκή Κεντρική Τράπεζα, 19 Απριλίου 2017
- Σταμπέρνας Σωτήριος, "Τεχνολογίες αλυσίδας συστοιχιών και έξυπνα συμβόλαια στο πλαίσιο του Διαδικτύου των Πραγμάτων", 2018, Πανεπιστήμιο Πειραιώς (μεταπτυχιακή διατριβή)

Νομοθεσία και λοιπά Νομικά Κείμενα

- ΦΕΚ. Τεύχος Β’ 1756/22.05.2017, Εφημερίδα της Κυβερνήσεως: 17803, 17805, 17807 κ.ε.. 22 Μαΐου 2017
- Blockchain & Cryptocurrency Laws and Regulations | United Kingdom | GLI - https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/united-kingdom
- Study on the use of innovative technologies in the justice field https://op.europa.eu/en/publication-detail/-/publication/4fb8e194-f634-11ea-991b-01aa75ed71a1/language-en/format-PDF/source-279592216
- Απόφαση Europass (ΕΕ) 2018/646
- Οδηγία DSM (2019/790)
- Κατευθυντήριες Γραμμές 04/2019 του ΕΣΠΔ για το άρθρο 25 ΓΚΠΔ
- Επίσημη Εφημερίδα της ΕΕ- L360_Οκτώβριος 2021 https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2021:360:FULL&from=EN
- https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/apofaseis_eparkeias
- Απόφαση Schrems II - C-311/2018
- Νόμος 3917/2011 - Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.
- Νόμος 3471/2006 - Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον
- τομέα των ηλεκτρονικών επικοινωνιών
- Οδηγία NIS2
- Κανονισμός του ENISA είναι ο Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ της 17ης Απριλίου 2019 (Νόμος για την ασφάλεια στον κυβερνοχώρο)
- Article 29 Working Party, Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN, 18
- Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 20
- Article 29 Working Party, Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN

- Πρόταση: Κανονισμός Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου
- για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους
- (Πράξη για τα δεδομένα)
- https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52022PC0068
- Κανονισμός Ρώμη I
- Κανονισμός Ρώμη II
- Ο νόμος 4727/2020 ενσωμάτωσε τον Κανονισμό eIDAS και κατήργησε το ΠΔ 150/2001
- Παράρτημα II Κανονισμού eIDAS
- Κανονισμός (ΕΕ) αριθ. 1025/2012 Του Ευρωπαϊκου Κοινοβουλίου Και Του Συμβουλίου της 25ης Οκτωβρίου 2012
- The European Union Blockchain Observatory And Forum - Blockchain and digital Identity https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
- Commission Nationale de l'Informatique et des Libertés (06 November 2018) Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data https://www.cnil.fr/en/blockchain-and-gdpr-solutionsresponsible-use-blockchain-context-personal-data
- Report of the European Blockchain Observatory and Forum (16 October 2018) Blockchain and the GDPR 20 https://www.eublockchainforum.eu/reports
- Case C-25/17 Jehovan Todistajat [2018] EU:C:2018:551, para 62
- CNIL, Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
- Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles?, 2018
- https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles
- European Parliament, "Blockchain and the General Data Protection Regulation can distributed ledgers be squared with European data protection law?", 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/ERPS_STU(2019)634445_EN.pdf
- Smart Legal Contracts: Summary - Law Commission United Kingdom
- Berberich M and Steiner M (2016), 'Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?' 2 European Data Protection Law Review 422, 425
- Finck M., "Blockchains and Data Protection in the European Union", 2018, 4 European Data Protection Law Review 17.
- Zuiderveen Borgesius F., "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation", 2016, 32 Computer Law & Security Review 256, 260.

