



Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Καταναεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	ΕΦΑΡΜΟΓΗ ΤΗΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ BLOCKCHAIN ΓΙΑ ΤΗΝ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΣΕ ΕΡΓΑ ΨΗΦΙΑΚΟΥ ΠΟΛΙΤΙΣΜΟΥ INTELLECTUAL PROPERTY MANAGEMENT FOR DIGITAL CULTURE ASSETS USING BLOCKCHAIN.
Ονοματεπώνυμο Φοιτητή	ΚΩΝΣΤΑΝΤΙΝΟΣ ΒΕΡΓΟΠΟΥΛΟΣ
Πατρώνυμο	ΠΑΝΑΓΙΩΤΗΣ
Αριθμός Μητρώου	ΜΠΚΣΑ/ 18006
Επιβλέπων	Καθηγητής Δ. Βέργαδος

Ημερομηνία Παράδοσης Οκτώβριος 2021

Τριμελής Εξεταστική Επιτροπή

Δημήτριος Βέργαδος
Καθηγητής

Άγγελος Μιχάλας
Καθηγητής

Ιωάννης Τασούλας
Επίκουρος Καθηγητής

Abstract

In a global economic landscape of hyper-commodification and financialization, efforts to assimilate digitalization (including digital arts products) into the high-stakes commercial cultural market have so far been rather unsuccessful, presumably because either digital artefacts cannot easily assume the status of precious object worthy of collection or those digital means and technologies are not yet mature enough to handle challenges effectively. This paper will focus primarily on the possible opportunities that blockchain may offer with respect to the future of IP law and discuss its potential impact on the registration, management and enforcement of intellectual property rights. Blockchain technology is claimed to be and perceived as one of the revolutionary technologies that will have an enormous impact on our lives in the forthcoming years and decades. The technological advancements offered by blockchain promise wide ranges of use in a variety of sectors and legal areas, including intellectual property (IP) law. The chapters compiled here elaborate the potential impact of the technology in modes of registration, management and enforcement of IP law. The snapshot of the current and rapidly evolving technological and economic situation allows authors to elaborate on legal or regulative options, economic impact, and policy choices of the Blockchain technology in the context of IP law.

Keywords

Blockchain, Digital art, Financialisation, Intellectual property, Copyright, Digital rights management, Technology adoption, Maturity model, copyright, smart contracts, distributed ledger technology (DLT), copyright registries, automated licensing, digital rights management (DRM), IoT networks, Consensus, digital culture

Περίληψη

Σε ένα παγκόσμιο οικονομικό περιβάλλον υπερ-εμπορευματοποίησης, οι προσπάθειες αφομοίωσης ψηφιακών μέσων (συμπεριλαμβανομένων αγαθών ψηφιακού πολιτισμού) στην εμπορική πολιτιστική κληρονομιά ήταν μέχρι στιγμής μάλλον ανεπιτυχείς, πιθανώς επειδή είτε τα ψηφιακά αντικείμενα δεν μπορούν εύκολα να αναγνωριστούν ως αντικείμενα που αξίζει να συλλεχθούν είτε τα μέσα δεν είχαν την κατάλληλη ωριμότητα να αντιμετωπίσουν αποτελεσματικά τις σχετικές προκλήσεις. Αυτή η διατριβή διερευνά τη χρήση τεχνολογιών blockchain για την διαχείριση των δικαιωμάτων πνευματικής ιδιοκτησίας (ΠΙ) σε αντικείμενα ψηφιακής κληρονομιάς. Η τεχνολογία Blockchain θεωρείται μια από τις επαναστατικές τεχνολογίες που θα έχουν τεράστιο αντίκτυπο στη ζωή μας τις επόμενες δεκαετίες. Οι τεχνολογικές εξελίξεις που προσφέρονται από το blockchain υπόσχονται ευρύ φάσμα χρήσης σε διάφορους τομείς, συμπεριλαμβανομένου του νόμου περί ΠΙ. Προς αυτή τη κατεύθυνση αναλύουμε τον πιθανό αντίκτυπο της τεχνολογίας στην εγγραφή, τη διαχείριση και την επιβολή των δικαιωμάτων ΠΙ. Δεδομένης της υφιστάμενης και ταχέως εξελισσόμενης, τεχνολογικής, οικονομικής και πολιτικής κατάστασης αναλύουμε τη τεχνολογία έναντι νομικών ή κανονιστικών επιλογών συνυπολογίζοντας τις οικονομικές επιπτώσεις της αφομοίωσης της τεχνολογίας.

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο Τμήμα Πληροφορικής της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών του Πανεπιστημίου Πειραιώς. Η υπόδειξη του θέματος έγινε σε συνεργασία με τους Δρ. Θ. Καραντζιά, καθηγητή Δρ. Δ. Βέργαδο και τον Δρ. Σταύρο Ι. Παπαπαναγιώτου Γενικό Διευθυντή της εταιρείας Διαδικτυακές Επιχειρήσεις Ελλάδος, ο οποίος επιπλέον χρηματοδότησε την έρευνα.

Θα ήθελα να ευχαριστήσω από καρδιάς την οικογένεια (Ελένη και Κατερίνα), τη σύντροφο (Σταματίνα) και τους φίλους μου, που μου έδειξαν άνευ όρων υποστήριξη και με ενθάρρυναν να συνεχίσω υπερπηδώντας κάθε εμπόδιο και δυσκολία.

Κλείνοντας αφιερώνω την παρούσα στον αείμνηστο πατέρα μου Παναγιώτη. Το ξεκινήσαμε μαζί.. το τελειώνω μόνος μου.

Πίνακας Περιεχομένων

Abstract	2
Keywords	3
Περίληψη	4
Ευχαριστίες	5
Πίνακας Περιεχομένων	6
Πίνακες	9
Σχήματα.....	9
1 Εισαγωγή.....	10
1.1 Κίνητρα	11
1.2 Ευρύτερο πλαίσιο Πνευματικής Ιδιοκτησίας.....	11
1.2.1 Πολιτικό και Οικονομικό υπόβαθρο	11
1.3 Μεθοδολογία και πηγές.....	12
2 Τεχνολογία Blockchain.....	13
2.1 Ορισμός.....	13
2.2 Διακριτοποίηση (Tokenization) και έλλειψη ψηφιακών πόρων (digital scarcity)	14
2.3 Επισκόπηση της τεχνολογίας blockchain.....	14
2.3.1 Αρχιτεκτονική.....	14
2.3.2 Επαλήθευση συναλλαγών ταυτότητας και ιδιοκτησίας.....	16
2.3.3 Βασικές λειτουργίες	17
2.4 Κρυπτογραφία	20
2.4.1 Hash	21
2.5 Αξιολόγηση ασφάλειας.....	21
2.5.1 Έλεγχος ταυτότητας και εξουσιοδότηση (authentication-authorization)	21
2.5.2 Εμπιστευτικότητα (confidentiality)	22
2.5.3 Ακεραιότητα (integrity)	22
2.5.4 Μη αποκλεισμός (non- repudiation)	22
2.5.5 Διαθεσιμότητα	22
2.6 Μηχανισμοί συναίνεσης (Consensus Mechanisms)	22
2.6.1 Αλγόριθμος συναίνεσης βάσει απόδειξης (Proof-based Consensus Algorithm)	23
2.6.2 Voting Consensus Algorithm.....	26
2.6.3 Σύνοψη Μηχανισμών συναίνεσης	30
2.7 Έξυπνα συμβόλαια (Smart contracts)	31
2.7.1 Ορισμός.....	31

2.7.2	Επισκόπηση Dapps (Decentralized Applications)	32
2.7.3	Πλεονεκτήματα	33
2.8	Εξέλιξη της τεχνολογίας.....	34
2.9	Φιλοσοφία του Blockchain (4 ^η βιομηχανική επανάσταση)	34
2.10	Εγκατεστημένα (Υφιστάμενα) Blockchain συστήματα (Use cases)	35
2.11	Εφαρμογές Οικονομικής φύσης.....	35
2.11.2	Εφαρμογές άλλων κλάδων	36
2.12	Διείσδυση στην αγορά και επίπεδο ωριμότητας της τεχνολογίας Blockchain.	36
2.12.1	Gartner Hype Cycle	37
2.12.2	Αναδυόμενες τεχνολογίες του 2018 (Emerging Technologies)	38
2.12.3	Ανάλυση SWOT.....	39
2.12.4	Κρίσιμοι Παράγοντες Επιτυχίας.....	41
2.12.5	Σύνοψη	41
3	Ψηφιακός Πολιτισμός- Τέχνη (Digital Culture).....	43
3.1	Πνευματική ιδιοκτησία	43
3.1.1	Εμπορικά σήματα (Trademark Law)	45
3.1.2	Πνευματικά δικαιώματα (Copyright Law)	45
3.1.3	Ευρεσιτεχνίες	46
3.1.4	Βιομηχανικά σχέδια	46
3.2	Κατακερματισμός	47
3.2.1	Ευρωπαϊκός Κανονισμός φορητότητας περιεχομένου.	48
3.3	Πνευματική ιδιοκτησία, δικαιώματα και ορθή χρήση μεταξύ των εικαστικών καλλιτεχνών, των ακαδημαϊκών και των μουσείων εικαστικών τεχνών	48
3.3.1	Προκλήσεις	49
3.4	Τεχνητή Νοημοσύνη. Μηχανές που παράγουν έργα ψηφιακού πολιτισμού!	50
4	Ψηφιακός πολιτισμός στο Blockchain	52
4.1	Δικαιώματα ΠΙ.....	52
4.1.1	Διαχείριση ΠΙ.....	52
4.1.2	Καταχώρηση ΠΙ.	53
4.1.3	Περιορισμός της πρόσβασης στα μέσα αναπαραγωγής	54
4.1.4	Κάτοχοι δικαιωμάτων και αδειοδότηση μέσω έξυπνων συμβολαίων	54
4.2	Διπλώματα ευρεσιτεχνίας (Patents)	56
4.3	Εμπορικά σήματα	57
4.4	Οικονομικά στοιχεία	57
4.4.1	Τα οφέλη του blockchain για διαχείριση δικαιωμάτων ΠΙ και πληρωμών	58

4.4.2	Το άυλο περιουσιακό στοιχείο: Προσωπικά Δεδομένα Χρηστών (Data monetization)	58
4.4.3	Νέα μοντέλα πληρωμών	59
4.4.4	Χρονική σήμανση (timestamping) ψηφιακών έργων με blockchain	59
4.5	Πρωτοβουλίες	60
4.5.1	Πρωτοβουλία IPwe	61
5	Κανονιστικά, νομικά και ηθικά ζητήματα Blockchain	62
5.1	Νομικές επιπτώσεις	62
5.2	Lex Mercatoria	62
5.2.1	Συνεργατικός και αποκεντρωμένος νόμος (Collaborative and decentralized)	62
5.3	Περιβάλλον	63
5.4	Πρωτοβουλίες	63
5.5	Υπογραφή Συμβολαίων	64
5.6	Ο κώδικας είναι νόμος	64
5.6.1	Blockchain και έξυπνα συμβόλαια	65
5.7	Περιορισμοί	66
6	Συμπεράσματα	67
6.1	Κατευθύνσεις μελλοντικής έρευνας	68
	Βιβλιογραφία	69

Πίνακες

ΠΙΝΑΚΑΣ 1 ΘΕΜΕΛΙΩΔΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ BLOCKCHAIN ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΑ ΔΗΜΟΣΙΑ, ΙΔΙΩΤΙΚΑ ΚΑΙ ΚΟΙΝΟΠΡΑΚΤΙΚΑ BLOCKCHAIN ΣΥΣΤΗΜΑΤΑ	20
ΠΙΝΑΚΑΣ 2 SWOT ANALYSIS.....	41
ΠΙΝΑΚΑΣ 3 ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ (COPYRIGHT, PATENTS, TRADEMARKS).....	44

Σχήματα

ΣΧΗΜΑ 1 ΠΑΡΑΔΕΙΓΜΑ BLOCKCHAIN ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ (ΚΕΦΑΛΙΔΑ)	15
ΣΧΗΜΑ 2 ΑΝΤΙΚΕΙΜΕΝΑ ΜΕΣΑ ΣΤΟ BLOCK	16
ΣΧΗΜΑ 3 ΠΩΣ ΕΝΑ ΣΥΣΤΗΜΑ ΕΠΑΛΗΘΕΥΣΗΣ ΣΥΝΑΛΛΑΓΩΝ ΚΑΛΕΙΤΑΙ ΑΠΟ ΤΟΝ ΑΠΟΣΤΟΛΕΑ.	17
ΣΧΗΜΑ 4 ΟΙ 5 ΒΑΣΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ BLOCKCHAIN	18
ΣΧΗΜΑ 5 PRIVATE BLOCKCHAIN	20
ΣΧΗΜΑ 6 PUBLIC BLOCKCHAIN.....	20
ΣΧΗΜΑ 7 ΜΗΧΑΝΙΣΜΟΣ ΣΥΝΑΙΝΕΣΗΣ PROOF OF WORK	24
ΣΧΗΜΑ 8 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ΡΑΧΟΣ. ΟΙ PROPOSERS ΥΠΟΒΑΛΛΟΥΝ ΠΡΟΤΑΣΕΙΣ ΣΤΟΥΣ ACCEPTORS	28
ΣΧΗΜΑ 9 THE ARCHITECTURE OF A BLOCKCHAIN SYSTEM INCLUDING CONSENSUS LAYER	29
ΣΧΗΜΑ 10 COMPARISONS OF DIFFERENT CONSENSUS METHODS.....	30
ΣΧΗΜΑ 11 SMART CONTRACT. SOURCE: RICHARD BROWN	31
ΣΧΗΜΑ 12 APPS VS DAPPS (PRATIK, 2018).....	32
ΣΧΗΜΑ 13 GARTNER HYPE CYCLE PHASES	38
ΣΧΗΜΑ 14 GARTNER HYPE CYCLE, 2018 [49].....	39
ΣΧΗΜΑ 15 PORTRAIT OF EDMOND BELAMY, 2018, CREATED BY GAN (GENERATIVE ADVERSARIAL NETWORK), WHICH WAS OFFERED AT CHRISTIE'S IN OCTOBER 2018.....	51
ΣΧΗΜΑ 16 ΨΗΦΙΑΚΟΣ ΠΟΛΙΤΙΣΜΟΣ ΣΤΟ BLOCKCHAIN	52
ΣΧΗΜΑ 17 BLOCKCHAIN FOR PATENTS	56
ΣΧΗΜΑ 18 OVERVIEW OF TRUSTED TIMESTAMPING SYSTEM FUNCTIONALITY	60
ΣΧΗΜΑ 19 HTTPS://WWW.CBINSIGHTS.COM/ . HOW BLOCKCHAIN TECHNOLOGY COULD DISRUPT REAL ESTATE	64

1 Εισαγωγή

Λίγα ακαδημαϊκά και ερευνητικά θέματα έχουν αποκτήσει τόσο μεγάλη προσοχή στον κόσμο της τεχνολογίας της πληροφορίας όσο το blockchain, καθιστώντας σχεδόν αναπόφευκτο το γεγονός ότι οι φορείς που εμπλέκονται στην ανάπτυξη και διαχείριση συστημάτων τεχνολογίας πληροφοριών (IT) το μελετούν στα πλαίσια λειτουργίας τους.

Το Blockchain βασίζεται σε αρχές που προέρχονται από την κρυπτογραφία, τη θεωρία παιγνίων και τη δικτύωση peer-to-peer. Είναι ένα αρχείο ψηφιακών γεγονότων που μοιράζεται μεταξύ διαφορετικών μερών. Οι πληροφορίες που προστίθενται δεν μπορούν ποτέ να διαγραφούν και μπορούν να ενημερωθούν μόνο με κάποιου είδους συναίνεση μεταξύ των συμμετεχόντων (κόμβων) στο σύστημα/ δίκτυο.

Στην απλούστερη περιγραφή του, το blockchain είναι ένα καταμεμημένο κατάστιχο (distributed ledger), ή μια βάση δεδομένων μόνο προσάρτησης (append only) στην οποία κάθε χρήστης έχει ένα συνεχώς ενημερωμένο και έγκυρο αντίγραφο. Όσοι συμμετέχουν στο κατάστιχο έχουν πρόσβαση στο ίδιο πλήρες ιστορικό γεγονότων και τη δυνατότητα επαλήθευσης της εγκυρότητας όλων των εγγραφών. Εξελιγμένοι μηχανισμοί συναίνεσης διασφαλίζουν ότι οι νέες εγγραφές μπορούν να προστεθούν στην καταμεμημένη βάση δεδομένων μόνο εάν είναι συνεπείς με προηγούμενες εγγραφές και τις απαιτήσεις του δικτύου.

Ανάλογα με τον τεχνολογικό σχεδιασμό, ένας κάτοχος λογαριασμού μπορεί να είναι (ανώνυμο / ψευδώνυμο) άτομο, νομική οντότητα, έξυπνη σύμβαση (κώδικας λογισμικού) ή οποιαδήποτε ομάδα ή συνδυασμός αυτών. Τα δείγματα, όπως αναλύεται στην επόμενη ενότητα, μπορούν να αντιπροσωπεύουν σχεδόν οτιδήποτε: μια μονάδα εικονικού νομίσματος, ένα στοιχείο, ένα φυσικό αντικείμενο στον κόσμο ή οποιαδήποτε άλλη αφηρημένη οντότητα. Πέρα από τα παραπάνω, κάθε blockchain μπορεί να ακολουθεί διαφορετικές αρχές σχεδιασμού, όπως αναλύεται παρακάτω και επηρεάζει ουσιαστικά τη λειτουργία του.

Μια σύντομη ανασκόπηση της διαθέσιμης βιβλιογραφίας καταδεικνύει ότι υπάρχουν διαφορετικές απόψεις σχετικά με το τι είναι το blockchain και τα DLTs και τι μπορούν να κάνουν. Χρονική σήμανση συναλλαγών, ασφαλής καταγραφή, κατακερματισμός ή ψηφιακή υπογραφή εγγραφών, σύνδεση δεδομένων αρχειοθέτησης περιγράφονται συχνά ως μοναδικές δυνατότητες blockchain, αλλά αυτές στην πραγματικότητα είναι λειτουργίες εφικτές με συμβατικά/ υφιστάμενα εργαλεία πληροφορικής. Ωστόσο, αυτές οι λειτουργίες έχουν γίνει πιο γνωστές και διερευνώνται πληρέστερα με την ευρύτερη δημοσιότητα των περιπτώσεων χρήσης που βασίζονται σε blockchain και έχουν μεγάλες δυνατότητες παροχής τεχνολογικής μετατόπισης σε αξιόπιστη ανταλλαγή/ συναλλαγή δεδομένων και καταγραφή γεγονότων.

Η πρώτη χρήση της τεχνολογίας blockchain πραγματοποιήθηκε με τη δημιουργία του Bitcoin, ψηφιακό κρυπτονομίσμα όπως παρουσιάστηκε το 2009 [1]. Ακολούθησαν περισσότερα από 700 άλλα ψηφιακά και εικονικά κρυπτονομίσματα που δημιουργήθηκαν χρησιμοποιώντας παρόμοια τεχνολογία. Αναπόφευκτα, πιθανές εφαρμογές της τεχνολογίας blockchain σε τομείς διαφορετικούς από τα κρυπτονομίσματα (όπως ασφάλιση, υγειονομική περίθαλψη, ναυτιλία και πνευματική ιδιοκτησία) άρχισαν να σχηματίζονται, να συλλαμβάνονται και να αναπτύσσονται από διάφορα ενδιαφερόμενα μέρη. Παρόλο που το bitcoin δημιουργήθηκε σε μια προσπάθεια να αποφευχθεί η εμπλοκή των κεντρικών τραπεζών στις συναλλαγές, πολλά χρηματοπιστωτικά ιδρύματα ενδιαφέρονται τώρα για τη νέα τεχνολογία και αναζητούν τρόπους για να το εφαρμόσουν προς όφελός τους. Οι τράπεζες επενδύουν εκατομμύρια δολάρια σε έρευνα για τον σχεδιασμό και ενσωμάτωση εφαρμογών blockchain. Σύμφωνα με τον Όμιλο Aite,

ερευνητική εταιρεία χρηματοοικονομικών υπηρεσιών, οι τράπεζες αυξήσαν τις δαπάνες τους για αυτή τη νέα τεχνολογία έως και 400 εκατομμύρια δολάρια το 2019 σε σύγκριση με 75 εκατομμύρια δολάρια που επενδύθηκαν το 2015 [2].

Η τεχνολογία Blockchain (και τα κρυπτονομίσματα) εξελίσσεται σε παγκόσμιο ψηφιακό φαινόμενο. Αποτελεί ένα από τα καυτά θέματα έρευνας ανεξαρτήτου βιομηχανίας (ιδίως της οικονομικής). Εν συντομία, η τεχνολογία blockchain υποστηρίζει επιχειρήσεις και ιδιώτες να πραγματοποιούν συναλλαγές χωρίς την έγκριση τρίτων.

1.1 Κίνητρα

Κατά μεγάλο βαθμό η επικρατούσα άποψη στη βιομηχανία, τους διεθνείς οργανισμούς και τον ακαδημαϊκό χώρο είναι πως η τεχνολογία blockchain και DLTs μπορεί να επιλύσουν όλα τα θέματα «εμπιστοσύνης» ανταλλαγής δικτυακά δεδομένων, δίνοντας παράλληλα λίγη προσοχή στους περιορισμούς που εισάγουν. Συχνά, ορισμένες από τις λειτουργίες που αποδίδονται στο blockchain είναι εφικτές μέσω κανονικής ψηφιοποίησης, διαχείρισης ταυτότητας και πρόσβασης, καταγραφής ενεργειών, χρονικής σήμανσης, τυποποίησης, δημιουργίας αντιγράφων ασφαλείας,

1.2 Ευρύτερο πλαίσιο Πνευματικής Ιδιοκτησίας

Η τεχνολογία Blockchain είναι πολλά υποσχόμενη σχετικά με πιθανές εφαρμογές της σε διάφορους τομείς που σχετίζονται με θέματα πνευματικής ιδιοκτησίας. Από την αρχική «δημιουργία» δικαιώματος πνευματικής ιδιοκτησίας, έως τη νομική καταγραφή του στα σχετικά μητρώα (registries), την αδειοδότηση και επιβολή (enforcement) η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την επίτευξη διαφόρων αξιόλογων κρίκων της αλυσίδας. Παρά τις κοινωνικές, νομικές, κανονιστικές και τεχνολογικές προκλήσεις που ανακύπτουν, η νέα τεχνολογία, περιγράφει ένα αυτοματοποιημένο, αξιόπιστο, αποτελεσματικό και αποδοτικό σύστημα προστασίας και διαχείρισης ΠΙ και αποτελεί ένα σημαντικό κίνητρο για την αντιμετώπιση προκλήσεων. Ως εκ τούτου η ενσωμάτωση της τεχνολογίας σε αυτό το τομέα αποτελεί μια νέα πραγματικότητα

1.2.1 Πολιτικό και Οικονομικό υπόβαθρο

Αρκετές σημαντικές πολιτικές και οικονομικές αλλαγές τα τελευταία 30 χρόνια έχουν αλλάξει τις συνθήκες παραγωγής και διανομής πνευματικών αγαθών (intellectual goods). Ο πολιτικός νεοφιλελευθερισμός άνθισε, ενώ η επιλογή μιας σοσιαλιστικής εναλλακτικής σοβιετικού τύπου έχει καταρρεύσει. Οι διεθνείς εμπορικές συμφωνίες επέτρεψαν περαιτέρω τη διακρατική λειτουργία του καπιταλισμού. Ο πλουραλισμός των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ), οι οποίες αποτελούν αναπόσπαστο μέρος του διακρατικού συντονισμού του καπιταλισμού, μείωσε δραστικά το κόστος παραγωγής και διανομής πνευματικών αγαθών. Η εξέλιξη της πληροφορικής μείωσε δραματικά το κόστος παραγωγής πολλών τύπων πνευματικών αγαθών και το Διαδίκτυο και άλλες τεχνολογίες επικοινωνιών διευκολύνουν όχι μόνο τη διανομή χαμηλού κόστους, αλλά δημιουργούν καταμεμημένες και συνεργατικές κοινωνικές ρυθμίσεις που διευκολύνουν περαιτέρω την παραγωγή και διανομή πνευματικών αγαθών.

Όταν κάθε ψηφιακή κυκλοφορία είναι επίσης μια πράξη αναπαραγωγής, η κατανάλωση ενός GIF ή αρχείου MP3 μπορεί να είναι ταυτόχρονη σε σημαντικό αριθμό καταναλωτών. Στο παρελθόν ήταν απαγορευτική η κλοπή και διάθεση ενός βιβλίου. Πλέον φθηνά ηλεκτρονικά είδη ευρείας κατανάλωσης και νέες τεχνικές, από την αντιγραφή και επικόλληση έως την αντιγραφή ενός CD, καθιστούν την αναπαραγωγή ψηφιακών αρχείων μια απλή διαδικασία. Η ανάπτυξη εξελιγμένων κωδικοποιήσεων για οπτικοακουστικό περιεχόμενο επιτρέπει τη συμπίεση μεγάλων αρχείων πολυμέσων, και

διευκολύνει την αποθήκευση και τη μετάδοση τους. Επιπλέον μπορεί να προστεθεί σαν παράμετρος στην εξίσωση η ραγδαία εξέλιξη στα δίκτυα υψηλού εύρους ζώνης. Αυτά λοιπόν καθιστούν σχετικά εύκολη την αποθήκευση και την κυκλοφορία περιεχομένου και ενσωματώνει ένα σύνολο προκλήσεων στην πολιτιστική βιομηχανία. Ο ψηφιακός πολιτισμός, θα μπορούσαμε να πούμε, προσανατολίζεται και επιζητά να είναι ελεύθερος.

Επιπλέον, στη σημερινή οικονομία, ένα αυξανόμενο μερίδιο της επιχειρηματικής αξίας προκύπτει μέσω των άυλων περιουσιακών στοιχείων. Έτσι, η επιτυχία συχνά εξαρτάται από την ικανότητα διαχείρισης και εκμετάλλευσης της πνευματικής ιδιοκτησίας. Για το λόγο αυτό, οι εταιρείες απαιτούν από τους διαχειριστές να αποκτούν, να κυβερνούν και να εμπορευματοποιούν αποτελεσματικά περιεχόμενο που προστατεύεται από πνευματικά δικαιώματα και διπλώματα ευρεσιτεχνίας.

Σε αυτό το ευρύτερο πλαίσιο, ο στόχος της παρούσας μελέτης, είναι να συμβάλει στη συζήτηση σχετικά με τη δυναμική χρήση του blockchain και των DLT στη διαχείριση της πνευματικής ιδιοκτησίας για αγαθά ψηφιακού πολιτισμού, λαμβάνοντας υπόψη την λειτουργικότητα της τεχνολογίας και όχι τις δυνατότητες των υφιστάμενων πλατφορμών ή λύσεων. Είτε αυτές χρησιμοποιούνται στην προώθηση προϊόντων, ή καλύπτοντας απαιτήσεις σε υποθετικά σενάρια, ή αποτελούν απόδειξη ιδέας και πιλοτικές εφαρμογές. Αντ' αυτού μελετώνται προβλέψεις σχετικά με τη μακροπρόθεσμη «προσαρμογή» των τεχνολογιών για την κάλυψη των υφιστάμενων και μελλοντικών επιχειρηματικών αναγκών μέσω περιπτώσεων χρήσης.

1.3 Μεθοδολογία και πηγές

Αυτή η μελέτη βασίζεται σε μια ανασκόπηση διαθέσιμων στο κοινό πληροφοριών, συμπεριλαμβανομένων εκθέσεων και δημοσιεύσεων που παρέχονται από τη βιομηχανία, ομάδες προβληματισμού (think tanks), εξειδικευμένα μέσα ενημέρωσης, δημόσιες αρχές, καθώς και ακαδημαϊκή βιβλιογραφία σχετικά με το θέμα. Επιπλέον, ζητήθηκε η γνώμη των σχετικών νομικών πράξεων όπου ήταν απαραίτητο.

Για τη διενέργεια της τεχνολογικής ανάλυσης διατίθενται πολλές κριτικές σε μορφή παρουσιάσεων προϊόντων (είτε από τον πάροχο της εκάστοτε πλατφόρμας είτε από πελάτες), διαδικτυακά φόρουμ κοινότητας, εκπαιδευτικές εξηγήσεις, έγγραφα ανάλυσης συμβούλων, μελέτες, κυβερνητικές κριτικές, δηλώσεις από θεσμικά όργανα της ΕΕ, περιγραφές έργων απόδειξης της έννοιας αλλά και επιστημονικά άρθρα. Οι πιο αξιόπιστες πηγές περιλαμβάνουν εκθέσεις συμβούλων και επιστημονικά άρθρα, τα οποία εξηγούν ότι τα στοιχεία αυτά είναι ως επί το πλείστον συμβατά με οποιαδήποτε ανάπτυξη συστήματος, όχι μόνο με την τεχνολογία Blockchain. Οι πιο κρίσιμες πηγές, όσον αφορά την αξιολόγηση της εφαρμοσιμότητας και την διενέργεια ανάλυσης λειτουργιών, είναι ίσως οι διαδικτυακές τεχνολογικές κριτικές της κοινότητας και οι περιγραφές προϊόντων. Ωστόσο, υπάρχει πολύ λίγη βιβλιογραφία που σχετίζεται με το blockchain σε συστήματα πληροφορικής μεγάλης κλίμακας. Με αυτήν την διατριβή στοχεύουμε να καλύψουμε αυτό το κενό αναφορικά στον ψηφιακό πολιτισμό τουλάχιστον σε κάποιο βαθμό .

2 Τεχνολογία Blockchain

Το Blockchain είναι ένα ακατάλυτο ψηφιακό κατάστιχο που εξυπηρετεί τη διαδικασία καταγραφής συναλλαγών και παρακολούθησης γεγονότων σε ένα δίκτυο. Τα γεγονότα μπορεί να αφορούν σε απτά αντικείμενα όπως μετρητά, σπίτια και αυτοκίνητα ή άυλα όπως πνευματική ιδιοκτησία, διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα ή ακόμη και εταιρική επωνυμία.

2.1 Ορισμός

Η τεχνολογία Blockchain προήλθε από ένα founding paper με ονομασία «Bitcoin: Peer-to-Peer Cash System» που δημοσιεύτηκε από τον μελετητή «Satoshi Nakamoto» [3], αλλά δεν έχει ακόμη σχηματιστεί ένας αναγνωρισμένος ορισμός blockchain. Η ορολογία blockchain γενικά αναφέρεται στο συνδυασμό μπλοκ γεγονότων σε συγκεκριμένες δομές δεδομένων ανά αλυσίδα με χρονολογική σειρά και κρυπτογραφικά εγγυημένη αποκεντρωμένη κοινή χρήση γενικών κατάστιχων για την αποτροπή παραποίησης. Μια άλλη προσέγγιση ορισμού αναφέρεται σε ένα καταναμημένο πρότυπο υπολογιστών σε ένα αποκεντρωμένο πλαίσιο υποδομής για δημιουργία δεδομένων και ενημέρωση, χρησιμοποιώντας αλγόριθμο συναίνεσης καταναμημένων κόμβων, επικύρωση και αποθήκευση δεδομένων χρησιμοποιώντας κρυπτογραφημένη δομή μπλοκ αλυσίδας, χειρισμό δεδομένων και προγραμματισμό χρησιμοποιώντας αυτοματοποιημένο κομμάτι (script) κώδικα (έξυπνη σύμβαση).

Τα βασικά πλεονεκτήματα της τεχνολογίας blockchain περιλαμβάνουν αποκέντρωση, συλλογική συντήρηση, ασφάλεια και αξιοπιστία, δεδομένα χρονολογικών σειρών και προγραμματιζόμενα δεδομένα.

- Αποκέντρωση (Decentralization): Με βάση την καταναμημένη δομή, ολοκληρώνεται η διαδικασία λογιστικής, επαλήθευσης, αποθήκευσης, συντήρησης και διαβίβασης δεδομένων. Αντί να βασίζεται σε μια κεντρική αυθεντία/ εξουσία/ οργανισμό η οποία καθιερώνει τη σχέση εμπιστοσύνης μεταξύ καταναμημένων κόμβων, βασίζεται σε μαθηματικές μεθόδους για να σχηματιστεί ένα αξιόπιστο αποκεντρωμένο καταναμημένο σύστημα.
- Συλλογική συντήρηση: Χρησιμοποιείται ένας ειδικός μηχανισμός οικονομικών κινήτρων για να διασφαλιστεί ότι όλοι οι κόμβοι στο καταναμημένο σύστημα μπορούν να συμμετάσχουν στη διαδικασία επαλήθευσης του μπλοκ δεδομένων (το bitcoin "mining" είναι ένα τυπικό παράδειγμα) και υιοθετείται ένας αλγόριθμος συναίνεσης για την επιλογή ενός συγκεκριμένου κόμβου που θα αναλάβει να συνδέσει το νέο μπλοκ με το blockchain.
- Ασφάλεια και αξιοπιστία: Τα δεδομένα κρυπτογραφούνται με μεθόδους ασύμμετρης κρυπτογραφίας και η ισχυρή υπολογιστική δύναμη που σχηματίζεται από τον αλγόριθμο συναίνεσης χρησιμοποιείται για την άμυνα ενάντια σε επιθέσεις από εξωτερικούς παράγοντες για να διασφαλιστεί ότι τα δεδομένα στο blockchain δεν μπορούν να πλαστογραφηθούν ή/ και να αλλοιωθούν.
- Δεδομένα χρονοσειρών: Η αποθήκευση δεδομένων ολοκληρώνεται μέσω δομής μπλοκ αλυσίδων με χρονική σήμανση, δημιουργώντας χρονοσειρές δεδομένων και συνεπώς διευκολύνεται η ιχνηλασιμότητα και η επαλήθευση.
- Προγραμματιζόμενο: παρέχεται ευέλικτο σύστημα κωδικοποίησης σεναρίων (scripting code) στους χρήστες για την ανάπτυξη προηγμένων έξυπνων συμβολαίων, νομισμάτων και ποικίλων άλλων αποκεντρωμένων εφαρμογών [4].

2.2 Διακριτοποίηση (Tokenization) και έλλειψη ψηφιακών πόρων (digital scarcity)

Τα καταμεμημένα κατάστιχα καταγράφουν την ιδιοκτησία και τις συναλλαγές ψηφιακών διακριτικών (tokens). Το Tokenization είναι η διαδικασία δημιουργίας μιας ψηφιακής αναπαράστασης ενός στοιχείου και η παρακολούθηση της ιδιοκτησίας του, χρησιμοποιώντας ψηφιακά διακριτικά. Εικονικά, οποιοδήποτε είδος πληροφοριών μπορεί να εκφραστεί ως διακριτικό, χρησιμοποιώντας μια κρυπτογραφική υπογραφή. Οποιοδήποτε τέτοιο διακριτικό μπορεί να «αποθηκευτεί» σε ένα blockchain ή ένα καταμεμημένο κατάστιχο. Στον τομέα των πνευματικών δικαιωμάτων, τα διακριτικά μπορούν να αντιπροσωπεύουν έναν αριθμό διαφορετικών στοιχείων [5]. Αρχικά, μπορούν να αντιπροσωπεύουν ένα αντίγραφο μιας προστατευόμενης εργασίας. Αυτή η αντιπροσώπευση μπορεί να γίνει τη στιγμή της δημιουργίας (π.χ. μια ψηφιακή κάμερα ή ένας επεξεργαστής κειμένου μπορεί να δημιουργήσει ένα διακριτικό κατά τη στιγμή της ολοκλήρωσης της εργασίας) ή στη συνέχεια, από τον κάτοχο των σχετικών δικαιωμάτων ή από εξουσιοδοτημένο τρίτο μέρος. Δεύτερον, τα διακριτικά μπορούν να αντιπροσωπεύουν μια εγγραφή RMI (Right Management Information) για προστατευμένο περιεχόμενο. Τρίτον, τα διακριτικά μπορούν να κωδικοποιήσουν ένα υποσύνολο πληροφοριών που αναφέρονται στον ορισμό του RMI, δηλαδή τους όρους χρήσης προστατευμένου περιεχομένου, για παράδειγμα τους τυπικούς όρους άδειας χρήσης των αδειών Creative Commons (CC). Ωστόσο, είναι επίσης δυνατό να προβλεφθούν όροι χρήσης που αναφέρονται στην ιδιαίτερη κατάσταση μιας εργασίας, όπως εάν είναι ορφανό έργο (orphan work) ή έργο δημόσιου τομέα [6]. Οι όροι χρήσης είναι συχνά στατικοί/γενικοί ή δυναμικοί/ υπό όρους. Τα πρώτα ρυθμίζονται μία φορά και (υποτίθεται) δεν αλλάζουν. Αντίθετα, δυναμικοί ή υπό όρους όροι χρήσης μπορεί να εξελίσσονται με την πάροδο του χρόνου. Αυτό ισχύει για τα περισσότερα RMI, τα οποία αλλάζουν κάθε φορά που μεταβιβάζονται τα πνευματικά δικαιώματα ή αλλάζουν οι αντίστοιχοι όροι χρήσης. Τέλος, τα διακριτικά μπορούν να αντιπροσωπεύουν την αμοιβή για τη χρήση μιας εργασίας, η οποία μπορεί να κωδικοποιηθεί σε λεγόμενα κρυπτονομίσματα (π.χ. Bitcoin, Bitcash) ή ισοδύναμα νομισμάτων fiat, που αποτελούν την αντίθετη απόδοση για μια συναλλαγή στο αντίστοιχο (αντίγραφο) έργο.

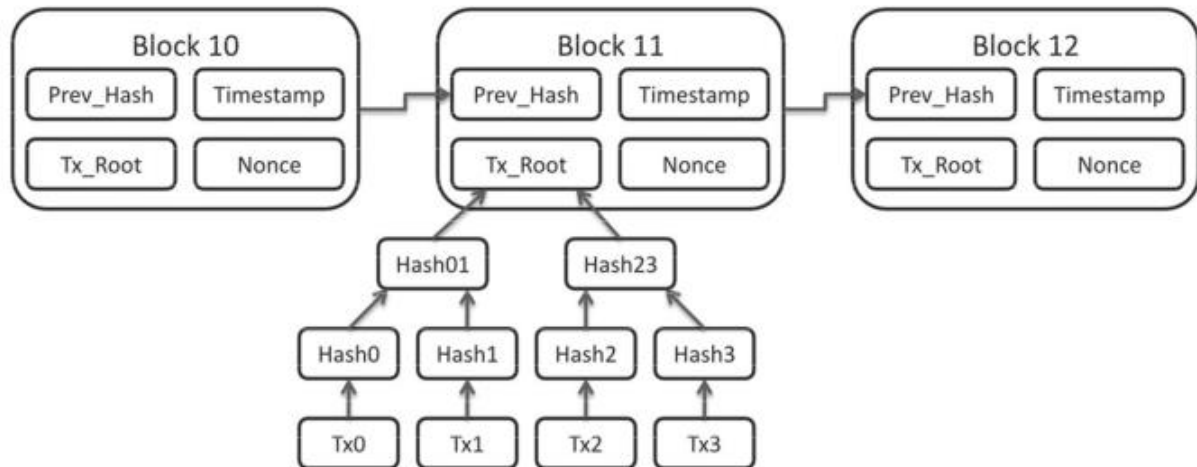
Τα μεμονωμένα διακριτικά (individual tokens) είναι μοναδικά. Οι συναλλαγές με διακριτικά σε ένα blockchain οργανώνονται με τρόπο που αποτρέπει τη διπλή δαπάνη των διακριτικών (διπλογραφία). Στην πράξη, αυτό σημαίνει ότι τα διακριτικά είναι το όχημα μέσω του οποίου η τεχνολογία blockchain επαναφέρει την έλλειψη (scarcity) ή περιορισμό πόρων στον ψηφιακό κόσμο.

2.3 Επισκόπηση της τεχνολογίας blockchain

Αυτή η ενότητα παρέχει μια επισκόπηση του Blockchain, το οποίο περιλαμβάνει την επαλήθευση συναλλαγών και την αρχιτεκτονική των block εντός του Blockchain.

2.3.1 Αρχιτεκτονική

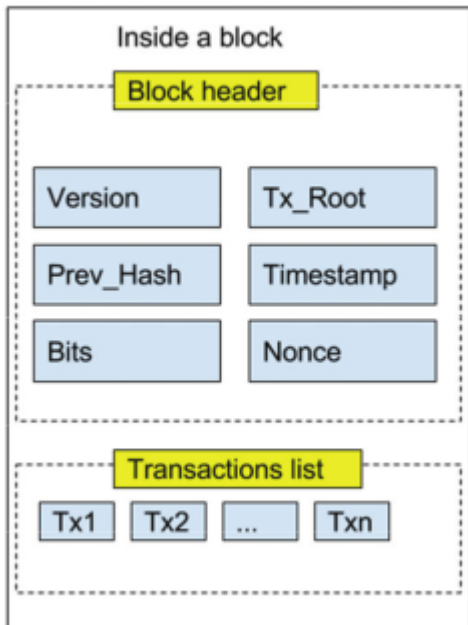
Όπως αναφέρθηκε παραπάνω, περιγραφικά το Blockchain είναι μια σειρά μπλοκ, τα οποία συνδέονται διαδοχικά μεταξύ τους σε μια αλυσίδα. Κάθε μπλοκ περιέχει πολλές συναλλαγές, οι οποίες επικυρώνονται, όπως φαίνεται στην προηγούμενη ενότητα. Το Σχ. 1 είναι ένα παράδειγμα Blockchain αρχιτεκτονικής όπου περιγράφονται μόνο ορισμένες κύριες οντότητες μέσα στην κεφαλίδα (header) του μπλοκ.



Σχήμα 1 Παράδειγμα Blockchain αρχιτεκτονικής (κεφαλίδα)

Πιο συγκεκριμένα στο παραπάνω σχήμα περιγράφεται η αρχιτεκτονική μέσα σε ένα block. Πέραν μιας λίστας συναλλαγών εμπεριέχονται τα κάτωθι αντικείμενα στην κεφαλίδα του block.

- **Prev_Hash:** αυτό το αντικείμενο μπορεί να χαρακτηριστεί ως αναφορά στους γονείς, το οποίο αποτελεί τον σύνδεσμο ενός μπλοκ με το προηγούμενο στην αλυσίδα. Όλες οι πληροφορίες στο προηγούμενο μπλοκ θα εισαχθούν σε μια συνάρτηση κατακερματισμού για να λάβουν μια τιμή, και στη συνέχεια αυτή η τιμή θα αντιστοιχιστεί στο πεδίο Prev_Hash στο νέο μπλοκ. Στο Bitcoin χρησιμοποιείται για τη λήψη αυτής της τιμής, μια συνάρτηση κατακερματισμού (hash) 256-bit [23].
- **Χρονική σήμανση (χρονοσειρά/ timestamp):** η ώρα που ενσωματώθηκε το μπλοκ.
- **Tx_Root:** αυτό το αντικείμενο, το οποίο είναι επίσης γνωστό ως Merkle root [24], περιέχει την τιμή κατακερματισμού όλων των επικυρωμένων συναλλαγών του μπλοκ. Όπως φαίνεται από το παράδειγμα στο Σχ. 2, όλες οι συναλλαγές κατακερματίζονται σε μια τιμή κατακερματισμού (hashed value). στη συνέχεια συνδυάζονται μεταξύ τους ανά ζεύγος και εισάγονται σε άλλη συνάρτηση κατακερματισμού. Αυτή η εργασία επαναλαμβάνεται έως ότου υπάρχει μόνο μία οντότητα, που χαρακτηρίζονται Merkle root.
- **Έκδοση (version):** το αντικείμενο περιέχει την έκδοση του πρωτοκόλλου που χρησιμοποιεί ο κόμβος που ζητά την αλλαγή στην αλυσίδα.
- **Nonce (αριθμός που χρησιμοποιείται μόνο μία φορά):** αυτό το αντικείμενο χρησιμοποιείται στη περίπτωση PoW, το οποίο αποδεικνύει τις προσπάθειες που έχει καταβάλει ένας κόμβος για να πάρει το δικαίωμα να προσθέσει το μπλοκ του στην αλυσίδα. Το αντικείμενο αναλύεται στην επόμενη ενότητα.
- **Bits:** αυτό το αντικείμενο δείχνει το επίπεδο δυσκολίας στη περίπτωση PoW. Το αντικείμενο αναλύεται στην επόμενη ενότητα.



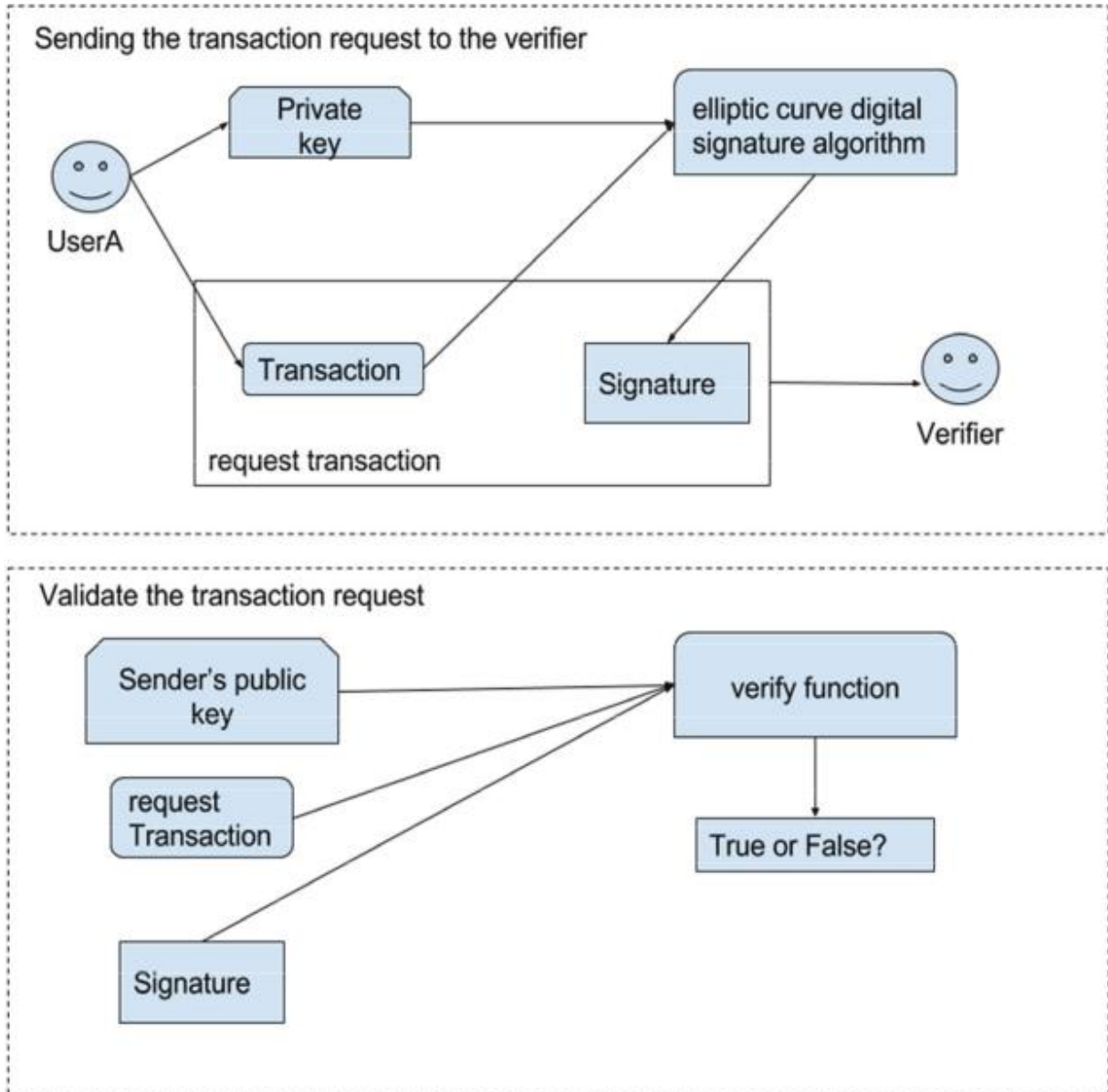
Σχήμα 2 Αντικείμενα μέσα στο block

2.3.2 Επαλήθευση συναλλαγών ταυτότητας και ιδιοκτησίας

Η βασική διεργασία κάθε συστήματος συναλλαγών είναι να επαληθεύσει την ταυτότητα του αποστολέα, δηλαδή να διασφαλίσει πως η συναλλαγή μεταξύ του αποστολέα και του παραλήπτη ζητείται/ αρχικοποιείται από τον "πραγματικό" αποστολέα και όχι από κανέναν άλλο. Στα υφιστάμενα συστήματα (πριν το blockchain), το παραπάνω αίτημα επιβεβαιώνεται από ένα τρίτο μέρος. Αυτός ο μεσάζον πρέπει να επιβεβαιώσει το αίτημα του πραγματικού αποστολέα.

Το παρακάτω σχήμα (Σχήμα 3) δείχνει μια επισκόπηση αυτής της επαλήθευσης στην περίπτωση ενός blockchain συστήματος. Πιο συγκεκριμένα χρησιμοποιούνται δύο ορισμοί: δημόσια και ιδιωτικά κλειδιά [9], τα οποία είναι γνωστά ως ψηφιακές υπογραφές. Όταν οποιοσδήποτε χρήστης κάνει μια συναλλαγή, πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να «υπογράψει» τη συναλλαγή. Οι πληροφορίες της συναλλαγής και το ιδιωτικό κλειδί του χρησιμοποιούνται ως είσοδοι σε μια συνάρτηση υπογραφής για να δημιουργήσουν την ψηφιακή υπογραφή. Στη συνέχεια, η συναλλαγή συνδυάζεται με αυτήν την ψηφιακή υπογραφή για να μετατραπεί σε αίτημα συναλλαγής. Ο επαληθευτής θα ελέγξει εάν αυτή η οντότητα ανήκει στο σωστό άτομο ή όχι, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα, το οποίο είναι γνωστό από όλους. Έπειτα, η συναλλαγή, η υπογραφή του αποστολέα και το δημόσιο κλειδί του θα εισαχθούν μαζί σε μια συνάρτηση επαλήθευσης η οποία επιστρέφει αποτέλεσμα: true ή false. Εάν το αποτέλεσμα είναι αληθές, τότε ο αιτών είναι ο πραγματικός αποστολέας στη συναλλαγή και το αντίστροφο. Εφόσον έχει χρησιμοποιηθεί αλγόριθμος κρυπτογράφησης 256 bits, για κάθε υπογραφής σε κάθε συναλλαγή, αν κάποιος θέλει να παραποιήσει αυτήν την υπογραφή για να κάνει μια δόλια συναλλαγή, πρέπει να «μαντέψει» 2^{256} περιπτώσεις, κάτι που είναι αδύνατο (μέχρι σήμερα). Εκτός από τον έλεγχο της εγκυρότητας του αποστολέα, ο επαληθευτής πρέπει επίσης να ελέγξει την εγκυρότητα της συναλλαγής ως προς το εάν ο αποστολέας έχει αρκετά χρήματα για να στείλει στον παραλήπτη ή όχι. Αυτό θα μπορούσε

να γίνει κοιτάζοντας το κατάστιχο, το οποίο περιέχει πληροφορίες για κάθε προηγούμενη επιτυχημένη συναλλαγή.

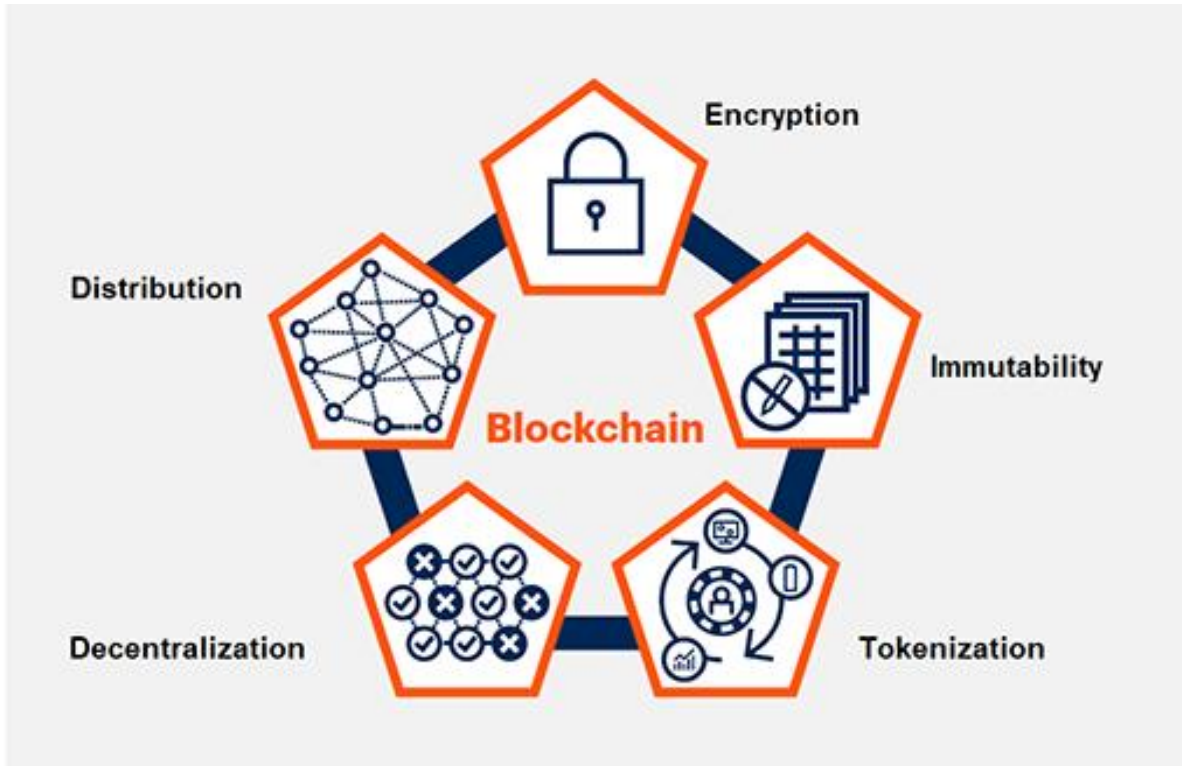


Σχήμα 3 Πως ένα σύστημα επαλήθευσης συναλλαγών καλείται από τον αποστολέα.

2.3.3 Βασικές λειτουργίες

Ένα από τα βασικά στοιχεία του blockchain και των κατακεντρωμένων κατάστιχων είναι η δημιουργία και διαχείριση εμπιστοσύνης μεταξύ των συμμετεχόντων στο δίκτυο. Αυτό επιτρέπει σε πρόσωπα (φυσικά και νομικά), καθώς και σε μηχανές, να πραγματοποιούν συναλλαγές χωρίς να έχουν προηγούμενη σχέση εμπιστοσύνης μεταξύ τους και επιπλέον να μην βασίζονται σε μεσολαβητικές οντότητες που τους παρέχουν υπηρεσίες δημιουργίας

σχέσης εμπιστοσύνης. Βέβαια παρόλο που δεν υπάρχει ανάγκη κεντρικής αρχής εμπιστοσύνης, Απαιτείται ένας συντονισμός στην έκδοση των πιστοποιητικών και ο καθορισμός των κανόνων συμπεριφοράς του οικοσυστήματος [7].



Σχήμα 4 Οι 5 βασικές λειτουργίες του Blockchain

2.3.3.1 Κατανεμημένο Σύστημα (Distributed).

Η κατανεμημένη φύση της αποθήκευσης δεδομένων σε οικοσυστήματα blockchain στοχεύει στην εξάλειψη του δυνητικού κινδύνου ενός μόνο σημείου αποτυχίας (δηλαδή δεν υπάρχει κεντρικός ή ενδιάμεσος κόμβος, ο οποίος είναι κρίσιμος για τη λειτουργία του δικτύου και μπορεί να υποβληθεί σε κυβερνοεπίθεση), ωστόσο το τελικό σημείο, η δημιουργία αντιγράφων ασφαλείας και η ασφάλεια του συστήματος πρέπει να αντιμετωπιστούν όσο και σε τυπικά συστήματα με πολλές τοποθεσίες.

Στον πυρήνα του, ένα blockchain είναι ένα διαφανές και αυτόνομο αποκεντρωμένο κατάστιχο. Κάθε κόμβος του κατάστιχου αποθηκεύει ένα πλήρες αντίγραφο του, γράφει νέες καταχωρήσεις όταν λαμβάνει συναίνεση από το υπόλοιπο δίκτυο, μεταδίδει τις συναλλαγές που πραγματοποιεί ο χρήστης με το υπόλοιπο δίκτυο, για επαλήθευση με συναίνεση και καταχώρηση και τέλος ελέγχει τακτικά ότι το αντίγραφο του κατάστιχου είναι πανομοιότυπο με το καθένα του υπόλοιπου δικτύου [1].

2.3.3.2 Κοινόχρηστο Σύστημα (Shared)

Η κοινόχρηστη φύση των κατανεμημένων κατάστιχων, όπου οι πληροφορίες είτε διανέμονται είτε αντιγράφονται σε όλα τα μέρη του δικτύου και είναι διαθέσιμες για έλεγχο, καθιστούν τις συναλλαγές πιο διαφανείς και ανιχνεύσιμες. Οι νέες οντότητες δεδομένων μπορούν να εγγραφούν μόνο επιπρόσθετα στις υφιστάμενες εγγραφές ή μητρώα συνόλων δεδομένων, συμβάλλοντας έτσι στη διασφάλιση της ακεραιότητας των

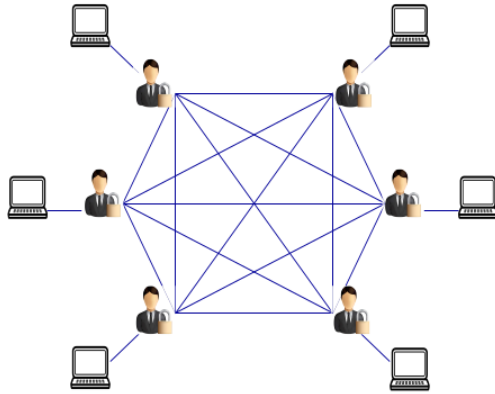
δεδομένων. Καθώς αυτά τα μητρώα/ εγγραφές αποθηκεύονται σε αμετάβλητα κατάστιχα, υπάρχει λιγότερη ανάγκη για κεντρικές οντότητες επικύρωσης συναλλαγών.

2.3.3.3 Αμετάβλητα δεδομένα

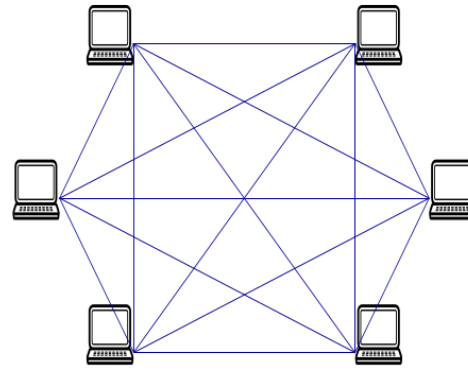
Το αμετάβλητο των δεδομένων δεν είναι απαραίτητως η πιο σημαντική πτυχή σε όλες τις αρχιτεκτονικές λύσεις, καθώς ορισμένα από τα δεδομένα ίσως πρέπει να αλλάξουν. Παρ' όλα αυτά συνήθως απαιτείται να διατηρηθεί ένα αρχείο καταγραφής της αλλαγής και τα εμπλεκόμενα μέρη θα πρέπει να ενημερωθούν για αυτή. Τυπικά σε μια αρχιτεκτονική blockchain δεν προβλέπεται η τροποποίηση ή διαγραφή παλαιών μπλοκ, για λόγους που αναφέρθηκαν παραπάνω (permissionless blockchain). Σε περίπτωση όμως που τα αρχεία στους κόμβους γίνουν υπερβολικά σε μέγεθος ή εάν υπάρχουν λόγοι συμμόρφωσης με νομοθετικά πλαίσια, ενδέχεται να χρειαστεί να γίνουν τέτοιες διαγραφές (permissioned blockchain).

2.3.3.4 Δικαιώματα και προσβασιμότητα συστήματα (Ιδιωτικά και δημόσια)

Υπάρχουν ορισμένες περιπτώσεις αρχιτεκτονικών blockchain που έχουν σχεδιαστεί από εταιρείες ή οργανισμούς για συγκεκριμένες εφαρμογές με περιορισμένη πρόσβαση στο κοινό. Τα πιο γνωστά ιδιωτικά blockchains είναι μέρος του έργου Hyperledger, το οποίο είναι μια συνεργασία μεταξύ πολλών γνωστών εταιρειών και φιλοξενείται από το Ίδρυμα Linux. Η πρόσβαση σε αυτά τα blockchain ή η συμμετοχή στο πρωτόκολλο συναίνεσης επιτρέπεται και εξαρτάται από τρίτο μέρος. Επομένως, τα ιδιωτικά blockchains "συγκεντρώνονται" σε κάποιο βαθμό, κάτι που έρχεται σε αντίθεση με την αρχική ιδέα του blockchain να αποκεντρωθεί και να διανεμηθεί πλήρως. Ωστόσο, αυτά τα blockchain έχουν χαμηλότερες υπολογιστικές απαιτήσεις και μεγαλύτερες ταχύτητες απόκρισης δικτύου που τα καθιστά κατάλληλα για εφαρμογές IoT. Σε ορισμένα ιδιωτικά blockchain, ορισμένοι από τους κόμβους έχουν πλήρη πρόσβαση σε όλα τα αποθηκευμένα μπλοκ. Έτσι, τα ιδιωτικά blockchains προσφέρουν περισσότερη ιδιωτικό ήτα στις πληροφορίες. Τα ιδιωτικά blockchains είναι πιο ασφαλή από τις παραδοσιακές βάσεις δεδομένων λόγω της χρήσης κρυπτογραφικών πρωτοκόλλων παρόμοιων με τα δημόσια αλλά δεν είναι τόσο ασφαλή (όσο τα δημόσια) τα οποία χρησιμοποιούν πρωτόκολλα εντατικής υπολογιστικής όπως η απόδειξη της εργασίας. Έτσι, υπάρχει η πιθανότητα παραβίασης των αποθηκευμένων δεδομένων σε ιδιωτικά blockchain. Τέλος υπάρχουν και μερικώς ιδιωτικά blockchain που ονομάζονται κοινοπραξίες ή κοινοπρακτικά blockchain. Ενώ ένα πλήρως ιδιωτικό blockchain ελέγχεται από μία εταιρεία, οι κοινοπραξίες blockchain ελέγχονται από διάφορα ιδρύματα, τα οποία συμμετέχουν άμεσα στο πρωτόκολλο συναίνεσης. Τα ιδιωτικά blockchain μπορούν να ακολουθήσουν διαφορετικές μεθόδους συναίνεσης όπως πρακτική ανοχή βυζαντινών σφαλμάτων, απόδειξη του παρελθόντος χρόνου και απόδειξη πονταρίσματος που θα περιγράψουν στην επικείμενη ενότητα. Τα ιδιωτικά και τα δημόσια blockchain συγκρίνονται στις παρακάτω εικόνες.



Σχήμα 5 Private blockchain



Σχήμα 6 Public blockchain

2.3.3.5 Σύγκριση βάση των δικαιωμάτων και προσβασιμότητας

Πίνακας 1 Θεμελιώδη χαρακτηριστικά της blockchain τεχνολογίας στα δημόσια, ιδιωτικά και κοινοπρακτικά blockchain συστήματα

	ΔΗΜΟΣΙΑ	ΙΔΙΩΤΙΚΑ	ΚΟΙΝΟΠΡΑΚΤΙΚΑ
ΑΝΩΝΥΜΙΑ	Ναι	Όχι	Όχι
ΑΜΕΤΑΒΛΗΤΟΤΗΤΑ	Ναι	Όχι	Όχι
ΑΠΟΔΟΤΙΚΟΤΗΤΑ	Χαμηλή	Υψηλή	Υψηλή
ΔΙΑΦΑΝΕΙΑ	Απόλυτη	Σχετική	Σχετική
ΑΠΟΚΕΝΤΡΩΣΗ	Πλήρης	Μηδενική	Μερική
ΣΥΝΕΚΤΙΚΟΤΗΤΑ	Ναι	Ναι	Ναι
ΕΠΕΚΤΑΣΙΜΟΤΗΤΑ	Ελάχιστη	Υψηλή	Υψηλή
ΕΥΚΑΜΨΙΑ	Χαμηλή	Υψηλή	Μέτρια
ΔΙΑΘΕΣΙΜΟΤΗΤΑ	Πλήρης	Μηδενική	Ελάχιστη
ΕΛΕΓΚΤΙΚΗ	Μηδενική	Απόλυτη	Μερική

2.4 Κρυπτογραφία

Η κρυπτογραφία, περιλαμβάνει παραδοσιακά δυο πολύ συγγενείς περιοχές: την κρυπτογραφία και την κρυπτοανάλυση. Η κρυπτογραφία ασχολείται με την κρυπτογράφηση των μηνυμάτων, δηλ. Τον μετασχηματισμό των μηνυμάτων σε κρυπτογραφικά κείμενα υπό τη χρήση ενός κλειδιού με τρόπο ώστε το κρυπτογραφικό κείμενο (μετασχηματισμένο μήνυμα) να μπορεί να ανακτηθεί από το κρυπτό- σύστημα μονό με τη γνώση του κλειδιού. Η κρυπτοανάλυση είναι το αντίστοιχο της κρυπτογραφίας και ασχολείται με την ανάκτηση κρυπτογραφικών κειμενων από μηνύματα χωρίς τη γνώση του κλειδιού.

2.4.1 Hash

Το hash αποτελεί έναν σύντομο κώδικα καθορισμένου μήκους που χρησιμεύει ως δακτυλικό αποτύπωμα για ένα ψηφιακό έγγραφο. Ένα πρόγραμμα που ονομάζεται hash-generator επιτρέπει σε έναν χρήστη να τροφοδοτήσει (input) οποιαδήποτε σειρά κειμένου και να δημιουργήσει ένα μοναδικό αναγνωριστικό (output). Κάθε φορά που εκτελείται η ίδια σειρά κειμένου μέσω του hash-generator, θα δοθεί το ίδιο αναγνωριστικό εγγράφου. Η συμβολή του κατακερματισμού ως μηχανισμός για την αντιμετώπιση των βασικών αρχών της ασφάλειας του λογισμικού (Εμπιστευτικότητα, Ακεραιότητα, Μη Αποποίηση Ευθυνών) είναι σημαντική: αν αλλάξει ένα γράμμα σε ένα έγγραφο, θα δημιουργηθεί αυτόματα ένα εντελώς διαφορετικό αναγνωριστικό. Τα hash είναι μονόδρομοι (Gurta, S2017). Αυτό σημαίνει ούτι η γεννήτρια κατακερματισμού μπορεί να χρησιμοποιηθεί για να δημιουργήσει ένα hash από το έγγραφο, αλλά είναι μαθηματικά αδύνατο να δημιουργηθεί ένα έγγραφο από ένα hash. Σε ένα blockchain, κάθε μπλοκ συναλλαγών είναι εξασφαλισμένο με τη προσθήκη ενός hash στο μπλοκ πληροφοριών, καθώς και του προηγούμενου μπλοκ, επιτρέποντας έτσι σε όλα τα μέρη να εγγυηθούν ότι καμιά από τις συναλλαγές δεν έχει τροποποιηθεί ή αλλοιωθεί (Lemieux, 2016).

2.5 Αξιολόγηση ασφάλειας

Στη παρούσα ενότητα θα παραθέτουμε τα θέματα ασφάλειας που άπτονται των ενδιαφερόντων της διατριβής. Συγκεκριμένα, θα δούμε τα βασικά θέματα των λειτουργιών και αρχιτεκτονικών ασφαλείας, θα αναφερθούμε στην βασική θεωρία της κρυπτογραφίας και τους κύριους μηχανισμούς ταυτοποίησης. Η Ασφάλεια των Πληροφοριακών Συστημάτων (Information Security) ασχολείται με την ασφάλεια των πληροφοριών. Ακολουθεί ως αρχές την "CIA Triad"- Confidentiality- Integrity- Availability (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα). Ωστόσο έχουν προταθεί και εναλλακτικές ταξινομήσεις των βασικών αρχών, όπως η Parkerian Hexad [Park98]. Αυτή επεκτείνει τη τριάδα CIA προτείνοντας έξι ατομικά στοιχεία (atomic elements), τα οποία δεν μπορούν να διασπαστούν σε απλούστερα. Αυτά είναι: Confidentiality, Possession, Integrity, Authenticity, Availability και Utility (Εμπιστευτικότητα, Κατοχή, Ακεραιότητα, Αυθεντικότητα, Διαθεσιμότητα και Χρήση). Όλες οι άλλες λειτουργίες ασφάλειας είναι παράγωγα αυτών των ατομικών στοιχείων.

Συστήματα βασισμένα στο Blockchain θα μπορούσαν δυνητικά να βοηθήσουν στη βελτίωση της «άμυνας» στον κυβερνοχώρο, καθώς η τεχνολογία μπορεί να εξασφαλίσει, να αποτρέψει δόλιες δραστηριότητες μέσω μηχανισμών συναίνεσης και να εντοπίσει παραβίαση δεδομένων βάσει των υποκείμενων χαρακτηριστικών της αμεταβλητότητας, διαφάνειας, ελέγχου, κρυπτογράφησης δεδομένων και λειτουργικής ανθεκτικότητας (ενός σημείου αποτυχίας).

2.5.1 Έλεγχος ταυτότητας και εξουσιοδότηση (authentication- authorization)

Το Blockchain παρέχει μεθόδους που ενθυλακώνουν κανόνες περί απορρήτου δεδομένων μιας και εφαρμόζουν το δικαίωμα «στη λήθη» (right to be forgotten), οπότε εγγυάται πως τίποτα δεν θα διαγραφεί. Το Blockchain παρέχει γρήγορο και αποτελεσματικό σχήμα ελέγχου ταυτότητας multicast, έτσι ώστε όλοι οι δέκτες να μοιράζονται το δημόσιο κλειδί των αποστολών. Πάνω απ' όλα το Blockchain παρέχει κατάλληλες διαδικασίες διαχείρισης κλειδιών, ασφαλείς βασικές πρακτικές διακυβέρνησης. Ένα παράδειγμα επαρκούς προστασίας είναι η χρήση κλειστών αποθετηρίων κλειδιών ειδικού σκοπού που εφαρμόζουν τεχνολογίες όπως Hardware Security Modules [8] για την διατήρηση των βασικών ευαίσθητων δεδομένων (κλειδιών).

2.5.2 Εμπιστευτικότητα (confidentiality)

Το Blockchain μπορεί να παρέχει προηγμένους ελέγχους ασφαλείας, για παράδειγμα, αξιοποιώντας την υποδομή δημόσιου κλειδιού (PKI) για έλεγχο ταυτότητας και εξουσιοδότηση μερών και κρυπτογράφηση των επικοινωνιών τους (το PKI είναι ένα σύνολο ρόλων, πολιτικών και διαδικασιών που απαιτούνται για τη δημιουργία, διαχείριση, χρήση, αποθήκευση, και ανάκληση ψηφιακών πιστοποιητικών και διαχείριση κρυπτογράφησης δημόσιου κλειδιού. Δεν υπάρχει ανάγκη ελέγχου της πρόσβασης στο δίκτυο, καθώς τα πρωτόκολλα αλυσίδων επιτρέπουν σε οποιονδήποτε να έχει πρόσβαση και να συμμετέχει στο δίκτυο, αρκεί να εγκαταστήσει πρώτα το λογισμικό. Σε μια κατάσταση όπου ένας εισβολέας προσπαθεί να κάνει έναν άνδρα-στη-μέση (man in the middle) επίθεση ο εισβολέας δεν θα είναι σε θέση ούτε να αποκαλύψει την ταυτότητα του συνομιλητή ούτε να αποκαλύψει δεδομένα κατά τη μεταφορά. Επιτυγχάνεται με τη χρήση ζεύγους δημόσιου/ ιδιωτικού κλειδιού και διεύθυνσης που προέρχεται χρησιμοποιώντας λειτουργίες κατακερματισμού και ελέγχου στο δημόσιο κλειδί. Απομένει μόνο η έκθεση της διεύθυνσης κάτι το οποίο δεν αποτελεί κενό ασφαλείας υψηλού κινδύνου.

2.5.3 Ακεραιότητα (integrity)

Η τεχνολογία Blockchain μπορεί να διασφαλίσει, να αποτρέψει δόλιες δραστηριότητες μέσω μηχανισμών συναίνεσης και να εντοπίσει παραβίαση δεδομένων με βάση τα υποκείμενα χαρακτηριστικά της αμετάβλητης, διαφάνειας, ελέγχου, κρυπτογράφησης δεδομένων και λειτουργικής ανθεκτικότητας. Η διατήρηση της συνοχής των δεδομένων και η διασφάλιση της ακεραιότητας, καθ' όλη τη διάρκεια του κύκλου ζωής της, είναι ζωτικής σημασίας σε αποκεντρωμένα περιβάλλοντα, έτσι μια μέθοδος κατακερματισμού SHA-384 παρέχει αναλλοίωτες αποδείξεις γεγονότων γράφοντας το κατακερματισμό των συναλλαγών σε αυτό. Κάθε νέα συναλλαγή που προστίθεται σε Blockchain θα έχει ως αποτέλεσμα την αλλαγή της παγκόσμιας κατάστασης του κατάστιχου. Αυτό συνεπάγεται ότι με κάθε νέα επανάληψη του συστήματος, η προηγούμενη κατάσταση θα αποθηκευτεί, με αποτέλεσμα ένα πλήρως ανιχνεύσιμο αρχείο καταγραφής ιστορικού. Οι πληροφορίες που συλλέγονται ως μέρος των δεσμευμένων συναλλαγών είναι εξαιρετικά δύσκολο να αλλάξουν (τουλάχιστον δεδομένης της υφιστάμενης τεχνολογίας).

2.5.4 Μη αποκλεισμός (non- repudiation)

Το Blockchain παρέχει ιχνηλασιμότητα δεδομένου ότι κάθε συναλλαγή που προστίθεται στο κατάστιχο είναι ψηφιακά υπογεγραμμένη και χρονική σημασμένη, Με αυτό τον τρόπο το σύστημα μπορεί να εντοπίσουν συναλλαγές για μια συγκεκριμένη χρονική περίοδο και να προσδιορίσει τα εμπλεκόμενα μέρη της.

2.5.5 Διαθεσιμότητα

Το γεγονός ότι ένα σύστημα βασισμένο στο Blockchain είναι καταναμεμημένο και κοινόχρηστο (όπως περιγράφεται παραπάνω) το καθιστούν ανθεκτικό σε διακοπές λειτουργίας λόγω αποτυχίας υλικού. Δεν υπάρχει κανένα μοναδικό σημείο αποτυχίας, οπότε παρέχει ελαστικότητα λειτουργίας.

2.6 Μηχανισμοί συναίνεσης (Consensus Mechanisms)

Η συναίνεση ορίζεται ως τα ιδανικά και τις αξίες που αναζητούν άνθρωποι διαφορετικών στρωμάτων και συμφερόντων σε μια κοινωνία [9]. Οι μηχανισμοί συναίνεσης διασφαλίζουν τη σύγκλιση προς μια ενιαία, αμετάβλητη έκδοση του κατάστιχου. Επιτρέπουν στους κόμβους του δικτύου να συμφωνήσουν σχετικά με τις

πληροφορίες που καταγράφονται στα κατανεμημένα κατάστιχα, λαμβάνοντας υπόψη το γεγονός ότι ορισμένοι φορείς μπορεί να είναι αναξιόπιστοι ή κακόβουλοι.

Οι αλγόριθμοι συναίνεσης είναι η διαδικασία επιλογής μεθόδου για την επίτευξη του ίδιου τελικού στόχου, που είναι ο συντονισμός της συμφωνίας σε ένα αποκεντρωμένο δίκτυο. Είναι ένας τύπος απόφασης βασισμένος στα πλαίσια της ομοφωνίας ανεξάρτητα της ατομικής επιλογής του κόμβου. Ομοφωνία σημαίνει απλώς μια γενική συμφωνία, αλλά για ένα peer-to-peer δίκτυο υπολογιστών που δεν έχουν ιεραρχία, διαχειριστή, συντονιστή ή διευθυντή, η επίτευξη συναίνεσης απαιτεί τον σωστό συνδυασμό κρυπτογράφησης, ανταμοιβές και τιμωρίες. Αυτοί οι υπολογιστές στο δίκτυο, επίσης γνωστοί ως κόμβοι, πρέπει να έχουν κάποιο βασικό σύνολο κανόνων για το πώς να συμφωνήσουν ή να προσδιορίσουν τι είναι αλήθεια. Οι αλγόριθμοι συναίνεσης είναι δύο τύπων με βάση την απόδειξη και με βάση την ψηφοφορία [10].

Ως ο πυρήνας ενός συστήματος blockchain, ο μηχανισμός συναίνεσης όχι μόνο βοηθά στη διατήρηση της συνοχής των δεδομένων των κόμβων, αλλά επιπλέον συμμετέχει στην έκδοση διακριτικών και την πρόληψη επιθέσεων. Από τη στιγμή που γεννήθηκε το πρώτο σύστημα blockchain, οι μηχανισμοί συναίνεσης βελτιώνονται συνεχώς και επεκτάθηκαν σε πολλαπλούς νέους κλάδους (εκτός blockchain).

2.6.1 Αλγόριθμος συναίνεσης βάσει απόδειξης (Proof-based Consensus Algorithm)

Στον αλγόριθμο συναίνεσης βάσει απόδειξης, οι κόμβοι που συμμετέχουν στο δίκτυο πρέπει να λύσουν ένα κρυπτογραφικό πρόβλημα για να αποκτήσουν το δικαίωμα προσάρτησης του μπλοκ. Στο δημόσιο blockchain, οι κόμβοι λαμβάνουν ανταμοιβές αφού προσθέσουν το block στο blockchain. Η πρώτη έκδοση του αλγόριθμου συναίνεσης βάσει αποδείξεων είναι η απόδειξη της εργασίας που πρότεινε ο Satoshi Nakamoto [11]. Μέχρι σήμερα υπάρχουν διαφορετικές εκδόσεις συναίνεσης βάσει αποδείξεων όπως παρακάτω:

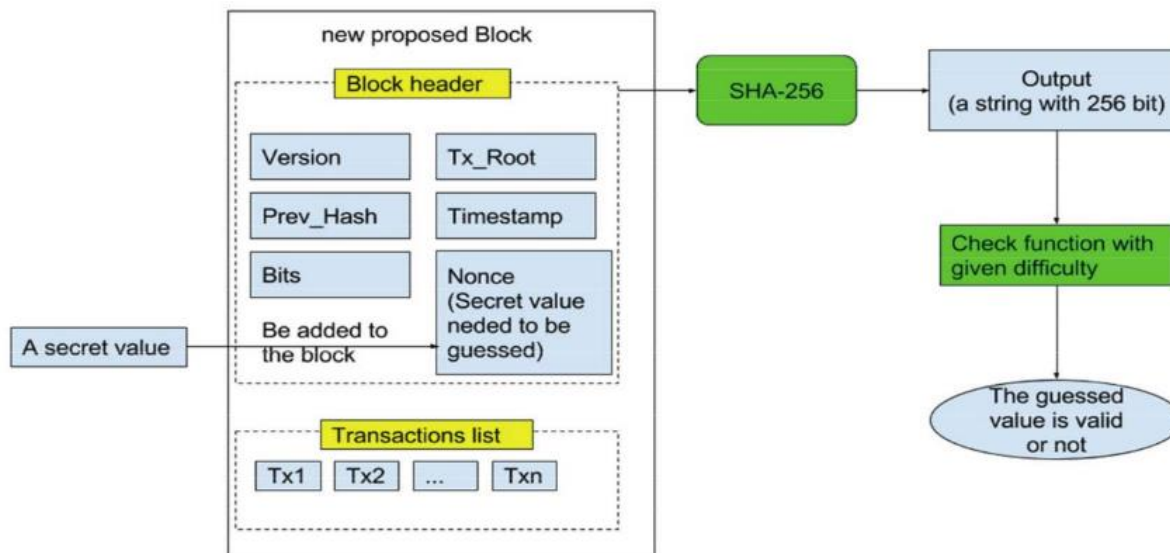
2.6.1.1 Απόδειξη εργασίας - επίλυση μαθηματικού παζλ. (POW)

Θεμελιώδης αρχή: Η επίλυση του είναι δύσκολη αλλά είναι εύκολο το να ελέγξεις το αποτέλεσμα της διαδικασίας.

Ο αλγόριθμος συναίνεσης PoW περιλαμβάνει την επίλυση ενός μαθηματικού προβλήματος που απαιτεί υπολογιστικές προκλήσεις προκειμένου να δημιουργηθούν νέα block στην αλυσίδα του blockchain. Η διαδικασία είναι γνωστή ως «εξόρυξη» και οι κόμβοι του δικτύου που ασχολούνται με την εξόρυξη είναι γνωστοί ως «ανθρακωρύχοι» (miners). Συγκεκριμένα στόχος είναι η επίλυση των δύσκολων υπολογιστικών μαθηματικών προβλημάτων για την εύρεση της κατάλληλης διαδικασίας που έπειτα μπορείς να προσαρτήσει το νέο block στην αλυσίδα τηρώντας ταυτόχρονα συγκεκριμένους κανόνες. Τα άτομα που είναι υπεύθυνα για την εξόρυξη ενός νέου block ανταγωνίζονται μεταξύ τους για να βρουν την λύση σε έναν ψευδοτυχαίο αριθμό που σε συνδυασμό με τα δεδομένα που βρίσκονται στα blocks αλλά και μιας συνάρτησης κατακερματισμού (hash) πρέπει να παράξουν ένα αποτέλεσμα που να ταιριάζει με συγκεκριμένες συνθήκες. Όταν βρεθεί ένα αποτέλεσμα που ταιριάζει, εκπέμπεται ταυτόχρονα σε ολόκληρο το δίκτυο και οι άλλοι κόμβοι επαληθεύουν την εγκυρότητα του αποτελέσματος. Κίνητρο για την εργασία τους είναι πως ο κόμβος αυτός που θα βρει την λύση, δηλαδή ο Miner που έρχεται πρώτος στην εύρεση της σωστής διαδικασίας, θα ανταμειφθεί με την προκαθορισμένη αμοιβή που υπάρχει από το blockchain για κάθε νέο block που προστίθεται αλλά και με το έσοδο για την περάτωση της συναλλαγής που δόθηκε προς πραγματοποίηση.

Όπως φαίνεται στο παρακάτω σχήμα, μια μυστική τιμή υπολογίζεται από τον κόμβο «ανθρακωρύχος». Αφού θέσει μια (υποθετική/ πιθανή) τιμή που ονομάζεται nonce, γίνεται κατακερματισμός με τη βοήθεια της συνάρτησης SHA 256 και η έξοδος ελέγχεται στο δεδομένο επίπεδο δυσκολίας. Εάν η τιμή κατακερματισμού γίνει αποδεκτή, τότε το

nonce υπολογίστηκε επίσης σωστά. Σε αντίθετη περίπτωση επαναλαμβάνεται ολόκληρη η διαδικασία (δηλαδή θέτει μια νέα τιμή nonce και την ελέγχει), έως ότου βρεθεί η σωστή. Εφόσον εντοπιστεί η σωστή τιμή nonce, επιτρέπεται στους κόμβους να μεταδίδουν την



Σχήμα 7 Μηχανισμός συναίνεσης Proof of work

τιμή κατακερματισμού των μπλοκ και την τιμή nonce σε άλλους κόμβους στο δίκτυο για επαλήθευση και προσάρτηση στο δικό τους κατάστιχο. Πλεονέκτημα της μεθόδου είναι πως είναι πολύ ασφαλής αν και προϋποθέτει υψηλή υπολογιστική ισχύ. Λόγω των μειονεκτημάτων της, αναπτύχθηκε το Proof of Stake και πολλοί άλλοι αλγόριθμοι συναίνεσης με βάση την απόδειξη.

2.6.1.2 Απόδειξη συμμετοχής Proof of Stake – δίκαιος καταμερισμός εργασίας. (POS)

Θεμελιώδης αρχή: Η εμπιστοσύνη στο δίκτυο υπάρχει μέσω των ατόμων που επικυρώνουν τις συναλλαγές που θέτουν ως δέσμευση τους δικούς του πόρους για την δημιουργία ενός νέου Block. Όσο μεγαλύτερος είναι ο αριθμός των κρυπτονομισμάτων που κατέχει κάποιος, τόσο μεγαλύτερη είναι η πιθανότητα προσάρτησης.

Ο όρος "staking" αναφέρεται στην πράξη των επικυρωτών που δεσμεύουν πόρους στο σύστημα, επομένως, οι επικυρωτές μπορούν να συμμετάσχουν στη διαδικασία παραγωγής νέων μονάδων μόνον εάν «κλειδώσουν» τα coins τους. Τα «κλειδωμένα» αυτά κεφάλαια θα λειτουργήσουν τότε ως εξασφάλιση, πράγμα που σημαίνει ότι εάν κάποια άτομα προβούν σε κακόβουλες επικυρώσεις πιθανότατα θα χάσουν το ποντάρισμά τους και θα εκδιωχθούν από το δίκτυο εάν δεν επέλθει η συναίνεση. Σε αντίθετη περίπτωση οι έντιμοι επικυρωτές θα επιβραβευτούν με την αμοιβή του νέου block που θα παραχθεί. Στον αλγόριθμο η επιλογή του ατόμου που επικυρώνει την διαδικασία, γίνεται ανάλογα με το μερίδιο που του ανήκει. Δηλαδή εάν ένας κατέχει το 10% των κρυπτονομισμάτων θα μπορεί να επικυρώσει το 10% των συναλλαγών. Η ιδέα είναι ότι όσο μεγαλύτερη αναλογία κρυπτονομισμάτων έχουν τα άτομα που επικυρώνουν τις συναλλαγές, τόσο λιγότερο ενδιαφέρον θα έχουν στο να χειραγωγήσουν την διαδικασία της επικύρωσης των συναλλαγών.

Όπως αναλύεται παραπάνω το PoW υποτίθεται ότι είναι «άδικο»: ενώ μερικοί «ανθρακωρύχοι» που διαθέτουν σύγχρονο και ισχυρό εξοπλισμό θα μπορούσαν να βρουν

το σωστό nonce ταχύτερα, άλλοι με μικρότερη υποδομή θα δυσκολεύονταν να είναι οι πρώτοι που το θα βρουν. Το PoS υποτίθεται ότι αντιμετωπίζει αυτήν την ανισότητα. Για πρώτη φορά παρουσιάστηκε και συζητήθηκε στο φόρουμ Bitcoin το 2011 [12]. Το PoS είχε αρκετές παραλλαγές. Η βασική ιδέα αυτού του αλγορίθμου συναίνεσης είναι η χρήση του stake (κεφάλαιο) για να αποφασίσει ποιος θα έχει την ευκαιρία να εξορύξει το επόμενο μπλοκ της αλυσίδας. Η χρήση του stake ως απόδειξη έχει ένα πλεονέκτημα: όποιος κατέχει μεγάλο μερίδιο συμμετοχής (κεφάλαιο) είναι ταυτόχρονα και πιο αξιόπιστος. Δεν θα επιλέξει να προβεί σε δόλιες ενέργειες έναντι της ακεραιότητας της αλυσίδας γιατί εμπεριέχει σε μεγάλο βαθμό το κέρδος του. Επιπλέον, η απόδειξη συμμετοχής θα απαιτούσε από τους εισβολείς να κατέχουν τουλάχιστον το 51% συμμετοχής στο δίκτυο για να εκτελέσουν μια επίθεση διπλής δαπάνης (double spending attack), κάτι που είναι πολύ δύσκολο.

Υπάρχουν επί του παρόντος δύο δημοφιλή είδη συναίνεσης που χρησιμοποιούν το PoS: εκείνο που βασίζεται στο καθαρό ποντάρισμα για τη συναίνεση, και το υβριδικό, το οποίο συνδυάζει PoS και PoW.

2.6.1.3 Απόδειξη παρελθόντος χρόνου

Θεμελιώδης αρχή: τα μπλοκ δημιουργούνται σε ένα αξιόπιστο περιβάλλον σε ίσες περιόδους

Προτάθηκε αρχικά από την (Intel) [13], και χρησιμοποιήθηκε σε μια πλατφόρμα Blockchain με το όνομα Sawtooth Lake [14]. Αυτός ο τύπος συναίνεσης εκτελείται σε ένα ειδικό περιβάλλον το οποίο ονομάζεται «αξιόπιστο περιβάλλον εκτέλεσης» (trusted execution environment T.E.E.) [15], κάνοντας χρήση μιας ειδικής, φυσικής συσκευής της Intel γνωστή ως «Software Guard Extensions (XGS)». Προκειμένου να εκτελέσουν τον αλγόριθμο συναίνεσης, οι ανθρακωρύχοι αιτούνται ταυτόχρονα χρόνο αναμονής από έναν αξιόπιστο θύλακα, ο οποίος είναι επίσης γνωστός ως συνάρτησης συναίνεσης μέσα στο XGS. Στη συνέχεια, όλοι οι ανθρακωρύχοι θα λάβουν τον χρόνο αναμονής από τον θύλακα, και μαζί θα περιμένουν μέχρι να παρέλθει ο χρόνος που τους αναλογεί. Όταν παρέλθει ο χρόνος αναμονής ένας ανθρακωρύχου, αλλά δεν έχει βρει κανέναν να έχει τελειώσει νωρίτερα τον αγώνα αναμονής, θα μεταδώσει σε όλους τους άλλους ανθρακωρύχους ότι είναι ο νικητής, γεγονός που του δίνει την ευκαιρία να προσαρτήσει νέο μπλοκ. Εν ολίγοις, ο ανθρακωρύχος που διαθέτει τον συντομότερο λαμβανόμενο χρόνο αναμονής, λογικά θα είναι αυτός που θα προσαρτήσει το νέο μπλοκ. Προκειμένου να υποστηριχθεί αυτό το είδος συναίνεσης, χρησιμοποιούνται δύο συναρτήσεις: η CreateTime η οποία θα ενημερώσει τους ανθρακωρύχους για το χρόνο που πρέπει να περιμένουν και η συνάρτηση CheckTimer η οποία θα ελέγξει εάν ο ανθρακωρύχος έχει περιμένει αρκετό χρόνο ή όχι. Επειδή αυτή η συναίνεση εκτελείται σε TEE που παρέχεται από συσκευές XGS, υποτίθεται ότι πως με την χρήση των δύο παραπάνω συναρτήσεων η παραποίηση/ εξαπάτηση είναι πολύ δύσκολη.

2.6.1.4 Απόδειξη τύχης - τυχαία επιλογή.

Ο Milutinovic et al [16] πρότεινε ένα είδος συναίνεσης, το οποίο επίσης εκτελείται στο TEE με συσκευές XGS, που ονομάζεται απόδειξη τύχης. Η λειτουργία έχει ως εξής, αφού συγχρονιστούν όλα τα κατάστιχα όλων των ανθρακωρύχων, κάθε ανθρακωρύχος θα δημιουργήσει για τον εαυτό του ένα νέο μπλοκ και θα το προσαρτήσει στην δική του αλυσίδα, τότε θα εκχωρηθεί ένας τυχαίος αριθμός από 0 έως 1 σε κάθε δημιουργημένη αλυσίδα, ο λεγόμενος «τυχερός αριθμός». Όλοι οι κόμβοι θα πρέπει να συμφωνήσουν ότι η αλυσίδα με το συνολικά μεγαλύτερο «τυχερό αριθμό» θα είναι η κύρια αλυσίδα (με την εγκεκριμένη προσάρτηση). Ως αποτέλεσμα, η απόδειξη της τύχης θεωρείται δίκαιη για όλους τους ανθρακωρύχους. Επιπλέον, θα ήταν πολύ δύσκολο να πραγματοποιηθούν

επιθέσεις, όπως η επίθεση διπλών δαπανών, επειδή ο εισβολέας θα πρέπει να είναι πολύ τυχερός να εκτελέσει τις παράνομες ενέργειές του με επιτυχία.

2.6.1.5 Απόδειξη χώρου (space) - απαιτείται σκληρός δίσκος μεγαλύτερου μεγέθους.

Θεμελιώδης αρχή: Η ποσότητα εργασίας που θα εκτελέσει ένας ανθρακωρύχος εξαρτάται από το ποσό του ελεύθερου χώρου στο δίσκο που αφιερώνεται στη διαδικασία plotting.

Το Proof of Space [17], γνωστό και ως Proof of Capacity (PoC), χρησιμοποιείται στα κρυπτονομίσματα SpaceMint [18] και Burst [19] παρέχοντας πιο διανεμημένη και οικονομική συμμετοχή και μικρότερη κατανάλωση πόρων συγκριτικά με το PoW. Αντί για υπολογιστικές μονάδες οι χρήστες πρέπει να επενδύσουν σε, δεδομένα φθινότερο, αποθηκευτικό χώρο για να μπορέσουν να ολοκληρώσουν τα απαραίτητα υπολογιστικά προβλήματα στο σύστημα. Ο PoC αλγόριθμος κατά τη διάρκεια της εργασίας δημιουργεί πολλά μεγάλα σύνολα δεδομένων στο σκληρό δίσκο (plots), με τους κόμβους να διεκδικούν το δικαίωμα του επόμενου μπλοκ ανάλογα με την ποσότητα των δεδομένων που διαθέτουν. Εφόσον ένας κόμβος δεν διαθέτει επαρκή αποθηκευτικό χώρο αποκλείεται από την συμμετοχή στη διαδικασία συναίνεσης. Συνεπώς, αν και το PoC είναι μία ενεργειακά και χρηματικά περισσότερο συμφέρουσα επιλογή από το PoW, η διαδικασία ομοφωνίας που ακολουθείται φαίνεται να ευνοεί τους κόμβους εκείνους που διαθέτουν περισσότερο αποθηκευτικό χώρο στις υπολογιστικές τους μονάδες δημιουργώντας πρόβλημα στην έννοια της αποκέντρωσης. Επίσης η ασφάλεια δεν είναι δεδομένη καθώς οι κακόβουλοι χρήστες δεν ελέγχονται από το σύστημα με αποτέλεσμα να μπορούν πιθανώς να το εκμεταλλευτούν, εισάγοντας για παράδειγμα κακόβουλο λογισμικό εξόρυξης.

2.6.2 Voting Consensus Algorithm

Οι μηχανισμοί συναίνεσης που βασίζονται σε αλγόριθμους ψηφοφορίας αναφέρονται αποκλειστικά στα ιδιωτικά blockchain συστήματα, στα οποία οι κόμβοι είναι δεδομένοι. Αυτή είναι και η δομική διαφορά με τα παραπάνω συστήματα συναίνεσης στα οποία σε γενικές γραμμές επιτρέπεται σε νέους κόμβους να ενταχθούν ή/ και να αποσυρθούν από το δίκτυο ελέγχου κατά το δοκούν.

Στα συστήματα ψηφοφορίας προαπαιτείται η δημοσίευση στο δίκτυο του block πριν την προσάρτηση του. Για να προχωρήσει η προσάρτηση στην αλυσίδα ενός κόμβου θα πρέπει κατ' ελάχιστον x (προκαθορισμένο κατώτατο όριο συναίνεσης) άλλοι κόμβοι να συμφωνούν στην προσάρτηση και μόνο τότε ολοκληρώνεται. Αν υπάρχουν αρκετοί κόμβοι εκτός λειτουργίας στο δίκτυο ενδέχεται να μην καλύπτεται η απαίτηση του προκαθορισμένου κατώτατου ορίου συναίνεσης που οδηγεί σε «Περίπτωση Αστοχίας» (Crashing case) του δικτύου. Για να αποτραπεί η «Περίπτωση Αστοχίας» σε δίκτυο με f κόμβους, θα πρέπει κατ' ελάχιστον να υπάρχουν $f+1$ κόμβοι σε κανονική λειτουργία [20]. Η «Περίπτωση Αστοχίας» αναπαράγεται παρόμοια με το κλασικό πρόβλημα «Byzantine στρατηγούς» (Byzantine generals) όπως προτάθηκε από τους Lamport et al. [21]:

Μια ομάδα Byzantine στρατηγών επιτίθενται σε ένα αντίπαλο στρατόπεδο. Αποφασίζουν να χωρίσουν το στράτευμα τους σε N ομάδες, διοικούμενες από N στρατηγούς, οι οποίες θα επιτεθούν από διαφορετικές πλευρές. Αν συγχρονιστούν όλες οι ομάδες στην επίθεση θα κερδίσουν. Αν δεν κατορθώσουν να επιτεθούν ταυτόχρονα θα χάσουν. Συνεπακόλουθα οι στρατηγούς θα πρέπει να συμφωνήσουν στην ακριβή ώρα της επίθεσης, ανταλλάσσοντας μηνύματα (αποφάσεις) και τηρώντας το μήνυμα (απόφαση) της πλειοψηφίας. Για κακή τους τύχη υπήρχαν αντίπαλοι κατάσκοποι στις γραμμές τους, οι οποίοι αποπροσανατόλισαν την διαδικασία, μεταβιβάζοντας λανθασμένα μηνύματα

(αποφάσεις) στους στρατηγούς,. Με αποτέλεσμα οι στρατηγοί να μην καταφέρουν να επιτεθούν ταυτόχρονα.

Οι Lamport et al. [21] απέδειξαν πως η ανοχή του συστήματος τους σε f αποπροσανατολισμένους στρατηγούς είναι να τους ακολουθούν επιπλέον $2f+1$ «κανονικοί» στρατηγοί. Δηλαδή αν ο αριθμός των αποπροσανατολισμένων στρατηγών (έστω f) είναι μικρότερος κατά ένα βαθμό ($2f+1$) από τους «κανονικούς» στρατηγούς, η επικοινωνία τους θα είναι σωστή και θε κερδίσουν

Επιστρέφοντας σε όρους Blockchain, όταν ένας κόμβος εκτελεί το μηχανισμό συναίνεσης (αιτούμενος έλεγχο αποτελέσματος) ίσως κάποιοι άλλοι κόμβοι θέλουν να παραποιήσουν τη διαδικασία, στέλνοντας λανθασμένα αποτελέσματα στους υπόλοιπους. Αν καταφέρουν να αλλοιώσουν το αποτέλεσμα (είναι παραπάνω από την ανοχή του δικτύου), τα κατάστιχα θα είναι διαφορετικά ανάλογα τον κόμβο.

Οι συναίνεση ψηφοφορίας κατηγοριοποιείται ως εξής:

2.6.2.1 Byzantine – Nodes are crashed and unsettle

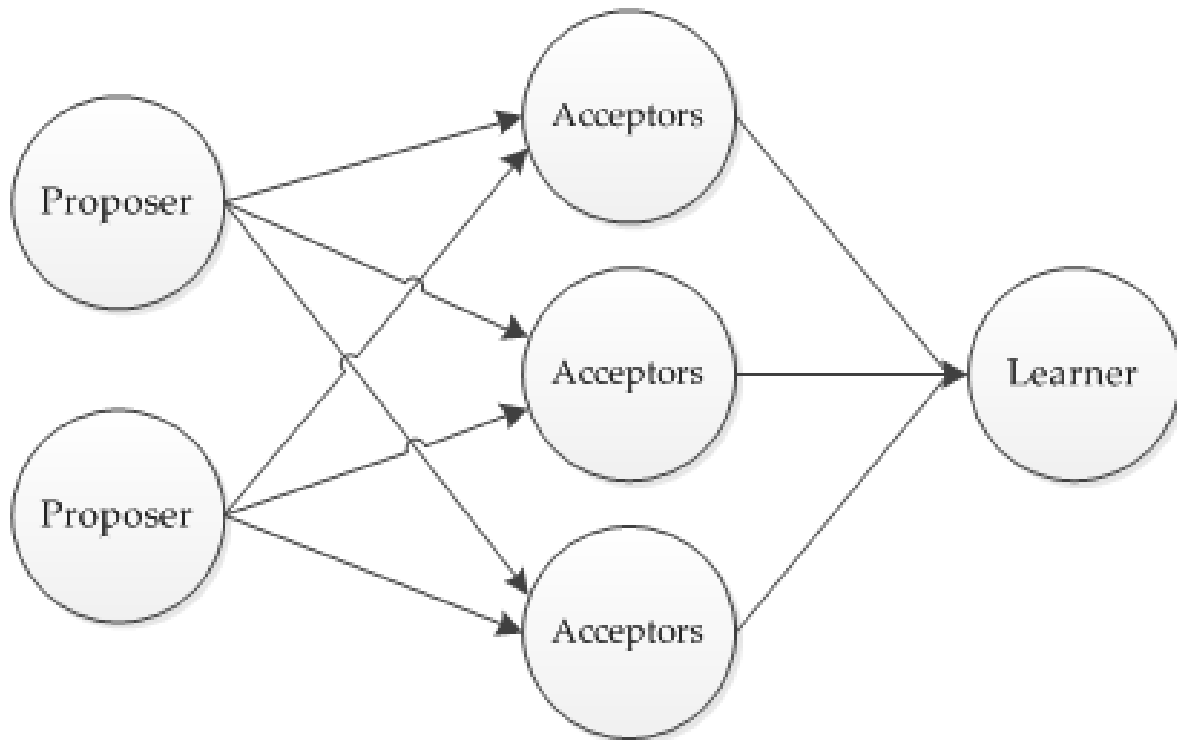
Πολλές εταιρείες όπως η IBM (για το Hyperledger Fabric [22]), χρησιμοποιούν την πλατφόρμα Hyperledger Blockchain platform [20]. Για την ανάπτυξη Hyperledger Fabric εφαρμόστηκε μια μορφή Byzantine fault tolerance που ονομάστηκε Practical Byzantine Fault Tolerance (PBFT) και προτάθηκε από τους Castro και Liskov [23]. Στο PBFT, υπάρχουν 2 τύποι κόμβων. Ένας κόμβος «καθοδηγητή» και κάποιοι «επικύρωσης». Αυτοί οι κόμβοι θα εκτελέσουν μια σειρά από αιτήματα προσάρτησης block στην αλυσίδα τους, όπως περιγράφεται παρακάτω στην εικόνα [20].

Αρχικά οι «client» στέλνουν αίτημα συναλλαγής στον κόμβο «επικύρωσης» που τους αντιστοιχεί. Έπειτα αναλαμβάνει ο κόμβος «επικύρωσης» αναλαμβάνει να επικυρώσει την συναλλαγή και να την επικοινωνήσει στους υπόλοιπους κόμβους συμπεριλαμβανομένου του «καθοδηγητή». Όταν συγκεντρωθούν στον «καθοδηγητή» μια προκαθορισμένη σειρά από αιτήματα (ταξινομημένα με βάση την ημερομηνία δημιουργίας) ή περάσει ένας προκαθορισμένος χρόνος αναμονής τους, τα ταξινομεί και τα παραθέτει σε ένα block (block αιτημάτων). Στη συνέχεια εκτελούνται οι 3 φάσεις του PBFT.

Η επίτευξη ομοφωνίας μέσω του PBFT δεν απαιτεί ιδιαίτερη ενεργειακή δαπάνη, ενώ το περιβάλλον εμπιστοσύνης που απαιτείται να κυριαρχεί στην αλληλεπίδραση μεταξύ των κόμβων καθιστά το δίκτυο ιδιαίτερα αποδοτικό με μηδαμινές χρονικές καθυστερήσεις και θεωρητικά δεκάδες χιλιάδες συναλλαγών. Αναφέρουμε τη λέξη θεωρητικά καθώς το PBFT έχει δοκιμαστεί σε δίκτυα της τάξεως των 10-20 κόμβων όπου οι συναλλαγές δεν μπορούν να επιτύχουν τόσο μεγάλες επιδόσεις. Η διαδικασία αυτή αποτελείται από πέντε στάδια-φάσεις: request, pre-prepare, prepare, commit, reply.

1. Στην φάση PRO- Προετοιμασίας (Pre-prepare) ο κόμβος «καθοδηγητή», επικοινωνεί το νέο αυτό block αιτημάτων στους υπόλοιπους, οι οποίοι το αποθηκεύουν τοπικά.
2. Ακολουθεί η φάση Προετοιμασίας. Για να επιβεβαιωθεί πως όλοι οι κόμβοι έχουν το έγκυρο block αιτημάτων (αυτό που δημιούργησε ο «καθοδηγητής») κάνουν επιπλέον έλεγχο στέλνοντας πίσω στον «καθοδηγητή» κατά την φάση Προετοιμασίας (Preprepare) και την φάση Παράδοσης (Commit)
3. Αν οποιοσδήποτε κόμβος λάβει block το οποίο είναι ίδιο με εκείνο που έχουν αποθηκευμένο τοπικά , από περισσότερους των $2/3$ των κόμβων εκτελούν την commit φάση

4. Στη συνέχεια η ίδια διαδικασία επαναλαμβάνεται μετά την commit φάση, και τελικά όλοι οι κόμβοι προσαρτούν στην αλυσίδα τους το προτεινόμενο block.



Σχήμα 8 Τρόπος λειτουργίας του Paxos. Οι proposers υποβάλλουν προτάσεις στους acceptors

2.6.2.2 Αλγόριθμος Παξός (Paxos)

Το όνομά του αλγόριθμου προήλθε από το ελληνικό νησί των Παξών. Το Κοινοβούλιο των Παξών έπρεπε να λειτουργήσει παρόλο που οι νομοθέτες απουσίαζαν συνεχώς από την κοινοβουλευτική αίθουσα (για διαπραγματεύσεις ή εμπόριο). Ο αλγόριθμος Paxos [21] εντάσσεται στους αλγόριθμους συναίνεσης και λειτουργεί ως αλγόριθμος ψηφοφορίας και έχει τρεις οντότητες:

- Proposers: Δέχονται τιμές από τους Clients και προσπαθούν να πείσουν τους acceptors να δεχτούν τις προτεινόμενες τιμές τους. Ο client εκδίδει ένα αίτημα στο κατανεμημένο σύστημα και περιμένει μια απάντηση.
- Acceptors: Αποδέχονται ορισμένες προτεινόμενες τιμές από τους Proposers και τους ενημερώνει εάν κάτι άλλο έγινε αποδεκτό. Η απάντηση ενός αποδέκτη αντιπροσωπεύει μια ψήφο για μια συγκεκριμένη πρόταση.
- Learners: Ανακοινώνουν το αποτέλεσμα.

Ο αλγόριθμος Paxos είναι ένα πρωτόκολλο στο οποίο κερδίζει η πλειοψηφία. Ένας client στέλνει ένα αίτημα σε οποιονδήποτε proposer του Paxos. Στη συνέχεια, ο proposer εκτελεί ένα πρωτόκολλο δύο φάσεων με τους acceptors. Αυτό σημαίνει ότι οι proposers αλληλοεπιδρούν δύο φορές με τους acceptors. Παρακάτω περιγράφονται οι δύο φάσεις:

- Φάση 1: Ένας proposer ρωτά όλους τους acceptors εάν κάποιος έχει ήδη λάβει μια πρόταση. Εάν η απάντηση είναι όχι, προτείνει μια τιμή.

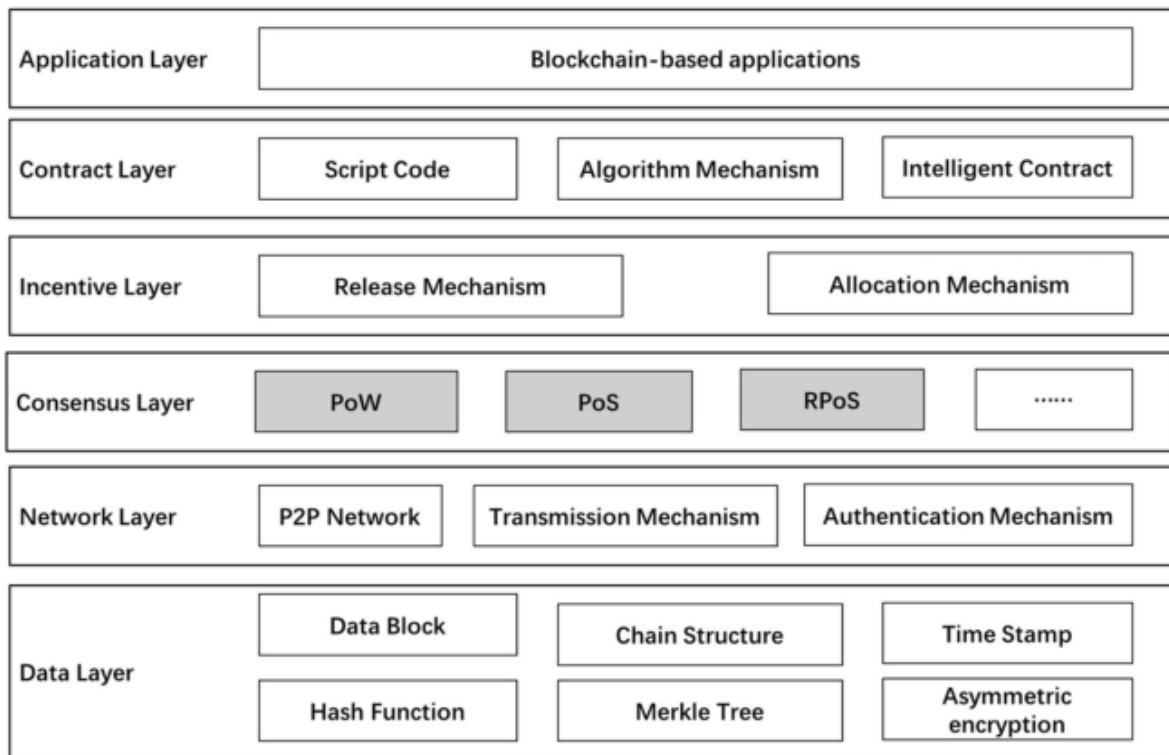
- Φάση 2: Εάν η πλειοψηφία των acceptors συμφωνεί με αυτήν την τιμή, τότε αυτή είναι η συναίνεσή μας.

Όταν ένας proposer λαμβάνει από τον client ένα αίτημα για να επιτύχει συναίνεση σχετικά με μια τιμή, ο proposer πρέπει να δημιουργήσει μια πρόταση με έναν αριθμό. Αυτός ο αριθμός πρέπει να έχει δύο ιδιότητες:

- Πρέπει να είναι μοναδικός. Κανένας proposer δεν μπορεί να προτείνει τον ίδιο αριθμό.
- Πρέπει να είναι μεγαλύτερος από οποιοδήποτε άλλο αναγνωριστικό που χρησιμοποιήθηκε στο δίκτυο.

Ένας proposer μπορεί να χρησιμοποιήσει έναν αυξανόμενο μετρητή ή να χρησιμοποιήσει μια χρονική σήμανση επιπέδου νανοδευτερόλεπτου για να το επιτύχει. Εάν ο αριθμός δεν είναι μεγαλύτερος από αυτόν που χρησιμοποιήθηκε προηγουμένως, ο proposer θα το ανακαλύψει απορρίπτοντας την πρότασή του και θα πρέπει να προσπαθήσει ξανά. (Krzyszowski, 2018)

Λόγω της πολυπλοκότητας του Paxos, ο Ongaro παρουσίασε έναν απλούστερο αλγόριθμο που λέγεται Raft. Το Raft σχεδιάστηκε για καλύτερη κατανόηση του πώς μπορεί να επιτευχθεί η συναίνεση. Πριν από το Raft, το Paxos θεωρούνταν το ιερό δισκοπότηρο για την επίτευξη συναίνεσης. Ο αλγόριθμος Raft είναι ένα ασύμμετρο μοντέλο βασισμένο σε ηγέτες. Ένας κόμβος σε να σύστημα μπορεί να βρίσκεται μόνο σε μία από τις τρεις καταστάσεις ανά πάσα στιγμή:



Σχήμα 9 The architecture of a blockchain system including consensus layer

- Ηγέτης: Μόνο ο κόμβος που έχει εκλεγεί ως ηγέτης μπορεί να αλληλοεπιδράσει με τον client. Όλοι οι άλλοι κόμβοι συγχρονίζονται με τον ηγέτη. Σε οποιαδήποτε στιγμή, μπορεί να υπάρχει το πολύ ένας ηγέτης.

- Ακόλουθος: Οι οπαδοί-κόμβοι συγχρονίζουν το αντίγραφο των δεδομένων τους με αυτό του ηγέτη μετά από κάποιο χρονικό διάστημα. Όταν ο κόμβος-ηγέτης «πέφτει» για οποιονδήποτε λόγο, ένας από τους οπαδούς μπορεί να διεξάγει εκλογές και να γίνει ηγέτης.
- Υποψήφιος: Κατά τη στιγμή της διεξαγωγής εκλογών για την επιλογή του κόμβου-ηγέτη, οι κόμβοι μπορούν να ζητήσουν ψήφους από άλλους κόμβους. Ως εκ τούτου, καλούνται υποψήφιοι όταν έχουν ζητήσει ψήφους. Αρχικά, όλοι οι κόμβοι βρίσκονται στην κατάσταση υποψηφίων. (Hooda, 2018)

2.6.3 Σύνοψη Μηχανισμών συναίνεσης

Έχοντας περιγράψει το κομμάτι συναίνεσης της αρχιτεκτονικής Blockchain μια συγκεντρωτική εικόνα των αλγορίθμων παρατίθεται σε πίνα στην παρακάτω εικόνα.

Consensus method	Accessibility ¹	Decentralization	Scalability	Throughput ²	Latency ³	Adversary tolerance	Computing overhead	Network overhead	Storage overhead
<i>PoW</i>	Public, PL.	High	High	Low	High	<25% Computing Power	High	Low	High
<i>PoC</i>	Public, PL.	High	High	Low	High	N/A	Low	Low	Very High
<i>PoET</i>	Private, P. or PL.	Medium	High	High	Low	N/A	Low	Low	High
<i>PoS</i>	Public P. or PL.	High	High	Low	Medium	<51% Stakes	Medium	Low	High
<i>DPoS</i>	Public, PL.	Medium	High	High	Medium	<51% Validators	Medium	N/A	High
<i>LPoS</i>	Public PL.	High	High	Low	Medium	<51% Stakes	Medium	Low	High
<i>PoI</i>	Public PL.	High	High	High	Medium	<51% importance	low	Low	High
<i>PoA</i>	Public, PL.	High	High	Low	Medium	<51% Online Stakes	High	Low	High
<i>Casper</i>	Public, PL.	High	High	Medium	Medium	<51% Validators	Medium	Low	High
<i>PoB</i>	Public, PL.	High	High	Low	High	<25% Computing Power	Medium	Low	High
<i>PBFT</i>	Private, P.	Medium	Low	High	Low	<33% Faulty Replicas	Low	High	High
<i>dBFT</i>	Private, P.	Medium	High	High	Medium	<33% Faulty Replicas	Low	High	High
<i>Stellar</i>	Public, PL.	High	High	High	Medium	Variable	Low	Medium	High
<i>Ripple</i>	Public PL.	High	High	High	Medium	<20% Faulty UNL nodes	Low	Medium	High
<i>Tendermint</i>	Private, P.	Medium	High	High	Low	<33% Voting power	Low	High	High
<i>ByzCoin</i>	Public, PL.	High	high	high	Medium	<33% Faulty Replicas	high	Medium	high
<i>Algorand</i>	Public, PL.	High	High	Medium	Medium	<33% Weighted Users	Low	High	High
<i>Dfinity</i>	Public, P. or PL.	High	High	N/A	Medium	N/A	Low	N/A	N/A
<i>RSCoin</i>	Private, P.	Low	High	High	Low	N/A	Low	Medium	High
<i>Elastico</i>	Public, PL.	High	High	Low	High	<25% Faulty Validators	Medium	High	High
<i>OmniLedger</i>	Public, PL.	High	High	High	Medium	<25% Faulty Validators	Medium	Medium	Low
<i>RapidChain</i>	Public, PL.	High	High	High	Medium	<33% Faulty Validators	Medium	Low	Low
<i>Raft</i>	Private, P.	Medium	High	High	Low	<50% crash fault	Low	N/A	High
<i>Tangle</i>	Public, PL.	Medium	High	High	Low	<33% Computing Power	Low	Low	Low

Σχήμα 10 Comparisons of different consensus methods

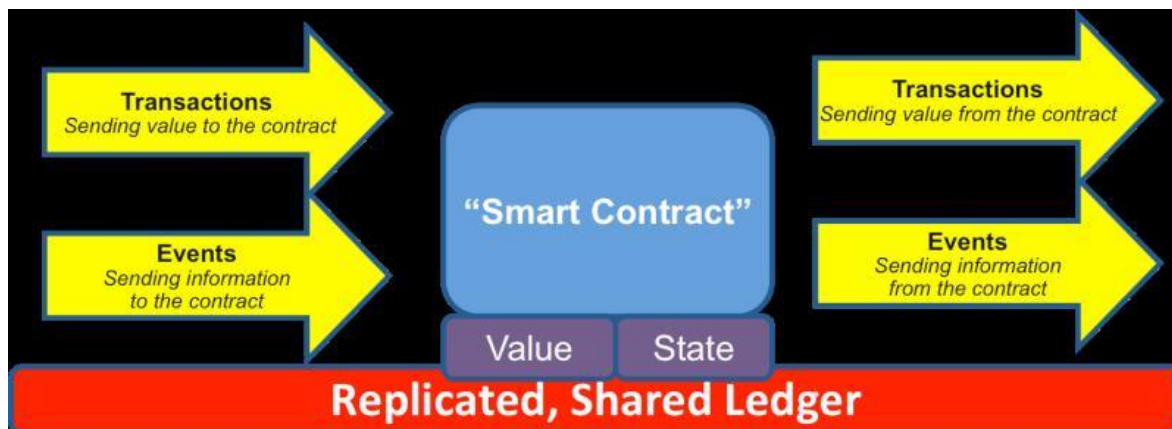
2.7 Έξυπνα συμβόλαια (Smart contracts)

Οι έξυπνες συμβάσεις είναι ακόμα ένα κρίσιμο χαρακτηριστικό ορισμένων blockchain, ειδικά από νομική και νομιμοποιητικής άποψη.

2.7.1 Ορισμός

Προκειμένου να εφαρμοστεί η επιχειρηματική λογική στο blockchain, έχουν εισαχθεί τα έξυπνα συμβόλαια (smart contracts), τα οποία αρχικά προτάθηκαν από τον [24]. Τα έξυπνα συμβόλαια είναι λογισμικά ηλεκτρονικών υπολογιστών, με σενάρια που επιβάλλουν κανόνες, χωρίς να απαιτούν παρέμβαση- επικύρωση από τρίτους. Με τον όρο smart contract μιλάμε «για ηλεκτρονικά πρωτόκολλα συναλλαγών» που επικυρώνουν, εκτελούν και επιβάλλουν τους προκαθορισμένους όρους μια σύμβασης.

Η αρχή λειτουργίας τους, σύμφωνα με την τρέχουσα βιβλιογραφία, δίνεται πάντοτε με κάποιο παράδειγμα. Όπως ότι είναι ως προγραμματιζόμενη αριθμομηχανή που μπορεί να λαμβάνει εισόδους – να εκτελέσει κώδικα – και στη συνέχεια να παρέχει έξοδο. Και επειδή βασίζεται σε ένα κατανεμημένο κατάστιχο, είναι δύσκολο για οποιοδήποτε μέρος να τροποποιήσει καταχρηστικά (κακόβουλα) την εκτέλεση του λογισμικού. Το λογισμικό ενσωματώνει τις υποχρεώσεις των μερών και εάν πληρούνται ορισμένες απαιτήσεις που προκαθορίζονται από τα μέρη (π.χ. χρόνος εκτέλεσης, συγκεκριμένη συναλλαγματική ισοτιμία, εγγραφή δικαιώματος ΠΙ κ.λπ.), τότε ένα έξυπνο συμβόλαιο εκτελεί την σχετική υποχρέωση, όπως πχ. η δανειοδότηση ΠΙ, ή η μεταβίβαση περιουσίας, χρημάτων ή οποιουδήποτε άλλου περιουσιακού στοιχείου.

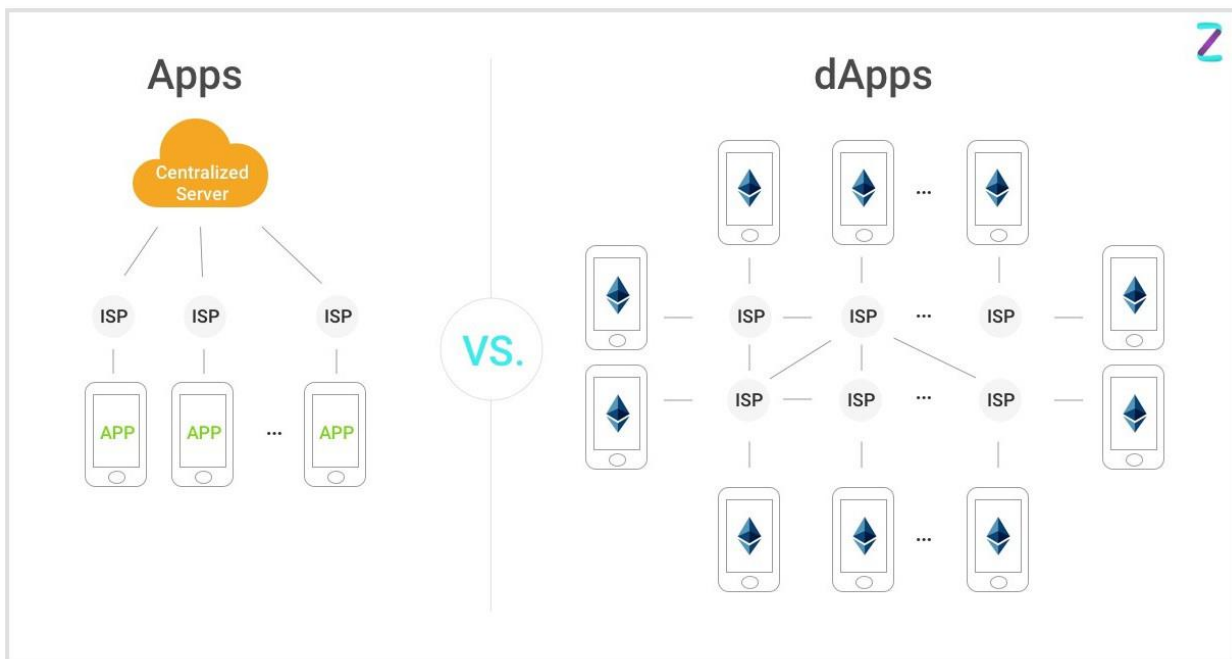


Σχήμα 11 Smart Contract. Source: Richard Brown

Δημιουργώντας ένα έξυπνο συμβόλαιο, μεταξύ των μερών υπάρχει εμπιστοσύνη, ως προς την μη παραβίαση των όρων του. Επιπλέον η σχέση εμπιστοσύνης δεν επιβάλλεται ή δεν εξαρτάται από κανένα ενδιάμεσο ή τρίτο μέρος, όπως πχ μια τράπεζα ή ένα κυβερνητικό όργανο ή εξουσία. Με τα έξυπνα συμβόλαια τα εμπλεκόμενα μέρη εμπιστεύονται την τήρηση των όρων του καθολικά και μπορούν να βασιστούν στις αρχές αμεταβλητότητας (immutability) και επαληθευσιμότητας (verifiability) της τεχνολογίας Blockchain. Εφόσον οι όροι ενός συμβολαίου συμφωνηθούν, τα εμπλεκόμενα μέρη εκφράζουν την αμοιβαία κατανόησή τους με τη μορφή ενός κώδικα (λογισμικού) έξυπνου συμβολαίου (smart contract code), το οποίο ενεργοποιείται και εκτελείται σε περίπτωση ψηφιακά υπογεγραμμένης και βασισμένης στο Blockchain συναλλαγής. Όταν ενεργοποιηθεί ο κώδικας έξυπνου συμβολαίου και ξεκινά η εκτέλεση του, δεν μπορεί να διακοπεί εκτός κι αν υπάρχει σχετική πρόβλεψη κατά τη συμφωνία του. Επί παραδείγματι στο εγγύς μέλλον, για να αποκτήσει πρόσβαση κάποιος ή κάποια στην αναπαραγωγή ενός τραγουδιού (ή άλλου αντικειμένου πνευματικής ιδιοκτησίας) θα πρέπει να χρεωθεί, βάση

του έξυπνου συμβολαίου που έχει ενεργοποιηθεί στο Blockchain που ανήκει. Σε αυτό το σενάριο, το έξυπνο συμβόλαιο θα πρέπει να ελέγξει την πιστωτική ικανότητα του χρήστη πριν από κάθε αναπαραγωγή και αν το υπόλοιπο του λογαριασμού δεν επαρκεί για να πληρώσει τότε ο κώδικας του έξυπνου συμβολαίου θα αποφασίσει να μην εκτελέσει τους όρους του άρα να μπλοκάρει την αναπαραγωγή. Συνεπακόλουθα αν ήταν επαρκής η πιστωτική ικανότητας του κατόχου της άδειας θα αφαιρέσει το ποσό της αμοιβής από τον λογαριασμό του και έπειτα θα αναπαράγει το τραγούδι.

Είναι σημαντικό να τονιστεί επιπροσθέτως πως δεν διαθέτουν όλα τα blockchain την δυνατότητα εκτέλεσης έξυπνων συμβολαίων. Για παράδειγμα, το bitcoin έχει την δυνατότητα να εκτελέσει ένα μικρό σύνολο έξυπνων συμβολαίων λόγω της γλώσσας προγραμματισμού που υποστηρίζει σε αντίθεση με άλλες πλατφόρμες όπως των Ethereum, NEO, EOS και LISK οι οποίες υποστηρίζουν έξυπνα συμβόλαιο με περισσότερες δυνατότητες οι οποίες επιτρέπουν την δυνατότητα καταμεμημένων εφαρμογών γνωστές ως dApps.



Σχήμα 12 Apps vs dApps (Pratik, 2018)

2.7.2 Επισκόπηση Dapps (Decentralized Applications)

Οι εφαρμογές dApps ή αποκεντρωμένες εφαρμογές είναι μια νέα σειρά εφαρμογών που δεν ελέγχονται ή ανήκουν σε μία μόνο αρχή και δεν μπορούν να διακόψουν την λειτουργία τους. Η ιδέα του dApp αποτελεί ακόμα αντικείμενο έρευνας. Δεν παρέχεται στη βιβλιογραφία συγκεκριμένος ορισμός που να ταιριάζει με όλα τα χαρακτηριστικά που κάνουν μια εφαρμογή αποκεντρωμένη. Σαν dApp απαιτείται μια εφαρμογή να παρουσιάζει τα ακόλουθα τέσσερα χαρακτηριστικά:

- Ανοικτού κώδικα: Το πρώτο και κύριο χαρακτηριστικό είναι ότι τέτοιες εφαρμογές θα πρέπει να παρέχουν ελεύθερη πρόσβαση στον πηγαίο τους κώδικα. Δεδομένου ότι τα βασικά χαρακτηριστικά των dApps είναι η

αυτονομία και η ομόφωνη συναίνεση, ουσιαστικά οι αλλαγές πρέπει να αποφασιστούν από το σύνολο ή την πλειοψηφία των χρηστών. Επίσης, ο κώδικας θα πρέπει να είναι διαθέσιμος σε όλους για έλεγχο.

- Αποκεντρωμένη αρχιτεκτονική: Όπως αναφέρεται παραπάνω, οι αποκεντρωμένες εφαρμογές αποθηκεύουν τα πάντα σε ένα αποκεντρωμένο blockchain ή οποιαδήποτε άλλη κρυπτογραφική τεχνολογία για να περιχαρακώσουν την εφαρμογή από τους κινδύνους της κεντρικής εξουσίας και να δημιουργήσουν την απαιτούμενη καθολική εμπιστοσύνη και αυτονομία.
- Ενθάρρυνση/ Κίνητρο: Καθώς η εφαρμογή βασίζεται στο αποκεντρωμένο blockchain, οι κόμβοι «επικυρωτές» των συναλλαγών στο δίκτυο πρέπει να επιβραβεύονται με κρυπτογραφικά νομίσματα ή οποιαδήποτε μορφή ψηφιακού στοιχείου που έχει αξία.
- Αλγόριθμος συναίνεσης: Η αποκεντρωμένη εφαρμογή πρέπει να έχει έναν μηχανισμό συναίνεσης στο κρυπτογραφικό σύστημα. Ουσιαστικά, αυτό προσδίδει αξία στο κρυπτογραφικό νόμισμα και δημιουργεί ένα πρωτόκολλο συναίνεσης σύμφωνα με το οποίο οι χρήστες συμφωνούν να παράγουν πολύτιμες κρυπτογραφικά διακριτικά (tokens).

2.7.3 Πλεονεκτήματα

Επιγραμματικά, τα έξυπνα συμβόλαια έχουν τα ακόλουθα πλεονεκτήματα:

- Ασφάλεια: Τα αρχεία συναλλαγών Blockchain είναι κρυπτογραφημένα και αυτό τα καθιστά πολύ δύσκολο να παραχαραχθούν ή υποκλαπούν. Επειδή κάθε μεμονωμένη εγγραφή συνδέεται με προηγούμενες και επόμενες εγγραφές στα διανεμημένα μητρώα (βασική αρχή του Blockchain), ολόκληρη η αλυσίδα των Blocks θα πρέπει να τροποποιηθεί για να αλλάξει μία εγγραφή.
- Εμπιστοσύνη: Τα έξυπνα συμβόλαια εκτελούν αυτόματα συναλλαγές σύμφωνα με προκαθορισμένους κανόνες και τα κρυπτογραφημένα αρχεία αυτών των συναλλαγών μοιράζονται στους συμμετέχοντες. Επομένως, κανείς δεν μπορεί να αμφισβητήσει αν οι πληροφορίες έχουν τροποποιηθεί για προσωπικό όφελος.
- Εξοικονόμηση χρημάτων: Τα έξυπνα συμβόλαια καταργούν την ανάγκη για μεσάζοντες, διότι οι συμμετέχοντες μπορούν να εμπιστευθούν τα ορατά δεδομένα και την τεχνολογία για να εκτελέσουν σωστά τη συναλλαγή. Δεν υπάρχει λόγος για επιπλέον πρόσωπο να επικυρώνει και να επαληθεύει τους όρους μιας συμφωνίας επειδή ενσωματώνεται στον κώδικα.
- Ταχύτητα και ακρίβεια: Τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα, οπότε δεν απαιτούνται χειρόγραφα έγγραφα. Ο κώδικας του υπολογιστή είναι επίσης ακριβέστερος από τη δομή που συντάσσονται τα παραδοσιακά συμβόλαια.

Μια επισήμανση που μπορεί να ληφθεί υπόψιν σαν μειονέκτημα είναι πως η αρχιτεκτονική των Έξυπνων Συμβολαίων είναι να μην διορθώνονται ή αναβαθμίζονται. Με άλλα λόγια, μόλις φορτωθεί το έξυπνο συμβόλαιο και χρησιμοποιείται, δεν μπορεί να ενημερωθεί ή να διορθωθεί εάν υπάρχει ευπάθεια ή βρέθηκε σφάλμα. Επομένως, υπάρχει ανάγκη επινόησης νέων τρόπων αφενός για την αναβάθμιση Έξυπνων Συμβολαίων και αφετέρου η ηθική αναφορά σφαλμάτων και τρωτών σημείων μέσω θεσμοθέτησης και προτυποποίησης.

2.8 Εξέλιξη της τεχνολογίας

Τα δομικά τεχνικά στοιχεία και το θεωρητικό υπόβαθρο της αρχιτεκτονικής Blockchain, προηγείται χρονικά κατά δεκαετίες από τη τεχνολογία και τον σχεδιασμό της. Οι ακαδημαϊκές έρευνες για την διαχείριση δημόσιου κλειδιού ή την ασύμμετρη κρυπτογραφία πρωτοεμφανίστηκαν τη δεκαετία του 1970, η κρυπτογράφηση «hash tree» ή «Merkle tree» την δεκαετία του 1980 [25] και η αρχική ιδέα για τη χρονική σήμανση ψηφιακών εγγράφων δημοσιεύτηκε το 1991 [26]. Μια ολοκληρωμένη επισκόπηση της εξέλιξης των δομικών στοιχείων και της ατομικής τους ένταξης σε διάφορες αρχιτεκτονικές Blockchain παρέχονται σε λιγοστές, αλλά επαρκώς ενημερωμένες πηγές [27]. Έκτοτε, τόσο η τεχνολογία κρυπτογράφησης ιδιωτικού κλειδιού (public key cryptography) όσο και η χρονοσήμανση (timestamping), έχουν εφαρμοστεί ευρέως σε συμβατικές αρχιτεκτονικές ασφάλειας δικτύων ή αρχιτεκτονικές ανταλλαγής δεδομένων μεταξύ υπολογιστικών συστημάτων (machine-to-machine data exchange) αρχής γενομένης της πρώτης δεκαετίας του 21^{ου} αιώνα. Μόνο με την εκτεταμένη εμφάνιση λύσεων και ακόλουθα της εισαγωγή της έννοιας του το 2008 από τον Nakamoto [11], το blockchain ήρθε στην επικαιρότητα και επεκτάθηκε από τα κρυπτονομίσματα, σε τομείς που περιλαμβάνουν την υγειονομική περίθαλψη, τη διαχείριση της εφοδιαστικής αλυσίδας, τη γεωργία, τη δασοκομία έως και τη διαχείριση των πνευματικών δικαιωμάτων. Έχει επαινεθεί και χαρακτηριστεί ως το «επόμενο Διαδίκτυο», η «επόμενη μεγάλη επανάσταση», ως η τεχνολογία με δυνατότητα να «διαταράξει» όλες τις βιομηχανίες.

Από τότε η λειτουργικότητα του Blockchain εξελίχθηκε ώστε να επιτρέπει σε ένα μηχανισμό (μια οντότητα) να δημιουργήσει μια αξιόπιστη, αυτόνομη δομή ανταλλαγής δεδομένων, καταγραφής αλλαγών σε αρχεία και κοινής χρήσης εγγραφών μεταξύ πολλών ομολόγων σε ένα κατανεμημένο δίκτυο ανεξάρτητα από το αν αυτές οι εγγραφές αφορούν σε bitcoin, άλλα διακριτικά (tokens) ή λίστες άδειας και ιδιοκτησίας. Όταν αλλάξει το ιδιοκτησιακό καθεστώς σε ένα πόρο, τα κατάστιχα όλων των εμπλεκόμενων μερών ενημερώνονται για ην αλλαγή και προσαρτούν την νέα πληροφορία. Κατ' αυτό τον τρόπο το Blockchain εγγυάται πως δεν μπορούν 2 διαφορετικά εμπλεκόμενα μέρη να αιτηθούν ιδιοκτησίας του εκάστοτε πόρου παρουσιάζοντας μια παλιότερη εγγραφή. Η προσάρτηση-ενημέρωση δεδομένων γίνεται ως αποτέλεσμα μηχανικής συναίνεσης (machine-managed consensus) μεταξύ των εμπλεκόμενων μερών.

Στο τρέχον στάδιο ανάπτυξης, όλοι οι σχηματισμοί των τεχνολογιών blockchain ασχολούνται πλήρως ή εν μέρει με τις βασικές ικανότητες και τα στοιχεία των λειτουργικών στοιχείων του δικτύου και των στοιχείων που υποστηρίζουν τη δημιουργία εμπιστοσύνης. Δηλαδή τους μηχανισμούς συναίνεσης για την ανανέωση, επεξεργασία και πρόσβαση σε αρχεία, διαχείριση χρηστών, συμφωνημένες ταυτότητες μελών, δικαιώματα πρόσβασης και διαδικασίες, κεντρική διαχείριση κανόνων από έναν ή περισσότερους κόμβους, τη διαμόρφωση της δομής και τις συμβάσεις για τη λειτουργία του οικοσυστήματος, τον τύπο αλγόριθμων συναίνεσης, τη χρονική σήμανση, τα καταγεγραμμένα αρχεία με αναστρέψιμη προβολή και τα συμμετρικά ή ασύμμετρα κατανεμημένα αρχεία. Ο συνδυασμός οποιονδήποτε παραπάνω ικανοτήτων και λειτουργικών στοιχείων έχουν σαν αποτέλεσμα ένα νέο και μοναδικό Blockchain σύστημα.

2.9 Φιλοσοφία του Blockchain (4^η βιομηχανική επανάσταση)

Η τεχνολογία διαδικτύου (το ίντερνετ) είναι η πλέον μετασχηματιστική ύπαρξη στο σύγχρονο κόσμο και τη νεωτερικότητα (modernity). Παρ' όλο που η πρώτη «φάση» του ίντερνετ διέπετε από την αρχή της ελεύθερης και πανανθρώπινης (καθολικής) μεταφορά πληροφοριών (transfer of information), μια νέα φάση του αναδύεται και σκιαγραφείται ως η ασφαλής αποκεντρωμένη μεταφορά αξίας (transfer of value). Το Blockchain εισάγει και εγκαθιδρύει τα μέσα για την μεταφορά αξίας σε δίκτυα. Στην πραγματικότητα αυτό

που έκανε το ίντερνετ είναι να πυροδοτήσει μια επανεξέταση του εαυτού, του κόσμου, της υλικότητας, της υποκειμενικότητας, της αντικειμενικότητας, των δυνατοτήτων, της χρονικότητας του ατόμου και της κοινωνίας όπως επίσης και άλλων φιλοσοφικών εννοιών, Ακριβώς όπως το Διαδίκτυο ήταν ένα επαναστατικό «περιστατικό» που πυροδότησε την αναζήτηση φιλοσοφικών εννοιών έτσι και το Blockchain χρίζει επίσης φιλοσοφικής έρευνας.

Η τεχνολογία Blockchain είναι βασικά ένα παγκόσμιο τεχνικό πλαίσιο που μπορεί να φέρει βαθιές αλλαγές σε όλους τους τομείς της βιομηχανίας και παραγωγής. Συχνά αναφέρεται ότι η τεχνολογία Blockchain θα μειώσει το ρόλο ενός από τους πιο κρίσιμους οικονομικούς και ρυθμιστικούς παράγοντες στην κοινωνία μας που ονομάζεται «μεσάζων» [24]. Με άλλα λόγια, η τεχνολογία Blockchain θα φέρει επανάσταση στη βιομηχανία και το εμπόριο και θα επιφέρει μια ριζική οικονομική αλλαγή σε παγκόσμια κλίμακα [25].

2.10 Εγκατεστημένα (Υφιστάμενα) Blockchain συστήματα (Use cases)

Σήμερα υπάρχει σημαντικό ενδιαφέρον για επιχειρηματικές εφαρμογές βασισμένες στο Blockchain, με αποτέλεσμα να έχει σχηματιστεί μεγάλο πλήθος start-up εταιριών ανάπτυξης τέτοιων συστημάτων. Βέβαια όπως αναφέρθηκε και παραπάνω, η υιοθέτηση συστημάτων Blockchain αντιμετωπίζει ακόμη ισχυρές προκλήσεις. Πέραν των start-up εταιριών μεγάλοι παίκτες της αγοράς όπως χρηματοπιστωτικά ιδρύματα (VISA, MASTERCARD, NASDAQ και τράπεζες) επενδύουν σημαντικά κεφάλαια στον σχεδιασμό και ανάπτυξη συστημάτων που εξυπηρετούν τα επιχειρηματικά και επιχειρησιακά τους μοντέλα. Στην πραγματικότητα ένα μεγάλο ποσοστό των επενδύσεων αφορά στην ανάπτυξη νέων επιχειρηματικών και επιχειρησιακών μοντέλων εξαιτίας του Blockchain.

2.11 Εφαρμογές Οικονομικής φύσης

2.11.1.1 Ιδιωτικό κεφάλαιο (Private Equity) NASDAQ

Η εταιρεία NASDAQ ξεκίνησε το δικό της ιδιωτικό ανταλλακτήριο μετοχών και μεταφοράς επενδύσεων το 2014. Αυτό το ανταλλακτήριο προορίζεται να παρέχει μια σειρά από λειτουργίες όπως το Cap Πίνακας (Ένας πίνακας που δείχνει την κεφαλαιοποίηση μιας επιχείρησης, ο οποίος συνήθως περιλαμβάνει το ποσό του κεφαλαίου που λαμβάνεται από κάθε πηγή, μακροπρόθεσμο χρέος, κοινά ίδια κεφάλαια και τους αντίστοιχους δείκτες κεφαλαιοποίησης) και την διαχείριση σχέσεων επενδυτών (investor relation management) για τις προ-IPO [<https://www.investopedia.com/terms/p/pre-ipo-placement.asp>] ή ιδιωτικές εταιρείες. Η υφιστάμενη διαδικασία συναλλαγής μετοχών στο ανταλλακτήριο είναι αναποτελεσματική και αργή εξαιτίας της εκτεταμένης διαμεσολάβησης τρίτων μερών. Η NASDAQ ξεκίνησε μια συνεργασία με μια start-up εταιρεία που εδρεύει στο San Fransisco και ονομάζεται chain.com, ώστε να δημιουργήσουν μια έκδοση του ανταλλακτηρίου η οποία θα σχεδιαστεί στις αρχές λειτουργίας του Blockchain. Η chain.com υλοποιεί εφαρμογές έξυπνων συμβολαίων βασισμένων στο Blockchain που θα χρησιμοποιηθούν στο ανταλλακτήριο. Το τελικό προϊόν αναμένεται να είναι ταχύτερο, αποτελεσματικότερο και εξιχνιάσιμο (traceable).

2.11.1.2 Everledger

Η Everledger είναι μια εταιρεία η οποία δημιουργεί σταθερά κατάστιχα πιστοποιητικών και ιστορικότητας συναλλαγών διαμαντιών με συστήματα βασισμένα στο blockchain. Τα μοναδικά χαρακτηριστικά τα οποία φέρουν τα διαμάντια, όπως πχ διαστάσεις, βάθος, χρώμα κλπ κατακερματίζονται (hashed) και κατοχυρώνονται

(registered) στο κατάστιχο. Η "επαλήθευση" των διαμαντιών γίνεται από αρμόδιες ασφαλιστικές ή δικηγορικές εταιρείες, από τους ιδιοκτήτες ή δικαιούχους τους. Η Everledger έχει αναπτύξει ένα απλό web service API για την εξέταση ενός διαμαντιού και τη δημιουργία, ανάγνωση ή ενημέρωση αξιώσεων από εμπλεκόμενα μέρη, καθώς το ίδιο και για αστυνομικές αναφορές διαμαντιών.

2.11.2 Εφαρμογές άλλων κλάδων

2.11.2.1 Συμβολαιογράφοι

Η πιστοποίησης αυθεντικότητας φυσικών και λοιπών εγγράφων ήδη πραγματοποιείται από συστήματα βασισμένα στο Blockchain τα οποία επιπρόσθετα εξαλείφουν την ανάγκη εμπλοκής οποιασδήποτε κεντρικής αρχής. Η υπηρεσία πιστοποίησης εγγράφων βοηθά στην απόδειξη της ιδιοκτησίας (ποιος την συνέταξε), στην απόδειξη της ύπαρξης (σε μια συγκεκριμένη χρονική στιγμή) και στην απόδειξη της ακεραιότητας (μη αλλοίωση) των εγγράφων. Δεδομένου ότι οι πιστοποιήσεις δεν είναι πλαστές και πως αυτό μπορεί να επαληθευτεί από ανεξάρτητα τρίτα μέρη, αυτές οι υπηρεσίες είναι νομικά δεσμευτικές. Η χρήση του blockchain στην πιστοποίηση συμβολαιογραφικής πράξης διασφαλίζει το απόρρητο του εγγράφου καθώς και εκείνους που ζητούν την πιστοποίηση. Η χρήση της τεχνολογίας blockchain εξαλείφει επίσης την ανάγκη για υψηλά τέλη πιστοποίησης της συμβολαιογραφικής πράξης, την αναποτελεσματικότητα στους τρόπους μεταφοράς εγγράφων και εξυπηρετεί την χρονική σήμανση τους.

2.11.2.2 Μουσική Βιομηχανία

Η μουσική βιομηχανία κλονίστηκε την τελευταία δεκαετία με την έλευση του Διαδικτύου και των διαδικτυακών εφαρμογών- τεχνολογιών μετάδοσης streaming. Η αλλαγή που υπέστη η βιομηχανία αφορά σε όλους τους εμπλεκόμενους: καλλιτέχνες, δισκογραφικές εταιρείες, εκδότες, συγγραφείς αλλά και τους παρόχους υπηρεσιών μετάδοσης. Η διαδικασία με την οποία καθορίζονται τα δικαιώματα πάνω στη μουσική ήταν πάντα περίπλοκη, αλλά η εξέλιξη του διαδικτύου περιπλέκει επιπλέον τα πράγματα, αυξάνοντας την ανάγκη για διαφάνεια στις πληρωμές δικαιωμάτων των καλλιτεχνών. Σε αυτό ακριβώς το σημείο παρεμβαίνει το Blockchain. Το Blockchain μπορεί να συμβάλει στη διατήρηση μιας ολοκληρωμένης και ακριβούς καταγεγραμμένης βάσης δεδομένων με πληροφορίες ιδιοκτησίας δικαιωμάτων μουσικής σε ένα δημόσιο κατάστιχο. Εκτός από τις πληροφορίες ιδιοκτησίας δικαιωμάτων, μπορούν να προστεθούν και οι πληροφορίες αναφορικά στην σχέση μεταξύ συν δικαιούχων και ποσοστά ιδιοκτησίας, όπως ορίζονται σε έξυπνες συμβάσεις. Αυτά τα έξυπνα συμβόλαια αποδίδουν τα κεφάλαια ανάλογα τις σχέσεις μεταξύ διαφορετικών ενδιαφερομένων και αυτοματοποιήσουν τις αλληλεπιδράσεις τους.

2.12 Διείσδυση στην αγορά και επίπεδο ωριμότητας της τεχνολογίας Blockchain.

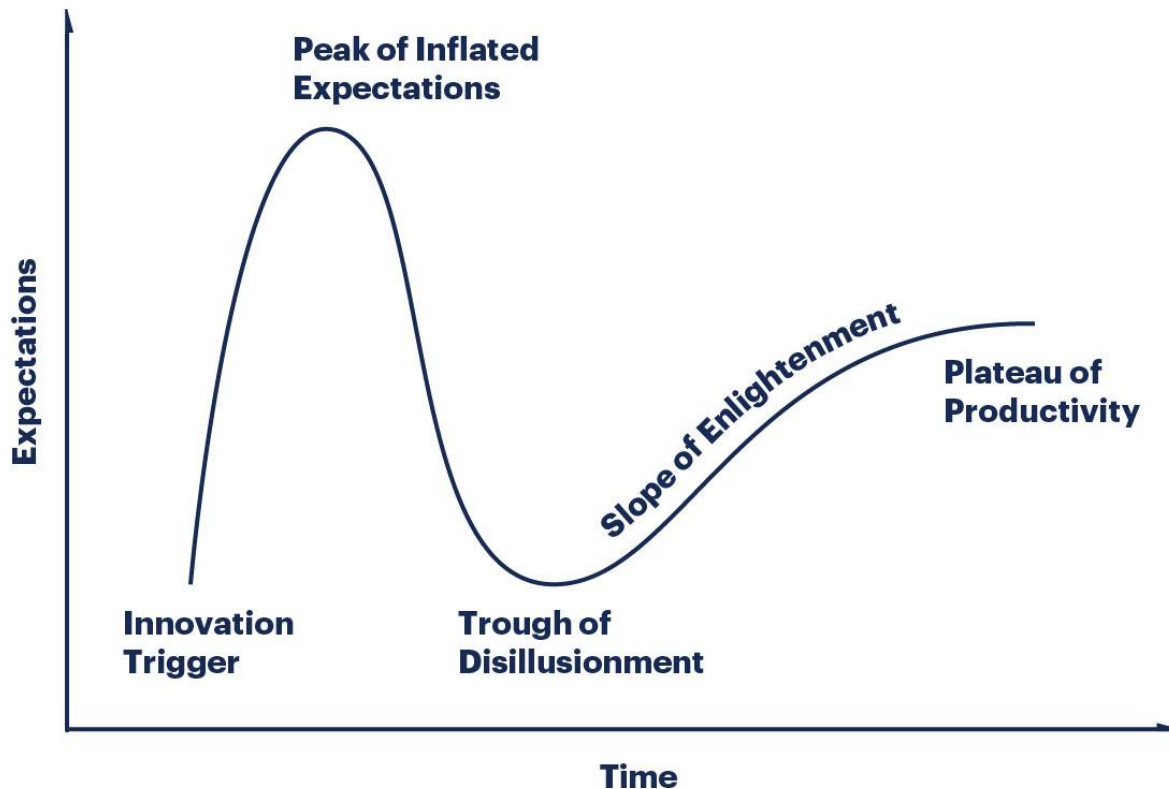
Στην επόμενη ενότητα αποτυπώνεται η προσπάθεια επιχειρησιακής διείσδυσης της συγκεκριμένης τεχνολογίας, η οποία περιλαμβάνει ανάλυση SWOT, ανάλυση Κύκλου Υπερβολής (HypeCycle) Gartner, αναφορά στους Κρίσιμους Παράγοντες Επιτυχίας (ΚΠΕ) και σχεδιασμό Δέντρου Απόφασης για την επιλογή ή όχι της τεχνολογίας αυτής από έναν οργανισμό.

2.12.1 Gartner Hype Cycle

Ο Κύκλος Υπερβολής της Gartner είναι μια γραφική απεικόνιση των τάσεων στην τεχνολογία και τη καινοτομία, που χρησιμοποιείται ως εργαλείο, κυρίως για την παρακολούθηση της ωριμότητας μιας τεχνολογίας και των μελλοντικών της δυνατοτήτων. Κάθε χρονιά η εταιρεία Gartner δημιουργεί περισσότερους των 90 κύκλων υποβολής ανεξαρτήτως εμπορικού ή ακαδημαϊκού κλάδου με σκοπό ο εκάστοτε ενδιαφερόμενος να παρακολουθεί τη τεχνική ωριμότητα και πιθανή διείσδυση στην αγορά του. Οι φάσεις του Κύκλου Υπερβολής είναι οι εξής:

- **Technology Trigger:** μια ανακάλυψη, η έναρξη διάθεσης ενός προϊόντος ή κάποιο άλλο γεγονός που προκαλεί τη προσοχή (στη περίπτωση μας η έναρξη του bitcoin και κατόπιν του ethereum).
- **Peak of Inflated Expectations:** μια φάση υπερβολικού ενθουσιασμού και μη ρεαλιστικών προσδοκιών, λόγω των δημοσιοποιημένων πρώιμων επιτυχιών της τεχνολογίας, από την οποία όμως δεν λείπουν και οι αποτυχίες (στη περίπτωση μας η μικρή ανάπτυξη των PoC έργων) καθώς η τεχνολογία δεν είναι ώριμη.
- **Trough of Disillusionment:** η τεχνολογία δεν ανταποκρίνεται στις υπερβολικές προσδοκίες και γρήγορα χάνει την αρχική αίγλη της. Πράγματι, στη περίπτωση που μας ενδιαφέρει, είναι χαρακτηριστικό ότι σύμφωνα με την Gartner, μόλις το 15% των σχετικών επιχειρηματικών προσπαθειών επιβιώνει μετά τον πρώτο χρόνο, ενώ και στο Github43, τα έργα που σχετίζονται με το BC, αν και αγγίζουν τις 8.600/έτος, έχουν μέση διάρκεια ζωής 1,2 έτη και μόλις το 8% είναι ενεργά (Trujillo, et al., 2017). Σύμφωνα με την Gartner, σε αυτή τη φάση βρίσκεται τώρα η τεχνολογία BC.
- **Slope of Enlightenment:** οι πειραματισμοί και οι επίπονες προσπάθειες από διάφορους οργανισμούς ποικίλου φάσματος οδηγούν στη κατανόηση των πραγματικών δυνατοτήτων της τεχνολογίας, των κινδύνων και των ωφελειών της.

- **Plateau of Productivity:** τα πραγματικά οφέλη της τεχνολογίας γίνονται ευρέως αποδεκτά, ενώ τα σχετικά εργαλεία και οι μεθοδολογίες σταθεροποιούνται.



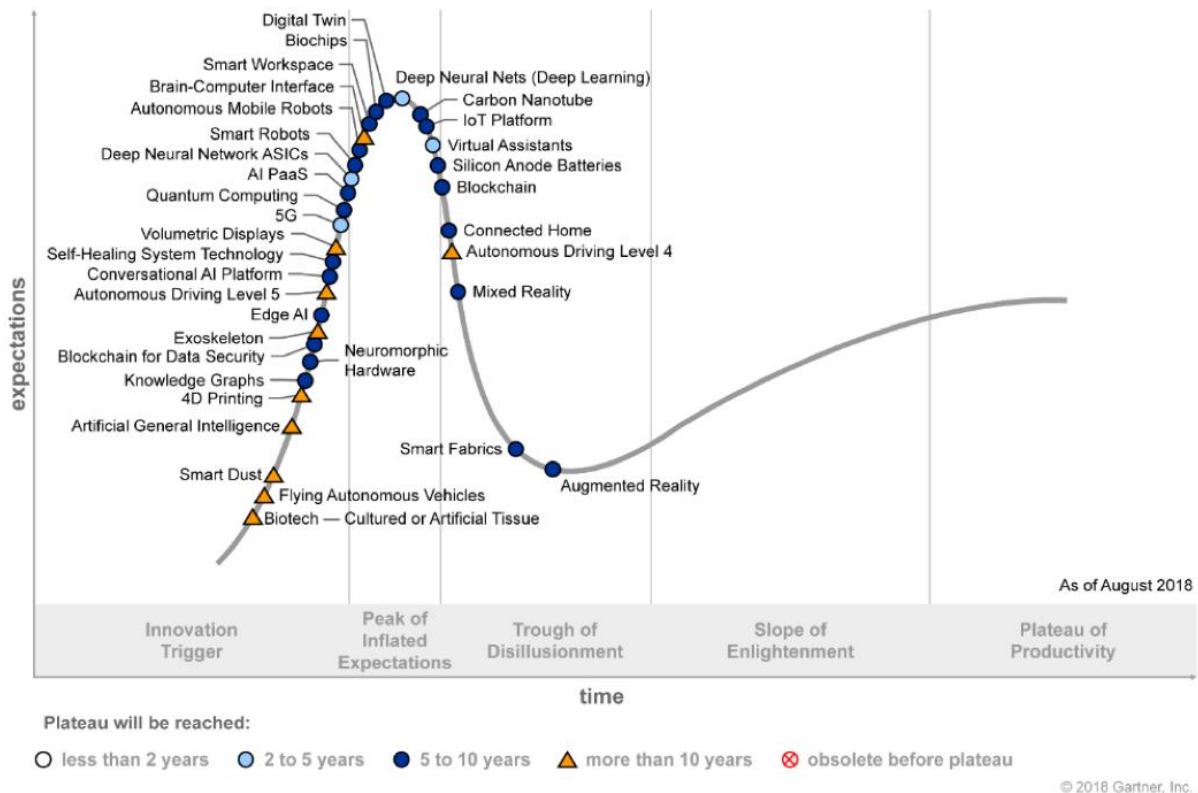
Σχήμα 13 Gartner Hype Cycle phases

2.12.2 Αναδυόμενες τεχνολογίες του 2018 (Emerging Technologies)

Σύμφωνα λοιπόν με σχετική ανάλυση της Gartner για το 2018, όπως φαίνεται στην παρακάτω εικόνα, το Blockchain παραμένει στο σημείο "Peak of Inflated Expectations" με πρόβλεψη να φτάσει στο σημείο "Plateau of Productivity". Παράλληλα όμως φαίνεται να έχει καθοδική τάση στην φάση "Trough of Disillusionment". Εξαιτίας της ευρείας υιοθέτησης τεχνολογιών Blockchain σε μεγάλη κλίμακα εμπορικών και ακαδημαϊκών κλάδων, πέραν των κρυπτονομισμάτων, προδιαγράφεται αλλαγή στην κατάσταση ωριμότητας από το στάδιο "5 έως 10 έτη" στο στάδιο "από 2 έως 5 έτη". Το Blockchain εμπεριέχει σημαντική δυναμική στους τομείς

- Ισχυροποίησης της θέσης των πολιτών, με την υιοθέτηση εφαρμογών e-governance
- Ταυτοποίησης, ιδιοκτησίας, καταχώρησης και συναλλαγών πολύτιμων αγαθών όπως τα διαμάντια (όπως αναλύεται παραπάνω) και ο χρυσός.
- υγείας με έμφαση στις διακρατικές μεταφορές ιστορικών ασθενών
- οικονομικής ένταξης (Financial Inclusion)

Για να υιοθετεί όμως η τεχνολογία στους παραπάνω τομείς προαπαιτείται η συναίνεση των κρατικών πολιτικών εξουσιών με ριζοσπαστικές αποφάσεις.



Σχήμα 14 Gartner Hype Cycle, 2018 [47]

2.12.3 Ανάλυση SWOT

Στις προηγούμενες ενότητες παρουσιάστηκαν κάποια σημαντικά πλεονεκτήματα και ευκαιρίες του Blockchain, που αποτελούν ουσιαστικά και την προστιθέμενη αξία της τεχνολογίας για τη κοινωνία. Επίσης, είναι εφικτό να εντοπιστούν κάποια κρίσιμα μειονεκτήματα, αλλά και οι απειλές που εμφολοχωρούν στη συγκεκριμένη τεχνολογία. Είναι σημαντικό να επισημανθεί ότι η ανάλυση που ακολουθεί αφορά κυρίως το δημόσιο BC, καθώς το ιδιωτικό και κοινοπρακτικό Blockchain καταφέρνουν να αποφύγουν τα περισσότερα αρνητικά, με σημαντικές υποχωρήσεις όμως, όπως έχουν επισημανθεί προηγουμένως.

Η ανάλυση SWOT (Strengths, Weaknesses, Opportunities, Threats) είναι ένα εργαλείο στρατηγικού σχεδιασμού το οποίο χρησιμοποιείται για την ανάλυση του εσωτερικού και εξωτερικού περιβάλλοντος μίας επιχείρησης ή τεχνολογίας, όταν η επιχείρηση πρέπει να λάβει μία απόφαση σε σχέση με τους στόχους που έχει θέσει ή με σκοπό την επίτευξή τους. Γενικά, κατά την εφαρμογή της ανάλυσης επιχειρείται να απαντηθούν με όσο το δυνατόν πιο ποσοτικοποιημένο τρόπο ερωτήματα για την περιοχή όπως:

- Δυνάμεις:
 - Ποια είναι τα πλεονεκτήματα;
 - Ποιο είναι το πλέον ανταγωνιστικό προϊόν / υπηρεσία;
 - Ποιοι είναι οι διαθέσιμοι πόροι που είναι μοναδικοί ή έχουν το μικρότερο συγκριτικά κόστος;

- Τι θεωρούν οι τοπικοί οικονομικοί παράγοντες ως ενδογενή δύναμη της περιοχής;
- Αδυναμίες:
 - Τι θα μπορούσε να βελτιωθεί;
 - Τι θα έπρεπε να αποφευχθεί;
 - Τι θεωρούν οι τοπικοί οικονομικοί παράγοντες ως ενδογενή αδυναμία;

Η παραπάνω θεώρηση των Δυνάμεων – Αδυναμιών πραγματοποιείται τόσο από την εσωτερική οπτική, όσο και από την οπτική των «πελατών». Κρίσιμος παράγοντας, ο οποίος επιβάλει την προσπάθεια ποσοτικοποίησης των δεδομένων αποτελεί η δυνατότητα ρεαλιστικής (αντικειμενικής) αποτίμησης της υφιστάμενης κατάστασης. Η όλη ανάλυση οφείλει να γίνει συ σχετιζόμενη με τον ανταγωνισμό: για παράδειγμα, η παραγωγή ενός προϊόντος υψηλής ποιότητας, εφόσον παράγεται σε αφθονία και από τον ανταγωνισμό, δεν αποτελεί δύναμη για την περιοχή, αλλά αναγκαιότητα.

- Ευκαιρίες
 - Ποιες είναι οι καλές ευκαιρίες που προβάλλουν;
 - Ποιες είναι οι ενδιαφέρουσες τάσεις που αφορούν την περιοχή;
- Απειλές:
 - Ποια εμπόδια εμφανίζονται συνήθως;
 - Τι κάνουν οι ανταγωνιστές;
 - Εμφανίζονται αλλαγές στις προδιαγραφές για τα ήδη παρεχόμενα προϊόντα ή υπηρεσίες;
 - Οι τεχνολογικές αλλαγές απειλούν ή ακυρώνουν την υφιστάμενη οικονομία της περιοχής;
 - Υπάρχουν χρηματοδοτικά ή χρηματοοικονομικά προβλήματα;
 - Αποτελεί κάποια από τις Αδυναμίες πραγματική απειλή για την οικονομία της περιοχής;

Συνοψίζοντας την ανωτέρω ανάλυση, είναι εφικτό να σχεδιαστεί ένας πίνακας ανάλυσης SWOT με τις βασικότερες διαστάσεις, όπως αναφέρθηκαν:

Πίνακας 2 SWOT Analysis

Πλεονεκτήματα	Αδυναμίες	Ευκαιρίες	Απειλές
Ενισχυμένη ασφάλεια	Εξαιρετικά ενεργοβόρα	Έλεγχος στον ίδιο τον χρήστη	Δυσκολία επεκτασιμότητας
Μικρότερη πιθανότητα αποτυχίας του συστήματος	Ελλιπή συμμόρφωση με τον GDPR	Πλατφόρμα για Μεγάλα Δεδομένα	Επίθεση 51% και ανεπιθύμητη συγκέντρωση
Αυξημένη διαφάνεια και ιχνηλασιμότητα	Ελλιπής προστασία χρηστών	Νέα επιχειρηματικά μοντέλα	Κβαντικοί υπολογιστές
Μικρή πιθανότητα εκμετάλλευσης από κακόβουλους χρήστες	Ελλιπής διακυβέρνηση και απουσία τεχνικών προτύπων		Πιθανότητα μη ευρείας αποδοχής
Αυξημένη αποτελεσματικότητα ταχύτητα και μειωμένο κόστος			

2.12.4 Κρίσιμοι Παράγοντες Επιτυχίας

Είναι σημαντικό να γίνει κατανοητό ότι η τεχνολογία Blockchain δεν αποτελεί την ιδανική επιλογή σε κάθε περίπτωση. Λαμβάνοντας υπόψη και την έως τώρα ανάλυση είναι εφικτό να προσδιορίσουμε τους κρίσιμους παράγοντες επιτυχίας για την υιοθέτηση ή μη της συγκεκριμένης τεχνολογίας. Η αποτελεσματικότερη προσέγγιση για την λήψη απόφασης είναι να απαντηθούν τα παρακάτω θέματα:

- Καταλληλότητα της τεχνολογίας
- Σαφήνεια στην ανάλυση του πεδίου του έργου
- Κοινωνικοί και Πολιτισμικοί παράγοντες

2.12.5 Σύνοψη

Η εφαρμογή της τεχνολογίας αλλά και της φιλοσοφίας του Blockchain εντατικοποιείται πέραν του Bitcoin και γενικότερα των συναλλαγών. Η εντατικοποίηση αυτή οφείλεται στα εγγενή χαρακτηριστικά του, όπως: η ασφάλεια, η ιδιοτικότητα, η ιχνηλασιμότητα, η χρονο- σήμανση και βασικά η αυτάρκεια- ανεξαρτησία. Πλέον το Blockchain και οι παραλλαγές του χρησιμοποιούνται σε εφαρμογές διασφάλισης οποιονδήποτε συναλλαγών, είτε αυτές είναι μεταξύ ανθρώπων (human-to-human), είτε μεταξύ μηχανών (machine-to-machine). Η χρήση του αποδεικνύεται πως είναι ασφαλής και συνδυάζεται άψογα με την παγκόσμια έλευση του Internet of things. Επιπλέον η δυνατότητα αποκεντρωμένης εφαρμογής του στο ήδη παγκόσμια εγκατεστημένο διαδίκτυο, το καθιστά πολύ ελκυστικό όσον αφορά τη διασφάλιση, εφεδρεία (redundancy) δεδομένων και τελικά την «επιβίωση» τους. Από πολιτικής σκοπιάς έχει αναγνωριστεί η καταλληλότητα του Blockchain σε αναπτυσσόμενες χώρες όπου η διασφάλιση της εμπιστοσύνης είναι μείζονος σημασίας. Έτσι, η τεχνολογία Blockchain μπορεί να θεωρηθεί ως ένα ζωτικής σημασίας και απαραίτητο πρόσθετο συστατικό του, εκ φύση ελεύθερου Διαδικτύου. Συστατικό το οποίο επαναφέρει την ασφάλεια, την

εμπιστοσύνη, την ελευθερία της έκφρασης, της δικαιοσύνης και της ελεύθερης διακίνησης ιδεών, στα χέρια των χρηστών. Οι χρήστες θα μπορούν, πάντα με γνώμονα την εμπιστοσύνη, να δημιουργήσουν τους όρους λειτουργίας του δικτύου τους. Τέλος όπως αναφέρθηκε και παραπάνω το Blockchain προβλέπεται πως απέχει έως 5 έτη από το στάδιο της τελικής ωριμότητας του, εξαιτίας της διείσδυσης του στη παγκόσμια αγορά.

3 Ψηφιακός Πολιτισμός- Τέχνη (Digital Culture)

Ως πολιτιστικά αγαθά νοούνται οι μαρτυρίες της ύπαρξης και της ατομικής και συλλογικής δραστηριότητας του ανθρώπου. Επιπλέον ως άυλα πολιτιστικά αγαθά νοούνται εκφράσεις, δραστηριότητες, γνώσεις και πληροφορίες, όπως μύθοι, έθιμα, προφορικές παραδόσεις, χοροί, δρώμενα, μουσική, τραγούδια, δεξιότητες ή τεχνικές που αποτελούν μαρτυρίες του παραδοσιακού, λαϊκού και λόγιου πολιτισμού [28].

Αγαθά όπως η μουσική, η τέχνη ή οι ιδέες αναφέρονται από τους οικονομολόγους ως "μη ανταγωνιστικά" (non-rival) ή μη εξαιρετέα (non-excludable). Μη ανταγωνιστικά είναι τα αγαθά τα οποία επιτρέπουν την ταυτόχρονη χρήση, απόλαυση ή κατανάλωση από διαφορετικούς χρήστες [29].

3.1 Πνευματική ιδιοκτησία

Σύμφωνα με τον Παγκόσμιο Οργανισμό Πνευματικής Ιδιοκτησίας (ΠΟΠΙ) [World Intellectual Property Organization (WIPO)], πνευματική ιδιοκτησία (ΠΙ) είναι "οι δημιουργίες της διανοήσης, όπως ανακαλύψεις, λογοτεχνικά και καλλιτεχνικά έργα, σχέδια και σύμβολα, ονόματα, άδεια μουσικής, διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα, εμπορικά σήματα και οπτικοακουστικό υλικό που χρησιμοποιείται στο εμπόριο". Είναι ένας γενικός όρος για μια ποικιλία περιουσιακών στοιχείων που δημιουργούνται από το μυαλό. Διαφορετικά χαρακτηρίζονται και ως άυλα αγαθά.

Μεταξύ όλων των δημιουργικών βιομηχανιών, οι απτές εκφράσεις της ανθρώπινης διάνοιας που είναι μοναδικές και έχουν μια συγκεκριμένη αξία προστατεύονται νομοθετικά. Κι αυτό εξαιτίας του ότι θεωρούνται "ιδιοκτησία", μπορεί κανείς να τα αγοράσει, να τα πουλήσει ή να χορηγήσει άδεια χρήσης τους. Θεωρούνται ιδιοκτησία του δημιουργού τους. Μπορούμε να συμπεριλάβουμε σε αυτήν την κατηγορία όλα τα πρωτότυπα δημιουργικά έργα που προστατεύονται σύμφωνα με το νόμο περί πνευματικών δικαιωμάτων (π.χ. μουσική, βιβλία) και όλες τις νέες εφευρέσεις που προστατεύονται βάσει του νόμου περί ευρεσιτεχνιών. Επιπλέον, ο νόμος περί εμπορικών σημάτων προστατεύει λέξεις, σύμβολα ή λογότυπα που διακρίνουν αγαθά και υπηρεσίες. Ο κάτοχος ενός εμπορικού σήματος θεωρείται ο πρώτος χρήστης ή ο πρώτος που καταχωρεί το εμπορικό σήμα σε μια κεντρική αρχή.

Το πιο σημαντικό ζήτημα σχετικά με την πνευματική ιδιοκτησία είναι η αναγνώριση του πραγματικού δημιουργού και του τρέχοντος κατόχου. Σε κάθε χώρα έχει υιοθετηθεί διαφορετικό συγκεντρωτικό σύστημα καταχώρησης ιδιοκτησίας. Επί παραδείγματι ο ελληνικός "Οργανισμός Πνευματικής Ιδιοκτησίας" (ΟΠΙ). Ένα αποτελεσματικό και δίκαιο σύστημα πνευματικής ιδιοκτησίας μπορεί να βοηθήσει όλες τις χώρες να αξιοποιήσουν τις δυνατότητες της πνευματικής ιδιοκτησίας ως καταλύτη για την οικονομική ανάπτυξη και την κοινωνική και πολιτιστική ευημερία. Το σύστημα πνευματικής ιδιοκτησίας συμβάλλει στην εξισορρόπηση των συμφερόντων των οργανισμών καινοτομίας και του δημόσιου συμφέροντος, παρέχοντας ένα περιβάλλον στο οποίο η δημιουργικότητα και η εφεύρεση μπορούν να αναπτυχθούν, προς όφελος όλων.

Ο νόμος περί ΠΙ περιλαμβάνει τρόπους για την προστασία των δημιουργικών εκφράσεων που έχουν εμπορική και ηθική αξία. Οι διαφορετικοί τύποι ΠΙ όπως αναφέρθηκαν και παραπάνω είναι:

- Εμπορικά σήματα
- Διπλώματα ευρεσιτεχνίας
- Βιομηχανικά σχέδια
- Πνευματικά δικαιώματα

Οι βασικές διαφορές μεταξύ των νόμων περιγράφονται λεπτομερώς στις προσεχείς ενότητες και παρουσιάζονται στον παρακάτω πίνακα.

Πίνακας 3 Πνευματική ιδιοκτησία (Copyright, Patents, Trademarks)

	Πνευματικά δικαιώματα	Διπλώματα ευρεσιτεχνίας	Εμπορικά σήματα/ Βιομηχανικά σχέδια
Τι προστατεύεται;	Πρωτότυπα έργα όπως βιβλία, άρθρα, τραγούδια, φωτογραφίες, γλυπτά, χορογραφία, ηχογραφήσεις, κινηματογραφικές ταινίες και άλλα έργα	Εφευρέσεις, όπως διεργασίες, μηχανήματα, κατασκευές, συνθέσεις καθώς βελτιώσεις αυτές	Any word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others
Προϋποθέσεις	Ένα έργο πρέπει να είναι πρωτότυπο, δημιουργικό και σταθερό σε από μέσο	Μια εφεύρεση πρέπει να είναι νέα, χρήσιμη και μη προφανής	Ένα σήμα πρέπει να είναι διακριτικό (δηλαδή, πρέπει να είναι ικανό να προσδιορίζει την πηγή ενός συγκεκριμένου αγαθού)
Είδος προστασίας	Η ζωή του συγγραφέα συν 70 ακόμη χρόνια.	20 έτη	Όσο το σήμα χρησιμοποιείται στο εμπόριο
Απόδοση Δικαιωμάτων	Δικαίωμα ελέγχου της αναπαραγωγής, παραγωγής παράγωγων έργων, διανομής και δημόσιας απόδοσης και προβολής των έργων που προστατεύονται από πνευματικά δικαιώματα	Δικαίωμα αποτροπής από άλλους να κάνουν, να πωλούν χρησιμοποιώντας ή να εισάγουν την ευρεσιτεχνία της εφεύρεσης	Δικαίωμα χρήσης του σήματος και αποτροπή άλλων από τη χρήση σημάτων με τρόπο που θα μπορούσε να προκαλέσει σύγχυση σχετικά με την προέλευση των προϊόντων ή των υπηρεσιών

3.1.1 Εμπορικά σήματα (Trademark Law)

Σύμφωνα με το αμερικανικό γραφείο διπλωμάτων ευρεσιτεχνίας και εμπορικών σημάτων ("USPTO"), "ένα εμπορικό σήμα είναι μια λέξη, φράση, σύμβολο ή/ και σχέδιο που προσδιορίζει και διακρίνει την πηγή των αγαθών ενός μέρους από εκείνη των άλλων. Ένα σήμα υπηρεσίας (Service mark) είναι μια λέξη, φράση, σύμβολο ή / και σχέδιο που προσδιορίζει και διακρίνει την πηγή μιας υπηρεσίας και όχι ένα αγαθό. Παραδείγματα περιλαμβάνουν επωνυμίες, συνθήματα και λογότυπα. Εν γένη ο όρος "εμπορικό σήμα" χρησιμοποιείται και αναφέρεται τόσο στα εμπορικά σήματα όσο και στα σήματα υπηρεσιών. Τα εμπορικά σήματα βοηθούν τις επιχειρήσεις και το κοινό καθιστώντας σαφείς τις διαφορές μεταξύ των προϊόντων. Ο καθένας μπορεί να ξεκινήσει μια εταιρεία σόδας, αλλά μόνο μία σόδα μπορεί να ονομαστεί Coca-Cola, υπάρχουν πολλές αλυσίδες ξενοδοχείων, αλλά μόνο μία ονομάζεται Four Seasons και ούτω καθεξής. Σε μια ευρύτερη έννοια, τα εμπορικά σήματα προωθούν την πρωτοβουλία και τις επιχειρήσεις παγκοσμίως, ανταμείβοντας τους ιδιοκτήτες τους με αναγνώριση και οικονομικό κέρδος.

3.1.2 Πνευματικά δικαιώματα (Copyright Law)

Τα πνευματικά δικαιώματα είναι μια συλλογή δικαιωμάτων που παρέχονται αυτόματα μόλις δημιουργηθεί ένα πρωτότυπο έργο. Οι νόμοι περί πνευματικών δικαιωμάτων παρέχουν σε συγγραφείς, καλλιτέχνες και άλλους δημιουργούς προστασία για τις λογοτεχνικές και καλλιτεχνικές δημιουργίες τους, που αναφέρονται γενικά ως «έργα». Οι δικαιούχοι των δικαιωμάτων είναι:

- ερμηνευτές (όπως ηθοποιοί και μουσικοί) στις παραστάσεις τους.
- παραγωγοί οπτικοακουστικού υλικού (για παράδειγμα, μικροί δίσκοι) στις ηχογραφήσεις τους
- ραδιοτηλεοπτικοί οργανισμοί με ραδιοφωνικά και τηλεοπτικά προγράμματα.

Οι δημιουργοί έργων που προστατεύονται από πνευματικά δικαιώματα, καθώς και οι κληρονόμοι και οι διάδοχοί τους (γενικά αναφέρονται ως «κάτοχοι δικαιωμάτων»), έχουν ορισμένα βασικά δικαιώματα βάσει νόμου. Ο σωστός κάτοχος ενός έργου μπορεί να εγκρίνει ή να απαγορεύσει:

- την αναπαραγωγή του σε όλες τις μορφές, συμπεριλαμβανομένης της φόρμας εκτύπωσης και της ηχογράφησης.
- τη δημόσια απόδοσή του και την επικοινωνία με το κοινό.
- τη μετάδοσή του.
- τη μετάφρασή του σε άλλες γλώσσες.
- την προσαρμογή του, όπως από ένα μυθιστόρημα σε ένα σενάριο για μια ταινία.

Τα οικονομικά δικαιώματα που σχετίζονται με τα πνευματικά δικαιώματα είναι περιορισμένης διάρκειας - όπως προβλέπεται στις σχετικές συνθήκες του WIPO - ξεκινώντας από τη δημιουργία και την επιδιόρθωση του έργου και διαρκούν τουλάχιστον 50 χρόνια μετά το θάνατο του δημιουργού. Δικαιώματα που προβλέπονται σύμφωνα με τους νόμους περί πνευματικών δικαιωμάτων και συγγενικών δικαιωμάτων μπορούν να επιβληθούν από τους κατόχους δικαιωμάτων μέσω ποικίλων μεθόδων και φόρουμ, συμπεριλαμβανομένων αγωγών αστικής ευθύνης, διοικητικών προσφυγών και ποινικής δίωξης. Οι αγωγές, οι εντολές που απαιτούν καταστροφή των παραβατικών στοιχείων, οι εντολές επιθεώρησης, μεταξύ άλλων, χρησιμοποιούνται για την επιβολή αυτών των δικαιωμάτων.

3.1.3 Ευρεσιτεχνίες

Ένα δίπλωμα ευρεσιτεχνίας είναι μια επιχορήγηση από έναν εθνικό καταχωρητή π.χ. USPTO, που επιτρέπει στον κάτοχο του διπλώματος ευρεσιτεχνίας να διατηρήσει το μονοπώλιο για περιορισμένο χρονικό διάστημα (γενικά 20 χρόνια) που σχετίζεται με τη χρήση και την ανάπτυξη μιας καινοτομίας. Τα διπλώματα ευρεσιτεχνίας προστατεύουν νέες εφευρέσεις ή ανακαλύψεις όπως φαρμακευτικά προϊόντα, σύνθετα μηχανήματα ή προηγμένο λογισμικό, απαγορεύοντας σε άλλους να χρησιμοποιούν, να αναπαράγουν ή να εισάγουν την εφεύρεση. Το USPTO εκδίδει τρεις τύπους διπλωμάτων ευρεσιτεχνίας:

- Γενικά Διπλώματα ευρεσιτεχνίας (Utility Patents). Μια διαδικασία, μια μηχανή, μια κατασκευή, μια σύνθεση ενός θέματος ή μια βελτίωση μιας υπάρχουσας ιδέας.
- Διπλώματα ευρεσιτεχνίας σχεδιασμού (Design Patents). Νέα και πρωτότυπα σχέδια που στολίζουν ένα κατασκευασμένο αντικείμενο.
- Διπλώματα ευρεσιτεχνίας φυτών. Κάθε αναπαραγωγίμο φυτό (sexual or asexual), που είναι καινούργιο και μη προφανές.

Τα διπλώματα ευρεσιτεχνίας προστατεύουν τις εφευρέσεις, όχι τις ιδέες, επομένως δεν μπορεί να καταχωρηθεί με δίπλωμα ευρεσιτεχνίας η τηλεμεταφορά ή το ταξίδι στο χρόνο σαν δυνατότητα, εκτός και αν εφευρεθεί. Η εφεύρεση πρέπει επίσης να είναι «χρήσιμη» και «μη προφανής». Ένας κάτοχος διπλώματος ευρεσιτεχνίας έχει το δικαίωμα να αποφασίσει ποιος μπορεί - ή όχι - να χρησιμοποιήσει την κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας εφεύρεση για την περίοδο κατά την οποία προστατεύεται.

Είναι αυτονόητο ότι, σε αντίθεση με τα πνευματικά δικαιώματα και τα εμπορικά σήματα, τα διπλώματα ευρεσιτεχνίας λειτουργούν κάτω από το σύστημα «ο πρώτος εφευρέτης καταχωρεί». Αυτό σημαίνει ότι η αποτυχία καταχώρισης μιας εφευρέσης μπορεί να έχει καταστροφικές συνέπειες εάν κάποιος άλλος την καταχωρήσει πριν από εσάς, ακόμη και αν την εφευρίσκατε πρώτος.

3.1.4 Βιομηχανικά σχέδια

Ο βιομηχανικός σχεδιασμός αναφέρεται στις διακοσμητικές ή αισθητικές πτυχές ενός αντικειμένου. Προστατεύει την οπτική σχεδίαση αντικειμένων που δεν είναι καθαρά χρηστικά και συνίσταται στη δημιουργία σχήματος, διαμόρφωσης ή σύνθεσης μοτίβου ή χρώματος ή συνδυασμού μοτίβου και χρώματος σε τρισδιάστατη μορφή που περιέχει αισθητική αξία. Για να προστατεύεται σύμφωνα με τα περισσότερα εθνικά νομικά πλαίσια, ένας βιομηχανικός σχεδιασμός πρέπει να είναι νέος ή πρωτότυπος και μη λειτουργικός. Τα βιομηχανικά σχέδια είναι αυτά που κάνουν ένα αντικείμενο ελκυστικό. Ως εκ τούτου, προσθέτουν στην εμπορική αξία ενός προϊόντος και αυξάνουν την εμπορευσιμότητά του.

Στις περισσότερες χώρες, ένα βιομηχανικό σχέδιο πρέπει να καταχωρηθεί προκειμένου να προστατευθεί βάσει της νομοθεσίας περί βιομηχανικού σχεδιασμού ως «καταχωρημένο σχέδιο». Σε άλλες περιπτώσεις χωρών, τα βιομηχανικά σχέδια προστατεύονται βάσει του νόμου περί ευρεσιτεχνιών ως «διπλώματα ευρεσιτεχνίας σχεδιασμού». Ένα βιομηχανικό σχέδιο μπορεί να είναι ένα δισδιάστατο ή τρισδιάστατο σχέδιο που χρησιμοποιείται για την παραγωγή ενός προϊόντος, βιομηχανικού εμπορεύματος ή μιας χειροτεχνίας. Ανάλογα με το νομικό πλαίσιο, τα καταχωρημένα δικαιώματα σχεδιασμού έχουν διάρκεια μεταξύ 15 και 50 ετών. Τα μέλη του WIPO Hague πρέπει να δημοσιεύσουν τη μέγιστη διάρκεια προστασίας τους για τα δικαιώματα σχεδιασμού. Στην ΕΕ, για παράδειγμα, η προστασία για ένα καταχωρημένο κοινοτικό σχέδιο είναι έως και 25 χρόνια και υπόκειται στην καταβολή τελών ανανέωσης κάθε πέντε χρόνια.

3.2 Κατακερματισμός

Αν και δεν είναι ανακριβές να μιλάμε για διεθνή νομοθεσία περί πνευματικών δικαιωμάτων, όπως περιέχεται για παράδειγμα σε διεθνείς συνθήκες, δεν υπάρχει διεθνές δικαίωμα πνευματικής ιδιοκτησίας. Οι διεθνείς συνθήκες αναγνωρίζουν την προστασία των πνευματικών δικαιωμάτων αλλά ταυτόχρονα τις διαμοιράζουν (κατακερματίζουν) σε πολλές δικαιοδοσίες, όπου η κάθε μια έχει δικό της νομοθετικό πλαίσιο. Για παράδειγμα ένα έργο το οποίο "παράγεται" στον Καναδά ή την Ελλάδα, θα πρέπει να προστατεύεται με νόμο περί πνευματικής ιδιοκτησίας ταυτόχρονα και σε άλλα 175 κράτη μέλη της (Διεθνούς της Βέρνης) Berne Union (δηλαδή, χώρες που συμμετέχουν στη Σύμβαση της Βέρνης [30]) σύμφωνα με την κείμενη εθνική τους νομοθεσία. Επιπλέον αυτό το «έργο» ή μια δημιουργία με λειτουργικά χαρακτηριστικά θα μπορούσε να προστατεύεται σε μια δικαιοδοσία (πχ. ένα κράτος) αλλά όχι σε μια άλλη, με την αιτιολογία ότι στερείται πρωτοτυπίας. Σύμφωνα με τη Σύμβαση της Βέρνης, ένας συγγραφέας λαμβάνει κατ' αυτό το τρόπο 176 διαφορετικά εθνικά "πακέτα" δικαιωμάτων πνευματικής ιδιοκτησίας (πακέτο δικαιωμάτων: διανομής, αναπαραγωγής, πώλησης, μετάφρασης, ενοικίασης κλπ.), συνυπολογίζοντας την χώρα προέλευσης.

Πέραν του κρατικού κατακερματισμού, τα δικαιώματα πνευματικής ιδιοκτησίας, μπορούν να διαμοιραστούν περαιτέρω. Ο δημιουργός ενός έργου μπορεί να μεταφέρει οποιοδήποτε μεμονωμένο δικαίωμα από το πακέτο της ιδιοκτησίας του σε ένα τρίτο μέρος. Μπορεί επι παραδείγματι στην περίπτωση ενός μυθιστορήματος, να μεταφέρει σε ένα τρίτο μέρος τα δικαιώματα μετάφρασης ή εκμετάλλευσης του έργου σε μια άλλη γλώσσα ή αγορά. Με άλλα λόγια, κάθε δικαίωμα (ο όρος «right fragment» περιγράφει αυτόν τον «κατακερματισμό» των δικαιωμάτων [31]) στο πακέτο πνευματικών δικαιωμάτων μπορεί να ανήκει και να αξιοποιηθεί χωριστά, όσο ισχύει η Σύμβαση της Βέρνης, 176 φορές.

Η κατάσταση περιπλέκεται περαιτέρω. Κάθε χώρα μπορεί κατά το δοκούν να επιλέξουν ποια μορφή κανόνα «εξάντλησης» (exhaustion) θα εφαρμοστεί καθώς αυτό το ζήτημα δεν έχει ακόμη διευθετηθεί σε διεθνές επίπεδο. Υπάρχουν τρεις βασικοί κανόνες εξάντλησης: εθνικός, περιφερειακός και διεθνής. Σύμφωνα με τον εθνικό κανόνα εξάντλησης, ένα αντίγραφο ενός έργου μπορεί να πωληθεί μόνο με τη συγκατάθεση του κατόχου των πνευματικών δικαιωμάτων σε αυτήν την περιοχή. Επιπλέον σημαίνει ότι η παράλληλη εισαγωγή [32] δεν επιτρέπεται επειδή τα δικαιώματα των κατόχων πνευματικών δικαιωμάτων αντιμετωπίζονται ως εντελώς ανεξάρτητη οντότητα σε κάθε εθνική αγορά. Μια παραλλαγή του κανόνα είναι η περιφερειακή εξάντληση, ένα καθεστώς σύμφωνα με το οποίο ένα αντίγραφο που διατίθεται νόμιμα στην αγορά μπορεί να αξιοποιηθεί σε μια ευρύτερη περιοχή (διακρατική). Αυτό ισχύει για παράδειγμα στην ΕΕ, τουλάχιστον όσον αφορά τις πωλήσεις φυσικών αντιγράφων έργων πνευματικής ιδιοκτησίας [33]. Ο τελευταίος κανόνας είναι η διεθνής εξάντληση, ένα καθεστώς σύμφωνα με το οποίο ένα αντίγραφο που διατίθεται στην αγορά νόμιμα οπουδήποτε στον κόσμο, μπορεί να πωληθεί σε οποιαδήποτε χώρα, όπως οι ΗΠΑ, που επιλέγει αυτό το καθεστώς. [33].

Στη συνέχεια, λόγω του κανόνα περί μη διατυπώσεων (no-formalities rule), καμία υποχρεωτική καταχώρηση (registration) δεν μπορεί να εφαρμοστεί τουλάχιστον σε ξένους συγγραφείς σε οποιαδήποτε από τις 176 χώρες [33]. Η έννοια του «τίτλου ιδιοκτησίας» είναι χρήσιμη για την κατανόηση αυτής της ιδέας. «Τίτλος ιδιοκτησίας» είναι ο όρος που χρησιμοποιείται στο κοινό δίκαιο και αναφέρεται στη νομική σχέση μεταξύ ενός ατόμου που κατέχει περιουσία και του ίδιου του περιουσιακού στοιχείου [33]. Ένα «διεθνές δικαίωμα πνευματικής ιδιοκτησίας» (βάσει της Σύμβασης της Βέρνης) είναι στην πραγματικότητα 176 εθνικά πακέτα δικαιωμάτων, καθένα από τα οποία μπορεί να διαφέρει ως προς το πεδίο εφαρμογής ή/ και τη διάρκεια. Κάθε μεμονωμένο δικαίωμα από το πακέτο της ιδιοκτησίας, σε κάθε περιοχή, έχει τον δικό του τίτλο ιδιοκτησίας - δηλαδή, και κάθε τίτλος ιδιοκτησίας μπορεί θεωρητικά να έχει διαφορετικό ιδιοκτήτη. Αν κάποιος

ισχυριζόταν ότι υπάρχουν κατά μέσο όρο 10 μεμονωμένα δικαιώματα ανά περιοχή για κάθε έργο πνευματικής ιδιοκτησίας, αυτό θα σήμαινε 1760 μεμονωμένα δικαιωμάτων και επομένως 1760 «τίτλους ιδιοκτησίας». Κάθε τέτοιος τίτλος μπορεί να αξιοποιηθεί και να μεταφερθεί ανεξάρτητα από όλους τους άλλους.

Ο κάτοχος του τίτλου σε ένα μεμονωμένο δικαίωμα μπορεί να μεταβιβάσει τον τίτλο, αλλά μπορεί να αποφασίσει μόνο να επιτρέψει τη χρήση του από συγκεκριμένο τρίτο μέρος με άδεια χρήσης. Αυτή η άδεια μπορεί να είναι αποκλειστική ή μη αποκλειστική (exclusive or nonexclusive). Ένα παράδειγμα αποκλειστικής άδειας χρήσης θα ήταν όταν ο κάτοχος του δικαιώματος προσαρμογής σε ένα μυθιστόρημα (λογοτεχνικό έργο) εξουσιοδοτεί έναν συγκεκριμένο παραγωγό ταινιών να κάνει μια ταινία βασισμένη στο βιβλίο. Επεκτείνοντας το παράδειγμα μη αποκλειστική άδεια παραδίδει ο παραγωγός της ταινίας (ο οποίος έχει γίνει ιδιοκτήτης των πνευματικών δικαιωμάτων της ταινίας) όταν εξουσιοδοτεί 100 κινηματογραφικές αίθουσες να προβάλλουν την ταινία ταυτόχρονα. [33].

3.2.1 Ευρωπαϊκός Κανονισμός φορητότητας περιεχομένου.

Ένα παράδειγμα κατακερματισμού αφορά στον ανωτέρω ευρωπαϊκό κανονισμό [34] ο οποίος απαγορεύει τον γεω-αποκλεισμό του διαδικτυακού περιεχομένου εντός της Ευρωπαϊκής Ένωσης. Ο κανονισμός ρυθμίζει την απεριόριστη πρόσβαση σε (επί πληρωμή) εγγεγραμμένο διαδικτυακό περιεχόμενο όλων των Ευρωπαίων πολιτών, ανεξάρτητα από το πού βρίσκονται στην επικράτεια της ΕΕ. Οι πάροχοι διαδικτυακού περιεχομένου βάσει αμοιβών υποχρεούνται στη συνέχεια να εγγυώνται τη διασυννοριακή φορητότητα των συνδρομητών τους. Απαγορεύεται ο περιορισμός της πρόσβασης ή η απαίτηση πρόσθετων τελών. Ο κανονισμός φορητότητας δεν εφαρμόζεται απευθείας σε προσφορές που δεν υπόκεινται ή δεν υπόκεινται άμεσα σε πληρωμές, όπως οι βιβλιοθήκες πολυμέσων. Είναι μάλλον εθελοντικό για αυτούς τους παρόχους. Επιπλέον, ο Κανονισμός Φορητότητας περιλαμβάνει επίσης κανόνες για την ελαχιστοποίηση των προσωπικών δεδομένων του χρήστη που συλλέγονται προκειμένου να προσδιοριστεί το κράτος μέλος.

3.3 Πνευματική ιδιοκτησία, δικαιώματα και ορθή χρήση μεταξύ των εικαστικών καλλιτεχνών, των ακαδημαϊκών και των μουσείων εικαστικών τεχνών

Σύμφωνα με έκθεση που χρηματοδοτήθηκε από το Ίδρυμα Andrew W. Mellon [35] οι εικαστικοί καλλιτέχνες και άλλοι επαγγελματίες εικαστικών τεχνών, χρησιμοποιείται σε αυτήν την αναφορά για να συμπεριλάβει (μεταξύ άλλων) ιστορικοί τέχνης, εκπαιδευτικοί, καθηγητές, εκδότες, επαγγελματίες μουσείων και γκαλερίστες, μοιράζονται ένα κοινό πρόβλημα στη δημιουργία και κυκλοφορία του έργου τους: σύγχυση και παρανόηση της φύσης του νόμου περί πνευματικών δικαιωμάτων

- Η ορθή χρήση είναι ευέλικτη, διαθέσιμη, και σε πολλές περιπτώσεις αποτελεί τον πυρήνα δραστηριοτήτων εικαστικών και τέχνης.
- Τα μέλη της κοινότητας εικαστικών τεχνών συνήθως υπερεκτιμούν τον κίνδυνο να χρησιμοποιούν ορθή χρήση, γεγονός που τους οδηγεί να το αποφύγουν, ακόμη και σε περιπτώσεις όπου το επιτρέπει ο νόμος και κάτι τέτοιο δεν θα βλάψει τις προσωπικές σχέσεις που είναι απαραίτητες για το έργο τους.
- Πληρώνουν υψηλό τίμημα για τη σύγχυση και παρανόηση πνευματικών δικαιωμάτων. Η δουλειά τους περιορίζεται και λογοκρίνεται (περιορισμός που προκαλούν οι ίδιοι σαν αποτέλεσμα της σύγχυσης και του συνακόλουθου φόβου και άγχους τους).

- Το υψηλότερο κόστος είναι μια υποτροφία που αφήνεται ανολοκλήρωτη, μια γνώση που δεν διατηρείται για την επόμενη γενιά, περιορισμό των ευκαιριών που δημιουργεί η χρήση των ψηφιακών μέσων, το "χαμένο μέλλον".
- Οι καλλιτέχνες είναι πιο πιθανό να χρησιμοποιούν υλικό που προστατεύεται από πνευματικά δικαιώματα χωρίς άδεια, και λιγότερο πιθανό να εγκαταλείψουν ή να αποφύγουν έργα λόγω περιορισμένων πνευματικών δικαιωμάτων.

Το ένα τρίτο όλων των συμμετεχόντων στην έρευνα που διεξήχθη από το College Art Association, όπως αναφέρεται παραπάνω, δήλωσε ότι είχαν εγκαταλείψει ή αποφύγει ένα έργο λόγω προβλημάτων πνευματικής ιδιοκτησίας. Το ποσοστό ήταν το υψηλότερο κατά 57 τοις εκατό μεταξύ των συμμετεχόντων εκδοτών. Το ένα πέμπτο των καλλιτεχνών ανέφεραν ότι αποφεύγουν ή εγκαταλείπουν ένα έργο λόγω αυτό-λογοκρισίας που σχετίζεται με πνευματικά δικαιώματα.

Σε γενικές γραμμές έχει καλλιεργηθεί η κουλτούρα τήρησης των αδειών χρήσης μεταξύ των καλλιτεχνών όπως επίσης η ευρεία αποδοχή ότι όλες οι νέες χρήσεις περιεχομένου που προστατεύεται από πνευματικά δικαιώματα πρέπει να εγκρίνονται ρητά. Αυτή ακριβώς η υπόθεση έχει επηρεάσει αρνητικά κάθε εικαστικό και καλλιτεχνικό τομέα, συνυπολογίζοντας το έργο ιστορικών τέχνης, μουσείων, εκδοτών και καλλιτεχνών. Με την εντατικοποίηση της χρήσης ψηφιακών μέσων αυτή η κουλτούρα τήρησης των αδειών χρήσης έχει επανέλθει στο προσκήνιο. Ο κύριος λόγος για τους οποίους οι καλλιτέχνες αγνοούν την ορθή χρήση είναι η υπερβολική εκτίμηση του κινδύνου. Εξαιτίας της έλλειψης σαφήνειας σχετικά με την ερμηνεία της ορθής χρήσης, την έλλειψη γνώσεων περί πνευματικών δικαιωμάτων γενικά και τον υπερβολικό φόβο για την περίπτωση δικαστικής διαμάχη [35]

3.3.1 Προκλήσεις

Η συγγραφή ενός βιβλίου, η σύνθεση ενός μουσικού κομματιού, ο σχεδιασμός ενός παιχνιδιού, ή οποιαδήποτε άλλη άυλη δημιουργία μέσου επικοινωνίας, προϋποθέτει την καταχώρηση πνευματικής ιδιοκτησίας, ωστόσο το τρέχον σύστημα καταχώρησης δεν λειτουργεί αποτελεσματικά στην πράξη. Η νομοθεσία περί ΠΙ δεν είναι προς το παρόν αποτελεσματική, πιθανότατα γνωρίζετε πόσο εύκολο είναι να κλαπεί το περιεχόμενό σας στο διαδίκτυο. Εάν το να κυνηγάτε τους κλέφτες δεν είναι αρκετά δύσκολο, η επιβολή των νόμιμων δικαιωμάτων σας ως κατόχου έργου ΠΙ εξαρτάται από την απόδειξη ότι είστε ο κάτοχος. Ως καλλιτέχνης, είναι σημαντικό να διατηρήσετε τα δικαιώματα ιδιοκτησίας και την πίστωση, καθώς είναι απογοητευτικό να καταβάλλετε προσπάθεια και χρόνο στη δουλειά σας μόνο για να έχετε πρόσβαση σε άτομα ελεύθερα χωρίς αποζημίωση. Το Διαδίκτυο έχει κάνει τη λήψη βιβλίων στη μουσική, τόσο εύκολη, αλλά με κόστος του δημιουργού. Ένα σημαντικό πρόβλημα με το τρέχον μοντέλο είναι ότι τα δικαιώματα ΠΙ δεν μπορούν να καταχωρηθούν ολιστικά και καθολικά.

Επί του παρόντος, μόλις ένας συγγραφέας ανεβάσει το έργο του στο Διαδίκτυο, καθίσταται εξαιρετικά δύσκολο να διατηρηθεί ο έλεγχος αυτής της εργασίας και να παρακολουθεί ποιος το χρησιμοποιεί για ποιο σκοπό. Σε πολλές χώρες όπως το Ηνωμένο Βασίλειο, οι δημιουργοί δεν έχουν τη δυνατότητα εγγραφής πνευματικών δικαιωμάτων. Αυτό καθιστά δύσκολη την απόδειξη της ιδιοκτησίας. Μπορεί επίσης να είναι δύσκολο για τους δημιουργούς να γνωρίζουν ποιος χρησιμοποιεί ή να επωφελείται από την εργασία τους, και εξίσου δύσκολο για τρίτα μέρη που θα ήθελαν να ζητήσουν άδεια για να γνωρίζουν με ποιον να επικοινωνήσουν. Η έλλειψη κατάλληλης εγγραφής καθιστά δύσκολη τη διακοπή των παραβάσεων ή τη σωστή δημιουργία εσόδων από έργα.

Η ορθή χρήση είναι ζωτικής σημασίας για τις πολιτικές που ενσωματώνονται στη νομοθεσία της ΕΕ περί πνευματικών δικαιωμάτων. Ο στόχος αυτού του νόμου είναι να

προωθήσει την πολιτιστική άνθηση: να προωθήσει τη δημιουργία πολιτισμού και την ανταλλαγή ιδεών. Το πιο γνωστό χαρακτηριστικό του είναι η προστασία των δικαιωμάτων των κατόχων. Ωστόσο, η αντιγραφή, η παραπομπή και η γενική επαναχρησιμοποίηση του υπάρχοντος πολιτιστικού υλικού μπορεί να είναι ένα εξαιρετικά σημαντικό μέρος της δημιουργίας τόσο νέου πολιτισμού όσο και σχολιασμού. Στην πραγματικότητα, η αξία της αντιγραφής είναι τόσο καλά καθιερωμένη που γράφεται στην κοινωνική συμφωνία στην καρδιά του νόμου περί πνευματικών δικαιωμάτων.

Για τα αρχεία, τα μουσεία και τις εκπαιδευτικές οντότητες, λίγα έχουν γραφτεί σχετικά με ζητήματα που σχετίζονται με τα πνευματικά δικαιώματα [35], αλλά οι αρμόδιοι των αδειών του μουσείου τα έχουν συζητήσει στο πλαίσιο των περιπλοκών και των αμφισημιών των καθηκόντων τους. Μια αυξανόμενη βιβλιογραφία, ωστόσο, συζητά τα προβλήματα που μπορεί να θέσει η συμμόρφωση με τα πνευματικά δικαιώματα για διάφορες ψηφιακές πρωτοβουλίες. Τα σχολεία και οι βιβλιοθήκες υποφέρουν από ακατάλληλη καθοδήγηση σχετικά με τα πνευματικά δικαιώματα σχετικά με τις ψηφιακές χρήσεις του περιεχομένου στην εκπαίδευση. Οι θεσμικές πρωτοβουλίες για την παροχή ολοκληρωμένης διαδικτυακής τεκμηρίωσης των συλλογών και των σχετικών αντικειμένων [36]. είναι όλο και περισσότερο γεμάτες καθώς περισσότερα ιδρύματα διαθέτουν εικόνες σχετικά υψηλής ανάλυσης διαθέσιμες, γενικά σε ανοιχτή πρόσβαση. Μία από τις κορυφαίες συζητήσεις για την πολιτική και την πρακτική της ψηφιοποίησης συλλογής, το 2013 Best of Two Worlds του Smithsonian Institution [37], εκφράζει ανησυχία για τον κίνδυνο πνευματικών δικαιωμάτων. Ωστόσο, οι κατευθυντήριες γραμμές για τη δημόσια αδειοδότηση του Smithsonian ενθαρρύνουν το κοινό να εκμεταλλευτεί την ορθή χρήση

3.4 Τεχνητή Νοημοσύνη. Μηχανές που παράγουν έργα ψηφιακού πολιτισμού!

Τον Οκτώβρη του 2018, όταν και σηματοδοτήθηκε η έναρξη μιας νέας εποχής της τέχνης, η γκαλερί Christie's πραγματοποίησε την πρώτη παγκόσμια δημοπρασία έργου τέχνης που παράχθηκε από μηχανισμό Τεχνητής Νοημοσύνης για αντάλλαγμα \$432k! Η δημιουργικότητα πλέον δεν αφορά μόνο τους ανθρώπους, υπονοώντας ότι η μηχανή δημιουργεί αυτόνομα ένα έργο τέχνης. Ενώ η φράση «τεχνητή νοημοσύνη» προκαλεί εικόνες υπερ-ευφυών ρομπότ με δυνατότητες που μοιάζουν με ανθρώπους, αυτές οι έννοιες δεν έχουν γίνει ακόμη πραγματικότητα. Αντ' αυτού, μεγάλο μέρος αυτού που αποκαλούμε «TN» αντιστοιχεί τώρα σε προηγμένη στατιστική ανάλυση ή προβλέψεις και προγνώσεις βάσει μοντέλων που προέρχονται από αυτήν. Προκειμένου μια μηχανή να δημιουργήσει ένα αντικείμενο ψηφιακού πολιτισμού (ζωγραφική, τραγούδι, βίντεο, μυθιστόρημα κ.λπ.) απαιτούνται τα παρακάτω βασικά στοιχεία:

- Αλγόριθμοι μηχανικής μάθησης
- Νευρωνικά δίκτυα
- Τεχνικές ανάλυσης δεδομένων
- Σύνολα δεδομένων
- Υπολογιστές - Άλλη υποδομή
- Ανθρώπινοι πόροι (μια ομάδα επιστημόνων δεδομένων, μηχανικών, καλλιτεχνών και ιστορικών τέχνης)

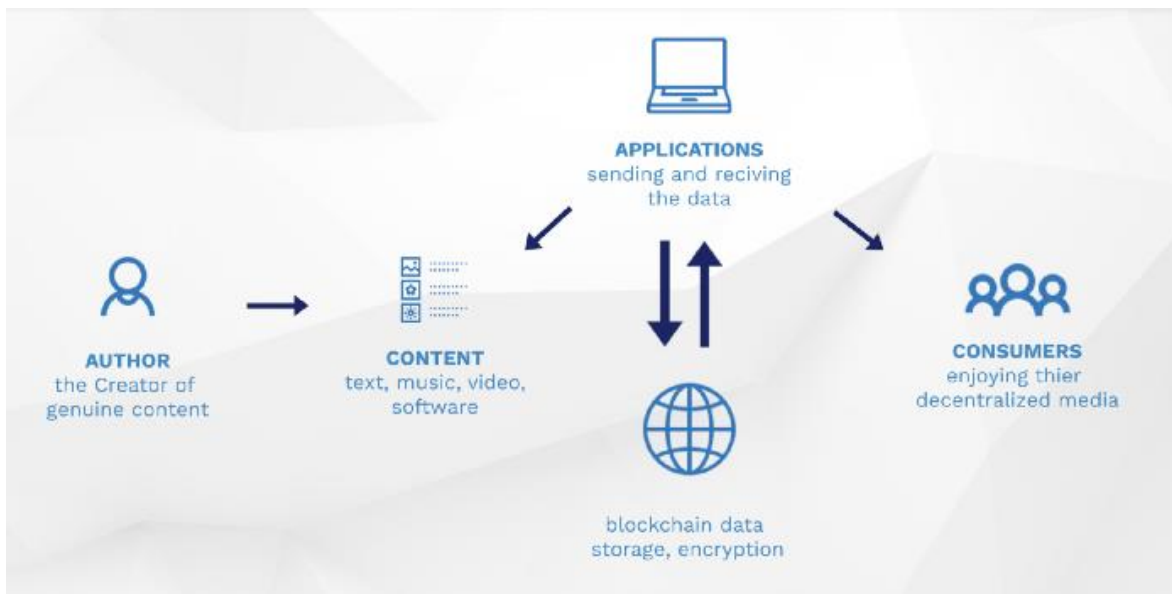


Σχήμα 15 Portrait of Edmond Belamy, 2018, created by GAN (Generative Adversarial Network), which was offered at Christie's in October 2018.

Όλοι οι πάροχοι των παραπάνω συστατικών μπορούν να διεκδικήσουν πνευματική ιδιοκτησία για το τελικό αποτέλεσμα. Αυτό είναι διαμετρικά αντίθετο με ένα παραδοσιακό έργο τέχνης, για το οποίο τα πνευματικά δικαιώματα είναι αυτόματα, λαμβάνονται από τον δημιουργό μόλις το έργο "καταχωρηθεί". Επιπρόσθετα η τέχνη της τεχνητής νοημοσύνης - και ευρύτερα μιλώντας, η δημιουργική τέχνη - είναι αλγοριθμικής φύσης (εξαιρετικά επαναλαμβανόμενη) και συχνά ανοιχτού κώδικα (με δυνατότητα κοινής χρήσης).

4 Ψηφιακός πολιτισμός στο Blockchain

Σε συνέχεια των ανωτέρω ακολουθεί ενότητα που αφορά σε πιθανές περιπτώσεις χρήσης του Blockchain ως βάση δεδομένων που καταγράφει και επαληθεύει συναλλαγές, ως μηχανισμό για την ασφάλεια, τον έλεγχο ταυτότητας και ως εμπορικό μέσο για τον ψηφιακό πολιτισμό. Ενώ αυτές οι προτάσεις βρίσκονται ακόμη στα πολύ πρώιμα στάδια ωριμότητας, παρατίθενται διπλώματα ευρεσιτεχνίας και ορισμένες νεοεμφανιζόμενες εταιρείες για να προσδιοριστούν οι βασικές επιχειρηματικές προτάσεις που υποβάλλονται και να μελετηθεί εάν το blockchain θα οδηγήσει σε ισχυρότερα ή ασθενέστερα δικαιώματα ιδιοκτησίας για τον ψηφιακό πολιτισμό και γενικότερα της πολιτιστικής κληρονομιάς.



Σχήμα 16 Ψηφιακός πολιτισμός στο Blockchain

4.1 Δικαιώματα ΠΙ.

Η προσθήκη ψηφιακών έργων τέχνης στο blockchain σημαίνει να καταγράφεται η ύπαρξή τους μαζί με λεπτομέρειες σχετικά με την προέλευσή τους, την αξία τους, το ιστορικό της έκθεσής τους κ.λπ., σε μια δημόσια, συγχρονισμένη βάση δεδομένων σε πραγματικό χρόνο, η οποία είναι εξαιρετικά δύσκολο να παραβιαστεί κακόβουλα. Δεδομένων των ιδιοτήτων του blockchain, μόλις τα δεδομένα αποθηκευτούν στο κατάστιχο, θα γίνει αμετάβλητο. Αυτό θα συμβεί χωρίς τον έλεγχο μιας κεντρικής αρχής και θα εξαλείψει την ανάγκη για κεντρικά μητρώα καταχώρησης δικαιωμάτων.

4.1.1 Διαχείριση ΠΙ

Εξ' ορισμού ένα δικαίωμα ΠΙ, όπως αναφέρθηκε παραπάνω, ενσωματώνει μια ομάδα από διαφορετικά στοιχεία όπως καταχωρήσεις, μεταδιδόμενα ιδιοκτησίας, όρους άδειας και αμοιβές. Σύμφωνα με αυτά τα χαρακτηριστικά, τα DLT φαίνεται να παρέχουν μια αποκεντρωμένη πλατφόρμα για την καταχώρηση και συντήρηση μητρώων έργων. Βασιζόμενοι στα μητρώα τέτοιων στοιχείων, τα έξυπνα συμβόλαια μπορούν να αυτοματοποιήσουν και να τυποποιήσουν ένα πλήθος συναλλαγών που σχετίζονται με πνευματικά δικαιώματα, για παράδειγμα εκείνων που επιτρέπουν τη χρήση, αναπαραγωγή και εκμετάλλευση περιεχομένου που προστατεύεται από πνευματικά δικαιώματα και των

αμοιβών. Πράγματι, παρά τα πρώτα στάδια της εφαρμογής της τεχνολογίας blockchain σε αγαθά και υπηρεσίες πνευματικών δικαιωμάτων, υπάρχει μεγάλη ανάπτυξη εφαρμογών σε αυτόν τον τομέα, ιδίως στον τομέα της μουσικής στο διαδίκτυο.

Λόγω των προαναφερθέντων χαρακτηριστικών, το blockchain μπορεί να είναι ένα χρήσιμο εργαλείο για την προστασία ΠΙ, καθώς θα μπορούσε να πιστοποιήσει την απόδειξη των καταχωρημένων και μη δικαιωμάτων ΠΙ. Παρέχει αποδείξεις ως μέσω ελέγχου ταυτότητας προέλευσης.

Για τις ευρωπαϊκές ΜΜΕ, αυτός θα μπορούσε να είναι ένας αποτελεσματικός τρόπος για να εξασφαλιστεί η προστασία ΠΙ κατά την επέκταση των επιχειρηματικών δραστηριοτήτων τους, καθώς το blockchain είναι διαθέσιμο 24/7 σε ψηφιακή μορφή. Μέσα στην επόμενη δεκαετία, η τεχνολογία blockchain θα μεταμορφώσει τον τρόπο καταχώρισης και παρακολούθησης ΠΙ των εταιρειών. Θα βελτιώσει τη διαχείριση των δικαιωμάτων με διάφορους βασικούς τρόπους. Πρώτον, οι εταιρείες που ελέγχουν τα πνευματικά δικαιώματα θα έχουν καλύτερη βάση για δεδομένα που μπορούν να καταγράψουν όλες τις εκδόσεις, επαναλήψεις και συνεισφορές σε ένα μεμονωμένο έργο. Όλες οι πληροφορίες για ένα τελικό προϊόν, όπως μια ταινία, ένα βιντεοπαιχνίδι ή μια διαφημιστική καμπάνια, είναι προσβάσιμες σε ένα ολοκληρωμένο πακέτο. Δεύτερον, η δυνατότητα γρήγορης επισκόπησης των συναλλαγών μεταξύ συνεργατών μέσω έξυπνων συμβολαίων θα βελτιώσει τις σχέσεις μεταξύ προμηθευτών, διανομέων και τρίτων. Καταγράφεται η ροή αδειών και πληρωμών σε πραγματικό χρόνο. Σε αυτό το μοντέλο, ένας πάροχος περιεχομένου μπορεί να συνεισφέρει σε ένα μέρος ενός τελικού προϊόντος και να διατηρεί την προβολή της απόδοσης της αγοράς και της χρηματοοικονομικής υποχρέωσης.

Καταργώντας τους μακροχρόνιους περιορισμούς στη διαχείριση δικαιωμάτων ΠΙ, οι επιχειρήσεις θα αναπτύξουν νέες λειτουργικές δυνατότητες και θα πραγματοποιήσουν στρατηγικές επενδύσεις σε ευκαιρίες αγοράς.

4.1.2 Καταχώρηση ΠΙ.

Παρόλο που η εγγραφή πνευματικών δικαιωμάτων δεν αποτελεί αποτελεσματική απαίτηση σε μια νομική διαφωνία ΠΙ, το πιστοποιητικό εγγραφής πνευματικών δικαιωμάτων αποτελεί σημαντικό πλεονέκτημα για τον κάτοχο του, καθώς μπορεί να χρησιμοποιηθεί ως απόδειξη στο δικαστήριο. Λόγω της αποκεντρωμένης φύσης του, το blockchain θα μπορούσε να βοηθήσει τις νομικές υπηρεσίες να αντιμετωπίσουν μια προβλεπόμενη αύξηση των απαιτήσεων εγγραφής πνευματικών δικαιωμάτων. Εάν ένας χρήστης μπορούσε να συνδεθεί σε έναν ιστότοπο εγγραφής πνευματικών δικαιωμάτων χρησιμοποιώντας την τεχνολογία blockchain, και μπορούσε να εγγράψει ανά πάσα στιγμή και από οπουδήποτε τη ΠΙ του, με αμετάβλητη χρονική σήμανση, τότε αυτή η καταχώρηση θα μπορούσε να αποτελεί μια ισχυρή απόδειξη κατοχής δικαιωμάτων. Άρα το Blockchain μπορεί να χρησιμεύσει ως μητρώο καταχώρησης ΠΙ όπου οι ιδιοκτήτες δικαιώματος ΠΙ μπορούν να διατηρούν κατακερματισμένα ψηφιακά πιστοποιητικά και να χρησιμοποιήσουν την πλατφόρμα για να λάβουν δικαιώματα από εκείνους που κάνουν χρήση των δημιουργιών και των εφευρέσεων τους χρησιμοποιώντας ξανά, έξυπνες συμβάσεις. Όπως αναλύθηκε παραπάνω λόγω της μακρόχρονης διαδικασίας έγκρισης και του πλήθους των εθνικών κανονιστικών πλαισίων περί ΠΙ, δεν υπάρχει σαφής τρόπος για να προσδιοριστεί ποιος κατέχει δικαιώματα ΠΙ. Με την εγγραφή των έργων τους σε ένα blockchain, οι συγγραφείς μπορούν να λάβουν αποδεικτικά στοιχεία παραβίασης της ιδιοκτησίας πνευματικών δικαιωμάτων. Μια συναλλαγή blockchain είναι αμετάβλητη, οπότε μόλις εγγραφεί μια εργασία σε ένα κατάστιχο, αυτές οι πληροφορίες δεν μπορούν να χαθούν ή να αλλάξουν. Τα τρίτα μέρη θα μπορούσαν να χρησιμοποιήσουν το blockchain για να δουν την πλήρη αλυσίδα ιδιοκτησίας ενός έργου, συμπεριλαμβανομένων οποιωνδήποτε αδειών, δευτερευουσών αδειών και εκχωρήσεων.

Για τις ευρωπαϊκές ΜΜΕ, η χρήση blockchain θα μπορούσε να προσφέρει ένα πιο αποτελεσματικό μέσο εγγραφής πνευματικών δικαιωμάτων. Το ευρωπαϊκό Γραφείο της Κεντρικής Επιτροπής Υποθέσεων Κυβερνοχώρου ανακοίνωσε την πρώτη παρτίδα των εγχώριων αρχειοθέτησης υπηρεσιών ΠΙ βασισμένο στο blockchain στις 30 Μαρτίου 2019 [38]. Τέτοια εμπορικά διαθέσιμα blockchain προσφέρουν στις ευρωπαϊκές ΜΜΕ υπηρεσίες που εξυπηρετούν στην προστασία της ΙΡ τους. Για παράδειγμα, το Blockchain της Anne Copyright είναι μια πλατφόρμα τρίτου μέρους που παρέχει υπηρεσίες εγγραφής DCI (Digital Copyright Identifier) χρησιμοποιώντας τεχνολογία blockchain.

Οι πλατφόρμες που βασίζονται σε blockchain, όπως το Binded, επιτρέπουν στους συγγραφείς να καταχωρήσουν τη ΠΙ τους. Η καταχώρηση μπορεί να χρησιμοποιηθεί για το πού και πώς χρησιμοποιείται το έργο στο Διαδίκτυο και να ζητήσει άδειες από τρίτα μέρη. Το Binded συνδυάζει τις καταχωρήσεις με το γραφείο πνευματικών δικαιωμάτων των ΗΠΑ, το Instagram και το Twitter για να παρακολουθεί τον τρόπο με τον οποίο χρησιμοποιούνται εικόνες που προστατεύονται από πνευματικά δικαιώματα. Αυτό μπορεί να βοηθήσει τρίτα μέρη να προσδιορίσουν τον δημιουργό ενός έργου και τους ιδιοκτήτες για την αντιμετώπιση παραβάσεων. Στην υφιστάμενη κατάσταση οι ιδιοκτήτες αντιμετωπίζουν δυσκολίες στην προστασία των δικαιωμάτων τους στο διαδίκτυο, δηλαδή μόλις μεταφορτωθεί το έργο στο Διαδίκτυο, καθίσταται δύσκολο να διατηρηθεί ο έλεγχος αυτής της εργασίας και να παρακολουθεί ποιος το χρησιμοποιεί για ποιο σκοπό. Όταν όμως το έργο καταχωρύνται και επαληθεύεται χρησιμοποιώντας πλατφόρμες που βασίζονται σε blockchain, οι συγγραφείς μπορούν να αναζητούν ταυτόχρονα ολόκληρο πλήθος διαφορετικών πηγών για να εξακριβώσουν ποιος χρησιμοποιεί το έργο τους. Αυτό επιτρέπει στους κατόχους ΠΙ να εντοπίζουν και να σταματούν παραβάσεις και διευκολύνει την άδεια χρήσης των δικαιωμάτων ΠΙ τους.

4.1.3 Περιορισμός της πρόσβασης στα μέσα αναπαραγωγής

Τα τελευταία χρόνια έχουν γίνει προσπάθειες μετριασμού της αναπαραγωγής ψηφιακών αντικειμένων χωρίς άδεια χρήσης. Οι πολιτιστικές και δημιουργικές βιομηχανίες εργάζονται για να δημιουργήσουν νόρμες σχετικά με την «πειρατεία» στο διαδίκτυο. Μια άλλη προσέγγιση βλέπει εκείνες τις ίδιες βιομηχανίες να ασκούν πιέσεις στις κυβερνήσεις να εφαρμόσουν τους νόμους περί ΠΙ πιο εκτεταμένα. Ωστόσο, για τεχνικούς λόγους είναι συχνά δύσκολο (ή απαγορευτικά δαπανηρό) να εντοπιστεί η παραβίαση πνευματικών δικαιωμάτων στο διαδίκτυο ή να αναζητηθεί προσφυγή κατά μεμονωμένων παραβατών. Μια άλλη πρόταση, λοιπόν, περιλαμβάνει την ανάπτυξη νέων τεχνικών διορθώσεων για την αποτροπή της εύκολης αναπαραγωγής ψηφιακών αρχείων. Το DRM (Digital Right Management) περιλαμβάνει την ανάπτυξη κωδικοποιητών, rootkit, ενσωματωμένων υδατογραφημάτων, κωδικών ασφαλείας και αλγοριθμικής προστασίας αντιγραφής για συγκεκριμένα έργα, ώστε να παρακάμπεται αυτόματα η αναπαραγωγή ψηφιακών αρχείων. Αυτή η προσπάθεια ήταν επίσης σε μεγάλο βαθμό ανεπιτυχής, είτε επειδή οι χρήστες βρήκαν παραβιάσεις και τρόπους αναπαραγωγής γύρω από τον τεχνικό έλεγχο ή επειδή οι προσεγγίσεις που ακολουθήθηκαν θεωρήθηκαν υπερβολικά παρεμβατικές από τους χρήστες και τους ρυθμιστικούς φορείς ομοίως. (η Amazon Kindle διαγράφει κρυφά τα αγορασμένα βιβλία το 2009 [39]. Η Sony Corporation εγκατέστησε λογισμικό ρίζας (root software) σε συσκευές χρηστών χωρίς να το γνωρίζουν το 2005 [40].

4.1.4 Κάτοχοι δικαιωμάτων και αδειοδότηση μέσω έξυπνων συμβολαίων

Με την δημιουργία- παραγωγή ενός έργου (πχ. Κομμάτι μουσικής ή λογοτεχνίας) που υπόκειται σε ΠΙ, αυτόματα δημιουργείται μια ομάδα από διακριτά αντικείμενα ΠΙ τα οποία ίσως ανήκουν σε διαφορετικές νομικές οντότητες. Η διαχείριση των αντικειμένων ΠΙ, άπαξ τη δημιουργία του έργου (πόσο μάλλον μετά από χρόνια) είναι μια πολύπλοκη

διαδικασία. Η αναγνώριση του κατάλληλου δικαιούχου και ο υπολογισμός του εκάστοτε ποσού πληρωμής του (ανάλογα την συμμετοχή του) είναι δύσκολη. Σήμερα τα σχετικά αρχεία (τίτλοι ιδιοκτησίας) διατηρούνται από την εκάστοτε κρατική- κυβερνητική αρχή ή ιδιωτικό οργανισμό. Επιπλέον στην συντήρηση, ανακύπτουν θέματα ασφάλειας της βάσης. Οι ιδιοκτήτες τίτλων ΠΙ, εξαρτώνται σε αυτά τα τρίτα μέρη για να διασφαλίσουν την ασφάλεια- και διαθεσιμότητα των τίτλων τους. Το κόστος συντήρησης μιας τέτοιας δημόσιας και δια λειτουργικής βάσης δεδομένων μπορεί κάλλιστα να υπερβαίνει τους διαθέσιμους πόρους της αρχής ή του οργανισμού με ίσως καταστροφικά αποτελέσματα. Κάπου εδώ έρχεται ίσως η τεχνολογία blockchain, με μια από τις πιθανές εφαρμογές της που μπορεί να απλουστεύσει, να κάνει πιο αποτελεσματική και διαφανή τη δικαιωμάτων ΠΙ. Όλα τα παραπάνω αρχεία και διαδικασίες μπορούν να καταγραφούν στην ασφαλή, συνεχή και διαφανή αλυσίδα του Blockchain και να νομιμοποιηθεί με την χρήση έξυπνων συμβολαίων. Η δημιουργία εκ του μηδενός ενός τέτοιου συστήματος είναι οικονομικότερη και ευκολότερη (ταχύτερη) συγκριτικά με το να συντηρηθεί το υφιστάμενο σύστημα και επιπρόσθετα θα το καταστήσει δημόσια προσβάσιμο από όλους. Περιγραφικά, κάθε χρήστης που θα έχει την Blockchain εφαρμογή θα αποτελεί ταυτόχρονα κόμβο της και θα μπορεί να έχει πρόσβαση στα δεδομένα αλλά και να συμμετέχει στην ασφάλεια και συνέχεια της, κατακερματίζοντας τα κόστη λειτουργίας. Σαν αποτέλεσμα τα κόστη που αφορούν στην απόδοση των αξιώσεων των ιδιοκτητών, θα μειωθεί σημαντικά. Ο χρόνος επεξεργασίας των πληροφοριών μειώνεται και η ασφάλεια αυξάνεται μιας και μπορούν να αποθηκεύονται σε κινητές συσκευές και φορητούς υπολογιστές κατακερματίζοντας την διαδικασία συντήρησης. Το πλέον βασικό χαρακτηριστικό που προσθέτει η τεχνολογία Blockchain, είναι πως οι ιδιοκτήτες δεν εξαρτώνται από τρίτα μέρη. Μπορούν να ανεξαρτητοποιήσουν και διασφαλίσουν ακόμη και τις μεταξύ τους συναλλαγές χωρίς την παρέμβαση χρηματοπιστωτικών ιδρυμάτων, μέσω έξυπνων συμβολαίων. Με την χρήση τέτοιων συμβολαίων που λειτουργούν αυτόματα σαν αναπόσπαστο κομμάτι του συστήματος, η επεξεργασία των συναλλαγών θα απλοποιηθεί σημαντικά. Σαν αποτέλεσμα της απλότητας του συστήματος οι ιδιοκτήτες θα αυξήσουν τα έσοδα τους μιας και θα περιοριστούν τα έξοδα συναλλαγών. Ας υποθέσουμε πως κάποιος παραγωγός (χρήστης) προτιμά τη πλατφόρμα μετάδοσης περιεχομένου Vimeo και θέλει να χρησιμοποιήσει ένα κομμάτι μουσικής ή ταινίας (που διατίθεται στην πλατφόρμα και υπόκειται σε ΠΙ τρίτου) για ένα νέο δικό του έργο. Σε αυτή τη περίπτωση είτε η πλατφόρμα θα του απαγορεύσει την αναπαραγωγή του νέου του έργου (μιας και αναγνωρίζει πως υπόκειται σε ΠΙ τρίτου) είτε θα διακόψει την δυνατότητα αναπαραγωγή του όταν το τρίτο μέρος το αναγνωρίσει (και αιτηθεί σχετικά). Ωστόσο σε ένα σύστημα βασισμένο στην τεχνολογία Blockchain που συμπεριλαμβάνει έξυπνα συμβόλαια στο μπλόκ του, θα μπορούσε εξ' αρχής ο νέος παραγωγός να υπογράψει το συμβόλαιο, να ενημερωθούν αυτοματοποιημένα όλα τα εμπλεκόμενα μέρη και νομιμοποιηθεί η αναπαραγωγή μέσω της πλατφόρμας. Σε ένα τέτοιο σενάριο, ο παραγωγός περιεχομένου θα μπορούσε να χρησιμοποιήσει το έργο που προστατεύεται από πνευματικά δικαιώματα (τρίτου) μέσα σε λίγα δευτερόλεπτα όπως επίσης η πλατφόρμα και ο σωστός κάτοχος να λάβουν αποζημίωση για τα δικαιώματα τους.

4.1.4.1 Περίπτωση Αρχαιολογικού Νόμου (Νόμος 3028/2002)

Σύμφωνα με την παραπάνω ανάλυση μια πιθανή εφαρμογή του Blockchain θα μπορούσε να αφορά στο Άρθρο 8 με τίτλο «Δήλωση, υπόδειξη ακινήτων αρχαίων και αμοιβή» του νόμου 3028/2002 [28]. Σύμφωνα με την συγκεκριμένη εθνική διάταξη περί προστασίας των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς, για κάθε ανακάλυψη νέου αγαθού απαιτείται η άμεση καταγραφή στις σχετικές εθνικές αρχές. Απαραίτητα στοιχεία καταγραφής είναι:

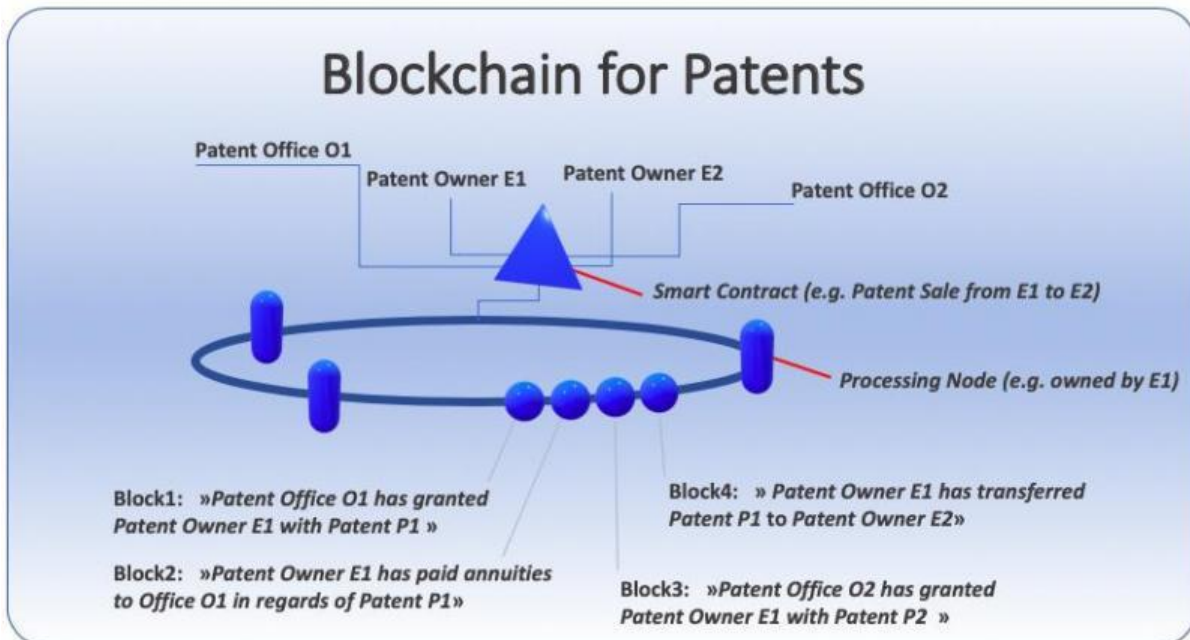
- Συντεταγμένες αγαθού,
- Αρχή προστασίας,

- Αναγκαία μέτρα φύλαξης και προστασίας,
- Χρηματική αμοιβή στο πρόσωπο ή πρόσωπα (ποσοστιαία)

Ένα οικοσύστημα παρακολούθησης των εγγραφών, βασισμένο στην αρχιτεκτονική Blockchain, θα μπορούσε να είναι πολύ αποτελεσματικό, δημόσιο, ασφαλές, διαφανές και αποδοτικό. Θα μπορούσε να εξυπηρετεί αποτελεσματικά πληρωμές εμπλεκόμενων μερών, τις εσωτερικές λειτουργίες και «διασυνδέσεις» των εμπλεκόμενων εθνικών αρχών.

4.2 Διπλώματα ευρεσιτεχνίας (Patents)

Τα διπλώματα ευρεσιτεχνίας κατανέμονται διακρατικά εκ φύσεως. Δεν υπάρχει ενιαίο μητρώο διπλωμάτων ευρεσιτεχνίας, αλλά πολλά διασκορπισμένα σε όλο τον κόσμο. Ως



Σχήμα 17 Blockchain for patents

εκ τούτου, η ιδέα ενός καταμεμημένου δικτύου παρέχει μια έξυπνη λύση στις υπηρεσίες διαχείρισης ευρεσιτεχνιών. Αλλά το πραγματικό όφελος του blockchain είναι για ακόμη μια φορά η χρήση έξυπνων συμβολαίων.

Ας μελετήσουμε ένα απλό παράδειγμα συναλλαγής, την αγορά μιας ευρεσιτεχνίας. Στην υφιστάμενη κατάσταση εμπλέκεται διαφορετικός πάροχος υπηρεσίας (service provider) για το κάθε βήμα της συναλλαγής ώστε να:

- ελεγχθεί η εκχώρηση του διπλώματος ευρεσιτεχνίας,
- ελεγχθεί η εγκυρότητα του διπλώματος ευρεσιτεχνίας,
- γίνει διαπραγμάτευση της συμφωνίας πώλησης,
- εκτελεσθεί και πληρωθεί η συναλλαγή,
- ενημερωθούν τελικά όλα οι εμπλεκόμενες υπηρεσίες διπλωμάτων ευρεσιτεχνίας για τη συναλλαγή (η οποία είναι τόσο περίπλοκη που σπάνια γίνεται).

Στο χώρο του blockchain όμως, όλες αυτές οι εργασίες αυτοματοποιούνται πλήρως. Το όφελος είναι, δραστική μείωση των συναλλαγών και της πολυπλοκότητας και τελικά μείωση του συνολικού κόστους λειτουργίας του συστήματος.

4.3 Εμπορικά σήματα

Αντίστοιχα με τα τις παραπάνω περιπτώσεις το blockchain μπορεί να δώσει λύσεις στην διαχείριση εμπορικών σημάτων. Υπάρχουν ήδη εγκατεστημένα blockchain συστήματα τα οποία διαθέτουν δυνατότητα καταχώρισης και προστασίας σημάτων. Τα συστήματα παρέχουν επιπλέον υπηρεσίες όπως αποδεικτικά στοιχεία ιδιοκτησίας διατηρώντας αρχεία συναλλαγών. Δεδομένου πως αυτή η εναλλακτική πλατφόρμα παγιωθεί, μπορεί να ανταγωνιστεί τις παραδοσιακές υπηρεσίες εμπορικών σημάτων που προσφέρονται από παρόχους υπηρεσίες ΠΙ, δικηγόρους και πράκτορες εμπορικών σημάτων.

Ο αγώνας κατά της παραποίησης, τόσο διαδικτυακά όσο και για φυσικά προϊόντα, δεν τελειώνει ποτέ για τους κατόχους σημάτων. Οι υπάρχοντες δείκτες γνησιότητας (όπως λογότυπα, κωδικοί QR, μάρκες NFC, κ.λπ.) ενώ είναι καλύτεροι από τίποτα, παρακάμπτονται σχετικά εύκολα, ειδικά όταν οι παραχαράκτες μπορούν να επωφεληθούν από τη μη ολοκληρωμένη καταχώριση διεθνών σημάτων. Αντίθετα, εάν ένα προϊόν φέρει ετικέτα με ένα μοναδικό αναγνωριστικό που αντιστοιχεί σε μια εγγραφή σε ένα μπλοκ για αυτό το συγκεκριμένο στοιχείο, είναι πολύ απλούστερο να επαληθεύσετε ότι το σχετικό προϊόν είναι νόμιμο και ανήκει στο σωστό μέρος, ακόμα και όταν έχει πωληθεί ή παραχωρηθεί μέρος χρήσης του (άδεια). Όπως πάντα ισχύει η αρχή "Garbage In Garbage Out", έτσι το Blockchain θα φέρει πλεονεκτήματα μόνο όταν η πώληση ή η σάρωση ως μέρος μιας αλυσίδας επιβάλλεται επιμελώς.

Η χρήση έξυπνων συμβολαίων σε ρυθμίσεις προσανατολισμένες στα εμπορικά σήματα είναι πιθανό να αυξηθεί. Επειδή η τεχνολογία λειτουργεί εκτός προκαθορισμένων συνθηκών που έχουν προγραμματιστεί ως μέρος συγκεκριμένων μπλοκ στην αλυσίδα, μη αναμενόμενα ζητήματα ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια και την εγκυρότητα των συναλλαγών. Τι μπορεί να βοηθήσει; Για την προώθηση βέλτιστων πρακτικών στη σχέση του νόμου περί εμπορικών σημάτων με το blockchain, οι συμπράξεις δημόσιου-ιδιωτικού τομέα μπορούν να προσφέρουν μια καλή λύση. Υπάρχουν κρίσιμοι ρόλοι για τις παραπάνω υπηρεσίες (WIPO, WTO και CIPO) να διαδραματίσουν στην προώθηση θεμιτών αρχών και προτύπων σε έξυπνα συμβόλαια προσανατολισμένα στα εμπορικά σήματα.

4.4 Οικονομικά στοιχεία

Στην παρακάτω ενότητα παραθέτουμε κάποια οικονομικά σχετικά με την κυκλοφορία έργων πολιτιστικής κληρονομιάς. Στο πλαίσιο της εξασφάλισης αμοιβής δημιουργού-δικαιούχου, η τεχνολογία blockchain μπορεί να παίξει σημαντικό ρόλο όπως ακολούθως. Αρχικά μπορεί με σιγουριά να διαχειριστεί τις πληρωμές όπως οι έως τώρα τεχνολογίες και οι υφιστάμενες πλατφόρμες. Δευτερευόντως όπως εκτενώς αναλύθηκε παραπάνω μπορεί να διαχειριστεί αποτελεσματικά πληρωμές που αφορούν σε δικαιούχους με άδεια χρήσης κάποιου επιμέρους δικαιώματος ΠΙ χρησιμοποιώντας έξυπνα συμβόλαια. Τέλος προσφέρει διαφάνεια, ασφάλεια και δεν απαιτεί την εμπλοκή ενδιάμεσων τρίτων μερών-μεσαζόντων. Για την αποτελεσματική απόδοση δικαιωμάτων ΠΙ και δικαιώματα εκμετάλλευσης η τεχνολογία blockchain του μέλλοντος θα πρέπει να αναπτυχθεί περαιτέρω σε τρεις ξεχωριστές φάσεις του κύκλου ζωής του: tokens που αντιπροσωπεύουν το αγαθό ή το περιουσιακό στοιχείο (δημιουργία ή/ και απόκτηση), υπηρεσίες παρακολούθησης (tracking) με γνώμονα την συνεισφορά στην εξέλιξη της διαχείρισης ΠΙ και τέλος μια πλατφόρμα για την διαχείριση πωλήσεων, αδειοδότησης και εκμετάλλευσης των δικαιωμάτων.

- Δημιουργία ή/ και απόκτηση δικαιωμάτων: Ένας παραγωγός αγοράζει το σενάριο για μια νέα παράσταση. Το σύστημα blockchain θα δημιουργήσει tokens που αντιπροσωπεύουν το σενάριο και κάθε υποκείμενο στοιχείο

(επιμέρους δικαίωμα) ΠΙ, συμπεριλαμβανομένων των δικαιωμάτων χρήσης χαρακτήρων και τίτλου.

- Συνεισφορά στην εξέλιξη της διαχείρισης ΠΙ: Μία εταιρεία μουσικής προσλαμβάνεται προσωπικό για να δημιουργήσει ένα τραγούδι θέματος για την παράσταση. Η μη εμπορική συμφωνία, συμπεριλαμβανομένων όρων και προϋποθέσεων, εντάσσεται/ προσαρτάται στο blockchain ως έξυπνο συμβόλαιο. Δημιουργούνται πιστωτικές και χρεωστικές πληροφορίες και αποστέλλονται σωστές χρεώσεις για υπηρεσίες σε κάθε πλευρά της συναλλαγής.
- Αδειοδότηση χρήσης: Υπογράφονται συμβάσεις μεταξύ του διανομέα (του προϊόντος) και των κατόχων δικαιωμάτων ΠΙ που επιτρέπουν τη χρήση του περιεχομένου τους. Καθώς ο διανομέας αναφέρει συναλλαγές σε πραγματικό χρόνο, η επιχειρηματική λογική ενεργοποιείται στο blockchain για τον αυτόματο υπολογισμό των όρων πληρωμής με βάση τον τύπο εκμετάλλευσης του προϊόντος στην αγορά. Επειδή οι συμβατικοί όροι μοιράζονται μεταξύ του δικαιούχου πληρωμής και του πληρωτή, κάθε μέρος μπορεί να επαληθεύσει τη σωστή οικονομική υποχρέωση.

4.4.1 Τα οφέλη του blockchain για διαχείριση δικαιωμάτων ΠΙ και πληρωμών

- Καλύτερη διαχείριση των άυλων περιουσιακών στοιχείων που είναι αποδεδειγμένα μοναδικά: Η ΠΙ μπορεί να αποδειχθεί όπως επίσης και τοίχων συνεισφορά τρίτων (πέραν του δικαιούχου) μπορεί να αποδοθεί εξ αρχής για κάθε κοινό περιουσιακό στοιχείο. Χρησιμοποιώντας υπάρχοντα εργαλεία, διάφορες ομάδες μπορούν να συνεργαστούν και να μοιράζονται το περιεχόμενο, διατηρώντας παράλληλα την προέλευση και την απόδοση πιστώσεων. Ωστόσο, η εισαγωγή της τεχνολογίας blockchain επιτρέπει την εμπορευματοποίηση περιουσιακών στοιχείων που μπορούν να επαναχρησιμοποιηθούν, να ανταλλαχθούν και να εκχωρηθούν ως νομισματική αξία.
- Αύξηση αποτελεσματικότητας και ταχύτητας διεκπεραίωσής συναλλαγών μέσω δικτύου peer-to-peer: Οι συναλλαγές και οι κινήσεις αξίας μοιράζονται στο δίκτυο, μειώνοντας έτσι τα στάδια της συναλλαγής κατά τη διάρκεια των διαδικασιών αδειοδότησης και διαχείρισης συμβάσεων. Καθώς καταγράφονται οι πραγματικές εισροές, ένα έξυπνο συμβόλαιο αυτοματοποιεί εξαρτώμενες συναλλαγές, ειδοποιεί σχετικά τρίτα μέρη και υπολογίζει αμέσως την εκάστοτε οικονομική υποχρέωση
- Βελτίωση στις σχέσεις μεταξύ συνεργατών σε ένα διαφανές κατάστιχο: Είναι συχνό το φαινόμενο διαφορετικά εμπλεκόμενα μέρη να ζητούν πρόσβαση σε περιουσιακά στοιχεία ή δικαιώματα ΠΙ πχ. όρους σύμβασης και το αρχείο καταγραφής συναλλαγών. Χρησιμοποιώντας ένα κοινόχρηστο κατάστιχο, η λειτουργία ελέγχου που επαναλαμβάνεται από τα διάφορα εμπλεκόμενα μέρη πρέπει να πραγματοποιηθεί μόνο μία φορά. Η πλατφόρμα επιτρέπει επίσης αναφορές αυτοεξυπηρέτησης μέσω προσαρμοσμένων εφαρμογών και ενοποίησης με τα υπάρχοντα συστήματα πληροφορικής.

4.4.2 Το άυλο περιουσιακό στοιχείο: Προσωπικά Δεδομένα Χρηστών (Data monetization)

Το Data Monetization είναι ένας γενικός όρος για να περιγράψει το πώς μια εταιρεία μπορεί να χρησιμοποιήσει τα δεδομένα που έχει στην διάθεση της για να αναπτύξει καινούργιες πηγές εσόδων. Οι συναλλαγές που βασίζονται στο Blockchain αποτελούν έναυσμα για ένα νέο επιχειρηματικό μοντέλο που εστιάζει όχι στα έσοδα από τις πωλήσεις

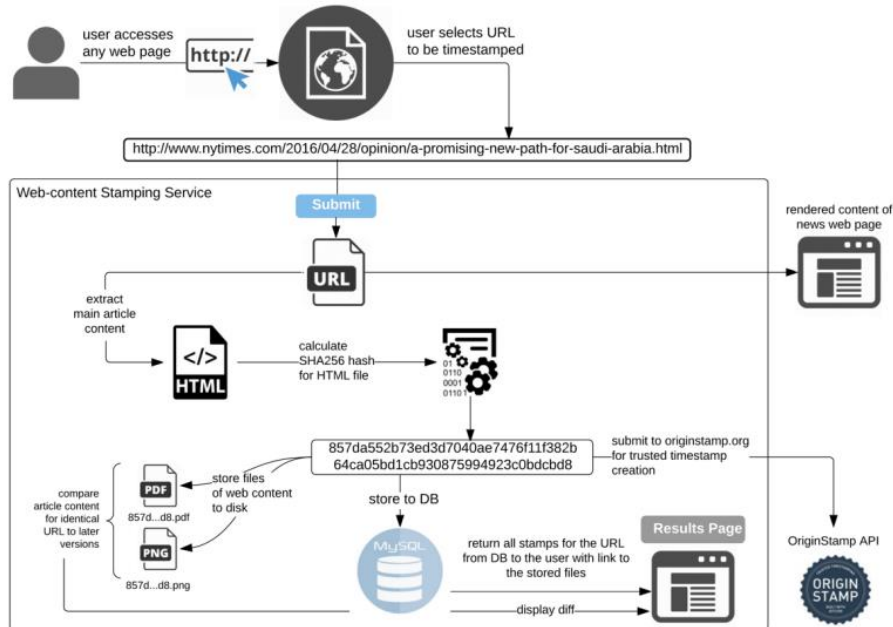
ή το crowdfunding αλλά στη δημιουργία εσόδων από δεδομένα που σχετίζονται με αυτές τις συναλλαγές. Η λογική μετατοπίζεται από την πώληση ψηφιακών αγαθών προς τη δημιουργία εσόδων δεδομένων σχετικά με τον τρόπο με τον οποίο οι καταναλωτές ή οι συλλέκτες αλληλοεπιδρούν και χρησιμοποιούν το περιεχόμενο, πώς κυκλοφορούν αρχεία, τι άλλο αγοράζουν οι χρήστες και ούτω καθεξής. Αυτά τα δεδομένα μπορούν να συγκεντρωθούν από άλλα κοινωνικά μέσα και δεδομένα δικτύου σχετικά με το τι τους αρέσει, τι αγοράζουν και τι λένε στα μέσα κοινωνικής δικτύωσης. Η δυνατότητα παρακολούθησης των συμπεριφορών των χρηστών είναι μια ισχυρή εισοδηματική ροή. Επίσης, το να υπάρχουν αναλυτικά δεδομένα σχετικά με τη κυκλοφορία και την κοινή χρήση κομματιών ενός καλλιτέχνη μπορεί να προσφέρει ενδείξεις για τη συνολική αξία του καλλιτέχνη εκτός των παραδοσιακών οικονομικών καναλιών. Εδώ, τα δεδομένα σχετικά με την κυκλοφορία της εργασίας και τη συνολική δημοτικότητά τους, τις επισημάνσεις "μου αρέσει" και τα μερίδια καθίστανται πληρεξούσιοι για την οικονομική αξία και μπορεί στην πραγματικότητα να είναι πιο πολύτιμα από το ίδιο το πολιτιστικό αγαθό.

4.4.3 Νέα μοντέλα πληρωμών

Πέραν όλων των παραπάνω περί αποτελεσματικότερης διαχείρισης δικαιωμάτων, το Blockchain μπορεί να εγκαταστήσει νέα μοντέλα πληρωμών, όπως χρηματοδότηση πλήθους (Crowd funding), "πλήρωσε αυτό που θέλεις" (pay what you want), ενοικίαση ή μικροπληρωμές μέσω έξυπνων συμβολαίων. Για παράδειγμα, ένας καταναλωτής μπορεί να επιλέξει να κάνει μια μικροπληρωμή (να πληρώσει μόνο για ένα κομμάτι του έργου) σε έναν καλλιτέχνη. Το μοντέλο αυτό μικροπληρωμών, της λογικής "πλήρωσε αυτό που θέλεις", χρησιμοποιήθηκε από το άλμπουμ των Radiohead In Rainbows το 2008, το οποίο δημιούργησε έσοδα 3 εκατομμυρίων δολαρίων. Ένα blockchain επιτρέπει επίσης νέες ομάδες εμπλεκόμενων μερών, συμπεριλαμβανομένων όσων έχουν συνεισφέρει σε οποιαδήποτε πτυχή ενός ψηφιακού έργου (όπως οι μουσικοί, οι συνθέτες τραγουδιών, οι μηχανικοί μίξης και mastering, οι μηχανικοί ήχου, οι καλλιτέχνες βίντεο και οι γραφίστες του εξωφύλλου) μπορούν όλοι να αμείβονται αυτόματα ανάλογα κάποιο προκαθορισμένο ποσοστό κατά την πώληση ενός έργου. Αν και αυτό παρέχεται ήδη από τις συμβατικές συμβάσεις, τέτοιες υποδιαιρέσεις δικαιωμάτων μπορούν να αυτοματοποιηθούν σε έξυπνα συμβόλαια. Επιπλέον, η νομιμότητα που απαιτείται για τη δημιουργία τόσο περίπλοκων υποδιαιρέσεων και το σχετικό κόστος δεν αποτελούν πρόβλημα. Τα έξυπνα συμβόλαια παρέχουν την ευκαιρία να αμείβουν πολλούς καλλιτέχνες που έχουν συμβάλει σε ένα πολιτιστικό αγαθό (μερικοί από τους οποίους μπορεί να είναι συνεργάτες, ή θαυμαστές ή και επενδυτές). Το θετικό σε αυτή τη προσέγγιση είναι πως πτυχές (επιμέρους δικαιώματα) ενός έργου αποζημιώνονται εντός της δομής, χωρίς εμπλοκή εξωτερικών τρίτων μερών κάτι που προσθέτει ανεξαρτησία, ελευθερία, αφοσίωση, ασφάλεια. Όλα τα παραπάνω καθιστούν το blockchain μια ισχυρή πλατφόρμα για μαζική δωρεάν κουλτούρα.

4.4.4 Χρονική σήμανση (timestamping) ψηφιακών έργων με blockchain

Όπως περιγράψαμε παραπάνω το ποσοστό των πληροφοριών/ δεδομένων που διατίθενται αποκλειστικά στο διαδίκτυο αυξάνεται εκθετικά συνεχώς. Εν αντίθεσή με τα φυσικά έντυπα μέσα ενημέρωσης, τα διαδικτυακά ειδησεογραφικά πρακτορεία, τα ηλεκτρονικά περιοδικά ή τα ιστολόγια διαθέτουν αναδρομική τροποποίηση. Μια τέτοια σημαντική και αναδρομική επεξεργασία κειμένου σε διαδικτυακές πηγές ειδήσεων μπορεί να γίνει εύκολα και απαρατήρητα. Αυτό αποτελεί πρόκληση για τη διατήρηση της ψηφιακής πολιτιστικής κληρονομιάς. Είναι σχεδόν αδύνατο για τους τακτικούς αναγνώστες να επαληθεύουν εάν το περιεχόμενο που συναντούν στο διαδίκτυο έχει τροποποιηθεί σε κάποιο σημείο από την αρχική του κατάσταση και σε ποια ώρα ή σε ποιο βαθμό το κείμενο τροποποιήθηκε στην τρέχουσα έκδοσή του. Το Blockchain μπορεί να



Σχήμα 18 Overview of trusted timestamping system functionality

παρέχει αποκεντρωμένες αξιόπιστες πληροφορίες χρονικής σήμανσης (DTT) από σημαντικές διαδικτυακές πηγές ψηφιακής πολιτιστικής κληρονομιάς. Η αξιόπιστη χρονική σήμανση είναι μια διαδικασία για την απόδειξη ότι ορισμένες ψηφιακές πληροφορίες υπήρχαν σε μια δεδομένη χρονική στιγμή [26]. Υπάρχουν ήδη πολλά πρωτόκολλα που μπορούν να χρησιμοποιηθούν για τη δημιουργία αυτόματων αξιόπιστων χρονικών σημείων για οποιοδήποτε διαδικτυακό περιεχόμενο. Μια επισκόπηση της λειτουργικότητας παρουσιάζεται παρακάτω [41].

4.5 Πρωτοβουλίες

Μια καινοτόμος ιδέα παρουσιάστηκε από την startup Verisart, η οποία σχεδιάζει να χρησιμοποιήσει τεχνολογία blockchain για τον έλεγχο της αυθεντικότητας των καλλιτεχνικών έργων. Αυτό συνεπάγεται τη δημιουργία ενός διεθνούς αρχείου που συμπεριλαμβάνει όλα τα έργα τέχνης και συλλεκτικά αντικείμενα, καθώς και των μεταδεδομένα μουσείων. Η τεχνολογία θα εγγυάται την ανωνυμία των μερών καθώς και θα προσφέρει αυξημένη ασφάλεια. Το αποτέλεσμα θα αποτελούσε πολύτιμο περιουσιακό στοιχείο για τους καλλιτέχνες, συλλέκτες και ακόμη και ασφαλιστές [7].

Επιπλέον, η Deloitte έχει μια νέα προσέγγιση για τη διασφάλιση της αυθεντικότητας των καλλιτεχνικών δημιουργιών και τον εντοπισμό της διακίνησης τους. Η απόδειξη της έννοιας «ArtTracktive» αντιμετωπίζει το πρόβλημα της κακής τεκμηρίωσης σχετικά με την προέλευση ενός έργου τέχνης. Με ένα σύστημα blockchain, όλες οι λεπτομέρειες σχετικά με την ιστορία και τις κινήσεις ενός έργου τέχνης θα καταγραφούν και θα είναι εύκολο να παρακολουθούνται.

Αφού έλαβε προτάσεις από την IP Australia και τη Ρωσική Ομοσπονδία, η Επιτροπή Προτύπων WIPO (CWS) δημιούργησε την "Ομάδα Εργασίας Blockchain" τον Οκτώβριο του 2018 για να εξετάσει τα ακόλουθα:

- Διερεύνηση της δυνατότητας χρήσης τεχνολογίας blockchain στις διαδικασίες παροχής προστασίας δικαιωμάτων IP, επεξεργασίας πληροφοριών σχετικά με αντικείμενα IP και τη χρήση τους.

- Συλλογή πληροφοριών σχετικά με τις εξελίξεις στο Γραφείο Διανοητικής Ιδιοκτησίας (IPO) στη χρήση και την εμπειρία με το blockchain, την αξιολόγηση των τρεχόντων Βιομηχανικών Προτύπων στο blockchain και την εξέταση της αξίας και της εφαρμογής σε IPO
- Ανάπτυξη ενός μοντέλου για την τυποποίηση προσεγγίσεων της χρήσης τεχνολογίας blockchain στο πεδίο IP, συμπεριλαμβανομένων των κατευθυντήριων αρχών, της κοινής πρακτικής και της χρήσης της ορολογίας ως πλαισίου που υποστηρίζει τη συνεργασία, κοινά έργα και αποδείξεις έννοιας.
- Προετοιμασία μιας πρότασης για ένα νέο πρότυπο WIPO που εφαρμόζει τεχνολογία blockchain στις διαδικασίες παροχής προστασίας δικαιωμάτων IP, επεξεργασίας πληροφοριών σχετικά με αντικείμενα IP και τη χρήση τους.

Στη συνέχεια, το WIPO φιλοξένησε ένα διήμερο εργαστήριο σχετικά με τα πρότυπα για την τεχνολογία Blockchain στη Γενεύη στις 29-30 Απριλίου 2019. Τα ευρήματα και τα αποτελέσματα αυτού του εργαστηρίου θα συζητηθούν στην προσεχή συνάντηση του CWS τον Ιούλιο του 2019.

4.5.1 Πρωτοβουλία IPwe

Η IPwe είναι η πρώτη παγκόσμια αγορά διπλωμάτων ευρεσιτεχνίας στον κόσμο που συνδυάζει πληροφορίες και εργαλεία για τον εντοπισμό, την έρευνα, την κατανόηση και τη συναλλαγή των διπλωμάτων. Το IPwe επιτρέπει τις παραδοσιακές συναλλαγές (άδειες και εξαγορές) και ενδυναμώνει νέες κατηγορίες συναλλαγών όπως χρηματοδοτήσεις, πληρωμές τελών συντήρησης και ασφάλιση. Η πλατφόρμα της IPwe είναι βασισμένη στην τεχνολογία Blockchain και η διαχείριση της ανήκει αποκλειστικά. Πρόσφατα όμως η IPwe δεσμεύτηκε να αλλάξει τη διακυβέρνηση του μητρώου της και να το παραδώσει σε μια ομάδα χρηστών (υπηρεσίες ευρεσιτεχνιών) εφόσον ενδιαφερθούν και φέρουν έγκυρα νομιμοποιητικά και πιστοποιητικά στοιχεία. Αυτή η δυνατότητα ενεργοποιείται αποκλειστικά από το blockchain. Ένα μειονέκτημα που αναφέρεται συχνά, αφορά στη ταχύτητα των συναλλαγών που όμως στον γενικότερο πλαίσιο των διπλωμάτων ευρεσιτεχνίας, δεν είναι βασική προϋπόθεση.

Η ρευστότητα και η αναποτελεσματικότητα του υφιστάμενου οικοσυστήματος διπλωμάτων ευρεσιτεχνίας αποθαρρύνουν εμπλεκόμενους όπως οι ΜΜΕ και τα πανεπιστήμια, να προστατεύσουν (και να χρηματοδοτήσουν) τις ιδέες τους. Οι τεχνολογίες Blockchain έχουν τη δυνατότητα να προσφέρουν μεγαλύτερη απλότητα, διαφάνεια, λιγότερους μεσάζοντες και τελικά να προωθήσουν την καινοτομία μεταξύ οντοτήτων που είχαν μια δύσκολη πρόσβαση στον κόσμο των διπλωμάτων ευρεσιτεχνίας [7].

5 Κανονιστικά, νομικά και ηθικά ζητήματα Blockchain

5.1 Νομικές επιπτώσεις

Το Blockchain ενσωματώνει χαρακτηριστικά που θα αποτελούσαν πολύτιμο πλεονέκτημα στην επιβολή του νόμου. Η διαφάνεια το απυρόβλητο και το αμετάβλητο των συναλλαγών το καθιστούν κατάλληλο για την επιβολή του νόμου όταν απαιτείται ο εντοπισμός όλων των συναλλαγών που εκτελούνται ή εκτελέστηκαν, πράγμα που είναι αδύνατο με «μετρητά» και τα λοιπά διαδεδομένα συστήματα. Αντιστοιχίζοντας μια διεύθυνση IP σε έναν μεμονωμένο χρήστη, θα μπορεί να εντοπιστούν όλες οι συναλλαγές στις οποίες έχει συμμετάσχει το άτομο με αυτήν τη διεύθυνση. Αν και δεν είναι εύκολη διαδικασία, καλύτερα εργαλεία και μέθοδοι δημιουργούνται συνεχώς για να καταστεί δυνατή αυτή η σύνδεση. Τα δεδομένα στο blockchain είναι μόνιμα, πλήρη, ακριβή και δημοσίως προσβάσιμα. Επομένως, τα δεδομένα δεν μπορούν να εξαφανιστούν μυστηριωδώς από το κατάστιχο. Δεν είναι απαραίτητη η κλήτευση ή το ένταλμα αναζήτησης που σημαίνει ότι η πρόσβαση στα δεδομένα γίνεται ευκολότερη, ανώνυμα και διακρατικά.

5.2 Lex Mercatoria

Ο όρος είναι λατινικός και κατά λέξη αποδίδεται ως "εμπορικός νόμος". Πρόκειται όμως για κάτι πέρα από έναν "εμπορικό νόμο": η lex mercatoria χρησιμοποιείται ως τεχνικός όρος για να αναφερθούμε σε ένα σύνολο κανόνων δικαίου, το οποίο επιλέγεται κατά τις διεθνείς συναλλαγές, ως το πιο πρόσφορο και για τα δύο μέρη, προκειμένου να αποφύγουν τις αμφισβητήσεις που θα δημιουργούσε η εφαρμογή του εκάστοτε τοπικού θετικού δικαίου, το οποίο δεν περιείχε διατάξεις για κάθε εμπορική διαφορά που θα μπορούσε να προκύψει. Ιστορικά, η lex mercatoria αναπτύχθηκε κατά τον μεσαίωνα από τους ευρωπαϊούς εμπόρους και αποτελούσε ένα κοινά αποδεκτό πλαίσιο εθιμικών κανόνων και βέλτιστων πρακτικών που είχαν καταξιωθεί στις συναλλαγές. Μπορεί να μην είχε δηλαδή μια θεσμική βάση σε συγκεκριμένο εθνικό δίκαιο, αλλά το ζητούμενο ήταν η αποτελεσματικότητα της εφαρμογής του, και κάτι ακόμα, το οποίο καμία θεσμική διαδικασία δεν μπορεί να υποκαταστήσει ως προς το βαθμό κανονιστικότητας: ήταν γνωστό σε όλους τους εμπλεκόμενους. Η ευρύτατη γνώση του κανόνα (η "γενική κοινοποίηση", κατά Καντ) είναι στην πραγματικότητα μια μήτρα κανονιστικότητας πολύ πιο ισχυρή από την νομιμοποίηση μέσω της θεσμικής διαδικασίας. Άλλωστε και οι νομοπαραγωγικοί θεσμοί, με όλο το τελετουργικό που ακολουθούν, αυτό επιδιώκουν: η θέσπιση των νόμων να γίνεται όσο το δυνατόν πιο δημόσια, ώστε ουδείς να μπορεί να επικαλεστεί άγνοια δικαίου. Η δημοσιότητα είναι το imperium του νομοθέτη. Αρχικά η lex mercatoria ήταν ένα σύνολο κανόνων και αρχών που ακολουθούσαν οι ίδιοι οι έμποροι, για να ρυθμίσουν τις συμφωνίες τους. Σε αυτό τους οδήγησε η ανάγκη για γρήγορη επίλυση των διαφωνιών: οι νομικές επιπλοκές και καθυστερήσεις δεν είναι ακριβώς ένας παράγοντας ανάπτυξης και προαγωγής του εμπορίου. Έτσι οι έμποροι επέλεξαν οι ίδιοι δικαστές για να εφαρμόσουν την lex mercatoria κατά την επίλυση των διαφορών τους, αποφεύγοντας τα κρατικά δικαστήρια που θα εφαρμόζαν το εθνικό δίκαιο.

5.2.1 Συνεργατικός και αποκεντρωμένος νόμος (Collaborative and decentralized)

Θα μπορούσαμε να πούμε ότι ομοίως, η διαδικτυακή επίλυση διαφορών προέκυψε από την ίδια ανάγκη δημιουργίας αξιόπιστης διακυβέρνησης και ελαχιστοποίησης της έκθεσης σε διασυνοριακούς εμπορικούς κινδύνους. Είναι δύσκολο να εμπιστευτεί κάποιος στο διαδικτυακό περιβάλλον, ειδικά επειδή οι διασυνοριακές συναλλαγές ασχολούνται συχνά με θέματα ασφάλειας και απορρήτου προσωπικών πληροφοριών. Σε αυτό ακριβώς

το σημείο τα έξυπνα συμβόλαια αποδεικνύονται χρήσιμα και πρακτικά. Με έξυπνα συμβόλαια, η εμπιστοσύνη κατανέμεται «από την υποδομή στην υποδομή». Αυτή η νέα εφαρμογή θα μπορούσε να φέρει επανάσταση στην ιδιωτική διακυβέρνηση, καθιστώντας την πλέον απαραίτητη να προσφέρει εμπιστοσύνη στις συμβατικές σχέσεις.

Η ιδέα του αποκεντρωμένου δικαίου μπορεί να εφαρμοστεί με επιτυχία σε σχέση με την αποκεντρωμένη επίλυση διαφορών. Ένας διαδικτυακός μηχανισμός επίλυσης διαφορών θα μπορούσε να αντικαταστήσει τον δικαστή ή την κριτική επιτροπή με χιλιάδες άτομα από όλο τον κόσμο, καθιστώντας τους διαιτητές, το λεγόμενο *crowdsourcing justice*. Αυτή η έννοια του «συνεργατικού δικαίου» είναι πιθανό να υλοποιηθεί, αλλά είναι σημαντικό να διευκρινιστεί ότι δεν πρέπει να εφαρμόζεται στο ποινικό δίκαιο, δεδομένου ότι τέτοια ευαίσθητα ζητήματα είναι καλύτερα να μην αποκεντρωθούν. Τα εμπλεκόμενα μέρη θα μπορούσαν να έχουν την ελευθερία να επιλέξουν τον αριθμό των ατόμων που θα αποφασίζουν για την επίλυση της διαφοράς, δυνατότητα που δεν είναι δυνατή μέχρι σήμερα, με εξαίρεση τη διαμεσολάβηση. Οι χρήστες μπορούν να επιλέξουν οι ίδιοι τον εφαρμοστέο νόμο που μπορεί να είναι ο νόμος άλλης δικαιοδοσίας, μπορούν ακόμη και να προσαρμόσουν έναν αριθμό διαφορετικών κωδικών ή να έχουν την ευκαιρία να γράψουν τον δικό τους νομικό κώδικα και να αποφασίσουν.

5.3 Περιβάλλον

Υπάρχουν ανησυχίες για τις περιβαλλοντικές πτυχές της λειτουργίας υποδομών υπολογιστών μεγάλης κλίμακας. Έχει αναφερθεί, για παράδειγμα, ότι η υπολογιστική ισχύς που απαιτείται για τη διατήρηση του δικτύου Bitcoin καταναλώνει τόση ενέργεια όσο χρησιμοποιείται από 159 από τις αναπτυσσόμενες χώρες του κόσμου [42]. Ενώ η βιομηχανία blockchain μεταβαίνει προς το παρόν σε λιγότερο απαιτητικές για ενέργεια λύσεις, η συνολική κατανάλωση ενέργειας όλων των ψηφιακών υποδομών σε όλο τον κόσμο θα αυξηθεί μόνο. Η υποδομή ΤΠΕ καταναλώνει ήδη το 10-15% της συνολικής παραγωγής ενέργειας. Η έρευνα προτείνει ότι τα κέντρα δεδομένων θα είναι ένας από τους μεγαλύτερους χρήστες της βιομηχανίας ενέργειας στον πλανήτη, φτάνοντας το 20% του συνόλου της διαθέσιμης ηλεκτρικής ενέργειας στον κόσμο έως το 2025. Η κύρια απαίτηση εδώ είναι επομένως να διασφαλιστεί ότι τυχόν εφαρμοσμένα κέντρα δεδομένων και υποδομές που βασίζονται σε έργα ESA θα λάβετε υπόψη και συμβάλλετε θετικά σε αυτό το ενεργειακό μέλλον (δηλ. εφαρμόζοντας ενεργειακά αποδοτικά βήματα επεξεργασίας ή βασιζόμενοι σε πράσινες και ανανεώσιμες πηγές ενέργειας).

5.4 Πρωτοβουλίες

Τον Οκτώβριο του 2018 το Ευρωπαϊκό Κοινοβούλιο εξέδωσε ψήφισμα σχετικά με τις «Κατανεμημένες τεχνολογίες καθολικών και μπλοκ: οικοδόμηση εμπιστοσύνης με διαμεσολάβηση» για την ενίσχυση του κανονισμού της ΕΕ σε αυτόν τον τομέα. Τα στοιχεία αυτού του εγγράφου έχουν ως στόχο την επίλυση των προκλήσεων της νομικής προστασίας και της ανταγωνιστικότητας που σχετίζονται με τη χρήση κατανεμημένων καθολικών, την αρχή της τεχνολογικής ουδετερότητας και τον θεμιτό ανταγωνισμό μεταξύ των παικτών. Επισημαίνει επίσης διάφορες χρήσεις DLTs στη χρηματοδότηση, συμπεριλαμβανομένων επιπτώσεων για το ηλεκτρονικό εμπόριο, την ενέργεια, την υγειονομική περιθαλψη, την εκπαίδευση και τις δημιουργικές βιομηχανίες (π.χ. για τη διαχείριση πνευματικών δικαιωμάτων ή διπλωμάτων ευρεσιτεχνίας), καθώς και στο δημόσιο τομέα (π.χ. ψηφιοποίηση και αποκεντρωμένη διαχείριση δημόσιες βάσεις δεδομένων, αδειοδότηση, πιστοποίηση κ.λπ.).

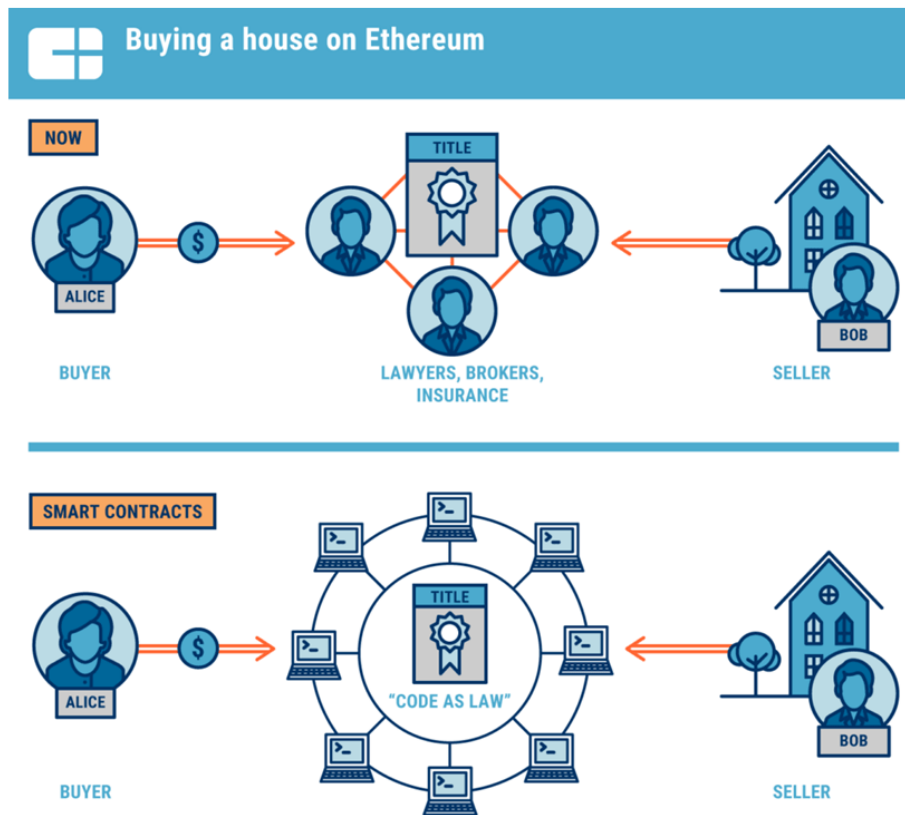
Επιπλέον, σημαντικά ζητήματα που σχετίζονται με το απόρρητο των δεδομένων στο blockchain, βρίσκονται όλο και περισσότερο στο επίκεντρο πολλών νομικών ζητημάτων, ιδίως ζητήματα που σχετίζονται με το «δικαίωμα να ξεχαστούν» έναντι της μη

αναστρέψιμης και αμετάβλητης δεδομένων σε ένα blockchain), και την προσέγγιση απορρήτου βάσει σχεδιασμού που απαιτείται από τον EU GDPR. Υπογραμμίζουν την ανάγκη ανάπτυξης περιπτώσεων χρήσης blockchain που συμμορφώνονται με το GDPR και το γεγονός ότι πολλές από τις απαιτήσεις του GDPR είναι ευκολότερες και απλούστερες στην ερμηνεία και την εφαρμογή σε ιδιωτικά, επιτρεπόμενα δίκτυα blockchain παρά σε δημόσια, χωρίς άδεια δίκτυα [43].

5.5 Υπογραφή Συμβολαίων

Όσον αφορά τα συμβαλλόμενα μέρη ενός έξυπνου συμβολαίου, αυτά πρέπει να είναι διακριτά και να υπογράψουν τη συμφωνία ή τουλάχιστον να υποδείξουν την αποδοχή της. Τα έξυπνα συμβόλαια χρησιμοποιούν τεχνικές όπως το PKI (Private Key Infrastructure) για αναγνώριση. Ως αποτέλεσμα, τα συμβόλαια μπορούν να υπογραφούν, να κρυπτογραφηθούν, να ενημερωθούν και να επικυρώσουν τα μέρη και να διασφαλιστεί η ακεραιότητα του κώδικα.

5.6 Ο κώδικας είναι νόμος



Σχήμα 19 <https://www.cbinsights.com/>. How Blockchain Technology Could Disrupt Real Estate

Ο όρος «κώδικας είναι νόμος» αναφέρεται στην ιδέα ότι, με την έλευση της ψηφιακής τεχνολογίας, ο κώδικας έχει σταδιακά καθιερωθεί ως ο κυρίαρχος τρόπος ρύθμισης της συμπεριφοράς των χρηστών του Διαδικτύου. Όπως δηλώνεται σαφώς από το «Code is Law» (1999) [44], ο κώδικας είναι τελικά η αρχιτεκτονική του Διαδικτύου και ως τέτοιος μπορεί να περιορίσει τις ενέργειες ενός ατόμου μέσω τεχνολογικών μέσων. Η

αρχιτεκτονική εφαρμογή σε διαδικτυακές πλατφόρμες εξαρτάται τελικά από τις συγκεκριμένες επιλογές των σχεδιαστών της πλατφόρμας, επιδιώκοντας να προωθήσει ή να αποτρέψει έναν συγκεκριμένο τύπο δράσεων. Οι παραδοσιακοί νομικοί κανόνες μπορούν να επιβληθούν μόνο εκ των υστέρων (δηλαδή μετά το γεγονός), η ρύθμιση με κώδικά μπορεί να επιβάλλει περιορισμούς σε μεμονωμένες ενέργειες με τρόπο που μπορεί να επιβληθεί εκ των προτέρων (δηλαδή ο κώδικας εμποδίζει τους χρήστες να παραβιάζουν τους τεχνικούς κανόνες, ακόμη και πριν ενεργήσουν).

Σε αντίθεση οι νομικούς κανόνες, γραμμένοι ως γενικοί κανόνες σε μια φυσική γλώσσα που είναι εγγενώς διφορούμενοι, οι τεχνικοί κανόνες μπορούν να εφαρμοστούν μόνο σε κώδικα, και ως εκ τούτου απαραίτητα βασίζονται σε επίσημους αλγόριθμους και μαθηματικά μοντέλα. Επομένως, η ρύθμιση με κώδικα είναι πάντα πιο συγκεκριμένη και λιγότερο ευέλικτη από τις νομικές διατάξεις.

Το πιο εμβληματικό παράδειγμα κώδικα που χρησιμοποιείται για την ενσωμάτωση και επιβολή υφιστάμενων νομικών διατάξεων μπορεί να παρατηρηθεί στο πλαίσιο της νομοθεσίας περί πνευματικών δικαιωμάτων όπως περιγράφεται παραπάνω. Το πλεονέκτημα των συστημάτων DRM είναι ότι διευκολύνουν τη διαδικασία επιβολής πνευματικών δικαιωμάτων επιτρέποντας στους κατόχους δικαιωμάτων να υπαγορεύουν τον τρόπο με τον οποίο οι χρήστες μπορούν να έχουν πρόσβαση ή να καταναλώνουν ένα έργο με τεχνολογικά μέσα, συμπεριλαμβανομένων των πληρωμών.

5.6.1 Blockchain και έξυπνα συμβόλαια

Η τεχνολογία Blockchain ενισχύει την τάση να χρησιμοποιούμε κώδικα (και όχι στο νόμο) για τη ρύθμιση μεμονωμένων ενεργειών και συναλλαγών. Το blockchain επιτρέπει έναν εντελώς νέο τύπο ρύθμισης μέσω κώδικα, ο οποίος σε συνδυασμό με έξυπνα συμβόλαια προωθεί επίσης έναν νέο τρόπο αντίληψης του νόμου. Τα έξυπνα συμβόλαια μπορούν να υποστηρίξουν την εκτέλεση συμβάσεων, μειώνοντας το κόστος διαπραγμάτευσης, επαλήθευσης και εκτέλεσης μετατρέποντας τις νομικές υποχρεώσεις σε συναλλαγές αυτό-εκτέλεσης. Όταν τα έξυπνα συμβόλαια εφαρμόζονται σε ένα blockchain, η εκτέλεση τους δεν πραγματοποιείται σε έναν κεντρικό διακομιστή, αλλά περισσότερο κατανέμεται στο δίκτυο των κόμβων. Τα έξυπνα συμβόλαια που βασίζονται σε Blockchain είναι επομένως πιο εξελιγμένα από τα παραδοσιακά μέσα τεχνολογικής ρύθμισης, δεδομένου ότι χαρακτηρίζονται ως κώδικες λογισμικού υπολογιστών που είναι ανεξάρτητα καθώς δεν εξαρτώνται από κανένα συγκεκριμένο τρίτο μέρος και αυτόνομα καθώς δεν μπορεί να χειραγωγηθεί- αλλοιωθεί από κανέναν [45]. Τα έξυπνα συμβόλαια μπορούν να αλληλοεπιδράσουν τόσο με τον άνθρωπο όσο και με άλλα έξυπνα συμβόλαια εντός του ίδιου οικοσυστήματος blockchain, μετατρέποντάς το σε έναν αυτοδιοικούμενο οργανισμό (μια οντότητα που περιλαμβάνει πολλά άτομα με συγκεκριμένο στόχο, όχι νομικά εγγεγραμμένο οργανισμό.) Που ελέγχεται αποκλειστικά και μόνο από ένα άφθαρτο σύνολο κανόνων, που εφαρμόζονται με τη μορφή έξυπνης σύμβασης.

Αυτό που κάνει το blockchain διαφορετικό από DRM συστήματα άλλων αρχιτεκτονικών είναι ότι τα έξυπνα συμβόλαια προορίζονται πραγματικά να αντικαταστήσουν τις νομικές συμβάσεις. Δεν θεωρούνται πλέον απλοί μηχανισμοί υποστήριξης ή επιβολής των υφιστάμενων νομικών κανόνων, αλλά ο κώδικας τους προορίζεται να έχει ως πρωταρχική λειτουργία το αποτέλεσμα του νόμου. Συνεπώς, καθώς όλο και περισσότερες συμβατικές διατάξεις εφαρμόζονται με τη μορφή έξυπνου συμβολαίου (σε αντίθεση με μια νομική σύμβαση), το blockchain αποκτά προοδευτικά την κατάσταση μιας «ρυθμιστικής τεχνολογίας», δηλαδή μιας τεχνολογίας που μπορεί να χρησιμοποιηθεί τόσο για τον καθορισμό όσο και για την ενσωμάτωση νομικών ή συμβατικών διατάξεων σε κώδικα, και για την επιβολή τους ανεξάρτητα από το εάν υπάρχει ή όχι υφιστάμενος νομικός κανόνας.

5.7 Περιορισμοί

Οι νόμοι και διατάξεις δεν μπορούν να καθοριστούν ολοκληρωτικά με τεχνολογικά μέσα, μιας και η τεχνολογία δεν μπορεί να αντικαταστήσει την δημοκρατική επιχειρηματολογία που ενέχεται αποκλειστικά στη νομική διαδικασία. Το νομικό οικοσύστημα ενσωματώνει μια σειρά από κανόνες και διαδικασίες που συλλογικά η κοινωνία έχει συμφωνήσει να τηρεί. Οι κανόνες αυτοί συλλογικά καθορίζουν και προστατεύουν τα δικαιώματα τις ελευθερίες και τις υποχρεώσεις των ατόμων της κοινωνίας και είναι εξίσου δεσμευτικές απέναντι τους (στην ιδανική μορφή της δημοκρατίας). Το νομικό σύστημα διασφαλίζει την ύπαρξη ενός δημόσιου, διαφανούς και ρητού συνόλου καθολικών κανόνων, του οποίου η νομιμότητα μπορεί εύκολα να τεθεί υπό αμφισβήτηση. Εν αντίθεσιν οι τεχνικοί κανόνες μπορούν να επιβληθούν μονομερώς από κατασκευαστές λογισμικού και παραγωγούς συσκευών, χωρίς να ακολουθήσουν με την δημοκρατική διαδικασία. Επιπλέον ο κανονισμός λειτουργίας (regulation) μέσω κώδικα εκπονείται κυρίως από ιδιωτικούς φορείς, οι οποίοι ενσωματώνουν ένα σύνολο αυθαίρετων κανόνων σε τεχνικά συστήματα, χωρίς καμία δημόσια συζήτηση και συχνά χωρίς να δίνουν την ευκαιρία στους χρήστες' να θέσουν υπό αμφισβήτηση αυτούς τους κανόνες.

Τα έξυπνα συμβόλαια έχουν και αυτά τους περιορισμούς τους που προκύπτουν από θέματα επιβολής, υιοθέτησης, ευελιξίας και ευθύνης (enforcement, adoption, flexibility, liability). Αναφορικά στην επιβολή και υιοθέτηση, αυτή τη στιγμή κάποια εμπλεκόμενα μέρη θα επιλέξουν να δομήσουν σύνθετες εμπορικές συναλλαγές μέσω τέτοιων συμβολαίων. Αντίθετα ανακύπτουν ζητήματα αναφορικά στην ευελιξία και ευθύνη. Αναφορικά στην ευελιξία το πρόβλημα έγκειται στο ότι συνήθως τα εμπλεκόμενα μέρη αποφεύγουν να συμφωνούν σε δεσμευτικές- άκαμπτες συμβάσεις μιας και μελλοντικά μπορεί να τους δεσμεύουν σε υποχρεώσεις που δεν μπορούν να εκπληρώσουν. Γι' αυτό και συνήθως ασκούνται επαναδιαπραγματεύσεις μεταξύ των μερών όταν προκύπτει μια απρόοπτη κατάσταση. Τα έξυπνα συμβόλαια δεν παρέχουν αυτή τη δυνατότητα και δεν παρέχουν λύση σε απρόβλεπτες καταστάσεις. Όμως, το πιο περίπλοκο και ευαίσθητο θέμα είναι αυτό που σχετίζεται με την ευθύνη. Η αρχή λειτουργίας των έξυπνων συμβολαίων είναι πως τα μέρη συμφωνούν και δεσμεύονται στον τρόπο συναλλαγής μεταξύ τους χωρίς όμως να απαιτείται επικύρωση από εξωτερικά τρίτα μέρη ή μεσολαβητές. Στην περίπτωση όμως απρόβλεπτων, μη προδιαγεγραμμένων καταστάσεων όπως αναφέρθηκε και παραπάνω, ποιος φέρει την ευθύνη για το αποτέλεσμα ή την επαναδιαπραγμάτευση;

Τέλος ίσως το πιο βασικό εμπόδιο αφορά στο ότι πολλοί από τους υφιστάμενους νόμους και κανονισμούς λειτουργίας προορίζονται να είναι αρκετά γενικοί ώστε να εφαρμόζονται σε ποικίλες διαφορετικές καταστάσεων, ορισμένες από τις οποίες δεν θα μπορούσαν να είχαν προβλεφθεί κατά τη σύνταξη τους. Στην πραγματικότητα για να είναι βιώσιμοι με την πάροδο του χρόνου, οι νομικοί κανόνες πρέπει να είναι εξαιρετικά γενικοί. Πρέπει να σχεδιάζονται σε ένα υψηλότερο, αφαιρετικό επίπεδο έτσι ώστε να παρέχουν αγνωστοκρατία στις ιδιαιτερότητες μιας υπόθεσης. Πρέπει να είναι αρκετά γενικές ώστε να μπορούν να καλύπτουν νέες και απρόβλεπτες καταστάσεις, οι οποίες στην πραγματικότητα είναι διαφορετικές από προηγούμενες περιπτώσεις, αλλά οι οποίες είναι πρακτικά, αξιακά ή ιδεολογικά ίδιες.

6 Συμπεράσματα

Μετά την αρχική επιτυχία τους στον τομέα των κρυπτονομισμάτων, το blockchain και τα DLT έχουν αναδυθεί ως τεχνολογίες γενικού σκοπού με τη δυνατότητα να μεταμορφώσουν σε άλλους εμπορικούς τομείς και μοντέλα. Στη παρούσα ανάλυση παραθέτουμε το τεχνικό, οικονομικό και ρυθμιστικό πλαίσιο που εφαρμόζεται στην τεχνολογία blockchain. Αναλύουμε τα επιμέρους τεχνικά αντικείμενα της τεχνολογίας (συναλλαγές, έξυπνα συμβόλαια, ασφάλεια, ωριμότητα κλπ.). Παραθέτουμε μοντέλα λειτουργίας και κινδύνους (περιβάλλον, προσωπικά δεδομένα κλπ.). Αν και οι τεχνολογίες που αναλύονται βρίσκονται ακόμη σε αρχικό στάδιο ανάπτυξης, η ταχεία διάδοσή τους ανεξαρτήτως πεδίου εφαρμογής, υποδηλώνει ότι ενδέχεται να έχουν μετασχηματιστική επίδραση στα υπάρχοντα συστήματα μεσοπρόθεσμα έως μακροπρόθεσμα. Στην υφιστάμενη κατάστασή τους επηρεάζουν ήδη τις εταιρικές διεργασίες που αφορούν σε ανταλλαγή δεδομένων από επιχείρηση σε επιχείρηση ή από επιχείρηση σε κυβερνητικές δομές, και την ηλεκτρονική διακυβέρνηση γενικότερα. Το blockchain και τα DLTs θα διαδραματίσουν πρωταγωνιστικό ρόλο στην ενθάρρυνση της κατανομημένης αποθήκευσης, ανταλλαγής δεδομένων και συναλλαγών.

Ο απώτερος στόχος του ψηφιακού πολιτισμού είναι η προώθηση της καινοτομίας και της δημιουργικότητας, παρέχοντας προστασία σε δικαιώματα πνευματικής ιδιοκτησίας. Η έμπνευση ενός όμορφου ή χρήσιμου έργου, περιχαρακώνεται νομικά, παρέχοντας δικαιώματα και οφέλη στους δημιουργούς, επιτρέποντάς τους να προσφέρουν στην ανθρωπότητα κάτι νέο ή καλύτερο.

Σήμερα η τεχνολογία Blockchain υπόσχεται να ξεπεράσει ή τουλάχιστον να ελαχιστοποιήσει αυτές τις προκλήσεις σε κάποιο βαθμό. Το Blockchain θα μπορούσε να χρησιμοποιηθεί ως ενοποιημένη βάση δεδομένων που επιτρέπει σε οποιονδήποτε να προσεγγίσει τις αμετάβλητες, αξιόπιστες πληροφορίες που είναι αποθηκευμένες εκεί. Ωστόσο, παρά το γεγονός ότι η τεχνολογία Blockchain παρέχει σημαντικά τεχνικά πλεονεκτήματα, από νομική άποψη δεν είναι τόσο σαφές. Πρέπει να καταβληθούν σοβαρές προσπάθειες σε νομικά και κανονιστικά θέματα για την προώθηση της καινοτομίας και ταυτόχρονα, την αποτροπή της χρήσης της για τη διευκόλυνση παράνομων δραστηριοτήτων. Το ισχύον νομικό σύστημα πρέπει να αναθεωρηθεί και να προσαρμοστεί προκειμένου να ενσωματωθεί αυτή η νέα τεχνολογία ώστε να επωφεληθούμε από τα πλεονεκτήματά της. Μιας και τα περισσότερα Blockchain συστήματα είναι ιδιωτικά ή μερικώς ιδιωτικά, θα χρειαστεί ένα είδος ρυθμιστικού συστήματος ώστε να διασφαλιστεί ότι η λειτουργία του ευθυγραμμίζεται με το δημόσιο συμφέρον. Τέλος, θα πρέπει να ενθαρρύνονται οι κανόνες για τον καθορισμό του πως θα λειτουργούν διεθνώς και διακρατικά αυτά τα συστήματα.

Η τεχνολογία παρέχει οικονομικές λύσεις στους δικαιούχους ΠΙ, ένα χαρακτηριστικό πλεονέκτημα το οποίο θα προσελκύσει νεοσύστατες επιχειρήσεις που θέλουν να προστατεύσουν τη ΠΙ τους. Η ολιστική αφομοίωση όμως της τεχνολογίας εξαρτάται από την στάση των υφιστάμενων υπηρεσιών διαχείρισης ΠΙ (όπως οι CIPO, WIPO και WTO). Αν ένα σύστημα βασισμένο σε blockchain τοποθετηθεί στην αγορά ως αντικαταστάτης των δικηγορικών εταιρειών και των υπηρεσιών ΠΙ, υπάρχει ρίσκο οι κάτοχοι των δικαιωμάτων να αποσιωπηθούν έναντι αυτών των υπηρεσιών αν οι εξελίξεις είναι αρνητικές απέναντί τους στις παραπάνω υπηρεσίες.

Η τεχνολογία περιγράφεται και ως αμετάβλητη, πράγμα που σημαίνει ότι οι πληροφορίες που είναι αποθηκευμένες στο blockchain δεν μπορούν να αλλοιωθούν. Ωστόσο, επειδή οι περισσότερες τεχνολογίες blockchain βρίσκονται ακόμη σε στάδιο ανάπτυξης, δεν είναι εντελώς απρόσβλητες από κακόβουλες ή ανεπιθύμητες παρεμβολές. Για παράδειγμα, το Διεθνές Εμπορικό Δικαστήριο της Σιγκαπούρης βρήκε έναν φορέα εκμετάλλευσης κρυπτονομισμάτων κατά παράβαση συμβολαίου για την πραγματοποίηση αλλαγών σε μια συναλλαγή που έγινε σε μια πλατφόρμα blockchain. Το περιστατικό έχει

δυναμικά σημαντικές επιπτώσεις για το εμπόριο και τη νομοθεσία, συμπεριλαμβανομένης τη ΠΙ Εάν τα αρχεία συναλλαγών ΠΙ μπορούν να τροποποιηθούν, η επίδραση σε προστιθέμενες αξίες και έσοδα μπορεί να είναι σημαντική.

6.1 Κατευθύνσεις μελλοντικής έρευνας

Με βάση την έως τώρα ανάλυση της παρούσας μελέτης, σε αυτή την ενότητα παρατίθεται πιθανές μελλοντικές ερευνητικές κατευθύνσεις για την εφαρμογή της τεχνολογίας blockchain στη διαχείριση της πνευματικής ιδιοκτησίας και δικαιωμάτων στον τομέα του ψηφιακού πολιτισμού ως ακολούθως.

Σύμφωνα με την υφιστάμενη γνώση και εφαρμογές το blockchain δεν μπορεί να χειριστεί ολιστικά τα θέματα δικαιωμάτων πνευματικής ιδιοκτησίας. Παρ' όλο που μέσω της τεχνολογίας μπορεί να γίνει αποτελεσματικά η αυθεντικοποίηση των πνευματικών-πολιτισμικών αγαθών, δεν υπάρχει ακόμη η κατάλληλη υποδομή για την αποτροπή της παράνομης αναπαραγωγής ψηφιακών έργων καθολικά. Η παράνομη αναπαραγωγή θα μπορούσε να αντιμετωπιστεί, μέσω της τεχνολογίας, μόνο αν ήταν καθολική η αποδοχή της.

Η λειτουργία του μοντέλου blockchain προϋποθέτει τη δημιουργία κατακερματισμένων στιγμιότυπων των ψηφιακών αγαθών. Για την αποτελεσματική διαχείριση της ιδιοκτησίας, αυτά τα στιγμιότυπα θα πρέπει να ενσωματώνονται σε ένα blockchain που περιλαμβάνει μια συλλογή έργων (για παράδειγμα, ο κατάλογος μιας δισκογραφικής εταιρείας ή πιο φιλόδοξα μια αποθήκη όλων των ψηφιακών αρχείων σε ολόκληρο το Διαδίκτυο). Επιπλέον αυτή η συλλογή θα έπρεπε να εγκατασταθεί σε υποδομή στην οποία θα έχει αποκλειστικά πρόσβαση ο πάροχος της (ή οποίος φέρει την κατάλληλη άδεια).

Παρ' όλο που κάτι τέτοιο θεωρητικά είναι εφικτό (ήδη εταιρείες έχουν αναπτύξει πατέντες βασισμένες στο παραπάνω θεωρητικό μοντέλο), προϋποθέτει ριζική αναδιοργάνωση των υπερσυνδέσμων που βασίζονται στο Διαδίκτυο. Επίσης, είναι μάλλον απίθανο, όσο ακραία μέτρα και να εφαρμοστούν, το περιεχόμενο να μην κυκλοφορεί εκτός της παραπάνω υποδομής (εκτός του κοινού δικτύου διανομής). Ενώ τα έξυπνα συστήματα ιδιοκτησίας θα μπορούσαν να χρησιμοποιηθούν για την ασφάλεια ενός αυτοκινήτου ή της πόρτας ενός διαμερίσματος Airbnb σχετικά αποτελεσματικά, υπάρχουν ακόμα πάρα πολλοί τρόποι για την αναπαραγωγή και την κυκλοφορία ψηφιακού περιεχομένου για να είναι εφαρμόσιμο το μοντέλο στον ψηφιακό πολιτισμό προς το παρόν.

Η τεχνολογία Blockchain υπάρχει για λιγότερο από μια δεκαετία και μπορεί να θεωρηθεί ότι βρίσκεται ακόμη στα σπάργανα. Ωστόσο, μπορούμε ήδη να προβλέψουμε ότι η τεχνολογία θα αντιμετωπίσει διάφορες προκλήσεις από τουλάχιστον τέσσερις διαφορετικές πτυχές της. Πιο συγκεκριμένα

- τεχνική,
- Εμπορική / επιχειρησιακή,
- συμπεριφορική / εκπαιδευτική και
- νομική / κανονιστική

Βιβλιογραφία

- [1] V. Gupta, «A Brief History of Blockchain,» 2017. [Ηλεκτρονικό]. Available: <https://hbr.org/2017/02/a-brief-history-of-blockchain>. [Πρόσβαση june 2017].
- [2] G. Greenspan, *Smart Contracts: The Good, the Bad and the Lazy*, 2016.
- [3] N. Satoshi, *Bitcoin: a peer-to-peerelectronic cash system*, 2009.
- [4] W. F. Yuan Yong, *Current Development Status and Prospects of Blockchain*, 2016.
- [5] B. Balázs, D. Gervais και J. P. Quintais, «Blockchain and IP: Crystal Ball-gazing or Real Opportunity?»,» *PLC Maganize*, p. 39–44, 2017.
- [6] J. Goldenfein και D. Hunter, «Blockchains, Orphan Works, and the Public Domain,» *Columbia Journal of Law & the Arts.*, p. 41, 2017.
- [7] T. Lyons, L. Courcelas και K. Timsit, «Blockchain for Government and Public Services,» σε *European Union Blockchain Observatory and Forum*, 2018.
- [8] A. K. Maitha και S. Khaled, «ESTABLISHING A SECURITY CONTROL FRAMEWORK FOR B LOCKCHAIN TECHNOLOGY,» 2021.
- [9] A. Baliga, *Understanding blockchain consensus models*, τόμ. 4, 2017, p. 1–14.
- [10] P. Sunny, K. Avinash και P. Vinod, *Survey on Private Blockchain Consensus*, 2019.
- [11] N. Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*,, 2008.
- [12] «Topic: Proof of stake instead of proof of work,» *Bitcoin Forum*, 2011.
- [13] R. Echevarria, «The second coming of blockchain,» *linkedin*, 2017.
- [14] J. Nijse και A. Litchfield, «A Taxonomy of Blockchain Consensus Methods,» 2020.
- [15] M. Sabt, M. Achemlal και A. Bouabdallah, *Trusted execution environment: what it is, and what it is not*, Helsinki, 2015, pp. 57-64.
- [16] M. Milutinovic, W. He, H. Wu και M. S. Kanwal, *Proof of luck: an efficient Blockchain consensus protocol*, New York, 2016.
- [17] G. Ateniese, I. Bonacina, A. Faonio και N. Galesi, «Proofs of Space: When Space Is of the Essence,» 2014, pp. 538- 557.
- [18] P. Sunoo, P. Krzysztof, A. Joël, F. Georg και G. Peter, «Spacecoin : A Cryptocurrency Based on Proofs of Space,» *IACR Cryptol. ePrint Arch*, 2015.
- [19] S. Gauld, v. A. Franz και S. R., «The Burst Dymaxion An Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles,» *CryptoGuru PoC SIG*, 2017.
- [20] N. Giang-Truong και K. Kyungbaek, «A Survey about Consensus Algorithms,» *Journal of Information Processing Systems*, 2018.
- [21] L. Lamport, R. Shostak και M. Pease, *The Byzantine generals problem* Pease ACM Transactions on Programming Languages and Systems, τόμ. 4, 1982, pp. 382-401.
- [22] R. Bhuvana και P. S. Aithal, «Blockchain Based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric,» *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, 2020.

- [23] M. Castro και B. Lisko, Practical Byzantine fault tolerance, New Orleans, LA, 1999, pp. 173-186.
- [24] R. Brown, «A Simple Model for Smart Contracts,» 2015. [Ηλεκτρονικό]. Available: <https://gandal.me/2015/02/10/a-simple-model-for-smart-contracts/>.
- [25] M. Tree, «Protocols for Public Key Cryptosystems,» 1980.
- [26] S. Haber και S. W. Scott, «How to Time-Stamp a Digital Document Advances in Cryptology—CRYPTO '90 Proceedings 3, 2,» *Journal of Cryptology*, τόμ. 3, p. 99-111., 1990.
- [27] A. Narayanan και J. Clark, Bitcoin's Academic Pedigree, τόμ. 5, 2017.
- [28] ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3028/2002. Για την προστασία των Αρχαιοτήτων και εν γένει της Πολιτιστικής Κληρονομιάς., ΦΕΚ Α-153/28-6-2002, 2002.
- [29] Y. Benkler, «The wealth of networks: How social production transforms markets and freedom.,» 2006.
- [30] «Berne Convention for the Protection of Literary and Artistic,» 1886.
- [31] M. S. Van Houweling, «Author Autonomy and Atomism in Copyright Law,» σε *Virginia Law*, Virginia, 2010.
- [32] I. Calboli και E. Lee, Research Handbook on Intellectual Property Exhaustion and Parallel Imports, Edward Elgar, 2016, p. 85-105.
- [33] B. Bodó, D. G. Pedro και Q. João, Blockchain and smart contracts: the missing link in copyright licensing?, τόμ. 26, 2018.
- [34] S. Engels και J. B. Nordemann, «The Portability Regulation,» *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018.
- [35] P. Aufderheide, P. Jaszi και T. Milosevic, «Copyright, Permissions, and Fair Use among Visual Artists and the Academic and Museum Visual Arts Communities,» Mellon, Foundation Andrew W., 2014.
- [36] S. Hall, J. Evans και S. Nixon, Representation, 1997.
- [37] G. W. Clough, Best of Both Worlds Museums, Libraries, and Archives in a Digital Age, 2013.
- [38] China IPR SME Helpdesk, «IPR Protection for AI Technology & Application of Blockchain in China,» Publications Office of the European Union, Luxembourg, 2019.
- [39] «<https://www.theguardian.com/technology/2009/jul/17/amazon-kindle-1984>».
- [40] «https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html».
- [41] B. Gipp, N. Meuschke, J. Beel και C. Breiteringer, «Using the Blockchain of Cryptocurrencies for Timestamping Digital Cultural Heritage.,» Bulletin of IEEE Technical Committee on Digital Libraries (TCDL, 2017.
- [42] M. Bernard, «The 5 Big Problems With Blockchain Everyone Should Be Aware Of,» *Forbes*, 2018.
- [43] T. Lyons και I. Courcelas, «Thematic Report on Blockchain and the GDPR,» EU Blockchain Observatory, 2018.
- [44] L. Lawrence, Code and Other Laws of Cyberspace, Basic Books, 1999.

- [45] W. Aaron και D. F. Primavera, «Decentralized Blockchain Technology and the Rise of Lex Cryptographia,» 2015.
- [46] Asselot και Pascal, «In a Nutshell: Blockchain and IP».
- [47] Gartner Inc, «Gartner Identifies Five Emerging Technology Trends That Will Blur the Lines Between Human and Machine,» STAMFORD, 2018.