ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

# ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νικόλαος Κ. Φραγκούλης

# «Η τεχνολογία Blockchain στην υπηρεσία της εκπαίδευσης, της έρευνας και των πνευματικών δικαιωμάτων»

**Επιβλέπων**: Συμεών Παπαβασιλείου,

Καθηγητής Ε.Μ.Π.

Αθήνα,……. 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

# ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Νικόλαος Κ. Φραγκούλης

# «Η τεχνολογία Blockchain στην υπηρεσία της εκπαίδευσης, της έρευνας και των πνευματικών δικαιωμάτων»

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ..... ..... 2018

| ..... | ..... | ..... |
|---|---|---|
| Συμεών Παπαβασιλείου | Γεώργιος Ματσόπουλος | Ιωάννα Ρουσσάκη |
| Καθηγητής Ε.Μ.Π. | Αν. Καθηγητής Ε.Μ.Π. | Επίκουρη Καθηγήτρια Ε.Μ.Π |

Αθήνα , ..... 2018

.....

Νικόλαος Κ. Φραγκούλης

# ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος "Τεχνο-οικονομικά Συστήματα" της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου το ακαδημαϊκό έτος 2017-2018.

Αντικείμενο της διπλωματικής εργασίας είναι η μελέτη της αποκεντρωμένης τεχνολογίας Blockchain, η οποία γίνεται ολοένα και πιο δημοφιλής μέσα από τον χώρο των κρυπτονομισμάτων βρίσκοντας ολοένα και περισσότερες εφαρμογές σε όλους τους τομείς του επιχειρηματικού κόσμου αλλά και όχι μόνο.

Υπεύθυνος κατά την εκπόνηση της διπλωματικής ήταν ο Καθηγητής κ. Συμεών Παπαβασιλείου, στον οποίο οφείλω ιδιαίτερες ευχαριστίες για την ανάθεση αυτής και τη δυνατότητα που μου δόθηκε να ασχοληθώ με αυτό το ενδιαφέρον θέμα.

Θα ήθελα επίσης να ευχαριστήσω θερμά τους Υπ. Διδάκτορες Μάριο Αυγέρη και Παπαδάκη Κώστα, για την πολύτιμη υποστήριξη και την συνεχή καθοδήγηση που μου παρείχαν κατά την εκπόνησή της.

Τέλος, θα ήθελα να εκφράσω την απεριόριστη ευγνωμοσύνη μου στην οικογένειά μου, η οποία καθ' όλη τη διάρκεια των σπουδών μου με έχει στηρίξει τόσο ηθικά όσο και οικονομικά και με έχει βοηθήσει να επιτύχω τους στόχους μου.

Αθήνα, Οκτώβριος 2018

Νικόλαος Φραγκούλης

# ΠΕΡΙΛΗΨΗ

Στη σημερινή εποχή των συνεχών συναλλαγών είναι απαραίτητη η διαφύλαξη της αξιοπιστίας από τις εκάστοτε συναλλασσόμενες πλευρές. Η αξιοπιστία αυτή απορρέει στην πλειοψηφία των περιπτώσεων, από μεσάζοντες διεθνώς αναγνωρισμένους, όπως μεγάλες κεντρικές τράπεζες, πολυεθνικές εταιρείες ή μεγάλους εκδοτικούς οίκους. Σε μια παραδοσιακή συναλλαγή, η εμπιστοσύνη πηγάζει από τη φήμη που ακολουθεί ένα αναγνωρισμένο ίδρυμα.

Στον τομέα αυτό έκανε την εμφάνιση της μια τεχνολογία, όχι τόσο καινούρια για τους γνώστες του αντικειμένου, η οποία όμως έφερε ραγδαίες αλλαγές στην δόμηση της εμπιστοσύνης, που βασίζεται στη συναίνεση των χρηστών που ανήκουν σε ένα δίκτυο, το Blockchain. Η τεχνολογία αυτή εισάγει την έννοια ενός αποκεντρωμένου μοντέλου το οποίο, βασίζεται στην συμφωνία των χρηστών του δικτύου, ως προς μια συναλλαγή ή ένα σύνολο συναλλαγών, έτσι ώστε κανένα άτομο ή οργάνωση να μην υπονομεύσει τους κανόνες που έχουν θεσπιστεί.

Η τεχνολογία Blockchain έγινε γνωστή στο ευρύ κοινό με την εκτόξευση της τεχνολογίας της οικονομίας(Financial Technology) και των κρυπτονομισμάτων, ιδιαίτερα μέσω του Bitcoin. Παρά το γεγονός ότι η γνωστοποίηση της τεχνολογίας οφείλεται στις προαναφερθείσες εφαρμογές, υφίσταται ακόμα ένα πλήθος τομέων που μπορούν να επωφεληθούν από την υιοθέτησή της. Η εφοδιαστική αλυσίδα, το Διαδίκτυο των Πραγμάτων, η ασφάλιση και ο τραπεζικός κλάδος έχουν κάνει ήδη τα πρώτα βήματα στην ένταξη της εν λόγω τεχνολογίας, μετασχηματίζοντας το επιχειρηματικό τους μοντέλο με σκοπό να βελτιστοποιήσουν την παραγωγική τους διαδικασία και την αποδοτικότητά τους. Ο πολύπλευρος χαρακτήρας αυτής της τεχνολογίας αποτέλεσε εφαλτήριο για την δημιουργία παράγωγων τεχνολογιών όπως αυτή του Ethereum και των έξυπνων συμβολαίων.

Η πρακτική εφαρμογή αυτής της τεχνολογίας δίνει τη δυνατότητα στον σύγχρονο άνθρωπο όχι μόνο να τροποποιήσει ριζικά τομείς της καθημερινότητάς του όπως η εκπαίδευση, αλλά και να διαφυλάξει τα πνευματικά δικαιώματα που απορρέουν από την ερευνητική διαδικασία. Εν κατακλείδι, η εξασφάλιση της αυθεντικότητας και της μοναδικότητας των δεδομένων θα αυξήσει την εγκυρότητα των ερευνητικών αποτελεσμάτων και κατ' επέκταση την αξιοπιστία της εκπαιδευτικής διαδικασίας.

Σκοπός της παρούσας διπλωματικής εργασίας είναι η διερεύνηση των τεχνολογιών Blockchain, η ανάλυση του τρόπου με τον οποίο λειτουργούν καθώς και των δυνητικών εφαρμογών του στην έρευνα, στην μάθηση και στη διαφύλαξη των πνευματικών δικαιωμάτων. Πιο συγκεκριμένα, αναλύθηκαν χρόνια δυσεπίλυτα προβλήματα των ανωτέρω τομέων και προτάθηκαν πιθανές λύσεις με τη χρήση του Blockchain.

Λέξεις Κλειδιά

Blockchain, Ethereum, Έξυπνα Συμβόλαια, Πνευματική Ιδιοκτησία, Έρευνα, Μάθηση

# ABSTRACT

In the modern era of continuous transactions, the safeguarding of both partners' credibility is considered to be necessary. In most cases this credibility stems from internationally recognized intermediaries, such as large central banks, multinational companies or large publishing houses. In a transaction following the traditional patterns, the trust derives from the reputation of an esteemed institution.

In this field a new technology appeared, that brought radical changes to the way trust is formed, based on the consensus between users forming a network, called a Blockchain. The Blockchain technology introduced the concept of a decentralized model, which is based on an agreement between the users of a network, concerning one or more transactions, so that the established rules can not be undermined neither by a person nor an organization.

The blockchain technology became widely known with the rise of Financial Technology and cryptocurrency, specifically Bitcoin Apart from these widely known applications, there is a range of other fields that can take advantage of this technology. The supply chain, the Internet of Things, the insurance and banking sectors have already taken the first steps in incorporating Blockchain technology, by transforming their business models, to optimize the production processes and their efficiency. The versatile character of Blockchain technology has given birth to several other forms of innovative technologies, such as Ethereum and smart contracts.

The practical application of this technology provides the ability not only to radically change aspects of daily life, such as education, but also to protect intellectual property rights, products of research processes. As a result, ensuring the authenticity and uniqueness of data will increase the validity of research results and, thus, the credibility of the educational process.

The purpose of this Master Thesis is the study of the Blockchain Technology, the analysis of the way this technology functions and all the possible applications in research, learning processes and protection of intellectual property rights. Specifically, chronic problems of the aforementioned sectors were analyzed and several suggestions were made, all using the main principles of the Blockchain Technology



# KEYWORDS

Blockchain, Ethereum, Smart Contracts, Intellectual Property, Research, Learning

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

# 1 ΕΙΣΑΓΩΓΗ

Καθώς η ζωή κινείται με γοργούς ρυθμούς προς το διαδίκτυο, μια από τις προκλήσεις που αντιμετωπίζουν οι χρήστες του ίντερνετ είναι η διεξαγωγή οικονομικών συναλλαγών σε ένα περιβάλλον όπου δεν μπορούν να γνωρίζουν ή να εμπιστεύονται το άλλο μέρος. Επίσης, η αλματώδης ανάπτυξη της πληροφορικής και της ψηφιοποίησης των δεδομένων συνέβαλε, μεταξύ άλλων στη δημιουργία κρυπτονομισμάτων. Συνεπώς, ορισμένα από αυτά τα θέματα εμπιστοσύνης μετριάστηκαν με την ανάπτυξη των κρυπτονομισμάτων όπως το Bitcoin.

Το Bitcoin είναι ένα αποκεντρωμένο νόμισμα, το οποίο εμφανίστηκε για πρώτη φορά το 2008 και το οποίο υπάρχει εξολοκλήρου ως "μοναδικές συμβολοσειρές από γράμματα και αριθμούς" [1]. Όλες οι συναλλαγές στην οικονομία του Bitcoin παρακολουθούνται από ένα "λογιστικό βιβλίο" που ονομάζεται Blockchain. Πολλαπλά αντίγραφα αυτού του βιβλίου υπάρχουν και συγκρίνονται συνεχώς μεταξύ τους, για να διασφαλιστεί ότι όλες οι συναλλαγές είναι νόμιμες και ότι έχουν καταγραφεί σωστά. Υπάρχουν και άλλα κρυπτονομίσματα όπως το Bitcoin, αλλά όλα χρησιμοποιούν ένα παρόμοιο λογισμικό Blockchain.

Παρόλο που τα κρυπτονομίσματα είναι ένα ενδιαφέρον και με πολλές δυνατότητες εξέλιξης αντικείμενο, η τεχνολογία στην οποία στηρίζονται, το Blockchain, έχει μετατραπεί σε ένα από τα πιο πολυσυζητημένα τεχνολογικά επιτεύγματα, με επενδύσεις δισεκατομμυρίων δολαρίων και μια ολόκληρη βιομηχανία να χτίζεται πάνω της. Οι χρήσεις τις συγκεκριμένης τεχνολογίας είναι πολλές, και κινούνται πέρα από την αγορά συναλλάγματος, καθώς συμπεριλαμβάνουν τη δημιουργία εγγράφων που είναι απαλλαγμένα από παραβιάσεις, κατανεμημένα δικαιώματα ιδιοκτησίας, καθολικά ιατρικά αρχεία κ.α.

Η Melanie Swan στο βιβλίο της με τίτλο "Blockchain, Blueprint for a New Economy" προβλέπει τρεις φάσεις υιοθέτησης της τεχνολογίας: Blockchain 1.0, 2.0 και 3.0. Ορίζει το Blockchain 1.0 ως την ηλεκτρονική φάση κρυπτονομισμάτων, εξετάζοντας το τρέχον σύστημα του Bitcoin. Η φάση αυτή ήδη βρίσκεται στο προσκήνιο, όπως αποδεικνύεται από τις χιλιάδες συναλλαγές Bitcoin που πραγματοποιούνται καθημερινά. Το Blockchain 2.0 έρχεται με γοργούς ρυθμούς στην επικαιρότητα και αναφέρεται σε συμβάσεις παρακολούθησης, στις καταχωρήσεις οικονομικών αρχείων και εγγραφών, δημόσιων αρχείων και κυριοτήτων ιδιοκτησίας στο Blockchain. Σύμφωνα με τη Swan το Blockchain 3.0 θα επεκταθεί στον τομέα της επιστήμης, της ιατρικής και της εκπαίδευσης. Προβλέπει ότι το Blockchain θα μεταφέρει πληροφορίες οι οποίες

θα έχουν κρυφθεί ή χειραγωγηθεί μεταξύ των ιδρυμάτων χρησιμοποιώντας παγκόσμια μητρώα και αποκεντρωμένα Blockchain. [2]

Τα οφέλη από την υιοθέτηση αυτής της τεχνολογίας είναι αναρίθμητα χάρη στην αρχιτεκτονική της. Το Blockchain είναι μια καινοτομία της οποίας οι αρχιτεκτονικές ιδιότητες προσφέρουν όλο και περισσότερες ουσιαστικές βάσεις στον ψηφιακό κόσμο, όπου υπάρχει διάθεση για τον καθορισμό υψηλότερων επιπέδων αυτονομίας και ανάθεσης. Αυτό περιλαμβάνει την αυξανόμενη χρήση των συναλλαγών από κινητό σε κινητό, τα ταχύτερα και ασφαλέστερα μοντέλα πληρωμών, την προέλευση δεδομένων των πελατών, τα μητρώα περιουσιακών στοιχείων, την ανίχνευση απάτης και την μείωση του κινδύνου από την έκθεση στο διαδίκτυο. [3]

# 2 ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

**Κόμβος(Node):** Ένα δίκτυο Blockchain διατηρείται από λογισμικό που τρέχει σε ένα έναν υπολογιστή που ονομάζεται κόμβος ή “peer”. Κάθε κόμβος συνδέεται με το δίκτυο Blockchain και μπορεί να υποβάλλει και να λαμβάνει συναλλαγές.

**Δίκτυο(Network):** Οι οργανισμοί και ενδεχομένως τα άτομα διατηρούν συστήματα υπολογιστών που ονομάζονται κόμβοι, οι οποίοι τρέχουν το λογισμικό Blockchain για να επικοινωνούν μεταξύ τους και να σχηματίζουν ένα δίκτυο Blockchain.

**Έξυπνα συμβόλαια ή συμβάσεις(Smart Contracts):** Οι συμβάσεις ή οι συναλλαγές που μετατρέπονται σε κώδικα για να εκτελεστεί σε Blockchain.

**Συναλλαγές(Transactions):** Οι χρήστες υποβάλλουν συναλλαγές στο δίκτυο αποστέλλοντας τις σε κόμβους του δικτύου, οι οποίοι στη συνέχεια τις διαδίδουν σε όλους τους άλλους κόμβους του δικτύου.

**Επικύρωση(Validation):** Οι κόμβοι λαμβάνουν, επεξεργάζονται και επικυρώνουν κρυπτογραφικά κάθε έγκυρη συναλλαγή ενώ απορρίπτουν τις μη έγκυρες συναλλαγές.

**Μπλοκ(Block):** Οι κόμβοι συγκεντρώνουν και ομαδοποιούν τις έγκυρες συναλλαγές σε μια δέσμη γνωστή και ως μπλοκ. Τα μπλοκ πρέπει να ακολουθούν ένα προκαθορισμένο σύνολο κανόνων για να είναι έγκυρα.

**Blockchain:** Κάθε νέο μπλοκ περιέχει μια αναφορά στο πιο πρόσφατο έγκυρο μπλοκ και τοποθετείται μετά από αυτό το μπλοκ στη βάση δεδομένων, σχηματίζοντας μια αλυσίδα των μπλοκ.

**Συναίνεση(Consensus):** Η διαδικασία με την οποία εξασφαλίζεται ότι κάθε κόμβος συμφωνεί σε ένα δίκτυο Blockchain.

**Κρυπτονόμισμα(Cryptocurrency):** Είναι ένα ψηφιακό νόμισμα το οποίο έχει αξία και έχει σχεδιαστεί για να λειτουργεί ως μέσο συναλλαγής. Βασίζεται στην κρυπτογραφία για να διασφαλιστεί ότι τα δεδομένα των συναλλαγών δεν μπορούν να αλλοιωθούν.

**Token:** Μπορεί να χαρακτηριστεί ως ένα ψηφιακό αγαθό ή ένα κλειδί, που πιστοποιεί με μονοσήμαντο τρόπο, ότι το πρόσωπο που το κατέχει είναι και ο ιδιοκτήτης μιας αξίας.

**Μητρώο(Ledger):** Είναι ένα ψηφιακό αρχείο καταγραφής δεδομένων για την αποθήκευση πληροφορίας.

**Εξόρυξη(Mining):** Είναι μια διαδικασία κατά την οποία επαληθεύονται οι συναλλαγές για διάφορες μορφές κρυπτονομισμάτων και προστίθενται στο μητρώο.

# 3 ΤΙ ΕΙΝΑΙ ΤΟ BLOCKCHAIN

Η τεχνολογία Blockchain είναι μια αποκεντρωμένη τεχνολογία δικτύων στην οποία τα δεδομένα καταγράφονται και διατηρούνται σε πολλαπλούς κόμβους(υπολογιστές συνδεδεμένους σε ένα δίκτυο) που είναι γεωγραφικά απομονωμένοι μεταξύ τους. Οφείλει το όνομα της στον τρόπο με τον οποίο αποθηκεύονται τα δεδομένα, σε πακέτα(Blocks), τα οποία είναι συνδεδεμένα μεταξύ τους σαν μια αλυσίδα(Chain). Πιο συγκεκριμένα, οι συναλλαγές, αφού ελεγχθούν με βάση τους κανόνες που έχουν προσυμφωνηθεί από τους συμμετέχοντες στο δίκτυο, τοποθετούνται με

χρονολογική σειρά σε ομάδες που ονομάζονται μπλοκ. Τα μπλοκ αυτά συνδέονται μεταξύ τους όπως μια αλυσίδα.

Πρόκειται για ένα είδος τεχνολογίας κατανεμημένου μητρώου(Distributed Ledger Technology-DLT) που έχει οριστεί ως μια "κατανεμημένη, κοινή, κρυπτογραφημένη βάση δεδομένων που χρησιμεύει ως μη αναστρέψιμη και άφθαρτη αποθήκη πληροφοριών" [4] η οποία διευκολύνει τη διαδικασία καταγραφής συναλλαγών και παρακολούθησης περιουσιακών στοιχείων σε ένα επιχειρηματικό δίκτυο. Ένα περιουσιακό στοιχείο μπορεί να είναι υλικό (ένα σπίτι, ένα αυτοκίνητο, μετρητά, γη) ή άυλο όπως η πνευματική ιδιοκτησία (διπλώματα ευρεσιτεχνίας, branding). Ουσιαστικά οτιδήποτε έχει αξία μπορεί να εντοπιστεί και να διακινηθεί σε ένα δίκτυο Blockchain, μειώνοντας το κόστος αλλά και τον κίνδυνο για όλους τους εμπλεκόμενους [5] [6] [7].

Τα πακέτα καταγράφουν και επικυρώνουν την ώρα και τη σειρά με την οποία πραγματοποιούνται οι συναλλαγές, οι οποίες στη συνέχεια καταγράφονται στο Blockchain μέσα σε ένα διακριτό δίκτυο το οποίο διέπεται από κανόνες που έχουν συμφωνηθεί από όλους τους συμμετέχοντες σε αυτό. Κάθε πακέτο περιέχει ένα ψηφιακό δακτυλικό αποτύπωμα ή μοναδικό αναγνωριστικό (hash), τη χρονική "σφραγίδα" των πρόσφατων έγκυρων συναλλαγών καθώς και το hash των προηγούμενων πακέτων. Το προηγούμενο αναγνωριστικό κάθε πακέτου συνδέει τα πακέτα μεταξύ τους και εμποδίζει οποιαδήποτε αλλαγή στα πακέτα είτε την εισαγωγή ενός πακέτου μεταξύ δύο ήδη υφιστάμενων. Με αυτό τον τρόπο κάθε επόμενο μπλοκ ενισχύει την επαλήθευση του προηγούμενου πακέτου και επομένως ολόκληρου του δικτύου

## 3.1 ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΝΕΜΗΜΕΝΟΥ ΜΗΤΡΩΟΥ

Η τεχνολογία κατανεμημένου μητρώου (Distributed Ledger Technology-DLT) αναφέρεται στην ικανότητα των χρηστών να αποθηκεύουν και να έχουν πρόσβαση σε πληροφορίες ή αρχεία που σχετίζονται με περιουσιακά στοιχεία ή εκμεταλλεύσεις σε μια κοινή βάση δεδομένων (π.χ. μητρώο-Ledger), ικανή να λειτουργήσει χωρίς κεντρικό σύστημα επικύρωσης βασιζόμενη στα δικά της πρότυπα ή διαδικασίες. [8]. Τα DLT συστήματα διαφέρουν από τα τυπικά λογιστικά βιβλία καθώς διατηρούνται από ένα κατανεμημένο δίκτυο συμμετεχόντων (γνωστοί ως κόμβοι) και όχι από μια κεντρική οντότητα όπως γίνεται

παραδοσιακά. Ένα άλλο χαρακτηριστικό της συγκεκριμένης τεχνολογίας είναι η χρήση της κρυπτογραφίας ως μέσου αποθήκευσης περιουσιακών στοιχείων και επικύρωσης συναλλαγών.

Τα κοινόχρηστα μητρώα είναι κατανεμημένα σε όλους τους συμμετέχοντες σε ένα δίκτυο, τα οποία είναι αμετάβλητα, περιέχουν όλες τις συναλλαγές του δικτύου και μπορούν να διαβαστούν από όλους. Με αυτό το κοινόχρηστο μητρώο, οι συναλλαγές καταγράφονται μία μόνο φορά, εξαλείφοντας την παραδοσιακή διπλότυπη καταγραφή των συναλλαγών. Ένα κοινόχρηστο μητρώο έχει τα ακόλουθα χαρακτηριστικά:

- Καταγράφει όλες τις συναλλαγές όλου του δικτύου, άρα είναι η μόνη πηγή αλήθειας.
- Μοιράζεται μεταξύ όλων των μελών του δικτύου, μέσω της αντιγραφής του κοινόχρηστου μητρώου.
- Είναι προσβάσιμα ανάλογα με τα δικαιώματα που έχει κάθε μέλος της αλυσίδας.

Η τεχνολογία κατανεμημένου μητρώου έχει πολλές εφαρμογές κυρίως στον κλάδο χρηματοπιστωτικών υπηρεσιών. Πιο συγκεκριμένα με τη χρήση αυτής της τεχνολογίας θα μπορούσε να δώσει στους χρήστες πρόσβαση στην κοινή βάση δεδομένων και εκείνοι με τη σειρά τους να εκκαθαρίζουν και να πραγματοποιούν συναλλαγές χωρίς τη ύπαρξη κάποιου μεσάζοντα. Δεδομένου ότι όλες οι πληροφορίες και τα αρχεία θα διανεμηθούν μεταξύ όλων των χρηστών, οι συναλλαγές που θα διεξάγονται μέσω DLT θα έχουν τη δυνατότητα να εκκαθαριστούν και να επικυρωθούν σχεδόν ακαριαία.

## 4 Ο ΔΗΜΙΟΥΡΓΟΣ

Η τεχνολογία Blockchain εμφανίστηκε για πρώτη φορά το 2008 μέσα από μια έρευνα που δημοσιεύτηκε με τίτλο “Bitcoin: A Peer-to-Peer Electronic Cash System” [9]. Ο υπογράφων αυτής της έρευνας χρησιμοποίησε το ψευδώνυμο Satoshi Nakamoto, ο οποίος μέχρι σήμερα παραμένει άγνωστος. Ο Nakamoto συνδυάζοντας αρκετές προγενέστερες εφευρέσεις και τεχνολογίες δημιούργησε για πρώτη φορά στην ιστορία ένα πλήρως αποκεντρωμένο σύστημα πληρωμών. Μέσα από αυτό το σύστημα μπορεί να μεταφερθεί αξία(Bitcoin) μεταξύ δύο άγνωστων ανθρώπων χωρίς να χρειάζεται καμία κεντρική αρχή να επικυρώσει τις συναλλαγές. [10] [7]

Πολλοί πιστεύουν ότι πίσω από αυτό το ψευδώνυμο βρίσκεται μια ομάδα ειδικών-χάκερ στην κρυπτογραφία και στην επιστήμη των υπολογιστών. Η υπόθεση αυτή απορρέει από την

υπηρεσία ανώνυμης αλληλογραφίας (Vistomail) που χρησιμοποίησαν στη δημοσίευση, καθώς και τον δωρεάν λογαριασμό ηλεκτρονικού ταχυδρομείου (gmx.com) από τον οποίο έστελναν email, όταν συνδεόταν μέσω Tor. Πιθανότατα, χρησιμοποίησαν το όνομα Satoshi το οποίο σημαίνει "σοφία" ή "λόγος" και Nakamoto για να υποδηλώσουν "Κεντρική πηγή" [11]. Η εξόρυξη του πρώτου Bitcoin πραγματοποιήθηκε το 2009 και ο ιδρυτής, έχει στην κατοχή του περίπου ένα εκατομμύριο Bitcoin, τα οποία τον Οκτώβριο του 2017 είχαν συνολική αξία 5.8 δισεκατομμύριο δολάρια [12].

Τον Ιούλιο του 2015, ένας νεαρός καναδός προγραμματιστής με το όνομα Vitalik Buterin δημιούργησε ένα άλλο κρυπτονόμισμα με την ονομασία Ether, το οποίο έλαβε την ίδια αποδοχή από τον κόσμο όπως έγινε και με το Bitcoin. Με αφορμή την εισαγωγή αυτών των κρυπτονομισμάτων ξεκίνησε μια μεγάλη "τεχνολογική επανάσταση" η οποία βασίζεται στη χρήση της τεχνολογίας Blockchain.

## 5 ΤΥΠΟΙ BLOCKCHAIN

Η "Λευκή Βίβλος" για το Bitcoin που δημοσιεύτηκε από τον Satoshi Nakamoto ήταν η αρχή για τη υιοθέτηση της τεχνολογίας Blockchain στον κόσμο της τεχνολογίας. Δεδομένου ότι το πρωτόκολλο του Bitcoin είναι ανοιχτού κώδικα, οποιοσδήποτε μπορεί να το διαχειριστεί, να τροποποιήσει τον κώδικά, και να ξεκινήσει τη δική του έκδοση των χρημάτων P2P.

Στην συνέχεια, προέκυψαν πολλά από τα λεγόμενα "altcoins", τα οποία προσπάθησαν να είναι καλύτερα, ταχύτερα ή πιο ανώνυμα από το Bitcoin. Σύντομα, ο κώδικας τροποποιήθηκε όχι μόνο για να δημιουργήσει καλύτερα κρυπτονομίσματα, αλλά ορισμένα έργα προσπάθησαν επίσης να αλλάξουν την ιδέα του Blockchain πέρα από την περίπτωση χρήσης για ανταλλαγή χρημάτων P2P.

Αναλύοντας την λειτουργία και τη σχεδίαση του Bitcoin, προέκυψε η ιδέα ότι το συγκεκριμένο είδος Blockchain, θα μπορούσε να χρησιμοποιηθεί για οποιαδήποτε συναλλαγή αξίας ή για οποιοδήποτε είδος συμφωνίας, όπως η P2P ασφάλιση, η εμπορία ενέργειας P2P, η κοινή χρήση P2P, κ.α. Τα Colored Coins και Mastercoin προσπάθησαν να λύσουν διάφορα προβλήματα με βάση το πρωτόκολλο Blockchain του Bitcoin.

Το έργο με το όνομα Ethereum, προσπάθησε να δημιουργήσει το δικό του Blockchain, με πολύ διαφορετικές ιδιότητες από το Bitcoin, αποσυνδέοντας το επίπεδο των έξυπνων συμβολαίων από το κεντρικό πρωτόκολλο του Blockchain, προσφέροντας ένα νέο ριζοσπαστικό τρόπο δημιουργίας ηλεκτρονικών αγορών και προγραμματιζόμενων συναλλαγών, γνωστών "Smart Contracts".

Ιδιωτικά ιδρύματα όπως οι τράπεζες, συνειδητοποίησαν ότι θα μπορούσαν να χρησιμοποιήσουν την βασική ιδέα του Blockchain ως τεχνολογία κατανεμημένου καθολικού(Distributed Ledger Technology-DLT) και να δημιουργήσουν ένα αδειοδοτημένο Blockchain(ιδιωτικό ή ομοσπονδιακό), όπου ο ελεγκτής εγκυρότητας είναι μέλος μιας κοινοπραξίας ή ξεχωριστών νομικών προσώπων του ίδιου οργανισμού.

Ένα δίκτυο blockchain μπορεί να δημιουργηθεί με την προϋπόθεση ότι για να διαβάσει κάποιος τις πληροφορίες των συναλλαγών ή να δημιουργήσει νέα μπλοκ θα πρέπει να έχει το κατάλληλα δικαιώματα - μια μοναδική ταυτότητα. Με αυτή τη δυνατότητα περιορισμού των δικαιωμάτων, οι επιχειρήσεις θα μπορούν να συμμορφωθούν ευκολότερα με διεθνή πρότυπα προστασίας προσωπικών δεδομένων, αλλά και ο τρόπος ελέγχου των δεδομένων που προσαρτώνται σε ένα blockchain να γίνεται αποτελεσματικότερα.

Ένας προγραμματιστής blockchain μπορεί να επιλέξει αν θα κάνει το σύστημα καταγραφής, διαθέσιμο για να το διαβάζει ο καθένας, όπως επίσης μπορεί να μην επιτρέψει σε κάποιους να γίνουν κόμβοι του δικτύου, εξυπηρετώντας την ασφάλεια του αλλά και την επαλήθευση των συναλλαγών που πραγματοποιούνται σε αυτό. Σε κάθε περίπτωση κάθε μέλος ενός blockchain διαθέτει ένα ψηφιακό πιστοποιητικό το οποίο παρέχει πληροφορίες πιστοποίησης, το οποίο είναι ανθεκτικό στην πλαστογράφηση και μπορεί να ταυτοποιηθεί επειδή εκδόθηκε από ένα αξιόπιστο οργανισμό.

Ο όρος Blockchain στο πλαίσιο του επιτρεπόμενου ιδιωτικού καθολικού είναι εξαιρετικά αμφιλεγόμενος και αμφισβητούμενος. Αυτός είναι ο λόγος για τον οποίο ο όρος κατανεμημένες τεχνολογίες καθολικού(DLT) εμφανίστηκε ως ένας πιο γενικός όρος. Λαμβάνοντας υπόψη τα ανωτέρω μπορούν να υπάρξουν τρεις διαφορετικές κατηγορίες Blockchain ανάλογα με:

- Αν το βιβλιάριο θα είναι κατανεμημένο
- Ποιοι χρήστες θα έχουν πρόσβαση σε αυτό
- Ποιοι χρήστες θα επαληθεύουν και θα καταχωρούν τις συναλλαγές δεδομένων στο βιβλιάριο.

## 5.1 PUBLIC BLOCKCHAINS

Πρόκειται για υπερσύγχρονα δημόσια πρωτόκολλα Blockchain που ασφαλίζονται από τα "cryptoeconomics"– ένα συνδυασμό από οικονομικά κίνητρα και την κρυπτογραφική επαλήθευση χρησιμοποιώντας μηχανισμούς και αλγόριθμους συναίνεσης όπως η απόδειξη εργασίας(Proof of Work - PoW) ή η απόδειξη συμμετοχής(Proof of Stake-PoS). Ακολουθούν μια γενική αρχή, σύμφωνα με την οποία, ο βαθμός στον οποίο κάποιος μπορεί να έχει επιρροή στη διαδικασία συναίνεσης είναι ανάλογη με την ποσότητα των οικονομικών πόρων που φέρει. Αυτά τα είδη Blockchain είναι ανοιχτού κώδικα, μη εξουσιοδοτημένα("not permissioned") και θεωρούνται πλήρως αποκεντρωμένα.

Οποιοσδήποτε μπορεί να συμμετάσχει χωρίς να λάβει κάποια άδεια, να κατεβάσει τον κώδικα και να ξεκινήσει την εκτέλεση ενός δημόσιου κόμβου σε ένα τοπικό υπολογιστικό σύστημα, επικυρώνοντας τις συναλλαγές στο δίκτυο, συμμετέχοντας έτσι στη διαδικασία της συναίνεσης· τη διαδικασία για τον προσδιορισμό των μπλοκ που θα προστεθούν στην αλυσίδα καθώς και της τρέχουσας κατάστασης της. Παράλληλα, οποιοσδήποτε στον κόσμο μπορεί να στείλει συναλλαγές μέσω του δικτύου και να περιμένει να τις δει να συμπεριλαμβάνονται στο Blockchain αν αυτές είναι έγκυρες. Επίσης, καθένας μπορεί να δει τις συναλλαγές που πραγματοποιούνται στον συγκεκριμένο δίκτυο καθώς όλες οι συναλλαγές είναι διαφανείς, αλλά ανώνυμες και ψευδώνυμες. Επιπλέον, το δίκτυο παρέχει συνήθως ένα μηχανισμό παροχής κινήτρων κατά το οποίο οι χρήστες κερδίζουν κρυπτονομίσματα κατά την επαλήθευση και επικύρωση των συναλλαγών τους, προκειμένου να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν σε αυτό και να χρησιμοποιούν το κρυπτονόμισμα.

Οι επιδράσεις αυτού του τύπου Blockchain είναι σημαντικές καθώς υπάρχει δυνατότητα μέσω αυτού, να διασπαστούν υπάρχοντα επιχειρηματικά μοντέλα μέσω της αποδιαμεσολάβησης. Αξιοσημείωτο κρίνεται και το γεγονός ότι τα δημόσια Blockchain τείνουν να είναι πιο ασφαλή από τους υπόλοιπους τύπους Blockchain λόγω του ότι κανένας οργανισμός ή κυβέρνηση δεν ελέγχει το δίκτυο και η συμμετοχή γίνεται ανώνυμα. Ο κώδικας με τη σειρά του ανανεώνεται αποκλειστικά από την κοινότητα του κάθε Blockchain δικτύου στην οποία συμμετέχουν εθελοντικά προγραμματιστές. Επιπλέον, το δημόσιο δίκτυο Blockchain είναι πιο αποτελεσματικό σε σχέση με άλλα αφού, δεδομένου ότι είναι ανοιχτό, είναι δυνατόν να χρησιμοποιηθεί από πάρα πολλές οντότητες, οι οποίες μπορούν να αξιοποιήσουν τις δυνατότητες του δικτύου. Παραδείγματα τέτοιων δυνατοτήτων είναι οι ανταλλαγές τομέων(domain) στο διαδίκτυο, οι

ανταλλαγές περιουσιών και τίτλων κ.α. Στο συγκεκριμένο τύπο δικτύου οι ανταλλαγές είναι εμφανείς από όλους και δεν μπορεί να υπάρξει κάποιο είδος μη τήρησης ενός συμβολαίου ή κάποιας ανταλλαγής από κάποια από τις δύο πλευρές.

Επίσης, το συγκεκριμένο μοντέλο Blockchain δεν απαιτεί κανένα κόστος υποδομής αφού δεν χρειάζεται να διατηρηθούν διακομιστές ή διαχειριστές συστημάτων, μειώνοντας ριζικά το κόστος δημιουργίας και λειτουργίας αποκεντρωμένων εφαρμογών(DApps). Παραδείγματα τέτοιων μοντέλων είναι το Bitcoin, το Ethereum, το Monero, το Litecoin κ.α. [13] [7]

## 5.2 FEDERATED - CONSORTIUM BLOCKCHAINS

Τα ομοσπονδιακά Blockchain λειτουργούν υπό την ηγεσία μιας ομάδας. Σε αντίθεση με τα δημόσια δίκτυα Blockchain, δεν επιτρέπουν σε κανένα άτομο με πρόσβαση στο διαδίκτυο, να συμμετέχει στη διαδικασία επαλήθευσης των συναλλαγών. Το συγκεκριμένο είδος Blockchain είναι ταχύτερο(υψηλότερη δυνατότητα κλιμάκωσης), εξουσιοδοτημένο (permissioned [14]) παρέχοντας περισσότερη ιδιωτικότητα στις συναλλαγές και θεωρείται μερικώς αποκεντρωμένο.

Τα ομοσπονδιακά Blockchain χρησιμοποιούνται κατά κύριο λόγο στον τραπεζικό τομέα. Η διαδικασία της συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Για παράδειγμα, σε μια κοινοπραξία 15 χρηματοπιστωτικών ιδρυμάτων, καθένα από τα οποία λειτουργεί έναν κόμβο του δικτύου και από τα οποία τα 10 πρέπει να υπογράψουν κάθε μπλοκ για να είναι έγκυρο. Το δικαίωμα ανάγνωσης του Blockchain μπορεί να είναι δημόσιο ή να περιορίζεται στους συμμετέχοντες.

Οι επιδράσεις αυτού του τύπου Blockchain είναι κρίσιμης σημασίας καθώς μειώνουν το κόστος των συναλλαγών και την ανάγκη για εφεδρεία δεδομένων(data redundancy), αντικαθιστά τα παλαιότερα συστήματα, απλοποιώντας τον χειρισμό εγγράφων βοηθώντας στην απαλλαγή από μηχανισμούς μη αυτόματης συμμόρφωσης. Παραδείγματα τέτοιων δικτύων έχουν εισχωρήσει στον τραπεζικό κλάδο(W3), στον κλάδο της ενέργειας(EWF) και της ασφάλισης(B3i).

Κάποιοι υποστηρίζουν ότι ένα τέτοιο σύστημα δεν μπορεί να οριστεί ως Blockchain, καθώς η συγκεκριμένη τεχνολογία βρίσκεται ακόμα σε πρώιμο στάδιο. Δεν είναι ακόμα σαφές πως η τεχνολογία θα είναι αποδοτική και πως θα υιοθετηθεί. Πολλοί ισχυρίζονται ότι τα ιδιωτικά ή τα ομοσπονδιακά δίκτυα Blockchain ενδέχεται να επηρεαστούν από τη μοίρα των Intranets τη

δεκαετία του 1990, όταν οι ιδιωτικές εταιρείες έχτισαν τα δικά τους ιδιωτικά δίκτυα LAN η WAN, αντί να χρησιμοποιούν το δημόσιο Διαδίκτυο και όλες τις υπηρεσίες του, τα οποία έχουν ξεπεραστεί με τον ερχομό του Software as a Service(SaaS) στο Web 2.0. [13] [6]

## 5.3 FULLY PRIVATE BLOCKCHAINS

Στο συγκεκριμένο είδος Blockchain, τα δικαιώματα εγγραφής κρατιούνται συγκεντρωτικά σε έναν οργανισμό. Τα δικαιώματα ανάγνωσης ενδέχεται να είναι δημόσια ή περιορισμένα σε αυθαίρετο βαθμό. Αν τα δικαιώματα ανάγνωσης είναι περιορισμένα, τα ιδιωτικά δίκτυα Blockchain μπορούν να παρέχουν μεγαλύτερο επίπεδο προστασίας προσωπικών δεδομένων. Παραδείγματα εφαρμογών περιλαμβάνουν τη διαχείριση βάσεων δεδομένων, τον έλεγχο, κλπ. τα οποία βρίσκονται εσωτερικά σε μια ενιαία εταιρεία έτσι ώστε η δυνατότητα ανάγνωσης από το κοινό μπορεί σε πολλές περιπτώσεις να μην είναι απαραίτητη. Σε άλλες περιπτώσεις η δυνατότητα δημόσιου ελέγχου ωστόσο κρίνεται επιθυμητή.

Οι επιδράσεις αυτού του τύπου δικτύου είναι αξιοσημείωτες, καθώς μια κοινοπραξία ή εταιρεία που εκμεταλλεύεται ένα ιδιωτικό δίκτυο Blockchain μπορεί εύκολα, αν το επιθυμεί, να αλλάξει τους κανόνες του συγκεκριμένου δικτύου, να επαναφέρει τις συναλλαγές, να τροποποιήσει τα υπόλοιπα κλπ. Σε ορισμένες περιπτώσεις, όπως για παράδειγμα στα εθνικά κτηματολόγια, αυτή η λειτουργικότητα είναι απαραίτητη. Επίσης, οι επικυρωτές των συναλλαγών είναι γνωστοί, επομένως δεν υπάρχει οποιοσδήποτε κίνδυνος επίθεσης που προέρχεται από κάποια αθέμιτη σύμπραξη από miners. Παράλληλα, οι συναλλαγές αυτού του τύπου δικτύου είναι φθηνότερες, αφού χρειάζεται να επαληθευτούν μόνο από μερικούς κόμβους που έχουν μεγάλη επεξεργαστική ισχύ και δεν χρειάζεται να επαληθευτούν για παράδειγμα, από ένα μεγάλο αριθμό φορητών υπολογιστών(laptops). Οι κόμβοι του συγκεκριμένου δικτύου μπορεί να θεωρηθεί ότι είναι πολύ καλά συνδεδεμένοι μεταξύ τους και οι βλάβες μπορούν γρήγορα να διορθωθούν με ανθρώπινη παρέμβαση, επιτρέποντας τη χρήση αλγόριθμων συναίνεσης οι οποίοι προσφέρουν το τελικό αποτέλεσμα μετά από πολύ μικρούς χρόνους επεξεργασίας των μπλοκ.

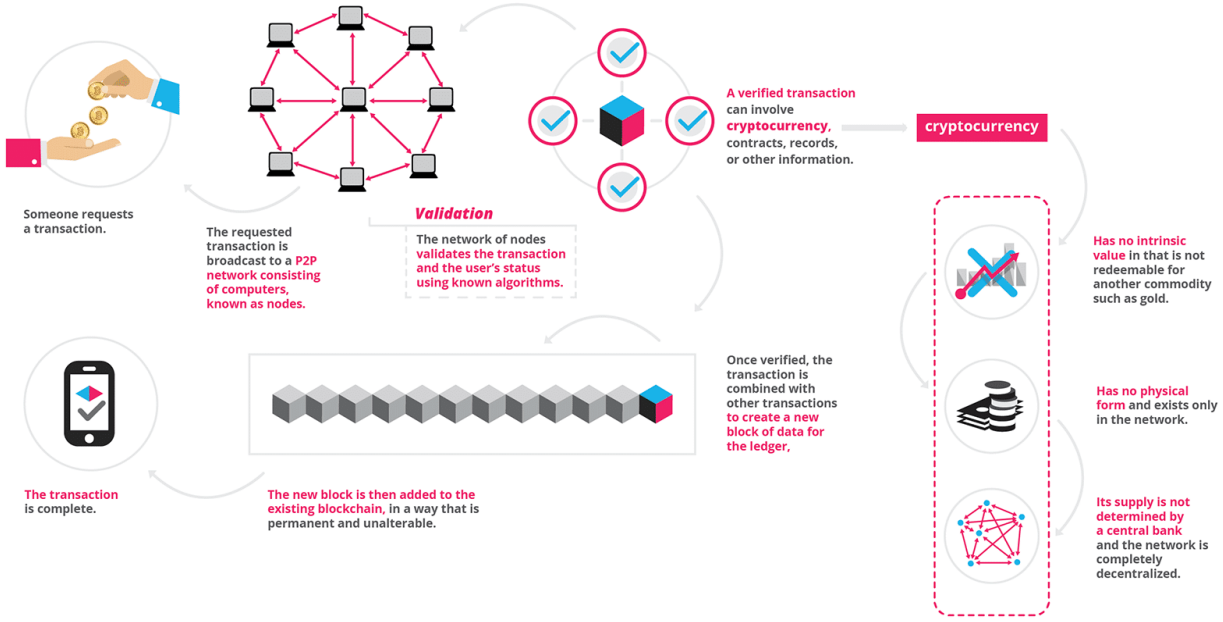
Τα ιδιωτικά δίκτυα Blockchain είναι ένας τρόπος να επωφεληθούν οι εταιρείες από το συγκεκριμένο μοντέλο καθώς παρέχει τη δυνατότητα δημιουργίας ομάδων και συμμετεχόντων οι οποίοι μπορούν να επαληθεύσουν τις συναλλαγές εσωτερικά. Το μοντέλο αυτό θέτει σε κίνδυνο

το σύστημα όσον αφορά τις παραβιάσεις ασφαλείας ακριβώς όπως σε ένα κεντρικοποιημένο σύστημα, σε αντίθεση με το δημόσιο δίκτυο Blockchain όπου η ασφάλεια εξασφαλίζεται από μηχανισμούς κινήτρων. Ωστόσο, τα ιδιωτικά δίκτυα έχουν εφαρμογή, ειδικότερα όταν πρόκειται για κλιμάκωση και συμμόρφωση ως προς τους κανόνες περί απορρήτου δεδομένων και άλλα ρυθμιστικά θέματα [13] [5] [7].

Σε γενικές γραμμές, μέχρι στιγμής δεν δόθηκε ιδιαίτερη έμφαση στη διάκριση μεταξύ Consortium και Fully Private Blockchains, κάτι το οποίο είναι σημαντικό. Το πρώτο είδος αποτελεί μία μείξη μεταξύ της "χαμηλής εμπιστοσύνης" που παρέχεται από τα δημόσια Blockchain και του μοντέλου "ενιαίας υψηλής εμπιστοσύνης οντότητα" που παρέχεται από τα ιδιωτικά Blockchain δίκτυα. Το δεύτερο είδος μπορεί να περιγραφεί με μεγαλύτερη ακρίβεια ως ένα παραδοσιακό κεντρικοποιημένο σύστημα με ένα βαθμό κρυπτογραφικής ελεγξιμότητας. Καθώς η τεχνολογία Blockchain βρίσκεται ακόμα σε αρχικό στάδιο όσον αφορά την υιοθέτησή τους από τις επιχειρήσεις, συχνά πραγματοποιείται διάκριση μεταξύ δημόσιων και ιδιωτικών Blockchain δικτύων. Δεδομένων όλων αυτών, για πολλούς χρήστες του Blockchain, μπορεί να φανεί ότι τα ιδιωτικά δίκτυα είναι η καλύτερη επιλογή για ιδρύματα ή επιχειρήσεις. Ωστόσο, ακόμα και στα πλαίσια μιας επιχείρησης ή οργανισμού, τα δημόσια δίκτυα Blockchain έχουν πολύ μεγάλη αξία, όπου αυτή η αξία βρίσκεται σε σημαντικό βαθμό στις πεποιθήσεις των υποστηρικτών των δημόσιων δικτύων, όπου κυριαρχεί η ελευθερία, η ουδετερότητα και η ελεύθερη προσπέλαση.

Η λύση που είναι βέλτιστη για μια συγκεκριμένη βιομηχανία εξαρτάται σε μεγάλο βαθμό από το ποιο ακριβώς είναι το αντικείμενο αυτής, καθώς και από τα αποτελέσματα που θέλει να πετύχει χρησιμοποιώντας την τεχνολογία Blockchain. Σε κάποιες περιπτώσεις, το δημόσιο δίκτυο είναι σαφώς καλύτερο, ενώ σε άλλες ο βαθμός του ιδιωτικού ελέγχου είναι απλά απαραίτητος ώστε να χρησιμοποιηθεί ένα ιδιωτικό δίκτυο.

# 6 Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ BLOCKCHAIN




ΕΙΚΟΝΑ 1: ΔΙΕΚΠΕΡΑΙΩΣΗ ΜΙΑΣ ΣΥΝΑΛΛΑΓΗΣ ΜΕΣΩ BLOCKCHAIN [47]

**Στάδιο 1ο :**

Δύο πλευρές θέλουν να διεκπεραιώσουν μία συναλλαγή.

**Στάδιο 2ο :**

Η συναλλαγή αποτυπώνεται online ως μπλοκ. Το μπλοκ μεταδίδεται-εκπέμπεται(broadcast) ανώνυμα σε όλους τους συνδεδεμένους χρήστες-κόμβους στο δίκτυο. Οι συγκεκριμένοι χρήστες είναι συνδεδεμένοι μεταξύ τους μέσω τοπολογίας Peer-to-peer(P2P).

**Στάδιο 3ο :**

Οι χρήστες του δικτύου «εγκρίνουν» τη συναλλαγή καθώς και την κατάσταση του χρήστη που θέλει να πραγματοποιήσει την συναλλαγή, χρησιμοποιώντας γνωστούς αλγόριθμους. Μία εγκεκριμένη συναλλαγή μπορεί να περιέχει κρυπτογράφηση, έξυπνα συμβόλαια, αρχεία και άλλες πληροφορίες.

**Στάδιο 4ο:**

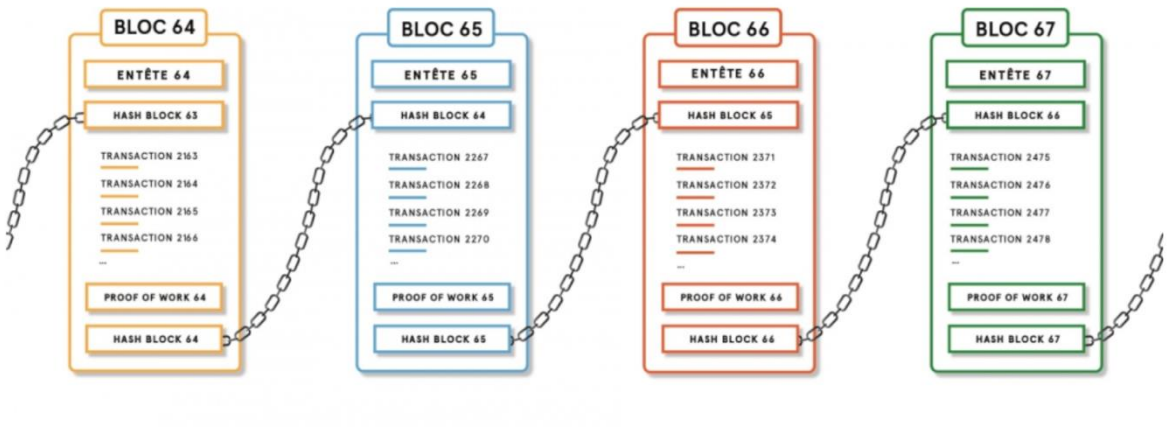
Η εγκεκριμένη συναλλαγή ενώνεται τότε με το υπόλοιπο δίκτυο σαν ένα καινούριο block στην αλυσίδα (blockchain) με τρόπο που την καθιστά μόνιμη και αδιάλλακτη, με απόλυτη διαφάνεια σε όλο το δίκτυο.

**Στάδιο 5ο :**

Η συναλλαγή ολοκληρώνεται.

# 7 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ BLOCKCHAIN

Η αρχιτεκτονική του Blockchain βασίζεται κυρίως σε 5 βασικά στοιχεία: τα μπλοκ(Block), την αλυσίδα(Chain), τις ψηφιακές υπογραφές(Digital Signatures), το δίκτυο ομότιμων χρηστών(Peer-to-Peer Network) και τον μηχανισμό εμπιστοσύνης(Consensus Protocol).

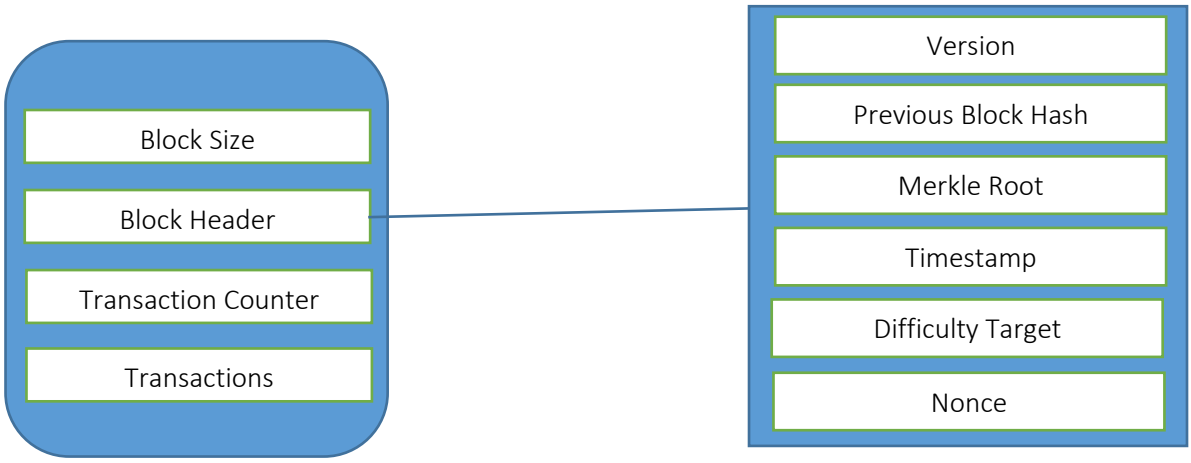



ΕΙΚΟΝΑ 2: ΣΤΙΓΜΙΟΤΥΠΟ ΕΝΟΣ ΤΥΠΙΚΟΥ BLOCKCHAIN [15]

## 7.1 BLOCK

Τα μπλοκ είναι δομές δεδομένων όπου σκοπό έχουν να συγκεντρώσουν και να καταγράψουν σύνολα συναλλαγών και να τα διανείμουν σε όλους τους κόμβους του δικτύου Blockchain. Δημιουργούνται από τους “Miners” και στην ουσία αποτελούν μια μόνιμη “αποθήκη

δεδομένων", τα οποία, μόλις γραφτούν δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν . Η τυπική δομή κάθε μπλοκ σε ένα δίκτυο Blockchain αποτελείται από 4 κύρια μέρη:




ΕΙΚΟΝΑ 3: ΔΟΜΗ ΕΝΟΣ ΜΠΛΟΚ

1. **Το μέγεθος του μπλοκ(Block Size):** το οποίο περιλαμβάνει το μέγεθος τους συγκεκριμένου μπλοκ, μετρημένο σε bytes.
2. **Την επικεφαλίδα του μπλοκ:(Block Header)**: αποτελείται από μεταδεδομένα(metadata) τα οποία βοηθούν στην επαλήθευση της εγκυρότητας ενός μπλοκ. Η επικεφαλίδα περιλαμβάνει:
    a) Version: η οποία περιλαμβάνει την έκδοση του παρόντος μπλοκ και αποτελεί στην ουσία έναν αριθμό μέσω του οποίου παρακολουθούνται οι αναβαθμίσεις λογισμικού.
    b) Previous Block Hash: που αποτελεί το Hash του αμέσως προηγούμενου μπλοκ.
    c) Merkle Root: που αποτελεί ένα κρυπτογραφημένο Hash το οποίο δημιουργείται από όλες τις συναλλαγές που περιλαμβάνονται σε αυτό το μπλοκ.
    d) Timestamp: που περιλαμβάνει το χρόνο σε δευτερόλεπτα UNIX Epoch time, που δημιουργήθηκε το συγκεκριμένο μπλοκ.
    e) Difficulty Target: αποτελεί τη δυσκολία που απαιτείται για να επικυρωθεί αυτό το μπλοκ.
    f) Nonce ("Number used once"): είναι ένας ακέραιος τυχαίος αριθμός ο οποίος χρησιμοποιείται από τον αλγόριθμο "Proof of Work" και προσαυξάνεται κατά τη διάρκεια της εξόρυξης. Χωρίς ένα nonce, τα δεδομένα ενός μπλοκ είναι σταθερά

και έτσι η συνάρτηση κατακερματισμού(hash) επιστρέφει πάντα το ίδιο αποτέλεσμα.

3. **Τον μετρητή των συναλλαγών(Transaction Counter):** είναι ο συνολικός αριθμός των συναλλαγών στο μπλοκ.
4. **Τις συναλλαγές(Transactions):** είναι όλες οι συναλλαγές που έχουν καταχωρηθεί στο μπλοκ.

## 7.2 CHAIN

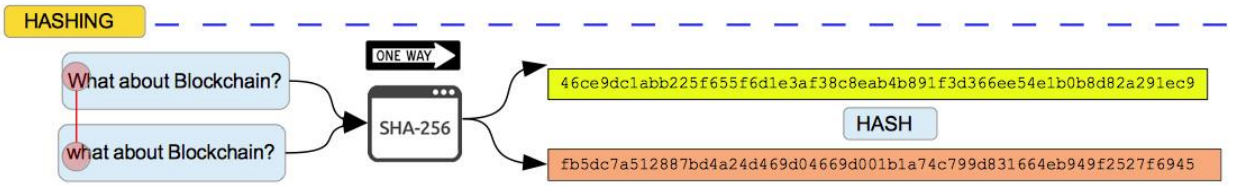
Ο όρος αλυσίδα(Chain) σχετίζεται με τον τρόπο που είναι ταξινομημένα τα μπλοκ σε ένα δίκτυο Blockchain. Σύμφωνα με τον Αντωνόπουλο "Η δομή των δεδομένων στο Blockchain είναι μια ταξινομημένη λίστα από μπλοκ συνδεδεμένη προς τα πίσω". Αυτή η ταξινόμηση των μπλοκ σχηματίζει τελικά την αλυσίδα. Η σύνδεση μεταξύ των μπλοκ πραγματοποιείται μέσα από τη συνάρτηση κατακερματισμού(Hash) [16].

## 7.3 HASH FUNCTION

Οι συναρτήσεις κατακερματισμού, είναι μαθηματικές συναρτήσεις που δέχονται ως είσοδο κάποιο δεδομένο, τυχαίου τύπου και μεγέθους και επιστρέφουν μία αναπαράσταση σταθερού μεγέθους (συνήθως μικρότερου από το μέγεθος εισόδου) που μοιάζει με τυχαία δεδομένα. Το μέγεθος αυτό μπορεί να είναι από 32 bit μέχρι 256 bit ή περισσότερα ανάλογα με το λόγο χρήσης της συνάρτησης. Όπως αναφέρει η Laurence "Το Hash είναι η μαγική κόλλα που ενώνει τα μπλοκ μεταξύ τους και επιτρέπει εμπιστοσύνη με μαθηματική ακρίβεια". [7].

Στο πλαίσιο των κρυπτονομισμάτων όπως το Bitcoin, χρησιμοποιείται ο αλγόριθμος Secure Hashing Algorithm 256 (SHA-256). Κάθε συναλλαγή και μπλοκ αναπαρίσταται από 16 δεκαεξαδικούς χαρακτήρες. Αυτό οφείλεται στο γεγονός ότι αυτοί οι "αναγνωριστικοί αριθμοί" υπολογίζονται ντετερμινιστικά με την σειριοποίηση των περιεχομένων των συναλλαγών/μπλοκ σε bytes και στη συνέχεια κατακερματίζονται σε bytes (δύο φορές) χρησιμοποιώντας τον SHA-256.

Στην περίπτωση του SHA-256, δεν λαμβάνεται υπόψη το μέγεθος των δεδομένων που εισέρχονται, αφού η έξοδος θα έχει πάντα 256-bits μέγεθος. Η ιδιαιτερότητα αυτή είναι σημαντική όταν υπάρχει μεγάλος όγκος δεδομένων και συναλλαγών. Έτσι, αντί να θυμάται κάποιος τα δεδομένα που εισήγαγε, τα οποία μπορεί να είναι άπειρα, μπορεί μόνο να θυμάται τον κατακερματισμό τους και να τον παρακολουθεί. Η λειτουργία του αλγορίθμου χαρακτηρίζεται μη αναστρέψιμη και λειτουργεί σαν ψηφιακό αποτύπωμα το οποίο είναι μοναδικό και δεν μπορεί να αποκρυπτογραφηθεί. [7] [16].




ΕΙΚΟΝΑ 4: ΔΙΑΦΟΡΕΤΙΚΗ ΕΙΣΟΔΟΣ ΑΠΟΔΙΔΕΙ ΔΙΑΦΟΡΕΤΙΚΗ ΕΞΟΔΟ [25]

Ο μηχανισμός αυτός ελέγχει την ακεραιότητα των συναλλαγών και των μπλοκ. Όπως μια ασύμμετρη υπογραφή δεν μπορεί να μεταβληθεί από κάποιο κακόβουλο χρήστη, έτσι και το περιεχόμενο μιας συναλλαγής δεν μπορεί να αλλοιωθεί λόγω της αντοχής του σε συγκρούσεις (collision resistance)[1]. Αυτό παρέχει μια εγγύηση στους συμμετέχοντες σε ένα Blockchain, καθώς όταν δύο από αυτούς, μοιράζονται το ίδιο κατακερματισμένο μπλοκ, τότε γνωρίζουν ότι μοιράζονται κάθε είσοδο/έξοδο σε κάθε προηγούμενη συναλλαγή/μπλοκ.

Μία συνηθισμένη χρήση του κατακερματισμού σήμερα είναι στα αρχεία δακτυλικών αποτυπωμάτων, γνωστά και ως αθροίσματα ελέγχου(checksums). Αυτό σημαίνει ότι χρησιμοποιώντας τον κατακερματισμό μπορεί κάποιος να ελέγξει αν ένα αρχείο έχει αλλοιωθεί ή επεξεργαστεί, από κάποιον ο οποίος δεν είναι ο δημιουργός του.

[1] Έννοια σύμφωνα με την οποία μια συνάρτηση κατακερματισμού F είναι ανθεκτική σε συγκρούσεις τιμών εισόδου εάν είναι αρκετά δύσκολο αν όχι αδύνατο να οδηγηθούμε σε κοινή τιμή εξόδου από διαφορετικά ορίσματα. Η αντοχή στις συγκρούσεις αφορά τις συναρτήσεις για τις οποίες συγκρούσεις δύσκολα προκύπτουν(π.χ. SHA-256)

## 7.4 CRYPTOGRAPHY

Η κρυπτογραφία είναι ο κλάδος των μαθηματικών που επιτρέπει τη δημιουργία μαθηματικών αποδείξεων οι οποίες παρέχουν υψηλά επίπεδα ασφάλειας. Είναι ένας από τους δύο κλάδους της κρυπτολογίας (ο άλλος είναι η κρυπτανάλυση), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς ώστε δύο ή περισσότερα άκρα επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών, κλπ.) να ανταλλάζουν μηνύματα, χωρίς κανένας τρίτος να είναι ικανός να διαβάζει την περιεχόμενη πληροφορία εκτός από τα δύο κύρια άκρα.

Η κρυπτογραφία χρησιμοποιήθηκε για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, κατανοητή μορφή σε έναν «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Ένας από τους αντικειμενικούς σκοπούς της κρυπτογραφίας είναι ότι η πληροφορία μπορεί να αλλοιωθεί μόνο από εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγορίθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Οι “πρώτοι” αριθμοί είναι ζωτικής σημασίας για την κρυπτογράφηση δεδομένων. Ο μεγαλύτερος πρώτος αριθμός μέχρι στιγμής, έχει μήκος 22 εκατομμύρια ψηφία.

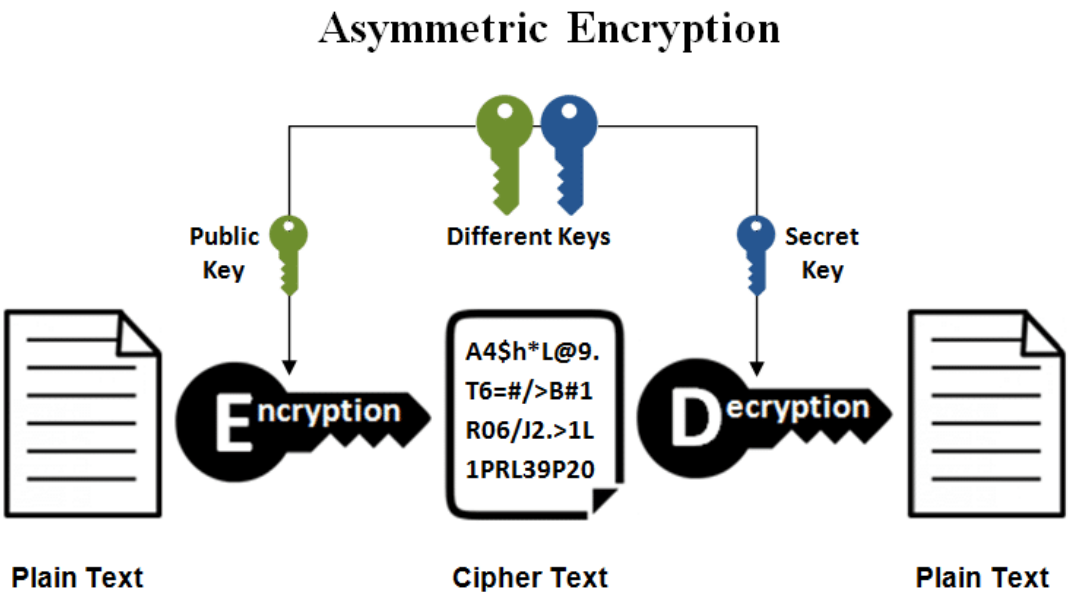
Σήμερα, κάθε κρυπτογράφηση δεδομένων βασίζεται σε υπολογιστές. Όμως όποιον αλγόριθμο κι αν επινοήσει ο άνθρωπος, όσο περίπλοκος και αν είναι, είναι υπερβολικά εύκολο να τον αποκωδικοποιήσει ένας κατάλληλα προγραμματισμένος υπολογιστής. Η κρυπτογράφηση υπολογιστή γενικά ανήκει σε δύο κατηγορίες:

- Κρυπτογράφηση με χρήση συμμετρικού κλειδιού (Symmetric Key Encryption).
- Κρυπτογράφηση με χρήση Δημόσιου κλειδιού – Ασύμμετρη κρυπτογράφηση (Public Key – Asymmetric Key Encryption).

Η τεχνολογία Blockchain χρησιμοποιεί κυρίως τη δεύτερη κατηγορία κρυπτογράφησης. Σε αυτή τη μέθοδο κρυπτογράφησης υπάρχουν δύο κλειδιά. Το δημόσιο κλειδί (Public Key) και το ιδιωτικό κλειδί (Private Key). Στην ασύμμετρη κρυπτογραφία οι ψηφιακές υπογραφές:

- Αποδεικνύουν ότι αυτός που υπογράφει έχει πρόσβαση στο ιδιωτικό κλειδί.
- Δεν αποκαλύπτουν το ιδιωτικό κλειδί.
- Είναι εύκολο να επαληθευτούν, αλλά δύσκολο να πλαστογραφηθούν ή να αλλαχθούν.

Το Bitcoin χρησιμοποιεί τις παραμέτρους secp256k1 του Αλγόριθμου Ψηφιακής Υπογραφής Ελλειπτικής Καμπύλης (Elliptical Curve Digital Signing Algorithm-ECDSA) συμβάλλοντας στην έτσι στην ασφάλεια των συναλλαγών των χρηστών. Το ECDSA[2] επινοήθηκε το 1985 από τους Victor Miller (IBM) και Neil Koblitz (University of Washington) ως ένας εναλλακτικός μηχανισμός για την υλοποίηση της κρυπτογραφίας του δημόσιου κλειδιού και έγινε πρότυπο ISO, ANSI, IEEE το 1998-2000. Το κυριότερο πλεονέκτημά του έναντι του RSA (που είναι ο πιο γνωστός αλγόριθμος Public/Asymmetric Key όσον αφορά το Internet), είναι ότι χρησιμοποιεί πολύ μικρότερα κλειδιά και υπογραφές για να επιτύχει το ίδιο επίπεδο ασφάλειας, κάτι το οποίο τον καθιστά πιο δύσκολο να παραβιαστεί.



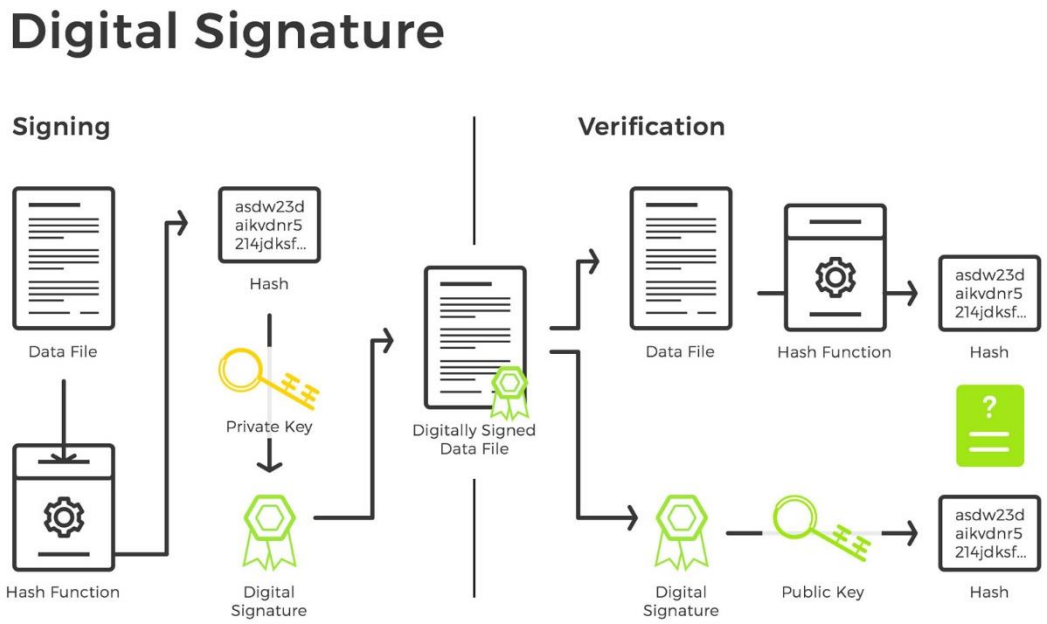

ΕΙΚΟΝΑ 5: ΚΡΥΠΤΟΓΡΑΦΙΑ ΑΣΥΜΜΕΤΡΟΥ ΚΛΕΙΔΙΟΥ [49]

Μια από τις κύριες περιπτώσεις που χρησιμοποιείται η ασύμμετρη κρυπτογράφηση είναι η κρυπτογράφηση δημόσιου κλειδιού. Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώσει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν ειδικοί εξυπηρετητές δημόσιων κλειδιών (Public Key Servers) στους οποίους μπορεί κανείς να

[2] https://www.certicom.com/content/certicom/en/ecc.html

απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του, για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (δημόσιο και ιδιωτικό) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία τέτοιων αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.



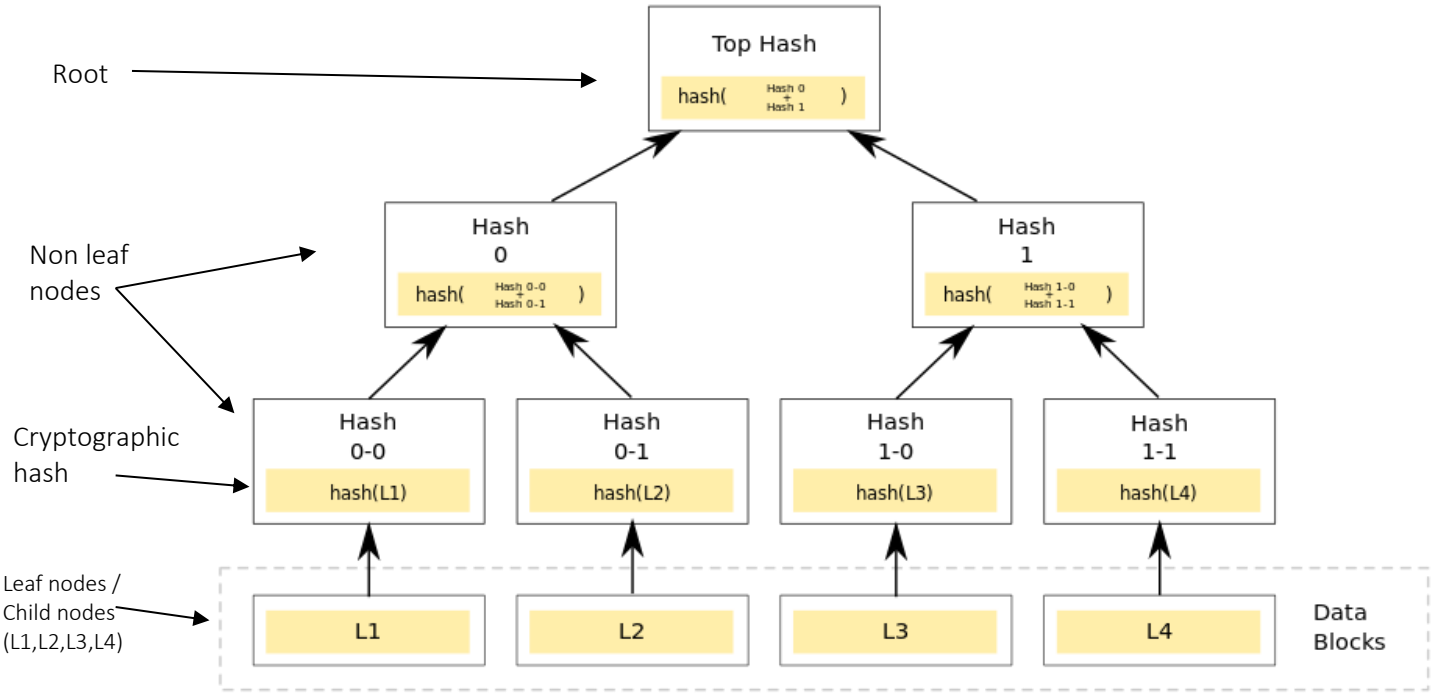

ΕΙΚΟΝΑ 6: ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΣΤΟ BLOCKCHAIN [50]

## 7.5 MERKLE TREES

Μια βάση δεδομένων Blockchain αποτελείται από δύο είδη εγγραφών: συναλλαγές και μπλοκ. Τα μπλοκ κρατούν το σύνολο των έγκυρων συναλλαγών που έχουν κατακερματιστεί και τις κωδικοποιούν σε δέντρο Merkle. Τα δέντρα Merkle είναι μια δομή δεδομένων που αποθηκεύει την ψηφιακή υπογραφή για ολόκληρη την λίστα συναλλαγών σε ένα μπλοκ. Χρησιμοποιείται για

την επαλήθευση της ακεραιότητας μιας συναλλαγής, με αποτελεσματικό τρόπο με τη βοήθεια ενός δυαδικού δέντρου. [10]

Στην κρυπτογραφία και στην επιστήμη των υπολογιστών ένα δέντρο κατακερματισμού ή ένα δέντρο Merkle, είναι ένα δέντρο το οποίο αποτελείται από δύο είδη κόμβων: τους κόμβους φύλλων(leaf nodes) και τους κόμβους μη-φύλλων(non leaf nodes). Κάθε κόμβος φύλλων, φέρει ετικέτα με ένα μπλοκ δεδομένων και κάθε κόμβος μη-φύλλων φέρει μία ετικέτα με ένα κρυπτογραφημένο κατακερματισμό(cryptographic hash) η οποία περιέχει τις ετικέτες των κόμβων από τους οποίους δημιουργήθηκε(child nodes). Τα δέντρα Merkle, τα οποία είναι δυαδικά δέντρα, είναι μια γενίκευση των λιστών και των αλυσίδων κατακερματισμού και επιτρέπουν την αποτελεσματική και ασφαλή επαλήθευση του περιεχομένου των μεγάλων δομών δεδομένων.




ΕΙΚΟΝΑ 7: Η ΔΟΜΗ ΕΝΟΣ MERKLEE TREE

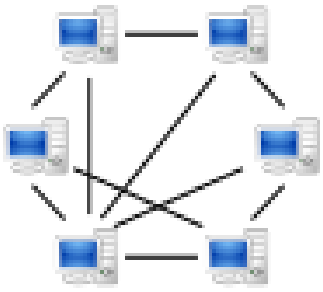
Η αποθήκευση δεδομένων σε σειρά, θα απαιτούσε πολύ χρόνο καθώς κάθε μπλοκ περιέχει μεγάλο αριθμό συναλλαγών. Με τον τρόπο αυτό η εύρεση μιας συναλλαγής θα ήταν χρονοβόρα αλλά και δυσλειτουργική. Με τη χρήση των Merkle Trees, μειώνεται σημαντικά ο χρόνος που απαιτείται για να διαπιστωθεί αν μία συναλλαγή βρίσκεται σε ένα συγκεκριμένο μπλοκ. Τα δέντρα Merkle επιτρέπουν σε έναν κόμβο να κατεβάσει μόνο την κεφαλίδα(Header) ενός μπλοκ και έναν μικρό αριθμό κόμβων από το δέντρο για να επικυρώσει τη συναλλαγή. Η δυνατότητα λήψης και

επικύρωσης μόνο ενός τμήματος ενός μπλοκ για την επικύρωση μεμονωμένων συναλλαγών είναι σημαντική για τη βιωσιμότητα του δικτύου. Ένας πλήρης κόμβος για την αποθήκευση και επεξεργασία όλων των συναλλαγών κάθε μπλοκ, καταναλώνει 15 GB χώρου στο δίσκο, σύμφωνα με στοιχεία του Απριλίου του 2014 και αυξάνεται κατά 1 GB ανά μήνα. Έτσι γίνεται κατανοητό ότι η αποθήκευση τέτοιας ποσότητας δεδομένων σε μια κινητή συσκευή δεν είναι εφικτή. [17]

Η έννοια των κατακερματισμένων δέντρων πήρε το όνομά της από τον Ralph Merkle που την κατοχύρωσε το 1979 και τα οποία χρησιμοποιούνται σε κατανεμημένα συστήματα αρχείων, όπως IPFS, συστήματα κοινής χρήσης αρχείων όπως BitTorrent και σε NoSQL βάσεις δεδομένων όπως η Cassandra.

## 7.6 PEER-TO-PEER PROTOCOL

Στον κόσμο του διαδικτύου σήμερα δύο είναι τα κυρίαρχα μοντέλα δικτυακών εφαρμογών: η αρχιτεκτονική πελάτη-εξυπηρετητή (Client-Server) και η αρχιτεκτονική ομότιμων χρηστών(Peer-to-Peer-P2P). Ένα πρωτόκολλο Blockchain λειτουργεί σε ένα P2P δίκτυο υπολογιστών, που όλοι τρέχουν το πρωτόκολλο και κατέχουν ένα πανομοιότυπο αντίγραφο του μητρώου συναλλαγών, επιτρέποντας συναλλαγές P2P, χωρίς τη χρήση διαμεσολαβητών.



ΕΙΚΟΝΑ 8: P2P ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Στην αρχιτεκτονική πελάτη-εξυπηρετητή υπάρχει πάντα ενεργός υπολογιστής(Server), ο οποίος εξυπηρετεί αιτήσεις για υπηρεσίες από άλλους υπολογιστές, τους πελάτες. Γίνεται κατανοητό ότι ο ρόλος του εξυπηρετητή σε ένα τέτοιο δίκτυο είναι καθοριστικής σημασίας. [18]

Αντίθετα, σε ένα δίκτυο Ομότιμων Χρηστών (Peer-to-peer – P2P) κάθε κόμβος που μετέχει είναι ισότιμος με κάθε άλλο και μπορεί να ενεργήσει είτε σαν πελάτης (Client) είτε σαν εξυπηρετητής (Server). Οι περισσότερες εφαρμογές που υπάρχουν σήμερα χρησιμοποιούν τέτοιου είδους δίκτυα. Έχοντας κόμβους-χρήστες οι οποίοι επικοινωνούν ευθέως μεταξύ τους (σε αντίθεση με τη χρήση αξιόπιστων τρίτων παρόχων), μοιράζονται τους πόρους τους ισοδύναμα δημιουργώντας έτσι αποκεντρικοποιημένα και κατανεμημένα συστήματα. Το δίκτυο αυτό

χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Πληροφορίες που βρίσκονται σε στον έναν κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

Τα συστήματα αυτά δεν απαιτούν διαχείριση και συντήρηση, οικονομικές αξιώσεις ή άλλους νομικούς περιορισμούς. Οι κόμβοι προσαρμόζονται, αυτοοργανώνονται καθώς εισέρχονται ή αποχωρούν από το σύστημα, ικανοποιώντας την ιδιότητα της κλιμάκωσης και της ανοχής στις αποτυχίες. Οι λειτουργίες τους είναι κατανεμημένες στους κόμβους που μετέχουν σε ένα τέτοιο σύστημα, όπου εκατομμύρια διαφορετικοί χρήστες μπορούν να είναι παρόντες ταυτόχρονα. Το πλεονέκτημα της χρήσης ενός P2P δικτύου είναι ότι για την αποθήκευση και επιβεβαίωση της ορθότητας της κάθε συναλλαγής, δεν χρειάζεται κάποιος ενδιάμεσος ή κάποια κεντρική αρχή, κάτι το οποίο κάνει το δίκτυο πιο ασφαλές από κακόβουλες επιθέσεις. [16]

Τα δίκτυα Ομότιμων Χρηστών έκαναν την πρώτη εμφάνισή τους το 1999 με την εισαγωγή του συστήματος διαμοιρασμού αρχείων Napster. Το ίντερνετ παρέχει ένα εξαιρετικό δίκτυο για πρωτόκολλα P2P. Τα πρωτόκολλα δικτύου Gossip (Gossip Network Protocols) έχουν χρησιμοποιηθεί σε πολλές βάσεις δεδομένων NoSQL συμπεριλαμβανομένων των Amazon Dynamo, Cassandra και Riak.

## 7.7 CONSENSUS PROTOCOL

Κάθε δίκτυο ομότιμων χρηστών βασισμένο σε Blockchain μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση όλων των χρηστών, αφού δεν υπάρχει κεντρική αρχή για να παρέχει εμπιστοσύνη και ακεραιότητα στις πληροφορίες που ανταλλάζονται. [7] [16]

Για να υπάρξει λοιπόν συναίνεση, χρειάζεται ένας τρόπος για να αποφασιστεί ποια δεδομένα είναι έγκυρα και ποια όχι. Η διαδικασία της επικύρωσης δεδομένων σε ένα δίκτυο P2P ονομάζεται εξόρυξη(mining) και απαιτεί τη χρήση σύνθετων αλγορίθμων όπως Proof-of-Work, Proof-of-Stake και Practical Byzantine Fault Tolerance. Μέσω αυτής της διαδικασίας επιταχύνεται επίσης η προσθήκη των επικυρωμένων μπλοκ από συναλλαγές στην αλυσίδα του Blockchain.

### 7.7.1 PROOF-OF-WORK SYSTEM

Το σύστημα Απόδειξης Εργασίας ή Proof of Work (PoW) είναι ένα πρωτόκολλο το οποίο έχει ως κύριο στόχο τη διασφάλιση της διαδικασίας επικύρωσης των δεδομένων καθώς και την αποτροπή επιθέσεων στον κυβερνοχώρο, όπως μια κατανεμημένη επίθεση κατάργησης μιας υπηρεσίας (Distributed Denial-of-Service attack - DDoS), η οποία αποσκοπεί στην εξάντληση των πόρων ενός ηλεκτρονικού συστήματος με την αποστολή πολλαπλών ψεύτικων αιτημάτων. Η ιδέα του Proof-of-Work υπήρχε ακόμα πριν από το Bitcoin, αλλά ο Satoshi Nakamoto εφάρμοσε αυτή την τεχνική στο δικό του ψηφιακό νόμισμα φέρνοντας επανάσταση στον τρόπο που έχουν οριστεί οι παραδοσιακές συναλλαγές. Στην πραγματικότητα η ιδέα του PoW δημοσιεύτηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1993 στο άρθρο τους με τίτλο “Pricing via Processing or Combatting Junk Mail”, αλλά ο όρος “Proof-of-Work” χρησιμοποιήθηκε για πρώτη φορά το 1999 από τους Markus Jakobsson και Ari Juels σε ένα έγγραφο που δημοσίευσαν με τίτλο “Proofs of Work and Bread Pudding Protocols”.

Η PoW είναι μια έξυπνη εφαρμογή των συναρτήσεων κατακερματισμού. Αποτελεί μια απαίτηση ώστε να οριστεί ένας ακριβός υπολογισμός μέσω υπολογιστή, ο οποίος ονομάζεται εξόρυξη(mining). Η εξόρυξη πρέπει να εκτελεστεί προκειμένου να δημιουργηθεί μια νέα ομάδα εμπιστευτικών συναλλαγών (το λεγόμενο μπλοκ) σε ένα κατανεμημένο μητρώο (distributed ledger), το Blockchain. Με τη χρήση του mining, αφενός επαληθεύεται η νομιμότητα μιας συναλλαγής και αποφεύγεται η λεγόμενη διπλή δαπάνη[3] και αφετέρου, επιβραβεύονται οι miners (με νέα ψηφιακά νομίσματα) για την εκτέλεση της προηγούμενης εργασίας.

Όταν δημιουργείται ένα μπλοκ, οι κόμβοι του δικτύου προσπαθούν να το “εξορύξουν”, κάτι το οποίο σημαίνει να το προσθέσουν στο Blockchain. Για να γίνει αυτό, οι miners θα πρέπει να βρουν το Hash αυτού του μπλοκ λύνοντας ένα μαθηματικό πρόβλημα γνωστό ως πρόβλημα απόδειξης εργασίας (Proof-of-Work Problem). Ο miner που θα λύσει πρώτος το πρόβλημα κάθε μπλοκ, παίρνει μια ανταμοιβή. Αυτό το μαθηματικό πρόβλημα, έχει βασικό χαρακτηριστικό της ασυμμετρία. Στην πραγματικότητα, στην πλευρά του αιτούντα πρέπει η δυσκολία επίλυσης να είναι μεγαλύτερη σε σχέση με τον έλεγχο που θα πραγματοποιηθεί στο δίκτυο. Αυτή η ιδέα είναι γνωστή ως κόστος λειτουργίας επεξεργαστή (CPU cost function). Όλοι οι miners του δικτύου ανταγωνίζονται για να βρουν πρώτοι μια λύση για το μαθηματικό πρόβλημα που αφορά το

[3] Η διπλή δαπάνη είναι το φαινόμενο το οποίο εμφανίζεται όταν ένας κακόβουλος χρήστης προσπαθεί να ξοδέψει τα κρυπτονομίσματά του σε δύο διαφορετικούς παραλήπτες ταυτοχρόνως.

υποψήφιο μπλοκ, ένα πρόβλημα που δεν μπορεί να λυθεί με άλλους τρόπους παρά μόνο με υπολογιστική δύναμη, κάτι το οποίο απαιτεί ένα τεράστιο αριθμό προσπαθειών. Όταν κάποιος miner βρει τελικά τη σωστή λύση, το ανακοινώνει σε όλο το δίκτυο ταυτόχρονα, λαμβάνοντας ένα βραβείο κρυπτογράφησης (την ανταμοιβή) που παρέχει το πρωτόκολλο.

Από τεχνικής άποψης, η διαδικασία εξόρυξης είναι μια λειτουργία αντίστροφου κατακερματισμού (hashing). Λειτουργεί υπολογίζοντας τον κατακερματισμό (Hash) ενός μηνύματος σε σχέση με πολλές διαφορετικούς nonce (συντομογραφία του "number used once"), μέχρι να βρεθεί ένα αποτέλεσμα το οποίο πληροί ένα σπάνιο κριτήριο. Κάθε φορά που αποτυγχάνει ο χρήστης να αποκτήσει ένα Hash το οποίο θα είναι ικανό να επαληθεύσει το μπλοκ, μπορεί να ενημερώσει το nonce και να προσπαθήσει ξανά. Αυτό εξασφαλίζει ότι οι miners του δικτύου πρέπει να εργαστούν για να προσθέσουν ένα μπλοκ στο Blockchain. [19] Δεδομένου ότι κάθε Hash είναι εξίσου απίθανο να ικανοποιήσει αυτά τα κριτήρια, καθορίζοντας ένα δύσκολο κριτήριο, αποτελεί έναν τρόπο να αποδειχθεί ότι κάποιος ξόδεψε ισχύ του επεξεργαστή (CPU Cycles). Η δυσκολία αυτή καθορίζει τον ανταγωνιστικό χαρακτήρα του mining, αφού όσο περισσότερη υπολογιστική ισχύς προστίθεται στο δίκτυο, τόσο αυξάνεται αύτη η παράμετρος της δυσκολίας, αυξάνοντας επίσης τον μέσο αριθμό των υπολογισμών που απαιτούνται για τη δημιουργία ενός νέου μπλοκ. Αυτή η μέθοδος αυξάνει επίσης το κόστος δημιουργίας μπλοκ, πιέζοντας τους miners να βελτιώσουν την αποδοτικότητα των "ορυχείων" τους για να διατηρήσουν μια θετική ισορροπία.

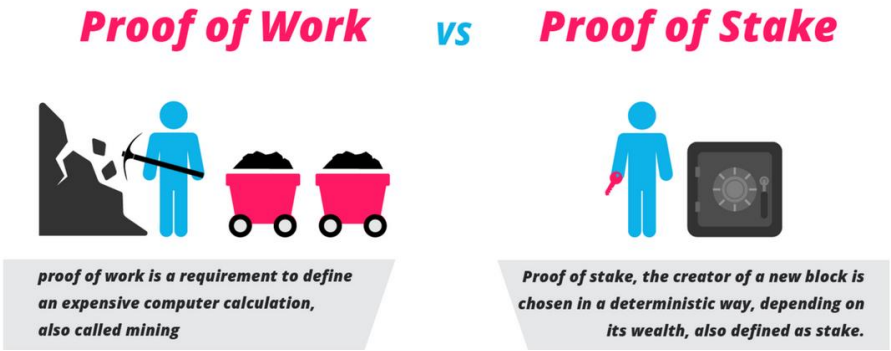
Με τη χρήση της PoW επιτυγχάνεται αξιόπιστη και κατανεμημένη συναίνεση αλλά ταυτόχρονα γίνεται απίθανη και συνάμα ακριβή, μια επίθεση σε ένα blockchain. Ένα αξιόπιστο και κατανεμημένο σύστημα συναίνεσης σημαίνει ότι εάν κάποιος θέλει να στείλει ή να λάβει χρήματα από κάποιον, δεν χρειάζεται να εμπιστευτεί σε υπηρεσίες τρίτων. Στις παραδοσιακές μεθόδους πληρωμής, πρέπει να εμπιστευτεί κάποιος τις υπηρεσίες τρίτων για να ορίσει μια συναλλαγή (Visa, MasterCard, Paypal, τράπεζες), οι οποίοι διατηρούν δικό τους ιδιωτικό μητρώο, το οποίο αποθηκεύει το ιστορικό των συναλλαγών και τα υπόλοιπα του κάθε λογαριασμού.

### 7.7.2 PROOF-OF-STAKE SYSTEM

Το σύστημα Απόδειξης Συμμετοχής ή Proof-of-Stake (PoS) είναι ένας τύπος αλγορίθμου με τον οποίο ένα δίκτυο blockchain μπορεί να επικυρώσει και να επιτύχει κατανεμημένη συναίνεση. Η πρώτη ιδέα της PoS προτάθηκε στο διαδικτυακό φόρουμ bitcointalk.org το 2011, αλλά η πρώτη φορά που εφαρμόστηκε ήταν στο ψηφιακό νόμισμα Peercoin το 2012. Ο σκοπός του PoS είναι ίδιος με την Απόδειξη Εργασίας (PoW), αλλά η διαδικασία για την επίτευξη του στόχου είναι αρκετά διαφορετική.

Σε αντίθεση με την Απόδειξη Εργασίας, η οποία βασίζεται στην υπολογιστική δύναμη-χωρητικότητα των κόμβων του δικτύου, η Απόδειξη Συμμετοχής βασίζεται στο ύψος του πονταρίσματος που πραγματοποιεί κάποιος. Ο δημιουργός ενός μπλοκ επιλέγεται με ντετερμινιστικό τρόπο, λαμβάνοντας υπόψη τον πλούτο του, που επίσης ορίζεται ως συμμετοχή-ποντάρισμα (Stake). Έτσι όσο μεγαλύτερη συμμετοχή έχει κάποιος στο δίκτυο τόσο περισσότερο mining μπορεί να κάνει κάποιος σε ένα blockchain. Για παράδειγμα, αν ένας miner κατέχει μερίδιο 5% των συνολικών κρυπτονομισμάτων που κυκλοφορούν, μπορεί να κάνει mining στο 5% των διαθέσιμων μπλοκ. Στο συγκεκριμένο σύστημα δεν υπάρχει κάποιο είδους ανταμοιβής. Όσον αφορά τα ψηφιακά νομίσματα, δεν δημιουργούνται νέα και ο αριθμός τους δεν αλλάζει ποτέ, αλλά παραμένουν όσα έχουν δημιουργηθεί στο παρελθόν. Οι miners, γνωστοί και ως πλαστογράφοι (forgers), παίρνουν αμοιβές από τις συναλλαγές.

Από θέμα ασφάλειας, σε ένα δίκτυο κρυπτονομισμάτων, ο επιτιθέμενος θα πρέπει να κατέχει μεγάλο ποσοστό από τα κρυπτονομίσματα. Όσο περισσότερο αγοράζει κάποιος τόσο περισσότερο πιθανόν να αυξάνεται η τιμή τους. Έτσι όταν ο επιτιθέμενος έχει στην κατοχή του ένα μεγάλο ποσοστό των κρυπτονομισμάτων για να επιτεθεί στο δίκτυο, θα είναι αντιπαραγωγικό καθώς η επίθεσή του θα επηρεάσει τον ίδιο περισσότερο, αφού ο ίδιο θα κατέχει την πλειοψηφία. [20] [21] [22]




ΕΙΚΟΝΑ 9: PoW VS. PoS [66]

### 7.7.3 PRACTICAL BYZANTINE FAULT TOLERANCE

Το 1999, οι Miguel Castro και Barbara Liskov[4] εισήγαγαν τον αλγόριθμο "Practical Byzantine Fault Tolerance (PBFT)" που αποτέλεσε την πρώτη πρακτική λύση απέναντι στο πρόβλημα των "Βυζαντινών Στρατηγών", η οποία έγινε αποδεκτή από όλους.

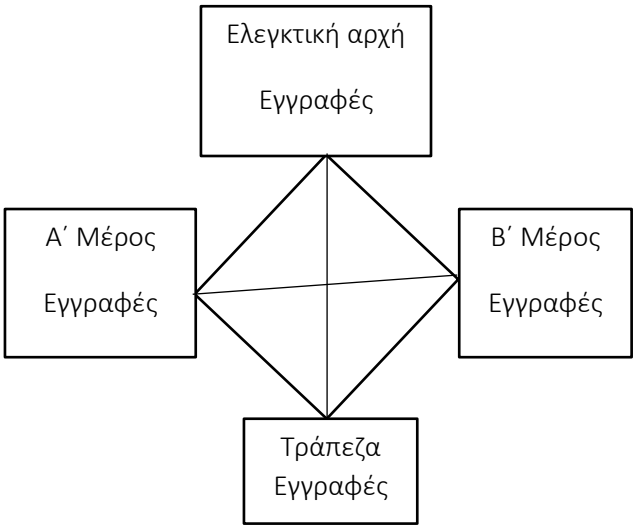
Στο πρόβλημα των "Βυζαντινών Στρατηγών[5]" το οποίο περιγράφηκε αρχικά από τους Marshall Pease, Robert Shostak και Leslie Lamport το 1982, μια ομάδα στρατηγών, καθένας από τους οποίους διοικεί τμήμα του βυζαντινού στρατού, πολιορκεί μια εχθρική πόλη. Οι στρατηγοί πρέπει να συμφωνήσουν σε ένα κοινό σχέδιο μάχης για την κατάληψη της πόλης. Ωστόσο, οι στρατηγοί μπορούν να επικοινωνούν μόνο μέσω αγγελιοφόρων. Οι αγγελιοφόροι μπορεί να συλληφθούν από τον εχθρό και τότε το μήνυμα δεν θα φτάσει στον άλλο στρατηγό. Η δυσκολία στη συμφωνία είναι ότι ένας ή περισσότεροι στρατηγοί μπορεί να είναι προδότες και να επιθυμούν να σαμποτάρουν το σχέδιο μάχης. Είναι πιθανό να στείλουν ψευδή μηνύματα, να αλλοιώσουν μηνύματα ή να καταστείλουν την αποστολή τους. Όλοι οι πιστοί στρατηγοί θα ενεργούν σύμφωνα με το σχέδιο. Ένας μικρός αριθμός προδοτών μπορεί να λοιπόν να ανατρέψει την πορεία των γεγονότων που έχουν σχεδιάσει οι πιστοί στρατηγοί.

Ο αλγόριθμος PBFT ήταν η πρώτη ουσιαστική λύση για την επίτευξη συναίνεσης εν όψει του παραπάνω προβλήματος. Ο συγκεκριμένος αλγόριθμος χρησιμοποιείται από εξουσιοδοτημένα Blockchain δίκτυα, όπως το Hyperledger Fabric, Ripple, Stellar και απαιτεί ο κάθε κόμβος να είναι γνωστός στο δίκτυο. Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Αναλυτικότερα, σε κάθε φάση της διαδικασίας, επιλέγεται με βάση ορισμένους κανόνες ένας κύριος εισηγητής κόμβος, ο οποίος είναι υπεύθυνος να εξετάσει αν τα δεδομένα είναι σωστά. Αφού εξετάσει τα δεδομένα, στέλνει τα αποτελέσματα σε όλους τους υπόλοιπους κόμβους του δικτύου. Ο εισηγητής θα περάσει στην επόμενη φάση εξέτασης των δεδομένων, αν τα 2/3 όλων των κόμβων έχουν ψηφίσει ότι συμφωνούν μαζί του. Αν οι ψήφοι είναι λιγότεροι, τότε εκλέγεται ένας καινούριος εισηγητής. Η διαδικασία ολοκληρώνεται σε 3 φάσεις, όπου σε κάθε φάση ακολουθείται η ίδια διαδικασία. [20]

[4] http://pmg.csail.mit.edu/papers/osdi99.pdf
[5] https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

# 8 Η "ΕΠΑΝΑΣΤΑΣΗ" ΤΟΥ BLOCKCHAIN

Σύμφωνα με τις παραδοσιακές μεθόδους καταγραφής συναλλαγών και παρακολούθησης των περιουσιακών στοιχείων, οι συμμετέχοντες σε ένα δίκτυο διατηρούν δικούς τους καταλόγους και αρχεία βάσεις δεδομένων, όπως φαίνεται στο παρακάτω σχήμα.



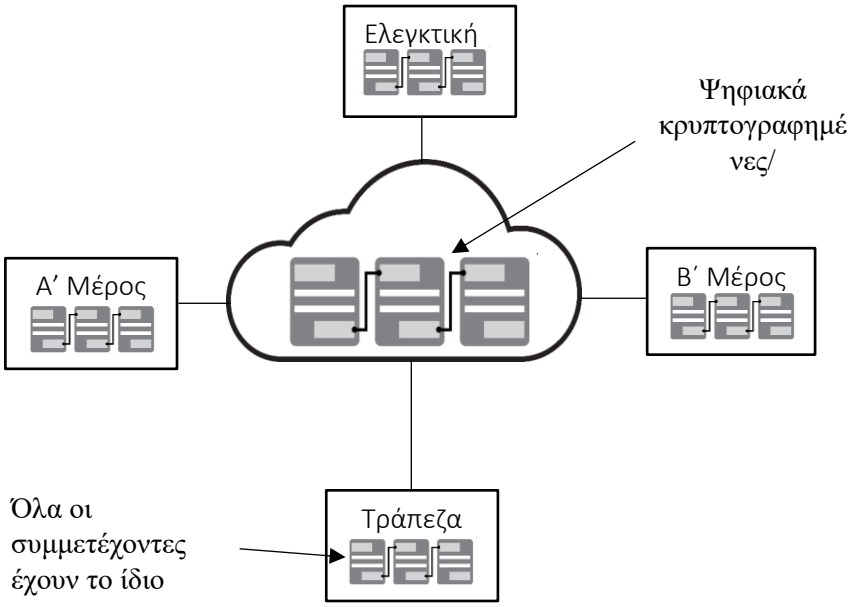

ΕΙΚΟΝΑ 10: ΠΑΡΑΔΟΣΙΑΚΟΣ ΤΡΟΠΟΣ ΔΙΑΝΟΜΗΣ ΕΓΓΡΑΦΩΝ

Η παραδοσιακή αυτή μέθοδος μπορεί να είναι δαπανηρή διότι εν μέρει οι μεσάζοντες που συμβάλλουν, χρεώνουν τέλη για τις υπηρεσίες τους. Είναι δυσλειτουργική, λόγω των καθυστερήσεων που δημιουργούνται στην προσπάθεια λήψης αποφάσεων, καθώς και της ανθρώπινης προσπάθειας που απαιτείται για να διατηρηθούν και να καταγραφούν τα απαραίτητα στοιχεία. Επίσης είναι ευάλωτη διότι εάν ένα κεντρικό σύστημα, για παράδειγμα μια τράπεζα, δεχτεί κάποια κυβερνο-επίθεση, κακόβουλη ενέργεια ή υπάρξει ανθρώπινο λάθος, επηρεάζεται ολόκληρο το επιχειρηματικό δίκτυο.

Η αρχιτεκτονική blockchain δίνει στους συμμετέχοντες τη δυνατότητα να μοιράζονται έναν κοινό λογαριασμό-αρχείο, μέσω της Peer-to-peer επικοινωνίας, κάθε φορά που πραγματοποιείται μια συναλλαγή.

Ένα δίκτυο υπολογιστών Peer-to-peer είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης των κόμβων.

Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον έναν κόμβο ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα. Μέσω της Peer-to-peer αναπαραγωγής που χρησιμοποιεί το blockchain, κάθε συμμετέχων(κόμβος) στο δίκτυο δρα και ως αποστολέας και ως παραλήπτης. Κάθε κόμβος μπορεί να στείλει και να λάβει συναλλαγές σε άλλους κόμβους και τα δεδομένα παραμένουν συγχρονισμένα σε όλο το δίκτυο.




ΕΙΚΟΝΑ 11: P2P ΣΥΣΤΗΜΑ ΑΝΤΑΛΛΑΓΗΣ ΑΡΧΕΙΩΝ ΣΤΟ BLOCKCHAIN

Το δίκτυο blockchain είναι οικονομικό και αποδοτικό, επειδή αφενός εξαλείφει την προσπάθεια που καταβάλλεται ώστε να διατηρηθούν τα στοιχεία σύμφωνα με τον παραδοσιακό τρόπο και αφετέρου μειώνει την ανάγκη για μεσάζοντες. Οι συναλλαγές είναι ασφαλείς και μπορούν να επαληθευτούν ανά πάσα στιγμή. Οι συμμετέχοντες και στα δύο συστήματα συναλλαγών είναι οι ίδιοι. Αυτό που αλλάζει είναι ότι το αρχείο συναλλαγών είναι κοινόχρηστο και διαθέσιμο σε όλους.

Ένα δίκτυο blockchain έχει τα ακόλουθα βασικά χαρακτηριστικά:

1. **Συναίνεση(Consensus):** Για να είναι έγκυρη μια συναλλαγή όλοι οι συμμετέχοντες πρέπει να συμφωνήσουν για την εγκυρότητά του. Σε ένα επιχειρηματικό δίκτυο όπου οι συμμετέχοντες είναι γνωστοί και αξιόπιστοι, οι συναλλαγές μπορούν να εξακριβωθούν και να δεσμευτούν

μέσω του κοινόχρηστου αρχείου με διάφορα μέσα συναίνεσης μερικά από τα οποία είναι Απόδειξη Συμμετοχής (PoS) ή Απόδειξη Εργασίας (PoW), Πολλαπλή Επικύρωση (Multi-signature) όπου η πλειοψηφία των συμμετεχόντων στο δίκτυο (π.χ. τα 3/5 του δικτύου) πρέπει να συμφωνήσουν ότι μία συναλλαγή είναι έγκυρα αλλά και από αλγόριθμους υπογραφής κατωφλίων (όπως ο Practical Byzantine Fault Tolerance Algorithm - PBFT). Με τη χρήση του συγκεκριμένου αλγορίθμου, επιλύονται οι διαφορές μεταξύ των κόμβων (συμμετέχοντες) του δικτύου, στην περίπτωση που κάποιος από αυτούς, δώσει διαφορετική έξοδο από τους υπόλοιπους.

2. **Διαφάνεια(Transparency):** Όλα τα δεδομένα σε ένα Blockchain είναι δημόσια και δεν είναι εύκολο να χειραγωγηθούν, καθώς διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων.
3. **Εφεδρεία(Redundancy):** κάθε χρήστης στο δίκτυο Blockchain διατηρεί ένα αντίγραφο των δεδομένων, οπότε δεν μπορεί εύκολα να τεθεί εκτός σύνδεσης εξαιτίας δυσλειτουργιών του συστήματος ή κακόβουλων ενεργειών τρίτων.
4. **Διαμεσολάβηση(Disintermediation):** η απομάκρυνση των μεσαζόντων όπως οι τράπεζες ή οι εταιρείες, μειώνει το κόστος συναλλαγών και τους κινδύνους που συνδέονται με την παρουσία τέτοιων ενδιάμεσων φορέων. Ωστόσο, δεν σημαίνει ότι δεν θα δημιουργηθεί ένα νέο είδος διαμεσολαβητών ως αποτέλεσμα την βαθύτερης εφαρμογής των τεχνολογιών Blockchain στον κοινωνικό ιστό.
5. **Προέλευση(Provenance):** Οι συμμετέχοντες γνωρίζουν από που προήλθαν τα περιουσιακά στοιχεία και πως έχει αλλάξει η κυριότητά τους στο χρόνο.
6. **Μη-μεταβλητότητα (Immutability):** Κανένας από τους συμμετέχοντες δεν μπορεί να μεταβάλει κάποια συναλλαγή η οποία έχει καταγραφεί στο κοινόχρηστο μητρώο (ledger). Εάν μία συναλλαγή είναι λάθος ή υπάρχει κάποιο λάθος σε αυτή τότε, μία νέα συναλλαγή πρέπει να υπάρξει για να μπορέσει να αναιρεθεί το λάθος σε μια προηγούμενη συναλλαγή. Και οι δύο αυτές συναλλαγές είναι ορατές στο δίκτυο.
7. **Οριστικότητα (Finality):** Ένα κοινόχρηστο μητρώο (ledger) αποτελεί το μέρος όπου κάποιος μπορεί να επαληθεύσει την κυριότητα ενός περιουσιακού στοιχείου καθώς και την ολοκλήρωση μιας συναλλαγής.

# 9 ETHEREUM BLOCKCHAIN

Το Ethereum είναι μια δημόσια, κατανεμημένη, ανοιχτού κώδικα υπολογιστική πλατφόρμα βασισμένη στην τεχνολογία Blockchain**.** Χρησιμοποιεί το Blockchain για την αποθήκευση όχι μόνο της κατάστασης των λογαριασμών των χρηστών, αλλά και του προγραμματιστικού κώδικα καθώς και της σχετιζόμενης κατάστασής στην οποία βρίσκεται. Σχεδιάστηκε, για να επιτρέπει σε οποιονδήποτε να γράψει έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές. Υποστηρίζει πολλές γλώσσες προγραμματισμού δέσμης ενεργειών(scripting) οι οποίες μπορούν να μεταγλωττιστούν σε byte κώδικα που εκτελείται στην εικονική μηχανή Ethereum(Ethereum Virtual Machine -EVM)

Μία αποκεντρωμένη εφαρμογή (DApp) εξυπηρετεί ένα συγκεκριμένο σκοπό για τους χρήστες της ,όπως για παράδειγμα το Bitcoin είναι μια αποκεντρωμένη εφαρμογή ηλεκτρονικών πληρωμών που επιτρέπει στους χρήστες της να κάνουν online πληρωμές μέσω Bitcoin.

Επειδή οι αποκεντρωμένες εφαρμογές αποτελούνται από κώδικα που λειτουργεί σε Blockchain, δεν ελέγχονται από κάποια μεμονωμένη κεντρική οντότητα. Οποιαδήποτε υπηρεσία που είναι κεντρικοποιημένη, όπως για παράδειγμα τα δάνεια που χορηγούν οι τράπεζες, τα συστήματα ψηφοφορίας κτλ. μπορούν να υιοθετήσουν την συγκεκριμένη τεχνολογία.

Το Blockchain του Ethereum είναι μια Turing Complete[6] κατανεμημένη υπολογιστική αρχιτεκτονική, στην οποία κάθε κόμβος του δικτύου εκτελεί και καταγράφει τις ίδιες συναλλαγές, οι οποίες οργανώνονται σε μπλοκ και προστίθενται στο Blockchain. Μόνο ένα μπλοκ μπορεί να προστεθεί κάθε φορά και κάθε μπλοκ περιέχει την απόδειξη εργασίας (Proof of Work), αν και λόγω προβλημάτων όπως ή μεγάλη κατανάλωση ισχύος, προτείνεται η μετάβαση στο σύστημα απόδειξης συμμετοχής(Proof of Stake). Οι κόμβοι που συντηρούν το δίκτυο, δηλαδή αυτοί που δημιουργούν τα μπλοκ ονομάζονται miners.

Η καινοτομία του Ethereum σε σχέση με το Bitcoin, είναι πως το Ethereum αποτελεί μία πιο ευέλικτη και προσαρμόσιμη πλατφόρμα, πάνω στην οποία μπορούν να δημιουργηθούν και να λειτουργήσουν με ασφάλεια αποκεντρωμένες εφαρμογές, ενώ το Bitcoin παρέχει κυρίως τη δυνατότητα οικονομικών συναλλαγών του κρυπτονομίσματος Bitcoin. Η γλώσσα δέσμης ενεργειών(Scripting Language) του Bitcoin δεν είναι Turing Complete, διότι ο κώδικας των

[6] Οποιοδήποτε σύστημα ή γλώσσα προγραμματισμού που είναι σε θέση να υπολογίσει οτιδήποτε υπολογίσιμο, δεδομένου ότι διαθέτει επαρκείς πόρους, λέγεται ότι είναι Turing Complete.

συμβολαίων περιέχει πολύπλοκους υπολογισμούς, όπως επαναληπτικές διαδικασίες, το οποίο χρησιμοποιεί μεγάλης ισχύς υπολογιστικούς πόρους καθώς και άπειρους βρόχους. Επομένως, μια αποκεντρωμένη πλατφόρμα, χωρίς δικαιώματα, πρέπει να αποφύγει τα ανεπιθύμητα μηνύματα για να είναι εφικτή. Η πλατφόρμα Ethereum λύνει αυτό το πρόβλημα, απαιτώντας την καταβολή "τέλους" για τα συμβόλαια, το οποίο θα καταναλώνεται από τους κόμβους, ώστε να ταιριάζουν με το κόστος επαλήθευσης του script. Ανάλογα με την πολυπλοκότητα του script και τον τρόπο με τον οποίο η εκτέλεση του συμβολαίου επεκτείνεται σε περισσότερους υπολογισμούς, τα συμβόλαια του Ethereum μπορεί να εξαντλήσουν όλο το "τέλος"(gas) και να απαιτείται επιπλέον καταθέσεις.

## 9.1 ETHEREUM VIRTUAL MACHINE -EVM

Όπως αναφέρθηκε και πριν, το Ethereum δεν παρέχει στους χρήστες απλά ένα προκαθορισμένο σύνολο λειτουργιών, όπως κάνει το Bitcoin, αλλά αντιθέτως τους παρέχει τη δυνατότητα να ορίσουν δικές τους λειτουργίες και κατ' επέκταση έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές. Η εικονική μηχανή του Ethereum επιτρέπει στους κόμβους του δικτύου να αποθηκεύουν και να επεξεργάζονται δεδομένα με αντάλλαγμα την πληρωμή, παρέχοντάς τους τη δυνατότητα να ανταποκρίνονται σε γεγονότα πραγματικού κόσμου, καθώς και νέες ευκαιρίες για την υποστήριξη εφαρμογών στην διαδικασία της αλυσίδας αξίας, κάτι το οποίο δεν ήταν διαθέσιμο για χρήστες και προγραμματιστές του πραγματικού κόσμου.

Η εικονική αυτή μηχανή επικεντρώνεται στην παροχή ασφάλειας και στην εκτέλεση κώδικα που δεν είναι αξιόπιστος από υπολογιστές σε όλο τον κόσμο. Παράλληλα, επικεντρώνεται στην αποτροπή των επιθέσεων άρνησης εξυπηρέτησης (Denial-of-service), οι οποίες έχουν γίνει κοινό φαινόμενο στο κόσμο των κρυπτονομισμάτων. Επιπλέον, η EVM, η οποία μπορεί να εκτελεί κώδικα αυθαίρετης αλγοριθμικής πολυπλοκότητας, εξασφαλίζει ότι τα προγράμματα δεν έχουν πρόσβαση στην κατάσταση του άλλου, εξασφαλίζοντας ότι η επικοινωνία μπορεί να πραγματοποιηθεί χωρίς πιθανή παρεμβολή.

Όπως και τα άλλα Blockchain, το Ethereum περιλαμβάνει ένα πρωτόκολλο δικτύου ομότιμων κόμβων. Το πρωτόκολλο αυτό είναι υπεύθυνο για τον συντονισμό των συνδεδεμένων κόμβων, με σκοπό την απρόσκοπτη λειτουργία του δικτύου. Κάθε κόμβος τρέχει το EVM και

εκτελεί τις ίδιες εντολές. Η μεγάλη αυτή παραλληλοποίηση των υπολογισμών δεν έχει σκοπό την απόδοση, αφού οι υπολογισμοί είναι πολύ πιο αργοί και ακριβοί απ' ότι θα γινόταν σε έναν απλό υπολογιστή, σκοπό έχει την ύπαρξη ομοφωνίας/συναίνεσης(consensus). Αυτό το χαρακτηριστικό δίνει στο Ethereum πολύ μεγάλη αντοχή σε σφάλματα, αδιάλειπτη λειτουργία και εγγυάται ότι τα δεδομένα μέσα στο Blockchain θα μείνουν αμετάβλητα.

Η εικονική μηχανή του Ethereum, δίνει τη δυνατότητα σε οποιονδήποτε χρήστη να εκτελέσει οποιοδήποτε πρόγραμμα, ανεξάρτητα από τη γλώσσα προγραμματισμού δεδομένων των πόρων και της υπολογιστικής ισχύς που χρησιμοποιεί. Με τη χρήση της συγκεκριμένης εικονικής μηχανής, η διαδικασία δημιουργίας εφαρμογών Blockchain γίνεται πιο εύκολη και αποτελεσματική. Για το λόγο αυτό, αντί να χρειαστεί να δημιουργηθεί ένα νέο πρωτότυπο Blockchain για κάθε νέα εφαρμογή, το Ethereum επιτρέπει την ανάπτυξη χιλιάδων διαφορετικών εφαρμογών, με τη χρήση μιας μόνο πλατφόρμας.

## 9.2 ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ETHEREUM

Η δομή του Ethereum είναι παρόμοια με αυτή του Bitcoin καθώς είναι ένα κοινό ιστορικό ολόκληρου του ιστορικού των συναλλαγών. Κάθε κόμβος στο δίκτυο αποθηκεύει ένα αντίγραφο αυτού του ιστορικού. Βασική διαφορά τους είναι ότι στο Ethereum, βασική μονάδα είναι ο λογαριασμός(account) ενώ στο Bitcoin, η λίστα των συναλλαγών (list of transactions).

Στο Ethereum blockchain παρακολουθείται η κατάσταση κάθε λογαριασμού και όλες οι μεταβάσεις κατάστασης, είναι μεταβιβάσεις αξίας και πληροφορίας μεταξύ των λογαριασμών. Υπάρχουν δύο είδη λογαριασμών:

1) Οι Externally Owned Accounts (Ds), οι οποίοι ελέγχονται από ιδιωτικά κλειδιά και ανήκουν σε μια εξωτερική οντότητα.
2) Οι λογαριασμοί συμβολαίων, οι οποίοι ελέγχονται από τον κώδικα του συμβολαίου και μπορούν να "ενεργοποιηθούν" μόνο από έναν EOA.

Οι EOA ελέγχονται από τους ανθρώπους που κατέχουν και ελέγχουν τα ιδιωτικά κλειδιά, ενώ οι λογαριασμοί συμβολαίων "ελέγχονται" από τον κώδικά τους. Ο "έλεγχος" των έξυπνων συμβολαίων προκύπτει από τον τρόπο που έχουν προγραμματιστεί να ελέγχονται από έναν EOA με μια συγκεκριμένη διεύθυνση, η οποία με τη σειρά της ελέγχεται από όποιον κατέχει τα ιδιωτικά

κλειδιά που ελέγχουν αυτόν τον EOA. Ο δημοφιλής όρος "έξυπνο συμβόλαιο" είναι πρακτικά ο κώδικας του λογαριασμού συμβολαίου, δηλαδή το πρόγραμμα που εκτελείται όταν μια συναλλαγή σταλεί στον λογαριασμό αυτό. Οι χρήστες που κατέχουν EOA, μπορούν να δημιουργήσουν νέα συμβόλαια, δημοσιεύοντάς τα στο Blockchain.

Οι χρήστες(λογαριασμοί EOA) στέλνουν συναλλαγές στο διαδίκτυο του Ethereum, υπογράφοντας τα δεδομένα της συναλλαγής με το ιδιωτικό τους κλειδί, χρησιμοποιώντας την κρυπτογραφία ελλειπτικών καμπυλών(ECDSA). Μια συναλλαγή είναι έγκυρη μόνο εάν είναι υπογεγραμμένη από τον αποστολέα της(από το ιδιωτικό του κλειδί). Σαν αποτέλεσμα, το δίκτυο είναι σίγουρο ότι ο αποστολέας της συναλλαγής είναι αυτός που ισχυρίζεται και όχι κάποιος κακόβουλος χρήστης.

Όπως και στο Bitcoin οι χρήστες πρέπει να πληρώσουν μικρά "τέλη" συναλλαγών στο δίκτυο. Αυτό προστατεύει το Blockchain του Ethereum από επιπόλαιες ή κακόβουλες υπολογιστικές διαδικασίες, όπως DDoS ή άπειρους βρόχους. Ο αποστολέας μιας συναλλαγής πρέπει να πληρώσει για κάθε βήμα του "προγράμματος" που ενεργοποίησε, συμπεριλαμβανομένης της υπολογιστικής ισχύς που χρησιμοποιήθηκε καθώς και του αποθηκευτικού χώρου. Το "τέλος" αυτό (gas) πληρώνεται σε κρυπτονόμισμα του Ethereum, το Ether. Τα "τέλη" εισπράττονται από τους κόμβους που επικυρώνουν το δίκτυο, τους miners.

Η EVM δεν κάνει διάκριση μεταξύ των δύο τύπων λογαριασμού. Κάθε λογαριασμός έχει αποθήκες κλειδιών-τιμών(key-value stores) τα οποία περιλαμβάνουν την αποθήκευση και το υπόλοιπο σε Wei τα οποία μπορεί να αλλάξουν, πραγματοποιώντας συναλλαγές που περιέχουν Ether.

## 9.3 ETHER

Η ποσότητα gas που απαιτείται μπορεί να αγοραστεί με ανταλλαγή Ether. Οι τιμές του gas είναι χαμηλές και αγοράζονται σε Wei, την ελάχιστη υποδιαίρεση του Ether(1 Ether = $10^{18}$ Wei). Η τιμή του gas είναι κυμαινόμενη και διέπεται από το νόμο προσφοράς και ζήτησης που υπάρχει στο δίκτυο του Ethereum.

ΕΙΚΟΝΑ 12: 'ETHER' Η ΚΙΝΗΤΗΡΙΟΣ ΔΥΝΑΜΗ ΤΟΥ ETHEREUM [67]

Μια συναλλαγή μπορεί να είναι οτιδήποτε, από τη μεταφορά κεφαλαίων μεταξύ των λογαριασμών έως την εκτέλεση έξυπνων συμβολαίων. Έτσι, εάν ο χρήστης Χ επιθυμεί να στείλει μια ποσότητα Ether Ε στον χρήστη Υ, ο χρήστης Χ θα στείλει την ποσότητα Ε και την προεπιλεγμένη τιμή ποσότητα gas, όπου η προεπιλεγμένη τιμή του gas καθορίζεται από ένα σύνολο ενεργειών που εμπλέκονται στην εκτέλεση μιας συναλλαγής, όπως η κρυπτογράφηση SHA3 και ο όγκος των δεδομένων που υπάρχουν στην συναλλαγή. Κάθε 256 bits δεδομένων τα οποία πρόκειται να κατακερματιστούν, αντιπροσωπεύουν 6 μονάδες gas.

Αυτό το κόστος συναλλαγής μπορεί να θεωρηθεί ως η αγορά χώρου ή ως η τιμή που απαιτείται για να συμπεριληφθεί η συναλλαγή αυτή σε ένα μπλοκ που εξορύσσεται από έναν miner. Το επιπλέον gas που παραμένει μετά την εκτέλεση της συναλλαγής παρέχεται στο miner από το δίκτυο επιπλέον της ανταμοιβής εξόρυξης. Ένας miner έχει την ελευθερία να επιλέξει αν θα συμπεριλάβει μια συγκεκριμένη συναλλαγή στο μπλοκ του ή όχι. Ως εκ τούτου, όσο περισσότερο το επιπλέον gas που αποστέλλεται με την συναλλαγή, τόσο αυξάνεται η πιθανότητα να πραγματοποιηθεί η εξόρυξη νωρίτερα. Η αποστολή ανεπαρκούς ποσότητας gas με μια συναλλαγή, μπορεί να αποθαρρύνει τους miners να συμπεριλάβουν αυτή τη συναλλαγή στο μπλοκ τους, οδηγώντας έτσι σε μεγαλύτερο χρόνο συναλλαγής.

Κάθε φορά που ένας miner εισάγει ένα νέο μπλοκ στο δίκτυο λαμβάνει τα Ether που αντιστοιχούν στις συναλλαγές που περιέχει το μπλοκ. Αυτό το ποσόν είναι που δίνει κίνητρο στους miners να εκτελούν την εργασία αυτή. Οι miners είναι κόμβοι του δικτύου που λαμβάνουν, διαδίδουν, επικυρώνουν και εκτελούν συναλλαγές. Συγκεντρώνουν ορισμένες συναλλαγές κάθε φορά σε μπλοκ και στη συνέχεια ανταγωνίζονται τους υπόλοιπους miners ώστε αυτοί να το εισάγουν στο Blockchain.

## 9.4 ETHEREUM ΚΑΙ ΕΞΟΡΥΞΗ

Το Blockchain του Ethereum έχει πολλές ομοιότητες με αυτό του Bitcoin. Η πιο σημαντική διαφορά είναι πως ένα μπλοκ περιέχει όχι μόνο έναν κατάλογο συναλλαγών αλλά και ολόκληρη την κατάσταση του δικτύου. Η κατάσταση αποθηκεύεται σε μια δομή δεδομένων που ονομάζεται “Patricia Tree”.

Το Patricia Tree είναι ένα τροποποιημένο Merkle Tree το οποίο είναι βελτιστοποιημένο ως προς την εισαγωγή και τη διαγραφή κόμβων. Καταγράφει την κατάσταση όλων των συμβολαίων και των EOA. Κάθε μπλοκ αποθηκεύει μια αναφορά στη ρίζα(root) του δέντρου και ενημερώνει μόνο τα τμήματα που αλλάζουν λόγω των επιδράσεων των συναλλαγών σε αυτό το μπλοκ. Αυτό επιτρέπει στους νέους κόμβους να κατεβάζουν μόνο το Patricia Tree αντί για όλα τα μπλοκ με σκοπό να ανακτήσουν την κατάσταση όλων των λογαριασμών, κάτι το οποίο εξοικονομεί σημαντικό χώρο στο δίσκο.

Για να εισαχθεί ένα νέο μπλοκ στο Blockchain θα πρέπει να συνοδεύεται από την απόδειξη εργασίας(nonce). Αυτό αποτελεί τη λύση ενός δύσκολου μαθηματικού προβλήματος, όπως γίνεται και στο Bitcoin. Η διαφοροποίηση του Ethereum έγκειται στο γεγονός ότι το πρόβλημα αυτό έχει μεγάλες απαιτήσεις μνήμης, έτσι για την εξόρυξη είναι απαραίτητα και η CPU και η μνήμη, ενώ στο Bitcoin απαιτείται μόνο η GPU.

Το Ethereum χρησιμοποιεί επίσης έναν διαφορετικό αλγόριθμο Proof-of-Work, ο οποίος ονομάζεται Ethash και παράγει ένα μπλοκ κάθε 12 δευτερόλεπτα κατά μέσο όρο, σε σύγκριση με το Bitcoin, όπου είναι 10 λεπτά. Αυτό έχει το πλεονέκτημα ότι οι συναλλαγές μπορούν να επεξεργαστούν γρηγορότερα και ο παραλήπτης μιας συναλλαγής δεν χρειάζεται να περιμένει πολύ μέχρι να θεωρήσει ότι μια συναλλαγή είναι ασφαλής. Επίσης, αυξάνει την αλληλεπίδραση των εφαρμογών οι οποίες αλληλεπιδρούν με τα συμβόλαια στο Blockchain. Επιπλέον, ο Ethash είναι “memory-hard” κάτι το οποίο τον κάνει ανθεκτικό σε ολοκληρωμένα κυκλώματα ειδικών εφαρμογών(Application-Specific Integrated Circuits-ASICs). Το αποτέλεσμα λοιπόν, είναι ότι η απόδειξη εργασίας(PoW) του Ethereum είναι πιο ανθεκτική απέναντι σε ASICs, οδηγώντας σε μεγαλύτερη αποκεντροποίηση του δικτύου, δηλαδή σε μεγαλύτερη ασφάλεια(πολλοί και μικροί miners αντί λίγοι και ισχυροί).

# 10 ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ(SMART CONTRACTS)

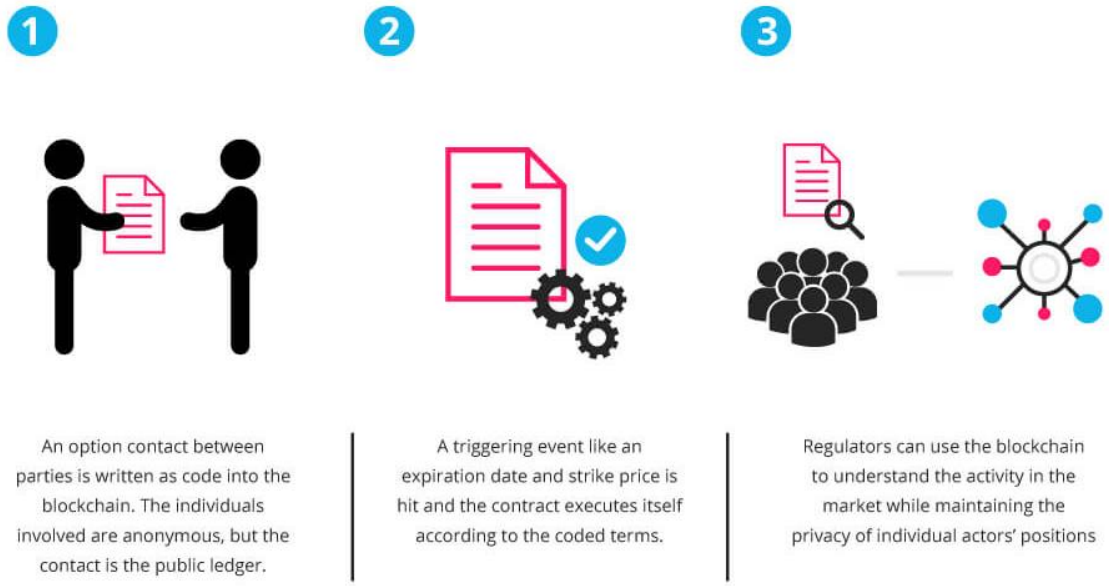
Ένα από τα βασικότερα πλεονεκτήματα της τεχνολογίας Blockchain είναι ότι, επειδή αποτελεί ένα αποκεντρικοποιημένο σύστημα το οποίο υπάρχει ανάμεσα σε όλα τα μέρη που συμμετέχουν σε ένα σύστημα, δεν υπάρχει ανάγκη για μεσάζοντες (Middlemen), οι οποίοι απαιτούν κόστος, χρόνο και μερικές φορές δημιουργούνται συγκρούσεις. Τα συστήματα που υιοθετούν την τεχνολογία blockchain πιθανόν να αντιμετωπίσουν κάποια προβλήματα, παρόλα αυτά έχουν αξιολογηθεί ότι είναι αναμφισβήτητα, ταχύτερα, ασφαλέστερα και φθηνότερα από τα παραδοσιακά συστήματα, για αυτό οι τράπεζες και οι κυβερνήσεις στρέφονται προς αυτά.

Το 1994, ο Nick Szabo[7], ένας νομικός μελετητής και κρυπτογράφος, συνειδητοποίησε ότι ένα αποκεντρωμένο μητρώο (ledger), θα μπορούσε να χρησιμοποιηθεί για έξυπνες συμβάσεις και συμβόλαια (Smart Contracts), αυτο-εκτελούμενα συμβόλαια, ψηφιακά συμβόλαια και συμβάσεις blockchain. Σε αυτή τη μορφή, τα συμβόλαια θα μπορούσαν να μετατραπούν σε κώδικα υπολογιστή, να αποθηκευτούν και να αναπαραχθούν στο σύστημα και να εποπτευθούν από τους υπολογιστές ενός δικτύου που τρέχουν σε blockchain.

Οι έξυπνες συμβάσεις μπορούν να οριστούν σαν ένα σύνολο από κανόνες που καθορίζουν τον τρόπο που πρέπει να πραγματοποιηθεί μια συναλλαγή σε ένα δίκτυο blockchain. Τα έξυπνα συμβόλαια επεκτείνουν τη λειτουργικότητα του blockchain με τη μοντελοποίηση σεναρίων του πραγματικού κόσμου χρησιμοποιώντας γλώσσες προγραμματισμού υψηλού επιπέδου. Ένα έξυπνο συμβόλαιο μόλις αξιοποιηθεί ο κώδικάς του δεν μπορεί να μεταβληθεί. Η εκτέλεση ενός έξυπνου συμβολαίου μπορεί να αντιμετωπιστεί σαν μία συναλλαγή.

Σκοπός τους είναι να παρέχουν ασφάλεια σε σχέση με τις παραδοσιακές μεθόδους, μειώνοντας παράλληλα το κόστος. Για παράδειγμα, ένα έξυπνο συμβόλαιο μπορεί να καθορίσει τους όρους με τους οποίους θα γίνει μια μεταφορά εταιρικών ομολόγων, ή ακόμα τους όρους και τις προϋποθέσεις ασφαλιστικής κάλυψης σε ένα ταξίδι, οι οποίοι θα ενεργοποιηθούν αυτόματα αν καθυστερήσει μία πτήση.

[7] https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/




ΕΙΚΟΝΑ 13: Η ΛΕΙΤΟΥΡΓΙΑ ΕΝΟΣ SMART CONTRACT [23]

Για να γίνει πιο κατανοητός ο τρόπος που λειτουργούν τα έξυπνα συμβόλαια ας υποθέσουμε ότι ο Β ενοικιάζει μία κατοικία από τον Α. Η συναλλαγή αυτή μπορεί να γίνει μέσω blockchain με τη χρήση κρυπτονομισμάτων. Ο Β λαμβάνει μια εικονική απόδειξη από το μεταξύ τους ψηφιακό συμβόλαιο. Ο Α υποχρεούται με βάση τους όρους του συμβολαίου να παρέχει στον Β ένα ψηφιακό κλειδί για την κατοικία έως μία συγκεκριμένη ημερομηνία, η οποία ορίζεται από το συμβόλαιο. Εάν για τον οποιοδήποτε λόγο καθυστερήσει η αποστολή του ψηφιακού κλειδιού το blockchain αυτόματα επιστρέφει τα χρήματα. Ακόμα, στην περίπτωση που ο Α αποστείλει το ψηφιακό κλειδί νωρίτερα από τη συμφωνημένη ημερομηνία το σύστημα επιτρέπει την παραλαβή του κλειδιού από τον Β όσο και τη χρέωσή του, στη συμφωνημένη ημερομηνία. Το σύστημα βασίζεται στις αρχές του If-Then και ελέγχεται από εκατοντάδες ανθρώπους, γεγονός που σημαίνει ότι είναι πολύ αξιόπιστο, σε θέματα συναλλαγών. Εν προκειμένω, εάν ο Α αποστείλει το ψηφιακό κλειδί, μπορεί να είναι βέβαιος για την πληρωμή του, ενώ εφόσον ο Β «καταθέσει» το απαραίτητο ποσό σε bitcoin, τότε είναι σίγουρος για την παραλαβή του κλειδιού. Τέλος το συμβόλαιο αυτό μετά από κάποιο χρονικό περιθώριο ακυρώνεται και δεν μπορεί να τροποποιηθεί κατά τον οποιοδήποτε τρόπο, από κανένα από τους συμμετέχοντες, καθώς όλοι ενημερώνονται ταυτόχρονα για τις πραγματοποιούμενες αλλαγές. Αυτό είναι απλά ένα παράδειγμα για τη χρήση

των bitcoins, καθώς όπως γίνεται κατανοητό η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί σε πληθώρα περιπτώσεων.

Η χρήση των έξυπνων συμβολαίων έχει πολλά πλεονεκτήματα τα οποία μπορούν αν αξιοποιηθούν σωστά να αλλάξουν τον τρόπο που χρησιμοποιούνται τα συμβόλαια. Ο συνδυασμός έξυπνων συμβολαίων και της τεχνολογίας blockchain προσφέρει αυτονομία και εξοικονόμηση πόρων του χρήστη, καθώς ο κάθε χρήστης είναι αυτός που πραγματοποιεί τη συμφωνία, χωρίς τη διαμεσολάβηση τρίτων (πχ. δικηγόρων ή μεσιτών). Ακόμα ο συνδυασμός αυτός προσφέρει ασφάλεια και εμπιστοσύνη, καθώς τα προσωπικά δεδομένα και έγγραφα βρίσκονται κωδικοποιημένα σε μια κοινόχρηστη πλατφόρμα και με αυτόν τον τρόπο εξασφαλίζεται επίσης επαρκές backup καθώς τα έγγραφα και τα δεδομένα βρίσκονται σε πολλά ψηφιακά αντίγραφα. Τέλος είναι εύκολα κατανοητό ότι η ψηφιοποίηση των συμβολαίων είναι πολύ πιο έγκυρη από τα κλασσικά χειρόγραφα συμβόλαια, ενώ προφυλάσσει το χρήστη από πιθανά λάθη που μπορούν να προκύψουν από τη χειρόγραφη συμπλήρωση συμβολαίου.

# 11 DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)

Η έννοια του Decentralized Autonomous Organization – DAO ή αλλιώς Αποκεντρωμένη Αυτόνομη Οργάνωση προτάθηκε για πρώτη φορά από τον Daniel Larimer [24] σε ένα άρθρο του που δημοσιεύτηκε τον Σεπτέμβριο του 2013. Ο DAO αποτελεί ένα Smart Contract ή μια συλλογή από Smart Contracts τα οποία μπορούν να αναπαραστήσουν έναν οργανισμό σε ένα δίκτυο blockchain, αυτοματοποιώντας τη διαδικασία λήψης αποφάσεων καθώς και την διοίκηση ενός οργανισμού.

Μια Αποκεντρωμένη Αυτόνομη Οργάνωση, όπως κάθε άλλος οργανισμός, αποτελείται από μέλη τα οποία έχουν τη δυνατότητα να αντλούν κεφάλαια και να προτείνουν διαφορετικά είδη προτάσεων. Οι προτάσεις αυτές μπορεί να αφορούν οτιδήποτε, από τη μεταφορά χρημάτων μέχρι την εκτέλεση άλλων έξυπνων συμβολαίων.

Η ιδέα της Αποκεντρωμένης Αυτόνομης Οργάνωσης υλοποιήθηκε για πρώτη φορά το 2016, από μια ομάδα προγραμματιστών οι οποίοι δημιούργησαν το γνωστό “The DAO”. Ο “The DAO” ήταν ένας οργανισμός που σχεδιάστηκε για να είναι αυτοματοποιημένος και αποκεντρωμένος. Έδρασε ως οργανισμός που διαχειρίζεται και επενδύει κεφάλαια επιχειρηματικού κινδύνου

(Venture Capital Funds), βασισμένη σε πλατφόρμα ανοιχτού κώδικα και χωρίς τυπική μορφή διοίκησης ή κάποιο διοικητικό συμβούλιο, το οποίο θα είχε την εποπτεία αυτού του εγχειρήματος. Οι υπεύθυνοι που ανέπτυξαν το "the DAO" πίστεψαν ότι μέσω αυτού θα μπορούσαν να εξαλείψουν το ανθρώπινο λάθος ή την χειραγώγηση των κεφαλαίων των επενδυτών, τοποθετώντας την δύναμη της λήψης αποφάσεων στα χέρια ενός αυτοματοποιημένου συστήματος με πολλού συμμετέχοντες. Μέχρι τον Απρίλη του 2016 είχε συγκεντρώσει πάνω από 150 εκατομμύρια δολάρια για επενδύσεις οπότε και δημοσιεύτηκε ένα άρθρο που αφορούσε τις αδυναμίες ασφαλείας που είχε. Βάσει αυτών των τρωτών σημείων μια ομάδα hackers επιτέθηκε στο "The DAO" και απέκτησε πρόσβαση σε περίπου 50 εκατομμύρια δολάρια την εποχή εκείνη. [25]

Παρόλη την αδυναμία που επέδειξε το project "The DAO", οι δυνατότητες που μπορεί να αντλήσουν οι επιχειρήσεις που θέλουν να υιοθετήσουν ένα αποκεντρωμένο σύστημα οργάνωσης είναι αμέτρητες. Τα συστήματα DAO μπορούν να επιφέρουν πολλά πλεονεκτήματα και να εξελίξουν τον παραδοσιακό τρόπο οργανωσιακής διοίκησης μέσα από συστήματα λήψης αποφάσεων, συμμετοχής των ενδιαφερόμενων μερών του εσωτερικού και εξωτερικού περιβάλλοντος, συνεργατικότητας αλλά και με έναν διαφανή τρόπο με τον οποίο παίρνονται οι διάφορες αποφάσεις σε έναν οργανισμό .

## 12 DECENTRALIZED APPLICATIONS (DApps)

Μια αποκεντρωμένη εφαρμογή (Decentralized Application-DApp) είναι μια εφαρμογή που εκτελείται σε ένα δίκτυο ομότιμων χρηστών(Peer-to-Peer network), σε αντίθεση με έναν υπολογιστή και συνδέεται συχνά με το "Ethereum Project". Το βασικό όφελος από αυτό είναι ότι οι χρήστες του δικτύου, δεν εξαρτώνται από έναν κεντρικό υπολογιστή για την αποστολή και λήψη πληροφοριών. Για να θεωρηθεί μια εφαρμογή ως DApp θα πρέπει να πληροί τα ακόλουθα κριτήρια:

1. Η εφαρμογή θα πρέπει να πλήρως ανοιχτού κώδικα, πρέπει να λειτουργεί αυτόνομα και χωρίς να ελέγχει την πλειοψηφία των token. Η εφαρμογή μπορεί να προσαρμόσει το πρωτόκολλό της ώστε να ανταποκριθεί στις προτεινόμενες βελτιώσεις και στην

ανατροφοδότηση της αγοράς, αλλά όλες οι αλλαγές πρέπει να αποφασιστούν με συναίνεση των χρηστών της.

2. Τα δεδομένα της εφαρμογής και τα αρχεία λειτουργίας της πρέπει να αποθηκεύονται αφού κρυπτογραφηθούν, σε ένα δημόσιο, αποκεντρωμένο Blockchain προκειμένου να αποφευχθούν κεντρικά σημεία αποτυχίας.
3. Η εφαρμογή πρέπει να χρησιμοποιεί ένα κρυπτογραφικό κλειδί(token)- το Bitcoin ή ένα token που είναι εγγενές στο σύστημά του, το οποίο είναι απαραίτητο για την πρόσβαση στην εφαρμογή και οποιαδήποτε συμβολή αξίας από τους miners θα πρέπει να επιβραβεύεται σε token της εφαρμογής.
4. Η εφαρμογή θα πρέπει να παράγει token σύμφωνα με ένα πρότυπο κρυπτογραφικό αλγόριθμο που λειτουργεί ως απόδειξη της συμβολής των κόμβων αξίας στην εφαρμογή(όπως το Bitcoin χρησιμοποιεί τον αλγόριθμο Proof of Work).

# 13 ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN: ΕΠΑΝΑΣΤΑΤΙΚΗ Η ΕΞΕΛΙΚΤΙΚΗ ΤΕΧΝΟΛΟΓΙΑ;

Τα βασικά εργαλεία και έννοιες στις οποίες στηρίζεται το blockchain, όπως η κοινή βάση δεδομένων, οι συναλλαγές μεταξύ ομότιμων χρηστών, κτλ. δεν έκαναν τώρα την εμφάνισή τους. Τεχνολογίες όπως αυτή των torrent, χρησιμοποιούν ήδη αυτά τα εργαλεία. Αυτό που τροφοδότησε την τεχνολογία blockchain, είναι η διαθεσιμότητα φθηνών συσκευών διαδικτύου. Δεδομένου ότι αυτές οι συσκευές και τα εργαλεία, μπορούν να αγοραστούν και να εγκατασταθούν από τις επιχειρήσεις χωρίς να καταβληθούν μεγάλα χρηματικά ποσά, έχει υπάρξει μια στροφή προς αυτή την κατεύθυνση της τεχνολογίας για την πραγματοποίηση συναλλαγών. Για το λόγο αυτό, πολλοί ειδικοί υποστηρίζουν ότι το blockchain είναι απλά το επόμενο βήμα στην εξέλιξη των τεχνολογιών που υπάρχουν εδώ και πολύ καιρό.

Άλλοι ειδικοί υποστηρίζουν την άποψη, πως εάν το blockchain μπορεί να θεωρηθεί μια εξελικτική ή επαναστατική τεχνολογία, εξαρτάται από την χρήση στην οποία θα τεθεί, καθώς και από το είδος των επιχειρήσεων από τις οποίες θα υιοθετηθεί. Για παράδειγμα, στον κλάδο των τραπεζών, των κατασκευών και της εφοδιαστικής αλυσίδας θα μπορούσε να αποδειχτεί

επαναστατική. Νέες χρήσεις όπως η ασφαλής καταγραφή συναλλαγών και η έξυπνη δημιουργία συμβολαίων, θα τροποποιήσουν τον τρόπο που οι επιχειρήσεις διεξάγουν τις δραστηριότητές τους.

Οι άλλες δύο τεχνολογίες που γίνονται δημοφιλείς είναι η Τεχνητή Νοημοσύνη (Artificial Intelligence - AI) και το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT). Η Τεχνητή Νοημοσύνη, η οποία είναι μια επέκταση της μηχανικής μάθησης υπόσχεται να διαχειριστεί και να επεξεργαστεί τα Μεγάλα Δεδομένα (Big Data) και να καταλήξει σε μία λογική απόφαση. Η επεξεργασία τέτοιου μεγάλου όγκου δεδομένων από τον ανθρώπινο παράγοντα, είναι πέρα από τις ικανότητές του. Το IoT επιτρέπει στις μηχανές να επικοινωνούν με το ίντερνετ και να ανταλλάσσουν πληροφορίες αυτόνομα.

Ο συνδυασμός του blockchain με την τεχνητή νοημοσύνη αλλά και το Διαδίκτυο των πραγμάτων θα κάνει μια πραγματική επανάσταση. Συσκευές τεχνητής νοημοσύνης μπορούν με ασφάλεια και αυτονομία να έχουν πρόσβαση σε δεδομένα των συσκευών IoT και να τα επεξεργαστούν, κάτι που θα απαιτούσε μεγάλη ανθρώπινη προσπάθεια και πιθανότατα να ήταν και ακατόρθωτο. Στον κλάδο της βιομηχανίας, για παράδειγμα, η αυτόνομη και αυτόματη ανταλλαγή δεδομένων μεταξύ IoT μηχανημάτων θα μπορούσε να αποδειχτεί πολύ σημαντική για την παρακολούθηση και προσαρμογή του αποθέματος.

Κατά την έναρξη χρήσης της τεχνολογίας IoT πολλοί ειδικοί ανησυχούσαν για το πόσο ασφαλής ήταν η σύνδεση συσκευών στο ίντερνετ. Οι ανησυχίες αυτές μπορούν τώρα να αντιμετωπιστούν με την εφαρμογή της τεχνολογίας blockchain, η οποία καθιστά αδύνατη την αλλαγή μια συναλλαγής εφόσον έχει πραγματοποιηθεί.

Συμπερασματικά, καταλήγουμε ότι ανάλογα με το πώς θα αξιοποιηθεί η νέα αυτή τεχνολογία του blockchain, θα καθοριστεί αν πρόκειται για επανάσταση ή για εξέλιξη οποιασδήποτε άλλης τεχνολογίας.

# 14 USE CASES OF BLOCKCHAIN

Η αναγκαιότητα για ανάπτυξη νέων τεχνολογιών προκύπτει από την απαίτηση των σύγχρονων κοινωνιών για την επίλυση διαφόρων προβλημάτων τα οποία εμφανίζονται στην πορεία των χρόνων. Οι νέες τεχνολογίες εξελίσσονται καθημερινά, όσο καθημερινά εμφανίζονται νέα προβλήματα, άρα είναι απαραίτητο ο ανθρώπινος παράγοντας να εξετάζει συνεχώς τις πιθανές εφαρμογές των νέων μορφών τεχνολογίας στην καθημερινότητα του. Παραδείγματος χάριν η

τεχνολογία του Blockchain δεδομένων των κύριων χαρακτηριστικών της δομήθηκε ώστε να προσφέρει αξιοπιστία, μη αμφισβητούμενη κυριότητα καθώς και ασφάλεια παρακολούθησης ενός δεδομένου. Πολλές νεοφυείς επιχειρήσεις και εταιρείες από διάφορους τομείς και βιομηχανικούς κλάδους, εξετάζουν τις ευκαιρίες και τις απειλές ώστε να υιοθετήσουν την τεχνολογία Blockchain προς την κατεύθυνση της επίλυσης των ποικίλων προβλημάτων που προκύπτουν. Στη συνέχεια αναφέρονται κάποιες κατηγορίες που έχουν διεισδύσει στον περιβάλλον της τεχνολογίας αυτής:

## 14.1 ΤΡΑΠΕΖΕΣ/ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΑ

Η τεχνολογία blockchain θα χρησιμοποιηθεί για να παρέχει πρόσβαση σε χρηματοπιστωτικές υπηρεσίες σε δισεκατομμύρια ανθρώπους σε όλο τον κόσμο, προσφέροντας ελαχιστοποίηση του χρόνου και του κόστους διακανονισμού, καθώς και των διασυνοριακών πληρωμών. Εκτός από ένα αποκεντρωμένο μέσο πληρωμών, χωρίς την ανάγκη ύπαρξης ενδιάμεσων προσώπων, η τεχνολογία έχει εφαρμογές σε ένα πλήθος υπηρεσιών του χρηματοπιστωτικού τομέα. Για παράδειγμα ο παραδοσιακός τρόπος επεξεργασίας και εκκαθάρισης συναλλαγών, εκτός από δαπανηρός, είναι και περίπλοκος και κατ' επέκταση αργός, καθώς περισσότερα μέρη ενδέχεται να εμπλέκονται για την ολοκλήρωση μιας συναλλαγής, όπως πράκτορες, θεματοφύλακες, διαχειριστές εκκαθάρισης κ.ο.κ. Κάθε ένα από αυτά τα μέρη τηρεί το δικό του αρχείο, γεγονός το οποίο εκτός από ζητήματα πρακτικότητας αυξάνει τις πιθανότητες σφαλμάτων και ανακολουθιών. Η τεχνολογία Blockchain απλοποιεί σημαντικά τη διαδικασία ενώ καθιστά περιττή την ανάγκη ύπαρξης ενδιάμεσων προσώπων. Ο χρόνος επιβεβαίωσης και εκκαθάρισης συναλλαγών μειώνεται δραματικά, ανεξάρτητα μάλιστα από τη γεωγραφική θέση των συναλλασσόμενων.

Οι διεθνείς πληρωμές που πραγματοποιούνται σήμερα, ειδικά σε διαφορετικά νομίσματα, μπορούν να πάρουν αρκετές ημέρες για να υλοποιηθούν και σε μερικές περιπτώσεις ακόμα και εβδομάδες, με πολλούς ενδιάμεσους, όπως κατά κύριο λόγο τράπεζες, αλλά και άλλους σχετικούς οργανισμούς. Με τη χρήση του blockchain όλες αυτές οι χρονοβόρες διαδικασίες μπορούν να γίνουν άμεσα, σε πραγματικό χρόνο.

Στον κλάδο των εμπορικών χρηματοοικονομικών συναλλαγών θα υπάρξει μεγάλη απήχηση διότι η διαδικασία απόκτησης εγκρίσεων από τις διάφορες νομικές οντότητες (τελωνεία, λιμενικές αρχές, μεταφορικές εταιρείες) για τη διακίνηση εμπορευμάτων θα απλοποιηθεί. Μέσω της τεχνολογίας του blockchain, οι νομικές υπηρεσίες θα μπορούν να υπογράφουν τις απαραίτητες

εγκρίσεις για αποστολή εμπορευμάτων καθώς όλοι θα είναι ενημερωμένοι για τον πότε τα εμπορεύματα παρελήφθησαν, πότε έγινε η πληρωμή από την τράπεζα του εισαγωγέα ή του εξαγωγέα. Η Barclays, ήταν η πρώτη τράπεζα που πραγματοποίησε μια τέτοια συναλλαγή τον Σεπτέμβριο 2016 σε συνεργασία με την Israelifintech Wave. Η συναλλαγή ήταν μια εγγυητική επιστολή για μεταφορά γεωργικών εμπορευμάτων αξίας 100.000 δολαρίων από την Ιρλανδική συνεταιριστική εταιρεία Ornua στην εταιρεία εμπορικών συναλλαγών στις Σεϋχέλλες.

Οι παραδοσιακές μέθοδοι χρηματοδότησης του εμπορίου αποτελούν μεγάλο αγκάθι για τις επιχειρήσεις, δεδομένου ότι οι απαραίτητες διαδικασίες είναι χρονοβόρες, επηρεάζουν την ρευστότητα των επιχειρήσεων, δυσκολεύοντας έτσι την επιχειρηματική τους δραστηριότητα. Η εξαιρετικά ασφαλής τεχνολογία του Blockchain, το καθιστά χρήσιμο στον έλεγχο και την παρακολούθηση των λογιστικών αρχείων των εταιρειών. Δεδομένου ότι δεν μπορούν να γίνουν αλλαγές στους λογαριασμούς, η ανάγκη για λογιστικούς ελεγκτές μπορεί να εκλείψει.

Το Blockchain μπορεί να συμβάλει αποτελεσματικά στην προστασία από το ξέπλυμα χρήματος. Η κρυπτογράφηση, ως αναπόσπαστο κομμάτι της τεχνολογίας αυτής, χρησιμεύει στην καταπολέμηση της νομιμοποίησης παράνομων εσόδων καθώς οι εταιρείες μπορούν να εντοπίσουν και να επαληθεύσουν την ταυτότητα και τα περιουσιακά στοιχεία των πελατών τους.

## 14.2 ΑΣΦΑΛΙΣΗ

Η παγκόσμια ασφαλιστική αγορά βασίζεται στη διαχείριση εμπιστοσύνης, οπότε το Blockchain μπορεί να χρησιμοποιηθεί για την επαλήθευση πολλών τύπων δεδομένων σε ασφαλιστικά συμβόλαια, όπως η ταυτότητα του ασφαλισμένου, αν πραγματοποιήθηκε ένα ατύχημα κτλ. Με αυτοματοποιημένη την επεξεργασία ασφαλιστικών απαιτήσεων, συντάσσονται αυτόματα οι όροι της ασφάλισης σε ένα έξυπνο συμβόλαιο (Smart Contract), το οποίο είναι αποθηκευμένο σε ένα Blockchain και είναι προσβάσιμο δημόσια μέσω του ίντερνετ. Έτσι όταν πραγματοποιηθεί ένα συμβάν και αναφερθεί από μια αξιόπιστη πηγή, τότε πραγματοποιείται αυτόματα η απαραίτητη διαδικασία, ενεργοποιώντας το ασφαλιστικό συμβόλαιο, και σύμφωνα με τους όρους του έξυπνου συμβολαίου, ο πελάτης αποζημιώνεται. Με την αυτοματοποίηση της διαδικασίας εξαλείφεται το κόστος επεξεργασίας ασφαλιστικών απαιτήσεων και μειώνονται οι ευκαιρίες για ασφαλιστική απάτη, βελτιώνοντας με αυτόν τον τρόπο την ικανοποίηση του πελάτη.

## 14.3 ΤΗΡΗΣΗ ΜΗΤΡΩΩΝ

Η εφαρμογή συστημάτων βασισμένων σε Blockchain μπορεί να μειώσει σημαντικά τη γραφειοκρατία και να αυξήσει την ασφάλεια, την αποτελεσματικότητα και τη διαφάνεια των κυβερνητικών πράξεων. Καθώς η τεχνολογία Blockchain αποτελεί ουσιαστικά ένα νέο τρόπο καταχώρησης και αποθήκευσης πληροφοριών με τέτοιο τρόπο ώστε να δημιουργείται μια αλληλένδετη αλυσίδα δεδομένων, αποτρέποντας διπλές εγγραφές, κακόπιστες καταχωρήσεις κ.α., η πιο προφανής εφαρμογή της είναι στην τήρηση μητρώων όπως το ληξιαρχείο, το κτηματολόγιο[8], μητρώο εταιρειών, φορολογικό μητρώο, μητρώο δικαιωμάτων διανοητικής ιδιοκτησίας κλπ.

Οι εθνικές, κρατικές και τοπικές κυβερνήσεις είναι υπεύθυνες για τη διατήρηση των αρχείων των ανθρώπων, όπως ημερομηνίες γέννησης και θανάτου, η οικογενειακή κατάσταση, τα περιουσιακά στοιχεία κλπ. Η διαχείριση αυτών των αρχείων μπορεί να είναι αρκετά δύσκολη, χρονοβόρα και με μεγάλο κόστος καθώς ορισμένα από αυτά τα αρχεία υπάρχουν μόνο σε έντυπη μορφή. Επίσης, σε πολλές περιπτώσεις οι πολίτες πρέπει να επισκεφτούν τα αρμόδια γραφεία για να κάνουν τροποποιήσεις στα παρεχόμενα στοιχεία τους. Η λύση σε αυτή τη δύσκολη διαχείριση των πληροφοριών βρίσκεται στο Blockchain καθώς οι πολίτες θα μπορούν δίνοντας ελάχιστες πληροφορίες(ημερομηνία γέννησης) να αποδείξουν την ταυτότητά τους.

Εκατομμύρια πρόσφυγες σε όλο τον κόσμο παραμένουν αδήλωτοι χωρίς κάποια ταυτοποίηση για τους ίδιους αλλά και για τα παιδιά τους. Οι άνθρωποι στις φτωχότερες χώρες του κόσμου μπορεί να μην έχουν επαρκή αποδεικτικά έγγραφα για την ταυτοποίησή τους, καθώς μην ξεχνάμε πως οι χώρες προέλευσης στις περισσότερες των περιπτώσεων δε διαθέτουν ικανοποιητικές δημόσιες δομές, ώστε να υπάρχουν δεδομένα που να πιστοποιούν την ταυτότητα των πολιτών τους (όπως για παράδειγμα, λογαριασμοί που να αποδεικνύουν κάποια μόνιμη κατοικία). Οι οργανισμοί και οι κυβερνήσεις μπορούν να εφαρμόσουν την τεχνολογία Blockchain με την οποία θα μπορούν να εκδώσουν ψηφιακά πιστοποιητικά γέννησης τα οποία δεν θα μπορούν να πλαστογραφηθούν και θα είναι προσβάσιμα σε όλους. Μια τέτοια υλοποίηση θα μειώσει το κόστος και το χρόνο που απαιτούνται για την επαλήθευση της ταυτότητας των πολιτών. Έτσι θα βοηθήσει στην καταπολέμηση του φαινομένου της εμπορίας ανθρώπων αφού θα υπάρξει διαφάνεια στην έκδοση επίσημων εγγράφων.

[8] https://www.ubitquity.io/web/index.html

Επιπλέον, η τεχνολογία θα μπορούσε να εφαρμοστεί σε λογιστικές καταχωρήσεις εταιρειών, καθώς μειώνει σημαντικά την πιθανότητα σφαλμάτων και εξασφαλίζει, τουλάχιστον σε βαθμό μεγαλύτερο από τις σημερινές πρακτικές, την ακεραιότητα των εγγραφών. Η τροποποίηση των εγγραφών από τη στιγμή που θα καταχωρηθούν στη βάση δεδομένων Blockchain θα είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, ακόμη και από εκείνον που τηρεί το μητρώο/αρχείο.

Σε όλες τις παραπάνω περιπτώσεις, η καταχώρηση δεδομένων μπορεί να συνδυαστεί με επιπρόσθετες λειτουργικές δυνατότητες οι οποίες ενσωματώνονται στην εκάστοτε πλατφόρμα. Για παράδειγμα, σε μια πειραματική εφαρμογή της τεχνολογίας από το χρηματιστήριο του NASDAQ το 2016[9], καταχωρήθηκε η κυριότητα κινητών αξιών των χρηστών, όπως τηρείται από την κεντρική αρχή(CSD), και στη συνέχεια αποδόθηκαν δικαιώματα ψήφου μέσω token, ώστε οι χρήστες να μπορούν να "ξοδεύουν" token και να ψηφίζουν στις συνελεύσεις εφόσον ήταν και φορείς του αντίστοιχου δικαιώματος ψήφου.

## 14.4 ΔΙΑΚΥΒΕΡΝΗΣΗ

Η τεχνολογία Blockchain θα μπορούσε ακόμα να παίξει καθοριστικό ρόλο στο πώς πραγματοποιείται μια εκλογική διαδικασία. Οι ψηφοφόροι θα μπορούσαν να εγγραφούν σε κάποιο μητρώο, η λειτουργία του οποίου θα βασίζεται στην ανωτέρω τεχνολογία, έτσι θα απλοποιηθεί η εξακρίβωση της ταυτότητας τους και με αυτόν τον τρόπο θα μπορέσει να διασφαλιστεί ότι υπολογίζονται μόνο οι νόμιμες ψήφοι. Η ψηφιακή διακυβέρνηση και ηλεκτρονική ψηφοφορία καθίσταται πλέον πολύ πιο ασφαλής καθώς εκτός από την κρυπτογράφηση των δεδομένων με την μέθοδο που καθιστά εξαιρετικά δύσκολη την παραποίησή τους, διασφαλίζεται και η διαφάνεια αφού οι συμμετέχοντες είναι σε θέση να επιβεβαιώσουν ότι οι ψήφοι τους μετρήθηκαν και ότι το περιεχόμενό τους δεν αλλοιώθηκε. Τα DemocracyEarth και FollowMyVote αποσκοπούν στη δημιουργία πιο δίκαιων και δημοκρατικών ηλεκτρονικών συστημάτων ψηφοφορίας βασισμένα σε Blockchain.

[9] https://www.coindesk.com/nasdaq-declares-blockchain-voting-trial-a-success/

Ένας άλλος τομέας στον οποίο η νέα τεχνολογία θα έβρισκε σημαντικές εφαρμογές είναι αυτός των μη κερδοσκοπικών οργανισμών, αφού οι δωρητές θα είναι σε θέση να διαπιστώσουν με βεβαιότητα και διαφάνεια πού χρησιμοποιούνται τα χρήματά τους. Πέρα αυτού, η τεχνολογία Blockchain διευκολύνει την πιο αποτελεσματική διανομή των κεφαλαίων και ενισχύει τις δυνατότητες παρακολούθησής τους.

## 14.5 ΛΙΑΝΙΚΗ ΠΩΛΗΣΗ

Οι αποκεντρωμένες υπηρεσίες λιανικής που βασίζονται σε Blockchain συνδέουν αγοραστές και πωλητές χωρίς μεσάζοντα και συναφή τέλη. Σε αυτές τις περιπτώσεις, η εμπιστοσύνη προέρχεται από τα Smart Contract Systems, την ασφάλεια των ανταλλαγών και τα ενσωματωμένα συστήματα διαχείρισης διαδικτυακής φήμης.

Σε αντίθεση με τις δημοφιλείς πλατφόρμες Uber και Airbnb, οι οποίες λειτουργούν ως ενδιάμεσοι στο τομέα των μετακινήσεων και της βραχυχρόνιας μίσθωσης ακινήτων αντίστοιχα, πλατφόρμες βασισμένες στο Blockchain επιτρέπουν την άμεση αλληλεπίδραση μεταξύ των χρηστών, εξαλείφοντας την ύπαρξη των ενδιαμέσων. Ενεργοποιώντας τις πληρωμές ομότιμων χρηστών, το Blockchain ανοίγει το δρόμο για την άμεση αλληλεπίδραση μεταξύ των μερών, επιτυγχάνοντας έτσι μια τελείως αποκεντρωμένη ανταλλακτική οικονομία. Το OpenBazaar είναι μια Startup εταιρεία η οποία δραστηριοποιείται σε αυτό τον τομέα, δημιουργώντας ένα e-bay ομότιμων χρηστών. Χρησιμοποιώντας αυτή την εφαρμογή μπορεί κανείς να πραγματοποιήσει συναλλαγές με τους διάφορους πωλητές χωρίς κάποιο αντίτιμο συναλλαγής. Ο όρος “προσωπική φήμη”, θα γίνει ακόμα πιο σημαντικός δεδομένου ότι θα εξαλειφθούν οι κανόνες στον κόσμο των επιχειρήσεων.

## 14.6 ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ

Οι καταναλωτές παγκοσμίως θέλουν όλο και περισσότερο να γνωρίζουν ότι οι ηθικοί ισχυρισμοί των εταιρειών, σχετικά με τα προϊόντα που τους προσφέρουν είναι πραγματικοί. Το αμετάβλητο κοινό μητρώο που προσφέρει η τεχνολογία Blockchain, είναι κατάλληλο για την παρακολούθηση των αγαθών, καθώς κινούνται και αλλάζουν χέρια μέσα στην εφοδιαστική

αλυσίδα. Καταχωρήσεις στην βάση της Blockchain μπορούν να χρησιμοποιηθούν για τη δρομολόγηση γεγονότων στην αλυσίδα προμήθειας(όπως π.χ. η κατανομή των προϊόντων όπως φτάνουν σε ένα λιμάνι στα διαφορετικά containers). Η τεχνολογία Blockchain προσφέρει ένα νέο δυναμικό τρόπο για την οργάνωση και παρακολούθηση δεδομένων και προϊόντων.

Επιπλέον, αισθητήρες που τίθενται επί των προϊόντων παρέχουν πλήρη διαφάνεια και ακριβή γνώση της διαδικασίας προμήθειας προϊόντων καθώς παρέχουν δεδομένα σε πραγματικό χρόνο για την τοποθεσία και την κατάστασή τους, καθώς μεταφέρονται στην παγκόσμια αγορά. Σύμφωνα με έρευνα της Deloitte και του σωματείου εταιρειών μηχανογράφησης και εφοδιαστικής αλυσίδας τις ΗΠΑ MHI το 2016[10], παρόμοιοι αισθητήρες χρησιμοποιούνταν ήδη σχεδόν από τις μισές εταιρείες του χώρου ενώ η υιοθέτησή τους προβλέπεται να είναι καθολική τα επόμενα χρόνια. Η τεχνολογία Blockchain θα αποθηκεύει, διαχειρίζεται, προστατεύει και μεταφέρει τις έξυπνες αυτές πληροφορίες με τον βέλτιστο τρόπο, παρέχοντας διαφάνεια σε πραγματικό χρόνο καθώς όλοι οι συμμετέχοντες(υπολογιστές) θα τηρούν και από ένα πλήρως ενημερωμένο αρχείο αυτών των δεδομένων. Η εφοδιαστική αλυσίδα θα βιώσει μεγάλη εξέλιξη με τη χρήση της τεχνολογία αυτής και κατά συνέπεια, θα βελτιωθεί η καθημερινότητα των ανθρώπων και των επιχειρήσεων.

## 14.7 ΥΓΕΙΑ - ΙΑΤΡΙΚΗ ΑΣΦΑΛΙΣΗ

Το Blockchain θα μπορούσε να συνεισφέρει στον τομέα της υγείας, με την διασύνδεση των ιατρικών συσκευών με το ιατρικό ιστορικό του κάθε ατόμου, συμβάλλοντας έτσι στην πρωτογενή πρόληψη. Ο συγκεκριμένος τομέας είναι ευαίσθητος όσον αφορά τα προσωπικά δεδομένα του κάθε ανθρώπου, κάτι που δημιουργεί την ανάγκη, οι καταχωρημένες πληροφορίες να μην είναι προσβάσιμες από οποιονδήποτε, για τη διασφάλιση του ιατρικού απορρήτου. Οι πληροφορίες σχετικά με το ιστορικό του ασθενούς θα είναι προσβάσιμες από τους γιατρούς, τον ασθενή και τις αρμόδιες ρυθμιστικές και ασφαλιστικές αρχές. Με τον τρόπο αυτό ο θεράπων ιατρός θα έχει άμεση πρόσβαση σε πληροφορίες που αλλιώς είναι ιδιαίτερα χρονοβόρες στη συλλογή τους, έτσι ο ασθενής θα μπορεί να λαμβάνει γρήγορη αντιμετώπιση, προσωποποιημένη στις δικές του ανάγκες και με βάση το καταχωρημένο ιστορικό του. Ακόμα λόγω αυτής της άμεσης

[10] https://www.businesswire.com/news/home/20170405005008/en/80-Manufacturing-Supply-Chain-Executives-Digital-Supply

πρόσβασης σε κρίσιμες για τον ασθενή πληροφορίες, θα μπορούσε να επιτευχθεί μείωση του χρόνου νοσηλείας, μειώνοντας και το τελικό κόστος νοσηλείας. Λαμβάνοντας υπόψιν πως ο τομέας της υγείας είναι ένας εκ των πιο δαπανηρών για τη δημόσια οικονομία, καθώς και τις ασφαλιστικές εταιρίες αντιλαμβάνεται κανείς πως η γρηγορότερη και εγκυρότερη αντιμετώπιση των περιστατικών θα μειώνει το χρόνο επίλυσης ασφαλιστικών απαιτήσεων και θα αυξάνει την αποτελεσματικότητα στην παροχή ασφαλιστικών συμβολαίων.

## 14.8 ΙΝΤΕΡΝΕΤ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IOT)

Ως έξυπνες χαρακτηρίζονται οι συσκευές οι οποίες συνδέονται στο διαδίκτυο, αλληλοεπιδρώντας με τον κάτοχό τους και μεταξύ τους, παρέχοντας και λαμβάνοντας συνεχώς δεδομένα. Καθώς οι μηχανές αλληλεπιδρούν μεταξύ τους, οποιαδήποτε πληροφορία ανταλλάσσεται μπορεί να αποθηκευτεί σε ένα Blockchain, αυξάνοντας την αποδοτικότητα, την ακρίβεια, μειώνοντας παράλληλα το κόστος. Το Ίντερνετ των πραγμάτων(Internet of Things-IoT) ουσιαστικά προσφέρει τον έλεγχο των μηχανών- ηλεκτρικών συσκευών από το δίκτυο για παράδειγμα, την παρακολούθηση της θερμοκρασίας του αέρα σε μια αποθήκη. Οι έξυπνες συμβάσεις που χρησιμοποιεί το Blockchain μπορούν να αυτοματοποιήσουν την διαχείριση απομακρυσμένων συστημάτων.

Ένας συνδυασμός λογισμικού, αισθητήρων και δικτύου διευκολύνει την ανταλλαγή δεδομένων μεταξύ αντικειμένων και μηχανισμών. Το αποτέλεσμα αυξάνει την απόδοση του συστήματος και βελτιώνει την παρακολούθηση του κόστους. Με τον τρόπο αυτό θα υπάρξει μεγαλύτερη διαφάνεια στον τρόπο μεταφοράς εμπορευμάτων παγκοσμίως και θα μπουν οι βάσεις για την για “αυτονομία των εμπορευμάτων” (freight-autonomy). Ένα είδος εμπορεύματος αποτελεί και η ενέργεια, στην οποία η τεχνολογία Blockchain επιτρέπει στα ηλιακά πάνελ να αναδιανέμουν την ενέργεια μέσω έξυπνων συμβολαίων σε γειτονικά. [5]

## 14.9 ΕΚΠΑΙΔΕΥΣΗ

Καθώς η εκπαίδευση γίνεται πιο διαφοροποιημένη, εκδημοκρατισμένη και αποκεντρωμένη η οποία επενδύει συνεχώς στον εαυτό της, δημιουργείται η ανάγκη διατήρησης της φήμης της, της εμπιστοσύνης στην πιστοποίηση και στην αξιοκρατία καθώς και στην απόδειξη της μάθησης. Η αυξημένη εστίαση στην συνάφεια και στην απασχολισιμότητα μπορεί να ωθήσει στην κατεύθυνση της διαφάνειας. Η τεχνολογία blockchain θα μπορούσε να παράσχει ακριβώς ένα τέτοιο σύστημα, μία ανοιχτή, διαδικτυακή και ασφαλή βάση δεδομένων.

Ο τρόπος που αποκτάται η γνώση μπορεί να αλλάξει άρδην με τη χρήση αυτής της τεχνολογίας σύμφωνα με την Startup Knowledge.io η οποία έχει υιοθετήσει ένα νέο σύστημα ανταμοιβής της αποκτώμενης γνώσης. Ένας Δείκτης Γνώσης παρακολουθεί και μετρά την επάρκεια ενός ατόμου σε ένα ευρύ φάσμα θεμάτων. Στη συνέχεια τα λεγόμενα “Knowledge Tokens” που θα λαμβάνουν οι συμμετέχοντες θα μπορούν να χρησιμοποιηθούν σε ένα Οικοσύστημα Γνώσης, το οποίο θα περιέχει εγχειρίδια, βίντεο, άρθρα και περιοδικά στα θέματα που ενδιαφέρεται καθένας που συμμετέχει.

Μία άλλη χρήση της συγκεκριμένης τεχνολογίας στον τομέα της εκπαίδευσης είναι η πιστοποίηση των διπλωμάτων και των πτυχίων των φοιτητών. Το Ινστιτούτο Τεχνολογίας της Μασαχουσέτης (MIT), μέσω μιας εφαρμογής που ονομάζεται Blockcerts Wallet[11], εκδίδει εικονικά διπλώματα στους φοιτητές της οι οποίοι μπορούν να έχουν πρόσβαση μέσω των Smartphones τους, πέρα του πιστοποιητικού το οποίο λαμβάνουν μέσω του παραδοσιακού χαρτιού. Τα ψηφιακά αυτά πιστοποιητικά είναι απαραβίαστα και μπορούν να μοιραστούν με σχολεία, εργοδότες συγγενείς και φίλους. Εκτός από την τεχνολογία Blockchain η εφαρμογή χρησιμοποιεί και Touchstone, τον πάροχο ταυτότητας του MIT για να διασφαλίσει την ασφάλεια κάθε πτυχίου.

Η Sony χρησιμοποιώντας το Blockchain της IBM στο παγκόσμιο σύστημα εκπαίδευσής της, δημιούργησε μια πλατφόρμα που συγκεντρώνει και διαχειρίζεται αρχεία φοιτητών από διάφορα σχολεία, τα οποία μπορούν να χρησιμοποιούν οι διευθυντές σχολείων, εταιρείες προσλήψεων και άλλα ενδιαφερόμενα μέρη για να επαληθεύσουν την αξιοπιστία των αρχείων που τους έχουν υποβληθεί.

[11] https://www.blockcerts.org

Η τεχνολογία Blockchain μπορεί να συνεισφέρει σε μεγάλο βαθμό στην ασφάλεια και την απομακρυσμένη πρόσβαση μέσω Cloud, την πιστοποίηση και την εξοικονόμηση χρόνου και χρήματος καθώς και στην προστασία του περιβάλλοντος δεδομένης της μείωσης της χρήσης χαρτιού. Όπως συμβαίνει στις περιπτώσεις των μεγάλων αλλαγών που έχει επιφέρει η τεχνολογία, υπάρχουν ανησυχίες από πλήθος κόσμου κάτι το οποίο συμβαίνει και με την εξέλιξη της τεχνολογίας Blockchain. Παρόλα αυτά υπάρχουν σαφείς ενδείξεις για το ότι η τεχνολογία αυτή μπορεί να συνεισφέρει θετικά στον σύγχρονο κόσμο που περιλαμβάνει αναρίθμητες βάσεις δεδομένων.

# 15 ΔΙΑΧΕΙΡΙΣΗ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΚΑΙ BLOCKCHAIN

Ένα από τα βασικά ζητήματα στον τομέα της διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας είναι η περιπλοκότητα των δικαιωμάτων κτήσης, η κατανομή των αμοιβών και η διαφάνεια λειτουργίας των οργανισμών συλλογικής διαχείρισης. Η τεχνολογία Blockchain σε συνδυασμό με τα έξυπνα συμβόλαια μπορεί να παρέχει μία πλήρη και ακριβή βάση δεδομένων δικαιωμάτων πνευματικής ιδιοκτησίας, εξασφαλίζοντας διαφανή κατανομή των αμοιβών σε πραγματικό χρόνο σε όλους τους δικαιούχους σε διαφορετικά επίπεδα. Η χρήση ψηφιακών νομισμάτων για την άμεση καταβολή των αμοιβών από τους χρήστες θα διευκολύνει ακόμη περισσότερο τη βέλτιστη διαχείριση των εν λόγω δικαιωμάτων.

Η συνεχής πρόοδος και εξέλιξη των ψηφιακών τεχνολογιών και η ραγδαία αύξηση της χρήσης του διαδικτύου έχει οδηγήσει στη διακίνηση μεγάλου όγκου πολυμεσικού περιεχομένου στο διαδίκτυο. Η ψηφιοποίηση αλλάζει ταχύτατα τον τρόπο με τον οποίο το περιεχόμενο αυτό δημιουργείται και διαδίδεται. Αναμένεται ότι η παγκόσμια αγορά των ψηφιακών μέσων ενημέρωσης και ψυχαγωγίας θα αυξηθεί σε 2,2 τρισεκατομμύρια δολάρια μέχρι το έτος 2021[12]. Συγχρόνως, η ανάπτυξη τεχνολογιών που χρησιμοποιούν τις τεχνικές συμπίεσης, την κρυπτογράφηση και την ταχύτητα του διαδικτύου για την διευκόλυνση της διανομής των κειμένων, των στατικών και κινούμενων εικόνων και του ήχου έχουν περάσει σχεδόν απαρατήρητες από πολλούς υπαλλήλους και διαχειριστές βιβλιοθηκών. Η διαχείριση των

[12] https://www.statista.com/statistics/237749/value-of-the-global-entertainment-and-media-market/

ψηφιακών περιεχομένου κρίνεται αναγκαία και η ανάγκη υιοθέτησης συστημάτων ψηφιακής διαχείρισης πνευματικών δικαιωμάτων(Digital Right Management-DRM) επιτακτική. Υπηρεσίες όπως η Amazon.com και η BMG Music Service χρησιμοποιούν ορισμένα στοιχεία της συγκεκριμένης τεχνολογίας [15].

Η αναδυόμενη τεχνολογία Blockchain μπορεί να παίξει καθοριστικό ρόλο στην επίλυση τέτοιων προβλημάτων παρουσιάζοντας μεγάλο ενδιαφέρον ιδιαίτερα στον κλάδο της πνευματικής ιδιοκτησίας αλλά και των ψηφιακών δικαιωμάτων. Μία ιδιαίτερα τόσο πρακτική και προφανής εφαρμογή της τεχνολογίας του Blockchain στο κομμάτι της προστασίας και της διαχείρισης πνευματικών δικαιωμάτων, είναι η δημιουργία μιας βιβλιοθήκης, ενός μητρώου δικαιωμάτων πνευματικής ιδιοκτησίας, στο οποίο θα καταγράφονται και θα αποθηκεύονται τα πρωτότυπα έργα και αρχεία. Στο Ηνωμένο Βασίλειο, τα πνευματικά δικαιώματα δεν έχουν καταχωρηθεί αλλά δημιουργούνται αυτόματα κατά τη δημιουργία ενός πρωτότυπου έργου. Αυτό σημαίνει ότι, σε αντίθεση με τα καταχωρημένα εμπορικά σήματα τα οποία μπορούν να αποθηκευτούν και να προβληθούν σε διάφορα μητρώα σε όλο τον κόσμο, δεν υπάρχουν επαρκή μέσα έτσι ώστε οι δημιουργοί να μπορούν να καταγράψουν τα έργα τους. Ως εκ τούτου, η ιδιοκτησία μπορεί να είναι δύσκολο έως και αδύνατο να αποδειχθεί. Κατ' επέκταση δημιουργούνται ποικίλα προβλήματα τα οποία αφορούν τόσο στη διεκδίκηση των δικαιωμάτων ενός έργου όσο και στη χρησιμοποίηση των έργων από τρίτους, παραδείγματος χάριν μπορεί να είναι δύσκολο για τους συγγραφείς να δουν ποιος χρησιμοποιεί το έργο τους και εξίσου δύσκολο για τρίτους που χρησιμοποιούν ένα έργο να μάθουν από ποιον να ζητήσουν την απαραίτητη άδεια για να έχουν πρόσβαση σε αυτό. Αυτό όπως είναι εύκολα κατανοητό έχει ως αποτέλεσμα οι συγγραφείς να μην μπορούν να σταματήσουν τις μη εξουσιοδοτημένες χρήσεις των αρχείων τους καθώς και να μην αξιοποιούν στο έπακρο τα εν δυνάμει κέρδη από την αξιοποίηση των έργων τους.

Η χρήση του Blockchain ως ένα μητρώο δικαιωμάτων πνευματικής ιδιοκτησίας μπορεί να βοηθήσει στην αποσαφήνιση των πνευματικών δικαιωμάτων των δημιουργών, των ιδιοκτητών και των χρηστών. Καταγράφοντας τα έργα τους σε ένα Blockchain, οι συντάκτες θα μπορούν να αποδείξουν ότι η συγκεκριμένη δημιουργία είναι δική τους. Αυτό οφείλεται στο γεγονός ότι μια συναλλαγή σε ένα Blockchain σύστημα παραμένει αμετάβλητη, οπότε μόλις μια εργασία καταχωρηθεί σε αυτό, οι πληροφορίες αυτές δεν μπορούν να χαθούν ή να τροποποιηθούν. Θεωρητικά, τα τρίτα μέλη θα μπορούσαν να χρησιμοποιούν το Blockchain για να δουν την πλήρη ιδιοκτησία ενός έργου, συμπεριλαμβανομένων των αδειών, των δευτερευουσών αδειών και των

καταχωρήσεων. Επί του παρόντος, όταν ένας δημιουργός ανεβάσει στο διαδίκτυο ένα έργο του, γίνεται εξαιρετικά δύσκολο να διατηρηθεί ο έλεγχος αυτού του έργου και να παρακολουθείται, ποιος το χρησιμοποιεί και για ποιο σκοπό. Στα πλαίσια λοιπόν αναζήτησης λύσεων που θα μπορέσουν να βελτιώσουν την εκμετάλλευση των έργων από τους δημιουργούς τους, σε συνδυασμό με τη διασφάλιση των νόμιμων δικαιωμάτων τους, μπορούν να προταθούν λύσεις που προσφέρονται από την τεχνολογίας του Blockchain.

## 15.1 ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ

Η πνευματική ιδιοκτησία(Intellectual Property) είναι μια κατηγορία περιουσίας που αποτελείται από άυλες δημιουργίες του ανθρώπινου πνεύματος και περιλαμβάνει πρωτίστως τα πνευματικά δικαιώματα, τα διπλώματα ευρεσιτεχνίας και τα εμπορικά σήματα. Περιλαμβάνει επίσης και άλλα είδη δικαιωμάτων, όπως εμπορικά μυστικά, διαφημιστικά δικαιώματα, ηθικά δικαιώματα και δικαιώματα έναντι αθέμιτου ανταγωνισμού. Καλλιτεχνικά έργα όπως η μουσική και η λογοτεχνία, καθώς και μερικές ανακαλύψεις, εφευρέσεις, λέξεις, φράσεις, σύμβολα και σχέδια μπορούν όλα να προστατευθούν ως πνευματική ιδιοκτησία. Για να θεωρηθεί ένα έργο ως προστατευόμενο από πνευματικά δικαιώματα, πρέπει να είναι πρωτότυπο, καθορισμένο σε μια συγκεκριμένη μορφή και να διαθέτει ένα ελάχιστο επίπεδο δημιουργικότητας. [26]

Ο κύριος σκοπός του νόμου περί πνευματικής ιδιοκτησίας είναι να ενθαρρύνει τη δημιουργία μιας ευρείας ποικιλίας πνευματικών αγαθών. Για να επιτευχθεί αυτό, ο νόμος παρέχει στους ανθρώπους και στις επιχειρήσεις, δικαιώματα ιδιοκτησίας στα πληροφοριακά και πνευματικά προϊόντα που δημιουργούν, συνήθως για περιορισμένο χρονικό διάστημα. Για το λόγο του ότι οι δημιουργοί μπορούν να κερδίσουν από την εκμετάλλευση των έργων τους, τους παρέχει ένα επιπλέον κίνητρο για τη δημιουργία τους, το οικονομικό.

Ο άυλος χαρακτήρας της πνευματικής ιδιοκτησίας παρουσιάζει δυσκολίες σε σχέση με την παραδοσιακή ιδιοκτησία όπως η γη ή τα αγαθά. Σε αντίθεση με την παραδοσιακή ιδιοκτησία, η πνευματική ιδιοκτησία είναι αδιαίρετη αφού ένας απεριόριστος αριθμός ανθρώπων μπορεί να “καταναλώσει” ένα πνευματικό αγαθό χωρίς να εξαντληθεί. Επιπλέον, οι επενδύσεις σε πνευματικά αγαθά υποφέρουν από προβλήματα εκμετάλλευσης αφού ένας γαιοκτήμονας μπορεί να περιβάλλει τη γη του με ένα φράχτη για να το προστατεύσει, αλλά ένας δημιουργός

πληροφοριών ή πνευματικών αγαθών, μπορεί συνήθως να κάνει ελάχιστα για να σταματήσει τον πρώτο αγοραστή ο οποίος θα αντιγράψει, θα αναπαραγάγει και θα τα πωλήσει σε χαμηλότερη τιμή.

## 15.2 ΔΙΑΧΕΙΡΙΣΗ ΨΗΦΙΑΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Η διαχείριση ψηφιακών δικαιωμάτων(Digital Right Management-DRM) αποτελεί έναν τρόπο επέκτασης του ελέγχου σε ψηφιακά αντικείμενα στον κυβερνοχώρο. Το DRM χρησιμοποιείται σήμερα για να προστατέψει το ψηφιακό περιεχόμενο (κρυπτογράφηση), να ελέγξει συγκεκριμένες λειτουργίες σχετικά με το περιεχόμενο (αναπαραγωγή, εκτύπωση, αντιγραφή, αποθήκευση) και να περιορίσει τον αριθμό των περιπτώσεων που μια συγκεκριμένη λειτουργία μπορεί να ασκηθεί στο περιεχόμενο (π.χ. προβολή τρεις φορές). Οι περισσότερες τεχνολογίες DRM σήμερα "προστατεύουν διαρκώς" το περιεχόμενο, το οποίο δεν είναι σε μια αποκρυπτογραφημένη κατάσταση – κατά τη διάρκεια της αποθήκευσης, διανομής και κατανάλωσης και ισχύει για τις λήψεις περιεχομένου (download content) καθώς και το περιεχόμενο συνεχούς ροής (streaming content).

Το DRM χρησιμοποιεί πολλαπλές προσεγγίσεις για την προστασία του περιεχομένου. Ο έλεγχος της πρόσβασης στο περιεχόμενο αποτελεί το πρώτο στάδιο ελέγχου. Το να επιτρέπεται μόνο στους εξουσιοδοτημένους χρήστες να κάνουν λήψη του περιεχομένου μειώνει τον αριθμό των θέσεων που θα μπορούσαν να προέλθουν από διαρροές. Προκειμένου ένας καταναλωτής να αποκτήσει πρόσβαση σε ένα ψηφιακό περιεχόμενο ή αρχείο το οποίο ελέγχεται από σύστημα DRM, πρέπει να αποκτήσει δικαίωμα χρήσης. [27]

Το δεύτερο στάδιο ελέγχου περιλαμβάνει την κρυπτογραφία. Η κρυπτογραφία αποτρέπει την αποθήκευση περιεχομένου στο δίσκο ή στη μνήμη RAM σε απλό κείμενο. Οι πελάτες λαμβάνουν κλειδιά αποκρυπτογράφησης πριν από τη λήψη του περιεχομένου, όπως σε μια λιανική συναλλαγή, ή μετά τη λήψη του περιεχομένου όπως στην παραλαβή ελεγχόμενου περιεχομένου όπως για παράδειγμα αποτελεί ένα συνημμένο αρχείο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Αν οι πελάτες ενοικιάζουν ένα περιεχόμενο, τότε τα κλειδιά λήγουν όταν λήξει η περίοδος μίσθωσης. Το περιεχόμενο αποκρυπτογραφείται σε μικρές μονάδες και αποθηκεύεται στη μνήμη RAM μη κρυπτογραφημένο για περιορισμένο χρονικό διάστημα, για να προστατεύεται από τους

εισβολείς που διαβάζουν το περιεχόμενο της μνήμης RAM. Μόλις αποκρυπτογραφηθεί, το περιεχόμενο στέλνεται μέσω ενός ασφαλούς καναλιού (High-bandwidth Digital Content Protection-HDCP), στην οθόνη. Η άδεια που δίνεται σε κάθε πελάτη μέσω των κλειδιών είναι μοναδική για τη συσκευή του και περιλαμβάνει τα εξουσιοδοτημένα δικαιώματα χρήσης (π.χ. απεριόριστη προβολή, χωρίς εκτύπωση), το κλειδί για την παροχή πρόσβασης στο κρυπτογραφημένο αρχείο και διαχειρίζεται την λήψη ή τη ροή του περιεχομένου.

Το τελευταίο στάδιο ελέγχου πραγματοποιείται μετά από διαρροή περιεχομένου. Η εγκληματολογική σήμανση εντοπίζει με μοναδικό τρόπο τον αγοραστή ενός περιεχομένου, κάτι το οποίο βοηθά στην ανίχνευση των παραβιάσεων από μη εξουσιοδοτημένους χρήστες. Το ψηφιακό υδατογράφημα είναι μια μορφή εγκληματολογικής σήμανσης που αλλάζει ελαφρώς τις τιμές χρώματος ή ήχου και είναι ανιχνεύσιμο μόνο με χρήση ανιχνευτή και ενός μυστικού κλειδιού.

Οι περισσότερες τεχνολογίες DRM σήμερα συνδέουν μια “προσφερόμενη URL” με αντικείμενα περιεχομένου, δηλαδή την τοποθεσία δικτύου από την οποία θα αποκτήσουν τα δικαιώματα. Στην περίπτωση που το προστατευόμενο περιεχόμενο διανέμεται μέσω ηλεκτρονικού ταχυδρομείου, ο παραλήπτης δεν έχει πρόσβαση μέχρι να ληφθεί η κατάλληλη άδεια. Καθώς επιχειρείται η πρόσβαση σε κάποιο περιεχόμενο, η τοπική εφαρμογή λογισμικού, αναζητά πρώτα μια έγκυρη άδεια στον υπολογιστή ή τη συσκευή και εάν δεν υπάρχει, το λογισμικό διαβάζει την προσφερόμενη URL και καθοδηγεί το χρήστη σε έναν ιστότοπο για να αποκτήσει ένα. Ο καταναλωτής εκτελεί ξανά την επιλογή του, και η συναλλαγή έχει ως αποτέλεσμα την έκδοση της σχετικής άδειας. Δεδομένου ότι ο καταναλωτής έχει ήδη το περιεχόμενο, δεν απαιτείται επιπλέον λήψη.

Παρόμοια με τη βιομηχανία πιστωτικών καρτών που χρησιμοποιεί αξιόπιστους διαμεσολαβητές για την επεξεργασία συναλλαγών μεταξύ διαφόρων μερών (καταναλωτών, εμπόρων και τραπεζών), ο συναλλασσόμενος χαρακτήρας του DRM έχει οδηγήσει στην απαίτηση για ανεξάρτητους, αξιόπιστους εταίρους για την πραγματοποίηση των συναλλαγών. Συχνά αναφέρονται ως “διακανονιστές”, αυτά τα τρίτα μέρη υποστηρίζουν μία ή περισσότερες τεχνολογίες DRM, διατηρούν την ακεραιότητα στις επιχειρηματικές σχέσεις εντός της αλυσίδας αξίας του περιεχομένου (δικαιώματα διανομής, τιμολογιακή πολιτική, οικονομικοί διακανονισμοί, επεξεργασία δικαιωμάτων), παρέχοντας υποστήριξη στους πελάτες (πρόσβαση στο περιεχόμενο, αποκατάσταση δικαιωμάτων, μεταφορά δικαιωμάτων) .

# 16 ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΣΤΟ ΨΗΦΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ

Η νομοθεσία για τα δικαιώματα πνευματικής ιδιοκτησίας αποτελούν τη βάση πάνω στην οποία στηρίζονται όλοι οι δημιουργοί περιεχομένου τόσο στον φυσικό όσο και στον ψηφιακό κόσμο. Αν και οι κανονισμοί είναι συνήθως αποτελεσματικοί σε σύντομο χρονικό διάστημα μετά την έναρξή τους, ο εφήμερος χαρακτήρας της τεχνολογίας και συνεπώς οι μέθοδοι κατανάλωσης και διανομής έργων που προστατεύονται από πνευματικά δικαιώματα, καθιστούν γρήγορα ανεπαρκή την νομοθεσία για τα πνευματικά δικαιώματα. Συνεπώς ο νόμος περί πνευματικών δικαιωμάτων αποτελεί ένα σημείο αμφισβήτησης μεταξύ των νομοθετών, των κατόχων των πνευματικών δικαιωμάτων αλλά και των απλών χρηστών.

## 16.1 ΝΟΜΙΚΟ ΚΑΘΕΣΤΩΣ ΤΩΝ ΕΡΓΩΝ ΠΟΥ ΠΡΟΣΤΑΤΕΥΟΝΤΑΙ ΑΠΟ ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ.

Καθώς η τεχνολογία αναπτύσσεται και εξελίσσεται, αλλάζει συνεχώς και το πεδίο εφαρμογής του νόμου περί πνευματικής ιδιοκτησίας. Συνεπώς, οι νομικές διαδικασίες πρέπει να παρακολουθούν τις τεχνολογικές εξελίξεις και να προσαρμόζονται άμεσα σε αυτές, κάτι το οποίο δεν πραγματοποιείται. Ωστόσο, είναι αδύνατο για μια νομοθετική αρχή να αναθεωρεί συνεχώς τις νομοθετικές διαδικασίες, αλλάζοντας συνεχώς τους νόμους ώστε να βρίσκεται παράλληλα στις τεχνολογικές εξελίξεις. Στην πραγματικότητα, τα τελευταία χρόνια έχουν πραγματοποιηθεί ελάχιστες τροποποιήσεις στους νόμους που χρησιμοποιούνται για την προστασία των πνευματικών δικαιωμάτων, προκειμένου να προσαρμοστούν στις τεχνολογικές εξελίξεις, δίνοντας την ευκαιρία σε επιχειρήσεις να επωφεληθούν από τους ξεπερασμένους κανονισμούς. [28]

Πολλά από τα νομικά ζητήματα που προκύπτουν όσον αφορά τη διαχείριση των πνευματικών δικαιωμάτων, μπορούν να αποδοθούν δυστυχώς στη νομική καθυστέρηση. Εκτός από την παρατεταμένη νομοθετική διαδικασία, η νομική καθυστέρηση είναι επίσης αποτέλεσμα της δυναμικής και απρόβλεπτης φύσης της τεχνολογίας. Καθώς οι επιπτώσεις της τεχνολογίας είναι συχνά δύσκολο να κατανοηθούν έως ότου τεθεί σε συνήθη χρήση, είναι σχεδόν αδύνατον για τις ρυθμιστικές αρχές να τροποποιήσουν εύστοχα τη νομοθεσία. Συνεπώς, οι νόμοι περί

πνευματικής ιδιοκτησίας παραμένουν διατυπωμένοι ως πρότυπα ανοιχτού τύπου για να αποφευχθεί η συνεχής ανάγκη τροποποιήσεων και αναθεωρήσεων. Αυτή η νομοθετική ασάφεια οδηγεί σε εκμετάλλευση υλικού που προστατεύεται από πνευματικά δικαιώματα. [28]

Επιπλέον, οι νομοθετικές ασάφειες περί πνευματικής ιδιοκτησίας υποκινούν νομικές διενέξεις μεταξύ των ενδιαφερόμενων μερών. Όπως αποδεικνύεται από ένα μεγάλο αριθμό αγωγών περί πνευματικής ιδιοκτησίας, η ασάφεια στο νομοθετικό πλαίσιο οδηγεί συχνά σε δικαστικές διαμάχες. Αυτές οι δικαστικές διαμάχες επιδεινώνουν την κατάσταση δημιουργώντας καθυστερήσεις, δίνοντας εκείνη τη στιγμή την ευκαιρία σε χρήστες να συνεχίζουν να ενεργούν σε ένα ασαφές κανονιστικό πλαίσιο. Επίσης, είναι δυνατόν να προκύψει κατά την περίοδο αυτή μία νέα τεχνολογία, καθιστώντας έτσι τα τρέχοντα ζητήματα απαρχαιωμένα και ανούσια. Σημαντικός παράγοντας στην διαμόρφωση και εφαρμογή του κατάλληλου νομοθετικού πλαισίου παραμένει και η άγνοια αλλά και η εμπειρογνωμοσύνη των νομοθετικών αρχών σε τεχνολογικά θέματα. Υπάρχει έλλειψη πληροφόρησης καθώς και εμπειρίας πάνω στον τομέα των τεχνολογικών εξελίξεων και πως αυτές εφαρμόζονται και επηρεάζουν τα πνευματικά δικαιώματα.

## 16.2 ΕΛΛΕΙΨΗ ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

Η έλλειψη διαφάνειας καθώς και μιας κεντρικής βάσης δεδομένων η οποία θα οργανώνει πληροφορίες σχετικά με τη μουσική, τις φωτογραφίες, τα βιβλία, τα έγγραφα και άλλα αντικείμενα που προστατεύονται από πνευματική ιδιοκτησία, δημιούργησαν σημαντικά προβλήματα κατά τη διάρκεια προσδιορισμού του κατάλληλου ιδιοκτήτη προκειμένου να οργανωθεί η μεταγενέστερη χρήση τέτοιων αντικειμένων. Οι πληροφορίες σχετικά με τους κατόχους δικαιωμάτων πνευματικής ιδιοκτησίας διασκορπίζονται σε διάφορες βάσεις δεδομένων εκδοτών, δισκογραφικών εταιρειών, εταιρειών συλλογικής διαχείρισης και άλλων οντοτήτων, οι οποίοι δεν έχουν την τάση να τις μοιράζονται. Μερικές φορές οι πληροφορίες αυτές είναι απλώς μη διαθέσιμες ή η παραλαβή τους είναι απαγορευτικά δαπανηρή τόσο από χρονική όσο και από οικονομική άποψη.

Όλα αυτά δημιουργούν σημαντικό κόστος συναλλαγών για τους χρήστες τέτοιου ψηφιακού περιεχομένου, οι οποίοι μερικές φορές απέχουν από τη χρήση ορισμένων έργων που προστατεύονται από πνευματικά δικαιώματα, λόγω του ασαφούς νομικού καθεστώτος. Η έλλειψη

διαφάνειας και οι διαθέσιμες στο κοινό πληροφορίες σχετικά με την ιδιοκτησία των δικαιωμάτων πνευματικής ιδιοκτησίας επηρεάζουν και τους δημιουργούς και άλλους ιδιοκτήτες δικαιωμάτων, οι οποίοι δεν λαμβάνουν αποζημίωση για την χρήση των έργων τους ή πρέπει να μοιράζονται την αμοιβή αυτή με μεσάζοντες, όπως οι συλλογικές εταιρείες, οι οποίες διατηρούν σημαντικό μέρος αυτής της αμοιβής.

Τα παραπάνω ζητήματα οφείλονται σε σημαντικό βαθμό στην έλλειψη φιλικών προς το κόστος, ευρέως αποδεκτών τεχνολογιών. Η χρήση διαφορετικών, ιδιόκτητων βάσεων δεδομένων, οι οποίες δεν είναι διαλειτουργικές μεταξύ τους, αποτελεί ένα από τα εμπόδια για την ανταλλαγή δεδομένων. Η τεχνολογία Blockchain μπορεί να παίξει καθοριστικό ρόλο ώστε να φέρει αποτελέσματα τυποποίησης και δικτύωσης στον τομέα της διαχείρισης των πνευματικών δικαιωμάτων.

Ο βασικότερος λόγος έλλειψης διαφάνειας έγκειται στον ίδιο το νομικό πλαίσιο περί πνευματικής ιδιοκτησίας. Η ύπαρξη ενός πολύ χαμηλού ορίου το οποίο καθορίζει την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας, οδηγεί στην κυκλοφορία τεράστιων ποσοτήτων έργων που προστατεύονται τυπικά από “copyright”, ειδικά στο διαδίκτυο. Η απουσία τυπικών απαιτήσεων πιστοποίησης ή έγκρισης για την ιδιοκτησία πνευματικών δικαιωμάτων οδηγεί στην άγνοιά τους από τρίτους. Θα ήμασταν άδικοι εάν υποστηρίζαμε πως αυτό είναι ένα πρόβλημα το οποίο προκύπτει από την τεχνολογία και την εξέλιξή της, ωστόσο όμως πρέπει να δεχτούμε ότι ενισχύεται σημαντικά από αυτή. Επομένως, η σωστή τεχνολογία η οποία θα εφαρμοστεί κατάλληλα, μπορεί να το διορθώσει, αν όχι εντελώς, τουλάχιστον σε κάποιο βαθμό.

## 16.3 ΠΕΙΡΑΤΕΙΑ

Οι δικαιούχοι δεν μπορούν να ελέγξουν αποτελεσματικά τη χρήση των έργων τους στο διαδίκτυο. Τα ψηφιακά αντίγραφα είναι τέλεια αντίγραφα και καθένα από αυτά μπορεί να χρησιμοποιηθεί για περαιτέρω τέλεια αντίγραφα. Δεν υπάρχουν πλέον φυσικά εμπόδια στην παραβίαση και τη δημιουργία αντιγράφων, όπως η δαπάνη αναπαραγωγής και η μείωση της ποιότητας των διαδοχικών αντιγράφων σε αντίστοιχα μέσα. Σήμερα, ο μέσος ιδιοκτήτης ηλεκτρονικών υπολογιστών μπορεί εύκολα να επιλέξει το είδος και την έκταση της αντιγραφής,

τα οποία θα απαιτούσαν σημαντικό ποσό επενδύσεων και ίσως εγκληματική πρόθεση μόλις πριν από μερικά χρόνια. [29]

Επιπλέον, δεν υπάρχει τεχνολογικό όριο στον αριθμό ατόμων που μπορούν να έχουν πρόσβαση σε τέτοιου είδους ψηφιακά έργα, από οποιοδήποτε σημείο του πλανήτη που έχει σύνδεση στο διαδίκτυο. Εκτός αυτού, οι σύγχρονες τεχνολογίες διαδικτύου επιτρέπουν την αποστολή προϊόντων πληροφόρησης παγκοσμίως, φτηνά και σχεδόν στιγμιαία. Έτσι γίνεται ευκολότερο το έργο των πειρατών και ταυτόχρονα λιγότερο δαπανηρό, να πραγματοποιήσουν ή να διανείμουν μη εξουσιοδοτημένα αντίγραφα. [29]

Η κοινή χρήση ενός έργου στο διαδίκτυο συνεπάγεται την απώλεια του ελέγχου αυτού. Αν τα πνευματικά δικαιώματα ανήκουν σε ένα άτομο, πιθανότατα δεν γνωρίζει την παραβίαση, αλλά ακόμα και στην περίπτωση που την γνωρίζει, είναι πολύ επαχθές το να αναλάβει αποτελεσματική νομική δράση για αυτό. Σύμφωνα με τους McConaghy και Holtzman είναι "σαν να έχετε τον τίτλο και τα κλειδιά από το αυτοκίνητό σας, αλλά δεν γνωρίζεται που είναι· θεωρητικά το έχετε στην κατοχή σας, αλλά δεν μπορείτε να το χρησιμοποιήσετε με τον προβλεπόμενο τρόπο." [30]

Τα εργαλεία διαχείρισης ψηφιακής διαχείρισης δικαιωμάτων(DRM), μολονότι μπορούν να μετριάσουν σε κάποιο βαθμό τα ζητήματα πειρατείας, εξακολουθούν να μην παρέχουν τέλεια λύση σε αυτή. Πρώτα από όλα, το DRM προσθέτει πολυπλοκότητα στη διανομή ψηφιακών έργων μαζί με σημαντικά έξοδα συναλλαγής για το δικαιούχο. Επιπλέον, ο κάθε ιδιοκτήτης δεν είναι έτοιμος να εφαρμόσει το DRM για κάθε εργασία και να το διαχειριστεί. Δεύτερον, το DRM μπορεί να δημιουργήσει επιπλοκές σε τελικούς χρήστες, αφού δημιουργεί διακρίσεις στους χρήστες κατά περιοχές(π.χ. ένα αγγλόφωνο άτομο δεν μπορεί να αγοράσει εύκολα αγγλικά αντίγραφα ψηφιακού περιεχομένου στη Γερμανία). Το DRM ενδέχεται να δημιουργήσει ευπάθειες στο λογισμικό του καταναλωτή(π.χ. Η Sony εγκατέστησε ένα λογισμικό κατασκοπείας DRM σε μουσικά CD γνωστό και ως Sony rootkit, το οποίο είχε ως αποτέλεσμα την επιβράδυνση του υπολογιστή του χρήστη και τη δημιουργία επιπλέον κενών ασφαλείας τα οποία άνοιγαν πόρτες για άλλες περισσότερο κακόβουλες επιθέσεις[13]). Παράλληλα, το DRM ενδέχεται να αποτρέψει ορισμένες χρήσεις που ο νόμος θα αναγνώριζε ως νόμιμη. Υποστηρίζεται, ότι το DRM παρέχει στους κατόχους δικαιωμάτων πνευματικής ιδιοκτησίας την δυνατότητα να εξαλείφουν μονομερώς τα δικαιώματα χρήσης από το κοινό(π.χ. Η χρήση της κρυπτογράφησης από τη βιομηχανία κινηματογράφου σε

[13] https://fsfe.org/activities/drm/sony-rootkit-fiasco.el.html

DVD έχει περιορίσει την ικανότητα των καταναλωτών να κάνουν νόμιμα, προσωπικά αντίγραφα των ταινιών που έχουν αγοράσει[14]).

Τέλος, ακόμη και αν το DRM δεν εξαλείψει τη νόμιμη και θεμιτή χρήση του ψηφιακού περιεχομένου, το κάνει σίγουρα πιο βολικό. Επομένως, το DRM δεν αποτελεί λύση στο πρόβλημα και μερικές φορές μπορεί να γίνει πρόβλημα από μόνο του. Απαιτούνται καλύτερες λύσεις, πιο αποτελεσματικές από τεχνική άποψη και φιλικότερες τόσο για τους χρήστες όσο και για τους κατόχους δικαιωμάτων.

## 16.4 ΑΠΟΖΗΜΙΩΣΗ

Είναι ευρέως γνωστό ότι υπάρχει μεγάλη δυσκολία στη σωστή αποζημίωση των πραγματικών δημιουργών και διαχειριστών των πνευματικών δικαιωμάτων στις περιπτώσεις που αυτά αναπαράγονται χωρίς την άδειά τους. Στις περισσότερες περιπτώσεις, για να διευκολυνθεί η διαδικασία πληρωμής, απαιτείται η ύπαρξη ειδικής συμφωνίας που έχει υπογραφεί τόσο από το χρήστη όσο και από τον δικαιούχο, επιβάλλοντας σημαντικά έξοδα συναλλαγών και στις δύο πλευρές. Οι παραδοσιακές άδειες κοινής χρήσης λογισμικού δεν είναι κατάλληλες για άμεση εμπορευματοποίηση έργων, δεδομένου ότι δεν υπάρχει σαφές προσδιοριστικό πλαίσιο. Επίσης, οι άδειες ανοιχτού κώδικα που χρησιμοποιούνται για τη διανομή λογισμικού, περιλαμβάνουν διατάξεις δωρεάν διανομής. Σύμφωνα με το πρώτο κριτήριο του λογισμικού ανοιχτού κώδικα "η άδεια δεν απαιτεί υποχρέωση καταβολής δικαιωμάτων πνευματικής ιδιοκτησίας ή άλλα τέλη" για την πώληση λογισμικού[15]. Έτσι οι άδειες λογισμικού ανοιχτού κώδικα δεν είναι προσαρμοσμένες να λαμβάνουν αμοιβές από άδειες. Ο κύριος στόχος τους είναι να διευκολύνουν την ανταλλαγή των έργων που προστατεύονται από πνευματικά δικαιώματα, τη μεταγενέστερη νόμιμη χρήση τους, την ανταλλαγή τους, την επαναχρησιμοποίησή τους με τη σχετική απόδοση και την απαλλαγή από σχετικές υποχρεώσεις και εγγυήσεις. Η επίτευξη τέτοιων στόχων δεν συμβιβάζεται με την πολυπλοκότητα των διατυπώσεων που απαιτούνται για την πληρωμή των τελών άδειας σε μετρητά ή μέσω παραδοσιακών χρηματοπιστωτικών ιδρυμάτων.

[14] https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf
[15] https://opensource.org/osd

Η προσπάθεια χρησιμοποίησης του ηλεκτρονικού χρήματος ως φθηνού και βολικού μέσου μικροπληρωμών απέτυχε λόγω της έλλειψης πραγματικών παγκόσμιων συστημάτων πληρωμών ηλεκτρονικού χρήματος, τα οποία με τη σειρά τους οφείλονταν στην ποικιλομορφία των εθνικών νομοθεσιών και σε διάφορους ρυθμιστικούς περιορισμούς, όπως η νομισματική πολιτική, ο έλεγχος των νομισματικών ισοτιμιών, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες και άλλες νομοθετικές διατάξεις που σχετίζονται με το δημόσιο δίκαιο. Αντίθετα, τα περισσότερα επιχειρηματικά μοντέλα του Διαδικτύου βασίζονται στην επεξεργασία δεδομένων του χρήστη(τα προσωπικά δεδομένα έγιναν αξιοποιήσιμα περιουσιακά στοιχεία[16]) καθιστώντας έτσι εύκολο το δικαίωμα επεξεργασίας μέσω τυποποιημένων συμφωνιών όπως οι "Όροι χρήσης". Ωστόσο, τα προσωπικά δεδομένα ενός χρήστη του Διαδικτύου έχουν αξία για επεξεργασία μόνο εάν η ποσότητά τους είναι σημαντική και επιτρέπει τη δημιουργία γνώσεων. Ο συντάκτης ενός έργου που προστατεύεται από πνευματικά δικαιώματα δεν πληροί αυτά τα κριτήρια στις περισσότερες περιπτώσεις. Χρειάζεται κάτι πιο απτό και άμεσο σε αξία, όπως επίσης ευκολία χρήσης και παγκόσμια εμβέλεια. Χωρίς αυτή, είναι πραγματικά δύσκολο για τους δημιουργούς του ψηφιακού περιεχομένου να λαμβάνουν δίκαιη αποζημίωση για την εργασία τους.

Ένα άλλο πρόβλημα που υπάρχει είναι οι μεσάζοντες και οι υπηρεσίες ροής(Streaming). Η εισαγωγή υπηρεσιών ροής όπως το Spotify οδήγησε σε αύξηση της κατανάλωσης μουσικής καθώς και των συνολικών εσόδων της μουσικής βιομηχανίας. Αν και η ανάπτυξη της μουσικής βιομηχανίας είναι από πολλές απόψεις επωφελής, έχει καταστροφικό αποτέλεσμα για τις πωλήσεις τραγουδιών τόσο σε φυσικό όσο και σε ψηφιακό επίπεδο, έχοντας αλλάξει τη δομή ολόκληρης της βιομηχανίας. Μόνο το 2016, οι συνολικές πωλήσεις άλμπουμ και λήψεις τραγουδιών μειώθηκαν κατά 13,9% και 23,8% αντίστοιχα[17]. Η μετατόπιση αυτή της ιδιοκτησίας στις υπηρεσίες ροής είχε σαν αποτέλεσμα τα έσοδα να μετακινούνται μακριά από καλλιτέχνες και τραγουδοποιούς. Οι καλλιτέχνες λαμβάνουν μικρότερες αμοιβές και έχουν λιγότερη γνώση σχετικά με τον τρόπο τιμολόγησης, κοινής χρήσης ή διαφήμισης των έργων τους. Για παράδειγμα, στο Spotify θα χρειαζόταν 120 έως 170 ροές ώστε οι κάτοχοι δικαιωμάτων να λάβουν τα πρώτα τους χρήματα[18].

[16] http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
[17] http://www.buzzanglemusic.com/wp-content/uploads/BuzzAngle-Music-2017-Mid-Year-U.S.-Report.pdf
[18] https://www.weforum.org/agenda/2017/07/how-can-creative-industries-benefit-from-blockchain/

Λαμβάνοντας υπόψη τη διαπραγματευτική ισχύ τέτοιων διαδικτυακών διαμεσολαβητών, είναι δύσκολο να αναμένεται δικαιότερη κατανομή των εσόδων για τους δημιουργούς. Συνεπώς, υπάρχει ανάγκη για νέες προσεγγίσεις σχετικά με την πληρωμή αμοιβών για άδειες, οι οποίες θα είναι δίκαιες, εύχρηστες και θα έχουν πιθανή παγκόσμια εμβέλεια.

# 17 Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΩΣ ΜΕΣΟ ΕΠΙΛΥΣΗΣ ΝΟΜΙΚΩΝ ΖΗΤΗΜΑΤΩΝ ΨΗΦΙΑΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ

Η τεχνολογία Blockchain λόγω της αρχιτεκτονικής της έχει τη δυνατότητα να αλλάξει τον τρόπο με τον οποίο διανέμεται το περιεχόμενο που προστατεύεται από πνευματικά δικαιώματα σε ένα ψηφιακό κόσμο. Πιο συγκεκριμένα μπορεί να επιτρέψει την διαβαθμισμένη πρόσβαση σε συγκεκριμένες πληροφορίες ανάλογα με την κυριότητα των πνευματικών δικαιωμάτων, την διαφάνεια και την δυνατότητα ανίχνευσης των αλλαγών που θα προκύψουν. Επιπλέον, άμεση πληρωμή των τελών-κόστους και η κατοχή τεχνητής κυριαρχίας επί του ψηφιακού περιεχομένου θα γίνει πιο ελκυστική για τους κατόχους ψηφιακών δικαιωμάτων. Η απλοποιημένη διαδικασία χορήγησης αδειών με τη χρήση αυτοματοποιημένων έξυπνων συμβάσεων θα μειώσουν σημαντικά το κόστος συναλλαγής τόσο για τους κατόχους δικαιωμάτων όσο και για τους χρήστες και θα προστατεύσουν τους τελευταίους από τις ανησυχίες για παραβίαση πνευματικών δικαιωμάτων.

Η κρυπτογραφία αλλά και η εφαρμογή ενός αποκεντρωμένου μητρώου, στο οποίο θα αποθηκεύονται τα δεδομένα, θα προσφέρει παγκόσμια πρόσβαση για κάθε λήψη και ροή αρχείων. Παράλληλα, η καθημερινή παρακολούθηση συναλλαγών θα παρείχε όλες τις απαραίτητες πληροφορίες για δίκαιη πληρωμή τόσο για τους δημιουργούς όσο και για τους ενδιάμεσους. Επίσης, η συλλογή μεταδεδομένων, τα οποία θα περιέχουν στοιχεία για τους καλλιτέχνες, τους συγγραφείς, τους δημιουργούς και τους εκδότες θα μπορούσαν να αποδειχθούν χρήσιμα στατιστικά με την κατοχή και διάθεση πνευματικών δικαιωμάτων και αδειών.

Ωστόσο, η εφαρμογή της τεχνολογίας Blockchain προϋποθέτει την επίλυση ζητημάτων τα οποία μπορούν να λειτουργήσουν αρνητικά αν δεν γίνει έγκαιρα η αντιμετώπισή τους. Ένα από αυτά τα ζητήματα είναι η αρχιτεκτονική σχεδίαση του συστήματος καθώς και οι νομικές επιπτώσεις που θα δημιουργηθούν. Για παράδειγμα, το ψηφιακό περιεχόμενο θα αποθηκευτεί στο Blockchain μαζί με τα μεταδεδομένα ή χωριστά. Καθεμία από αυτές τις λύσεις έχει οφέλη και

προκλήσεις. Ένα άλλο ζήτημα που προκύπτει είναι η παραμετροποίηση του συστήματος λαμβάνοντας υπόψη τα δικαιώματα που θα έχουν οι κρατικές αρχές. Τα αρχεία του Blockchain πρέπει να τροποποιηθούν σύμφωνα με τις αποφάσεις των δικαστηρίων και των κρατικών αρχών, διαφορετικά η συγκεκριμένη τεχνολογία θα γίνει εχθρός του κράτους και όχι σύμμαχός του.

Η μη μεταβλητότητα των εγγραφών του Blockchain είναι το κύριο χαρακτηριστικό το οποίο παρέχει εμπιστοσύνη ανάμεσα στα συναλλασσόμενα μέρη. Επομένως, η εύρεση της σωστής ισορροπίας μεταξύ των συναλλασσόμενων μερών θα έχει αντίκτυπο στην ελκυστικότητα ενός τέτοιου συστήματος τόσο για τους κατόχους δικαιωμάτων όσο και για τους χρήστες. Λόγω των επιπτώσεων στο δίκτυο, η επαρκής παρουσία και των δύο μερών είναι κρίσιμης σημασίας για την επιτυχία οποιουδήποτε συστήματος διαχείρισης πνευματικών δικαιωμάτων.

Τέλος, είναι απαραίτητο να αντιμετωπιστούν πολλαπλά νομικά ζητήματα που σχετίζονται με την εφαρμογή των συστημάτων Blockchain σχετικά με τα πνευματικά δικαιώματα στην νομική πραγματικότητα. Κρίσιμης σημασίας θεωρείται η προσαρμογή του νομικού πλαισίου περί πνευματικών δικαιωμάτων στη χρήση της συγκεκριμένης τεχνολογίας, παρέχοντας τις απαραίτητες εγγυήσεις για την ορθή λειτουργία του. Παράλληλα, η εφαρμογή του Blockchain δύναται να χρησιμοποιηθεί και πέρα από αυτόν τον τομέα, αφού θα είναι δυνατή η εφαρμογή τέτοιων συστημάτων για άλλα αντικείμενα πνευματικής ιδιοκτησίας που θα οδηγήσουν στην εμφάνιση συγκεκριμένου τύπου πνευματικής ιδιοκτησίας όπως για παράδειγμα “Smart IP”[19].

## 17.1 ΔΙΑΦΑΝΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΙΔΙΟΚΤΗΣΙΑ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ.

Η τεχνολογία Blockchain μπορεί να αυξήσει σημαντικά την προβολή και τη διαθεσιμότητα των πληροφοριών σχετικά με την ιδιοκτησία των πνευματικών δικαιωμάτων. Τέτοιες πληροφορίες μπορούν να παρέχονται μέσω της λεγόμενης “Αξιόπιστης χρονικής σήμανσης(Trusted Timestamping)”. Η χρονοσήμανση είναι μια ακολουθία χαρακτήρων ή κωδικοποιημένων πληροφοριών που προσδιορίζουν πότε συμβαίνει ένα συγκεκριμένο συμβάν, δίνοντας συνήθως ημερομηνία και ώρα της ημέρας, μερικές φορές με τόσο ακρίβεια η οποία εκφράζεται ακόμα και

[19] http://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html

σε κλάσματα του δευτερολέπτου[20]. Η αξιόπιστη χρονική σήμανση[21], είναι η διαδικασία για την ασφαλή παρακολούθηση του χρόνου δημιουργίας και τροποποίησης ενός εγγράφου και αποτελεί ένα απαραίτητο εργαλείο στον σύγχρονο επιχειρηματικό κόσμο, καθώς επιτρέπει στα ενδιαφερόμενα μέρη να γνωρίζουν χωρίς καμία αμφιβολία ότι το συγκεκριμένο έγγραφο υπήρξε τη συγκεκριμένη ημερομηνία και ώρα, στοιχείο κρίσιμο για τη διατήρηση της αξιοπιστίας των συμβαλλόμενων.

Η τεχνολογία Blockchain μπορεί να θεωρηθεί ως μια βάση δεδομένων η οποία περιέχει επαληθευμένες δημόσιες χρονικές σημάνσεις. Δίνει τη δυνατότητα σε οποιονδήποτε χρήστη να δηλώσει δημόσια και αμετάκλητα ένα συγκεκριμένο γεγονός το οποίο συνέβη σε ένα συγκεκριμένο χρονικό σημείο. Έτσι το Blockchain μπορεί να αποδειχθεί πολύ χρήσιμο στη διαδικασία τεκμηρίωσης του συγγραφέα ενός έργου συμβάλλοντας στην επίλυση τέτοιων ζητημάτων στον τομέα των πνευματικών δικαιωμάτων. Σύμφωνα με τη Melanie Swan, "οι άνθρωποι μπορούν να χρησιμοποιήσουν την τεχνολογία Blockchain για να κατακερματίσουν πράγματα όπως οι τέχνες και το λογισμικό για να αποδείξουν την κυριότητα των έργων τους". [2]

Η λειτουργία κατακερματισμού(Hash) αποτελεί τη βάση για τη την ασφάλεια και την μη μεταβλητότητα των δεδομένων. Μέσω της συνάρτησης κατακερματισμού, η οποία είναι ένας μαθηματικός τύπος συνάρτησης που μετατρέπει τα αρχικά δεδομένα σε μια αναπαράσταση σταθερού μεγέθους  που μοιάζει με τυχαία δεδομένα και ονομάζεται Hash, ένας συγγραφέας ή κάποιος κάτοχος δικαιώματος μπορεί να αποκτήσει ένα μοναδικό κομμάτι του έργου που προστατεύεται από πνευματικά δικαιώματα. Δύο κομμάτια μπορεί να είναι ίδια μόνο αν τα αρχικά δεδομένα είναι ίδια. Ακόμα και μικρές διαφορές θα οδηγήσουν σε διαφορετικό Hash. Αυτός ο τρόπος κατακερματισμού διακρίνει εάν ένα έργο προστατεύεται από πνευματικά δικαιώματα σε σχέση με ένα άλλο. Εάν υπάρχει κάποια συναλλαγή με μια εργασία που προστατεύεται από πνευματικά δικαιώματα(π.χ. άδεια χρήσης), ένα hash της εργασίας αυτής περιλαμβάνεται στη συναλλαγή και αφού επαληθευτεί σύμφωνα με το πρωτόκολλο Blockchain(με τη διαδικασία της εξόρυξης), δίνεται χρονική σήμανση στη συναλλαγή και το περιεχόμενο της συναλλαγής κωδικοποιείται σε ένα blockchain. Αυτό έχει ως αποτέλεσμα, οι πληροφορίες σχετικά με την ιδιοκτησία των πνευματικών δικαιωμάτων και τις αλλαγές που έχουν πραγματοποιηθεί, να αποθηκεύονται σε ένα Blockchain χαρακτηριζόμενες πρώτον από έναν χρονικό προσδιορισμό και

[20] https://en.wikipedia.org/wiki/Timestamp
[21] https://www.ietf.org/rfc/rfc3161.txt

δεύτερον χωρίς να παρέχεται η δυνατότητα αλλαγής ή παραποίησής του. [31]. Έτσι, τα αρχεία σχετικά με τη ιδιοκτησία ενός έργου το οποίο προστατεύεται από πνευματικά δικαιώματα πρέπει να αποτυπώνονται αμετάβλητα στη βάση δεδομένων του Blockchain και επομένως να μπορούν εύκολα να επαληθευτούν από οποιονδήποτε ενδιαφερόμενο.

Η υλοποίηση μιας τέτοιας τεχνολογίας μπορεί να αντικαταστήσει τους υπάρχοντες δυσκίνητους μηχανισμούς απόδειξης της δημιουργίας ενός έργου που προστατεύεται από πνευματικά δικαιώματα(π.χ. εγγραφή λογισμικού στα γραφεία διπλωμάτων ευρεσιτεχνίας). Επιπλέον, το Blockchain αυξάνει το επίπεδο εμπιστοσύνης καθώς και τη δυνατότητα κλιμάκωσης καθώς η χρήση χρονοσήμανσης ή ενός ψηφιακού δακτυλικού αποτυπώματος επιτρέπει την απαλλαγή από ενδιαμέσους στο διαδίκτυο. Επομένως, ο τρόπος χρήσης της συγκεκριμένης τεχνολογίας εξαρτάται σε μεγάλο βαθμό από πολιτική της συγκεκριμένης πλατφόρμας που εφαρμόζεται καθώς και από την υποδομή της. Η σωστή χρήση του Blockchain, αρχή του οποίου είναι η αποκεντρωμένη διαχείριση, σύμφωνα με την οποία δεν υπάρχει εξάρτηση από κάποιο συγκεκριμένο πάροχο καθώς επίσης και το γεγονός ότι οι όροι χρήσης μπορούν να ενσωματωθούν στον κώδικα ώστε οποιαδήποτε αλλαγή τους θα απαιτούσε τη συναίνεση όλων των χρηστών του δικτύου. Η χρήση ενός τέτοιου συστήματος μπορεί να αποδειχθεί πιο αξιόπιστη και βιώσιμη μακροπρόθεσμα.

Εκτός αυτού, αν το μητρώο βασίζεται στην τεχνολογία Blockchain, τα αντίγραφά του είναι διαθέσιμα σε όλους τους χρήστες παρέχοντάς τους έτσι τη δυνατότητα να παρακολουθούν τις καταγραφές σχετικά με την ιδιοκτησία των πνευματικών δικαιωμάτων, τα οποία δεν θα χαθούν σε περίπτωση που μια εταιρεία έχανε τη βάση δεδομένων στα οποία θα ήταν αποθηκευμένα. Η μη-μεταβλητότητα η οποία αποτελεί θεμελιώδη αρχή του Blockchain εξασφαλίζει ότι το περιεχόμενο δεν θα αλλοιωθεί. Αυξάνει την αξιοπιστία των εγγραφών δίνοντας έτσι μια νέα δυνατότητα στους συγγραφείς και κατόχους πνευματικών δικαιωμάτων, αυτή της χρήση τους ως αποδεικτικά στοιχεία σχετικά με την κατοχή των συγκεκριμένων δικαιωμάτων σε περιπτώσεις δικαστικής διαμάχης.

Οι Kishigami, Fujimura, Watanabe, Nakadaira, & Akutsu περιέγραψαν ένα σύστημα διανομής περιεχομένου με βάση την τεχνολογία Blockchain. Το σύστημα αυτό διαχειρίζεται δικαιώματα πρόσβασης σε 4K βίντεο, το οποίο επιτρέπει στους κατόχους πνευματικών δικαιωμάτων να διαχειρίζονται τα δικαιώματα του περιεχομένου, συμπεριλαμβανομένης της κατάργησης του δικαιώματος χρήσης περιεχομένου από έναν χρήστη. Αυτό το σύστημα δεν

επιτρέπει την προβολή του περιεχομένου εκτός δικτύου, αφού ο πελάτης απαιτείται να έχει ένα αναγνωριστικό συναλλαγής από τους miners του δικτύου για να αποκωδικοποιήσει το περιεχόμενο. [32]

## 17.2 ΙΔΙΟΚΤΗΣΙΑ ΠΕΡΙΕΧΟΜΕΝΟΥ

Η τεχνολογία blockchain μπορεί να επαναπροσδιορίσει την έννοια της ιδιοκτησίας σε σχέση με το πως τη γνωρίζουμε σήμερα. Από το άτυχο εκείνο συμβάν του Ιουλίου του 2009, όπου η Amazon έσβησε εξ αποστάσεως τις ψηφιακές εκδόσεις δύο βιβλίων του George Orwell[22] το "1984" και το "Φάρμα των ζώων", τα οποία είχαν πουληθεί στην Amazon με την άδεια ενός εκδότη(MobileReference) ο οποίος όπως διαπιστώθηκε αργότερα δεν είχε τα ανάλογα πνευματικά δικαιώματα για τα έργα αυτά, γίνεται κατανοητό ότι το ψηφιακό περιεχόμενο δεν μπορεί να δημιουργείται, να αποκτάται και να προφυλάσσεται με τον ίδιο τρόπο όπως γίνεται με το φυσικό περιεχόμενο. Το ψηφιακό περιεχόμενο με την εξέλιξη που έχει επέλθει στον τομέα της τεχνολογίας, δεν μπορεί να είναι ασφαλές τόσο στο "σύννεφο" (cloud) μιας εταιρείας, όσο και σε έναν προσωπικό υπολογιστή.

Ο διαδικτυακός εκδοτικός οίκος Editions at Play, δημιούργησαν το "A Universe Explodes", ένα βιβλίο το οποίο είναι σχεδιασμένο σε Blockchain και έχει σκοπό να δείξει στους ανθρώπους, πως λειτουργεί η τεχνολογία αυτή αλλά και το πώς θα μπορούν οι άνθρωποι να αποκτήσουν ένα διαδικτυακό βιβλίο. Επιπλέον, οι Herbert Jeff και Litchfield Alan [32] χρησιμοποιήσαν την τεχνολογία Blockchain για την επικύρωση άδειας λογισμικού. Οι συγγραφείς προσδιορίζουν δύο μορφές Blockchain στην επικύρωση της άδειας. Στο "Master Bitcoin Model", ο καταναλωτής αποδεικνύει την ιδιοκτησία δείχνοντας ότι κατέχει ένα Bitcoin που προέρχεται από τον προμηθευτή του λογισμικού. Το "Bespoke Model" είναι ίδιο με το προηγούμενο, με διαθέσιμα πρόσθετα πεδία δεδομένων. Αυτό επιτρέπει στον κατασκευαστή του λογισμικού να αποθηκεύει τις πληροφορίες άδειας χρήσης όπως ο χρόνος μέχρι την λήξη της άδειας. Το "Bespoke Model" υλοποιήθηκε για έναν μόνο χρήστη ο οποίος είναι κάτοχος μιας ενιαίας άδειας. Οι μελλοντικές εργασίες που αναφέρονται στην συγκεκριμένη δημοσίευση θα επιτρέπουν στους

[22] https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html

πελάτες να κατέχουν εκατοντάδες αντίγραφα αδειών. Ένα άλλος τομέας που μπορεί η τεχνολογία αυτή να παίξει καθοριστικό ρόλο είναι η λεγόμενη πρώτη ψηφιακή πώληση. Το κύριο πρόβλημα με τα ηλεκτρονικά βιβλία (eBooks) είναι ότι δεν υπάρχουν ψηφιακά δικαιώματα πρώτης πώλησης. Κάποιος ο οποίος αγοράζει ένα εκτυπωμένο βιβλίο μπορεί να το πουλήσει σε αντίθεση με ένα ψηφιακό βιβλίο, το οποίο δεν μπορεί να το πουλήσει. Ένα επιχείρημα το οποίο δικαιολογεί αυτή την άποψη είναι ότι δεν είναι δυνατόν να αποδειχθεί η ιδιοκτησία των ηλεκτρονικών βιβλίων και κατά συνέπεια η πώλησή τους. Με τη χρήση της τεχνολογίας blockchain, μπορεί κάποιος να παρακολουθήσει την ιδιοκτησία ενός ηλεκτρονικού βιβλίου και να δέχεται συνεχή ενημέρωση για το πώς συναλλάσσεται αυτό, μεταξύ των ενδιαφερομένων. Τα στοιχεία αυτά, μαζί με τα αποδεδειγμένα δικαιώματα πρώτης πώλησης θα είναι διαθέσιμα δημόσια, δίνοντας στους εκδότες πολλά δεδομένα.

Οι McConaghy Trent και Holtzman David [30] χρησιμοποιήσαν το Blockchain του Bitcoin για να καταγράψουν την ιδιοκτησία μιας εικόνας. Το μητρώο αποθηκεύει τους όρους χρήσης καθώς και τη χρονική σήμανση. Το μητρώο αυτό αποθηκεύεται στο Blockchain μαζί με τις πληροφορίες ιδιοκτησίας. Ένα πρόγραμμα ανίχνευσης του ιστού χρησιμοποιεί μηχανική μάθηση για τον εντοπισμό εικόνων που έχουν εντοπιστεί σε κάποιον ιστότοπο χωρίς την άδεια του ιδιοκτήτη. [33]

## 17.3 ΈΛΕΓΧΟΣ ΨΗΦΙΑΚΩΝ ΑΝΤΙΓΡΑΦΩΝ

Κάθε ψηφιακό αντίγραφο του έργου που προστατεύεται από πνευματικά δικαιώματα είναι το ίδιο και δεν μπορεί να διακριθεί από τα άλλα ελέγχοντας την ποιότητά του. Με τη χρήση της τεχνολογίας Blockchain παρέχεται εξατομίκευση σε κάθε ψηφιακό αντίγραφο που προστατεύεται από πνευματικά δικαιώματα, μέσω της συνάρτησης κατακερματισμού και της αξιόπιστης χρονικής σήμανσης. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού βελτιστοποιούνται για να δημιουργήσουν ένα μοναδικό Hash με μικρές πιθανότητες σύγκρουσης, κάτι το οποίο σημαίνει ότι οι εισροές με μικρές διαφορές δημιουργούν πολύ διαφορετικά Hashes. Επομένως, μια συνάρτηση κατακερματισμού μπορεί να χρησιμοποιηθεί για να εκδίδει νέα και μοναδικά αναγνωριστικά για κάθε αντίγραφο, τα οποία μπορεί να έχουν μικρές διαφορές μεταξύ τους(π.χ.

η προσθήκη αύξοντα αριθμού σε κάθε ψηφιακό αντίγραφο θα δημιουργήσει διαφορετικό Hash ακόμα και αν το περιεχόμενο παραμείνει το ίδιο).

Η λειτουργικότητα της υπηρεσίας διαχείρισης δικαιωμάτων πνευματικής ιδιοκτησίας παρέχει τη δυνατότητα εκχώρησης ξεχωριστών όρων άδειας χρήσης σε κάθε αντίγραφο όπως για παράδειγμα, ένα αντίγραφο μπορεί να παρέχεται με δικαιώματα τροποποίησης ενώ ένα άλλο με περιορισμένα δικαιώματα δημόσιας πρόσβασης μέσω διαδικτύου. Επιπλέον, είναι δυνατόν να εκχωρηθούν διαφορετικοί τύποι αδειών ανοιχτού κώδικα σε κάθε αντίγραφο κώδικα που βρίσκεται σε κάποιον υπολογιστή του δικτύου Blockchain.

Η εξατομίκευση κάθε ψηφιακού αντιγράφου του περιεχομένου μαζί με τη δυνατότητα παρακολούθησης του ιστορικού και της πορείας του καθενός, δημιουργούν τις απαραίτητες προϋποθέσεις για την τεχνολογική άνθηση των δευτερογενών αγορών ψηφιακού περιεχομένου. Η εφαρμογή της τεχνολογίας Blockchain στον τομέα της μεταπώλησης αρχείων ψηφιακής μουσικής, ταινιών και ηλεκτρονικών βιβλίων μέσω διαδικτύου, θα δώσει τη δυνατότητα στους κατόχους δικαιωμάτων τόσο να ελέγχουν τη μεταγενέστερη διανομή όσο και να λαμβάνουν ανταμοιβή για τη χρήση τους. Παράλληλα, η παρακολούθηση του χρήστη που χρησιμοποιεί ένα συγκεκριμένο αντίγραφο ενός έργου που προστατεύεται από πνευματικά δικαιώματα είναι εφικτή και κρίσιμης σημασίας για την λήψη κατάλληλων μέτρων σε περιπτώσεις παραβίασης από τον δημιουργό του έργου.

## 17.4 ΣΤΟΙΧΕΙΑ ΔΗΜΙΟΥΡΓΙΑΣ

Η τεχνολογία Blockchain μπορεί να διαδραματίσει σημαντικό ρόλο στο πλαίσιο των μη εγγεγραμμένων δικαιωμάτων πνευματικής ιδιοκτησίας, όπως το “copyright” το οποίο σε πολλές δικαιοδοσίες και υπό τους όρους της Σύμβασης της Βέρνης[23] για την προστασία των λογοτεχνικών και καλλιτεχνικών έργων, δεν μπορεί να εγγραφεί σαν δικαίωμα πνευματικής ιδιοκτησίας. Επιπλέον, τα μη καταχωρημένα δικαιώματα επί σχεδίων και υποδειγμάτων μπορούν να κατοχυρωθούν δεδομένου ότι μπορούν να παρασχεθούν αποδεικτικά στοιχεία σχετικά με τη

[23] http://www.wipo.int/wipolex/en/text.jsp?file_id=216359

σύλληψή τους, τη χρήση τους καθώς και τα απαραίτητα πιστοποιητικά σχετικά με την πρωτοτυπία ή την χώρα στην οποία εμφανίστηκαν για πρώτη φορά.

Η εισαγωγή ενός πρωτότυπου σχεδίου ή έργου και οι λεπτομέρειες του σχεδιαστή ή του δημιουργού του, σε ένα Blockchain θα δημιουργήσουν ένα χρονικά σφραγισμένο αρχείο καθώς και ισχυρά αποδεικτικά στοιχεία για να αποδειχθούν τέτοιου είδους θέματα. Τα κατανεμημένα συστήματα αποθήκευσης της συγκεκριμένης τεχνολογίας, θα μπορούσαν να αποτελέσουν μια ενδιαφέρουσα λύση για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας καθώς και για διαχείριση και καταγραφή των μη καταγεγραμμένων δικαιωμάτων κυριότητας. [34]

## 17.5 ΑΥΤΟΜΑΤΕΣ ΠΛΗΡΩΜΕΣ

Η τεχνολογία Blockchain έγινε γνωστή από τη δημιουργία των κρυπτονομισμάτων, τα οποία διευκόλυναν ένα παγκόσμιο σύστημα πληρωμών, που δεν περιπλέκεται με τις διαδικασίες που συνδέονται με τη δημιουργία ενός τραπεζικού λογαριασμού. Τα πιο δημοφιλή από αυτά είναι το Bitcoin και το Ethereum, τα οποία έχουν πραγματική αγοραία αξία[24] και δεν απαιτούν πολύπλοκες διαδικασίες για τη χρήση τους. Έχουν παγκόσμια εμβέλεια και είναι διαθέσιμα σε όλους όσους έχουν πρόσβαση στο διαδίκτυο, καθιστώντας τα, ιδανικά μέσα πληρωμών για την παροχή άδειας για τη χρήση ψηφιακού περιεχομένου στο διαδίκτυο. Έτσι η χρήση κρυπτονομισμάτων αποτελεί την ιδανικότερη λύση στο πρόβλημα της δίκαιης αποζημίωσης των δημιουργών στον διαδίκτυο, γεγονός που δεν συνεπάγεται εξάρτηση από μεσάζοντες. Επιπλέον, ένα από τα βασικά στοιχεία της συγκεκριμένης λύσης είναι η δυνατότητα χρήσης έξυπνων συμβολαίων.

Τα έξυπνα συμβόλαια θα επιτρέψουν την αυτόματη και άμεση πληρωμή προς τα συμβαλλόμενα μέρη καθώς και την εκπνοή της άδειας χρήσης αρχείων μετά από ορισμένο χρονικό διάστημα. Τα δικαιώματα θα μπορούσαν μέσω αυτών των συμβολαίων να είναι πιο περιεκτικά, προσφέροντας δικαιότερους όρους για τους συνθέτες, τους στιχουργούς και τους μουσικούς και γενικότερα όλους τους εμπλεκόμενους στη διαδικασία δημιουργίας. Παράδειγμα τέτοιων λύσεων αποτελεί το PeerTracks.com[25] το οποίο είναι μια υπηρεσία για καλλιτέχνες που αναζητούν άμεσες

[24] https://www.coindesk.com/price/
[25] https://peertracks.com/

πληρωμές δικαιωμάτων και κυριότητα του περιεχομένου τους. Η συγκεκριμένη υπηρεσία λειτουργεί προσαρτώντας μια έξυπνη σύμβαση σε κάθε τραγούδι που "ανεβάζει" ένας καλλιτέχνης, μοιράζοντας τα έσοδα σύμφωνα με τους όρους που ορίζει η σύμβαση. Εκτός των ανωτέρω, η συγκεκριμένη λύση παρέχει ένα πρωτοφανές επίπεδο διαφάνειας, αφού οι δικαιούχοι μπορούν να δουν απευθείας τη ροή εσόδων τους καθώς και τα σχόλια από τους οπαδούς τους.

## 17.6 ΑΠΛΟΥΣΤΕΡΗ ΑΔΕΙΑ ΧΡΗΣΗΣ

Η σύμβαση άδειας χρήσης είναι η μόνη αποδεκτή μέθοδος για τη για τη χρήση έργων τα οποία προστατεύονται από πνευματικά δικαιώματα. Η προετοιμασία της σύμβασης άδειας χρήσης και οι επακόλουθες διαπραγματεύσεις με τον πιθανό χρήστη δεν είναι εύκολη διαδικασία για έναν μέσο συντάκτη ο οποίος δεν είναι εξοικειωμένος με το νομικό πλαίσιο περί πνευματικών δικαιωμάτων. Η διαδικασία γίνεται ακόμα πιο περίπλοκη από το γεγονός ότι δεν υπάρχει δίκαιο το οποίο να αναφέρεται στην άδεια χρήσης όπως για παράδειγμα είναι το δίκαιο περί πνευματικής ιδιοκτησίας. Υπάρχει μια ποικιλομορφία στους νόμους γύρω από αυτό το πλαίσιο που κάθε χώρα προσπαθεί να προσαρμοστεί υιοθετώντας και τροποποιώντας τους σχετικούς νόμους. Η ποικιλομορφία στην ορολογία, τα δόγματα πνευματικής ιδιοκτησία και η νομολογία παραμένουν και δημιουργούν πολλές πολύπλοκες διαδικασίες και μεγάλα κόστη ακόμα και για μεγάλες διακρατικές εταιρείες. Γίνεται έτσι κατανοητό ότι οι συμφωνίες παραχώρησης άδειας για έργα που προστατεύονται από πνευματικά δικαιώματα, τα οποία προορίζονται να διανεμηθούν σε διασυνοριακό περιβάλλον, θα πρέπει να λαμβάνουν υπόψη αυτή την ποικιλομορφία, απαιτώντας εξειδικευμένη βοήθεια νομικών προσώπων όπως επίσης και τα έξοδα συναλλαγών είναι δύσκολο να γίνουν αποδεκτά από έναν μέσο κάτοχο δικαιωμάτων.

Η εξάπλωση του Ελεύθερου Λογισμικού ή Λογισμικού Ανοιχτού Κώδικα(ΕΛ/ΛΑΚ) καθώς και η δημιουργία του Κινήματος Ανοιχτού Κώδικα(Open Source Movement) το οποίο δεν σχετίζεται με θέματα software μόνο, προάγει τη νομιμότητα, τον διαμοιρασμό και την επαναχρησιμοποίηση κώδικα, περιεχομένου, δηλαδή κειμένων, μουσικής ταινιών, πληροφοριών, δεδομένων, αρχείων και γνώσης εισάγοντας τους χρήστες σε έναν κόσμο που λειτουργεί και πράττει βάσει ενός διαφορετικού συστήματος αξιών. Σε κάποιο βαθμό, έχουν επιλυθεί μέσω

αυτών τα παραπάνω προβλήματα μέσω ειδικών τύπων (Creative Common Licenses) [26], τυποποιημένων συμφωνιών παραχώρησης άδειας χρήσης που μπορούν να χρησιμοποιηθούν για την ανταλλαγή λογισμικού και άλλων έργων που προστατεύονται από πνευματικά δικαιώματα σε παγκόσμια κλίμακα. Η αναγνώριση αυτών των συμβατικών μέσων είναι πολύ υψηλή και συνεχίζει να αυξάνεται καθώς διευκολύνουν την κοινή χρήση έργων που προστατεύονται από πνευματικά δικαιώματα στο διαδίκτυο.

Υπάρχει ένα βασικό πρόβλημα με τέτοιου τύπους συμφωνιών αδειοδότησης· είναι απαλλαγμένα από δικαιώματα εκμετάλλευσης. Η χρήση των έργων σύμφωνα με τους όρους τους δεν απαιτεί την πληρωμή οποιουδήποτε τέλους, μόνο την παραχώρηση και τη συμμόρφωση με τους προβλεπόμενους περιορισμούς χρήσης. Αυτό αρκεί για τους ιδιοκτήτες δικαιωμάτων που είναι πρόθυμοι να μοιραστούν τα έργα τους ελεύθερα, αλλά δύσκολα αποδεκτά για εκείνους που θέλουν να εμπορευματοποιηθούν οι προσπάθειές τους.

Η τεχνολογία Blockchain επιτρέπει τη χρήση νέου τύπου πληρωμών μέσω κρυπτονομισμάτων, η οποία με τη σειρά της μπορεί να χρησιμοποιηθεί ως αντάλλαγμα στις συμφωνίες παραχώρησης άδειας εκμετάλλευσης. Με τον τρόπο αυτό δίνεται η δυνατότητα να συνδυαστεί η απλή χρήση αδειών ανοιχτού κώδικα με την απόδειξη παραλαβής της άδειας χρήσης από τον πάροχο του δικαιώματος. Επιπλέον, η χρήση έξυπνων συμβολαίων μπορεί να διευκολύνει τη διαδικασία παροχής αδειών καθώς οι όροι των συμβάσεων αυτών μπορούν να περιγραφούν σε κατανοητή γλώσσα κάτι το οποίο γίνεται ήδη σε ότι αφορά τις άδειες Creative Commons. Ένας συγγραφέας ή κάποιος άλλος δικαιούχος που επιθυμεί να επωφεληθεί από τις πληρωμές μέσω κρυπτονομισμάτων μπορεί είτε να επιλέξει ένα ήδη υπάρχον πρότυπο έξυπνου συμβολαίου είτε να δημιουργήσει ένα νέο, και να προσαρμόσει τους όρους χρήσης της άδειας ακόμη και με διάσπαση μεταξύ διαφόρων δικαιούχων(π.χ. συγγραφείς).

[26] https://creativecommons.ellak.gr/

# 18 ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΕΠΙΣΤΗΜΟΝΙΚΗ ΔΙΑΔΙΚΑΣΙΑ

Η επιστημονική γνώση είναι αναμφισβήτητα το απόλυτο αποκεντρωμένο σύστημα, ιδιαίτερα τα τελευταία χρόνια όπου έγινε η μετάβαση από το αναλογικό περιεχόμενο στο ψηφιακό. Το επιστημονικό σύστημα δεν ελέγχεται από κάποια κεντρική αρχή και από τη φύση της απαιτεί δημόσιο έλεγχο και συνεχές προκλήσεις. Όμως, παρόλη την διαφάνεια και την αντικειμενικότητα που το χαρακτηρίζει, η σημερινή επιστημονική κοινότητα δεν λειτουργεί κατ' αυτόν τον τρόπο.

Το σημερινό σύστημα ακαδημαϊκής επικοινωνίας βασίζεται στον παραδοσιακό τρόπο που εδώ και χρόνια χρησιμοποιεί ξεπερασμένες μεθόδους για να λειτουργήσει και δεν ανταποκρίνεται στις σύγχρονες απαιτήσεις της έρευνας. Η διάδοση των επιστημονικών αποτελεσμάτων γίνεται κυρίως με τη μορφή συμβατικών άρθρων σε επιστημονικά περιοδικά ή πανεπιστημιακά ιδρύματα και δεν έχει ενστερνιστεί τη σύγχρονη ερευνητική πρακτική. Επιπλέον, η διαδικασία δημοσιεύσεων ερευνητικών εργασιών βασίζεται στην διαδικασία της αναθεώρησης από ομότιμους χρήστες(Peer Review). Μια ομάδας από εμπειρογνώμονες διαβάζουν γρήγορα μια μελέτη, την αξιολογούν παρέχοντας συμβουλές και προτείνουν αν θα πρέπει να δημοσιευτεί. Παράλληλα, η αναπαραγωγιμότητα έχει αποδειχθεί ως μια εξαιρετικά λανθασμένη διαδικασία. Οι ομότιμοι χρήστες υπόκεινται σε σημαντική πίεση χρόνου κάτι το οποίο έχει σαν αποτέλεσμα την δυσκολία στην μέτρηση της αξιοπιστίας όπως επίσης σε μερικές περιπτώσεις την εμφάνιση μεροληπτικής στάσης από αυτούς.

Η επικοινωνία αποτελεί ουσιαστικό μέρος της έρευνας. Ως μια καθαρά συνεργατική προσπάθεια, η έρευνα εξαρτάται από την αποτελεσματική ανταλλαγή ιδεών, υποθέσεων, δεδομένων και αποτελεσμάτων. Η ανταλλαγή αυτή πρέπει να ξεπεράσει τα γεωγραφικά και χρονικά εμπόδια, επιτρέποντας στους ερευνητές να συνεργάζονται με συναδέλφους τους που βρίσκονται σε διαφορετικά μέρη του κόσμου ή και ακόμα, στην ίδια χώρα και να δημιουργήσουν γνώση ακολουθώντας τα χνάρια των προκατόχων τους.

Είναι γενικά αποδεχτό ότι ο τρόπος που γίνεται αυτή η επικοινωνία σε ακαδημαϊκό και επιστημονικό επίπεδο αντιμετωπίζει σοβαρές προκλήσεις. Η ακαδημαϊκή επικοινωνία θεωρείται ότι πάσχει από παλιά έργα, ξεπερασμένα παραδείγματα και επιστημονικά ενδιαφέροντα που είναι εκ διαμέτρου αντίθετα με το συμφέρον της επιστήμης και της σύγχρονης γνώσης. Η ομοσπονδιακή κυβέρνηση των ΗΠΑ ξοδεύει πάνω από 150 δισεκατομμύρια [27] δολάρια ετησίως για τη

[27] http://www.sciencemag.org/news/2017/05/how-science-fares-us-budget-deal

χρηματοδότηση της επιστημονικής έρευνας, η οποία αποτελεί μία από τις κύριες πηγές χρηματοδότησης της επιστημονικής κοινότητας. Παράλληλα, ακαδημαϊκοί ερευνητές δημοσιεύουν εκατομμύρια επιστημονικά έγγραφα κάθε χρόνο, εκτός από άλλου είδους δημοσιεύσεων. Ωστόσο παρά το τεράστιο ποσό χρημάτων και χρόνου που αφιερώνει η ακαδημαϊκή κοινότητα στην έρευνα, η ικανότητα των μελετητών να εντοπίζουν και να παρακολουθούν τις πληροφορίες που προκύπτουν είναι περιορισμένη για πολλαπλούς λόγους.

## 18.1 ΑΝΑΠΑΡΑΓΩΓΙΜΟΤΗΤΑ

Αναπαραγωγιμότητα(Reproducibility) είναι η ικανότητα των επιστημόνων να αναπαράγουν τα αποτελέσματα άλλων επιστημόνων, αποτελώντας έτσι ακρογωνιαίο λίθο της ερευνητικής διαδικασίας. Η αναπαραγωγιμότητα μπορεί να λάβει χώρα σε διαφορετικές μορφές όπως εμπειρική, υπολογιστική και στατιστική. Διαφορετικοί άνθρωποι χρησιμοποιούν την αναπαραγωγιμότητα για να δημιουργήσουν επαναληψιμότητα, ευρωστία, αξιοπιστία και γενικευσιμότητα. Η ικανότητα αναπαραγωγής πειραμάτων βρίσκεται στο επίκεντρο της επιστήμης, όμως οι αποτυχημένες προσπάθειες πραγματοποίησης αυτού, αποτελεί συνηθισμένο φαινόμενο στην διαδικασία της έρευνας. Έτσι ενισχύεται η κρίση που υπάρχει γύρω από την αναπαραγωγιμότητα, δεδομένης της πίεσης για δημοσίευση, της επιλεκτικής αναφοράς, της κακής χρήσης των στατιστικών στοιχείων και των σχολαστικών πρωτοκόλλων, οι οποίοι αποτελούν σημαντικούς παράγοντες που δυσκολεύουν την αναπαραγωγή γνώσης και αποτελεσμάτων. Επιπλέον, οι δύσκολες τεχνικές, οι ελλιπείς περιγραφικές μέθοδοι και τα ανεπαρκή δεδομένα αποτελούν διαφορετικές πτυχές που παρεμποδίζουν τους ερευνητές να παράγουν γνώση και αποτελέσματα σε ένα ισορροπημένο περιβάλλον.

Τα προβλήματα γύρω από την αναπαραγωγιμότητα έχουν επέλθει ιδιαίτερης προσοχής κατά τη διάρκεια των τελευταίων χρόνων. Για παράδειγμα, το 2011 ξεκίνησε ένα έργο με τίτλο “The Reproducibility Project”[28] από το Κέντρο Ανοιχτής Επιστήμης (Center of Open Science) το οποίο αποσκοπούσε στην αναπαραγωγή 100 διαφορετικών μελετών που δημοσιεύτηκαν το 2008 στον κλάδο της ψυχολογίας. Τα αποτελέσματα αυτού του έργου που δημοσιεύτηκαν το 2015,

[28] https://en.wikipedia.org/wiki/Reproducibility_Project

έδειξαν ότι ενώ το 97% των αρχικών αποτελεσμάτων επέδειξε σημαντικό στατιστικό αποτέλεσμα, αυτό αναπαράχθηκε σε μόλις 36% της διαδικασίας, κάτι το οποίο δεν ξάφνιασε ιδιαίτερα την επιστημονική κοινότητα. Μερικά από τα στοιχεία που αναπαράχθηκαν, κατέληξαν σε αντίθετα αποτελέσματα από αυτά που προσπαθούσαν να αναπαραχθούν ξανά.

Ένα μεγάλο κομμάτι αυτού του αποτελέσματος υποδηλώνει ότι το επιστημονικό οικοσύστημα είναι εξαιρετικά αργό στην αποκατάσταση σφαλμάτων από λανθασμένες έρευνες. Επειδή τα ευρήματα δεν επαληθεύτηκαν ξανά, δεν σημαίνει ότι τα αρχικά αποτελέσματα ήταν λανθασμένα. Υπάρχουν πολλοί πιθανοί λόγοι που οδήγησαν στην αποτυχημένη αναπαραγωγή αποτελεσμάτων, συμπεριλαμβανομένων αγνώστων ή αναπόφευκτων αποκλίσεων από την αρχική μεθοδολογία.

## 18.2 ΤΑ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ ΩΣ ΜΕΣΟ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗΝ ΕΠΙΣΤΗΜΗ

Τα αποτελέσματα της έρευνας δημοσιεύονται κυρίως σε επιστημονικά και ακαδημαϊκά περιοδικά, τα οποία έχουν έντονη την τάση να δημοσιεύουν τα θετικά και καινοτόμα αποτελέσματα. Επιπλέον, οι ίδιοι οι ερευνητές είναι πιο επιρρεπείς στο να αναφέρουν τα θετικά αποτελέσματα στα οποία καταλήγουν μετά από την έρευνά τους, παρά στα αρνητικά και στις αποτυχημένες προσπάθειες που έχουν κάνει για να φτάσουν στο επιθυμητό αποτέλεσμα. Αυτό σημαίνει ότι πολλές έρευνες που δεν οδήγησαν σε θετικά αποτελέσματα παρέμειναν αδημοσίευτες και ως εκ τούτου άγνωστες.

Τα αρνητικά αποτελέσματα αλλά και τα αποτελέσματα που οδήγησαν σε ένα εσφαλμένο συμπέρασμα μπορούν να είναι εξίσου ενημερωτικά για τους ερευνητές σε σχέση με αυτά που επιβεβαιώνουν μια υπόθεση. Παράλληλα, η μη δημοσίευση ήδη πραγματοποιημένων ερευνών μπορεί να οδηγήσει σε σπατάλη πόρων και χρόνου, αφού ορισμένοι ερευνητές δεν γνωρίζουν ότι τα ερωτήματα που εξετάζουν μπορούν να εκτελεστούν με τα ίδια πειράματα που έχουν πραγματοποιηθεί ήδη από άλλους ερευνητές.

Επιπλέον, καθώς η μορφή των επιστημονικών περιοδικών και δημοσιεύσεων παρέμεινε σε μεγάλο βαθμό αμετάβλητη εδώ και πολλά χρόνια, δεν είναι καλά προσαρμοσμένη στην αντιμετώπιση άλλων τύπων περιεχομένου, οι οποίοι παίζουν σημαντικό ρόλο στον σημερινό τρόπο που πραγματοποιείται η έρευνα, όπως τα πρωτόκολλα και τα δεδομένα. Επίσης, η

κυριότερη μορφή των ηλεκτρονικών άρθρων, τα PDF, είναι στατική και περιοριστική όσον αφορά τις πληροφορίες που εμφανίζονται.

## 18.3 ΟΜΟΤΙΜΗ ΑΝΑΘΕΩΡΗΣΗ

Ομότιμη αναθεώρηση(Peer Review) ή επίσης αξιολόγηση από κριτές και αναθεώρηση από ομότιμους είναι η μέθοδος αξιολόγησης των επιστημονικών άρθρων από έναν ή περισσότερους ανθρώπους με παρόμοια αρμοδιότητα με εκείνους που παράγουν κάποιο έργο(peers). Τα άρθρα που υποβάλλονται σε μια τέτοια μέθοδο, αποστέλλονται σε αρκετούς επιστήμονες που εργάζονται στον ίδιο τομέα με τον συγγραφέα του άρθρου. Αυτοί οι αναθεωρητές – κριτές παρέχουν ανατροφοδότηση σχετικά με το άρθρο και ενημερώνουν τον συντάκτη της δημοσίευσης εάν θεωρούν ότι η μελέτη είναι αρκετά υψηλής ποιότητας για να δημοσιευτεί.

Η ομότιμη αναθεώρηση των επιστημονικών εγγράφων θεωρείται ένα κρίσιμο βήμα στη διαδικασία δημοσίευσης ποιοτικών αποτελεσμάτων σε αξιόπιστα περιοδικά. Παρόλα αυτά υπάρχουν λίγα κίνητρα για τους ερευνητές να συμφωνήσουν να διεξάγουν κατάλληλες κριτικές εγκαίρως και σε ορισμένες περιπτώσεις συμβαίνουν ασυνήθιστες πρακτικές στο πλαίσιο της παραγωγής ακαδημαϊκής έρευνας. Σχεδόν κάθε ακαδημαϊκός ερευνητής γνωρίζει το σημερινό περιβάλλον στο οποίο τα ιδρύματα αλλά και τα άτομα υπόκεινται σε κάποια μορφή αξιολόγησης και ένα σημαντικό της βαθμολογίας σταθμίζεται στην παραγωγή ακαδημαϊκών αποτελεσμάτων, συνήθως ως έγγραφα σε αξιόπιστα και αναγνωρισμένα περιοδικά.

Τα τελευταία χρόνια έχει δοθεί μεγάλη έμφαση στα θεμελιώδη προβλήματα που συνδέονται με τη διαδικασία αξιολόγησης των επιστημονικών δημοσιεύσεων από ομότιμους επιστήμονες, η οποία αποτελεί την βάση της της επιστημονικής επικοινωνίας. Τα προβλήματα που έχουν παρατηρηθεί είναι πολλά.

Ένα από αυτά είναι η έλλειψη αναγνώρισης των κριτών, των οποίων οι εργασίες και οι κριτικές παραμένουν σε μεγάλο βαθμό απαρατήρητες και άγνωστες. Παράλληλα, λόγω της ανώνυμης φύσης της αξιολόγησης από ομότιμους φαίνεται ότι υπάρχει μικρό κίνητρο για τους ανθρώπους να πραγματοποιήσουν αυτό το μέρος της διαδικασίας. Επίσης, ο αυξανόμενος ρυθμός των χειρόγραφων εργασιών που υποβάλλονται σε περιοδικά αλλά και η επακόλουθη ανάγκη για περισσότερους κριτές, έχουν σαν αποτέλεσμα την δυσκολότερη εύρεση των κατάλληλων και

ικανών κριτών. Επιπλέον, υπάρχουν περιπτώσεις χειραγώγησης των κριτικών που αφορούν τα επιστημονικά άρθρα, που σε ορισμένες από αυτές πραγματοποιείται πλαστογράφηση ταυτότητας κάτι το οποίο οδηγεί τους εκδότες να αποσύρουν τα άρθρα [35].

Είναι γενικότερα αποδεκτό το γεγονός ότι η κοινωνία είναι εξαιρετικά δυσλειτουργική ενάντια σε παρανοήσεις που έχουν ήδη υιοθετηθεί κυρίως μέσα από λανθασμένα αποτελέσματα ερευνών. Η λανθασμένη βιβλιογραφία μπορεί να εγκριθεί και να αναπαραχθεί μέσω της διαδικασίας σύνταξης και αξιολόγησης από ομότιμους χρήστες. Η διαδικασία αυτή έχει αρνητικές συνέπειες καθώς τα έγγραφα μέχρι την εξέτασή τους, θα έχουν χρησιμοποιηθεί σε νέες έρευνες(ανάλογα με την εγκυρότητά τους), δημιουργώντας έτσι αλυσιδωτά λανθασμένα αποτελέσματα. Επίσης, υπάρχει μεγάλος όγκος ψευδεπίγραφων ερευνών που μπορούν να επηρεάσουν ένα συγκεκριμένο επιστημονικό τομέα. Αν σκεφτούμε ότι σύμφωνα με εκτιμήσεις, οι δέκα πιο δημοφιλείς ερευνητικές δημοσιεύσεις έχουν αναφερθεί σε πάνω από 7.500 περιπτώσεις[29], αναλογιζόμαστε τις εν δυνάμει πιθανότητες αβάσιμων αναφορών. Κατά συνέπεια αναφορές σε ψευδείς δημοσιεύσεις θα μπορούσαν με τη σειρά τους να οδηγήσουν σε εντελώς ψευδείς ανακαλύψεις και καινοτομίες. Το επιστημονικό οικοσύστημα είναι ευάλωτο σε αναπαραγόμενα λάθη, καθώς μια λανθασμένη υπόθεση διατυπωμένη σε μια δημοσίευση, μπορεί να γίνει η αιτία δημιουργίας ενός φαύλου κύκλου αστήριχτων επερχόμενων ερευνών.

Γενικά, η διαδικασία της ομότιμης αναθεώρησης θεωρείται αδιαφανής και δαπανηρή, επιβραδύνοντας την ταχύτητα της επιστημονικής ανακάλυψης και της προόδου. Παρόλα αυτά τα προβλήματα που αναφέρθηκαν φαίνεται ότι η διαδικασία θα παραμείνει ενεργή στο εγγύς μέλλον δεδομένου ότι παρέχει ένα μηχανισμό για τη διατήρηση κάποιας μορφής ελέγχου ποιότητας μέσα σε ένα επιστημονικό κλάδο. Ωστόσο, με την εμφάνιση του διαδικτύου και όλων των σχετικών καινοτομιών, υπάρχουν περιθώρια για σημαντικές αλλαγές. Ορισμένες από αυτές τις αλλαγές είναι ήδη εμφανείς με την εμφάνιση αποθετηρίων δημοσίευσης ανοιχτής πρόσβασης, η συσχέτιση των ψηφιακών αναγνωριστικών αντικειμένου(Digital Object Identifier-DOI) με τα ακαδημαϊκά αποτελέσματα, όπως το ResearchGate[30], τον ανεξάρτητο μη κερδοσκοπικό οργανισμό ORCID[31] (Open Research and Contributor ID), την πλατφόρμα δημοσίευσης Ομότιμης Αναθεώρησης publons[32] κτλ.

[29] https://retractionwatch.com/the-retraction-watch-leaderboard/top-10-most-highly-cited-retracted-papers/
[30] http://researchgate.net/
[31] https://orcid.org/
[32] https://publons.com/home/

## 18.4 ΕΜΠΟΡΙΚΑ ΣΥΜΦΕΡΟΝΤΑ

Η έρευνα αποτελεί μια μη εμπορική δραστηριότητα, η οποία με τα χρόνια έχει γίνει μια από τις πιο προσοδοφόρες επιχειρηματικές βιομηχανίες στον κόσμο. Το 2015, η παγκόσμια αγορά εκδόσεων SMT(Scientific, Technical and Medical) εκτιμάται ότι ξεπέρασε τα 25 δισεκατομμύρια[33] δολάρια και αντιπροσωπεύει μόνο ένα τμήμα της παγκόσμιας αγοράς. Η επιστήμη ήταν πάντα ο παράγοντας της καινοτομίας και θα είναι πάντα στενά συνδεδεμένη με την πρόοδο της κοινωνίας. Αντιπροσωπεύει τον πιο αποτελεσματικό μηχανισμό που έχει δημιουργήσει ο άνθρωπος για να προωθήσει μια νέα οικονομική δραστηριότητα και να καλλιεργήσει νέες πρωτοποριακές βιομηχανίες, οι οποίες με τη σειρά τους μπορούν να καλυτερεύσουν τον κόσμο. Η άποψη αυτή καταγράφηκε από τον Joseph Schumpeter[34], σύμφωνα με τον οποίο "Η επιστήμη είναι, και πάντα βρισκόταν στο επίκεντρο του οικονομικού μας συστήματος", η οποία ισχύει μέχρι σήμερα.

Η βιομηχανία των εμπορικών εκδόσεων κυριαρχείται από μερικούς μεγάλους εκδοτικούς γίγαντες κάτι το οποίο προκαλεί πολλά ζητήματα στον τομέα της έρευνας. Οι υψηλές τιμές που χρεώνουν οι εμπορικοί εκδότες τις συνδρομές, απασχολεί σε μεγάλο βαθμό τη βιωσιμότητα των βιβλιοθηκών οι οποίες προσπαθούν να ανταπεξέλθουν στα οικονομικές απαιτήσεις των εκδοτικών οίκων, το οποίο συνεπάγεται πως το περιεχόμενο δεν είναι προσβάσιμο από όλους τους επιστήμονες στα διάφορα ιδρύματα.

Για την αντιμετώπιση των προβλημάτων που σχετίζονται με το παραδοσιακό μοντέλο των συνδρομών, η ελεύθερη πρόσβαση, το μοντέλο με το οποίο η πληρωμή μετατοπίζεται από τον αναγνώστη ή την βιβλιοθήκη στον δημιουργό, έχει τεθεί σε εφαρμογή, παρέχοντας καθολική πρόσβαση σε όλα τα άρθρα. Αρκετές δεκαετίες μετά την εισαγωγή αυτού του μοντέλου διάθεσης των επιστημονικών άρθρων, μόνο μια μειοψηφία από αυτά διαθέτουν ελεύθερη πρόσβαση.

Επιπλέον η ανοιχτή πρόσβαση έχει δημιουργήσει με τη σειρά της μια σειρά από νέα προβλήματα, όπως το κίνητρο των εκδοτών να δεχθούν άρθρα, κάτι το οποίο οδηγεί με τη σειρά του σε λιγότερο αυστηρούς κανόνες ποιότητας άρθρων. Παράλληλα, αυξάνεται η εμφάνιση των λεγόμενων "εκδοτών-αρπακτικών", οι οποίοι χρεώνουν τα τέλη δημοσίευσης στους δημιουργούς,

[33] https://medium.com/@jasonschmitt/can-t-disrupt-this-elsevier-and-the-25-2-billion-dollar-a-year-academic-publishing-business-aa3b9618d40a
[34] http://bev.berkeley.edu/ipe/Schumpeter%20Science%20and%20Ideology.pdf

χωρίς να τους παρέχουν τις υπηρεσίες σύνταξης και έκδοσης που σχετίζονται με νόμιμα περιοδικά και εκδότες.

## 18.5 ΑΝΑΞΙΟΠΙΣΤΕΣ ΑΝΑΦΟΡΕΣ

Τα συστήματα παραπομπής που χρησιμοποιούνται από ακαδημαϊκούς ερευνητές διαφέρουν μεταξύ των κλάδων. Ορισμένες περιλαμβάνουν υποσημειώσεις και άλλες πάλι χρησιμοποιούν αναφορές. Καθώς όλο και περισσότερα ακαδημαϊκά έργα δημιουργούνται ψηφιακά, οι υπερσυνδέσεις γίνονται μια λύση παραπομπής. Ωστόσο, ανεξάρτητα από το σύστημα ακαδημαϊκών παραπομπών που χρησιμοποιείται, θα έχει πάντα αρκετούς περιορισμούς.

Ένας περιορισμός που συναντάται συχνά αποτελεί το γεγονός ότι οι αναφορές είναι συχνά διφορούμενες επειδή οι ερευνητές τείνουν να ομαδοποιούν πολλαπλές αναφορές σε μία μόνο παραπομπή. Αυτό καταστεί δύσκολο να γνωρίζουμε ποια αξίωση σε ένα ακαδημαϊκό άρθρο ή βιβλίο αντιστοιχεί σε ποια πηγή σε μια παραπομπή. Επίσης, δεν υπάρχει κάποιο στοιχείο που μπορεί να εγγυηθεί ότι οι αναφορές είναι ακριβείς, σε ένα κόσμο όπου δεν υπάρχει κάποιος τρόπος να εμποδίσει τους ερευνητές να συνθέτουν οι ίδιοι τα δεδομένα αναφοράς. Δεν υπάρχει αυτόματος τρόπος για να επαληθεύσει κανείς τις πληροφορίες παραπομπής κάνοντας έτσι δύσκολο τον έλεγχο για κάποια απάτη. Ακόμη και τα πιο αναγνωρισμένα ακαδημαϊκά περιοδικά, τα οποία προσπαθούν να αποτρέψουν την απάτη μέσω αυστηρών διαδικασιών αξιολόγησης από ομότιμους, δημοσιεύουν μερικές φορές εργασίες που αποδεικνύονται ότι βασίζονται σε εντελώς δόλια στοιχεία.

Ένα στοιχείο το οποίο μπορεί να οδηγήσει σε ανακριβείς αναφορές είναι τυπογραφικά λάθη των ερευνητών. Για παράδειγμα, ένα τυπογραφικό λάθος μέσα σε μια παραπομπή μπορεί να προκαλέσει την αναφορά ενός λανθασμένου αριθμού σελίδας μιας εξωτερική εργασίας, γεγονός που δυσκολεύει ένα μελετητή να εντοπίσει την ακριβή πηγής μιας αξίωσης. Ακόμη και οι πιο επιμελείς μελετητές κάνουν λάθη όπως και οι καλύτεροι συντάκτες αντιγράφων σπάνια τις βρίσκουν. Κάτι τέτοιο θα ήταν μια κουραστική και παράλληλα χρονοβόρα διαδικασία για την εξακρίβωση μεταξύ αναφορών εξωτερικών πηγών που συχνά δεν είναι άμεσα διαθέσιμες.

### 18.6 ΈΛΛΕΙΨΗ ΠΑΓΚΟΣΜΙΩΝ ΕΡΕΥΝΗΤΙΚΩΝ ΜΗΤΡΩΩΝ

Η εύρεση επιστημονικών άρθρων για ένα συγκεκριμένο θέμα είναι μια επίπονη διαδικασία στον σημερινό επιστημονικό κόσμο δεδομένου ότι δεν υπάρχει μια παγκόσμια βάση δεδομένων ή κάποιο μητρώο όπου κάποιος θα μπορούσε να αναζητήσει κάποιο άρθρο ή δημοσίευση σε κάποιο επιστημονικό περιοδικό. Όταν οι ερευνητές θέλουν να μάθουν τι έχουν ήδη ανακαλύψει άλλοι ερευνητές σχετικά με ένα συγκεκριμένο θέμα συνήθως ακολουθούν μια τυπική και ταυτόχρονα καθόλου αποδοτική.

Ένας ερευνητής μπορεί να ψάξει σε μια μεγάλη ποικιλία από βιβλιοθήκες καθώς και βάσεις δεδομένων περιοδικών για να βρει κάποια έρευνα. Όμως η έλλειψη μιας ενιαίας βάσης δεδομένων στην οποία να είναι καταχωρημένα όλα τα επιστημονικά δημοσιεύματα, δημιουργεί αφερεγγυότητα στο αποτέλεσμα που θα προκύψει. Επιπλέον, επειδή οι ακαδημαϊκές εκδόσεις τείνουν να κινούνται αργά και οι βάσεις δεδομένων που περιέχουν έρευνες δεν ενημερώνονται συχνά μπορούν να οδηγήσουν σε μη αξιόπιστα αποτελέσματα τα οποία δεν αντανακλούν τις πιο πρόσφατες έρευνες πάνω σε ένα τομέα.

## 19 Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN ΩΣ ΛΥΣΗ ΣΤΑ ΖΗΤΗΜΑΤΑ ΤΗΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

Η τρέχουσα επιστημονική διαδικασία δημοσίευσης έχει αρκετά προβλήματα που επηρεάζουν την ερευνητική κοινότητα, όπως το υψηλό κόστος δημοσίευσης, τα δικαιώματα πνευματικής ιδιοκτησίας των εκδοτών αντί των δημιουργών, των ανταμοιβών και της αναγνώρισης των αναθεωρητών καθώς και τον πολλαπλασιασμό των περιοδικών χαμηλής ποιότητας. Χρησιμοποιώντας την τεχνολογία Blockchain, μπορεί να εξαλειφθεί η αναποτελεσματικότητα της αγοράς και να βελτιωθεί η ποιότητα και η αποτελεσματικότητα της επιστημονικής δημοσίευσης. Απώτερος στόχος, θα πρέπει να είναι η δημιουργία πλατφορμών δημοσίευσης για την ερευνητική κοινότητα, οι οποίες θα συμβάλλουν στην μοναδική και απρόσκοπτη ενσωμάτωση τεχνολογιών αιχμής για τη δημιουργία μιας πλατφόρμας επεξεργασίας, επικύρωσης και διάδοσης ερευνητικών δεδομένων και αποτελεσμάτων. Η συγκεκριμένη τεχνολογία μπορεί να μετατρέψει και να θέσει από την αρχή νέες βάσεις για τον πως λειτουργεί η

επιστημονική και η πανεπιστημιακή κοινότητα, αλλά και πως η γνώση μπορεί να είναι προσβάσιμη από όλους. Κρίσιμα ζητήματα που αντιμετωπίζει η επιστημονική κοινότητα παγκοσμίως ως προς την επικοινωνία, τη διαφάνεια, την εμπιστευτικότητα, την αναπαραγωγή δημοσιεύσεων αλλά και τα πνευματικά δικαιώματα, μπορούν να επιλυθούν με τη χρήση νέων τεχνολογιών.

Η αποκεντρωμένη τεχνολογία Blockchain χάρη στη δομή και τη λειτουργία της μπορεί να προσφέρει λύσεις στα παραπάνω προβλήματα. Με την χρήση της συγκεκριμένης τεχνολογίας, κάθε πτυχή της επιστημονικής διαδικασίας θα μπορούσε να γίνει διαφανής δίνοντας την δυνατότητα εφαρμογής ενός πραγματικού δημόσιου ελέγχου. Όσο αφορά τις δημοσιεύσεις που αφορούν άρθρα, αναφορές, βιβλία και περιοδικά, η τεχνολογία Blockchain, θα μπορούσε να επηρεάσει τις πωλήσεις, τα δικαιώματα, τις συμβάσεις και πολλά περισσότερα που εδώ και χρόνια αποτελούν κρίσιμους παράγοντες για τους ίδιους τους συγγραφείς αλλά και τις εταιρείες που τα διαχειρίζονται. Η συγκεκριμένη τεχνολογία μπορεί να αποδειχθεί χρήσιμο εργαλείο στη δυναμική επικύρωση της γνώσης μετά την δημοσίευση. Το Blockchain με την έμφυτη ανιχνευσιμότητα του θα καθιστούσε συνεχή και ανοιχτή σε όλους τη διαδικασία δημιουργίας της γνώσης. Παράλληλα, θα μπορούσαν να δοθούν κίνητρα οικονομικά και μη στους ομότιμους χρήστες ώστε να επιβραβεύεται η ακριβής και δίκαιη αξιολόγηση, τα ακριβή ερευνητικά έγγραφα και πολλές άλλες ζωτικές δραστηριότητες με σκοπό την διατήρηση της γνώσης στην επιστημονική κοινότητα.

Η ύπαρξη μιας ανοιχτής και αποκεντρωμένης πλατφόρμας θα προσφέρει ένα βέλτιστο τρόπο επίλυσης των στρεβλώσεων και ανακριβειών που δημιουργούν καχυποψία στην παραγωγή και διάδοση επιστημονικών γνώσεων παγκοσμίως. Με την εξακρίβωση της ταυτότητας και την πιστοποίηση των δημοσιευμένων ερευνητικών δεδομένων, η επιστημονική κοινότητα θα μπορούσε να μειώσει τα λάθη και να ανακτήσει την εμπιστοσύνη του κόσμου, προωθώντας αξιόπιστη έρευνα και διαχωρίζοντας το γεγονός από τη μυθοπλασία· το οποίο είναι ο ορισμός της επιστήμης.

## 19.1 Η ΕΦΑΡΜΟΓΗ ΤΟΥ BLOCKCHAIN ΣΕ ΒΙΒΛΙΟΘΗΚΕΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΑ ΑΠΟΘΕΤΗΡΙΑ

Η τεχνολογία Blockchain αφορά την αποθήκευση πληροφοριών και δεδομένων σε κατανεμημένη, ανθεκτική στις παραβιάσεις, μορφή. Η λειτουργία αυτή ταιριάζει απόλυτα με την απασχόληση των βιβλιοθηκονόμων οι οποίοι είναι υπεύθυνοι για την συλλογή, τη διατήρηση και την ανταλλαγή έγκυρων πληροφοριών. Η τεχνολογία αυτή μπορεί να τους βοηθήσει να επιτύχουν το έργο τους με ασφάλεια, και σε λιγότερο χρόνο, ειδικότερα στον κόσμο των επιστημονικών εκδόσεων.

Όσον αφορά τις βιβλιοθήκες η τεχνολογία αυτή θα μπορούσε να χρησιμοποιηθεί ως ένα είδος βάσης δεδομένων για την καταγραφή ανταλλαγής δεδομένων καθώς και την καταχώρηση διάφορων εγγραφών. Για παράδειγμα, μέσω Blockchain θα μπορούσαν να καταγραφεί η κυκλοφορία των βιβλίων, των δημοσιεύσεων, των περιοδικών καθώς αυτά συναλλάσσονται μεταξύ φοιτητών, καθηγητών, επιστημονικού προσωπικού, επιχειρήσεων και πανεπιστημίων. Αυτό γιατί πολλές βιβλιοθήκες σήμερα, δεν επιθυμούν να διατηρούν μόνιμα αρχεία που αφορούν αυτές τις συναλλαγές, κάτι το οποίο δημιουργεί δέσμευση χρόνου, χώρου και υπολογιστικών πόρων. Η τεχνολογία αυτή θα παρέχει μια μόνιμη καταγραφή των συναλλαγών οι οποίες αφορούν, το ποιος κατέχει τα άρθρα, τα βιβλία τα περιοδικά και τις δημοσιεύσεις καθώς και το πώς πραγματοποιούνται αυτές οι συναλλαγές μεταξύ των ενδιαφερομένων.

Μία πιθανή χρήση του Blockchain είναι η δημιουργία χρονικά επισημασμένων, επαληθεύσιμων εκδόσεων επιστημονικών άρθρων και δημοσιεύσεων. Η έλλειψη παγκόσμιων ερευνητικών μητρώων αλλά και ηλεκτρονικών αποθετηρίων τα οποία θα περιέχουν συγκεντρωμένη όλη την πληροφορία για τα διαθέσιμα άρθρα και δημοσιεύσεις θα μπορούσε να επιλυθεί με τη χρήση της τεχνολογίας Blockchain. Οι Irvin και Holden χρησιμοποίησαν το Blockchain του Bitcoin ως μια χαμηλού κόστους, ανεξάρτητα επαληθεύσιμη μέθοδο που θα μπορούσε εύκολα να χρησιμοποιηθεί για τον έλεγχο και την επιβεβαίωση της αξιοπιστίας των επιστημονικών μελετών. [36] Το έκαναν με τη δημιουργία κρυπτογραφικού κατακερματισμού(Hash) του κειμένου ενός εγγράφου και χρησιμοποίησαν αυτό το Hash για τη δημιουργία ενός ιδιωτικού κλειδιού Bitcoin. Αυτό δημιουργεί ένα αρχείο με χρονοσήμανση στο Blockchain, το οποίο όλοι οι ερευνητές μπορούν να επαληθεύσουν την ύπαρξη, την μεταβίβαση την αντιγραφή και την αλλαγή κάποιου επιστημονικού εγγράφου. Έτσι αν το έγγραφο έχει

αλλάξει, το Hash του νέου εγγράφου δεν θα ταιριάζει με αυτό που έχει αποθηκευτεί στο Blockchain.

Η πιο σημαντικός και παράλληλα ελπιδοφόρος ρόλος που μπορεί να αναλάβει η τεχνολογία Blockchain στον τομέα των βιβλιοθηκών, είναι η επικύρωση των πρωτογενών πηγών. Η ασφάλεια που παρέχει αυτή η τεχνολογία, θα μπορούσε να αποτρέψει την αλλοίωση των αρχείων των συναλλαγών. Όταν μια πηγή, ένα άρθρο, ένα βιβλίο ή περιοδικό, ενημερωθεί, η ενημέρωση αυτή μπορεί να προστεθεί στην αλυσίδα με μια αξιόπιστη σφραγίδα χρόνου - χρονοσήμανση (timestamp), καθιστώντας εύκολο τον προσδιορισμό την πιο πρόσφατης έκδοσης σε ένα αυθεντικό έγγραφο.

Παράλληλα, η ψηφιακή προέλευση των δεδομένων που αφορούν την έρευνα, θα μπορούσε να βασιστεί στην τεχνολογία blockchain με σκοπό τα δεδομένα αυτά, να διανέμονται σε όλους δημόσια και οι αλλαγές που πραγματοποιούνται να παρακολουθούνται και να καταγράφονται δημοσίως.

## 20 BLOCKCHAIN ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ

Τα 10 περίπου τελευταία χρόνια, η τεχνολογία παγκοσμίως έχει διαταράξει τις ισορροπίες σε πολλούς κλάδους της παγκόσμιας βιομηχανίας. Ο ξενοδοχειακός κλάδος ένιωσε μια τεράστια αφύπνιση χάρη στην πλατφόρμα Airbnb, η βιομηχανία των ταξί επηρεάστηκε σημαντικά από το Uber και η βιομηχανία της καλωδιακής τηλεόρασης αναγκάστηκε να αναθεωρήσει το επιχειρηματικό της μοντέλο εξαιτίας των υπηρεσιών Streaming, όπως το Netflix. Με την πάροδο του χρόνου, είναι γεγονός ότι ο αποδιοργανωτικός χαρακτήρας των τεχνολογικών εξελίξεων παγκοσμίως, γίνεται όλο και πιο διαδεδομένος και δεν υπάρχει κάποια απόδειξη ότι θα επιβραδυνθεί. Ωστόσο, ο κλάδος της εκπαίδευσης παραμένει σε μεγάλο βαθμό ανεπηρέαστος από αυτή την αλματώδη πρόοδο της τεχνολογίας παρόλο που τα σχολεία και τα πανεπιστήμια αποτελούν τις βασικές επιλογές των ανθρώπων ώστε να εξελίξουν τη σταδιοδρομία τους και να αυξήσουν τις ευκαιρίες απασχόλησής τους.

Σε όλες τις αναπτυγμένες χώρες του κόσμου, ο τομέας της εκπαίδευσης είναι στο επίκεντρο συμβάλλοντας καθοριστικά στην οικονομική ανάπτυξη και ευημερία μιας χώρας. Αυτό οφείλεται στο γεγονός ότι το μέλλον όλων των σημαντικών τομέων συμπεριλαμβανομένης της

επιστήμης, της ιατρικής, της γεωργίας αλλά και της βιομηχανίας εξαρτάται από το επίπεδο εκπαίδευσης της χώρας, καθώς τα εκπαιδευτικά ιδρύματα αποτελούν φυτώριο στη δημιουργία νέων επιστημόνων που θα οδηγήσουν τις κοινότητες παγκοσμίως σε οικονομική και κοινωνική ανάπτυξη. Παρά τις αξιοσημείωτες εξελίξεις στη ρομποτική, στο Διαδίκτυο και τις τεχνολογίες πληροφορικής ο ανθρώπινος παράγοντας εξακολουθεί να είναι ο πιο πολύτιμος πόρος σχεδόν για κάθε επιχείρηση. Είναι αποδεδειγμένο ότι οι προηγμένες τεχνολογίες συμβάλλουν στην βελτίωση της κατάρτισης του προσωπικού και στην επίλυση πολλαπλών προβλημάτων.

Όχι μόνο τα ιδιωτικά αλλά και δημόσια εκπαιδευτικά ιδρύματα είτε ετοιμάζονται να εφαρμόσουν εργαλεία που βασίζονται σε Blockchain, είτε διεξάγουν έρευνες για να εντοπίσουν τα δυνατά και αδύνατα σημεία της εφαρμογής της συγκεκριμένης τεχνολογίας στην εκπαίδευση. Η τεχνολογία Blockchain εκτός των άλλων μπορεί να παίξει καθοριστικό ρόλο στην αναδιάρθρωση του εκπαιδευτικού συστήματος παγκοσμίως. Οι δυνατότητες της συγκεκριμένης τεχνολογίας είναι πολύ μεγαλύτερες από αυτές που ήδη έχουν κάνει την εμφάνισή τους σε συγκεκριμένα εκπαιδευτικά ιδρύματα. Ορισμένα πανεπιστημιακά ιδρύματα και ινστιτούτα έχουν εφαρμόσει την τεχνολογία Blockchain στην εκπαίδευση και τα περισσότερα από αυτά χρησιμοποιούν για τη διαχείριση ακαδημαϊκών τίτλων καθώς και για την αξιολόγηση των μαθησιακών αποτελεσμάτων. [37]

## 20.1 ΠΙΣΤΟΠΟΙΗΣΗ

Τα ακαδημαϊκά πιστοποιητικά είναι σημαντικό περιουσιακό στοιχείο για κάθε άτομο. Είτε κάποιος υποβάλλει αίτηση για εργασία είτε για είσοδο στην τριτοβάθμια εκπαίδευση τα ακαδημαϊκά πιστοποιητικά αποτελούν ένδειξη για την ταυτότητα, τα προσόντα αλλά και την επιλεξιμότητα του ατόμου. Υπάρχουν πολλές αναφορές για πλαστογραφία στα συγκεκριμένα διαπιστευτήρια ή σε έγγραφα από κάποια εκπαίδευση κάτι το οποίο έχει φτάσει σε ένα επίπεδο άξιο αναφοράς. Το μεγαλύτερο πρόβλημα που παρατηρείται έγκειται στην ικανότητα του δικαιούχου να αποδείξει την αυθεντικότητα ενός πιστοποιητικού. Οι επιχειρήσεις καθώς και τα εκπαιδευτικά ιδρύματα χρειάζονται καλύτερα, πιο σύγχρονα και αξιόπιστα συστήματα για να αντιμετωπίσουν αυτό το πρόβλημα το οποίο θεωρείται κρίσιμης σημασίας στην διαδικασία μιας αξιοκρατικής εκπαίδευσης και κατά συνέπεια μιας πιο αξιοκρατικής κοινωνίας.

Ένα συχνό φαινόμενο που αντιμετωπίζει ο κάτοχος κάποιου πιστοποιητικού είναι η επίμονη διαδικασία που πρέπει να αντιμετωπίσει, για να αποκτήσει κάποιο αντίγραφο του πιστοποιητικού από τις αρμόδιες αρχές και να αποδείξουν την αυθεντικότητά τους. Η συγκεκριμένη διαδικασία μπορεί να αποβεί πολύ χρονοβόρα αλλά και να έχει μεγάλο κόστος ή να προκληθεί ακόμα και κάποια απώλεια πιστοποιητικού. Οι υπάρχουσες μέθοδοι επαλήθευσης των πιστοποιητικών δεν εγγυώνται αυθεντικές, ασφαλείς και ανθεκτικές στις αλλαγές στα έγγραφα. Η επαλήθευση ενός διπλώματος απαιτεί ένα μεγάλο χρονικό διάστημα και πιθανόν να απαιτηθεί από τους πιθανούς εργοδότες ή μεταπτυχιακά προγράμματα επιβεβαίωση των πιστοποιητικών των ενδιαφερομένων από τα πανεπιστήμια.

Παρόλο που τα πιστοποιητικά έχουν ανατεθεί και ανήκουν σε ένα άτομο, υπάρχει ισχυρή εξάρτηση από την εκδούσα αρχή σε περίπτωση που το άτομο χρειάζεται επανέκδοση ή επικύρωση του συγκεκριμένου πιστοποιητικού. Παράλληλα, υπάρχει η πιθανότητα απώλειας ή βλάβης σε κάποιο φυσικό έγγραφο. Σε τέτοιες περιπτώσεις ο ενδιαφερόμενος μπορεί να συναντήσει δυσκολίες στην επανέκδοση εγγράφων ή σε εξαιρετικές περιπτώσεις η επανέκδοση του εγγράφου μπορεί να καταστεί αδύνατη. Σε ακραίες περιπτώσεις όπου η αρχή έκδοσης παύσει να υπάρχει, τα αρχεία να μην μπορούν πλέον να διατεθούν. Επιπλέον, η επαλήθευση εγγράφων καθώς και οι συμβολαιογραφικές πράξεις για την πιστοποίηση αυθεντικότητας απαιτούν την καταβολή τελών κάτι το οποίο μπορεί να είναι δαπανηρό.

Λύσεις σε αυτά τα προβλήματα μπορεί να δώσει η τεχνολογία Blockchain.Ορισμένα πανεπιστήμια όπως το MIT, πειραματίζονται με πιλοτικά προγράμματα όπου οι πτυχιούχοι διαθέτουν τα πτυχία τους σε μια εφαρμογή που βασίζεται σε Blockchain. Οι απόφοιτοι μπορούν στη συνέχεια να μοιραστούν τα πιστοποιητικά τους με όποιον θέλουν και το δίπλωμα δεν μπορεί να αμφισβητηθεί λόγω της ασφάλειας και της ανθεκτικότητας που προσφέρει η αποκεντρωμένη τεχνολογία του Blockchain. Το εργαστήριο MIT Media Lab, με τη χρήση μηχανικής μάθησης(Machine Learning) ανέπτυξε το Blockcerts[35], την εφαρμογή που χρησιμοποιεί το πιλοτικό πρόγραμμα του MIT και επιδιώκει να επιτρέψει την ψηφιακή αυτοκυριαρχία για τα αρχεία των ατόμων. Άλλες εφαρμογές για παρόμοιες υπηρεσίες αποτελούν το Gradbase και το Stampery. Οι συγκεκριμένες εφαρμογές που βασίζονται σε Blockchain θα εξαλείψουν την ανάγκη ενασχόλησης του ιδρύματος στην διαδικασία επαλήθευσης των πιστοποιητικών των αποφοίτων

[35] http://www.blockcerts.org/guide/

καθώς η διαδικασία θα είναι αυτοματοποιημένη και θα είναι εμφανής σε όλους τους ενδιαφερόμενους.

Με την αποθήκευση των ακαδημαϊκών αρχείων σε μια αποκεντρωμένη βάση Blockchain, τα ακαδημαϊκά ιδρύματα μπορούν να επιτύχουν ένα σύστημα διαπιστευτηρίων το οποίο θα είναι ανθεκτικό στις κακόβουλες επιθέσεις και στις απάτες. Μόλις τα δεδομένα καταγραφούν στο Blockchain δίκτυο κανείς δεν μπορεί να τα αλλάξει χωρίς τη συγκατάθεση ολόκληρου του δικτύου. Η δόλια τροποποίηση των δεδομένων όπως οι βαθμοί ή οι ημερομηνίες βαθμολόγησης είναι ουσιαστικά αδύνατη. Επιπλέον, τα ακαδημαϊκά αρχεία που διατηρούνται σε μια κεντρική βάση δεδομένων κάποιου πανεπιστημίου ή κολλεγίου μπορούν να χαθούν σε περίπτωση που ο κεντρικός υπολογιστής σταματήσει να λειτουργεί ή το ίδρυμα αποφασίσει να διαγράψει τα δεδομένα. Ωστόσο, στο Blockchain τα δεδομένα υπάρχουν απεριόριστα και κατανέμονται ανάμεσα στους κόμβους του δικτύου και έτσι η εξαφάνιση ενός μόνο κόμβου ή κεντρικού υπολογιστή δεν θα οδηγήσει σε απώλεια δεδομένων.

Τα δεδομένα που αποθηκεύονται σε ένα δημόσιο Blockchain μπορούν να προσπελαστούν άμεσα από οποιονδήποτε και οπουδήποτε. Μεταφέροντας τα εκπαιδευτικά πιστοποιητικά στο Blockchain το ακαδημαϊκό υπόβαθρο του ατόμου μπορεί να επαληθευτεί σε χρόνο ρεκόρ από τους ενδιαφερόμενους. Επίσης, θα μπορούσα να δημιουργηθούν εργαλεία λογισμικού για την αυτόματη αναζήτηση των αρχείων στο Blockchain. Αυτό θα καθιστούσε τη διαδικασία επαλήθευσης πολύ πιο αποτελεσματική από την υποβολή χειρόγραφων αιτήσεων κάθε φορά που πρέπει να ανευρεθεί μια εγγραφή από το αρχείο κάποιου ιδρύματος. Η χρήση τεχνολογίας Blockchain για την αποθήκευση πληροφοριών σχετικά με το επίπεδο εκπαίδευσης ενός ατόμου θα καταστήσει αδύνατη την πλαστογραφία και την παραποίηση των πληροφοριών και των πιστοποιητικών.

Η χρήση της τεχνολογίας Blockchain στην εκπαίδευση έκανε την πρακτική της εφαρμογή της στο Πανεπιστήμιο της Λευκωσίας, το οποίο έχει ήδη ξεκινήσει την καταγραφή των πιστοποιητικών των αποφοίτων. Σε ανακοίνωσή του το συγκεκριμένο πανεπιστήμιο θα ξεκινήσει να δημοσιεύει τα διπλώματα για όλους τους φοιτητές στο Blockchain του Bitcoin[36]. Η επίσημη ανακοίνωση ακολούθησε το δοκιμαστικό πρόγραμμα που ξεκίνησε το πανεπιστήμιο την άνοιξη του 2014, όταν και άρχισε να δημοσιεύσει ακαδημαϊκά πιστοποιητικά στο Blockchain.

[36] https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

Δημοσιεύοντας τα διπλώματα όλων των μελλοντικών πτυχιούχων στο Blockchain, το Πανεπιστήμιο της Λευκωσίας εξασφαλίζει ότι τα αρχεία βαθμολόγησης των αποφοίτων του θα παραμείνουν μόνιμα διαθέσιμα και προσβάσιμα σε όποιον χρειάζεται να τα επιβεβαιώσει.

Εν ολίγοις, η τεχνολογία Blockchain προσφέρει μια πολύ πιο αποτελεσματική και αξιόπιστη λύση για την αποθήκευση πιστοποιητικών και παρέχει τη βάση για την επίλυση μακροχρόνιων προκλήσεων στο τομέα διαχείρισης πιστοποιητικών στον τομέα της εκπαίδευσης.

## 20.2 ΕΞΥΠΝΗ ΜΑΘΗΣΗ

Η μάθηση πλέον δεν αποτελεί μια δραστηριότητα η οποία εκτελείται κατά τη διάρκεια μιας αρχικής περιόδου στην ζωή ενός ανθρώπου και η οποία εμπλουτίζεται από την εμπειρία της επαγγελματικής και προσωπικής ζωής. Η δια βίου μάθηση έχει γίνει απαραίτητη, σύμφωνα με τον τρόπο της ανθρώπινης μάθησης που περιέγραψε ο Bruer, ειδικά τον 21ο αιώνα. Η μάθηση είναι συνεχής και υπερβαίνει τα όρια του χρόνου και του χώρου. [38]

Με τη δια βίου μάθηση να είναι πιο σημαντική από ποτέ καθώς οι εργαζόμενοι αντιμετωπίζουν συνεχείς προκλήσεις στον εργασιακό τους τομέα καθώς και την ανάγκη να βελτιώσουν τις δεξιότητες τους, τα εκπαιδευτικά συστήματα και οι διαδικασίες πρόσληψης πρέπει να είναι πιο αποτελεσματικές για να προσαρμοστούν στις διαφορετικές απαιτήσεις της αγοράς εργασίας. Η δυσκολία που αντιμετωπίζουν τα τμήματα ανθρώπινου δυναμικού των επιχειρήσεων είναι μεγάλη, καθώς δεν μπορούν να βρουν τους κατάλληλους εργαζόμενους στις κατάλληλες θέσεις για να καλύψουν τις ανάγκες τους. Σήμερα, η πρόσληψη για συγκεκριμένες θέσεις είναι μια χρονοβόρα και σύνθετη διαδικασία. Δεν υπάρχει κάποιος απλός αλγόριθμος που να είναι ικανός να περιορίσει την αναζήτηση μόνο σε εκείνους τους αιτούντες οι οποίοι έχουν τις απαιτούμενες γνώσεις. Επιπλέον, η έλλειψη παροχής πληροφοριών προς τους μελλοντικούς εργαζόμενους όσον αφορά τις δεξιότητες που πρέπει να αποκτήσουν όπως επίσης την εκπαιδευτική πορεία και επιστήμη που πρέπει να ακολουθήσουν αποτελούν τα προβλήματα που επικρατούν στην σημερινή αγορά εργασίας. Η διαδικασία αυτή γίνεται από δεδομένα που παρέχονται από εταιρείες όπως η LinkedIn, τα οποία δεν μπορούν να θεωρηθούν αξιόπιστα δεδομένου ότι μπορούν να αλλοιωθούν.

Αυτός είναι ο λόγος για τον οποίο το Blockchain έχει μεγάλες δυνατότητες εφαρμογής στο τομέα της μάθησης. Μπορεί να επιτρέψει στους εργαζόμενους να δημιουργήσουν ένα ασφαλές, επαληθεύσιμο ψηφιακό αρχείο το οποίο θα περιέχει τα τυπικά προσόντα, τις εμπειρίες καθώς και τις δεξιότητες που απέκτησαν στην διάρκεια της εκπαίδευσής τους. Έτσι, αντί να συγκεντρώνουν έγγραφα και πιστοποιητικά σχετικά με την εκπαίδευσή τους, κατά τη διάρκεια τη διάρκεια της ζωής τους, οι ενδιαφερόμενοι θα μπορούν να καταγράφουν αυτές τις πληροφορίες σε μια βάση δεδομένων Blockchain, οι οποίες θα είναι διαθέσιμες στους εργοδότες οπουδήποτε στον κόσμο. Αυτή η βάση δεδομένων θα περιλαμβάνει τα μαθήματα, τα σεμινάρια ή τις δεξιότητες οι οποίες έχουν αποκτηθεί καθώς και τις διαλέξεις οι οποίες παρακολουθήθηκαν. Χάρη σε αυτή τη βάση, οι εργοδότες θα μπορούν να αποκτούν και να φιλτράρουν γρήγορα και εύκολα πληροφορίες σχετικά με τη τις γνώσεις ενός υπαλλήλου χωρίς καμιά αμφιβολία ως προς την συνάφεια ή την αξιοπιστία τους. Ουσιαστικά θα αποτελεί ένα διαδικτυακό βιογραφικό το οποίο θα συμπληρώνεται από τα πτυχία, τις δεξιότητες και οποιεσδήποτε γνώσεις κατέχει ένας υποψήφιος είτε στα πλαίσια αναζήτησης εργασίας είτε σε ακαδημαϊκό επίπεδο.

Επιπλέον, χρησιμοποιώντας έξυπνα συμβόλαια, οι εφαρμογές Blockchain θα μπορούσαν να δώσουν στους μαθητές τη δυνατότητα να αποκτήσουν μεγαλύτερο έλεγχο της ατομικής τους εκπαίδευσης, προσφέροντας ευέλικτη πρόσβαση στο περιεχόμενο και στα μαθήματα που προτάθηκαν με βάση προηγούμενες επιτυχίες ή αποτυχίες και επιτεύγματα. Παράλληλα, η σύνδεση της αγοράς εργασίας με την εκπαίδευση θα μπορούσε να υλοποιηθεί μέσω του Blockchain δίνοντας την κατάλληλη καθοδήγηση στο να επιλέγουν οι μαθητές αλλά και τα εκπαιδευτικά ιδρύματα τα κατάλληλα μαθήματα που θα τους δώσουν τις γνώσεις και τα εφόδια που απαιτεί η αγορά εργασίας. Μια πλατφόρμα η οποία προσφέρει τέτοιου είδους λύση, η οποία βασίζεται σε Blockchain είναι η "Learning is Earning 2026"[37]. Η συγκεκριμένη πλατφόρμα βασίζεται στο μοντέλο του κατακερματισμού του προγράμματος σπουδών σε μικρά μπλοκ(δραστηριότητες ανάγνωσης, μαθήματα, κλπ.), όπου ο μαθητής επιλέγει σύμφωνα με τις δικές του ανάγκες και δεξιότητες. Κάθε μονάδα αυτού του προγράμματος μεταφράζεται σε ένα έξυπνο συμβόλαιο το οποίο θα εκτελεστεί όταν ο ενδιαφερόμενος έχει αποκτήσει σε ικανοποιητικό βαθμό τις γνώσεις, τις δεξιότητες ή ακόμα και τις κατάλληλες συμπεριφορές

Η εκπαίδευση είναι ένας πολύπλευρος τομέας όπου διαφορετικά συστήματα πρέπει να προσαρμοστούν για να προετοιμάσουν τους μαθητές για τις θέσεις εργασίας του αύριο. Έχοντας

[37] http://www.learningisearning2026.org

ένα σύστημα το οποίο στηρίζεται στην αντικειμενικότητα και την διαφάνεια και καταγράφει το ακαδημαϊκό ιστορικό ενός φοιτητή πριν και κατά τη διάρκεια της επαγγελματικής του ζωής, μπορεί όχι μόνο να βοηθήσει στην καταπολέμηση της ανεντιμότητας, αλλά μπορεί επίσης να βοηθήσει στην αντιμετώπιση ζητημάτων της μάθησης κατά ζήτηση[38]. Αυτό θα δώσει στους ανθρώπους την ευκαιρία να καθορίσουν την εκπαιδευτική τους πορεία για μια επιτυχημένη μελλοντική σταδιοδρομία.

## 20.3 ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΑΝΑΠΤΥΞΗ

Η αξιολόγηση αποτελεί ένα προβληματικό ζήτημα στο σημερινό εκπαιδευτικό ζήτημα. Η διαμορφωτική αξιολόγηση έχει υποστηριχθεί ως η πιο κατάλληλη διαδικασία η οποία όμως δεν έχει φτάσει στο επιθυμητό επίπεδο. Οι Black και William ορίζουν τη διαμορφωτική αξιολόγηση ως μια μέθοδο που χρησιμοποιεί την ανατροφοδότηση που παρέχεται από το μαθητή προς τον εκπαιδευτικό ή/και από τον εκπαιδευτικό προς το μαθητή αξιολογώντας όλες τις διδακτικές πρακτικές που πραγματοποιούνται μέσα στην τάξη και εντάσσει και τους δύο εμπλεκόμενους στη διαδικασία αυτή. [39] Αποτελεί ουσιαστικά μια διαδικασία που χρησιμοποιείται από τους εκπαιδευτικούς και τους φοιτητές κατά τη διδασκαλία, η οποία παρέχει ανατροφοδότηση για την αναπροσαρμογή της τρέχουσας διδασκαλίας και μάθησης, ώστε να βελτιωθούν τα επιτεύγματα των μαθητών σε σχέση με τους διδακτικούς στόχους που έχουν τεθεί. [40]

Η συγκεκριμένη διαδικασία δεν έχει εφαρμοστεί στο ακέραιο στο βαθμό που απαιτεί το σύγχρονο εκπαιδευτικό σύστημα, δεδομένου ότι δεν μπορεί να εντοπιστεί με ευκολία κάθε λεπτομέρεια της καθημερινής διδασκαλίας και της μάθησης. Παράλληλα, η αντικειμενικότητα της εκπαιδευτικής αξιολόγησης υπονομεύεται από τη στιγμή που ο δημιουργός ενός εκπαιδευτικού συστήματος είναι ταυτόχρονα και ο αξιολογητής του. Οι αξιολογητές ενός συστήματος δεν μπορούν να είναι αμερόληπτοι και αντικειμενικοί όταν εξαρτώνται οικονομικά από τους δημιουργούς του συγκεκριμένου εκπαιδευτικού συστήματος. Επίσης, η εκπαιδευτική αξιολόγηση μπορεί να θεωρηθεί άδικη, διότι οι σχεδιαστές της δεν λαμβάνουν υπόψη τους τις άνισες ευκαιρίες που προσφέρονται στους μαθητές με διαφορετική κοινωνική προέλευση.

[38] Η μάθηση κατά ζήτηση είναι μια φράση που συνδέεται με την έννοια Just-in-Time Learning. Σχετίζεται με τον ρόλο του εκπαιδευόμενου στον καθορισμό του τι θέλει ή τι χρειάζεται να μάθει ανά πάσα στιγμή.

Εφαρμόζοντας την τεχνολογία Blockchain στο εκάστοτε σύστημα αξιολόγησης αλλά και τα έξυπνα συμβόλαια μπορούν να δημιουργήσουν ένα αντικειμενικό και παράλληλα, διαφανές σύστημα. Ειδικότερα, η μη μεταβλητότητα, η ανιχνευσιμότητα και η αξιοπιστία που προσφέρει το Blockchain θα σήμαιναν, ότι τα δεδομένα που θα καταγράφονταν σε αυτό, θα ήταν πιο συγκεκριμένα, αυθεντικά και ανθεκτικά στις κακόβουλες ενέργειες. Για παράδειγμα, η συνεργατική μάθηση θεωρείται ένας εξαιρετικός τρόπος για να ενισχυθεί η επινοητικότητα, η συνεργασία και να καλλιεργηθεί η ικανότητα των μαθητών να δουλεύουν με άλλους. Ωστόσο, συχνά εμφανίζονται φαινόμενα τα οποία παρεμποδίζουν την δίκαιη αξιολόγηση του κάθε μέρους ξεχωριστά, όπως και φαινόμενα όπου κάποιο από τα συνεργαζόμενα μέρη δεν συμβάλλουν στον απαραίτητο βαθμό.

Η τεχνολογία Blockchain μπορεί να μετριάσει αυτά τα φαινόμενα χάρη στην αρχιτεκτονική σχεδίασή της. Κάθε φοιτητής θα υποβάλλει την εργασία του στην πλατφόρμα εκμάθησης μέσω του μοναδικού του λογαριασμού και το έξυπνο συμβόλαιο που θα εκτελείται σε αυτό θα αξιολογήσει την απόδοση του μαθητή και τα αποτελέσματα θα καταγραφούν σε μπλοκ. Όλες οι συμπεριφορές κατά τη διάρκεια της συνεργασίας θα αποθηκευτούν σε μπλοκ ως αποδεικτικά στοιχεία αξιολόγησης. Επιπλέον, το δημόσιο Blockchain είναι αποκεντρωμένο, κάτι το οποίο σημαίνει ότι υπάρχει συνέπεια μεταξύ των κόμβων. Έτσι, ως κόμβοι του δικτύου Blockchain, οι απόψεις των φοιτητών θα λαμβάνονται υπόψη κατά την αξιολόγησή τους. Σε αυτό το πλαίσιο, το Blockchain διασφαλίζει τη δικαιοσύνη κατά τη διαδικασία αξιολόγησης.

Από την πλευρά των εκπαιδευτικών, η διδασκαλία είναι μια πολύπλοκη διαδικασία η οποία είναι δύσκολο να αξιολογηθεί σωστά. Η παραδοσιακή μέθοδος αξιολόγησης των εκπαιδευτικών η οποία βασίζεται στην ανατροφοδότηση των σπουδαστών, τείνει να είναι μονόπλευρη, χωρίς υποκειμενικότητα κάτι το οποίο δεν βοηθά στη βελτίωση των εκπαιδευτικών. Ένα νέο σύστημα αξιολόγησης μπορεί να κατασκευαστεί με βάση το δίκτυο Blockchain και τα έξυπνα συμβόλαια. Αρχικά, οι εκπαιδευτές θα πρέπει να υποβάλλουν από πριν το πρόγραμμα που θα ακολουθήσουν και τις εκπαιδευτικές δραστηριότητες που θα πραγματοποιήσουν ως έξυπνα συμβόλαια στα σχολεία. Κατά τη διάρκεια της διδασκαλίας, όλες οι δραστηριότητες και διαδικασίες που ακολουθήθηκαν θα καταγράφονται στο δίκτυο Blockchain. Τα έξυπνα συμβόλαια θα επαληθεύουν τη συνέπεια του σχεδιασμού που δηλώθηκε πριν την έναρξη της διδασκαλίας, η οποία πρόκειται να αποτελέσει σημαντικό δείκτη αξιολόγησης της διδασκαλίας. Επιπλέον, ένα έξυπνο συμβόλαιο μεταξύ των εκπαιδευτικών και σχολείων, καθώς και αυτό μεταξύ των

εκπαιδευτικών και των μαθητών μπορεί να επαληθευτεί και να συμπληρωθεί μεταξύ τους για την δημιουργία ενός ιδανικού εκπαιδευτικού συστήματος τόσο για τους μαθητές όσο και για τους εκπαιδευτικούς. Οι εκπαιδευτικοί οι οποίοι πληρούν τα πρότυπα, θα λαμβάνουν κάποιο ψηφιακό νόμισμα το οποίο με τη σειρά του θα μπορεί να συνδεθεί με κάποιο άλλο εκπαιδευτική πηγή, όπως πληρωμή σεμιναρίου, είσοδο σε ηλεκτρονικά άρθρα, με σκοπό την ολοκληρωτική εξέλιξή τους. Ένα τέτοιο σύστημα θα έδινε αξία στους εκπαιδευτικούς και θα τους ενθάρρυνε για την απόκτηση περισσότερων διδακτικών δεξιοτήτων.

Από τη πλευρά της ανάπτυξης των σπουδαστών, ο επιβλέπων καθηγητής ή ο ακαδημαϊκός σύμβουλος είναι άμεσα υπεύθυνος για την επίβλεψη του προγράμματος σπουδών του σπουδαστή. Έχει την ευθύνη να βοηθά το σπουδαστή να σχεδιάζει προγράμματα σπουδών και να ενημερώνεται για τις ερευνητικές δραστηριότητες και την πρόοδο των σπουδαστών του. Στην πράξη, τα θέματα αυτά δεν ελέγχονται ούτε εποπτεύονται από κανένα, οπότε δεν θα μπορούσαν να αποδοθούν ευθύνες σε περίπτωση που στο μέλλον ο θεσμός του επιβλέποντα καθηγητή δεν απέδιδε τα δέοντα.

Αυτή η κατάσταση θα μπορούσε να αλλάξει με τη χρήση των έξυπνων συμβολαίων και της τεχνολογίας Blockchain στον συγκεκριμένο τομέα. Όλες οι λεπτομέρειες θα πρέπει να παρακολουθούνται από μια πλατφόρμα έξυπνων συμβολαίων και θα καταγράφονται σε ένα Blockchain. Οι λεπτομέρειες αυτές θα περιέχουν πληροφορίες σχετικά με την επικοινωνία καθηγητή και φοιτητή όπως για παράδειγμα, πόσες φορές έχει συζητήσει ο επιβλέπων καθηγητής με τους φοιτητές το προηγούμενο εξάμηνο ή πόσες φορές εξέτασε την διατριβή ή την διπλωματική εργασία του φοιτητή σε αρχικό και τελικό στάδιο είτε ακόμα εάν ο καθηγητής παρείχε κατάλληλη και στοχευμένη καθοδήγηση στους μαθητές του σχετικά με το ποια μαθήματα θα επιλέξουν καθώς και πως θα σχεδιάσουν μια επικείμενη έρευνα. Χάρη στην ανιχνευσιμότητα και την μη μεταβλητότητα που παρέχει το Blockchain, οι συμπεριφορές και οι λεπτομέρειες της επικοινωνίας θα καταγράφονται τόσο για τους μαθητές όσο και για τους επιβλέποντες τους. Έτσι θα προστατευτούν τα συμφέροντα  και των δύο μερών χωρίς να υπάρχουν κρυφά σημεία στη μεταξύ τους επικοινωνία.

## 20.4 ΔΙΑΔΙΚΤΥΑΚΗ ΜΑΘΗΣΗ

Η διαχρονική εξέλιξη του διαδικτύου δεν θα μπορούσε να αφήσει ανεπηρέαστο και τον κλάδο της εκπαίδευσης. Κατά καιρούς έχουν δημιουργηθεί διαδικτυακές πλατφόρμες γνωστές και ως Μαζικά Ανοιχτά Διαδικτυακά Μαθήματα(MOOC – Massive Open Online Courses), όπως το Udemy και το Coursera, οι οποίες περιέχουν μια σειρά από μαθήματα, όπου οποιοσδήποτε χρήστης από όλο τον κόσμο που έχει πρόσβαση στο διαδίκτυο μπορεί να εγγραφεί και να τα παρακολουθήσει είτε δωρεάν, είτε με ένα μικρό χρηματικό αντάλλαγμα. Μεγάλα πανεπιστήμια όπως το Stanford, Harvard και MIT προσφέρουν δωρεάν μαθήματα online από τα προγράμματα σπουδών τους και τα οποία έχουν προσελκύσει μεγάλο ποσοστό του ακαδημαϊκού κόσμου.

Παρόλο που η ηλεκτρονική εκπαίδευση έχει προσφέρει στους ανθρώπους τη δυνατότητα να μαθαίνουν από την άνεση του σπιτιού τους, υπάρχουν ορισμένα θέματα που πρέπει να ξεπεραστούν. Παραδείγματος χάριν η παρακολούθηση μαθημάτων μέσω διαδικτύου, ακόμα και στη σημερινή εποχή, δε θεωρείται από πολλούς, τόσο φοιτητές όσο και μέλη της πανεπιστημιακής κοινότητας γενικότερα, αντίστοιχης αξίας, βαρύτητας και αποτελεσματικότητας όσο η παραδοσιακή από αμφιθέατρο παρακολούθηση. Επίσης, τα ποσοστά των χρηστών οι οποίοι παραμένουν εγγεγραμμένοι ή ολοκληρώνουν τα διαδικτυακά μαθήματα, παραμένουν χαμηλά, κάτι το οποίο αποτελεί ένα από τα κυριότερα προβλήματα των πλατφορμών ηλεκτρονικής εκπαίδευσης. Σύμφωνα με έρευνα που πραγματοποιήθηκε το 2015[39] σε πλατφόρμες ηλεκτρονικής εκπαίδευσης εγγράφονται περίπου 25000 μαθητές από τους οποίους όμως μόνο το 15% αυτών κατά μέσο όρο ολοκληρώνουν το μάθημα το οποίο εγράφησαν. Οι περισσότεροι από αυτούς τους μαθητές θα ολοκλήρωναν το διαδικτυακό μάθημα που έκαναν εγγραφή, αν αναγνωριζόταν ισότιμα με κάποιο μάθημα από το πρόγραμμα σπουδών κάποιου πανεπιστημίου. Παρόλο που η επιδίωξη για γνώση είναι υψηλή και εξαιρετικά σημαντική, η απόκτηση πτυχίου ή διαπιστευτηρίων τα οποία θα αναγνωρίζονται από την αγορά εργασίας και θα βελτιώνουν τις προοπτικές απασχόλησης είναι το κύριο στοιχείο επιδίωξης των μαθητών. Έτσι, εάν οι περισσότεροι άνθρωποι δεν ολοκληρώνουν αυτά τα μαθήματα, τότε τα οφέλη της διαδικτυακής εκπαίδευσης δεν μπορούν να αφομοιωθούν πλήρως. Όταν κάποιος φοιτητής εγγράφεται σε κάποιο μάθημα, η μόνη ανταμοιβή που λαμβάνει είναι ένας βαθμός. Η διαδικασία αυτή της ανταμοιβής μπορεί να δώσει κάποια κίνητρα στους συμμετέχοντες, αλλά στην περίπτωση της ηλεκτρονικής

[39] http://www.katyjordan.com/MOOCproject.html

αυτοδιδασκαλίας αυτό δεν αρκεί. Οι περισσότεροι άνθρωποι δεν έχουν την πειθαρχία να συνεχίσουν να μαθαίνουν πράγματα, έξω από μια τυποποιημένη διαδικασία μάθησης

Επιπλέον, τα online μαθήματα δίνουν τη δυνατότητα σε έναν μαθητή να συνδυάσει μαθήματα από διαφορετικές πλατφόρμες και να σχηματίσει ένα μείγμα από μαθήματα που ανταποκρίνονται σε ένα πρόγραμμα προπτυχιακών σπουδών κάποιου πανεπιστημίου. Παρόλο που κάποιος μαθητής μπορεί να ολοκληρώσει αυτά τα μαθήματα, δεν θα έχει στα χέρια του κάποιο αποδεικτικό(πτυχίο) το οποίο να αναγνωρίζεται και να πιστοποιεί ότι έχει συμπληρώσει τα απαιτούμενα μαθήματα από τα οποία θα λάμβανε κάποιο πτυχίο. Δεδομένου ότι οι γνώσεις αποκτήθηκαν από πολλαπλές σελίδες και πλατφόρμες, δεν υπάρχει για τον εργοδότη διαφανής και ασφαλής τρόπος να ελέγξει αν ο υποψήφιος υπάλληλος έχει τις απαιτούμενες ικανότητες που βασίζονται στα μαθήματα που έχει ολοκληρώσει για να καλύψει τις απαιτήσεις της αντίστοιχης θέσης. Αυτό καθιστά τα διαδικτυακά μαθήματα λιγότερο ελκυστικά για τους μαθητές.

Ένα άλλο ζήτημα που μαστίζει τον διαδικτυακό χώρο της εκπαίδευσης είναι η έλλειψη μαθημάτων ενδιάμεσου επιπέδου. Η πλειοψηφία των μαθημάτων που είναι διαθέσιμα στις πλατφόρμες διαδικτυακής μάθησης αποσκοπεί σε άτομα που βρίσκονται σε αρχικό στάδια σχετικά με το θέμα που παρουσιάζεται σε κάθε μάθημα. Πλατφόρμες όπως το Udemy και το Coursera παρέχουν βραχυπρόθεσμα μαθήματα που επιτρέπουν στα άτομα να αποκτήσουν μια καλή βάση στο θέμα που θα επιλέξουν να παρακολουθήσουν. Αυτή η αρχική εκπαίδευση είναι ζωτικής σημασίας για όλους εκείνους που ξεκινούν την ενασχόλησή τους με κάποιο θέμα, αλλά κατά τη μετάβαση από το στάδιο των αρχάριων στο επόμενο, υπάρχει δυσκολία στο να βρεθεί επαρκές υλικό που να είναι συνδεδεμένο με το προηγούμενο επίπεδο και το οποίο θα δώσει συνέχεια στις γνώσεις που αποκτήθηκαν.

Τη λύση στα παραπάνω προβλήματα μπορεί να δώσει η τεχνολογία Blockchain μέσω της χρήση ψηφιακών κλειδιών(Token). Η ανταμοιβή των μαθητών οι οποίοι θα συμμετέχουν σε κάποιο διαδικτυακό μάθημα θα γίνεται μέσω των token κατά τη διάρκεια της προόδου τους. Τα ψηφιακά κλειδιά που θα λάβει ο κάθε μαθητής κατά τη διάρκεια παρακολούθησης και ολοκλήρωσης κάποιου μαθήματος, θα μπορούν να ανταλλάσσονται σε κρυπτονομίσματα για τα οποία θα υπάρχει δυνατότητα είτε να τα μετατρέψουν σε μετρητά είτε να τα εξαργυρώσουν σε άλλα μαθήματα ή εκπαιδευτικό υλικό. Η διαδικασία αυτή θα τους δώσει περισσότερα κίνητρα για να ολοκληρώσουν τα διαδικτυακά μαθήματα.

Ένας άλλος τρόπος με τον οποίο μπορεί να επωφεληθεί η διαδικτυακή διδασκαλία από την τεχνολογία Blockchain είναι η βελτίωση του επιπέδου των προσφερόμενων μαθημάτων μέσω της ανταμοιβής των δημιουργών τους. Τα token του Blockchain μπορούν να παρέχουν κίνητρα στους εκπαιδευτικούς που δημιουργούν τα διαδικτυακά μαθήματα, επιβραβεύοντάς τους για τη δημιουργία περιεχομένου υψηλής ποιότητας. Η διαδικασία αυτή έχει υιοθετηθεί από το Youtube, όπου οι "Youtubers" δημιουργούν διασκεδαστικά βίντεο που παρακολουθούν οι θαυμαστές τους. Όσοι περισσότεροι θαυμαστές παρακολουθούν τα βίντεο, τόσο περισσότερα χρήματα καταβάλλονται στους Youtubers μέσω δικαιωμάτων και εγγραφών.

Η ιδέα της ύπαρξης ενός αποκεντρωμένου, διαφανούς και ανθεκτικό στις κακόβουλες επιθέσεις συστήματος το οποίο θα παρέχει τα εκπαιδευτικά προσόντα και την πρόοδο για τα άτομα που επιλέγουν να είναι στην πλατφόρμα ηλεκτρονικής εκπαίδευσης, κερδίζει όλο και περισσότερο έδαφος. Για παράδειγμα ένας μαθητής μπορεί να επιλέξει να παρακολουθήσει ένα μάθημα σχετικό με τα οικονομικά από το Udemy και ένα μάθημα σχετικό με τον προγραμματισμό από το Coursera. Με την ολοκλήρωση αυτών των μαθημάτων η διαδικτυακή πλατφόρμα θα μπορεί να τα επαληθεύσει μέσω του Blockchain, ενημερώνοντας τα εκπαιδευτικά προσόντα του μαθητή και να του δώσει το κατάλληλο πτυχίο. Από την πλευρά του εργοδότη, θα υπάρχει ευκολία στον τρόπο με τον οποίο θα μπορεί να επαληθεύσει τα πτυχία και τις γνώσεις του υποψήφιου εργαζόμενου μέσω της πλατφόρμας Blockchain, από την οποία θα μπορεί να μάθει ποια μαθήματα έχει ολοκληρώσει από που και πότε. Στο μέλλον, τέτοιου είδους ηλεκτρονικές πλατφόρμες θα μπορούν ενδεχομένως να υποβληθούν στον απαραίτητο έλεγχο από κάποιο ρυθμιστικό φορέα, ο οποίος θα διασφαλίζει ότι θα προσφέρονται μαθήματα με ακριβείς γνώσεις, μέσω καλά σχεδιασμένων προγραμμάτων διδασκαλίας όπως επίσης θα διαθέτουν τα κατάλληλα εργαλεία και χαρακτηριστικά για να παίρνουν οι σπουδαστές τα εφόδια που επιθυμούν. Πέρα από δυνατότητα της προσαρμογής των μαθημάτων που θα παρακολουθήσει κάποιος μαθητής, ένα τέτοιο σύστημα θα επιτρέψει την είσοδο και άλλων τεχνολογιών όπως η Μηχανική Μάθηση(Machine Learning) και η Τεχνητή Νοημοσύνη(Artificial Intelligence), οι οποίες θα συνεισφέρουν στη διαμόρφωση ενός εκπαιδευτικού συστήματος το οποίο θα είναι άμεσα συνδεδεμένο με την αγορά εργασίας.

# 21 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Blockchain αποτέλεσε μια επαναστατική καινοτομία η οποία έχει ήδη δείξει τα οφέλη της στον σύγχρονο κόσμο. Παρόλο που έγινε γνωστή στο ευρύ κοινό μέσα από τα κρυπτονομίσματα και συγκεκριμένα το Bitcoin, είναι μια τεχνολογία με δυνατότητες σε διάφορους τομείς. Ο λόγος που η συγκεκριμένη τεχνολογία έχει πολλές προοπτικές υιοθέτησης έγκειται στην ικανότητα της να μετατρέπει ένα σύστημα κεντρικοποιημένης καταγραφής δεδομένων σε ένα κατανεμημένο σύστημα, το οποίο θα εξασφαλίζει ότι τα δεδομένα και οι πληροφορίες δεν μεταβάλλονται καθώς και το ότι παρέχεται η δυνατότητα προστασίας της ιδιωτικότητας.

Στα προηγούμενα κεφάλαια αναλύθηκε η αρχιτεκτονική του Blockchain, το Ethereum, τα έξυπνα συμβόλαια, καθώς και οι πιθανές χρήσεις σε διάφορους κλάδους. Επίσης, ιδιαίτερη έμφαση δόθηκε στον τομέα της πνευματικής ιδιοκτησίας στο διαδίκτυο και στα προβλήματα που αντιμετωπίζουν οι δημιουργοί οποιασδήποτε μορφής ψηφιακού περιεχομένου, στα οποία το Blockchain μπορεί να δώσει λύσεις. Τέλος, έγινε εκτενής αναφορά στην ικανότητα του Blockchain να συνεισφέρει αποτελεσματικά στην επιστημονική έρευνα και τη μάθηση. Οι δύο αυτοί κλάδοι είναι άρρηκτα συνδεδεμένοι μεταξύ τους διότι αφενός μεν η επιστημονική έρευνα, μέσω της συμβολής της στην ανάπτυξη της γνώσης, της πρακτικής βελτίωσης και της ευημερίας μπορεί να συμβάλει καθοριστικά στην εξέλιξη της ανθρωπότητας, αφετέρου δε τα ευρήματα από την επιστημονική έρευνα μπορούν να χρησιμοποιηθούν από τα εκπαιδευτικά συστήματα για να βελτιώσουν και να εξελίξουν τις διαδικασίες διδασκαλίας και μάθησης. Λαμβάνοντας υπόψη τη σημασία των πληροφοριών που διακινούνται κατά καιρούς είτε στον τομέα της έρευνας είτε της μάθησης, η πνευματική ιδιοκτησία αυτών, δεν θα μπορούσε να μην αποτελέσει ακρογωνιαίο λίθο στη δημιουργία του κατάλληλου υπόβαθρου για την ανάπτυξη και εξέλιξη των επιστημονικών διαδικασιών.

Το Blockchain έχει αρχίσει να συνεισφέρει μέσω των ιδιοτήτων και των παροχών του στην πρόοδο της κοινωνίας. Η αναβάθμιση ολόκληρων κλάδων, όπως αυτός της βιομηχανίας και της παγκόσμιας οικονομίας δε θα μπορούσε να μην συμπαρασύρει και αυτόν της εκπαίδευσης, καθώς οι προαναφερθέντες κλάδοι είναι άρρηκτα συνδεδεμένοι με τη ροή των γνώσεων που παρέχονται μέσω της εκπαιδευτικής διαδικασίας. Η επιστημονική έρευνα η οποία αποτελεί ίσως την αρχαιότερη μορφή παραγωγής γνώσης, μπορεί να εξελιχθεί με την βοήθεια του Blockchain σε ένα κλάδο ο οποίος θα δημιουργεί τη γνώση που θα συντελέσει καταλυτικά στην ανάπτυξη και

ευημερία του παγκόσμιου πληθυσμού. Τα αποτελέσματα της έρευνας δίνουν κίνητρο στον κλάδο της μάθησης ο οποίος αποτελεί το συστατικό στοιχείο της εκπαίδευσης και της καλλιέργειας του ανθρώπινου γένους. Η εκπαίδευση είναι ένας πολύπλευρος τομέας όπου τα διαφορετικά συστήματα θα πρέπει να προσαρμοστούν ώστε να προετοιμάσουν τους μαθητές για τις θέσεις εργασίας του αύριο. Απαραίτητη θεωρείται η διασφάλιση των πνευματικών δικαιωμάτων όχι μόνο για λόγους εκμετάλλευσης του εκάστοτε έργου αλλά κυρίως επειδή αυτό αποτελεί προϊόν μόχθου της επιστημονικής κοινότητας. Είναι γεγονός ότι μόνο με την υιοθέτηση ενός δημόσιου Blockchain μπορεί να εκμεταλλευτεί κάποιος πλήρως τα πλεονεκτήματα της συγκεκριμένης τεχνολογίας.

Τα προβλήματα είναι χρόνια και δυσεπίλυτα, τώρα όμως περισσότερο από ποτέ οι συνθήκες έχουν ωριμάσει ώστε να οδηγηθούμε στις βέλτιστες και πλέον μακροπρόθεσμες λύσεις, με την ελπίδα ότι με την περαιτέρω εξέλιξη της τεχνολογίας, αυτές θα αποδεσμεύσουν μόνιμα το σύστημα από τα συνεχώς εμφανιζόμενα προβλήματα. Τροχοπέδη στην εφαρμογή των προσφερόμενων από το Blockchain, λύσεων είναι το γεγονός ότι αποτελεί μια πρόσφατη τεχνολογία η οποία έχει συνδεθεί από την κοινή γνώμη με κλάδους κυρίως της οικονομίας. Εκεί ακριβώς πρέπει η επιστημονική και εκπαιδευτική κοινότητα να αποδείξει ότι μπορεί να εφαρμόσει τους κανόνες αυτής της τεχνολογίας, οδηγώντας την κοινωνία σε επίπεδα αριστείας, αξιοποιώντας τις δυνατότητες για αξιοκρατία και διαφάνεια που αυτή προσφέρει.

# 22 ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

Η παρούσα διπλωματική εργασία ασχολήθηκε κυρίως με τον τρόπο λειτουργίας του Blockchain, την τεχνολογία που κρύβεται πίσω από το Bitcoin και με τα οφέλη της αναδυόμενης τεχνολογίας Blockchain στους τομείς της πνευματικής ιδιοκτησίας, της επιστημονικής έρευνας και της μάθησης. Σκοπός ήταν η ανάλυση των προβλημάτων που έχουν παρατηρηθεί κατά καιρούς καθώς επίσης και η πρόταση λύσεων πάνω σε αυτά.

Όπως έχει αναφερθεί πολλάκις, η πλειοψηφία των εφαρμογών της τεχνολογίας του Blockchain είναι ακόμα σε πιλοτικό επίπεδο στις καθημερινές πρακτικές. Πρέπει λοιπόν με την πορεία του χρόνου να ενταχθεί πιο ουσιαστικά στην καθημερινότητα μας. Μια τέτοια προοπτική βέβαια απαιτεί την δημιουργία διάφορων εφαρμογών που να υλοποιούν την πραγματοποίηση των

όσων περιγράφονται στην παρούσα διπλωματική σε θεωρητικό επίπεδο. Η σύνταξη των εφαρμογών του Blockchain σε μορφή κώδικα, μπορεί να αποτελέσει πεδίο σημαντικής ενασχόλησης για τους χρήστες στο μέλλον.

Αυτή η θεωρητική ανάλυση που πραγματοποιήθηκε κατέστησε σαφή την ανάγκη υλοποίησης μιας αποκεντρωμένης πλατφόρμας με τη χρήση έξυπνων συμβολαίων, η οποία θα χρησιμοποιηθεί από τα εκπαιδευτικά ιδρύματα με σκοπό τη συνένωση των ερευνητικών τους αποτελεσμάτων. Αυτά τα ερευνητικά αποτελέσματα θα είναι διαθέσιμα σε όλα τα ενδιαφερόμενα μέρη τα οποία θα μπορούν να αποκτήσουν τη γνώση που παράγεται και να συνεισφέρουν σε αυτή. Παράλληλα, η διασύνδεση των παραγόμενων αποτελεσμάτων με παγκόσμιες διαδικτυακές πλατφόρμες θα μπορούσε να προσφέρει μάθηση η οποία θα μπορούσε να συμβαδίζει με τα πιο πρόσφατα επιστημονικά επιτεύγματα. Η πρόσβαση σε αυτές τις πληροφορίες θα είναι δυνατή τόσο για εκείνους που ενδιαφέρονται να συνεισφέρουν στην παγκόσμια γνώση και στην προσωπική τους ανάπτυξη όσο και για αυτούς που ενδιαφέρονται να ενταχθούν στην αγορά εργασίας.

Η εφαρμογή μιας τέτοιας καινοτομίας όπως είναι αναμενόμενο θα συναντήσει πολλές δυσκολίες στην εφαρμογή της καθώς απαιτεί ριζικές αλλαγές στον τρόπο διαχείρισης και διαμοιρασμού των κοινόχρηστων πληροφοριών. Αυτές οι δυσκολίες θα μπορέσουν να υπερνικηθούν μέσω συνεχούς εκπαίδευσης και κατανόησης της αναγκαιότητας αναδιάρθρωσης των υπαρχόντων συστημάτων. Συμπερασματικά, τέτοιες ρηξικέλευθες αλλαγές απαιτούν τη συμμετοχή πολλών παραγόντων οι οποίοι θα συνεργαστούν σε μια προσπάθεια βελτιστοποίησης και ανανέωσης των ήδη διαθέσιμων μέσων της διαχείρισης της πληροφορίας.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


[1] J. Bohannon, «The Bitcoin busts,» *Science,* 11 March 2016.

[2] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly, 2015.

[3] «Blockchain Technology as a platform for digitization, Implications for the insurance industry,» October 2017. [Ηλεκτρονικό]. Available: https://www.ey.com/Publication/vwLUAssets/EY-blockchain-technology-as-a-platform-for-digitization/%24FILE/EY-blockchain-technology-as-a-platform-for-digitization.pdf.

[4] A. Wright και P. De Filippi, «Decentralized Blockchain Technology and the Rise of Lex Cryptographia,» 2015.

[5] M. Gupta, Blockchain for Dummies IBM Limited Edition, United States of America: John Wiley & Sons, 2017.

[6] D. Tapscott και A. Tapscott, Blockchain Revolution, New York: Penguin Random House LLC, 2016.

[7] T. Laurence, Blockchain For Dummies, Canada: John Wiley & Sons, 2017.

[8] A. Pinna και W. Ruttenberg, «Distributed ledger technologies in securities post-trading,» European Central Bank, 2016.

[9] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [Ηλεκτρονικό]. Available: https://bitcoin.org/bitcoin.pdf. [Πρόσβαση January 2018].

[10] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, United States of America: O'REILLY, 2014.

[11] «Satoshi Nakamoto,» 2018. [Ηλεκτρονικό]. Available: https://en.bitcoin.it/wiki/Satoshi_Nakamoto. [Πρόσβαση February 2018].

[12] R. Wile, «Bitcoin's Mysterious Creator Appears to be Sitting On a $5.8 Billion Fortune,» 2017.

[13] B. Vitalik, «On Public and Private Blockchains,» 2015.

[14] H. Kakavand και N. Kost De Sevres, «THE BLOCKCHAIN REVOLUTION: AN ANALYSIS OF REGULATION AND TECHNOLOGY RELATED TO DISTRIBUTED LEDGER TECHNOLOGIES,» Commissioner Bart Chilton.

[15] D. M. Davis, «Digital rights management: implications for libraries,» 2002.

[16] A. M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, United States of America: O'Reilly Media, 2017.

[17] V. Buterin, «Tags A next-generation smart contract and decentralized application platform,» 2014.

[18] J. Kurose και K. Ross, Δικτύωση Υπολογιστών, Γκιούρδας, 2013.

[19] L. Pinsard, «Deploy Your First Ethereum Smart Contract on a Blockchain,» 2018.

[20] E. Buchman, «Tendermint: Byzantine Fault Tolerance in the Age of Blockchains,» Canada, 2016.

[21] D. E. O'Leary, «Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems,» 2017.

[22] P. Jayachandran, «The difference between public and private blockchain,» 2017.

[23] «Smart Contracts: The Blockchain Technology That Will Replace Lawyers,» 6 November 2016. [Ηλεκτρονικό]. Available: https://blockgeeks.com/guides/smart-contracts/. [Πρόσβαση 1 August 2018].

[24] V. Buterin, «DAOs, DACs, DAs and More: An Incomplete Terminology Guide,» 6 May 2014. [Ηλεκτρονικό]. Available: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. [Πρόσβαση 6 June 2018].

[25] P. v. Emst, «Please tell me, what is blockchain and how does it work?,» 2017.

[26] D. Hesse και T. Q. Lynn, Simon & Schuster Handbook for Writers (9th Edition), 2015.

[27] E. Diehl, «Securing Digital Video: Techniques for DRM and Content Protection,» Springer, 2012.

[28] B. Depoorter, «Technology and Uncertainty: The Shaping Effect on Copyright Law.,» *University of Pennsylvania Law Review,* 2009.

[29] N. R. Council U.S., The Digital Dilemma: Intellectual Property in the Information Age, Washington: National Academy Press, 2000.

[30] T. McConaghy και D. Holtzman, Towards An Ownership Layer for the Internet, ascribe GmbH, 2015.

[31] M. Casey και P. Vigna, The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order, St. Martin's Press, 2016.

[32] J. Herbert και A. Litchfield, «A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology,» 38th Australasian Computer Science Conference, 2015.

[33] J. Rinaldi, «PEER TO PEER DIGITAL RIGHTS MANAGEMENT USING BLOCKCHAIN,» University of the Pacific , 2018.

[34] B. Clark, «Blockchain and IP Law: A Match made in Crypto Heaven?,» *WIPO Magazine,* 2018.

[35] J. R. Adler, «A new age of peer reviewed scientific journals,» Surg Neurol Int., 2012.

[36] G. Irving και J. Holden, «How Blockchain-Timestamped Protocols Could Improve the Trustworthiness of Medical Science,» 2016.

[37] M. Sharples και J. Domingue, «The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,» European Conference on Technology Enhanced Learning, 2016.

[38] J. Bruer, The Myth of the First Three Years: A New Understanding of Early Brain Development and Lifelong Learning, 2002.

[39] B. Black και D. William , Inside the black box: Raising standards through classroom assessment, Phi Delta Kappan, 1998.

[40] J. W. Popham, Transformative Assessment, Alexandria: Association for Supervision and Curriculum Development, 2008.

[41] R. Takahashi, «How can creative industries benefit from blockchain?,» 18 July 2017. [Ηλεκτρονικό]. Available: https://www.weforum.org/agenda/2018/07/podcast-a-glimpse-into-the-future-of-cities-and-urbanization. [Πρόσβαση February 2018].

[42] A. Savelyev, «Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law,» 2017.

[43] «Blockchain: The Operating System for the Music.,» Revelator, [Ηλεκτρονικό]. Available: https://www.weusecoins.com/assets/pdf/library/Blockchain%20Solution%20for%20the%20Music%20Industry.pdf. [Πρόσβαση March 2018].

[44] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira και A. Akutsu, «The blockchain-based digital content distribution system in Big Data and Cloud Computing,» IEEE Fifth International Conference, 2015.

[45] Π. Β. Κοντογιάννης, «Bitcoin, πλατφόρμα Blockchain και ECDSA,» NTUA, Athens, 2018.

[46] A. Savelyev, «Copyright in the blockchain era: Promises and challenges,» 2017.

[47] «What is Blockchain Technology? A Step-by-Step Guide For Beginners,» [Ηλεκτρονικό]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/.

[48] L. Pinsard, «Deploy Your First Ethereum Smart Contract on a Blockchain!,» 31 January 2018. [Ηλεκτρονικό]. Available: https://blog.theodo.fr/2018/01/deploy-first-ethereum-smart-contract-blockchain/. [Πρόσβαση 6 May 2018].

[49] O. Jallouli, «Chaos-based security under real-time and energy constraints for the Internet of Things,» 2017.

[50] N. Kovalova, «Our choice of digital signature algorithm,» 27 September 2017. [Ηλεκτρονικό]. Available: https://exonum.com/blog/09-27-17-digital-signature/. [Πρόσβαση 20 May 2018].

[51] M. Spearpoin, «A Proposed Currency System for Academic Peer Review Payments Using the BlockChain Technology,» MDPI, 2017.

[52] A. Romero, «Academic Publishing is Big Business, And How Blockchain Can Make A Differen,» 12 July 2018. [Ηλεκτρονικό]. Available: https://www.nasdaq.com/article/academic-publishing-is-big-business-and-how-blockchain-can-make-a-difference-cm990552. [Πρόσβαση 15 July 2018].

[53] M. L. Voight και J. B. Hoogenboom,, «PUBLISHING YOUR WORK IN A JOURNAL: UNDERSTANDING THE PEER REVIEW PROCESS,» US National Library of Medicine National Institutes of Health , 2012.

[54] N. D. FAKOTAKIS, «Blockchain: The Technology That Can Detect Falsified Researches,» 5 July 2018. [Ηλεκτρονικό]. Available: https://www.evolving-science.com/information-communication/blockchain-technology-00713. [Πρόσβαση 10 July 2018].

[55] C. Tozzi, «Blockchain-Based Solutions for Scientific Research,» 5 June 2018. [Ηλεκτρονικό]. Available: https://www.nasdaq.com/article/blockchain-based-solutions-for-scientific-research-cm973435. [Πρόσβαση 25 June 2018].

[56] M. B. Hoy, «An Introduction to the Blockchain and Its Implications for Libraries and Medicine,» 2017.

[57] G. Dütsch και S. Neon , «Use Cases for Blockchain Technology in Energy & Commodity Trading,» 2017.

[58] C. Tozzi, «Graduating Blockchains: Managing Education Credentials on Distributed Ledgers,» 10 November 2017. [Ηλεκτρονικό]. Available: https://www.nasdaq.com/article/graduating-blockchains-managing-education-credentials-on-distributed-ledgers-cm875503. [Πρόσβαση 1 August 2018].

[59] C. Rogers, «What is the role of blockchain in education?,» 30 May 2018. [Ηλεκτρονικό]. Available: https://edtechnology.co.uk/Article/what-is-the-role-of-blockchain-in-education. [Πρόσβαση 6 July 2018].

[60] V. Gupta, «The Promise of Blockchain Is a World Without Middlemen,» 2017.

[61] A. R. Bartolomé, C. Bellver, L. Castañeda και J. Adell, «BLOCKCHAIN IN EDUCATION: INTRODUCTION AND CRITICAL REVIEW OF THE STATE OF THE ART,» 2017.

[62] C. Guang , X. Bing , L. Manli και C. Nian-Shing , «Exploring blockchain technology and its potential applications for education».

[63] M. J. Garbade, «Blockchain In Online Education: Impact And Benefits,» 12 January 2018. [Ηλεκτρονικό]. Available: https://elearningindustry.com/blockchain-in-online-education-impact. [Πρόσβαση 28 July 2018].

[64] C. M. EDITOR, «Is Blockchain the missing piece for online education platforms?,» 2018.

[65] Γ. Ν. Παπαδόδημας, «Ανάπτυξη Έξυπνων Συμβολαίων στο Blockchain και εφαρμογή στο IoT,» NTUA, 2018.

[66] «Proof of Work vs Proof of Stake: Basic Mining Guide,» 2017. [Ηλεκτρονικό]. Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

[67] «What is Ethereum? A Step-by-Step Beginners Guide,» 2017. [Ηλεκτρονικό]. Available: https://blockgeeks.com/guides/ethereum/. [Πρόσβαση 2018].

[68] Σ. Κύπρος, «Δημιουργία Εφαρμογής Blockchain Ethereum και Κρυπτονομίσματος,» 2018.

[69] T. Cox, «Blockchain and Potential Implications for International Book Publishing,» 9 October 2017. [Ηλεκτρονικό]. Available: https://publishingperspectives.com/2017/10/frankfurt-blockchain-potential-implications-publishing/. [Πρόσβαση 1 August 2018].

[70] A. Chang, «Outdated and Ineffective: The Problems with Copyright Law,» 11 April 2018. [Ηλεκτρονικό]. Available: https://5clpp.com/2018/04/11/outdated-and-ineffective-the-problems-with-copyright-law/#_ftn2. [Πρόσβαση 2 August 2018].

[71] A. Dagirmanjian, «BLOCKCHAIN AND INTELLECTUAL PROPERTY: HOW BITCOIN TECHNOLOGY MIGHT CHANGE IP PROTECTION AND REGISTRY,» 4 October 2017. [Ηλεκτρονικό]. Available: http://www.fordhamiplj.org/2017/10/04/blockchain-intellectual-property-bitcoin-technology-might-change-ip-protection-registry/. [Πρόσβαση 2 August 2018].

[72] A. a. C. A. F. Grech, «Blockchain in Education,» European Union 2017, 2017.

[73] K. L. Niedringhaus, «Transforming Customer Service in the Post-Digital Law Library,» American Association of Law Libraries, Chicago, 2017.

[74] Χ. Γεώργίος, «Η ΣΥΝΕΙΣΦΟΡΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ ΩΣ ΕΝΑ ΝΕΟ ΜΕΣΟ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ ΩΣ ΕΝΑ ΚΑΙΝΟΤΟΜΟ ΣΥΣΤΗΜΑ ΠΛΗΡΩΜΩΝ ΣΤΟΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟ ΚΟΣΜΟ,» Πανεπιστήμιο Μακεδονίας, 2016.

[75] D. Meijer, «Consequences of the implementation of blockchain technology,» Delft University of Technology, 2017.

[76] R. Xu, Z. Lu, Z. Huawei και P. Yun, «Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology,» IEEE 13th International Symposium on Autonomous Decentralized Systems, 2017.

[77] D. J. V. ROSSUM, «Blockchain for Research Perspectives on a New Paradigm for Scholarly Communication,» Digital Science , 2017.

[78] M. Martén, «DIGITAL RIGHTS MANAGEMENT – BLOCKCHAIN AND DIGITAL MUSIC CONTENT MANAGEMENT,» UNIVERSITY OF JYVÄSKYLÄ, 2017.

[79] F. Schüpfer, «Design and Implementation of a Smart Contract Application,» University of Zurich, 2017.

[80] M. Lamichhane, «A SMART WASTE MANAGEMENT SYSTEM USING IOT AND BLOCKCHAIN TECHNOLOGY,» ITMO University, 2017.

[81] Μ. Χρήστος, «Η Προοπτική του Blockchain στην Ενεργειακή Βιομηχανία,» Πανεπιστήμιο Πειραιώς, Πειραιάς, 2018.

[82] «Elliptic Curve Cryptography (ECC)».