Ιστοσελίδες

- https://www.dhs.gov/science-and-technology/blockchain-portfolio
- https://www.lawcom.gov.uk/project/smart-contracts/
- Raul Zambrano, Andrew Young, and Stefaan Verhulst, "Seeking Ways to Prevent Electoral Fraud using Blockchain in Sierra Leone" https://blockchan.ge/blockchange-election-monitoring.pdf

- Uzma Jafar,Mohd Juzaiddin Ab Aziz andZarina Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges” https://www.mdpi.com/1424-8220/21/17/5874
- https://el.wikipedia.org/wiki/Ethereum#cite_note-4
- https://www.fortunegreece.com/article/efarmoges-blockchain-gia-proti-fora-ston-dimo-katerinis/
- https://en.wikipedia.org/wiki/David_Chaum
- IBM, “ The four Vs of big data”,2018 http://www.ibmbigdatahub.com/infographic/four-vs-big-data
- https://www.investopedia.com/terms/e/ecash.asp
- https://data-flair.training/blogs/features-of-blockchain/
- https://www.coindesk.com/markets/2016/06/24/coindesks-ethereum-research-report-now-available/
- https://ethereum.org/en/developers/docs/evm/
- Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP,An Introduction to Smart Contracts and Their Potential and Inherent Limitations 2018 https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/
- Geroni D., “What Are Ricardian Contracts? A Comprehensive Guide”, 2021
- https://101blockchains.com/ricardian-contracts/
- Czarnecki J., “Who is the data controller in a blockchain?”, 2018 https://newtech.law/en/author/jacek-czarnecki/
- Wirth C and Kolain M (2018), ‘Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data’ in Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design , https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf
- https://scholar.law.colorado.edu/faculty-articles/148/
- https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
- https://irishtechnews.ie/global-blockchain-adoption-which-countries-are-leading-the-charge/
- https://www.mytilineos.gr/news/press-releases/mytilineos-is-securing-a-new-ppa-in-australia-through-the-blockchain-technology/
- https://blog.chain.link/blockchain-technology-real-estate/
- https://www.unlock-bc.com/news/2020-03-16/finlands-housing-market-now-securely-on-the-blockchain/
- https://news.bloombergtax.com/daily-tax-report-international/eu-inches-toward-blockchain-in-fight-against-vat-fraud-1
- Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business - https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital
- https://en.wikipedia.org/wiki/Mercosur
- Blockchain in Tax Administrations - https://www.ciat.org/blockchain-in-tax-administrations/?lang=en
- https://www.blockchain-council.org/blockchain/blockchain-land-registries-across-the-globe/
- Rose A., “Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights” https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html
- https://en.wikipedia.org/wiki/KodakCoin
- Blockchain Use Case for Notary https://4irelabs.com/cases/notarization-in-blockchain/#:~:text=Notarization%20is%20an%20official%20fraud,cannot%20be%20edited%20or%20deleted

- Courts and Smart Dubai to launch world's first "Court of the Blockchain" https://www.engage.hoganlovells.com/knowledgeservices/news/difc-courts-and-smart-dubai-to-launch-worlds-first-court-of-the-blockchain
- Vivien Chan , Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb
- Το δικαίωμα προαίρεσης συνιστά περιουσιακό και διαπλαστικό δικαίωμα, που λειτουργεί ως εξής: Ο μέτοχος ή τρίτος υπέρ του οποίου το σχετικό δικαίωμα μπορεί, κατ΄αποτέλεσμα, να προβεί, μόνος αυτός, σε αγορά ή πώληση μετοχών. https://koumentakislaw.gr/arthra/dikaioma-proairesis-sth-metabibash-metohon/#:~:text=%CE%A4%CE%BF%20%CE%B4%CE%B9%CE%BA%CE%B1%CE%AF%CF%89%CE%BC%CE%B1%20%CF%80%CF%81%CE%BF%CE%B1%CE%AF%CF%81%CE%B5%CF%83%CE%B7%CF%82%20%CF%83%CF%85%CE%BD%CE%B9%CF%83%CF%84%CE%AC%2C%20%CE%BA%CE%B1%CF%84,%CF%83%CE%B5%20%CE%B1%CF%80%CF%8C%CE%BA%CF%84%CE%B7%CF%83%CE%B7%20%CE%AE%20%CE%BC%CE%B5%CF%84%CE%B1%CE%B2%CE%AF%CE%B2%CE%B1%CF%83%CE%AE%20%CF%84%CE%BF%CF%85%CF%82
- https://www.defense.gov/News/Feature-Stories/story/Article/3072635/the-berlin-airlift-what-it-was-its-importance-in-the-cold-war/
- https://edilibrary.wordpress.com/2016/08/29/father-of-edi-army-master-sargent-edward-a-guilbert/
- https://www.edistaffing.com/blog/2015/11/06/electronic-data-interchange-edi-trivia/
- Solidity: El lenguaje de programación de los Contratos Inteligentes - Cardaniers https://cardaniers.com/solidity/
- https://www.homodigitalis.gr/wp-content/uploads/2018/08/%CE%94%CE%95%CE%95%CE%9D%CE%BF%CE%BC%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1-2001-2018.pdf
- https://ec.europa.eu/newsroom/article29/items
- Buterin Vitalik, «So where did the name Ethereum come from?» , 2014
- About Blockchain Based Notary Proof Of Concept https://joinup.ec.europa.eu/collection/blockchain-egov-services/solution/blockchain-based-notary-proof-concept/about#:~:text=DIGIT%20has%20developed%20a%20Blockchain,a%20distributed%20and%20decentralized%20ledger.
- https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/6.7776_LC_Smart_Legal_Contracts_2021_Final.pdf
- https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf
- https://www.techtarget.com/searchdatamanagement/definition/5-Vs-of-big-data
- https://www.teradata.com/Glossary/What-are-the-5-V-s-of-Big-Data
- 5 Types of analytics: Prescriptive, Predictive, Diagnostic, Descriptive and Cognitive Analytics https://www.weirdgeek.com/2018/11/types-of-analytics/?amp
- https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910
- https://www.eett.gr/parochoi/ilektronikes-epikoinonies/ypiresies-empistosynis/genikes-plirofories/katalogos-empisteysis-egkekrimenon-parochon-ypiresion-empistosynis-trusted-list/
- https://www.techtarget.com/searchsecurity/definition/Diffie-Hellman-key-exchange#:~:text=Diffie%2DHellman%20key%20exchange%20is,encrypt%20and%20decrypt%20their%20messages.

- https://www.rapid7.com/blog/post/2017/08/28/rsa-rivest-shamir-and-adleman/
- https://www.stellarinfo.com/blog/complete-history-ibm-lotus-notes-hcl-notes/
- https://www.slideshare.net/edbrill/lotusphere-2010-an-oral-history-of-ibm-lotus-notes-first-20-years/4-Lotus_Notes_10_1989_of
- https://ec.europa.eu/commission/presscorner/detail/el/ip_22_1113
- https://www.europarl.europa.eu/doceo/document/A-9-2023-0031_EL.html
- https://www.ey.com/el_gr/tax/tax-alerts/l-4961-2022-the-greek-legal-framework-on-emerging-technologies
- Philipps Erb K., "IRS Tries Again To Make Coinbase Turn Over Customer Account Data", 2017
- https://www.forbes.com/sites/kellyphillipserb/2017/03/20/irs-tries-again-to-make-coinbase-turn-over-customeraccount-data/#1841d9e5175e
- https://docs.soliditylang.org/en/v0.8.13/solidity-by-example.html#blind-auction
- https://twitter.com/VitalikButerin/status/1051160932699770882
- https://lawtechuk.io/insights/cryptoasset-and-smart-contract-statement
- https://www.jdsupra.com/legalnews/the-ucc-and-emerging-technologies-8250345/
- https://cryptoslate.com/cryptos/oracle/
- Posted by Stuart D. Levi and Alex B. Lipton, Skadden, Arps, Slate, Meagher & Flom LLP,An Introduction to Smart Contracts and Their Potential and Inherent Limitations 2018 https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/
- Geroni D., "What Are Ricardian Contracts? A Comprehensive Guide", 2021
- https://101blockchains.com/ricardian-contracts/
- Czarnecki J., "Who is the data controller in a blockchain?", 2018 https://newtech.law/en/author/jacek-czarnecki/
- Wirth C and Kolain M (2018), 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' in Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design , https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf