UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

Postgraduate Program in

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Master Thesis Title:

«Blockchain technologies in agrifood supply chains»

Gregory G. Kalisiakis

A.M: 00397

Supervisor: Thanasis Loukopoulos, Assistant Prof.

2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ:

«Ασφάλειας Υπολογιστικών και Τηλεπικοινωνιακών Συστημάτων, Διαχείρισης Μεγάλου Όγκου Δεδομένων και Προσομοίωσης»

Τίτλος Μεταπτυχιακής Εργασίας:

«Τεχνολογίες Blockchain στην διατροφική αλυσίδα»

Γρηγόριος Γ. Καλησιάκης

Α.Μ: 00397

Επιβλέπων Καθηγητής: Λουκόπουλος Αθανάσιος

2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Εφαρμογές Blockchain στην αγροδιατροφική αλυσίδα» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία
Υπογραφή

«Τεχνολογίες Blockchain στην διατροφική αλυσίδα»

Καλησιάκης Γ. Γρηγόριος

Τριμελής Επιτροπή:

Λουκόπουλος Αθανάσιος (επιβλέπων)

Κακαρούντας Αθανάσιος

Δαδαλιάρης Αντώνιος

Επιστημονικός Σύμβουλος:

.....

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ - ΑΦΙΕΡΩΣΕΙΣ

Αφιερώνεται στους καθηγητές και την οικογένειά μου.

ΠΕΡΙΛΗΨΗ

Η τεχνολογία κατανεμημένου καθολικού (distributed ledger technology), είναι μια βάση δεδομένων συναλλαγών, κατανεμημένη σε ένα ομότιμο (P2P) δίκτυο υπολογιστών. Κάθε κόμβος του δικτύου μπορεί να διαβάζει τις αποθηκευμένες πληροφορίες και, ανάλογα με το επίπεδο πρόσβασης που έχει (permissions), να προσθέτει και δικές του πληροφορίες. Όλα τα δεδομένα συναλλαγών σε ένα distributed ledger έχουν χρονοσήμανση (timestamp) και επομένως υπάρχει μια χρονολογική σειρά. Επίσης τα δεδομένα έχουν και μια μοναδική κρυπτογραφική υπογραφή (unique cryptographic signature).

Μια ειδική περίπτωση αυτής της τεχνολογίας, ίσως η πιο γνωστή, είναι η τεχνολογία blockchain (αλυσίδα συστοιχιών). Ο όρος αλυσίδα συστοιχιών, προκύπτει από το γεγονός ότι οι συναλλαγές ομαδοποιούνται σε συστοιχίες (blocks). Τα blocks συνδέονται μεταξύ τους, δημιουργώντας μια αλυσίδα (chain). Η πιο γνωστή εφαρμογή της blockchain technology, είναι τα κρυπτονομίσματα που πρωτοεμφανίστηκαν με το Bitcoin.

Η εμπορική επιτυχία του Bitcoin, συγκέντρωσε την προσοχή των ερευνητών και της βιομηχανίας, με αποτέλεσμα η έρευνα να επικεντρωθεί στην τεχνολογία blockchain, που ήταν πίσω από το Bitcoin και τις δυνατές εφαρμογές αυτής της τεχνολογίας και σε άλλα πεδία της οικονομίας, πέραν των κρυπτονομισμάτων. Η τεχνολογία blockchain, όπως θα δούμε προσφέρει πολλά πλεονεκτήματα και έχει πολλές δυνατότητες εφαρμογής και είναι μια «επαναστατική» τεχνολογία, με την έννοια ότι δυνητικά μπορεί να μετασχηματίσει τις οργανωτικές δομές και τον τρόπο λειτουργίας, τόσο της οικονομίας αλλά και της κοινωνίας, με τον τρόπο που έγινε και με την υιοθέτηση της τεχνολογίας του διαδικτύου. Όπως ήταν αναμενόμενο, όλο και περισσότεροι οργανισμοί αλλά και εταιρείες επενδύουν στην έρευνα σχετικά με την τεχνολογία blockchain και σε πιλοτικές εφαρμογές της,.

Αν και υπάρχει πολλή βιβλιογραφία γύρω από την εφαρμογή της τεχνολογίας στα κρυπτονομίσματα, δεν υπάρχουν αντίστοιχα πολλές έρευνες για άλλους τομείς, όπως για παράδειγμα η χρήση της σε εφοδιαστικές αλυσίδες και ιδιαίτερα στον αγροδιατροφικό τομέα, που έννοιες όπως η ασφάλεια και η διαφάνεια της όλης

διαδικασίας παραγωγής τροφίμων απασχολούν όλο και περισσότερο τους καταναλωτές.

Σε παρούσα διπλωματική εργασία, ασχολούμαστε με την εφαρμογή της ίδιας τεχνολογίας στην αγροδιατροφική αλυσίδα εφοδιασμού.

- Διευκρινίζουμε βασικές έννοιες της τεχνολογίας blockchain. Εντοπίζουμε και αναφέρουμε προοπτικές από την εφαρμογή της τεχνολογίας σε διάφορους τομείς της οικονομίας, καθώς και πιθανά προβλήματα. Ιδιαίτερα εξετάζουμε την δυνατότητα εφαρμογής της στον αγροδιατροφικό τομέα, παραθέτοντας υπάρχοντα παραδείγματα εφαρμογής της.
- Εξετάζουμε (case study) την δυνατότητα εφαρμογής της, στον κλάδο του ελαιόλαδου, ένα αγροδιατροφικό προϊόν με ιδιαίτερη σημασία για τον Έλληνα καταναλωτή, παραγωγό και έμπορο.
- Προτείνουμε μια μεθοδολογία σταδιακής υιοθέτησης της τεχνολογίας blockchain από επιχειρήσεις.
- Συγκρίνουμε διάφορες πλατφόρμες blockchain για ανάπτυξη τέτοιων εφαρμογών, εστιάζοντας στα κύρια γνωρίσματα τους.
- Δίνουμε ένα απλό παράδειγμα δημιουργίας μια private blockchain χρησιμοποιώντας την open source πλατφόρμα Multichain.
- Παρουσιάζουμε ένα απλοποιημένο σενάριο εφαρμογής της, τεχνολογίας blockchain σε μια επιχείρηση αγροδιατροφικού κλάδου, σύμφωνα με συγκεκριμένη μεθοδολογία, με χρήση της πλατφόρμας Multichain και open source κώδικα (Github: https://github.com/AravindNico/blockchain_agri_usecase).
- Τέλος παρουσιάζουμε συμπεράσματα, σχετικά με τα προβλήματα εφαρμογής αλλά και τις δυνατότητες και προοπτικές της τεχνολογίας blockchain σε αγροδιατροφικές αλυσίδες εφοδιασμού.

Οι βιβλιογραφικές αναφορές είναι σύμφωνες με το IEEE Citation Style.

Λέξεις κλειδιά

Τεχνολογία blockchain, εξόρυξη, εφοδιαστικές αλυσίδες, αγροδιατροφικές αλυσίδες, ιχνηλασιμότητα τροφίμων, διαφάνεια στα τρόφιμα, ασφάλεια τροφίμων, Multichain.

Abstract

Distributed ledger technology, is a transactional database distributed over a peer-to-peer (P2P) computer network. Each node in the network can read the stored information and, depending on its permissions, add its own information. All transaction data is timestamped and therefore there is a chronological order. The data are also encrypted and digitally signed. Each node of the network replicates and saves an identical copy of the database (distributed ledger). With the use of consensus algorithms there is no need of a central trusted authority or centralized data storage.

The most popular member of this family of technologies is Blockchain technology. The term “blockchain”, derives from the fact that transactional data are grouped into blocks. The blocks are connected together, forming a chain. Every node has a copy of the blockchain, containing all transactions that have been executed. The best known application of blockchain technology is the cryptocurrencies that first appeared with Bitcoin.

In this thesis we deal with the main characteristics of the blockchain technology and its possible applications in agri-food supply chains (Case Study: olive oil).

Furthermore, we compare different blockchain platforms, focusing on their general description, their main technological properties. Additionally, we will perform a hypothetical case study (a simplistic scenario of an agrifood supply chain implementation with only 3 nodes, using Multichain). Finally we present our conclusions, indicating possible risks and business opportunities.

References are cited according to IEEE Citation Style.

Key words

Bblockchain technology, mining, supply chains, agrifood supply chains, food traceability, food transparency, food safety, Multichain.

ΠΡΟΛΟΓΟΣ

Η πρόσφατη εμπορική επιτυχία του Bitcoin και των υπόλοιπων «κρυπτονομισμάτων» εστίασε το ενδιαφέρον της βιομηχανίας αλλά και της επιστημονικής κοινότητας, μεταξύ άλλων, στην τεχνολογία blockchain (μετάφραση στα ελληνικά: τεχνολογία «αλυσίδας συστοιχιών»), που βρίσκεται πίσω από αυτά. Αρχικά η τεχνολογία blockchain έγινε συνώνυμο των κρυπτονομισμάτων, όμως γρήγορα έγινε κατανοητό ότι οι εφαρμογές της μπορούν να επεκταθούν και σε άλλους στους τομείς της οικονομίας και επιπλέον μπορούν να αλλάξουν τον τρόπο οργάνωσης και λειτουργίας της οικονομίας, επιφέροντας αντίστοιχα κοινωνικές, πολιτικές και νομικές αλλαγές.

Η αποκεντρωμένη φύση της νέας τεχνολογίας, το γεγονός ότι δεν απαιτεί την ύπαρξη μιας κεντρικής έμπιστης αρχής ή ότι δεν απαιτείται εμπιστοσύνη μεταξύ των χρηστών, καθιστούν το Blockchain ελκυστικό. Όλο και περισσότερες εφαρμογές αναπτύσσονται καλύπτοντας όλα σχεδόν τα πεδία της οικονομίας. Δημόσιες αρχές και οργανισμοί, αλλά και εταιρείες επενδύουν και εφαρμόζουν πιλοτικά τη νέα τεχνολογία. Αναφέρουμε ενδεικτικά του ενδιαφέροντος που επικρατεί, την σύσταση παρατηρητηρίου και forum blockchain (τον Φεβρουάριου του 2018), με σκοπό την παρακολούθηση των εξελίξεων και την προώθηση της νέας τεχνολογίας, σε επίπεδο Ευρωπαϊκής Ένωσης

Πρόσφατα, υπάρχει εκτεταμένη έρευνα και βιβλιογραφία για την τεχνολογία Blockchain, αλλά η εφαρμογή της σε αλυσίδες εφοδιασμού (supply chains) είναι ακόμη σχετικά ανεξερεύνητη. Υπάρχουν εταιρείες που έχουν ξεκινήσει πιλοτικά projects για τη χρήση του Blockchain στη διαχείριση της αλυσίδας εφοδιασμού. Επίσης οι επιχειρήσεις που ενεργοποιούνται στην παραγωγή αγροδιατροφικών προϊόντων (agrifood products) βλέπουν δυνατότητες στη χρήση αυτής της τεχνολογίας για βελτιωμένη ιχνηλασιμότητα (traceability) στην αλυσίδα παραγωγής, τυποποίησης και διακίνησης των προϊόντων τους.

Στην παρούσα διπλωματική εργασία θα διερευνήσουμε την δυνατότητα εφαρμογής της τεχνολογίας Blockchain σε αγροδιατροφικές εφοδιαστικές αλυσίδες. Θα παρουσιάσουμε τις βασικές πτυχές της νέας τεχνολογίας και θα δούμε περιπτώσεις εφαρμογής της σε διάφορους τομείς της οικονομίας, σύμφωνα με τη σχετική

βιβλιογραφία. Θα παρουσιάσουμε συμπεράσματα σχετικά με την αποτελεσματικότητα της τεχνολογίας Blockchain ως μέσου για τη βελτίωση της ιχνηλασιμότητας τροφίμων, ενώ θα δούμε και τη δυνατότητα εφαρμογής της συγκεκριμένης τεχνολογίας στην περίπτωση του έξτρα παρθένου ελαιόλαδου, που έχει ιδιαίτερο ενδιαφέρον από πλευράς αγροδιατροφικού προϊόντος για την Ελλάδα. Επίσης θα εξετάσουμε αν η χρήση αυτής της καινοτόμου τεχνολογίας μπορεί να αποτελέσει αναπτυξιακό εργαλείο του αγροδιατροφικού τομέα.

Γίνεται χρήση πηγών από σχετική βιβλιογραφία και το διαδίκτυο.

ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ - ΜΕΘΟΔΟΛΟΓΙΑ

ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

Αρχικά θα πρέπει να αποσαφηνίσουμε ορισμένες βασικές έννοιες, που χρησιμοποιούνται στην παρούσα εργασία.

Κεντρικό Δίκτυο (Centralized network)

Ένα δίκτυο αποτελείται από κόμβους (nodes) και κανάλια επικοινωνίας (message channels), μέσω των οποίων επικοινωνούν οι κόμβοι μεταξύ τους.. Οι κόμβοι επεξεργάζονται και αποθηκεύουν δεδομένα και ανταλλάσουν αυτά τα δεδομένα μεταξύ τους ή όπως λέμε «συναλλάσσονται» μεταξύ τους. Σε ένα κεντρικό δίκτυο, όλοι οι κόμβοι συνδέονται με έναν κεντρικό κόμβο και επικοινωνούν μεταξύ τους μόνο μέσω αυτού του κόμβου. Λέγονται και δίκτυα αρχιτεκτονικής Client-Server (όπου server είναι ο κεντρικός κόμβος και clients οι υπόλοιποι). Στην περίπτωση ενός τέτοιου δικτύου, αν βγει εκτός λειτουργίας ο server, καταρρέει όλο το δίκτυο. Το δίκτυο είναι ιεραρχημένο.

Αποκεντρωμένο Δίκτυο (Decentralized network)

Σε ένα αποκεντρωμένο δίκτυο υπάρχουν περισσότεροι servers μέσω των οποίων συνδέονται οι υπόλοιποι κόμβοι. Σε αυτή την περίπτωση πετυχαίνουμε μεγαλύτερη «ανθεκτικότητα» του δικτύου, αφού στην περίπτωση που κάποιοι από τους κύριους κόμβους καταρρεύσουν, το δίκτυο θα συνεχίσει να λειτουργεί κανονικά μέσω των υπόλοιπων διαθέσιμων servers. Το δίκτυο είναι ιεραρχημένο.

Κατανεμημένο Δίκτυο (Distributed network)

Το κατανεμημένο δίκτυο, είναι ένα έντονα διασυνδεδεμένο δίκτυο. Όλοι οι κόμβοι είναι συνδεδεμένοι μεταξύ τους, χωρίς την χρήση κεντρικού κόμβου. Και σε αυτή την περίπτωση, αν μέρος του δικτύου καταρρεύσει, το υπόλοιπο δίκτυο συνεχίζει να λειτουργεί κανονικά, αφού η επικοινωνία μπορεί να γίνεται μέσω των υπολοίπων κόμβων. Τα κατανεμημένα δίκτυα είναι πιο ανθεκτικά.

Ομότιμη σύνδεση (Peer to Peer - P2P)

Η ομότιμη σύνδεση (P2P), αναφέρεται σε ένα κατανεμημένο δίκτυο. Ο όρος ομότιμη, σημαίνει ότι οι όλοι οι κόμβοι του δικτύου είναι ομότιμοι/ίσοι μεταξύ τους. Δεν υπάρχουν κεντρικοί κόμβοι. Δεν υπάρχει ιεραρχία στο δίκτυο. Κάθε κόμβος κατέχει το σύνολο των διαμοιραζόμενων δεδομένων (shared data). Κάθε φορά που αλλάζουν τα

διαμοιραζόμενα δεδομένα, μέσω μιας συναλλαγής, ενημερώνονται όλοι οι κόμβοι σε πραγματικό χρόνο.

Συναλλαγή (transaction)

Ο όρος συναλλαγή, αναφέρεται στη ανταλλαγή πληροφοριών-δεδομένων μεταξύ δύο κόμβων ενός δικτύου.

Καθολικό/Μητρώο/Δημόσιο Βιβλιάριο Καταγραφής Συναλλαγών

Το δημόσιο βιβλιάριο καταγραφής συναλλαγών ή καθολικό ή μητρώο (ledger) είναι ένα ψηφιακό αρχείο καταγραφής δεδομένων, στο οποίο όλοι έχουν πρόσβαση και όλοι μπορούν να διαβάσουν δεδομένα που περιέχει ή να προσθέσουν νέα δεδομένα συναλλαγών σε αυτό. Τα δεδομένα συναλλαγών φέρουν χρονοσήμανση.

Κατανεμημένο Καθολικό (distributed ledger)

Είναι το καθολικό το οποίο είναι αποθηκευμένο σε περισσότερους κόμβους ενός ομότιμου κατανεμημένου δικτύου. Στον κάθε κόμβο, διατηρείται έγκυρο αντίγραφο του τρέχοντος καθολικού. Από την στιγμή που τα δεδομένα μιας συναλλαγής επικυρωθούν και καταγραφούν στο δημόσιο καθολικό, δεν μπορούν να διαγραφούν, ούτε να αλλάξουν και με την έννοια αυτή είναι αναλλοίωτα (immutable). Σε ένα distributed ledger, οι κόμβοι μπορεί να είναι ανώνυμοι (anonymous) ή έμπιστοι (trusted). Στην πρώτη περίπτωση κάθε κόμβος έχει την ευθύνη διατήρησης του δικού του επικυρωμένου αντιγράφου του ledger και συμμετέχει στην διαδικασία επικύρωσης και καταγραφής νέων συναλλαγών. Στην δεύτερη περίπτωση, μόνο οι έμπιστοι κόμβοι συμμετέχουν στην διαδικασία επικύρωσης και καταγραφής νέων συναλλαγών και διατηρούν ένα επικυρωμένο αντίγραφο του ledger, ενώ οι υπόλοιποι κόμβοι αναφέρονται σε αυτούς.

Blockchain

Σύμφωνα με τον Tapscott (2016), βλ. σχετικά [5], *«το blockchain είναι ένα αδιάφθορο ψηφιακό λογιστικό βιβλίο για οικονομικές συναλλαγές, που μπορεί να προγραμματιστεί να καταγράφει όχι μόνο οικονομικές συναλλαγές αλλά ουσιαστικά οτιδήποτε έχει αξία»*. Το blockchain κυριολεκτικά είναι μια αλυσίδα (chain) από blocks δεδομένων συναλλαγών, σε ψηφιακή μορφή. Πρόκειται μια βάση δεδομένων συναλλαγών, κατανεμημένη σε ένα ομότιμο (P2P) δίκτυο υπολογιστών. Κάθε κόμβος του δικτύου μπορεί να διαβάζει τις αποθηκευμένες πληροφορίες και ανάλογα με το επίπεδο πρόσβασης που έχει (permissions), να προσθέτει και δικές του πληροφορίες. Όλα τα

δεδομένα συναλλαγών έχουν χρονοσήμανση (timestamp) και επομένως υπάρχει μια χρονολογική σειρά. Επίσης τα δεδομένα έχουν και μια μοναδική κρυπτογραφική υπογραφή (unique cryptographic signature). Οτιδήποτε συμβαίνει σε ένα blockchain, είναι μια λειτουργία του δικτύου. Τα πρωτόκολλα του δικτύου του blockchain, είναι υπεύθυνα να επιβεβαιώσουν την ακεραιότητα και την ορθότητα των συναλλαγών. Με χρήση αλγορίθμων συναίνεσης, δεν απαιτείται η ύπαρξη μιας κεντρικής έμπιστης αρχής, ούτε απαιτείται εμπιστοσύνη μεταξύ των χρηστών. Επίσης δεν απαιτείται κεντρική αποθήκευση των δεδομένων σε κάποιον server του δικτύου. Όλα τα δεδομένα είναι δημόσια και εύκολα επαληθεύσιμα.

Κρυπτονόμισμα (Cryptocurrencies)

Με τον όρο «κρυπτονόμισμα» αναφερόμαστε σε ψηφιακό νόμισμα. Είναι δηλαδή μια μορφή χρήματος. Ως χρήμα εννοείται οποιοδήποτε επαληθεύσιμο μέσο ή εγγραφή το οποίο έχει αξία και λειτουργεί ως συναλλακτικό μέσο. Τα κρυπτονομίσματα δεν έχουν φυσική υπόσταση, αλλά αποτελούν επαληθεύσιμες ψηφιακές εγγραφές. Ο όρος κρυπτονόμισμα προκύπτει από την χρήση κρυπτογραφικών μεθόδων, προκειμένου να είναι ασφαλείς οι συναλλαγές και να μην είναι δυνατή η αλλοίωση των δεομένων. Υπάρχουν περίπου 700 κρυπτονομίσματα σε κυκλοφορία, ενώ τα πιο γνωστά από αυτά, είναι το Bitcoin και το Ether.

Συστοιχία (Block)

Η συστοιχία (block), είναι ένα σύνολο από δεδομένα, που αφορούν μια συναλλαγή του blockchain. Τα blocks αντιστοιχούν θα λέγαμε, στις ψηφιακές «σελίδες» του καθολικού (ledger). Είναι ένα αρχείο, το οποίο περιέχει και επικυρώνει συναλλαγές στο blockchain. Σε προκαθορισμένα χρονικά διαστήματα, ένα νέο block που περιλαμβάνει συναλλαγές συνδέεται στην αλυσίδα των blocks, μέσω της διαδικασίας της «εξόρυξης» (mining). Τα δεδομένα των blocks διακρίνονται, ως προς την φύση τους, σε αυτά που αφορούν πληροφορίες με ανθρώπινο εννοιολογικό περιεχόμενο και αντιστοιχούν σε κάποια ανθρώπινη συναλλαγή (transaction data) και σε αυτά που προστίθενται στο block προκειμένου να εξασφαλιστεί η σωστή αποθήκευση και διαφύλαξη των δεδομένων στο blockchain (metadata).

Κόμβος Blockchain

Το blockchain είναι ένα δίκτυο «κόμβων». Κάθε κόμβος (node), απαιτεί την ύπαρξη συσκευής με κατάλληλο λογισμικό, προκειμένου να επικοινωνεί με άλλους κόμβους

του blockchain, μέσω διαδικτύου. Κάθε κόμβος ενός blockchain διαθέτει ένα αντίγραφο του τρέχοντος αρχείου του blockchain, το οποίο λαμβάνει αυτόματα όταν συνδέεται στο δίκτυο του blockchain. Είναι σημαντικό να σημειωθεί ότι αυτό δεν είναι ένα μικρό σε μέγεθος αρχείο, αφού πρέπει να «κατεβεί» (download), ολόκληρο το ιστορικό του blockchain. Για το λόγο αυτό, μπορεί σε ένα δίκτυο blockchain να υπάρχουν διαφοροποιημένοι κόμβοι, ανάλογα με τον τρόπο λειτουργίας τους. Διακρίνουμε τους κόμβους ενός blockchain σε full nodes εξυπηρετούν και light nodes (lightweight clients). Ένας full node είναι ένας κόμβος, που επιβάλλει πλήρως όλους τους κανόνες του blockchain (πιστοποιεί και επικυρώνει συναλλαγές, διατηρεί ένα έγκυρο αντίγραφο του blockchain και θεωρείται ως «έμπιστος» (trusted) κόμβος του blockchain). Ένας light node, δεν διατηρεί δικό του αντίγραφο του blockchain αλλά αναφέρεται σε ένα αντίγραφο ενός full node (για παράδειγμα ένας full node, επιτρέπει στους clients να μεταδώσουν transactions στο δίκτυο και τους ειδοποιεί αν ένα transaction τους αφορά).

Bitcoin Δίκτυο (Bitcoin Network)

Το Bitcoin ήταν το πρώτο κρυπτονόμισμα. Ο όρος Bitcoin Δίκτυο αναφέρεται σε ένα σύνολο από κόμβους οι οποίοι εκτελούν το πρωτόκολλο Bitcoin.

Satoshi Nakamoto

Το όνομα Σατόσι Νακαμότο χρησιμοποιήθηκε από τον ανώνυμο δημιουργό (ή τους ανώνυμους δημιουργούς) που είχαν την ιδέα του bitcoin, υπέγραψαν τη Λευκή Βίβλο του bitcoin, αλλά και ανέπτυξαν την πρώτη υλοποίηση αναφορών (reference implementation) του bitcoin. Ως μέρος της υλοποίησης, ανέπτυξαν την πρώτη βάση δεδομένων του blockchain και έλυσαν το πρόβλημα της διπλής δαπάνης (double spending). Ήταν ενεργοί στην ανάπτυξη του bitcoin μέχρι και τον Δεκέμβριο του 2010.

Πορτοφόλια (Wallets)

Ένα πορτοφόλι χρήστη, είναι στην ουσία ένα λογισμικό, μια client εφαρμογή, που αντιστοιχεί σε μια διεύθυνση του δικτύου blockchain και αποθηκεύει ιδιωτικά και δημόσια κλειδιά του χρήστη. Αποθηκεύει tokens και επιτρέπει στους χρήστες να διενεργούν συναλλαγές στο blockchain, χωρίς να απαιτείται να γνωρίζουν τεχνικές λεπτομέρειες για το blockchain και χωρίς να συμμετέχουν απαραίτητα στην διαδικασία εξόρυξης (mining) νέων blocks.

Κρυπτογραφία

Η κρυπτογραφία αφορά την δημιουργία μεθόδων και την χρήση κατάλληλων πρωτοκόλλων, προκειμένου να εμποδίσουμε τρίτα «κακοπροαίρετα» μέρη (adversaries), να διαβάσουν ιδιωτικά μηνύματα.

Η όλη διαδικασία περιλαμβάνει 2 στάδια:

- την εφαρμογή κατάλληλων αλγορίθμων για την κρυπτογράφηση (encryption) των δεδομένων ώστε να είναι ασφαλή κατά την μετάδοση τους μέσω ενός δικτύου,
- την εφαρμογή κατάλληλων αλγορίθμων για την αποκρυπτογράφηση (decryption) των δεδομένων κατά την παραλαβή τους.

Κατά την κρυπτογράφηση και της αποκρυπτογράφηση γίνεται χρήση δύο ψηφιακών κλειδιών:

1. Το Public key, το οποίο είναι δημόσιο και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων.
2. Το Private Key, το οποίο είναι ιδιωτικό και μυστικό και σε συνδυασμό με το Public Key, χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων.

Κρυπτογραφική Συνάρτηση Κατακερματισμού (- Hash value)

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού είναι ένα βασικό εργαλείο της σύγχρονης κρυπτογραφίας. Μια Κρυπτογραφική Συνάρτηση Κατακερματισμού (Cryptographic Hash Function - CHF) είναι μια συνάρτηση κατακερματισμού που είναι κατάλληλη για χρήση στην κρυπτογραφία. Πρόκειται για έναν αλγόριθμο που αντιστοιχεί δεδομένα αυθαίρετου μεγέθους (αρχικό μήνυμα) σε μια συμβολοσειρά από bits, σταθερού μεγέθους. Η συμβολοσειρά αυτή ονομάζεται "hash value" ή απλά "hash". Η λειτουργία αυτή είναι μη αντιστρέψιμη, αφού είναι πρακτικά ανέφικτο να παράγουμε από το hash το αρχικό μήνυμα και επομένως το αρχικό μήνυμα δεν μπορεί να αποκρυπτογραφηθεί. Στο blockchain, χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης SHA-256 (Secure Hash Algorithm), ο οποίος κάνει χρήση ενός συνόλου κρυπτογραφικών συναρτήσεων κατακερματισμού και κρυπτογραφεί τα δεδομένα, επιστρέφοντας πάντα ένα μοναδικό αλφαριθμητικό Hash 256-bit (32-byte).

Παράδειγμα SHA-256

μήνυμα: *hello greg!*

hash: *3f4a96ebb097c54e75005dafd27d7443a492cb886bece8c3046dff195e005bd0*

μήνυμα: *blockchain rules*

hash: *e630bcb38a039af9a4a2ceb3a4d80b097d917fdcd04cef59d39bc1d84b9d289f*

Ψηφιακή υπογραφή (Digital Signature)

Η ψηφιακή υπογραφή είναι ένας αλγόριθμος για την επαλήθευση της αυθεντικότητας των ψηφιακών μηνυμάτων ή εγγράφων. Μια έγκυρη ψηφιακή υπογραφή, εξασφαλίζει στον παραλήπτη ενός μηνύματος, ότι το μήνυμα δημιουργήθηκε από έναν γνωστό αποστολέα (ταυτοποίηση - authentication), καθώς και ότι το μήνυμα δεν μεταβλήθηκε κατά τη μεταφορά (ακεραιότητα δεδομένων - data integrity). Στην ψηφιακή υπογραφή μηνυμάτων ή εγγράφων, γίνεται χρήση μεθόδων κρυπτογράφησης/αποκρυπτογράφησης καθώς και ψηφιακών κλειδιών. Σε αυτή την διαδικασία, ο αποστολέας ενός μηνύματος υπογράφει ψηφιακά το μήνυμα, προσθέτοντας έτσι στο αρχικό μήνυμα δεδομένα, κρυπτογραφημένα με το ιδιωτικό του κλειδί. Ο παραλήπτης του μηνύματος, λαμβάνει τόσο το μήνυμα όσο και την υπογραφή. Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να επαληθεύσει την αυθεντικότητα του μηνύματος και του αποστολέα.

Παραστατικό χρήμα (fiat currency)

Το παραστατικό χρήμα είναι το μέσο πληρωμής που σχετίζεται με ένα εθνικό νόμισμα, όπως το αμερικανικό δολάριο ή το ευρώ.

Μάρκες (Tokens)

Μια μάρκα (token), είναι μια μονάδα ενός ψηφιακού αγαθού (digital asset) σε μια αλυσίδα blockchain. Τα tokens σαν έννοια είναι ευρύτερη από την έννοια του κρυπτονομίσματος. Για παράδειγμα το Ether είναι το native token σε ένα Ethereum blockchain. Όμως υπάρχουν blockchains πλατφόρμες που υποστηρίζουν την χρήση πολλών κρυπτονομισμάτων ή άλλων ψηφιακών αγαθών. Η συμμετοχή σε ένα δίκτο blockchain, προϋποθέτει την αγορά tokens με χρήση fiat currency (π.χ ευρώ) ή με συμβατό κρυπτονόμισμα (π.χ bitcoin, ether).

Εξόρυξη (Mining)

Εξαιτίας της κρυπτογραφημένης φύσης των κρυπτονομισμάτων, η εξακρίβωση των συναλλαγών απαιτεί ένα τεράστιο ποσό υπολογιστικής δύναμης και εξειδικευμένου hardware. Ως αντάλλαγμα για την υπολογιστική δύναμη που καταναλώνουν, οι κόμβοι ενός δικτύου blockchain, που εγκρίνουν μια συναλλαγή, αμείβονται για τις συναλλαγές που επιβεβαιώνουν. Αυτή η διαδικασία ονομάζεται εξόρυξη και οι κόμβοι

που μετέχουν σε αυτή την διαδικασία παραγωγής και πιστοποίησης νέων blocks ονομάζονται miners.

Διχάλα (Fork)

Η διχάλα είναι μια διαδικασία κατά την οποία δημιουργείται μια εναλλακτική εκδοχή του blockchain, επιτρέποντας σε δύο αλυσίδες να τρέχουν παράλληλα σε διαφορετικές περιοχές του δικτύου.

Ως soft fork, ονομάζουμε μια backward-compatible αλλαγή στα πρωτόκολλα του blockchain δικτύου. Οι παλιοί κόμβοι (old nodes) του blockchain δικτύου, θα αναγνωρίζουν τα νέα blocks ως έγκυρα (valid) . Δεν απαιτεί να αναβαθμιστούν όλοι οι κόμβοι στα νέα πρωτόκολλα, αρκεί ένας ικανός αριθμός από miners να αναβαθμιστεί για να επιβάλλει την αλλαγή των πρωτοκόλλων στο blockchain.

Ως hard fork, ονομάζουμε μια ριζική αλλαγή στα πρωτόκολλα του blockchain δικτύου που στην ουσία κάνει προηγούμενα blocks και transactions μη έγκυρα. Οι παλιοί κόμβοι (old nodes) του blockchain δικτύου, δεν θα αναγνωρίζουν τα νέα blocks ως έγκυρα (valid) δλδ το hard fork δεν είναι backward-compatible. Κάθε κόμβος (node) του blockchain, πρέπει να αναβαθμιστεί (upgrade) στην τελευταία έκδοση των πρωτοκόλλων του blockchain.

Πρώτη συναλλαγή (Genesis Block)

Πρόκειται για το πρώτο block ενός blockchain.

Έξυπνα συμβόλαια (Smart Contracts)

Εκτός από τα κρυπτονομίσματα ή tokens, κάποιες αλυσίδες υποστηρίζουν επίσης τα έξυπνα συμβόλαια. Τα έξυπνα συμβόλαια είναι στην ουσία προγράμματα τα οποία ενεργοποιούνται και εκτελούν αυτόματα μια συναλλαγή, όταν ικανοποιηθούν συγκεκριμένες προϋποθέσεις. Τα έξυπνα συμβόλαια εκτελούνται από τους κόμβους και οι συναλλαγές καταγράφονται στο blockchain καθιστώντας την πληροφορία αμετάβλητη και αδιαμφισβήτητη. Το όνομα «Έξυπνα Συμβόλαια» το επινόησε ο Nick Szabo το 1994. Τα έξυπνα συμβόλαια προσφέρουν, ασφάλεια και μείωση κόστους. Η επικρατέστερη μορφή έξυπνων συμβολαίων είναι το Ethereum.

Blockchain Oracles

Τα oracles είναι υπηρεσίες που αποστέλλουν και επαληθεύουν τα γεγονότα του πραγματικού κόσμου και υποβάλλουν αυτές τις πληροφορίες σε έξυπνα συμβόλαια εντός ενός blockchain, προκαλώντας έτσι συναλλαγές. Τα blockchains και τα έξυπνα συμβόλαια δεν μπορούν να έχουν πρόσβαση σε δεδομένα εκτός του δικτύου τους. Επομένως για να μάθει τι πρέπει να κάνει, ένα έξυπνο συμβόλαιο συχνά χρειάζεται πρόσβαση σε «δεδομένα από τον έξω κόσμο» (δλδ transactional data) που σχετίζονται με τη συμβατική συμφωνία, με τη μορφή ψηφιακών δεδομένων.

Υπάρχουν διαφορετικοί τύποι oracles:

- Software Oracle – εισάγουν δεδομένα από online πηγές
- Hardware Oracle - εισάγουν δεδομένα που προέρχονται από hardware πηγές
- Inbound Oracle - εισάγουν transactional data
- Outbound Oracle - εξάγουν transactional data
- Consensus-based Oracle - εισάγουν δεδομένα από prediction markets

Αποκεντρωμένες Εφαρμογές (Decentralized Applications – dApps)

Σε αντίθεση με τις συγκεντρωτικές εφαρμογές που εκτελούνται σε ένα μόνο υπολογιστή, οι αποκεντρωμένες εφαρμογές (dApps), εκτελούνται σε δίκτυο υπολογιστών P2P. Έχουν υπάρξει από την εμφάνιση δικτύων P2P. Οι αποκεντρωμένες εφαρμογές δεν χρειάζεται απαραίτητα να λειτουργούν πάνω από ένα δίκτυο blockchain. Η διεπαφή με το χρήστη (user interface) των αποκεντρωμένων εφαρμογών δεν διαφέρει από οποιαδήποτε ιστοσελίδα ή εφαρμογή για κινητά σήμερα. Τα έξυπνα συμβόλαια αποτελούν στοιχειώδεις αποκεντρωμένες εφαρμογές σε ένα blockchain.

Αρκετά Καλό Απόρρητο (Pretty Good Privacy - PGP)

Πρόκειται για ένα πρόγραμμα κρυπτογράφησης το οποίο παρέχει απόρρητο κρυπτογράφησης και επαλήθευσης για την επικοινωνία δεδομένων. Ο Φιλ Ζίμερμαν ανέπτυξε το PGP το 1991.

Απόδειξη εργασίας (Proof-of-work)

Αλγόριθμος συναίνεσης, σύμφωνα με τον οποίο blocks δεδομένων συναλλαγών στο blockchain εξορύσσονται και επικυρώνονται από εξειδικευμένους υπολογιστές μέσα από την επίλυση μαθηματικών εξισώσεων.

Απόδειξη κυριότητας (Proof-of-stake)

Αλγόριθμος συναίνεσης που χρησιμοποιείται εναλλακτικά του proof-of-work σε πλατφόρμες blockchain για την εξόρυξη και επικύρωση blocks δεδομένων συναλλαγών. Δεν χρησιμοποιεί την επίλυση μαθηματικών εξισώσεων, αλλά επιτυγχάνεται με συνδυασμό άλλων κριτηρίων (όπως τον αριθμό των κρυπτονομισμάτων που έχει ο κόμβος που επαληθεύει το block). Η απόδειξη κυριότητας ενθαρρύνει τους ανθρώπους που έχουν στην ιδιοκτησία τους μια πλειάδα από blockchain tokens να λάβουν αποφάσεις για την επικύρωση της αλυσίδας. Προτιμάται ως μέθοδος έναντι του proof-of-work, αφού καταναλώνει λιγότερους πόρους (υπολογιστική ισχύ).

Χρηματική εγγύηση (Escrow)

Η χρηματική εγγύηση είναι μια οικονομική συμφωνία, σύμφωνα με την οποία ένα τρίτο μέλος αποταμιεύει και ρυθμίζει την πληρωμή των κεφαλαίων που απαιτείται από τα δύο μέλη που συμμετέχουν σε μια συγκεκριμένη συναλλαγή. Συντελεί στο να κάνει τις συναλλαγές πιο ασφαλείς, διατηρώντας την πληρωμή σ' έναν ασφαλή εγγυητικό λογαριασμό, ο οποίος αποδεσμεύεται μόνο όταν όλοι οι όροι της συμφωνίας έχουν τηρηθεί, υπό την επίβλεψη της εγγυήτριας εταιρείας.

Blockchain escrow services

Οι υπηρεσίες μεσεγγύησης (escrow services) είναι ένας από τους πιο αξιόπιστους τρόπους για να ξεπεραστούν αδυναμίες, όπως σημαντικές διακυμάνσεις στην αξία του κρυπτονομίσματος, στον χρόνο που χρειάζεται για να ολοκληρωθεί μια συναλλαγή. Οι υπηρεσίες Escrow εξασφαλίζουν ότι οι συναλλαγές εκτελούνται με ασφαλή και έγκαιρο τρόπο. Για παράδειγμα το Themis είναι ένα blockchain-based, έμπιστο και δίκαιο «ανταλλακτήριο» ψηφιακών κρυπτονομισμάτων, που παρέχει μια αποκεντρωμένη escrow service.

MultiChain

Η MultiChain είναι μια πλατφόρμα ανάπτυξης private Blockchains. Παρέχει ένα απλό API και command-line interface. Είναι open source και υποστηρίζει εκτός άλλων και την γλώσσα Python.

JSON file format

Ένα αρχείο JSON είναι ένα αρχείο που αποθηκεύει απλές δομές δεδομένων (data structures) και αντικείμενα (objects), στη μορφή JavaScript Notation Object (JSON), η οποία είναι μια τυπική μορφή ανταλλαγής δεδομένων. Χρησιμοποιείται κυρίως για τη μετάδοση δεδομένων μεταξύ μιας web application και ενός server. Το JSON χρησιμοποιείται συνήθως στον προγραμματισμό Ajax Web application αλλά και από την πλατφόρμα Multichain.

Εφοδιαστική Αλυσίδα (Supply Chain)

Με τον όρο Εφοδιαστική Αλυσίδα εννοούμε το δίκτυο όλων των ατόμων, των οργανισμών, των πόρων, των δραστηριοτήτων και της τεχνολογίας που εμπλέκονται στη δημιουργία και την πώληση ενός προϊόντος, από την παράδοση πρώτων υλών από τον προμηθευτή στον κατασκευαστή μέχρι την τελική του παράδοση στον τελικό χρήστη.

Διαχείριση Εφοδιαστικής Αλυσίδας (Supply Chain Management)

Ως διαχείριση μιας εφοδιαστικής αλυσίδας, εννοούμε την διαχείριση της ροής αγαθών και υπηρεσιών και περιλαμβάνει όλες τις διαδικασίες που μετατρέπουν τις πρώτες ύλες σε τελικά προϊόντα. Περιλαμβάνει τον ενεργό εξορθολογισμό των δραστηριοτήτων της επιχείρησης με στόχο την μεγιστοποίηση της αξίας των πελατών και την απόκτηση ανταγωνιστικού πλεονεκτήματος στην αγορά. Συχνά αναφέρεται και με τον όρο Logistics.

Ακαθάριστο Εγχώριο Προϊόν (ΑΕΠ)

Ως Ακαθάριστο Εγχώριο Προϊόν (Gross Domestic Product - GDP), εννοούμε το σύνολο των αγαθών και υπηρεσιών που παράγονται σε μια χώρα στην διάρκεια μιας ορισμένης χρονικής περιόδου (συνήθως αναφερόμαστε σε ετήσιο ΑΕΠ).

Σύμφωνα με τον Παγκόσμιο Γεωγραφικό Άτλαντα, το ΑΕΠ το διακρίνουμε σε τρεις παραγωγικούς τομείς: τον πρωτογενή, τον δευτερογενή και τον τριτογενή. Ο πρωτογενής περιλαμβάνει την παραγωγή αγαθών απευθείας από τη φύση (γεωργία, κτηνοτροφία, αλιεία), ο δευτερογενής περιλαμβάνει την παραγωγή αγαθών τα οποία έχουν προέλθει από την επεξεργασία ακατέργαστων ή μέτρια επεξεργασμένων υλικών και ο τριτογενής τομέας αφορά δραστηριότητες που παρέχουν υπηρεσίες στο κοινωνικό σύνολο, χωρίς να παράγεται κάποιο υλικό προϊόν.

Διατροφικός Τομέας

Αναφέρεται στη μεταποίηση, αποθήκευση/διατήρηση, διανομή/διάθεση και παροχή τροφίμων και ποτών.

Αγροδιατροφικός τομέας (agrifood/agriculture and food sector)

Όταν οι άνθρωποι ακούνε τους όρους αγροτική παραγωγή (agriculture) ή τρόφιμα (food), σκέφτονται συνήθως τη γεωργία ή την κτηνοτροφία. Ο όρος «αγροδιατροφικός τομέας» είναι πιο σύνθετος. Σύμφωνα με την Agriculture and Agri-Food Canada, βλ. σχετικά [67], το «σύστημα γεωργικών προϊόντων διατροφής περιλαμβάνει διάφορες βιομηχανίες, συμπεριλαμβανομένων των κλάδων παραγωγής γεωργικών πρώτων υλών και προμηθευτών, πρωτογενούς γεωργίας, επεξεργασίας τροφίμων και ποτών, διανομής τροφίμων, λιανικής, χονδρικής και βιομηχανίας τροφίμων». Επομένως ο όρος «αγροδιατροφικός τομέας», αντιπροσωπεύει μια ολιστική άποψη όλων παραπάνω δραστηριοτήτων. Οι βασικές όμως δραστηριότητες περιλαμβάνουν:

- Φυτικές καλλιέργειες (συμπεριλαμβάνονται καλλιέργειες για καύσιμα όπως αιθανόλη, για ίνες όπως βαμβάκι, καλλιέργειες για λουλούδια κλπ).
- Αλιεία και οι ζωική παραγωγή (συμπεριλαμβάνεται η εκτροφή ζώων για μαλλί ή γούνα, η μελισσοκομία, τα ιχθυοτροφεία κλπ).
- Μεταποίηση τροφίμων (πχ εταιρείες που επεξεργάζονται και συσκευάζουν προϊόντα διατροφής).
- Διανομή τροφίμων και ποτών (πχ εφοδιαστικές αλυσίδες, καταστήματα τροφίμων, οι αγορές κρέατος, αγορές φρούτων και λαχανικών).

ΜΕΘΟΔΟΛΟΓΙΑ

Σύμφωνα με τους Jansson και Petersen (2017), βλ. σχετικά [38], προκειμένου μια επιχείρηση να κάνει την μετάβαση στην Τεχνολογία Blockchain, θα πρέπει να προχωρήσει στις παρακάτω προτεινόμενες ενέργειες:

- Identify problem (να αναγνωρίσει, αξιολογήσει το επιχειρηματικό πρόβλημα και τι θέλει να βελτιώσει με την χρήση της νέας τεχνολογίας).
- Check if Blockchain solution applies to problem (να δει αν η τεχνολογία BlockChain έχει εφαρμογή στην περίπτωση του).

- Create a draft application using appropriate platform (να προχωρήσει στην σχεδίαση μιας πιλοτικής εφαρμογής επιλέγοντας κατάλληλη πλατφόρμα υλοποίησης).
- Evaluate application suitability and applicability (μετά την υλοποίηση της εφαρμογής και την πιλοτική της χρήση, να προχωρήσει σε αξιολόγηση της).

Θα εφαρμόσουμε την παραπάνω μεθοδολογία στην εργασία, δηλαδή:

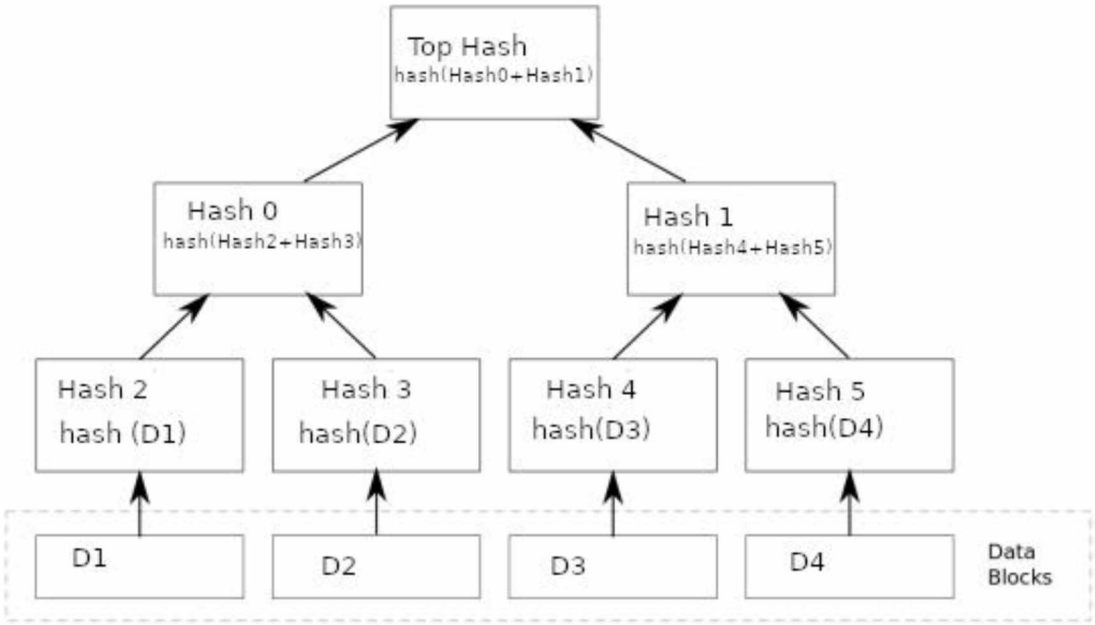
- Θα δούμε τα βασικά χαρακτηριστικά της τεχνολογίας blockchain.
- Θα εξετάσουμε τα προβλήματα που υπάρχουν στον αγροδιατροφικό τομέα και τι θέλουμε να επιλύσουμε με χρήση αυτής της τεχνολογίας.
- Θα εξετάσουμε υπάρχουσες πλατφόρμες blockchain και πως θα μπορούσαμε να σχεδιάσουμε μια πιλοτική εφαρμογή για το πρόβλημα.
- Θα αξιολογήσουμε τα παραπάνω και θα διατυπώσουμε συμπεράσματα.

ΚΕΦΑΛΑΙΟ 2 - ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

Σύντομη ιστορική αναδρομή

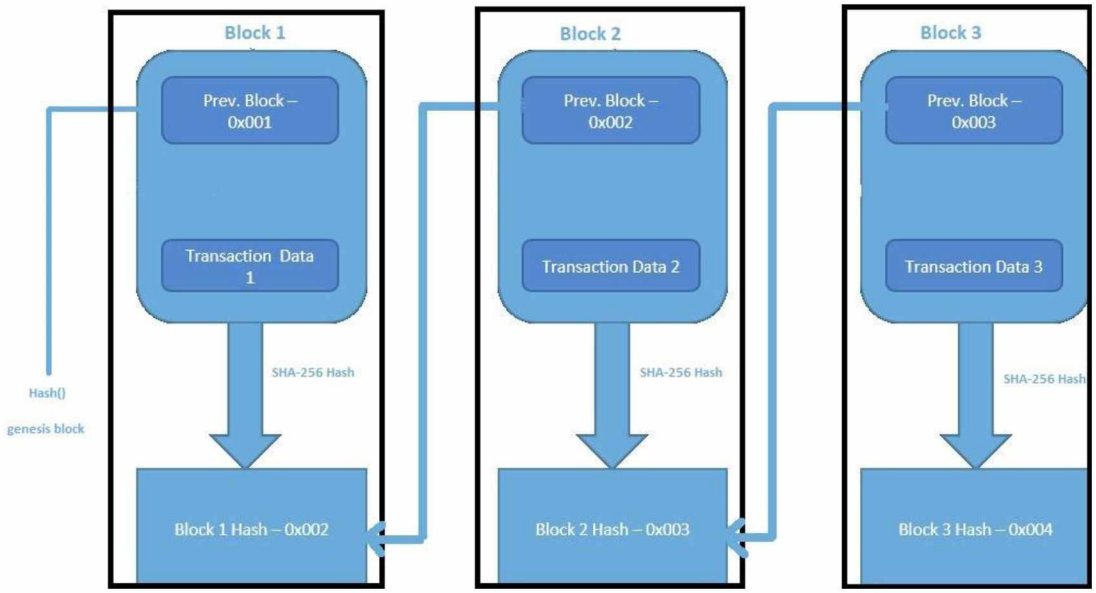
Όπως εξηγήσαμε περιληπτικά στο προηγούμενο κεφάλαιο, το blockchain (αλυσίδα συστοιχιών), είναι ένα distributed ledger, στο οποίο αποθηκεύονται κι επαληθεύονται πληροφορίες και δεδομένα διάφορων συναλλαγών, με χρήση κρυπτογραφικών μεθόδων. Τα δεδομένα των συναλλαγών, ομαδοποιούνται σε συστοιχίες (blocks) και φέρουν χρονοσήμανση. Τα blocks συνδέονται μεταξύ τους με χρονολογική σειρά δημιουργώντας μια αλυσίδα (chain). Τα δεδομένα των συναλλαγών που έχουν καταγραφεί στο blockchain είναι αναλλοίωτα (immutable), αφού κάθε τροποποίηση τους, επηρεάζει αναγκαστικά όλες τις μεταγενέστερες καταγραφές.

Σύμφωνα με το Wikipedia, βλ. σχετικά [6], η πολύ πρωτόγονη μορφή του blockchain ήταν το δέντρο κατακερματισμού ή αλλιώς δέντρο Merkle (hash tree). Αυτή η δομή δεδομένων προτάθηκε από τον Ralph Merkle το 1979 με σκοπό την επαλήθευση και τη διαχείριση δεδομένων μεταξύ συστημάτων ηλεκτρονικών υπολογιστών. Σε ένα δίκτυο ομότιμων κόμβων (υπολογιστών), που κάθε κόμβος συνδέεται και επικοινωνεί με τους υπόλοιπους, είναι σημαντικό να γνωρίζουμε ότι τα δεδομένα δεν χάθηκαν ή αλλοιώθηκαν κατά τη μεταφορά τους από κόμβο σε κόμβο. Το hash tree χρησιμοποιείται για να διατηρήσει και να αποδείξει (επικυρώσει) την ακεραιότητα των διαμοιραζόμενων δεδομένων. Σε ένα hash tree, κάθε κόμβος έχει μια τιμή Hash, που προκύπτει από το Hash των παιδιών του, ενώ στα φύλλα του δέντρου αποθηκεύονται τα δεδομένα (data blocks).



Εικόνα 2.1 - Binary hash tree

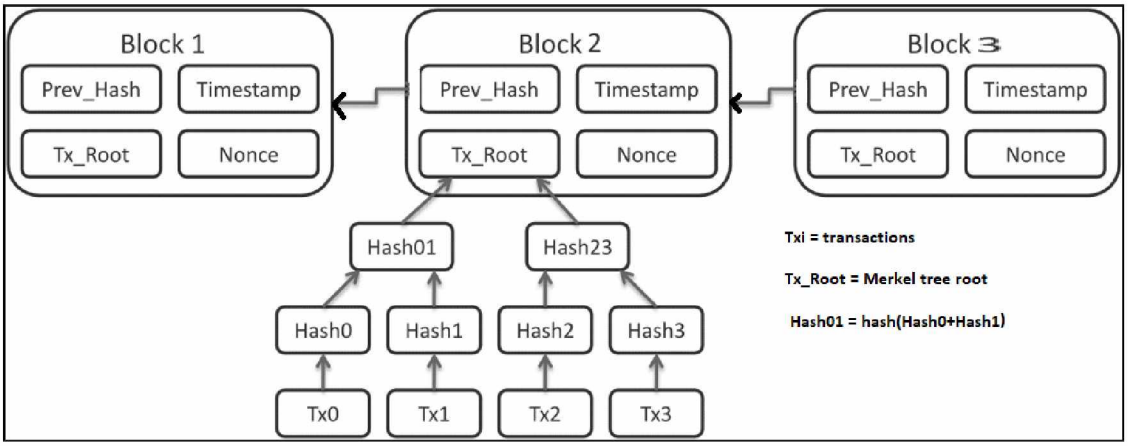
Το 1991, το δέντρο Merkle χρησιμοποιήθηκε για να δημιουργήσει μια μια συνδεδεμένη λίστα (linked list) από αρχεία δεδομένων (data blocks), καθένα από τα οποία συνδέεται με το προηγούμενο μέσω ενός δείκτη (pointer), δημιουργώντας έτσι μια αλυσίδα από blocks.



Εικόνα 2.2 - linked list using hash pointer

Ο δείκτης όμως στο προηγούμενο block, αντί να περιέχει μόνο τη διεύθυνση του προηγούμενου block περιέχει επίσης το Hash των δεδομένων μέσα στο προηγούμενο block. Με αυτό τον τρόπο, η συνδεδεμένη λίστα από data blocks, περιέχει την ιστορία ολόκληρης της αλυσίδας. Το πρώτο block ονομάζεται "genesis block" και ο δείκτης σε αυτό δημιουργείται αυτόματα από την πλατφόρμα του blockchain.

Το 2008, ο Satoshi Nakamato είχε την ιδέα του κατανεμημένου blockchain, το οποίο θα περιλάμβανε ένα ασφαλές ιστορικό ανταλλαγής δεδομένων, θα χρησιμοποιούσε ένα δίκτυο peer-to-peer για τη χρονική σφράγιση (time stamp) και την επαλήθευση κάθε ανταλλαγής και θα μπορούσε να το διαχειριστεί αυτόνομα χωρίς κεντρική αρχή. Αυτό έγινε η ραχοκοκαλιά του Bitcoin που ήταν και η πρώτη εμπορική εφαρμογή της τεχνολογίας blockchain.



Εικόνα 2.3 - Δομή του Bitcoin

Τα blocks κρυπτογραφούνται (και υπογράφονται ψηφιακά) με χρήση του αλγορίθμου SHA-256 που είδαμε στο προηγούμενο κεφάλαιο, με τρόπο μη αναστρέψιμο (one way encryption), δίνοντας πάντα ένα κρυπτογραφημένο αποτέλεσμα (hash value) σταθερού μεγέθους (32-byte), άσχετα από το μέγεθος των δεδομένων που καταχωρούμε.

Κάθε block περιέχει το Hash και τα δεδομένα των έγκυρων συναλλαγών (transactions). Κάθε block ελέγχεται και επικυρώνεται από τους υπόλοιπους κόμβους που συμμετέχουν στο blockchain, σύμφωνα με πρωτόκολλα. Το Hash του κάθε block είναι μοναδικό και επιτρέπει την σύνδεση των blocks μεταξύ τους, με τρόπο που διατηρεί την χρονική αλληλουχία της αλυσίδας. Έτσι εξασφαλίζεται η ασφάλεια των δεδομένων

αφού εμποδίζεται η αλλοίωση ή η διαγραφή τους, καθώς και η παρεμβολή άλλου block μεταξύ δύο συνδεδεμένων blocks.

Η αλλοίωση των δεδομένων ενός κόμβου στο blockchain είναι αδύνατη, καθώς δεν θα μπορούσε να επιβεβαιωθεί (κρυπτογραφικά) από τους υπόλοιπους κόμβους, αφού θα υπήρχε ασυμφωνία μεταξύ δεδομένων και hashes. Κατά την εισαγωγή νέων blocks, επαληθεύονται όλα τα προηγούμενα blocks της αλυσίδας (σε όλους τους κόμβους ενημέρωσης) και επομένως αυτή η διαδικασία είναι σημαντική για την διατήρηση της ασφάλειας της αλυσίδας.

Τύποι Blockchain

Ένα blockchain μπορεί να είναι δημόσια (Public), ιδιωτική (Private) ή υβριδική (Hybrid-Permissioned).

Κοινά χαρακτηριστικά όλων των τύπων:

- Τόσο τα δημόσια όσο και τα ιδιωτικά blockchains έχουν αποκεντρωμένα δίκτυα .
- Όλοι οι συμμετέχοντες στο δίκτυο διατηρούν μαζί τους το αντίγραφο του κοινόχρηστου καθολικού (distributed ledger).
- Το δίκτυο διατηρεί αντίγραφα του distributed ledger και συγχρονίζει την τελευταία ενημέρωση με τη βοήθεια συναίνεσης (consesus).
- Οι κανόνες για τη μετατόπιση και την ασφάλεια του distributed ledger αποφασίζονται και εφαρμόζονται στο δίκτυο, ώστε να αποφεύγονται οι κακόβουλες επιθέσεις.

Δημόσιο (Public) blockchain

Όπως υποδηλώνει το όνομα, ένα δημόσιο Blockchain είναι ένα μητρώο (ledger) χωρίς να απαιτεί άδεια πρόσβασης, οπότε είναι προσβάσιμο από οποιονδήποτε. Οποιοσδήποτε με πρόσβαση στο Διαδίκτυο έχει δικαίωμα λήψης και πρόσβασης σε αυτό. Επιπλέον, μπορείτε επίσης να ελέγξετε τη συνολική ιστορία του blockchain μαζί με τις συναλλαγές μέσω αυτού.

Τα δημόσια Blockchains όπως είναι για παράδειγμα το Bitcoin και το Ethereum είναι μεγαλύτερα, όσον αφορά τον αριθμό των κόμβων. Ο κάθε χρήστης (node) είναι

ανώνυμος (anonymous), έχει πρόσβαση στο distributed ledger και έχει ένα αντίγραφο αυτού, ενώ μπορεί να συμμετέχει σαν απλός χρήστης, διενεργώντας συναλλαγές, ή να συμμετέχει στην επαλήθευση και επικύρωση των συναλλαγών λαμβάνοντας μια αμοιβή (mining).

Τα δημόσια Blockchains δεν ελέγχονται από κάποια κεντρική αρχή, η συμμετοχή είναι ανώνυμη και θεωρούνται πιο ασφαλή. Ο κώδικας αναπτύσσεται από την κοινότητα του κάθε Blockchain δικτύου, από εθελοντές προγραμματιστές (developers) και είναι κατά κανόνα open source.

Εξετάζοντας τα μειονεκτήματα των δημόσιων Blockchains, όπως είναι το Bitcoin, θα μπορούσαμε να αναφέρουμε ότι απαιτούν μεγάλη υπολογιστική ισχύ, είναι ενεργοβόρα και λόγου μεγέθους και αυξανόμενου όγκου συναλλαγών είναι συχνά πιο αργά ενώ απαιτούν και πολύ αποθηκευτικό χώρο.

Ιδιωτικό (Private) Blockchain

Σε αντίθεση με τα δημόσια, τα ιδιωτικά Blockchains, το ledger διαμοιράζεται μόνο μεταξύ των έμπιστων συμμετεχόντων και με αυτή την έννοια δεν είναι δημόσιο αλλά ιδιωτικό. Οι κόμβοι δεν είναι ανώνυμοι, αλλά γνωστοί και έμπιστοι. Ο συνολικός έλεγχος του δικτύου ανήκει σε μια κεντρική έμπιστη αρχή.

Οι κανόνες ενός ιδιωτικού Blockchain μπορούν να τροποποιούνται ανάλογα με τα διαφορετικά επίπεδα δικαιωμάτων, την έκθεση, τον αριθμό των μελών, την εξουσιοδότηση κ.λ.π.

Τα ιδιωτικά blockchains μπορούν να λειτουργούν ανεξάρτητα ή μπορούν να ενσωματωθούν σε άλλα blockchains. Χρησιμοποιούνται συνήθως από επιχειρήσεις και οργανισμούς. Το επίπεδο εμπιστοσύνης που απαιτείται μεταξύ των συμμετεχόντων, είναι υψηλότερο σε ιδιωτικά Blockchains.

Τα ιδιωτικά Blockchains είναι μικρότερα, όσον αφορά τον αριθμό των κόμβων, σε σχέση με τα δημόσια. Το δίκτυο είναι ελεγχόμενο από μια κεντρική αρχή, που αποφασίζει για το ποιος έχει πρόσβαση σε αυτό καθώς και τα δικαιώματα πρόσβασης.

Είναι πιο γρήγορα από τα δημόσια blockchain και λόγου μεγέθους, αλλά και λόγου του γεγονότος ότι η επικύρωση των δεδομένων γίνεται πιο γρήγορα (γίνεται χρήση διαφορετικών πρωτοκόλλων). Επιπλέον απαιτούν μικρότερη υπολογιστική ισχύ και επομένως είναι λιγότερο ενεργοβόρα. Μπορούν να υλοποιηθούν σε πολύ σύντομο χρονικό διάστημα, ενώ πιθανά το δίκτυο υποστηρίζεται και αναπτύσσεται από εταιρείες ή οργανισμούς. Σύμφωνα με τον Gupta (2017), βλ. σχετικά [9], πολλά ιδιωτικά Blockchains δεν χρησιμοποιούν κρυπτονόμισμα και είναι λιγότερο ασφαλή από ένα δημόσιο Blockchain δίκτυο.

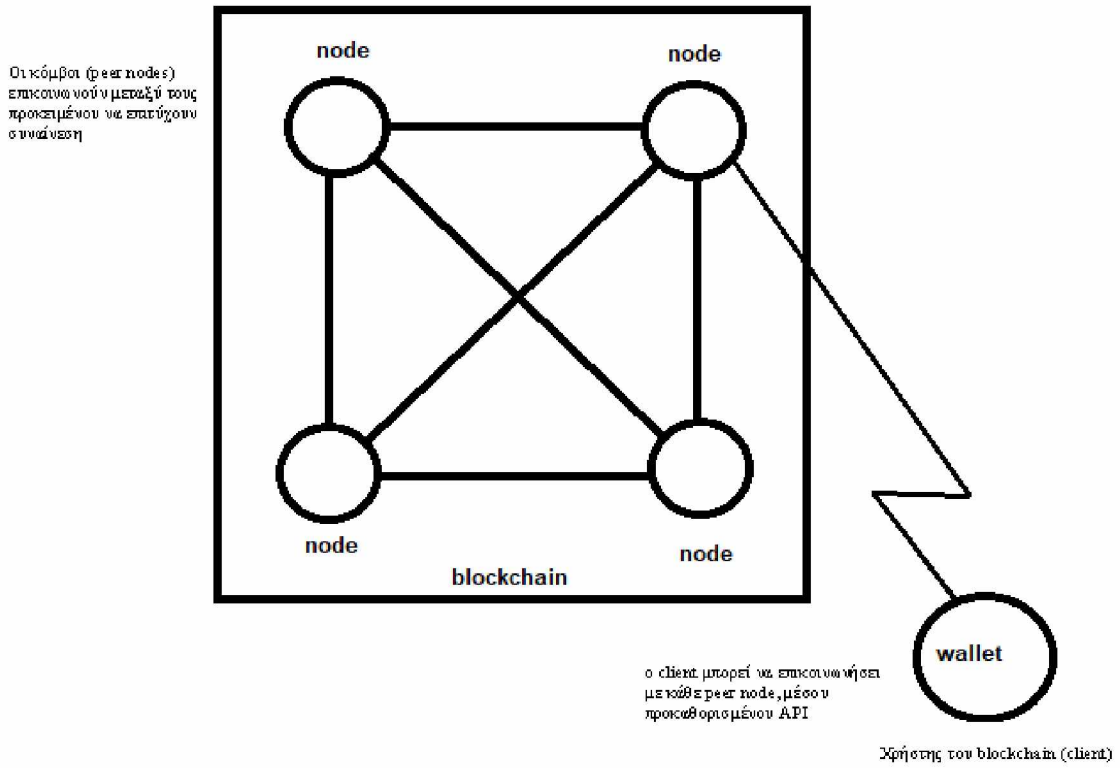
Υβριδικό (Hybrid - Permissioned - Federated - Consortium) Blockchain

Το υβριδικό Blockchain, δανείζεται κάποια χαρακτηριστικά και από το δημόσιο και από το ιδιωτικό. Υπάρχει ένα κοινόχρηστο διαμοιραζόμενο ledger, όμως η πρόσβαση σε αυτό ελέγχεται από μια έμπιστη κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και εξουσιοδοτεί (permission) σε έμπιστα προς αυτούς άτομα (primary nodes), το δικαίωμα επικύρωσης των συναλλαγών.

Βέβαια, η ύπαρξη κεντρικής αρχής ή η προϋπόθεση ύπαρξης έμπιστων κόμβων, στα ιδιωτικά και υβριδικά blockchains, αναιρεί την κεντρική ιδέα και την "επαναστατικότητα" της νέας τεχνολογίας, δηλαδή την πρόσβαση όλων των χρηστών του blockchain σε ένα πραγματικά δημόσιο και ανοικτό μητρώο δεδομένων και πληροφοριών, καθώς και την εμπέδωση της εμπιστοσύνης μεταξύ των συμμετεχόντων χρηστών χωρίς την ύπαρξη μίας έμπιστης κεντρικής αρχής που ελέγχει, επικυρώνει και αποθηκεύει το ledger.

Αρχιτεκτονική του blockchain

Γενικά, ένα σύστημα blockchain αποτελείται από έναν αριθμό κόμβων, καθένα από τα οποία έχει ένα τοπικό αντίγραφο ενός κατανεμημένου μητρώου (distributed ledger). Στα περισσότερα συστήματα, οι κόμβοι ανήκουν σε διαφορετικούς χρήστες. Οι κόμβοι επικοινωνούν μεταξύ τους προκειμένου να επιτευχθεί συμφωνία σχετικά με το περιεχόμενο.



Εικόνα 2.4 - Αρχιτεκτονική δικτύου blockchain

Η διαδικασία επίτευξης αυτής της συμφωνίας ονομάζεται συναίνεση (consensus) και γίνεται με χρήση κατάλληλων αλγορίθμων που θα δούμε παρακάτω.

Οι χρήστες στέλνουν αιτήσεις συναλλαγών στο blockchain προκειμένου να εκτελέσουν τις λειτουργίες που έχουν σχεδιαστεί για την παροχή της αλυσίδας. Μόλις ολοκληρωθεί μια συναλλαγή, μια εγγραφή της συναλλαγής προστίθεται σε ένα ή περισσότερα από τα block και δεν μπορεί ποτέ να μεταβληθεί ή να αφαιρεθεί.

Σε ένα δημόσιο blockchain, αρμόδιοι για τον έλεγχο και την τήρησή του ledger είναι οι ομότιμοι κόμβοι (peer nodes), δηλαδή χρήστες οι οποίοι, έχουν το απαιτούμενο λογισμικό και ενημερώνουν ταυτόχρονα, το μητρώο (ledger) για τις αλλαγές σε αυτό. Οι peer nodes διατηρούν πανομοιότυπα αντίγραφα του μητρώου, αφού συμφωνήσουν ως προς την τρέχουσα κατάσταση του. Με την επίτευξη συναίνεσης (consensus) ανάμεσα στους peer nodes, τα δεδομένα που καταγράφονται στο μητρώο θεωρούνται έμπιστα και σωστά. Μάλιστα, όσο περισσότεροι είναι οι peer nodes, που συμμετέχουν στην διαδικασία τόσο αυξάνει ο έλεγχος και η ασφάλεια των δεδομένων του μητρώου. Οι peer nodes που συμμετέχουν σε αυτή την διαδικασία επικύρωσης και τήρησης του

μητρώου ονομάζονται miners και αμείβονται, προκειμένου να υπάρχει κίνητρο για την συμμετοχή τους στην ανάπτυξη και λειτουργία του blockchain.

Ο τρόπος καταχώρησης των δεδομένων στο μητρώο, ο τρόπος επαλήθευσης και επικύρωσης τους καθώς και το τι είδους δεδομένα καταχωρούνται, καθορίζονται από τα πρωτόκολλα και το λογισμικό της κάθε πλατφόρμας blockchain. Επίσης μια πλατφόρμα blockchain ορίζει και το κρυπτονόμισμα ή tokens που υποστηρίζει.

Σύμφωνα με τον Σταμπέρνα (2018), βλ.σχετικά [13], σε κάθε πλατφόρμα Blockchain θα μπορούσαμε να διακρίνουμε τα παρακάτω δομικά στοιχεία:

- το block (Block),
- την αλυσίδα (Chain),
- τις ψηφιακές υπογραφές (Digital Signatures) και κρυπτογράφηση,
- το Peer-to-Peer δίκτυο
- τον έμπιστο μηχανισμό (Consensus Protocols).

Δομή του Block και φύση των δεδομένων

Όπως είδαμε και σε προηγούμενες ενότητες, τα blocks εκτός από τα δεδομένα των συναλλαγών (transactional data) περιέχουν κι άλλα δεδομένα (metadata) που εγγυώνται την απρόσκοπτη λειτουργία ενός blockchain σύμφωνα με τα πρωτόκολλα του δικτύου. Τα δεδομένα των συναλλαγών έχουν εννοιολογικό περιεχόμενο, το οποίο εξαρτάται από την εφαρμογή του συγκεκριμένου blockchain. Έτσι στην περίπτωση του Bitcoin τα δεδομένα αυτά περιγράφουν την κατάσταση ενός από κοινού τραπεζικού χαρτοφυλακίου, ενώ σε μια εφαρμογή blockchain για ηλεκτρονική ψηφοφορία και καταμέτρηση ψήφων, τα δεδομένα αφορούν ένα εκλογικό αποτέλεσμα, βλ. σχετικά [6]. Όπως ήδη έχουμε αναφέρει στο blockchain χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης SHA-256, για την κρυπτογράφηση των δεδομένων.

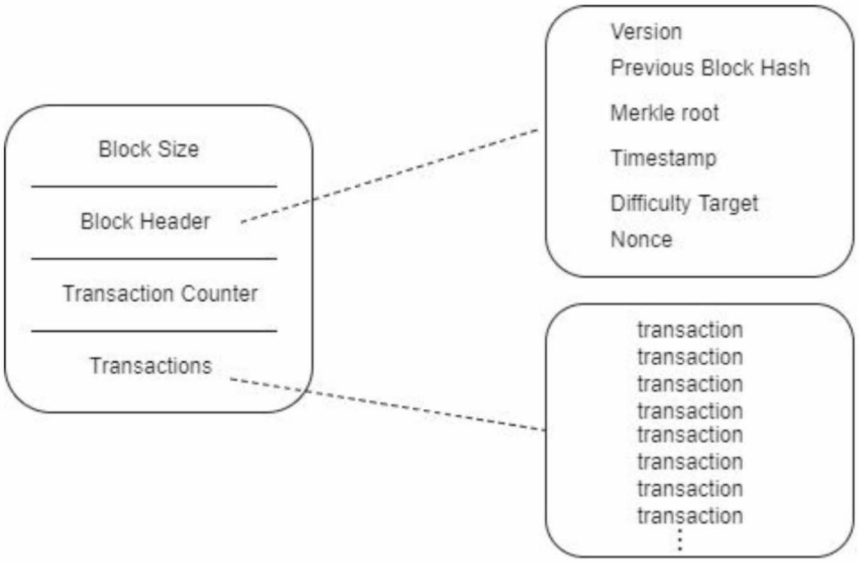
Η δομή του block μπορεί να διαφέρει ανάλογα με την πλατφόρμα του Blockchain. Ας δούμε για παράδειγμα την δομή ενός Bitcoin block.

Ένα Bitcoin block αποτελείται από την κεφαλίδα (header) και το κυρίως σώμα (body).

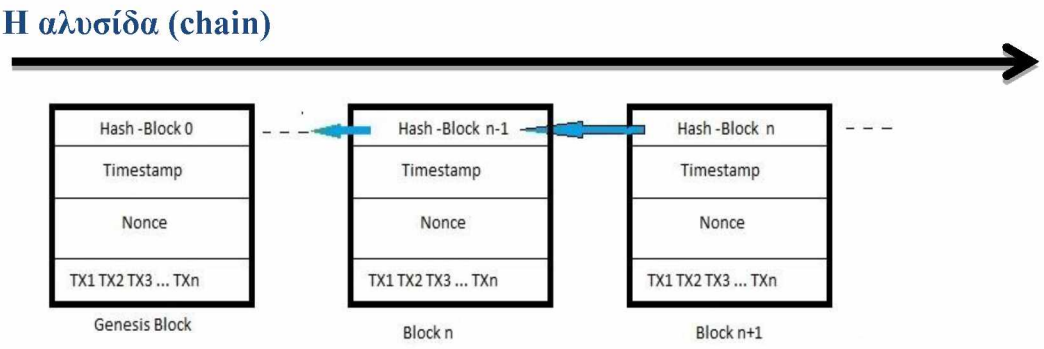
Το block header περιλαμβάνει την παρακάτω πληροφορία:

- Block version: δείχνει ποιό σύνολο πρωτοκόλλων επικύρωσης (set of block validation rules) ακολουθούμε.
- Parent block hash: είναι η 256-bit hash value που δείχνει στο προηγούμενο block (parent/previous block).
- Merkle tree root hash: η hash value όλων των transactions στο block.
- Timestamp: (current timestamp as seconds since 1970-01-01T00:00 UTC).
- Difficulty target - find a hash below given target.
- nBits: current hashing target in compact format.
- Nonce: used in proof-of-work systems to vary the input to a cryptographic hash function (4-byte πεδίο, συνήθως ξεκινά από 0 και αυξάνεται με κάθε hash)

Το block body αποτελείται από το transaction counter και την transactions list.



Εικόνα 2.5 - Bitcoin block structure



Εικόνα 2.6 - αλυσίδα από blocks

Την έννοια της αλυσίδας (chain) και πως αυτή σχηματίζεται την είδαμε και σε προηγούμενη ενότητα, θα πούμε ότι και πάλι ότι «*η δομή των δεδομένων στο Blockchain είναι μια ταξινομημένη λίστα από block συνδεδεμένη προς τα πίσω*», βλ. σχετικά [1], [10]. Αυτή η ταξινόμηση των block σχηματίζει τελικά την αλυσίδα.

Όπως προαναφέρθηκε, στα δεδομένα του Block Header υπάρχει το hash του προηγούμενου Block, άρα έχουμε ένα δείκτη στο προηγούμενο block συνδέοντας έτσι το τρέχον block με το προηγούμενο στο Blockchain. Ο δείκτης όμως στο προηγούμενο block, αντί να περιέχει μόνο τη διεύθυνση του προηγούμενου block περιέχει επίσης το Hash των δεδομένων μέσα στο προηγούμενο block, οπότε εμπεριέχεται όλο το ιστορικό της αλυσίδας. Σύμφωνα με το Laurence (2017),βλ. σχετικά [8], μπορούμε να πούμε ότι, *«το Hash είναι η μαγική κόλλα που ενώνει τα block μεταξύ τους και επιτρέπει εμπιστοσύνη με μαθηματική ακρίβεια»*.

Ψηφιακή υπογραφή (Digital Signature) και κρυπτογράφηση

Η διενέργεια μιας συναλλαγής στο Blockchain απαιτεί την χρήση ψηφιακής υπογραφής, προκειμένου να ελεγχθεί αν είναι έγκυρη. Όπως έχουμε αναφέρει και σε προηγούμενη ενότητα, στην ψηφιακή υπογραφή μηνυμάτων ή δεδομένων. κάθε χρήστης χρησιμοποιεί ένα ζευγάρι κλειδιών, ένα ιδιωτικό (private) και ένα δημόσιο (public).

- Το ιδιωτικό κλειδί, το οποίο γνωρίζει μόνο ο χρήστης χρησιμοποιείται για τη δημιουργία της ψηφιακής υπογραφής και την κρυπτογράφηση των δεδομένων.
- Το δημόσιο κλειδί, είναι ορατό προς όλους και χρησιμοποιείται για την επαλήθευση και την αποκρυπτογράφηση των δεδομένων.

Μια συναλλαγή μεταξύ δύο χρηστών, έστω χρήστης Α και Β, σε ένα blockchain διακρίνεται στην φάση της υπογραφής (sign) και την φάση της επαλήθευσης (verification), σύμφωνα με τα παρακάτω.

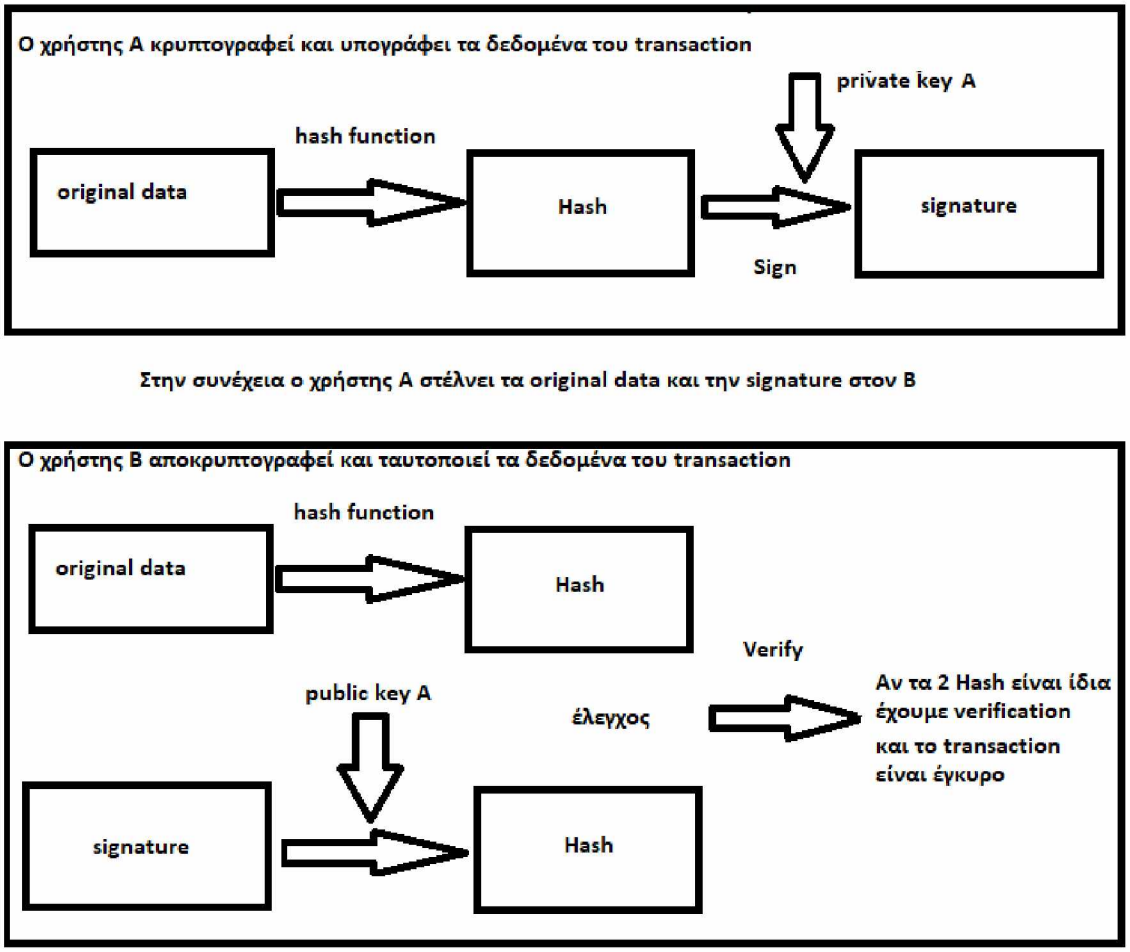
Έστω ότι ο χρήστης Α ξεκινά μια συναλλαγή, κοινοποιώντας δεδομένα στον χρήστη Β. Θα πρέπει να κάνει τα παρακάτω:

I. Αρχικά δημιουργεί ένα Hash από τα δεδομένα της συναλλαγής χρησιμοποιώντας αλγόριθμο κρυπτογράφησης (SHA-256).
II. Έπειτα δημιουργεί μια ψηφιακή υπογραφή αφού κρυπτογραφήσει την τιμή Hash χρησιμοποιώντας το ιδιωτικό κλειδί του χρήστη Α.
III. Τέλος, στέλνει στον χρήστη Β την ψηφιακή υπογραφή μαζί με τα αρχικά δεδομένα της συναλλαγής.

Ο χρήστης Β έχει τώρα στην κατοχή του τα δεδομένα της συναλλαγής και την ψηφιακή υπογραφή του χρήστη Α. Για να ελέγξει την εγκυρότητα της συναλλαγής ο χρήστης Β κάνει τα παρακάτω:

I. Αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του χρήστη Α για να ανακτήσει το Hash.
II. Δημιουργεί ένα 2ο Hash από τα δεδομένα που του έχουνε σταλεί.

Αν αυτά τα 2 Hash είναι ίδια τότε η συναλλαγή είναι έγκυρη.



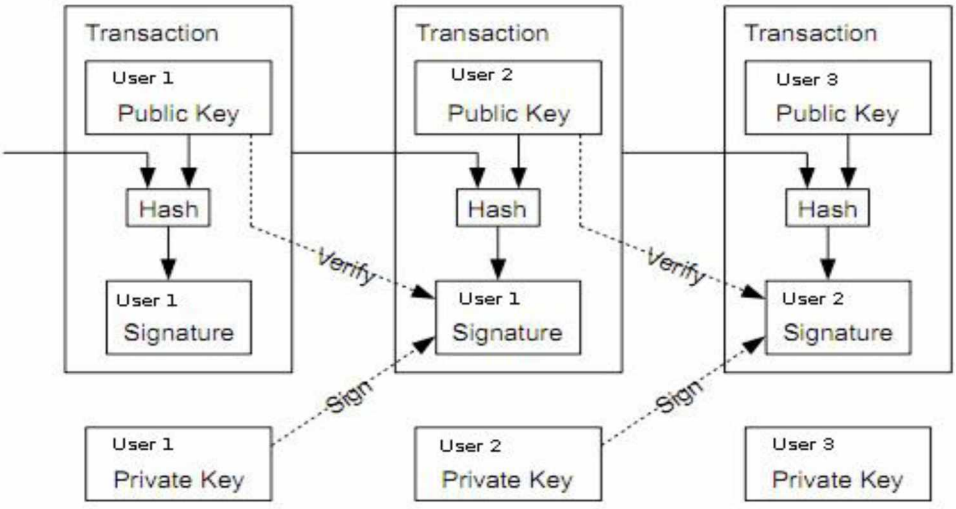
Εικόνα 2.7 - Ψηφιακή υπογραφή και κρυπτογράφηση

Ας δούμε πιο αναλυτικά τις παραπάνω λειτουργίες, έχοντας υπόψη μας και τα όσα αναφέρθηκαν σχετικά με την αρχιτεκτονική του Blockchain.

Με ένα σύνολο κρυπτογραφικών κλειδιών, έχετε μια μοναδική ταυτότητα, βλ. σχετικά [26]. Το δημόσιο κλειδί είναι το πώς οι άλλοι μπορούν να σας εντοπίσουν. Το ιδιωτικό κλειδί σας δίνει τη δυνατότητα ψηφιακής υπογραφής και έγκρισης διαφορετικών ενεργειών για λογαριασμό αυτής της ψηφιακής ταυτότητας, όταν χρησιμοποιείται με το δημόσιο κλειδί σας. Είναι σημαντικό να διατηρήσετε το ιδιωτικό κλειδί σας ασφαλές, αφού οποιοσδήποτε έχει το ιδιωτικό κλειδί σας, μπορεί να το χρησιμοποιήσει για να αποκτήσει πρόσβαση σε οποιοδήποτε από τα ψηφιακά σας στοιχεία που σχετίζονται με το δημόσιο κλειδί σας και να κάνει ό, τι θέλει με αυτό. Το δημόσιο κλειδί αντιπροσωπεύει τη διεύθυνση του πορτοφολιού σας και το ιδιωτικό σας κλειδί είναι αυτό που χρησιμοποιείται για συναλλαγές της ψηφιακής ιδιοκτησίας σας (digital assets). Η ανωνυμία των cryptocurrencies προέρχεται από το γεγονός ότι

το δημόσιο κλειδί είναι απλώς μια τυχαία ακολουθία αριθμών. Ένα δημόσιο κλειδί δεν λέει την πραγματική ταυτότητα του ατόμου πίσω από αυτό. Κάθε φορά που πραγματοποιείται μια συναλλαγή μεταξύ δύο χρηστών A και B, η συναλλαγή αυτή υπογράφεται από όποιον την εξουσιοδοτεί. Η συναλλαγή αυτή, θα περιλαμβάνει τη διεύθυνση του παραλήπτη B (δημόσιο κλειδί) και θα υπογραφεί με ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί και το ιδιωτικό κλειδί του αποστολέα A. Αυτή η συναλλαγή προστίθεται στο ledger του Blockchain, θα περιλαμβάνει επίσης ένα timestamp και ένα μοναδικό αναγνωριστικό.

Όταν πραγματοποιηθεί αυτή η συναλλαγή, μεταδίδεται σε δίκτυο ομότιμων κόμβων - που αναγνωρίζουν ότι αυτή η συναλλαγή έχει συμβεί και την προσθέτουν στο αντίγραφο του ledger που διατηρούν. Κάθε συναλλαγή του ledger θα έχει τα ίδια δεδομένα: ψηφιακή υπογραφή, δημόσιο κλειδί, σφραγίδα χρόνου και μοναδικό αναγνωριστικό.



Εικόνα 2.8 - Ψηφιακή υπογραφή και κρυπτογράφηση σε Bitcoin transactions

Το δίκτυο

Ένα blockchain αποτελείται από ένα δίκτυο ομότιμων κόμβων, οπότε θα λέγαμε ότι από πλευράς δικτύου ανήκει στην κατηγορία των P2P δικτύων. Το δίκτυο είναι αποκεντρωμένο (decentralized) και κατανεμημένο (distributed). Δεν υπάρχει ιεραρχία

μεταξύ των κόμβων, με την έννοια ότι οι συμμετέχοντες στο δίκτυο είναι ισότιμοι, αναφορικά με οποιαδήποτε διαδικασία εκλογής ή/και επιλογής μεταξύ αυτών.

Όλα οι κόμβοι του δικτύου blockchain, δημιουργούν, ενημερώνουν και διαμοιράζονται ένα αρχείο (distributed ledger), χωρίς να απαιτείται εμπιστοσύνη μεταξύ τους ή η ύπαρξη κάποιας έμπιστης κεντρικής αρχής, όσον αφορά τα διαμοιραζόμενα δεδομένα. Το distributed ledger δημιουργείται, αντιγράφεται, αποθηκεύεται και ενημερώνεται σε κάθε κόμβο χωριστά, με τη χρήση πρωτοκόλλων συναίνεσης (Consensus Protocols).

Τα P2P δίκτυα είναι κατάλληλα για real-time και concurrent εφαρμογές πχ ο έλεγχος των συστημάτων ενός αεροπλάνου απαιτεί ένα P2P δίκτυο επεξεργαστών (κόμβοι του δικτύου), που λαμβάνουν ταυτόχρονα (concurrent) δεδομένα από πολλούς αισθητήρες (sensors), σε πραγματικό χρόνο (real-time), ενώ υπάρχει πάντα ο κίνδυνος απώλειας ή αλλοίωσης των δεδομένων αυτών (πχ ένας αισθητήρας να δυσλειτουργεί ή βγει εκτός δικτύου).

Σύμφωνα με τον Lamport (1978), βλ. σχετικά [77], σε ένα κατανεμημένο σύστημα διακρίνουμε 3 βασικά χαρακτηριστικά:

- Τα επιμέρους μέρη του συστήματος επεξεργάζονται δεδομένα του συστήματος ταυτόχρονα.
- Κάθε κόμβος του συστήματος έχει δικό του χρονισμό (δεν υπάρχει κεντρικός συγχρονισμός).
- Τα πρωτόκολλα του συστήματος εξασφαλίζουν την σωστή λειτουργία και επικοινωνία των επιμέρους μερών του συστήματος.

Ένα κατανεμημένο σύστημα, όπως είναι και ένα P2P δίκτυο, θεωρείται ότι λειτουργεί «σωστά», αν τα επιμέρους μέρη του «συναινούν» ως προς τα δεδομένα του συστήματος- όταν δλδ δεδομένου ενός input, οι κόμβοι επεξεργάζονται τα δεδομένα και συμφωνούν ως προς το output. Ως απαρτία (quorum) σε ένα κατανεμημένο σύστημα, ορίζεται το σύνολο των κόμβων που επαρκούν για να επιτευχθεί «συναίνεση».

Πως λοιπόν οι κόμβοι ενός τέτοιου P2P δικτύου, αποφασίζουν αν τα δεδομένα, που πρέπει να επεξεργαστούν είναι έγκυρα; Τι γίνεται αν δύο ή περισσότεροι κόμβοι θελήσουν να διαβάσουν ή να τροποποιήσουν ταυτόχρονα το ίδιο πακέτο δεδομένων (πρόβλημα αμοιβαίου αποκλεισμού - mutual exclusion); Πως ένα σύνολο (group) ομότιμων κόμβων παίρνει μια συλλογική απόφαση, συναινεί δλδ σε μια απόφαση;

Με τον καιρό παρουσιάστηκαν διάφορες λύσεις, με την μορφή πρωτοκόλλων. Κάθε ομότιμος κόμβος ενός P2P δικτύου εμπιστεύεται τα πρωτόκολλα λειτουργίας του δικτύου, για τις κάθε είδους συναλλαγές του με άλλους ομότιμους κόμβους.

Θεώρημα CAP σε κατανεμημένα δίκτυα

Σύμφωνα με τον Chiesa (2018), βλ. σχετικά [76],το θεώρημα "CAP" εξετάζει τρεις βασικές ιδιότητες ενός κατανεμημένου δικτύου:

- Συνέπεια (Consistency),
- Διαθεσιμότητα (Availability) και
- Ανοχή σε κατάτμηση (Partition tolerance).

Η συνέπεια σε ένα κατανεμημένο δίκτυο, σημαίνει ότι κάθε κόμβος γνωρίζει την πιο πρόσφατη κατάσταση (state) του συνολικού δικτύου. Δλδ στην περίπτωση ενός distributed ledger, κάθε κόμβος έχει το ίδιο επικυρωμένο αντίγραφο του ledger. Η συνέπεια σε ένα σύστημα λέει, ότι δύο κόμβοι δεν διατηρούν διατηρούν διαφορετικά αντίγραφα του ledger σε οποιαδήποτε δεδομένη στιγμή. Διαφορετικά, ο κόμβος δεν μπορεί να συμμετέχει σε συναλλαγές.

Η διαθεσιμότητα σε ένα σύστημα σημαίνει ότι κάθε κόμβος έχει συνεχή πρόσβαση στο ledger και διακαιώματα ανάγνωσης και εγγραφής σε αυτό. Με άλλα λόγια, ένα διαθέσιμο σύστημα μου επιτρέπει να ενημερώνω και να ανακτώ το ledger χωρίς καθυστέρηση.

Σαν κατάτμηση ενός κατανεμημένου δικτύου ορίζουμε την αδυναμία δύο ή περισσότερων κόμβων σε ένα δίκτυο να επικοινωνήσουν μεταξύ τους. Εάν ο κόμβος Α δεν μπορεί να λάβει μηνύματα από τον κόμβο Β και αντίστροφα, αυτό σημαίνει ότι υπάρχει μια κατάτμηση (partition) μεταξύ των δύο. Κατά κανόνα θεωρούμε ότι σε ένα

κατανεμημένο δίκτυο, θα συμβεί κάποια κατάτμηση. Επομένως, η ανοχή κατάτμησης είναι η ικανότητα να λειτουργεί το δίκτυο ακόμα και σε αυτή την περίπτωση.

Ένα κατανεμημένο δίκτυο μπορεί να έχει μόνο δύο από τις τρεις από αυτές τις ιδιότητες ανά πάσα στιγμή. Στην τεχνολογία distributed ledger και κατ΄ επέκταση του blockchain, το partition tolerance, ενώ ως προς τις άλλες δύο ιδιότητες γίνεται κάποιου είδους «συμβιβασμός», δλδ ανάλογα με την υλοποίηση και τα πρωτόκολλα επιλέγουμε αν ένας κόμβος που δεν διαθέτει επικυρωμένο ledger δεν συμμετέχει καθόλου σε συναλλαγές ή συμμετέχει με την λάθος έκδοση του ledger (σε αυτή την περίπτωση τα πρωτόκολλα του δικτύου εξασφαλίζουν ότι κάποια στιγμή όλοι οι κόμβοι θα διαθέτουν το ίδιο επικυρωμένο αντίγραφο του ledger).

Το πρόβλημα του double spending

Οι κόμβοι ενός blockchain επικοινωνούν μέσα από το P2P δίκτυο. Όμως σε ένα τέτοιο δίκτυο, μπορεί να υπάρξουν καθυστερήσεις κατά την μετάδοση των δεδομένων των συναλλαγών. Οι συναλλαγές (πχ ένας κόμβος Α ξεκινά μια $1^η$ συναλλαγή με ένα κόμβο Β και πριν ο Β επεξεργαστεί και επικυρώσει την $1^η$ συναλλαγή, ο κόμβος Α ξεκινά και $2^η$ συναλλαγή) δεν λαμβάνονται από τον παραλήπτη αναγκαστικά με τη σειρά με την οποία δημιουργούνται.

Σύμφωνα με τους Crosby et al (2016), βλ. σχετικά [57], στο blockchain υπάρχει ενσωματωμένη στα δεδομένα του block, η χρονολογική σειρά των συναλλαγών που μεταδίδονται από κόμβο σε κόμβο στο P2P δίκτυο,. Οι συναλλαγές του ίδιου block θεωρείται ότι έχουν συμβεί την ίδια στιγμή.

Το πρόβλημα της συναίνεσης

Οποιοσδήποτε κόμβος στο δίκτυο μπορεί να συλλέξει μη επιβεβαιωμένες συναλλαγές και να δημιουργήσει ένα block και στη συνέχεια να το μεταδώσει (προτείνει) στο υπόλοιπο δίκτυο, ως το επόμενο block στο blockchain. Πώς αποφασίζει το δίκτυο ποιο block θα πρέπει να είναι το επόμενο στο blockchain αφού μπορούν να δημιουργηθούν πολλαπλά blocks από διαφορετικούς κόμβους ταυτόχρονα;

Όπως έχουμε αναφέρει σε προηγούμενες ενότητες, υπάρχουν κόμβοι στο δίκτυο που επικυρώνουν τις συναλλαγές που πραγματοποιούνται και καταγράφονται σε ένα

Blockchain. Στο Bitcoin, αυτοί οι κόμβοι καλούνται miners και χρησιμοποιούν το πρωτόκολλο της «απόδειξη εργασίας» (Proof-of-Work) για να επικυρώσουν τις συναλλαγές στο δίκτυο. Ένας κόμβος που δημιουργεί και προτείνει στους υπόλοιπους ένα νέο block, πρέπει να αποδείξει ότι έχει λύσει ένα πολύ ιδιαίτερο μαθηματικό πρόβλημα. Κάθε block μπορεί να αποδεκτό στο blockchain υπό τον όρο ότι περιέχει έγκυρη απάντηση στο παραπάνω πρόβλημα. Οι κόμβοι αυτοί λέγονται miners και έχουν οικονομικό αντάλλαγμα για την προσπάθεια τους, καθώς καταναλώνουν υπολογιστική ισχύ.

Στο Biticoin για παράδειγμα, στο ένας κόμβος μπορεί να χρειαστεί να βρει ένα "Nonce", που όταν έχει χρεωθεί με τις δύο συναλλαγές και τα hashes των προηγούμενων blocks, δημιουργεί ένα hash με ορισμένο αριθμό μηδενικών bits στην αρχή του. Σύμφωνα με τους Crodby et al (2016), βλ. σχετικά [57], η μέση προσπάθεια που απαιτείται αυξάνει εκθετικά σε σχέση με τον αριθμό των απαιτούμενων μηδενικών bits, αλλά η διαδικασία επαλήθευσης είναι πολύ απλή και μπορεί να γίνει με την εκτέλεση ενός απλού hash function.

Η πολυπλοκότητα του προς επίλυση μαθηματικού προβλήματος, μπορεί να ρυθμιστεί έτσι ώστε κατά μέσο όρο να διαρκεί συγκεκριμένο χρονικό διάστημα (δέκα λεπτά για έναν κόμβο στο δίκτυο Bitcoin). Η πιθανότητα να δημιουργηθούν περισσότερα από ένα blocks στο σύστημα σε δεδομένη χρονική στιγμή είναι πολύ μικρή. Ο πρώτος κόμβος, που θα λύσει το πρόβλημα μεταδίδει (προτείνει) το νέο block στο υπόλοιπο δίκτυο (σ.σ περιστασιακά ωστόσο, περισσότερα από ένα blocks θα λυθούν ταυτόχρονα, οδηγώντας σε διάφορους πιθανούς «κλάδους», ωστόσο, επειδή το δίκτυο αποδέχεται μόνο τον κλάδο με το μεγαλύτερο «μήκος», δλδ τα περισσότερα blocks, το blockchain σταθεροποιείται γρήγορα και μετά από αυτό, κάθε κόμβος συμφωνεί στην σειρά των επικυρωμένων blocks).

Εάν ένας hacker προσπαθήσει να επιτεθεί στο δίκτυο και να αλλάξει πληροφορίες για οποιοδήποτε συγκεκριμένο block, η παραβίαση θα εντοπιστεί καθώς το τροποποιημένο hash δεν θα ταιριάζει με το αρχικό. Σύμφωνα με τον Mayank (2018), βλ. σχετικά [15], αυτό εξασφαλίζει ότι το Blockchain είναι αναλλοίωτο και

οποιαδήποτε αλλαγή που γίνεται θα αντανακλάται σε όλο το δίκτυο και θα εντοπίζεται εύκολα

Πρωτόκολλα Συναίνεσης (Consensus Protocols)

Σύμφωνα με τον Lawrence (2017), βλ. σχετικά [8] και όπως επισημαίνει και ο Στεφάνου (2019), βλ. σχετικά [1], βασική προϋπόθεση για την σωστή λειτουργία ενός δικτύου Blockchain, είναι η πλήρη συναίνεση όλων των χρηστών ως προς τα διαμοιραζόμενα δεδομένα, αφού δεν απαιτείται οι χρήστες να είναι έμπιστοι, ούτε υπάρχει κεντρική έμπιστη αρχή που να επιβεβαιώνει την ακεραιότητα των διαμοιραζόμενων δεδομένων (ledger). Σύμφωνα με τον Αντωνόπουλο, βλ. σχετικά [10], *«η συναίνεση είναι ένα αναδυόμενο δημιούργημα της ασύγχρονης αλληλεπίδρασης χιλιάδων ανεξάρτητων κόμβων, ακολουθώντας απλούς κανόνες».*

Για να υπάρξει λοιπόν συναίνεση, απαιτείται να βρεθεί ένας τρόπος επικύρωσης των δεδομένων, προκειμένου να αποφασιστεί ποια δεδομένα είναι έγκυρα και ποια όχι. Η διαδικασία της επικύρωσης των δεδομένων σε ένα δίκτυο P2P ονομάζεται συνήθως «εξόρυξη» (mining) και απαιτεί τη χρήση σύνθετων αλγορίθμων ή όπως λέμε πρωτοκόλλων συναίνεσης (Consensus Protocols). Τα επικυρωμένα block των συναλλαγών προστίθενται στην συνέχεια στην αλυσίδα του Blockchain.

Υπάρχουν 3 απαιτήσεις οποιουδήποτε Consensus Protocols σε ένα P2P δίκτυο:

- Εγκυρότητα (Validity):
  σε κάθε αίτημα/ερώτημα (request), δίνεται μια έγκυρη απάντηση (reply) από ένα κόμβο του δικτύου.
- Συμφωνία (Agreement):
  όλοι οι έγκυροι κόμβοι συμφωνούν/συναινούν στην ίδια απάντηση.
- Τερματισμός (Termination):
  οι κόμβοι που λειτουργούν σωστά, απαντούν σε ένα αίτημα μέσα σε πεπερασμένο χρονικό διάστημα.

Nakamoto Consensus

Το πρωτόκολλο χρησιμοποιείται για να επιτευχθεί συναίνεση σε ένα P2P δίκτυο, όπου εξ΄ ορισμού περιέχει με άγνωστους, μη αξιόπιστους (unknown, untrusted) κόμβους..

Σύμφωνα με τον Chiesa (2017), βλ. σχετικά [76], το Bitcoin ήταν το πρώτο κατανεμημένο σύστημα που χρησιμοποίησε το Nakamoto Consensus.

Θυμίζουμε το πρόβλημα: Οποιοσδήποτε κόμβος στο δίκτυο μπορεί να δημιουργήσει ένα block από μη επιβεβαιωμένες συναλλαγές και στη συνέχεια να το μεταδώσει στο υπόλοιπο δίκτυο, ως μια πρόταση ως προς το ποιο block θα πρέπει να είναι το επόμενο στο blockchain. Επιπλέον, οποιοσδήποτε χρήστης μπορεί να έχει όσα ζεύγη δημόσιου/ιδιωτικού κλειδιού (public/private key pairs) θέλει, μπορεί να έχει δλδ πολλές ψηφιακές ταυτότητες. Πώς αποφασίζει το δίκτυο ποιο block θα πρέπει να είναι το επόμενο στο blockchain αφού μπορούν να δημιουργηθούν πολλαπλά blocks από διαφορετικούς κόμβους ταυτόχρονα, οποιοσδήποτε κόμβος μπορεί να συμμετέχει ή να εγκαταλείψει το δίκτυο ανά πάσα στιγμή, ή ακόμη και να στείλει κατεστραμμένα ή ψευδή μηνύματα (corrupted/false messages) σε άλλους κόμβους;

Η λογική του αλγόριθμου είναι η εξής:
1) Επέλεξε τυχαία έναν «επικεφαλή» κόμβο (leader node) που θα δημιουργήσει τυχαία το επόμενο block.
2) Η επιλογή δεν είναι ακριβώς τυχαία, αφού περισσότερες πιθανότητες να επιλεγούν έχουν οι κόμβοι που καταναλώνουν έναν «ακριβό πόρο» του δικτύου (δλδ ένα κόμβος που «ξοδεύει» περισσότερο από αυτό τον πόρο έχει περισσότερες πιθανότητες να εκλεγεί leader και να δημιουργήσει το επόμενο block που θα προταθεί για ενσωμάτωση στην αλυσίδα). Επομένως οι leaders (λέγονται και miners ή validators όπως θα δούμε παρακάτω) πληρώνουν αντάλλαγμα, για το δικαίωμα τους να δημιουργούν και να προσθέτουν νέα blocks στην αλυσίδα αλλά επίσης ανταμείβονται για αυτό.
3) Οι υπόλοιποι κόμβοι στην συνέχεια «ενσωματώνουν» αυτό το block στην αλυσίδα τους.

Το Bitcoin χρησιμοποιεί όπως θα δούμε στην επόμενη ενότητα, την υπολογιστική ισχύ (computational power) ως ακριβό πόρο, αλλά αυτό είναι μόνο ένας από τους πολλούς πιθανούς πόρους που δαπανάται για να επιτευχθεί η συναίνεση.

Proof of Work

Σύμφωνα με την Wikipedia, βλ. σχετικά [6], η ιδέα του αλγορίθμου Proof-of-Work (PoW) δημοσιεύθηκε αρχικά από τους Cynthia Dwork και Moni Naor το 1993 σε ένα άρθρο με τίτλο "Pricing via Processing or Combatting Junk Mail". Αργότερα μια παρόμοια ιδέα που ονομάζεται Hashcash προτάθηκε το 1997 από τον Adam Back. Ο όρος "Proof-of-Work" προτάθηκε από τους Markus Jakobsson και Ari Juels σε ένα paper που δημοσιεύθηκε το 1999, με τίτλο «Proofs of Work and Bread Pudding Protocols (Extended Abstract)». Ο αλγόριθμος αυτός χρησιμοποιείται από το Bitcoin και χρησιμοποιείται ευρύτατα στην τεχνολογία Blockchain.

Θα δούμε την λειτουργία του αλγορίθμου PoW στο δίκτυο Bitcoin. Σύμφωνα με τον Αντωνόπολου (2017), βλ. σχετικά [10] και όπως επισημαίνει και ο Στεφάνου (2019), βλ. σχετικά [1], όταν πραγματοποιείται μια συναλλαγή στο δίκτυο Bitcoin, καταγράφεται και αποθηκεύεται σε ένα προσωρινό block. Όταν το block γεμίσει με συναλλαγές, μεταδίδεται σε όλους τους κόμβους που συμμετέχουν στο δίκτυο. Κάθε κόμβος, προκειμένου να ελέγξει την εγκυρότητα του block, προσθέτει στο block header το «nonce», (ένα frame δεδομένων μεγέθους 32-bit). Τα δεδομένα του block (μαζί με το nonce), κρυπτογραφούνται με χρήση του SHA-256 και παράγεται ένα Hash. Το πρωτόκολλο του Bitcoin θέτει αυτόματα ένα «στόχο δυσκολίας» (difficulty target) και το παραγόμενο Hash πρέπει να είναι μικρότερο ή ίσο με τον τρέχοντα στόχο για να γίνει αποδεκτό από το δίκτυο. Όλοι οι miners στο δίκτυο προσπαθούν να βρουν ένα αποδεκτό Hash. Συνεχίζουν να αλλάζουν (αυτόματα) την τιμή του «nonce» και να δοκιμάζουν το «block + (καινούργιο) nonce» στον SHA-256, μέχρις ότου βρουν αποδεκτό Hash. Ο πρώτος που θα το πετύχει, έχει επίσημα επικυρώσει τις συναλλαγές στο block και κερδίζει ως αμοιβή ένα ποσό από bitcoins. Τότε αποστέλλεται σε όλους τους υπόλοιπους κόμβους το «block + nonce + Hash» και αφού πιστοποιήσουν οι υπόλοιποι κόμβοι ότι είναι σωστή η λύση, το block συνδέεται στο Blockchain. Η διαδικασία αυτή η οποία διαρκεί περίπου 10 λεπτά. Στην συνέχεια ξεκινά και πάλι για νέες συναλλαγές.

Σύμφωνα με τον Morabito (2017), βλ. σχετικά [12], ο PoW είναι ευάλωτος σε επιθέσεις «πλειοψηφίας» (majority attack ή 51 percent attack). Σε αυτή την περίπτωση ένας χρήστης ή μια ομάδα χρηστών ελέγχουν την πλειοψηφία της «εξορυκτικής» δύναμης (mining power). Οι επιτιθέμενοι έχουν αρκετή δύναμη για να ελέγχουν τα

περισσότερα συμβάντα στο δίκτυο. Μπορούν να μονοπωλήσουν την παραγωγή νέων blocks και να λάβουν ανταμοιβές, καθώς είναι σε θέση να εμποδίσουν άλλους miners να ολοκληρώσουν τα blocks ή να αντιστρέψουν συναλλαγές. Τέτοιου είδους επιθέσεις όμως, δεν έχουν οικονομικά νόημα, αφού απαιτούν τεράστια mining power, ενώ σε περίπτωση επιτυχούς επίθεσης το blockchain θεωρείται «τρωτό» και συνακόλουθα το κρυπτονόμισμα του χάνει την αξία του.

Proof of Stake

Ο αλγόριθμος Proof-of-Stake (PoS) προτάθηκε σαν εναλλακτικός του PoW, για την επικύρωση των συναλλαγών σε ένα blockchain. Σύμφωνα με την Wikipedia, βλ. σχετικά [6], προτάθηκε αρχικά σαν ιδέα στο διαδικτυακό φόρουμ bitcointalk.org το 2011, αλλά το πρώτο κρυπτονόμισμα που έκανε χρήση αυτής της μεθόδου ήταν το Peercoin το 2012, μαζί με το ShadowCash, το Nxt, το BlackCoin, το NuShares/NuBits, το Qora και το NavCoin.

Ο κόμβος που θα επικυρώσει τις συναλλαγές λέγεται validator και επιλέγεται με αιτιοκρατικό τρόπο (σε αντίθεση με τον PoW που η επιλογή είναι τυχαία αφού δεν ξέρουμε ποιος miner θα επιλύσει πρώτος το μαθηματικό πρόβλημα εύρεσης κατάλληλου Hash). Οι κόμβοι για να είναι υποψήφιοι validators, αρκεί να «στοιχηματίσουν» στο δίκτυο ένα ποσό (stake), αγοράζοντας κρυπτονομίσματα του συγκεκριμένου blockchain. Θα επιλεγεί τελικά ο κόμβος με το υψηλότερο stake. Σε περίπτωση που επιλεγεί ένας κόμβος για την δημιουργία και επικύρωση του επόμενου block στην αλυσίδα. λαμβάνει ένα ποσό από την κάθε συναλλαγή, σαν ανταμοιβή.

Στις πρώτες εκδόσεις του PoS, η μόνη προϋπόθεση για να μπορεί κάποιος να επιλέγει ως validator ήταν να διαθέτει tokens στο wallet του. Το stake είναι ανακτήσιμο (retrievable), σε περίπτωση που δεν επιλεχθούν, με την έννοια ότι αυτά τα tokens μπορούν να χρησιμοποιηθούν για άλλες συναλλαγές. Η ιδέα είναι ότι, αν κάποιος επένδυε σε tokens ενός συγκεκριμένου blockchain, θα ενδιαφερόταν άμεσα για την επιτυχία της επένδυσης του και άρα και του δικτύου. Όσα περισσότερα επένδυε, τόσο περισσότερα «διακυβεύονταν» (at stake) για αυτόν σε περίπτωση αποτυχίας του blockchain.

Η ιδέα αυτή δεν θεωρείται από πολλούς, σαν αρκετή δικλείδα ασφαλείας. Μία από τις βασικές ανησυχίες τους ήταν το "nothing to stake" πρόβλημα. Το πρόβλημα μπορεί να συμβεί οποτεδήποτε παρουσιάζεται ένα fork στο blockchain, είτε εξαιτίας μιας κακόβουλης ενέργειας είτε όταν δύο validators προτείνουν blocks ταυτόχρονα. Σε αυτή την περίπτωση, οι υπόλοιποι κόμβοι επιλέγουν να προσθέσουν τυχαία ένα από τα προτεινόμενα blocks στο αντίγραφο του blockchain που διατηρούν. Τελικά η μακρύτερη από τις αλυσίδες που προκύπτουν από το fork, θεωρείται ως έγκυρη και υιοθετείται από όλους. Στον PoS, σε αντίθεση με τον PoW, δεν είναι υπολογιστικά δαπανηρό για τους validators να προσθέτουν νέα blocks στο τέλος του blockchain, επομένως κάθε φορά που συμβαίνει ένα fork, είναι προς το συμφέρον όλων των validators να συνεχίσουν να «εξορύσσουν» και τις δύο αλυσίδες που προκύπτουν από το fork. Αν οι validators συνεχίσουν να εξορύσσουν μόνο σε μια από τις αλυσίδες που προκύπτουν από ένα fork, τότε δεν θα επωφεληθούν αν επέλεξαν την μικρότερη αλυσίδα. Αν όμως όλοι οι validators συνεχίσουν να εξορύσσουν και στις δύο αλυσίδες του fork, γίνεται πιο δύσκολο να επιτευχθεί συναίνεση (consesus) και το δίκτυο γίνεται πιο ευάλωτο σε επιθέσεις double-spending.

Για να λυθεί το "nothing to stake" πρόβλημα, σε νεότερες υλοποιήσεις του PoS, οι κόμβοι που επιθυμούν να επικυρώσουν συναλλαγές (να επιλεγούν δλδ ως validators) πρέπει να καταθέσουν ένα ποσό ως εγγύηση (escrow). Αν ένας validator παράγει κάτι άκυρο, ένα μέρος ή το σύνολο της εγγύησης του παρακρατείται και παύουν να θεωρούνται validators (βλ. παρακάτω και τον Proof-of-Burn).

Proof of Activity

Ο Proof-of-Activity (PoA) είναι ένας υβριδικός αλγόριθμος συναίνεσης που δανείζεται ιδέες τόσο από τον PoW όσο και από τον PoS.

Ο γενικός αλγόριθμος έχει ως εξής:

- Αρχικά, οι miners επιλύουν και προτείνουν ένα σύνολο από πιθανά blocks στο δίκτυο, σύμφωνα με τα βήματα του PoW.
- Στη συνέχεια, ο αλγόριθμος δουλεύει σαν PoS. Μια τυχαία ομάδα από validators επιλεγεί το νέο block, από τα πιθανά blocks που προτείνουν οι miners. Και όπως στον PoS, οι validators επιλέγονται με βάση το stake.

Οι miners καταναλώνουν υπολογιστική ισχύ και οι validators καταναλώνουν ψηφιακό νόμισμα.

Proof of Burn

Το Proof-of-Burn (PoB) είναι παρόμοιος με τον αλγόριθμο Proof-of-Stake, με την διαφορά ότι το stake δεν είναι ανακτήσιμο σε περίπτωση που δεν επιλεγεί ο κόμβος σαν validator. επομένως σε αυτή την περίπτωση λέμε ότι το stake «καίγεται» (burn). Το stake μπορεί να είναι οποιοδήποτε κρυπτονόμισμα.

Αλγόριθμοι όπως ο PoW, χρησιμοποιούν την υπολογιστική ισχύ σαν ανταλλάξιμο πόρο στην εξόρυξη (mining) νέων blocks. Το Bitcoin δεν μπορεί να υπάρξει χωρίς την χρήση ισχυρών υπολογιστών, που εκτελούν πολύπλοκους υπολογισμούς, το αποτέλεσμα των οποίων όμως δεν μπορεί να έχει άλλη χρησιμότητα πέραν της δημιουργίας κρυπτονομίσματος. Άρα έχουμε σπατάλη υπολογιστικής ισχύος. Επιπλέον, οι υπολογιστές αυτοί με τη σειρά τους, καταναλώνουν ηλεκτρικό ρεύμα. Η κατανάλωση ρεύματος για την παραγωγή κρυπτονομισμάτων έχει υπολογιστεί ότι αντιστοιχεί στην ετήσια κατανάλωση της Ελλάδας (έτος αναφοράς το 2018). Πέραν της σπατάλης ηλεκτρικού ρεύματος, αν λάβουμε υπόψη ότι το ρεύμα παράγεται κυρίως από την καύση ορυκτών καυσίμων, έχουμε σαν αποτέλεσμα την αυξημένη εκπομπή διοξειδίου του άνθρακα. Επομένως αλγόριθμοι σαν το PoW είναι «ενεργοβόροι» και περιβαλλοντικά επιζήμιοι. Για το λόγο αυτό προτάθηκαν αλγόριθμοι που καταναλώνουν άλλους πόρους για την επικύρωση των νέων blocks.

Proof of Space/Proof of Capacity

Το Proof-of-Space χρησιμοποιεί τον αποθηκευτικό χώρο (disk usage) σαν πόρο για την δημιουργία και επικύρωση νέων blocks.

Proof of Elapsed Time

Το Proof-of-Elapsed-Time χρησιμοποιεί τον χρόνο (idle time) σαν πόρο για την δημιουργία και επικύρωση νέων blocks. Ζητάμε απλώς από τους χρήστες να περιμένουν για τυχαίο χρονικό διάστημα, και μόλις αυτό τελειώσει, τότε θα επιλεγούν για να προτείνουν και να επικυρώσουν το επόμενο block στην αλυσίδα.
Οι δύο υποθέσεις που κάνουμε είναι:

1) ότι ο χρόνος που ζητάμε από τους χρήστες να περιμένουν είναι στην πραγματικότητα τυχαίος και

2) ότι όντως ο κάθε κόμβος περίμενε τόσο πολύ.

Αυτή η λειτουργικότητα είναι ενσωματωμένη σε Περιβάλλοντα Αξιόπιστων

Εκτελέσεων(Trusted Execution Environments), όπως το Intel SGXs.

Practical Byzantine Fault Tolerance

Σε ένα κατανεμημένο δίκτυο, η λειτουργικότητα των κόμβων του, περιλαμβάνει την αποστολή, την λήψη, την αποθήκευση και την επεξεργασία πληροφοριών. Όλοι οι συμμετέχοντες κόμβοι πρέπει να συμφωνούν σε κάθε μήνυμα που μεταδίδεται μεταξύ των κόμβων.

Υπάρχουν δύο κύριοι τύποι θεμελιωδών σφαλμάτων σε ένα τέτοιο δίκτυο.

- Fail-stop fault: Κατά τη διάρκεια ενός fail-stop fault, οι κόμβοι βγαίνουν εκτός δικτύου και σταματούν να απαντούν. Ένα fail-stop fault σημαίνει ότι ένας κόμβος είναι εκτός λειτουργίας και ανιχνεύεται εύκολα από τους άλλους κόμβους.
- Byzantine fault: Κατά τη διάρκεια ενός byzantine fault, οι κόμβοι στέλνουν αλλοιωμένες ή ψευδείς πληροφορίες. Αυτό το σφάλμα μπορεί να είναι προσωρινό ή να διαρκέσει για άγνωστο χρονικό διάστημα. Ένα Byzantine fault σημαίνει ότι ο προβληματικός κόμβος μπορεί να παράγει αυθαίρετα δεδομένα, συμπεριλαμβανομένων δεδομένων που το κάνουν να φαίνεται σαν λειτουργικός, οπότε δύσκολα ανιχνεύεται. Δεν είναι αναγκαστικά πρόβλημα ασφάλειας αφού μπορεί να προκύψει από σφάλματα υλικού ή λογισμικού.

Εάν κάποιος κόμβος είναι προβληματικός ή εκτός λειτουργίας ή το μήνυμα που μεταδίδει είναι αλλοιωμένο, τότε το P2P δίκτυο στο σύνολό του, θα πρέπει να δείχνει αντοχή στα λάθη (fault tolerance) και θα πρέπει να μπορεί να πετύχει συναίνεση όλων των ομότιμων κόμβων, ως προς τα διαμοιραζόμενα δεδομένα.

Το 1999, οι Miguel Castro και Barbara Liskov πρότειναν τον αλγόριθμο "Practical Byzantine Fault Tolerance" (PBFT). Ο PBFT αποτέλεσε την πρώτη πρακτική λύση στο «πρόβλημα των βυζαντινών στρατηγών». Το πρόβλημα παρουσιάζεται όταν διαφορετικοί κόμβοι ενός αναξιόπιστου δικτύου, πρέπει να συναινέσουν σε μια τελική απόφαση (consensus), ελέγχοντας τα δεδομένα που ανταλλάσσονται.

Το πρόβλημα περιγράφηκε αρχικά από τους Marshall Pease, Robert Shostak και Leslie Lamport το 1982. Βασίζεται στο σενάριο ότι, τμήματα του Βυζαντινού στρατού που πολιορκούν μια εχθρική πόλη, αντιμετωπίζουν προβλήματα με τη δημιουργία ενός κοινού σχεδίου δράσης. Η πολιορκία δεν μπορεί να συνεχιστεί για απεριόριστο χρονικό διάστημα, ενώ η πόλη μπορεί να καταληφθεί μόνο με ταυτόχρονη έφοδο όλων των τμημάτων, σε διαφορετική περίπτωση όλα τα τμήματα πρέπει να υποχωρήσουν προκειμένου να μην υποστούν απώλειες. Κάθε τμήμα διοικείται από το δικό του στρατηγό. Θα πρέπει επομένως, μετά από μία συγκεκριμένη περίοδο, όλοι οι στρατηγοί να συμφωνήσουν αν θα επιτεθούν ή θα υποχωρήσουν ταυτόχρονα. Κατά την μετάδοση των μηνυμάτων μεταξύ των στρατηγών, υπάρχει κίνδυνος παραποίησης τους από κακόβουλους πληροφοριοδότες οι οποίοι έχοντας συμμαχήσει με τους αντιπάλους, μπορούν να μεταδώσουν ψευδείς πληροφορίες ή ακόμα κάποιος από τους στρατηγούς να είναι προδότης και να μεταδώσει ό ίδιος ψευδείς πληροφορίες.

Με βάση λοιπόν τα παραπάνω, ότι οι στρατηγοί πρέπει να βρουν έναν τρόπο, προκειμένου:

- Το σχέδιο δράσης αποτελεί ομόφωνη απόφαση όλων των στρατηγών.
- Η ενδεχόμενη ύπαρξη ενός περιορισμένου αριθμού προδοτών δεν θα οδηγήσει στην υιοθέτηση ενός επιβλαβούς σχεδίου δράσης.

Η αντιστοίχιση των εννοιών στο παραπάνω πρόβλημα, με το πρόβλημα συναίνεσης σε ένα δίκτυο blockchain δίνεται στον παρακάτω πίνακα:

Πρόβλημα Βυζαντινών Στρατηγών	**Blockchain**
Γεωγραφική απόσταση	Κατανεμημένο δίκτυο
Στρατηγοί	Κόμβοι
Προδότες στρατηγοί	Ελαττωματικοί ή κακόβουλοι κόμβοι
Μη έμπιστοι πληροφοριοδότες	Μη έμπιστο δίκτυο/μη έμπιστοι κόμβοι
Κοινό σχέδιο δράσης (επίθεση/οπισθοχώρηση)	Συναίνεση ως προς το ledger

Ο αλγόριθμος «PBFT» μπορεί να διαχειριστεί f σφάλματα (που προκαλούνται από faulty/malicious nodes) σε ένα δίκτυο με 3f+1 κόμβους.

Ο αλγόριθμος «PBFT» χρησιμοποιείται σε permissioned Blockchain δίκτυα, όπως το Hyperledger Fabric, το Ripple, το Stellar. Προϋπόθεση είναι οι κόμβοι να μην είναι ανώνυμοι. Οι κόμβοι επικοινωνούν μεταξύ τους ανταλάσσοντας μηνύματα (messages). Τα μηνύματα περιέχουν έναν sequence number. Επίσης περιέχουν υπογραφές (signatures) και άλλα δεδομένα (metadata) που επιτρέπουν στους κόμβους να καθορίζουν αν το μήνυμα είναι έγκυρο (valid). Κάθε φορά που πραγματοποιείται μια συναλλαγή, επικυρώνεται μέσω μιας συγκεκριμένης διαδικασίας. Αρχικά, επιλέγεται με βάση ορισμένους κανόνες ένας κύριος κόμβος (primary node), ο οποίος θα εξετάσει την ορθότητα των δεδομένων και θα στείλει τα αποτελέσματα σε όλους τους υπόλοιπους κόμβους του δικτύου. Αν τα 2/3 όλων των κόμβων συμφωνούν μαζί του, ο primary node θα περάσει στην επόμενη φάση εξέτασης των δεδομένων. Αν όχι, τότε επιλέγεται νέος primary node. Η διαδικασία ολοκληρώνεται σε 3 φάσεις. Σε κάθε φάση επαναλαμβάνεται η ίδια διαδικασία.

Σύμφωνα με τον Buchman (2016), βλ. σχετικά [14], η διαδικασία ξεκινά όταν ένας client node, υποβάλει ένα «αίτημα» (request) στον primary node.

- Φάση 1- pre-prepare :

  Ο primary node στέλνει ένα μήνυμα προ-προετοιμασίας (pre-prepare message) σε όλους τους άλλους.

- Φάση 2- prepare :

  Αν ένας παραλήπτης κόμβος (receiving node) λάβει ένα pre-prepare message, με την σειρά του στέλνει ένα μήνυμα προετοιμασίας (prepare message) σε όλους τους άλλους. Τα prepare messages γίνοναι αποδεκτά από τους παραλήπτες κόμβους (receiving nodes), μόνο εφόσον είναι έγκυρα (valid), με βάση τον αριθμό ακολουθίας, την υπογραφή και άλλα metadata. Ένας κόμβος θεωρείται «προετοιμασμένος» (prepared), εάν έχει «λάβει» το αρχικό αίτημα από τον primary node, προετοιμάστηκε (pre-prepared) και έχει «λάβει» 2f prepare messages.

- Φάση 3- commit:

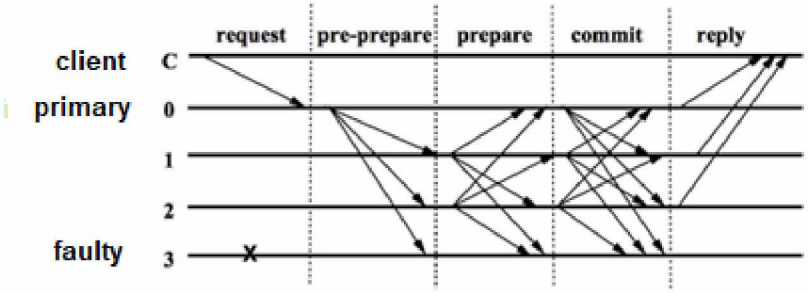
  Όταν οι κόμβοι προετοιμαστούν, στέλνουν ένα μήνυμα δέσμευσης (commit message). Αφού επιτρέπουμε το πολύ f σφάλματα, αν ο primary node λάβει f + 1 valid commit messages, δλδ ίδιες απαντήσεις, αυτό εξασφαλίζει ότι η απόκριση είναι έγκυρη.

Τέλος στέλνεται απ' όλους η απάντηση στο αίτημα του client.

Παράδειγμα:

Σε ένα δίκτυο με (3f +1) κόμβους, ο αλγόριθμος «PBFT» μπορεί να διαχειριστεί f σφάλματα, οπότε για 4 κόμβους ο PBFT μπορεί να διαχειριστεί 1 ελαττωματικό κόμβο (faulty node).

Συνολικά η διαδικασία σε ένα δίκτυο με 4 κόμβους θα έχει όπως παρακάτω:



Εικόνα 2.9 - Φάσεις εκτέλεσης PBFT

Εκτέλεση συναλλαγών στο blockchain

Αφού είδαμε τα βασικά στοιχεία ενός blockchain, θα περιγράψουμε συνολικά την διαδικασία δημιουργίας και επικύρωσης μιας συναλλαγής στο blockchain (με χρήση του proof of work).

Για να δημιουργήσει ο χρήστης μία συναλλαγή, δεν χρειάζεται να γνωρίζει τεχνικές λεπτομέρειες. Αρκεί να διαθέτει ένα wallet (μια διεύθυνση) στο συγκεκριμένο blockchain και κάποιο απόθεμα σε tokens. Το wallet είναι μια lightweight client εφαρμογή, που αναλαμβάνει την διεκπεραίωση της συναλλαγής. Τα wallets αποθηκεύουν επίσης και tokens του χρήστη (στην ουσία δεδομένα που είναι «κλειδωμένα», με τα ψηφιακά κλειδιά του χρήστη).

Επομένως, ο χρήστης για να ξεκινήσει μια συναλλαγή με κάποιον άλλο χρήστη του blockchain, αρκεί να εισάγει στο wallet, το ποσό του asset που θέλει να ανταλλάξει και την διεύθυνση (το wallet) του παραλήπτη. Ο χρήστης που δημιουργεί μια συναλλαγή (αποστολέας), δεσμεύει την αξία των ανταλλασσόμενων assets και περιμένει από τον παραλήπτη την ψηφιακή υπογραφή του για την ολοκλήρωση της συναλλαγής. Καθώς

μόνο ο παραλήπτης, έχει το wallet με κλειδιά που αντιστοιχούν σε αυτή την διεύθυνση, μόνο αυτός μπορεί να ολοκληρώσει την συναλλαγή. Το wallet προσθέτει στην συναλλαγή ένα μικρό ποσό, που είναι η αμοιβή του miner για την επικύρωση του block της συναλλαγής και την καταγραφή του block στο Blockchain.

Το wallet ενός χρήστη μπορεί να στείλει μία καινούρια συναλλαγή σε οποιοδήποτε άλλο χρήστη του Blockchain, μέσα από το P2P δίκτυο. Η συναλλαγή μεταδίδεται σε όλο το δίκτυο, αλλά δεν καταγράφεται αμέσως στο ledger. Κάθε κόμβος διαθέτει ένα "buffer" ή αλλιώς "pool", όπου αποθηκεύει προσωρινά μη επικυρωμένες συναλλαγές.

Οι κόμβοι που λειτουργούν ως miners, μόλις λάβουν από το δίκτυο ένα νέο επικυρωμένο block για να το ελέγξουν και να το προσθέσουν στο αντίγραφο του ledger που διατηρούν, ξεκινούν την δημιουργία νέου (μη επικυρωμένου) block. Επιλέγουν μη επικυρωμένες συναλλαγές από το pool τους (σύμφωνα με κάποια κριτήρια) και τις ομαδοποιούν σε block, μαζί με το hash του επικυρωμένου block που έλαβαν. Ξεκινούν την διαδικασία επικύρωσης (με χρήση του proof of work) για το νέο μη επικυρωμένο block, δλδ προσπαθούν να βρουν ένα hash για το νέο block με πολύ συγκεκριμένα χαρακτηριστικά. Σημειώνουμε ότι αυτή η διαδικασία γίνεται ταυτόχρονα απ' όλους τους miners (αφού οι μη επικυρωμένες συναλλαγές κοινοποιούνται σε όλους τους κόμβους). Ο πρώτος που θα βρει ένα έγκυρο hash, επικυρώνει το block, εισπράττει την αμοιβή και κοινοποιεί το επικυρωμένο block στους υπόλοιπους κόμβους, προκειμένου να το ελέγξουν και να το προσθέσουν στο αντίγραφο του ledger που διατηρούν. Οι συναλλαγές του επικυρωμένου block διαγράφονται από το pool του κάθε κόμβου.

Επισημαίνουμε ότι ο έλεγχος του επικυρωμένου block είναι απλός (με εφαρμογή μιας hash συνάρτησης). Επίσης η όλη διαδικασία είναι τυχαία, αφού δεν γνωρίζουμε από πριν ποιος miner θα επικυρώσει πρώτος το νέο block. Με την προσθήκη του νέου block στην αλυσίδα, τα υπάρχοντα αντίγραφα του Blockchain ενημερώνονται σε όλους τους κόμβους του δικτύου.

Ασφάλεια του Blockchain

Τα ακόλουθα χαρακτηριστικά καθιστούν την επαναστατική τεχνολογία του Blockchain ξεχωριστή:

- Αποκεντρωμένο
- Δίκτυο Peer-to-Peer
- Αμετάβλητο
- Παράνομη παραβίαση

Το blockchain θεωρείται «αμετάβλητο» (immutable), αφού δεν μπορεί να μεταβληθεί το ιστορικό των καταγεγραμμένων δεδομένων στην αλυσίδα. Για να το κατανοήσουμε, σκεφτείτε το ανάλογο της αποστολής ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Αφού στείλουμε ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε ένα πολύ μεγάλο αριθμό παραληπτών, δεν μπορούμε να το πάρουμε πίσω. Για να βρούμε έναν τρόπο, θα πρέπει να ζητήσουμε από όλους τους παραλήπτες να διαγράψουν το email, πράγμα αρκετά δύσκολο και χρονοβόρο. Έτσι περίπου λειτουργεί και η αμετάβλητη λειτουργία του Blockchain. Αν προσπαθήσουμε να αλλάξουμε τα δεδομένα ενός block, θα πρέπει να αλλάξουμε ολόκληρο το Blockchain που ακολουθεί, καθώς και κάθε block που αποθηκεύει το hash του προηγούμενου block. Η αλλαγή σε ένα hash θα οδηγήσει σε αλλαγή σε όλα τα επόμενα hashes και αυτό απαιτεί πολλή υπολογιστική ισχύ. Ως εκ τούτου, τα δεδομένα που αποθηκεύονται σε ένα block αλυσίδα δεν είναι ευαίσθητα σε αλλοιώσεις ή επιθέσεις ενός hacker. Αν αυτό από μόνο του δεν αρκεί, το Blockchain έχει και κάποια άλλα εγγενή χαρακτηριστικά που παρέχουν πρόσθετη ασφάλεια.

Τα αρχεία σε ένα Blockchain είναι ασφαλή, δεδομένου ότι γίνεται χρήση κρυπτογράφησης και ψηφιακής υπογραφής. Οι συμμετέχοντες στο δίκτυο χρησιμοποιούν τα ιδιωτικά τους κλειδιά και την ψηφιακή τους υπογραφή, στις συναλλαγές που πραγματοποιούν. Εάν αλλάξει μια εγγραφή, η υπογραφή θα καταστεί άκυρη και το blockchain, θα γνωρίζει αμέσως ότι έχει συμβεί κάτι.

Τα Blockchains χρησιμοποιούν αποκεντρωμένα και κατανεμημένα σε δίκτυα ομότιμων κόμβων, που ενημερώνονται συνεχώς και διατηρούν συγχρονισμένα αντίγραφα του ledger. Δεν απαιτούν κεντρική αποθήκευση δεδομένων, ώστε να είναι

ευάλωτα στην περίπτωση που κάποιος αποκτούσε πρόσβαση σε μια κεντρική βάση δεδομένων. Τα πρωτόκολλα συναίνεσης εξασφαλίζουν την συναίνεση των κόμβων ως προς την εγκυρότητα των δεδομένων. Σε κάθε περίπτωση, όσο μεγαλύτερο είναι το δίκτυο, τόσο πιο ανθεκτικό θα είναι το Blockchain.

Σύμφωνα με τον Miles (2017), βλ. σχετικά [16], οι δημόσιες και ιδιωτικές Blockchains διαφέρουν, ως προς το επίπεδο ασφάλειας που παρέχουν, Η πιο προφανής διαφορά είναι ότι τα δημόσια blockchains χρησιμοποιούν ανώνυμους κόμβους συνδεδεμένους στο διαδίκτυο (miners) για να επικυρώσουν τις συναλλαγές και να προσθέσουν blocks στο ledger. Οι ιδιωτικές blockchains, από την άλλη πλευρά, επιτρέπουν μόνο γνωστούς (έμπιστους ή εξουσιοδοτημένους) κόμβους. Το δίκτυο δεν είναι δημόσιο, ούτε οι κόμβοι ανώνυμοι, και οι συναλλαγές επικυρώνονται από έμπιστους κόμβους. Το πλεονέκτημα αυτού για τις επιχειρήσεις, είναι ότι μόνο οι συμμετέχοντες με την κατάλληλη πρόσβαση και δικαιώματα, μπορούν να διατηρήσουν το ledger. Βέβαια, ένα δίκτυο αποκλεισμού, όπως τα ιδιωτικά blockchains, που αποκλείει την πρόσβαση σε μη έμπιστους άγνωστους κόμβους, είναι εξίσου ασφαλές με την υποδομή του.

ΚΕΦΑΛΑΙΟ 3 - ΔΥΝΑΜΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ BLOCKCHAIN

Εφαρμογές της τεχνολογίας Blockchain

Η τεχνολογία Blockchain, έχει την δυναμική να μετασχηματίσει τις οργανωτικές δομές και τον τρόπο λειτουργίας της οικονομίας. Η εφαρμογή της όμως συνεπάγεται αλλαγές στις κοινωνικές και πολιτικές διαδικασίες. Αυτό προϋποθέτει τη δημιουργία κατάλληλου θεσμικού πλαισίου και την τροποποίηση υφιστάμενων ρυθμίσεων, προκειμένου η νέα τεχνολογία να μπορέσει να απελευθερώσει το πλήρες δυναμικό της.

Σύμφωνα με την Investopedia, βλ. σχετικά [3], το Blockchain είναι ένα αποκεντρωμένο και κατανεμημένο μητρώο και μπορεί να χρησιμοποιηθεί για την καταγραφή δεδομένων οποιασδήποτε μορφής σε ένα δίκτυο από ανεξάρτητους και άγνωστους μεταξύ τους χρήστες. Σε ένα blockchain μπορούμε να καταγράψουμε οποιαδήποτε δεδομένα, όπως για παράδειγμα τους τίτλους ιδιοκτησίας ενός οικοπέδου (φυσικά δεδομένα) ή πνευματικά δικαιώματα για ένα τραγούδι (άυλα δεδομένα). Επεκτείνοντας τα παραπάνω, θα μπορούσαμε να πούμε ότι σε ένα δίκτυο Blockchain, μπορούμε να καταγράψουμε σε ψηφιακή μορφή και να διαχειριστούμε οτιδήποτε έχει αξία (asset).

Χρηματοπιστωτικές - Ασφαλιστικές υπηρεσίες (Financial /Trade - Insurances)

Σύμφωνα με μια μελέτη που δημοσίευσε η Accenture και η McLagan (Ιανουάριος 2017), το 77% του κλάδου των χρηματοπιστωτικών υπηρεσιών σχεδιάζει να υιοθετήσει το blockchain μέχρι τα τέλη του 2020. Οι τράπεζες που ήταν το ένα τρίτο των ερωτηθέντων οργανισμών έχουν δείξει μια τάση να ενσωματώσουν το blockchain στις δραστηριότητές τους.

.

Ο παραδοσιακός τρόπος επεξεργασίας κι εκκαθάρισης τραπεζικών συναλλαγών, είναι δαπανηρός, περίπλοκος και αργός και αυξάνει τις πιθανότητες λαθών, καθώς περισσότερα μέρη εμπλέκονται για την ολοκλήρωση μίας συναλλαγής. Η τεχνολογία blockchain δίνει την δυνατότητα πραγματοποίησης τραπεζικών συναλλαγών, αποκεντρωμένα και χωρίς την ανάγκη ύπαρξης ενδιάμεσων προσώπων, ενώ μπορεί να περιορίσει και φαινόμενα απάτης.

Σύμφωνα με σχετική έρευνα της ΕΚΤ (2019), βλ. σχετικά [18], με την τεχνολογία blockchain ο χρόνος επιβεβαίωσης και εκκαθάρισης συναλλαγών θα μειωθεί δραματικά, ανεξάρτητα από τη γεωγραφική θέση των συναλλασσόμενων και θα γίνεται χωρίς τη μεσολάβηση τρίτων (τράπεζας).

Από την περικοπή του κόστους και την αποσυμφόρηση της γραφειοκρατίας στη βιομηχανία fintech, το blockchain έχει χαρακτηριστικά και δυνατότητες να κάνει την τραπεζική πιο απρόσκοπτη και αποτελεσματική εμπειρία τόσο για τις τράπεζες όσο και για τους πελάτες.

Η νέα τεχνολογία μπορεί να έχει εφαρμογή και στον ασφαλιστικό τομέα, με την χρήση μητρώων όπου θα καταχωρούνται και θα ενημερώνονται με ασφάλεια οι σχετικές πληροφορίες.

Τήρηση μητρώων (Records - Land Title Recording - Mortgages)

Η πιο προφανής εφαρμογή της τεχνολογίας Blockchain είναι η τήρηση μητρώων, όπως το κτηματολόγιο, το ληξιαρχείο, μητρώο εταιρειών, φορολογικό μητρώο, μητρώο δικαιωμάτων διανοητικής ιδιοκτησίας κλπ. Μπορεί να εξασφαλίσει την εγκυρότητα των δεδομένων, αποτρέποντας τις διπλές εγγραφές, κακόπιστες καταχωρήσεις κ.λ,π.

Η τεχνολογία blockchain μπορεί να αποτελέσει μια εύκολη και φθηνή λύση σε θέματα πνευματικών δικαιωμάτων. Μπορεί επίσης να χρησιμοποιηθεί από τις τελωνειακές και αστυνομικές αρχές για την αντιμετώπιση των απομιμητικών προϊόντων επιτρέποντας τη χρήση ασφαλών και μη τροποποιήσιμων πιστοποιητικών.

Έξυπνα συμβόλαια (Smart contracts)

Ένα έξυπνο συμβόλαιο είναι μια αυτοεπιβαλλόμενη (self-enforcing) σύμβαση ενσωματωμένη στον κώδικα (λογισμικό) του υπολογιστή που διαχειρίζεται ένα blockchain. Ο κώδικας περιέχει ένα σύνολο κανόνων βάσει των οποίων τα μέρη του έξυπνου συμβολαίου, συμφωνούν να αλληλεπιδρούν μεταξύ τους.
Όταν πληρούνται οι προκαθορισμένοι κανόνες, η συμφωνία εφαρμόζεται αυτομάτως.
Ένα smart contract trigger είναι ένας μηχανισμός που ενεργοποιεί την εκτέλεση

έξυπνων συμβολαίων. Ένα blockchain που παρέχει έξυπνα συμβόλαια θα πρέπει να παρέχει πολλαπλά triggers για τα έξυπνα συμβόλαια που εκτελούνται σε αυτό, ώστε να είναι λειτουργικά σε διαφορετικά περιβάλλοντα.

Σύμφωνα με τον Σταμπέρνα (2018), βλ. σχετικά [13], τα έξυπνα συμβόλαια παρέχουν μηχανισμούς για την αποτελεσματική διαχείριση των στοιχείων ενεργητικού μεταξύ δύο ή περισσοτέρων μερών. Οι υποκείμενες αξίες αποθηκεύονται σε ένα blockchain, όπου προστατεύονται από τη διαγραφή, την παραβίαση και την αναθεώρηση.

Ένα «έξυπνο συμβόλαιο» μπορεί να αναλυθεί σε δύο χωριστά μέρη:
• Τον κώδικα του έξυπνου συμβολαίου (Smart Contract Code): Ο κώδικας του έξυπνου συμβολαίου που αποθηκεύεται, επαληθεύεται και εκτελείται στο blockchain.
• Τις έξυπνες νομικές συμβάσεις (Smart Legal Contracts): Οι νομικές συμβάσεις τις οποίες υλοποιεί ο Smart Contract Code.

Τα blockchains και τα έξυπνα συμβόλαια δεν μπορούν να έχουν πρόσβαση σε δεδομένα εκτός του δικτύου τους. Επομένως για να μάθει τι πρέπει να κάνει, ένα έξυπνο συμβόλαιο συχνά χρειάζεται πρόσβαση σε «δεδομένα από τον έξω κόσμο» (δλδ transactional data) που σχετίζονται με τη συμβατική συμφωνία, με τη μορφή ψηφιακών δεδομένων. Τα oracles είναι υπηρεσίες που αποστέλλουν και επαληθεύουν τα γεγονότα του πραγματικού κόσμου και υποβάλλουν αυτές τις πληροφορίες σε έξυπνα συμβόλαια εντός του blockchain.

Ηλεκτρονική Διακυβέρνηση (e-gov)

Η πολιτική ατζέντα των κυβερνήσεων όσον αφορά την τεχνολογία Blockchain θα έπρεπε να επικεντρωθεί κυρίως στο να άρει φραγμούς και δυσκολίες που δεν έχουν να κάνουν με την καθ' αυτό τεχνολογία του Blockchain, αλλά κυρίως με το υφιστάμενο νομικό και θεσμικό πλαίσιο, προκειμένου να ωθήσει τους δημόσιους οργανισμούς και φορείς, τις επιχειρήσεις, και τα άτομα να υιοθετήσουν και να αποδεχτούν την νέα τεχνολογία, «μετασχηματίζοντας» διαδικασίες, τρόπο σκέψης και λειτουργίας.

Σύμφωνα με το Forbes (2018), βλ. σχετικά [23], ένα παράδειγμα της εφαρμογής του Blockchain στην ψηφιακή διακυβέρνηση είναι η ηλεκτρονική ψηφοφορία. Το

αποτελέσμα της ψηφοφορίας θα είναι αδιάβλητο, διαφανές και προσβάσιμο από όλους. Τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση της όλης διαδικασίας.

Επίσης το blockchain μπορεί να έχει εφαρμογή στην εταιρική διακυβέρνηση.

Διαχείριση ψηφιακής ταυτότητας (Digital Identity)

Μια επιτυχημένη Κοινωνία της Πληροφορίας, προϋποθέτει τη χρήση πληροφοριακών συστημάτων και υποδομών σε όλους τους τομείς: την οικονομία, την διαχείριση κυβερνητικών υποθέσεων, στις ηλεκτρονικές υπηρεσίες τελικών χρηστών και πολλά άλλα. Αυτό απαιτεί από τους χρήστες του Διαδικτύου να έχουν έναν σταθερό, ασφαλή και βολικό τρόπο για να ταυτοποιούν τον εαυτό τους online - μια ψηφιακή ταυτότητα (digital identity).

Προκειμένου να επιτύχουμε τα παραπάνω με αποτελεσματικό, ασφαλή και χρησιμοποιήσιμο τρόπο, απαιτείται η χρήση ενός Συστήματος Διαχείρισης Ψηφιακής Ταυτότητας (Digital Identity Management – DIM) που θα αντιστοιχεί τα άτομα με την αντίστοιχη ψηφιακή τους ταυτότητα. Ένα τέτοιο σύστημα θα απαιτούσε την έκδοση και τη διατήρηση καρτών ταυτότητας, πιστοποιητικών για πληροφοριακά συστήματα και την υποδομής που θα επιτρέπει την επαλήθευση των ηλεκτρονικών συναλλαγών.

Η τεχνολογία blockchain θα μπορούσε να αποτελέσει τη βάση για ένα τέτοιο σύστημα.

Διαδίκτυο των πραγμάτων (Internet Of Things - IoT)

Όπως έχει οριστεί από την ITU, βλ. σχετικά [34], το Διαδίκτυο των πραγμάτων (Internet Of Things - IoT) αναφέρεται στο σύνολο διάφορων έξυπνων συσκευών με πρόσβαση στο διαδίκτυο. Σύμφωνα με στοιχεία του Gartner (2019), βλ. σχετικά [22], 20 δισεκ. έξυπνες συσκευές θα είναι διασυνδεδεμένες στο διαδίκτυο μέχρι τα τέλη του 2020. Μια έξυπνη συσκευή είναι συνδεδεμένη στο διαδίκτυο, και αλληλεπιδρά με τον κάτοχό της αλλά και με άλλες έξυπνες συσκευές, στέλνοντας και λαμβάνοντας συνεχώς δεδομένα. Έτσι επιτυγχάνεται αποτελεσματικότερη απόδοση, βέλτιστη κατανάλωση ενέργειας, απομακρυσμένος έλεγχος και καλύτερη συντήρηση των συσκευών.

Η χρήση της τεχνολογίας blockchain, παρέχει την δυνατότητα κρυπτογράφησης αυτών των δεδομένων εξασφαλίζοντας υψηλότερο επίπεδο ασφάλειας κατά την μετάδοση τους.

Διαχείριση εφοδιαστικής αλυσίδας (Supply Chains and logistics)

Όπως αναφέραμε σε προηγούμενες ενότητες, τα δεδομένα που καταγράφονται σε ένα blockchain, θεωρούνται αμετάβλητα (immutable), υπό την έννοια ότι δεν μπορεί να τροποποιηθεί το ιστορικό των συναλλαγών που έχουν καταγραφεί στην αλυσίδα. Το παραπάνω χαρακτηριστικό της τεχνολογίας blockchain την καθιστά ιδανική επιλογή για την παρακολούθηση των προϊόντων μιας εφοδιαστική αλυσίδας.

Επίσης η δυνατότητα δημιουργίας έξυπνων συμβολαίων πάνω σε μια πλατφόρμα blockchain καθώς και η δυνατότητα χρήσης διάφορων triggers αλλά και αισθητήρων επί των προϊόντων που θα ενεργοποιούν αυτά τα έξυπνα συμβόλαια, μπορούν να δρομολογήσουν γεγονότα (όπως π.χ. η διανομή των προϊόντων κατά την άφιξη τους σε ένα λιμάνι σε διαφορετικά containers), προσφέροντας έτσι ένα νέο δυναμικό τρόπο οργάνωσης και παρακολούθησης δεδομένων και προϊόντων στην εφοδιαστική αλυσίδα.

Η χρήση καρτών RFID ή QR code επί των προϊόντων, σε συνδυασμό με την τεχνολογία blockchain, δίνει την δυνατότητα, να υπάρχει πλήρες ιστορικό και επομένως διαφάνεια και ακριβή γνώση της διαδικασίας παραγωγής και διακίνησης των προϊόντων, παρέχοντας δεδομένα σε πραγματικό χρόνο στον τελικό καταναλωτή ή τον έμπορο.

Αναφέρουμε ενδεικτικά ότι στις Η.Π.Α., σύμφωνα με έρευνα της Deloitte και του σωματείου εταιρειών μηχανογράφησης κι εφοδιαστικής αλυσίδας, παρόμοιοι αισθητήρες και τεχνολογία, χρησιμοποιούνταν ήδη από το 2016, στις μισές εταιρείες του χώρου ενώ η υιοθέτησή τους προβλέπεται να είναι σχεδόν καθολική μέσα στα επόμενα χρόνια.

Νομικές πτυχές της εφαρμογής της τεχνολογίας Blockchain

Υπάρχουν όπως είναι φυσικό πολλά θέματα που προκύπτουν από την υιοθέτηση της νέας τεχνολογίας του Blockchain σε νομικό επίπεδο. Σύμφωνα με τον Μαρκουλή (2019), βλ. σχετικά [27], η προσαρμογή του νομικού και θεσμικού πλαισίου είναι

προϋπόθεση για την απρόσκοπτη υιοθέτηση της νέας τεχνολογίας σε διάφορους τομείς της οικονομίας και της κοινωνίας, ενώ την αρμοδιότητα και ευθύνη την έχουν οι κυβερνήσεις και οι διεθνείς οργανισμοί.

Προσωπικά δεδομένα

Η τεχνολογία blockchain και ο τρόπος που καταχωρεί και αποθηκεύει δεδομένα, θα πρέπει να εξεταστεί αν είναι συμβατή με το δίκαιο προστασίας προσωπικών δεδομένων.

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], είναι δύσκολο, ιδίως σε δημόσιες πλατφόρμες blockchain, να διακρίνει κανείς ρόλους και αρμοδιότητες στην διαδικασία καταγραφής και επεξεργασίας προσωπικών δεδομένων, μέσα σε ένα περιβάλλον μιας πλατφόρμας blockchain. Επίσης είναι δύσκολο να ελέγξει κανείς αν προβλέψεις του νέου Κανονισμού για την προστασία των προσωπικών δεδομένων (GDPR), όπως το δικαίωμα διαγραφής ή ενημέρωσης των προσωπικών δεδομένων, τηρούνται σε μία δημόσια, κατανεμημεμένη και αμετάβλητη βάση δεδομένων, όπως είναι το blockchain.

Κρυπτονομίσματα

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], απαραίτητη προϋπόθεση για την συστηματική ένταξη των κρυπτονομισμάτων σε κανόνες δικαίου, είναι ο νομικός χαρακτηρισμός τους. Σχεδόν κανένα από τα κρυπτονομίσματα δεν λειτουργεί ως νόμισμα. Λειτουργούν περισσότερο ως ψηφιακά περιουσιακά στοιχεία (digital assets) η αξία των οποίων είναι συνδεδεμένη και υπάρχει μόνο μέσα στο πλαίσιο λειτουργίας ενός συγκεκριμένου blockchain.

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], τον Οκτώβριο του 2015 το Δικαστήριο της Ευρωπαϊκής Ένωσης το Δικαστήριο της ΕΕ (ΔικΕΕ, υπόθεση C-264/14, σκέψη 24), στο πλαίσιο της ερμηνείας της Οδηγίας 2006/112/ΕΚ περί Φ.Π.Α. έκρινε ότι «*το bitcoin, δεν μπορεί να χαρακτηριστεί ως ενσώματο αγαθό κατά την έννοια του άρθρου 14 της οδηγίας περί ΦΠΑ, διότι έχει ως αποκλειστικό σκοπό να αποτελέσει μέσο πληρωμής καθώς και ότι η ανταλλαγή παραδοσιακών νομισμάτων έναντι bitcoins απαλλάσσεται από τον Φ.Π.Α.*», βλ. σχετικά [30].

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], το Δικαστήριο της ΕΕ (ΔικΕΕ, υπόθεση C-264/14, σκέψη 49), οι πράξεις που αφορούν μη συμβατικά νομίσματα, δηλαδή νομίσματα που δεν αποτελούν εκ του νόμου μέσα πληρωμής σε μία ή περισσότερες χώρες, είναι χρηματοπιστωτικές πράξεις, υπό την προϋπόθεση ότι τα εν λόγω μη συμβατικά νομίσματα γίνονται δεκτά από τους συναλλασσόμενους ως εναλλακτικό, σε σχέση με τα συμβατικά νομίσματα, μέσο πληρωμής και χρησιμοποιούνται αποκλειστικά ως μέσα πληρωμής, βλ. σχετικά [31]. Αξίζει να σημειωθεί ότι σύμφωνα με την απόφαση παραπομπής του αιτούντος δικαστηρίου (Ανώτατο Διοικητικό Δικαστήριο της Σουηδίας) στην ανωτέρω υπόθεση, η διεύθυνση bitcoin [σσ. το δημόσιο κλειδί ενός χρήστη] μπορεί να συγκριθεί με τον αριθμό τραπεζικού λογαριασμού.

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], η Ευρωπαϊκή Κεντρική Τράπεζα με έκθεσή της τον Φεβρουάριο του 2015, δεν θεωρεί τα εικονικά νομίσματα, όπως το Bitcoin ως μία μορφή χρήματος, όπως ορίζεται στην οικονομική επιστήμη, αλλά ούτε και από νομικής απόψεως. Για τους σκοπούς της εν λόγω έκθεσης, η ΕΚΤ όρισε τα εικονικά νομίσματα ως «*μία ψηφιακή αποτύπωση αξίας, η οποία δεν εκδίδεται από μία κεντρική τράπεζα, χρηματοπιστωτικό ίδρυμα ή ένα ίδρυμα ηλεκτρονικού χρήματος, η οποία, σε ορισμένες περιπτώσεις, μπορεί να χρησιμοποιηθεί ως εναλλακτική του – παραδοσιακού – χρήματος*». Για την ΕΚΤ, η υφιστάμενη ρύθμιση που ισχύει για τον παραδοσιακό οικονομικό τομέα δεν μπορεί να εφαρμοστεί καθώς δεν υπάρχουν τα παραδοσιακά οικονομικά μέρη, και κατηγοριοποιεί το bitcoin ως «*μετατρέψιμο αποκεντρωμένο εικονικό νόμισμα*». Η Ευρωπαϊκή Ένωση σχεδιάζει να ρυθμίσει, τουλάχιστον εν μέρει τη διάθεση εικονικών νομισμάτων, στο πλαίσιο της αναθεώρησης της 4ης Οδηγίας (ΕΕ) 2015/849 για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], σχεδόν όλες οι δημόσιες πλατφόρμες blockchain προβλέπουν την δημιουργία tokens τα οποία είναι απαραίτητα για τη συμμετοχή στην πλατφόρμα αυτή. Πρόσφατα, σε μία περίπτωση διάθεσης tokens μέσω της πλατφόρμας του Ethereum, η Επιτροπή Κεφαλαιαγοράς των Η.Π.Α., (SEC), βλ. σχετικά [29], έκρινε ότι αυτά πρέπει να αντιμετωπίζονται ως κινητές αξίες και συνεπώς η διάθεσή τους διέπεται από την ισχύουσα νομοθεσία.

Δίκαιο προστασίας καταναλωτή

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], η εφαρμογή της τεχνολογίας blockchain στα κρυπτονομίσματα, εγείρει σημαντικά ζητήματα που άπτονται ευθέως του δικαίου του καταναλωτή (έλλειψη διαφάνειας ως προς τον τρόπο λειτουργίας τους, ασαφές νομικό καθεστώς, έλλειψη εγγυήσεων κ.λ.π).

Έξυπνα συμβόλαια

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], η εφαρμογή της τεχνολογίας blockchain και η υποστήριξη των έξυπνων συμβολαίων, περιορίζει σημαντικά τα περιθώρια διαφορετικών ερμηνειών των συμβατικών όρων κατά την εκτέλεσή τους. Όμως είναι δύσκολη η τροποποίηση των όρων ενός έξυπνου συμβολαίου εξαιτίας πιθανών αλλαγών στο νομικό πλαίσιο. Από την ΕΚΤ, βλ. σχετικά [32], έχουν προταθεί λύσεις όπως η διασύνδεση των έξυπνων συμβολαίων με νομικές βάσεις δεδομένων προκειμένου να ενημερώνονται αυτόματα για το ισχύον νομοθετικό πλαίσιο και ο διαχωρισμός των όρων σε τροποποιήσιμους και μη. Επίσης προκύπτουν επίσης νομικά ζητήματα κατά το στάδιο της εκτέλεσης των συμβολαίων που αφορούν την μη συμμόρφωση με όρους του συμβολαίου καθώς επίσης και με το πτωχευτικό δίκαιο.

Δικονομία

Σύμφωνα με το Λαγαρά (2019), βλ. σχετικά [28], η τεχνολογία blockchain, θα επιφέρει αλλαγές στη δικονομία κυρίως όσον αφορά τα αποδεικτικά μέσα (τίτλοι κυριότητας, απόδειξη συναλλαγών, βεβαίωση χρονολογίας πραγματικών περιστατικών), αφού θα μπορούν να χρησιμοποιηθούν στοιχεία που καταχωρούνται σε μία πλατφόρμα blockchain, ως τεκμήρια. Ομοίως γνωστοποιήσεις με βέβαιο χρονολογίας, βέβαιο περιεχόμενο και βέβαιη παραλαβή (επιδόσεις εγγράφων) θα μπορούν να γίνονται με βάση τη νέα τεχνολογία. Η λύση αυτή θα ήταν σύμφωνη και με τον Κανονισμό (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014 , σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές.

Αναπτυξιακές πτυχές της τεχνολογίας Blockchain

Η τεχνολογία Blockchain, όπως και κάθε νέα τεχνολογία, μπορεί να αποτελέσει εργαλείο οικονομικής ανάπτυξης.

Σύμφωνα με τους Τριαντόπουλο και Φιλίνη (2019), βλ. σχετικά [73], ο όρος οικονομική ανάπτυξη είναι ένας ποιοτικός δείκτης, ο οποίος σχετίζεται με τις δυνατότητες ικανοποίησης των ατομικών και κοινωνικών αναγκών. Συχνά έναντι του όρου οικονομική ανάπτυξη, χρησιμοποιείται ο όρος οικονομική μεγέθυνση και το αντίστροφο. Ως οικονομική μεγέθυνση ορίζεται η ετήσια ποσοστιαία μεταβολή μιας μεταβλητής (του εισοδήματος ή του παραγόμενου προϊόντος). Η οικονομική μεγέθυνση είναι ποσοτικός δείκτης. Η οικονομική μεγέθυνση είναι προϋπόθεση για την οικονομική ανάπτυξη. Οι σημαντικότερες θεωρίες οικονομικής μεγέθυνσης έχουν διατυπωθεί από τους Thomas Robert Malthus, W.W. Rostow, Harrod - Domar και Robert M. Solow.

Σύμφωνα με τους Τριαντόπουλο και Φιλίνη (2019), βλ. σχετικά [73], το υπόδειγμα οικονομικής μεγέθυνσης του Robert M. Solow, αποδεικνύει την αλληλεξάρτηση μεταξύ της αύξησης του αποθέματος κεφαλαίου, της αύξησης του εργατικού δυναμικού και της τεχνολογικής προόδου. Αν βελτιωθεί η τεχνολογία, τότε για κάθε ποσότητα κεφαλαίου θα παράγεται περισσότερο προϊόν. Η επιστημονική πρόοδος, μέσω της έρευνας και ανάπτυξης, οδηγεί στην τεχνολογική πρόοδο, που με τη σειρά της οδηγεί στην αύξηση της παραγωγικότητας και επομένως στην οικονομική ευημερία. Η παραγωγή της γνώσης προωθεί την οικονομική ανάπτυξη. Επιπλέον σε μια Κοινωνία της Πληροφορίας, η πληροφορία είναι ταυτοχρόνως αγαθό αλλά και μέσο βελτίωσης της παραγωγικής διαδικασίας.

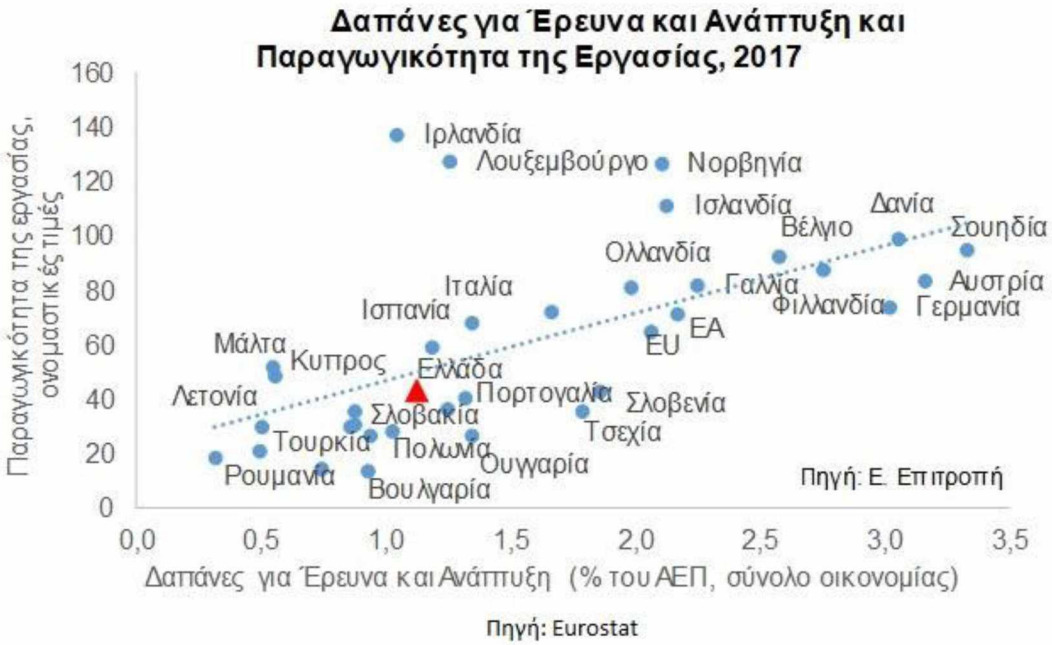
Θα λέγαμε ότι η περίπτωση της τεχνολογίας Blockchain, αποτελεί χαρακτηριστική περίπτωση καινοτόμου τεχνολογίας που μπορεί να οδηγήσει στην αύξηση της παραγωγικότητας και επομένως στην οικονομική ευημερία και ανάπτυξη.

Βέβαια, προϋπόθεση είναι οι επιχειρήσεις να επενδύουν μέρος των κεφαλαίων τους, σε έρευνα και ανάπτυξη και να υιοθετούν καινοτόμες τεχνολογίες στις παραγωγικές τους

διαδικασίες. Επίσης, το κράτος μπορεί να συμβάλει στην τεχνολογική πρόοδο, άρα και στη μεγέθυνση μιας οικονομίας, μέσα από την:

- δημιουργία θεσμικού πλαισίου που ευνοεί τις επενδύσεις σε έρευνα και ανάπτυξη τόσο σε επιχειρήσεις όσο και σε ερευνητικά κέντρα και Πανεπιστήμια,
- την δημιουργία θεσμικού πλαισίου που ευνοεί την εφαρμογή καινοτόμων τεχνολογιών στην οικονομία
- την δημιουργία οικονομικών κινήτρων (επιδοτήσεις, φοροαπαλλαγές).

Σύμφωνα με στοιχεία της Eurostat για το 2017 και σχετική μελέτη της Alphabank, βλ. σχετικά [78], η παραγωγικότητα μιας χώρας, συνδέεται άμεσα με τις επενδύσεις σε έρευνα και ανάπτυξη. Χώρες που επενδύουν σε έρευνα και ανάπτυξη παρουσιάζουν μεγαλύτερη παραγωγικότητα, όπως φαίνεται και στο παρακάτω γράφημα.



Εικόνα 3.1 - Σχέση παραγωγικότητας και καινοτομίας – Πηγή: Eurostat

Η Ελλάδα είναι σε χαμηλότερα επίπεδα σε δαπάνες για Έρευνα και Ανάπτυξη (ως ποσοστό του ΑΕΠ) σε σχέση με τον μέσο όρο της ΕΕ. Η αύξηση των επενδύσεων για Έρευνα και Ανάπτυξη καθώς και η επιχειρηματική καινοτομία, θα αύξανε μέσω της διάχυσης της τεχνολογίας, καταλυτικά την παραγωγικότητα της εργασίας και θα έδινε συγκριτικό πλεονέκτημα στις ελληνικές επιχειρήσεις.

Επομένως, υπό τις παραπάνω προϋποθέσεις η τεχνολογία Blockchain, μπορεί να αποτελέσει εργαλείο οικονομικής ανάπτυξης. Ειδικά στην περίπτωση της Ελλάδας μπορεί να αποτελέσει λύση, σε προβλήματα που δημιούργησε η πρόσφατη οικονομική κρίση και η μακροχρόνια ύφεση. Αποτέλεσμα της οικονομικής κρίσης και της παρατεταμένης περιόδου οικονομικής ύφεσης στην Ελλάδα, ήταν η μεγάλη αύξηση του ποσοστού ανεργίας. Τα υψηλά ποσοστά ανεργίας, είχαν σαν αποτέλεσμα την εμφάνιση των φαινομένων brain drain και brain waste.

Brain drain

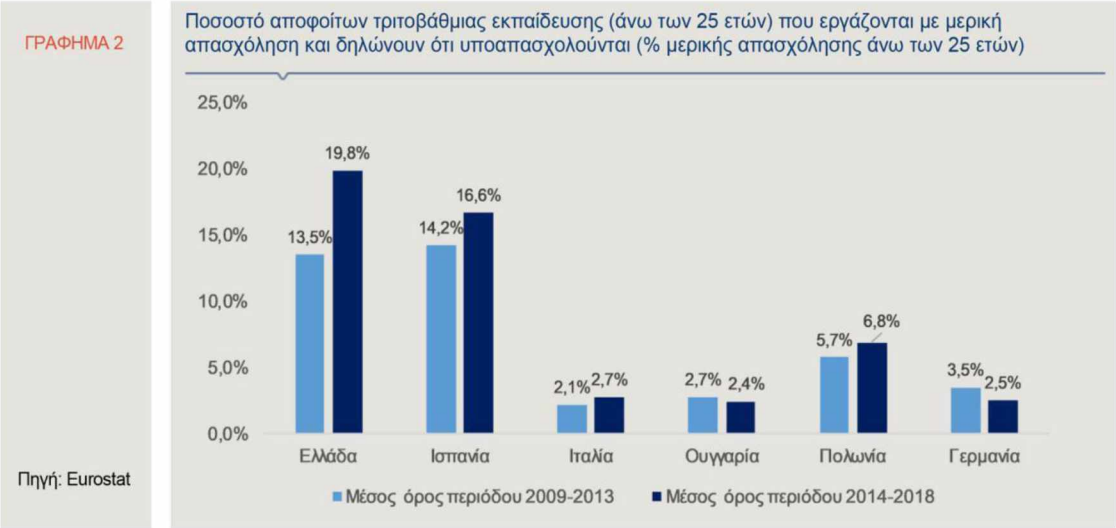
Ως brain drain ορίζουμε την διαρκή «αιμορραγία» επιστημονικού δυναμικού, με σκοπό την εξασφάλιση καλύτερων συνθηκών διαβίωσης. Σύμφωνα με έρευνα της ΕΛΣΤΑΤ, ολοένα και περισσότεροι Έλληνες κάτω των 25 ετών επιλέγουν να μεταναστεύσουν για να αναζητήσουν καλύτερες ευκαιρίες ώστε να ανελιχθούν και να εξελιχθούν τόσο ακαδημαϊκά όσο και επαγγελματικά. Τα μεγαλύτερα ποσοστά σημειώνονται στις ηλικίες 20 – 29, γεγονός που δείχνει πως τα νέα μυαλά της Ελλάδας «στραγγίζονται» συνεχώς.

Εικόνα 3.2 - Το «brain drain» σε γράφημα – Πηγή: ΕΛΣΤΑΤ,Eurostat

Τα επίσημα στατιστικά στοιχεία για το ενεργό εργατικό δυναμικό στην Ελλάδα αποτυπώνουν σε μεγάλο βαθμό τις επιπτώσεις του brain drain στην αγορά εργασίας..

Brain waste

Ως brain waste ορίζουμε την υποαπασχόληση του εργατικού δυναμικού με υψηλά προσόντα (απόφοιτους τριτοβάθμιας εκπαίδευσης) σε θέσεις εργασίας χαμηλής εξειδίκευσης και σε θέσεις ακούσιας μερικής απασχόλησης.



Εικόνα 3.3 - Το «brain waste» σε γράφημα – Πηγή : Eurostat

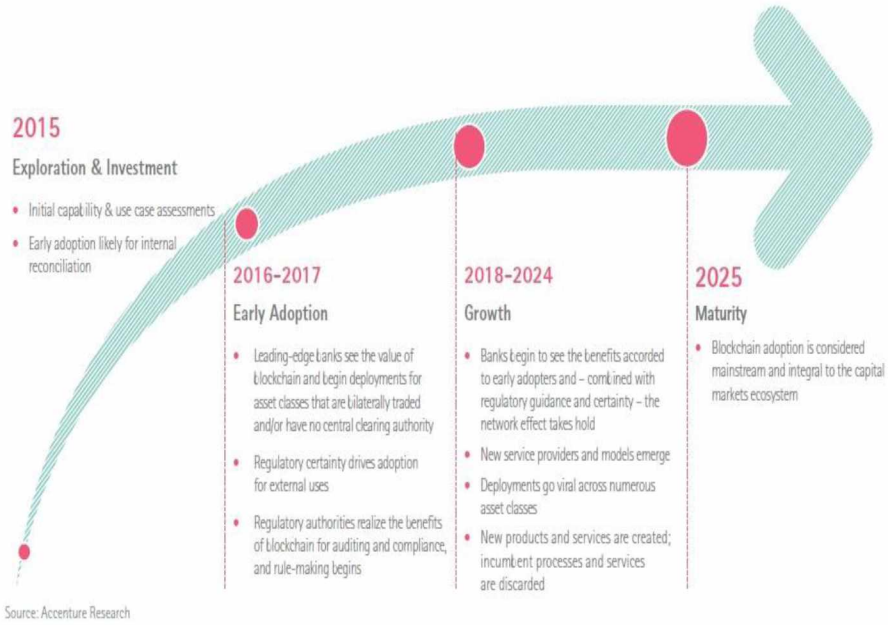
Σύμφωνα με έρευνα της Eurostat, κατά το χρονικό διάστημα 2014-2019 το ποσοστό των Ελλήνων αποφοίτων τριτοβάθμιας εκπαίδευσης (άνω των 25 ετών), που εργάζονται με μερική απασχόληση και δηλώνουν ότι υποαπασχολούνται, αυξήθηκε σε σχέση με την προηγούμενη 4ετία και πλέον ανέρχεται σε 19,8%.

Η ανάπτυξη εφαρμογών τεχνολογίας blockchain και η χρήση τους στην οικονομία και παραγωγική διαδικασία, θα μπορούσε να οδηγήσει σε οικονομική ανάπτυξη την χειμαζόμενη ελληνική οικονομία, μειώνοντας την ανεργία και τα φαινόμενα brain drain και brain waste, αφού θα δημιουργούσε νέες θέσεις εργασίας (τόσο στον τομέα της έρευνας και ανάπτυξης, όσο και στον πρωτογενή, δευτερογενή και τριτογενή τομέα) και θα απαιτούσε ανθρώπινο δυναμικό «υψηλών προδιαγραφών».

Εκτίμηση αποδοχής και υιοθέτησης της τεχνολογίας Blockchain

Σε αυτή την ενότητα θα προσπαθήσουμε να κάνουμε μια εκτίμηση του βαθμού αποδοχής και υιοθέτησης (adoption stage) της νέας τεχνολογίας blockchain, σε διάφορους τομείς της οικονομίας και της κοινωνίας σήμερα και στα επόμενα χρόνια.

Σύμφωνα με το Accenture's maturity model, βλ. σχετικά [36], αλλά και τον Gartner's 2015 Hype Cycle for Emerging Technologies, βλ. σχετικά [65], σχετικά με την αποδοχή/υιοθέτηση της τεχνολογίας blockchain από φορείς της κοινωνίας/οικονομίας, μέχρι το 2025 η τεχνολογία blockchain θα φτάσει σε στάδιο ωριμότητας. Αυτό σημαίνει ότι σήμερα βρισκόμαστε σε στάδιο ανάπτυξης (growth) της τεχνολογίας blockchain.



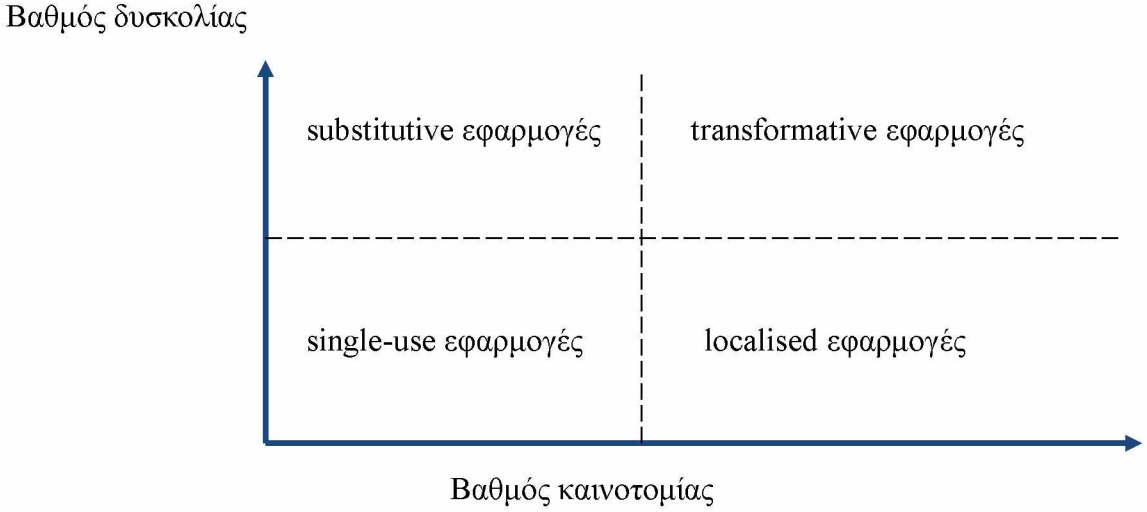
Εικόνα 3.4 - Εκτίμηση βαθμού αποδοχής της τεχνολογίας Blockchain σύμφωνα με Accenture's maturity model

Σύμφωνα με τους Iansiti και Lakhani (2017), μπορεί να γίνει εκτίμηση της αποδοχής της τεχνολογίας blockchain σε διάφορους τομείς της οικονομίας από τις επιχειρήσεις, βασιζόμενοι στην υπόθεση ότι η υιοθέτηση κάθε νέας τεχνολογίας εξαρτάται από το βαθμό της καινοτομίας που εισάγει, καθώς και από το βαθμό δυσκολίας (πολυπλοκότητας και του συντονισμού) που απαιτεί η υιοθέτηση και η υλοποίηση της, από τις επιχειρήσεις.

Οι νέες τεχνολογίες υιοθετούνται από τις επιχειρήσεις σε 4 στάδια:

- Απλή χρήση (Single use),
- περιορισμένη χρήση (localisation),
- χρήση ως υποκατάσταστο άλλης τεχνολογίας (substitution),

πλήρης αποδοχή και συνολικός μετασχηματισμός της επιχείρησης (transformation).



Εικόνα 3.5 – Συσχέτιση βαθμού δυσκολίας και καινοτομίας μια νέας τεχνολογίας

Κάθε στάδιο απαιτεί διαφορετικό επίπεδο συντονισμού και πολυπλοκότητας και εισάγει διαφορετικό βαθμό καινοτομίας.

- **Single-Use** - Οι single-use εφαρμογές είναι περισσότερο κατάλληλες για αρχική υιοθέτηση της τεχνολογίας. Εμπεριέχουν χαμηλό ρίσκο και μικρό βαθμό πολυπλοκότητας, αλλά δεν είναι ιδιαίτερα καινοτόμες.
- **Localisation** - Οι localised εφαρμογές είναι καινοτόμες. Εμπεριέχουν χαμηλό ρίσκο και μικρό βαθμό πολυπλοκότητας και αποτελούν το επόμενο βήμα μιας single-use εφαρμογής της τεχνολογίας.
- **Substitution** - Οι substitutive εφαρμογές αλλάζουν τον τρόπο σκέψης των στελεχών της επιχείρησης, δεν είναι ιδιαίτερα καινοτόμες αλλά περιέχουν υψηλό βαθμό πολυπλοκότητας. Συνήθως αντικαθιστούν διαδικασίες λήψης αποφάσεων και ενεργειών από μια επιχείρηση, που προκύπτουν από μια single-use ή localised εφαρμογή της νέας τεχνολογίας.
- **Transformation** - Οι transformative εφαρμογές είναι ιδιαίτερα καινοτόμες και περιέχουν υψηλό βαθμό πολυπλοκότητας και συντονισμού, αφού συνήθως απαιτούν αλλαγές και σε κοινωνικό, νομικό και πολιτικό επίπεδο. Αλλάζει συνολικά ο τρόπος λειτουργίας της επιχείρησης από μια τέτοια εφαρμογή της νέας τεχνολογίας.

Με βάση τα παραπάνω, οι Iansiti και Lakhani (2017), βλ. σχετικά [35], εκτιμούν ότι πιθανά στην περίπτωση του Blockchain δεν θα έχουμε κάποια «τεχνολογική επανάσταση», αλλά μια σταδιακή και ομαλή υιοθέτηση της τεχνολογίας αυτής.

Κόστη υιοθέτησης της τεχνολογίας Blockchain

• Το κόστος υλικού (Hardware cost)

Αυτά τα έξοδα σχετίζονται με το πρόσθετο υλικό (hardware) που ενδεχομένως χρειάζεται πάνω από το υπάρχον υλικό στον οργανισμό/εταιρεία.

• Το κόστος λογισμικού (Software cost)

Αυτές οι δαπάνες σχετίζονται με το επιπλέον λογισμικό που ενδεχομένως χρειάζεται επιπλέον του υφιστάμενου στον οργανισμό/εταιρεία.

• Το κόστος εφαρμογής (System implementation cost)

Αυτή η κατηγορία περιλαμβάνει το κόστος ανάπτυξης ή παραμετροποίησης του blockchain για τον συγκεκριμένο οργανισμό/εταιρεία.. Δαπάνες που αφορούν την ασφάλεια του συστήματος, πρέπει να προστεθούν εδώ.

• Κόστος λειτουργίας (Operational cost)

Το λειτουργικό κόστος αφορά το κόστος των πόρων (resources) που διατίθενται για την λειτουργία ολόκληρου του blockchain.

• Κόστος συντήρησης (Maintenance cost)

Το κόστος συντήρησης είναι το κόστος που απαιτείται για τη διατήρηση ολόκληρου του blockchain.

Οι κρίσιμοι παράγοντες για τον προσδιορισμό αυτών των δαπανών είναι:

• Το μέγεθος του οργανισμού/εταιρείας και

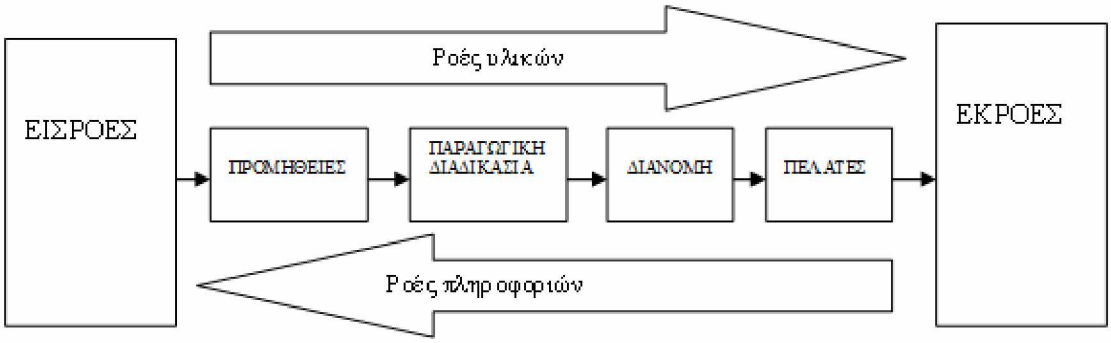
• Το εύρος υιοθέτησης της τεχνολογίας blockchain, στις διαδικασίες του οργανισμού/εταιρείας.

ΚΕΦΑΛΑΙΟ 4 - BLOCKCHAIN ΚΑΙ ΕΦΟΔΙΑΣΤΙΚΕΣ ΑΛΥΣΙΔΕΣ

Τι είναι η εφοδιαστική αλυσίδα και τα Logistics

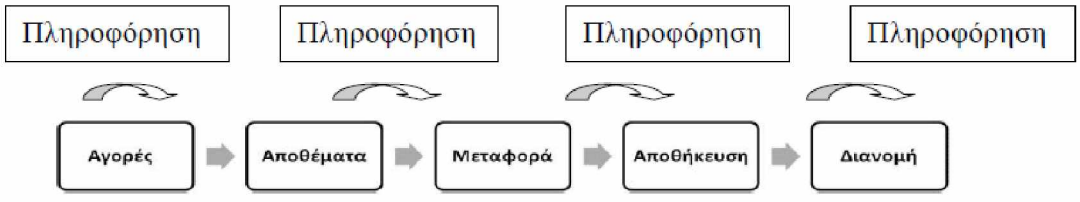
Σύμφωνα με τους Bozarth, Cecil, Handfield και Robert (2006), βλ. σχετικά [37], μια αλυσίδα εφοδιασμού (supply chain) είναι ένα δίκτυο κατασκευαστών, παραγωγών και παρόχων υπηρεσιών που συνεργάζονται για τη δημιουργία προϊόντων ή υπηρεσιών που χρειάζονται οι τελικοί χρήστες.

Σύμφωνα με την Σαρτζετάκη (2103), βλ. σχετικά [56], η «εφοδιαστική» ως επιστήμη στην οποία εντάσσεται η έννοια των Logistics, περιλαμβάνει τη διακίνηση και διαχείριση των προϊόντων από την παραγωγή έως την κατανάλωση με το μικρότερο δυνατό κόστος. Η ανάγκη γι' αυτό εντάθηκε από την ανάπτυξη ανταγωνιστικών συνθηκών μεταξύ των επιχειρήσεων στο να παράγουν ανταγωνιστικά προϊόντα (ποιότητα, τιμές, λειτουργικότητα) καθώς και υπηρεσίες εξυπηρέτησης των πελατών – καταναλωτών.



Εικόνα 4.1 - Οι βασικές διαδικασίες μιας αλυσίδας εφοδιασμού

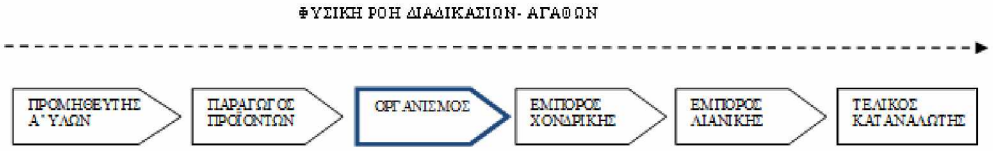
Σύμφωνα με την Σαρτζετάκη (2103), βλ. σχετικά [56], ως logistics νοείται η διαδικασία διαχείρισης των διαδικασιών που σχετίζονται με τη εφοδιαστική αλυσίδα και ολόκληρο το πλέγμα αλληλεξαρτήσεων έτσι, ώστε να υπάρχει σύνδεση μεταξύ σχεδιασμού και του συντονισμού της ροής υλικών.



Εικόνα 4.2 - Οι βασικές λειτουργίες των Logistics

Παράγοντες και ρόλοι σε μια εφοδιαστική αλυσίδα

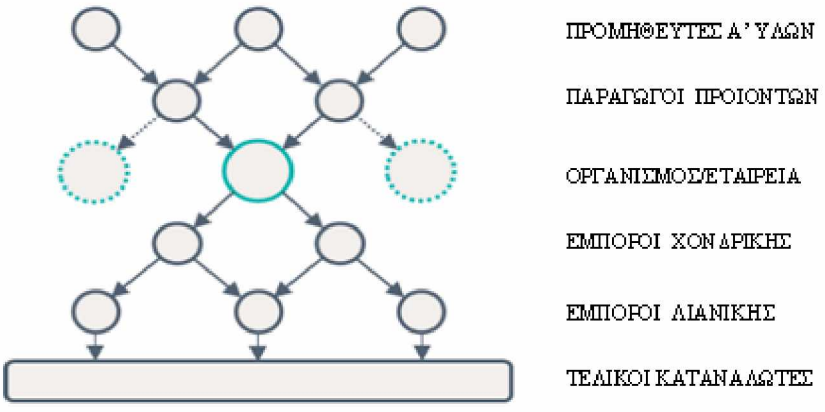
Σύμφωνα με τους Jansson kai Petersen (2017), βλ. σχετικά [38], οι παράγοντες μιας λιανικής αλυσίδας εφοδιασμού συνδέονται μεταξύ τους μέσω της φυσικής ροής προϊόντων από τους παραγωγούς στους τελικούς καταναλωτές.



Εικόνα 4.3 - Ρόλοι σε μια αλυσίδα εφοδιασμού

Οι πραγματικές σχέσεις όμως, μεταξύ των φορέων/ρόλων που συμμετέχουν στην αλυσίδα, είναι συχνά πιο περίπλοκες από το παραπάνω σχήμα.

Σύμφωνα με τους Jansson και Petersen (2017), βλ. σχετικά [38], οι οργανισμοί έχουν κατά κανόνα πολλούς προμηθευτές σε διαφορετικές βαθμίδες που συμμετέχουν σε ένα συγκεκριμένο προϊόν και οι προμηθευτές είναι συνήθως μη αποκλειστικοί για τον οργανισμό που εξετάζεται. Το αποτέλεσμα είναι ένα σύνθετο δίκτυο αλληλένδετων φορέων και ρόλων, όπως παρουσιάζεται στην παρακάτω εικόνα.



Εικόνα 4.4 - Μια σύνθετη αλυσίδα εφοδιασμού

Η σημασία της ιχνηλασιμότητας (traceability) στις εφοδιαστικές αλυσίδες

Στο σημερινό παγκοσμιοποιημένο σύστημα εμπορίου, οι αλυσίδες εφοδιασμού καθίστανται όλο και πιο σύνθετες και η ανίχνευση (tracing) αντικειμένων/προϊόντων είναι δύσκολη. Επομένως η ιχνηλασιμότητα ή ανιχνευσιμότητα (traceability) είναι κρίσιμο θέμα σε μια αλυσίδα εφοδιασμού.

Σύμφωνα με διάφορες πηγές της βιβλιογραφίας ανάλογα με τον τομέα εφαρμογής, υπάρχουν διάφοροι ορισμοί της ιχνηλασιμότητας από οργανισμούς, νομοθεσίες ή ερευνητές. Σε γενικές γραμμές θα λέγαμε ότι, η ιχνηλασιμότητα ορίζεται ως η παρακολούθηση της ροής αντικειμένων/προϊόντων /πληροφοριών. Η ιχνηλασιμότητα στα τρόφιμα αφορά πληροφορίες που έχουν να κάνουν με την προέλευση και την παραγωγή τους, την ημερομηνία παραγωγής και λήξης, την επεξεργασία τους, τον τρόπο αποθήκευσης και διανομή τους. Ένα σύστημα ιχνηλασιμότητας σε μια εφοδιαστική αλυσίδα, δημιουργεί για κάθε προϊόν μια ταυτότητα, σε όλα τα παραπάνω στάδια παραγωγής και διακίνησης. Η ταυτότητα του κάθε προϊόντος, καταγράφεται πάνω στο προϊόν με τη χρήση ενός κωδικού (Barcode,QRcode), ή τη χρήση μιας κάρτας RFID.

Βασικές έννοιες σχετικά με την ιχνηλασιμότητα προϊόντων

Σύμφωνα με τους Aung και Chang (2014), Bechini et al (2008), Golan et al (2004) και άλλες πηγές, υπάρχουν διάφορες παράμετροι και χαρακτηριστικά που αναφέρονται σε ένα σύστημα ιχνηλασιμότητας.

Παρακολούθηση και εντοπισμός

Σύμφωνα με τους Aung και Chang (2014), βλ. σχετικά [39], η ιχνηλασιμότητα μπορεί να χωριστεί στην ικανότητα παρακολούθησης (tracing) και στην ικανότητα εντοπισμού (tracking). Η παρακολούθηση ή η ιχνηλασιμότητα προς τα εμπρός (forward tracking) είναι η διαδικασία εύρεσης της θέσης ενός αντικειμένου από ένα δεδομένο κριτήριο. Ο εντοπισμός ή ιχνηλασιμότητα προς τα πίσω (backward tracking) είναι η διαδικασία εύρεσης στοιχείων ή χαρακτηριστικών από ένα δεδομένο κριτήριο.

Σύμφωνα με τους Kumari et al (2014), βλ. σχετικά [46], η ικανότητα παρακολούθησης επιτρέπει την αποτελεσματική ανάκληση μη συμμορφούμενων αντικειμένων, ενώ ο εντοπισμός είναι απαραίτητος για την εύρεση της αιτίας της μη συμμόρφωσης.

Είναι σημαντικό το σύστημα ιχνηλασιμότητας να μπορεί να εντοπίζει και να παρακολουθεί, καθώς ο αποτελεσματικός εντοπισμός δεν συνεπάγεται αποτελεσματική παρακολούθηση και αντίστροφα.

Μονάδα Ανιχνεύσιμων Πόρων

Σύμφωνα με το πρότυπο GS1 (2012), βλ. σχετικά [41], η μονάδα ανιχνεύσιμων πόρων (Traceable Resource Unit - TRU) είναι μια μονάδα με μοναδικό αναγνωριστικό που μπορεί να ανιχνευθεί ή να ανιχνευθεί σε μια αλυσίδα εφοδιασμού,. Το TRU διαφέρει ανάλογα με τη βιομηχανία και το προϊόν, και μπορεί να έχει διαφορετικά χαρακτηριστικά σε διάφορα στάδια της αλυσίδας εφοδιασμού.

Στο υψηλότερο επίπεδο, το TRU θα μπορούσε να είναι πλοίο μεταφοράς εμπορευματοκιβωτίων. Στο πιο χαμηλό επίπεδο, το TRU είναι το αντικείμενο που διασχίζει το σημείο πώλησης (Point of Sale - PoS) στον καταναλωτή.

Τα TRU μπορούν να χωριστούν στους παρακάτω τύπους:

- Μονάδα παρτίδας, ένα σύνολο στοιχείων που έχει υποβληθεί στις ίδιες διαδικασίες
- Εμπορική μονάδα, η μονάδα που διεξάγεται μεταξύ δύο μερών σε μια αλυσίδα εφοδιασμού
- Μονάδα εφοδιαστικής, μια διοικητική ομάδα αντικειμένων (π.χ. παλέτα ή δοχείο)

Εγγενώς, μια μονάδα παρτίδας μπορεί να είναι μια εμπορική μονάδα, μια μονάδα αποθήκευσης θα μπορούσε να αποτελείται από άλλες μονάδες υλικοτεχνικής υποστήριξης κ.λπ. Οποιοδήποτε στοιχείο εκτός των τριών παραπάνω τύπων μπορεί να είναι ένα TRU αν οι εταίροι ιχνηλασιμότητας συμφωνούν να θεωρήσουν ότι είναι ανιχνεύσιμο στοιχείο. Μια ανιχνεύσιμη εμπορική μονάδα μπορεί είτε να διασχίσει τον PoS στον καταναλωτή (π.χ. μία μονάδα καταναλωτή) είτε να μην διασχίσει το PoS (π.χ. ένα πακέτο πολλών καταναλωτικών μονάδων).

Εσωτερική, εξωτερική και ιχνηλασιμότητα αλυσίδας

Σύμφωνα με τους Jansson και Petersen (2017), βλ. σχετικά [38], αλλά και λοιπές πηγές της βιβλιογραφίας, η ιχνηλασιμότητα μπορεί να κατηγοριοποιηθεί σε δύο μέρη,:

- Εσωτερική ιχνηλασιμότητα και
- εξωτερική ιχνηλασιμότητα.

Μια οντότητα αλυσίδας εφοδιασμού παράγει εσωτερική ιχνηλασιμότητα (internal traceability), όταν επεξεργάζονται αντικείμενα εισόδου που επεξεργάζονται σε ανιχνεύσιμα αντικείμενα εξόδου.

Η εξωτερική ιχνηλασιμότητα(external traceability), επιτυγχάνεται όταν πραγματοποιείται μια συναλλαγή ενός ανιχνεύσιμου αντικειμένου μεταξύ δύο οντοτήτων.

Η πλήρης ιχνηλασιμότητα της αλυσίδας (chain traceability) επιτυγχάνεται όταν ολόκληρη η αλυσίδα εφοδιασμού μιας πληροφορίας αντικειμένου ανταλλάσσει και παρέχει εσωτερική και εξωτερική ιχνηλασιμότητα.

Εύρος, βάθος και ακρίβεια ενός συστήματος ιχνηλασιμότητας

Σύμφωνα με τους Golan et al (2004), βλ. σχετικά [45], τα συστήματα ιχνηλασιμότητας ποικίλλουν σε εύρος (breadth), βάθος (depth) και ακρίβεια (precision),.

Το εύρος ή πλάτος είναι το ποσό των πληροφοριών που συλλέγονται σε όλο το σύστημα. Οι πληροφορίες που συλλέγονται συνίστανται σε οτιδήποτε μετρήσιμο, όπως το βάρος, οι διαστάσεις ή το χρώμα του TRU, ή οποιαδήποτε πληροφορία σχετικά με το ανιχνεύσιμο γεγονός. Σε ένα στοιχείο μπορεί να προστεθούν νέα χαρακτηριστικά ή να χαθούν παλιά χαρακτηριστικά κατά μήκος της αλυσίδας.

Το βάθος του συστήματος είναι ένα μέτρο για το πόσο πίσω το σύστημα παρακολουθεί τα χαρακτηριστικά ενός στοιχείου. Το πλάτος του συστήματος συχνά δημιουργεί προϋποθέσεις για το βάθος του συστήματος.

Η ακρίβεια ενός συστήματος είναι ο βαθμός στον οποίο το σύστημα μπορεί να αναγνωρίσει ένα συγκεκριμένο TRU.

Σύμφωνα με το πρότυπο GS1 (2012), βλ. σχετικά [41], ως ακρίβεια θεωρείται η ικανότητα μονοσήμαντης ταυτοποίησης ενός αντικειμένου, ενώ το επίπεδο στην υλικοτεχνική ιεραρχία αναφέρεται στη λεπτομέρεια του υπό εξέταση αντικειμένου. Με αυτή τη διάκριση, μια μεγάλη αποστολή μπορεί να έχει υψηλή ακρίβεια και χαμηλή λεπτομέρεια αλλά όχι αντίστροφα.

Σύμφωνα με τους Jansson και Petersen (2017), βλ. σχετικά [38], το πλάτος, το βάθος και η ακρίβεια του συστήματος είναι εγγενώς συνδεδεμένα. Η διαρροή κάθε παραμέτρου αυξάνει την ποσότητα πληροφοριών που καταγράφονται στο σύστημα και πρέπει να αξιολογείται με βάση την αποτελεσματικότητα. Η τήρηση αρχείων σχετικά με το υπερβολικό εύρος, το βάθος και την ακρίβεια είναι δαπανηρή και θα πρέπει να εξετάζεται μόνο εάν δημιουργεί οικονομική απόδοση ή απόδοση. Αντίθετα, η έκταση του συστήματος πρέπει να βασίζεται στον στόχο του συστήματος.

Δεδομένα ιχνηλασιμότητας

Σύμφωνα με το πρότυπο GS1 (2012), βλ. σχετικά [41], τα δεδομένα ιχνηλασιμότητας (Traceability Data) μπορούν να ταξινομηθούν σε κυρίως δεδομένα και δεδομένα συναλλαγών.

- Τα κυρίως δεδομένα (master data) είναι συνεπή με την πάροδο του χρόνου και περιέχουν γενικές πληροφορίες σχετικά με το TRU. Αυτό περιλαμβάνει πρακτικές πληροφορίες όπως ονόματα κόμματος, διευθύνσεις, πληροφορίες επικοινωνίας και γενικά χαρακτηριστικά του TRU, όπως διαστάσεις, βάρος, αριθμός μοντέλου και προδιαγραφές προϊόντος.
- Τα δεδομένα συναλλαγών (transactional data) δημιουργούνται από διεργασίες και συμβάντα και περιλαμβάνουν μεταβλητές πληροφορίες, όπως πληροφορίες διεργασίας ή γεγονότος, πληροφορίες αποστολής, χρονικές σφραγίδες και πληροφορίες μονάδας εφοδιαστικής.

Τα δεδομένα ιχνηλασιμότητας μπορούν επίσης να είναι ιδιωτικά (private) ή δημόσια (public).

- Τα δημόσια δεδομένα αναφέρονται στα δεδομένα που μοιράζονται όλα τα μέρη στο σύστημα ιχνηλασιμότητας.

- Τα ιδιωτικά δεδομένα αποθηκεύονται μόνο σε ένα ή σε ορισμένα μέρη. Συνήθως αποτελούνται από πιο λεπτομερείς πληροφορίες, όπως η προέλευση των πρώτων υλών, η ποιότητα των αντικειμένων ή τα αποτελέσματα από την ανάλυση αντικειμένων.

Κεντρικό και αποκεντρωμένο μοντέλο

Σύμφωνα με τους Bechini et al (2008), βλ. σχετικά [44], υπάρχουν δύο μοντέλα συστημάτων ιχνηλασιμότητας:

- Ένα κεντρικό μοντέλο δεδομένων (centralized/push model) απαιτεί να μεταφέρονται όλα τα δεδομένα σε ένα σύστημα πληροφοριών ιχνηλασιμότητας και να αποθηκεύονται σε μία κεντρική τοποθεσία,
- Σε ένα μοντέλο αποκεντρωμένων δεδομένων (decentralized/pull model) τα δεδομένα αποθηκεύονται με μια κατανεμημένη αρχιτεκτονική. Συνήθως, ένα αποκεντρωμένο μοντέλο περιλαμβάνει έναν αξιόπιστο τρίτο, ο οποίος ενεργεί ως ενδιάμεσος στο σύστημα πληροφοριών. Ένα αποκεντρωμένο μοντέλο επιτρέπει στις οντότητες στο σύστημα ιχνηλασιμότητας να κατέχουν δεδομένα διαφορετικών δομών. Η διαλειτουργικότητα απαιτείται μόνο στην περίπτωση αλληλεπιδράσεων μεταξύ αποκεντρωμένων δεδομένων.

Βασικές αρχές ενός συστήματος ιχνηλασιμότητα σε αλυσίδες εφοδιασμού

Σύμφωνα με τους Olsen και Borit (2013), βλ. σχετικά [47], αλλά και το πρότυπο GS1 (2012), βλ. σχετικά [41], ένα σύστημα ιχνηλασιμότητας πρέπει να έχει τις παρακάτω ικανότητες ή να τηρεί τις παρακάτω αρχές:

Olsen και Borit (2013)	**πρότυπο GS1 (2012)**
Να ομαδοποιεί αντικείμενα ως TRUs	Να αναγνωρίζει και να ταυτοποιεί μοναδικά τα αντικείμενα
Να αναγνωρίζει και να ταυτοποιεί μοναδικά τα TRUs	Να καταγράφει σε αρχεία δεδομένα που αφορούν την ιχνηλασιμότητα
Να καταγράφει σε αρχεία τις διαδικασίες, σύμφωνα με τα μοναδικά αναγνωριστικά των TRUs	Να διαμοιράζει αυτά τα δεδομένα με όσους χρησιμοποιούν το σύστημα ιχνηλασιμότητας
Να έχει πρόσβαση στις καταγραμμένα αρχεία και πληροφορίες	Να συνδέει τα δεδομένα εισόδου με τα δεδομένα εξόδου

Εντοπισμός μονάδας (Unit Identifying)

Για να διαχωρίσετε επιτυχώς ένα TRU από το άλλο πρέπει να υπάρχει κάποιος τρόπος να τα διαφοροποιήσετε. Αυτό μπορεί να γίνει είτε προσθέτοντας πληροφορίες στην TRU είτε εξετάζοντας τα υπάρχοντα χαρακτηριστικά του TRU.

Παραδείγματα τεχνολογιών αναγνώρισης είναι:

α. Η ταυτοποίηση σειριακού αριθμού (Serial number identification)

Χρησιμοποιείται για την αναγνώριση ενός ευρέος φάσματος TRUs. Η GS1 έχει δημιουργήσει αρκετά πρότυπα για την μοναδική αναγνώριση αντικειμένων με διαφορετική ακρίβεια και λεπτομέρεια. Περιέχει πρότυπα όπως:

- Το GTIN (Global Trade Item Number). Το GTIN χρησιμοποιείται για την παροχή αριθμών αναγνώρισης στοιχείων, πακέτων και υπηρεσιών σε κοκκώδες επίπεδο.
- Το SSCC (Serial Shipper Container Code). Το SSCC είναι ένα πρότυπο για τον εντοπισμό μεγαλύτερων μονάδων εφοδιαστικής, που συχνά περιέχουν πολλές μικρότερες μονάδες TRU.
- Το GSIN (Global Identification Number). Το GSIN χρησιμοποιείται για τον εντοπισμό μιας ομάδας μονάδων εφοδιαστικής που αποτελούν μέρος της ίδιας αποστολής.

Σύμφωνα με το πρότυπο GS1 (2012), βλ. σχετικά [41], ο σειριακός αριθμός μπορεί να προσαρτηθεί στο φυσικό αντικείμενο με πολλούς τρόπους, όπως ένας γραμμωτός κώδικας (barcode), ένας δισδιάστατος γραμμωτός κώδικας (QR barcode) ή μια ετικέτα RFID (σ.σ οι ασύρματες κάρτες RFID (Radio frequency Identification), υποστηρίζουν την αποθήκευση και ασύρματη ανάκτηση δεδομένων μέσω μμικροσκοπικών συσκευών, τα ονομαζόμενα RFID tags ή transporders). Ο σειριακός αριθμός μπορεί να διαβαστεί με χρήση κατάλληλης συσκευής (scanner/reader).

β. Η αναγνώριση DNA (DNA identifying)

Αυτή η τεχνική αναγνωρίζει μια μονάδα μοναδικά από άλλους με δοκιμές DNA. Οι δοκιμές μπορούν να εκτελεστούν σε όλη την αλυσίδα για να καταγράψουν και να καταγράψουν δεδομένα. Ο έλεγχος DNA είναι δαπανηρός και αν και το DNA είναι αναμφισβήτητα επίμονο με την πάροδο του χρόνου, η επεξεργασία μονάδων με ένα μοναδικό DNA μπορεί μερικές φορές να βλάψει το DNA. Επομένως, η τεχνολογία έχει περιορισμούς όσον αφορά τόσο τη σύνδεση των δεδομένων.

γ. Τα λεπτομερή αρχεία (Detailed records)

Βασίζονται στη διατήρηση μιας λεπτομερούς περιγραφής που προσδιορίζει με μοναδικό τρόπο μια μονάδα. Αυτό απαιτεί η μονάδα να έχει διαστάσεις που μπορούν να τεκμηριωθούν με σημαντικές λεπτομέρειες, ότι καμία άλλη μονάδα αυτού του τύπου δεν έχει το ίδιο σύνολο διαστάσεων και ότι οι διαστάσεις είναι σταθερές με την πάροδο του χρόνου. Για παράδειγμα, οι τέσσερις παράγοντες ποιότητας ενός διαμαντιού (δηλαδή το χρώμα, η καθαρότητα, το κομμάτι και το βάρος σε καράτια θα μπορούσαν να περιγραφούν λεπτομερώς και να διατηρηθούν σε μια εγγραφή. Καθώς κανένα άλλο διαμάντι δεν έχει τις ίδιες διαστάσεις και οι διαστάσεις είναι σχεδόν αμετάβλητες, μπορεί κανείς να ισχυριστεί με υψηλό βαθμό βεβαιότητας ότι ένα συγκεκριμένο διαμάντι αντιστοιχεί σε ένα συγκεκριμένο μητρώο ενός διαμαντιού σε ένα ημερολόγιο.

Καταγραφή δεδομένων (Data Capturing)

Σύμφωνα με τους Aung και Chang (2014), βλ. σχετικά [39] αλλά και τους Jansson και Petersen (2017), βλ. σχετικά [38], όταν ένα αντικείμενο έχει υποβληθεί σε μια διαδικασία (επεξεργασία), πρέπει να υπάρχει κάποιος τρόπος να συνδεθεί η διαδικασία με το συγκεκριμένο αντικείμενο, δηλαδή να ληφθούν τα σχετικά δεδομένα.

Όταν η ταυτότητα ενός TRU φέρει ετικέτα με οπτικό κώδικα, όπως γραμμικό κώδικα (bar code) ή δισδιάστατο γραμμικό κώδικα (QR code), μπορεί να σαρωθεί με χειροκίνητους σαρωτές ή αυτοματοποιημένους σαρωτές σε κάθε ανιχνευόμενο συμβάν στην αλυσίδα εφοδιασμού. Με τη χρήση αυτής της τεχνολογίας, τα δεδομένα ιχνηλασιμότητας αποθηκεύονται στα εσωτερικά συστήματα, γεγονός που δημιουργεί την ανάγκη τεχνολογιών ανταλλαγής δεδομένων, εάν τα δεδομένα προορίζονται να μοιραστούν.

Αντί να ανιχνεύει ένα αντικείμενο και να καταγράφει τα σχετικά δεδομένα στο εσωτερικό σύστημα μιας εταιρείας, τα δεδομένα μπορούν να προσαρτηθούν στο αντικείμενο. Αυτό γίνεται συχνά στη βιομηχανία τροφίμων, όπου οι διαδικασίες χρονολογούνται στο αντικείμενο, γεγονός που καθιστά εύκολο τον προσδιορισμό της καλύτερης ημερομηνίας ενός προϊόντος. Οι συνημμένες πληροφορίες δεν είναι

απαραιτήτως χρονική σφραγίδα, αλλά μπορεί να είναι για παράδειγμα ένα δελτίο παράδοσης ή ένα αυτοκόλλητο, που σηματοδοτεί ότι το αντικείμενο έχει υποβληθεί σε συγκεκριμένη διαδικασία.

Τα ασύρματα δίκτυα αισθητήρων (WSN) μπορούν να χρησιμοποιηθούν για την ασύρματη λήψη πληροφοριών. Ένα WSN χρησιμοποιείται συνήθως σε συνδυασμό με τεχνολογία RFID. Αυτή η τεχνολογία μπορεί να βελτιώσει την αποτελεσματικότητα σε μια αλυσίδα εφοδιασμού, μειώνοντας τη χειρωνακτική εργασία Οι ετικέτες RFID εισάγουν επίσης τη δυνατότητα όχι μόνο να σαρώσουν δεδομένα, αλλά και να προσθέσουν νέα δεδομένα στο TRU. Τα μειονεκτήματα με την τεχνολογία RFID είναι ότι είναι δαπανηρή και ότι η αναγνωσιμότητα των ετικετών RFID μπορεί να μειωθεί με μέταλλα, γυαλί και υγρά.

Κοινή χρήση δεδομένων (Data Sharing)

Σύμφωνα με τους Aung και Chang (2014), βλ. σχετικά [39] αλλά και τους Jansson και Petersen (2017), βλ. σχετικά [38], μόλις σαρωθεί μια TRU και έχουν ληφθεί σχετικές πληροφορίες, οι πληροφορίες πρέπει να αποθηκευτούν κάπου.

Μια τεχνολογία κοινής χρήσης δεδομένων μπορεί να είναι οποιαδήποτε εφαρμογή ή σύνολα εφαρμογών που θα επιτρέπουν την αποθήκευση και την κοινοποίηση των δεδομένων ιχνηλασιμότητα μεταξύ των συμβαλλομένων. Σε περιπτώσεις εφαρμογών πολλαπλής ιχνηλασιμότητα, είναι απαραίτητη η χρήση παγκόσμιων προτύπων διαλειτουργικότητας για την επιτυχή επίτευξη ιχνηλασιμότητα της αλυσίδας.

Ορισμένες πληροφορίες μπορούν να αποθηκευτούν σε ιδιωτικούς διακομιστές ενώ άλλες πληροφορίες μοιράζονται μεταξύ ενός ή περισσοτέρων μερών στο σύστημα ιχνηλασιμότητας. Η GS1 έχει αναπτύξει αρκετά πρότυπα για την τεχνολογία ανταλλαγής δεδομένων ιχνηλασιμότητας, δύο από τα οποία είναι το GDSN και το EPCIS.

Σύμφωνα με το πρότυπο GS1 (2107b), βλ. σχετικά [48], το Δίκτυο Συγχρονισμού Δεδομένων GS1 (Global Data Synchronization Network - GDSN) χρησιμοποιεί ένα δίκτυο ομάδων δεδομένων που επιτρέπουν στους συνεργαζόμενους χρήστες, να

συγχρονίζουν με ασφάλεια τα βασικά δεδομένα. Η τεχνολογία είναι ιδιαίτερα χρήσιμη για την ανταλλαγή των πιο πρόσφατων πληροφοριών σχετικά με τα βασικά δεδομένα της TRU σε μια αλυσίδα εφοδιασμού, όπως για παράδειγμα όλες οι πρώτες ύλες που χρησιμοποιούνται σε ένα προϊόν. Με αυτόν τον τρόπο, οι τελευταίες πληροφορίες σχετικά με ένα προϊόν μπορούν να παραδοθούν με εμπιστοσύνη από έναν έμπορο λιανικής πώλησης στον καταναλωτή. Βοηθά επίσης όλα τα μέρη στην αλυσίδα εφοδιασμού να προβλέπουν και να προσαρμόζονται στις αλλαγές στις φυσικές διαστάσεις ενός TRU.

Σύμφωνα με το πρότυπο GS1 (2017c), βλ. σχετικά [49], οι ηλεκτρονικές υπηρεσίες πληροφοριών κώδικα προϊόντων (EPCIS) είναι ένα πρότυπο που αναπτύχθηκε για να επιτρέπει στα μέρη να ανταλλάσσουν πληροφορίες σχετικά με τη φυσική κίνηση και την κατάσταση των προϊόντων καθώς ταξιδεύουν σε όλη την αλυσίδα εφοδιασμού. Χρησιμοποιώντας αυτό το πρότυπο, όλα τα συναλλακτικά γεγονότα στην αλυσίδα εφοδιασμού θα πρέπει να καταγράφονται με πληροφορίες σχετικά με το τι, πού, ποιος και γιατί συνέβη ένα γεγονός. Αυτό το πρότυπο αποσκοπεί στη δημιουργία μιας κοινής προβολής σχετικά με το πού και το πότε (χρονική στιγμή) βρίσκεται ένα προϊόν. Μπορεί επίσης να χρησιμοποιηθεί για να αντλήσει δεδομένα πραγματικού χρόνου μιας τοποθεσίας της TRU, επιτρέποντας την αναμονή των χρόνων άφιξης.

Σύνδεση δεδομένων εισόδου με δεδομένα εξόδου (Linking Input- to Output Data)

Όταν ένα προϊόν υποβάλλεται σε επεξεργασία από μια εταιρεία στην αλυσίδα εφοδιασμού, η είσοδος TRU (s) ενδέχεται να μην είναι η ίδια με την έξοδο TRU (s). Οι τρεις προηγούμενες πτυχές σχετίζονται γενικά με την εξωτερική ιχνηλασιμότητα , ενώ η πτυχή αυτή σχετίζεται περισσότερο με την εσωτερική ιχνηλασιμότητα. Για να διατηρηθεί η ιχνηλασιμότητα ενός αντικειμένου μέσω μιας τέτοιας διαδικασίας μέσα σε μια επιχείρηση, πρέπει να περιγραφούν και να καταγραφούν οι λεπτομέρειες της διαδικασίας.

Εσωτερικές διαδικασιών θα μπορούσε να είναι η συσκευασία (χύμα) προϊόντων, η απόψυξη προϊόντων, η κατεργασία προϊόντων κ.λ.π.

Με τον εντοπισμό και την περιγραφή των εσωτερικών διαδικασιών, οι εταιρείες

μπορούν να διατηρήσουν την εσωτερική ιχνηλασιμότητά τους και να παράσχουν στην υπόλοιπη αλυσίδα εφοδιασμού επαρκείς πληροφορίες για την ανίχνευση της εξωτερικής και της αλυσίδας. Η σύνδεση των δεδομένων εισόδου με τα δεδομένα εξόδου δεν σχετίζεται μόνο με την εσωτερική ιχνηλασιμότητα, αλλά μπορεί επίσης να περιλαμβάνει τη σύνδεση και την ευθυγράμμιση των δεδομένων μεταξύ των μερών ενός συστήματος ιχνηλασιμότητας.

Βασικοί στόχοι ενός συστήματος ιχνηλασιμότητα σε αλυσίδες εφοδιασμού

Σύμφωνα με τους Aung και Chang (2014), βλ. σχετικά [39] αλλά και τους Jansson και Petersen (2017), βλ. σχετικά [38], τέσσερεις είναι οι κύριοι στόχοι για την ιχνηλασιμότητα (Supply Chain Traceability) σε αλυσίδες εφοδιασμού:

1) καλύτερη διαχείριση της αλυσίδας εφοδιασμού,
2) διαφοροποίηση προϊόντων και διασφάλιση ποιότητας,
3) καλύτερη αναγνώριση και ανίχνευση μη συμμορφούμενων προϊόντων,
4) συμμόρφωση προς πρότυπα, κανονιστικές απαιτήσεις και προδιαγραφές.

Αναλύουμε παρακάτω το ζητούμενο κάθε στόχου.

Καλύτερη διαχείριση αλυσίδας εφοδιασμού

Ένα σύστημα ιχνηλασιμότητα μπορεί να χρησιμοποιηθεί για την παρακολούθηση και τη βελτίωση της ποιότητας των πρώτων υλών για τη μείωση του κόστους. Το σύστημα μπορεί να υποστηρίξει τη διαχείριση αποθεμάτων, η οποία, εκτός από τη μείωση του κόστους, θα μπορούσε τελικά να οδηγήσει σε διαφοροποίηση των προϊόντων μέσω μικρότερων χρόνων παράδοσης. Οι δυνατότητες ιχνηλασιμότητα μπορούν επίσης να παρέχουν αποτελεσματικότητα ή μείωση του κόστους της εργασίας μέσω στοχοθετημένων συστημάτων ανάκλησης. Επίσης βελτίωση της επικοινωνίας μεταξύ των φορέων που μετέχουν στην αλυσίδα, μεγαλύτερη διαφάνεια, διαλειτουργικότητα και ασφάλεια στην αλυσίδα εφοδιασμού οδηγούν σε καλύτερη συνολική διαχείριση της αλυσίδας εφοδιασμού.

Διασφάλιση ποιότητας προϊόντος

Σύμφωνα με τους Golan et al (2004), βλ. σχετικά [45], η ιχνηλασιμότητα μπορεί να χρησιμοποιηθεί για την διαφοροποίηση και την διασφάλιση της ποιότητας του προϊόντος, ειδικά όταν συγκεκριμένες ιδιότητες ποιότητας ενός προϊόντος είναι ήπια ή

δύσκολο να επαληθευτούν. Τέτοια χαρακτηριστικά ποιότητας μπορεί να είναι ότι ένα προϊόν προέρχεται από μια συγκεκριμένη περιοχή (ΠΟΠ π.χ. κεφαλογραβιέρα Αμφιλοχίας) ή παράγεται από μια ειδική μάρκα. Στο παγκοσμιοποιημένο εμπόριο, όταν το προϊόν δεν αγοράζεται απευθείας από την πηγή προέλευσής του, τέτοια χαρακτηριστικά καθίστανται ένα ζήτημα για την επαλήθευση. Η ιχνηλασιμότητα συμβάλλει στην άμβλυνση αυτών των ζητημάτων, με λεπτομερείς πληροφορίες σχετικά με τη διαδρομή του προϊόντος μέσω της αλυσίδας εφοδιασμού.

Δυνατότητα ανίχνευσης μη συμμορφούμενων με τις προδιαγραφές προϊόντων

Η δυνατότητα εντοπισμού και ανίχνευσης εμπορευμάτων σε οποιοδήποτε στάδιο της αλυσίδας εφοδιασμού, όταν δεν πληρούνται τα πρότυπα ποιότητας ή ασφάλειας αποτρέπει την διάθεση στην αγορά προϊόντων ελαττωματικών ή επικίνδυνων για την δημόσια υγεία και ασφάλεια και επιτρέπει αποτελεσματικές ανακλήσεις. Επίσης η δυνατότητα ανίχνευσης μη συμμορφούμενων με τις προδιαγραφές προϊόντων (πχ έξτρα παρθένο ελαιόλαδο) στην αλυσίδα εφοδιασμού, επιτρέπει επίσης την αποτελεσματική αναγνώριση της υποκείμενης αιτίας της μη συμμόρφωσης.

Πρότυπα και κανονισμοί για την ιχνηλασιμότητα

Σύμφωνα με τους Marucheck et al (2011), βλ. σχετικά [50], τα πρότυπα (Standards) είναι κανόνες ή απαιτήσεις που δεν προβλέπουν νομικές κυρώσεις σε περιπτώσεις μη συμμόρφωσης. Τα πρότυπα μπορούν να σχετίζονται με τις πιστοποιήσεις που εκδίδονται από οργανισμούς τυποποίησης, όπως ο Διεθνής Οργανισμός Τυποποίησης (ISO). Άλλα παραδείγματα οργανισμών τυποποίησης είναι το Σουηδικό Ινστιτούτο Προτύπων (SIS), η Fairtrade International (εκδότης πιστοποιητικών Fairtrade) και η GS1.

Οι κυβερνητικοί οργανισμοί θεσπίζουν κανονισμούς (Regulations) που ορίζουν βασικούς κανόνες και ευθύνες στην διαδικασία μιας εφοδιαστικής αλυσίδας. Οι οργανισμοί αυτοί συχνά έχουν την εξουσία να εκδίδουν κυρώσεις ή πρόστιμα σε περιπτώσεις μη συμμόρφωσης. Ένα παράδειγμα οργανισμού ρύθμισης είναι η Livsmedelsverket στη Σουηδία ή ο ΕΟΦ στην Ελλάδα.

ΚΕΦΑΛΑΙΟ 5 - BLOCKCHAIN ΚΑΙ ΑΓΡΟΔΙΑΤΡΟΦΙΚΟΣ ΤΟΜΕΑΣ

Στην ενότητα αυτή θα εξετάσουμε θέματα και προβλήματα του αγροδιατροφικού τομέα και τις δυνατότητες εφαρμογής της τεχνολογίας blockchain σε αυτό τον τομέα.

Ο αγροτικός τομέας στην παγκόσμια οικονομία

Ο αγροτικός τομέας αποτελεί βασικό πυλώνα της παραγωγής και της οικονομίας, ενώ ταυτόχρονα ανήκει στους τομείς που η τεχνολογία χρησιμοποιείται λιγότερο, με αποτέλεσμα βασικά προβλήματα να παραμένουν άλυτα μέχρι σήμερα. Πολλά από τα προβλήματα αφορούν:

- Στις απώλειες ενέργειας και μείωση της παραγωγής, λόγω της αδυναμίας λήψης κατάλληλων μέτρων και αποφάσεων σε πραγματικό χρόνο για τα προβλήματα που προκύπτουν (καιρικά φαινόμενα, ασθένειες κλπ).
- Στα μεγάλα κόστη σε όλα τα στάδια, από την παραγωγή, την μεταφορά, την αποθήκευση, την ασφάλιση και πώληση των αγροτικών προϊόντων.
- Στην αδυναμία παρακολούθησης της παραγωγής λόγω μεγάλων και απομακρυσμένων εκτάσεων.
- Στην έλλειψη εργαλείων για την λήψη αποφάσεων και την πιο αποτελεσματική κατανάλωση των πόρων (ενέργεια, λιπάσματα κλπ).

Τα τελευταία χρόνια όμως, χρησιμοποιούνται καινοτόμες λύσεις παγκοσμίως. Όπως και άλλοι τομείς της οικονομίας, έτσι και ο αγροτικός τομέας, είναι σε ένα στάδιο ψηφιακού μετασχηματισμού και χρησιμοποιούνται νέες τεχνικές και καινοτόμες τεχνολογίες (Smart Farming):

- Precision agriculture
- Site-specific crop management (SSM)
- Climate smart agriculture (CMA)
- Variable rate technology (VRT) for precise seeding
- Automation in smart greenhouses and food hubs
- Sensing technologies & IoT
- Smart decision and prediction platforms
- Big data & Data analytics

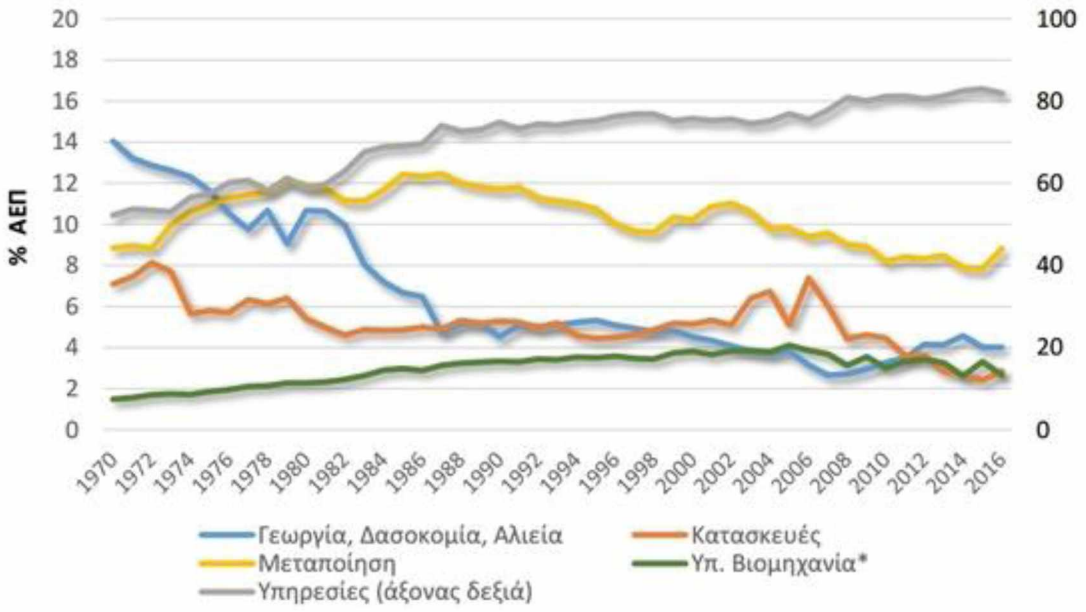
- Irrigation optimization and enhanced crop topology

Με την ενσωμάτωση καινοτόμων τεχνολογιών γεννιούνται νέες ευκαιρίες για προϊόντα και υπηρεσίες που έρχονται να φέρουν λύσεις και να απαντήσουν στις τεράστιες ανάγκες του αγροτικού τομέα (ο πληθυσμός της γης αναμένεται να φτάσει τα 9,6 δισεκατομμύρια το ως το 2050).

Ο αγροτικός τομέας εμπλέκεται σε ένα τεράστιο κομμάτι της παγκόσμιας οικονομίας, δημιουργώντας νέες δυνατότητες συνεργασίας με εταιρείες που παράγουν λύσεις και σε άλλους εμπλεκόμενους τομείς όπως fintech, smart cities, IoT λύσεις για real-time μετρήσεις (έδαφος, νερό, φως, υγρασία, θερμοκρασία κλπ) και dashboard για visualization, Blockchain λύσεις για βελτίωση του supply chain και των συναλλαγών, wallets, e-shops για αγροτικά προϊόντα κλπ.

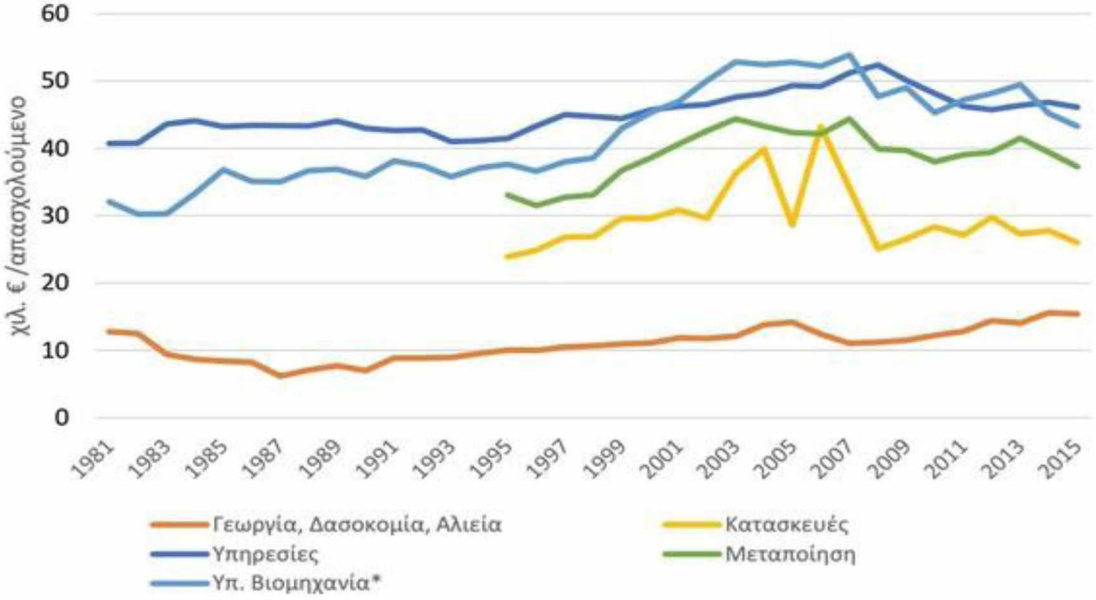
Ο αγροτικός τομέας στην Ελληνική οικονομία

Όπως προκύπτει από στοιχεία της ΕΛΣΤΑΤ και σύμφωνα με τον Γκόγκα (2017), βλ. σχετικά [75], η συμμετοχή του αγροτικού τομέα (ως ποσοστού) στο συνολικό ΑΕΠ της χώρας μας, μειώνεται σταδιακά από το 1970 μέχρι το 2010, ενώ εμφανίζεται να σταθεροποιείται τα τελευτία χρόνια.



Εικόνα 5.1 – Διαχρονική εξέλιξη του ελληνικού ΑΕΠ – Πηγή:ΕΛΣΤΑΤ

Επίσης, όπως προκύπτει από στοιχεία της ΕΛΣΤΑΤ και σύμφωνα με τον Γκόγκα (2017), βλ. σχετικά [75], η παραγωγικότητα του αγροτικού τομέα είναι χαμηλή σε σχέση με άλλους τομείς της ελληνικής οικονομίας.



Εικόνα 5.2 – Παραγωγικότητα αγροτικού τομέα – Πηγή:ΕΛΣΤΑΤ

Σύμφωνα με σχετική μελέτη του ΣΕΒ (2017), αλλά και σχετική μελέτη του ΔιαΝΕΟσις βλ. σχετικά [74], ο πρωτογενής τομέας στην Ελλάδα έχει μεγαλύτερο ποσοστό απασχόλησης και μεγαλύτερη προστιθέμενη αξία (σαν ποσοστό επί του ΑΕΠ), σε σχέση με το μέσο της ΕΕ. Ομοίως, όμως εμφανίζει χαμηλή παραγωγικότητα, χαμηλή προστιθέμενη αξία, μικρή διείσδυση σε ξένες αγορές και κατακερματισμό της παραγωγικής βάσης (εκτάρια/φάρμα, εκτάρια/μονάδα εργασίας).

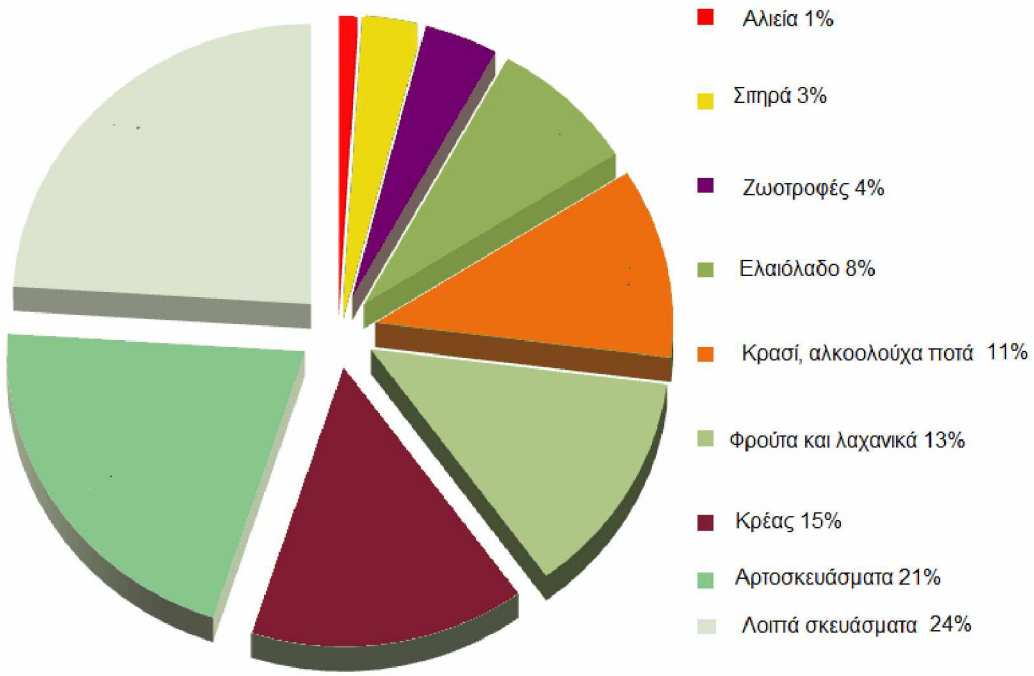
Ο Πρωτογενής Τομέας Στην Ευρώπη Και Την Ελλάδα

	Ελλάδα	ΕΕ
Ποσοστό (%) Απασχόλησης στον Πρωτογενή Τομέα	11,3%	4,5%
Απασχόληση στον πρωτογενή τομέα (% Πληθυσμού)	4,3%	2,0%
Επιδοτήσεις / Παραγωγή	27,4%	16,4%
Εκτάρια / Φάρμα	6,8	16,1
Ενεργητικό / Φάρμα (€)	130.020	327.198
Εκτάρια ανά μονάδα εργασίας	8	18
Ποσοστό (%) απασχόλησης σε φάρμες άνω των 30 εκταρίων	6,1%	22,3%
Ακαθάριστη προστιθέμενη αξία τομέα / ΑΕΠ	3,3%	1,4%
Προσθήκη αξίας από μεταποίηση	40%	70%

Πηγή: Αναδημοσίευση στοιχείων από τη μελέτη του ΣΕΒ (2017), διαθέσιμη εδώ: http://www.sev.org.gr/Uploads/Documents/50705/SPECIAL_REPORT_agro%202017_final.pdf

Εικόνα 5.3 – Ο πρωτογενή τομέας στην Ελλάδα και την ΕΕ – Πηγή: ΣΕΒ

Σύμφωνα με τον Γκέκα (2017), βλ. σχετικά [79], από δεδομένα που προέρχονται από στοιχεία του-Ευρωπαϊκού έργου AGROSTART "Διακρατικό δίκτυο για την υποστήριξη Μικρομεσαίων Επιχειρήσεων στον τομέα της κτηνοτροφίας και των οπωροκηπευτικών - AGRO-START», όσον αφορά τον αγροτικό τομέα η συνεισφορά της εκάστοτε παραγωγής στον αγροτικό τομέα, έχει όπως παρακάτω:



Εικόνα 5.4 - Ανάλυση αγροτικής παραγωγής στην Ελλάδα, σύμφωνα με στοιχεία AGRO-START

Σύμφωνα με τον Γκόγκα (2017), βλ. σχετικά [75] και όπως αναφέρει σχετικά και ο Γκέκας (2017), βλ. σχετικά [79], ο αγροδιατροφικός τομέας συμμετέχει σε μεγάλο ποσοστό στο εξαγώγιμο προϊόν της Ελλάδας. Το μεγαλύτερο ποσοστό εξαγωγών αγροδιατροφικών προϊόντων, όσον αφορά την ποσότητα, είναι σε φρούτα και λαχανικά, ενώ από άποψη αξίας, είναι σε ελαιόλαδο. Κατά τα δέκα τελευταία χρόνια ο ελληνικός αγροδιατροφικός κλάδος έχασε μερίδο στην παγκόσμια αγορά, συγκεκριμα μειώθηκε από 24% σε 20%. Ο αγροδιατροφικός κλάδος της Ελλάδας αδυνατεί να ανταγωνιστεί, σε μια παγκοσμιοποιημένη αγορά, χώρες με χαμηλό κόστος παραγωγής.

Προκύπτει λοιπόν η ανάγκη ανάπτυξης γρήγορων και αποτελεσματικών καινοτομιών, (σε μεθόδους παραγωγής και οργάνωσης), που θα προσδώσουν στον Έλληνα παραγωγό συγκριτικό πλεονέκτημα.

Σε σχετική μελέτη του ΔιαΝΕΟσις βλ. σχετικά [74], εξετάζεται το θέμα της πρωτογενούς παραγωγής ως μεγάλης ανεκμετάλλευτης ευκαιρίας για την χώρα μας. Ο πρωτογενής τομέας έχει κομβική σημασία, σε όλες τις έρευνες για την παραγωγική ανασυγκρότηση της χώρας (McKinsey, ΙΟΒΕ, ΚΕΠΕ).

Αν κάποιος θέλει να αναζητήσει μία απλή εξήγηση για την έλλειψη ανταγωνιστικού πλεονεκτήματος της ελληνικής αγροτικής παραγωγής, μπορεί να εστιάσει στο μέγεθος, των παραγωγικών μονάδων. Στην Ελλάδα οι γεωργικές εκμεταλλεύσεις είναι πολύ μικρές. Ως αποτέλεσμα δεν είναι ανταγωνιστικές, σε ό,τι αφορά το κόστος, την παραγωγικότητα και τις εξαγωγές. Κι αυτό δεν αφορά μόνο τους αγρότες, αλλά και τον κρίσιμο τομέα της μεταποίησης.

Σύμφωνα με σχετική μελέτη του ΔιαΝΕΟσις βλ. σχετικά [74], το μικρό μέγεθος, το οικογενειακό δίκαιο, η ιδιοκτησιακή κουλτούρα και γενικότερα η οικονομική μας ιστορία δεν έχουν διευκολύνει τις συνεργασίες και τις συγχωνεύσεις. Δεν δίνονται ιδιαίτερα κίνητρα, για εξωστρεφείς στρατηγικές και συνεργασίες. Τόσο μικρές επιχειρήσεις είναι εξαιρετικά δύσκολο να είναι ανταγωνιστικές σε διεθνείς αγορές, να βρουν συνεργάτες στον τομέα της μεταποίησης ή πρόσβαση σε δίκτυα διανομής, ή και να επενδύσουν σε marketing ή σε καινοτομία.

Σύμφωνα με σχετική μελέτη του ΔιαΝΕΟσις βλ. σχετικά [74], μια πιθανή λύση για την επίτευξη οικονομιών κλίμακας, είναι η συνεργατικότητα. Πρέπει να υπάρξουν συνεργατικά σχήματα μεταξύ αγροτών (συνεταιρισμοί, αγροτικές εταιρικές συμπράξεις), μεταξύ μεταποιητικών επιχειρήσεων (δίκτυα και clusters), μεταξύ αγροτών και των μεταποιητικών επιχειρήσεων (συμβολαιακή γεωργία, συνεργασία συνεταιρισμών και ιδιωτικών επιχειρήσεων). Επίσης πρέπει να υπάρξει σύνδεση και συνεργασία μεταξύ των επιχειρήσεων του κλάδου και των ερευνητικών κέντρων, προκειμένου, να αναπτυχθούν και να προταθούν καινοτόμες λύσεις και η τεχνολογία blockchain, με τα ιδιαίτερα χαρκτηριστικά προσφέρεται για τέτοιες λύσεις.

Οι έμποροι και διανομείς στις αγροδιατροφικές εφοδιαστικές αλυσίδες

Σύμφωνα με τους Dianhui et al (2018), βλ. σχετικά [52], το εμπόριο αγροτικών προϊόντων διατροφής δεν συνδέεται μόνο με το εισόδημα των αγροτών και την επιβάρυνση των καταναλωτών, αλλά είναι επίσης κεντρικό στοιχείο της κοινωνικής ζωής και της κοινωνικής σταθερότητας. Είναι επομένως ένας τομέας με υψηλή κοινωνική και πολιτική ευαισθησία.

Σύμφωνα με τους Minarelli et al (2016), βλ. σχετικά [53], υπάρχουν πολλοί ενδιαφερόμενοι στο εμπόριο γεωργικών προϊόντων διατροφής: γεωργοί, μεταποιητές, έμποροι, χονδρέμποροι, λιανοπωλητές και καταναλωτές. Αντιμετωπίζουν την αβεβαιότητα και ζητούν υψηλής ποιότητας και ασφαλή τρόφιμα, μαζί με όσο το δυνατόν περισσότερες πληροφορίες. Επομένως, ενδέχεται να υπάρχει πρόβλημα ασυμμετρίας πληροφόρησης. Οι ασύμμετρες πληροφορίες εμφανίζονται όταν τα μέρη που συμμετέχουν σε μια οικονομική συναλλαγή δεν είναι εξίσου ενημερωμένα. Η ασυμμετρία των πληροφοριών μπορεί να προκαλέσει μια σειρά προβλημάτων, όπως η ανεπάρκεια της αγοράς. Προς το παρόν, πολλές χώρες προσπαθούν να μειώσουν τις αποτυχίες της αγοράς και να δημιουργήσουν ένα δικαιότερο εμπορικό περιβάλλον στη γεωργία και τη βιομηχανία τροφίμων. Για παράδειγμα, στις 12 Απριλίου 2018, η Ευρωπαϊκή Επιτροπή, βλ. σχετικά [54], αποφάσισε να απαγορεύσει τις βλαπτικές εμπορικές πρακτικές που προκαλούνται από την ασυμμετρία της πληροφόρησης στο εμπόριο γεωργικών προϊόντων διατροφής, προκειμένου να διασφαλιστεί η δίκαιη μεταχείριση των μικρών και μεσαίων επιχειρήσεων τροφίμων και γεωργικών προϊόντων.

Τα προβλήματα αυτά όχι μόνο βλάπτουν τη σταθερότητα της αγοράς τροφίμων αλλά και μειώνουν την αποτελεσματικότητα των συναλλαγών. Επιπλέον, η πολυπλοκότητα της διαδικασίας συναλλαγής, το υψηλό κόστος συναλλαγής και οι μακρές προθεσμίες συναλλαγών μπορούν να οδηγήσουν σε αναποτελεσματικές συναλλαγές. Ως εκ τούτου, είναι απαραίτητο να βρεθούν λύσεις που να μπορούν να προστατεύουν τη δικαιοσύνη και να βελτιώνουν την αποτελεσματικότητα των συναλλαγών σε τρόφιμα.

Σύμφωνα με τους Trienekens et al (2012), βλ. σχετικά [51], οι σημερινές αλυσίδες

εφοδιασμού αντιμετωπίζουν πολλά θέματα που σχετίζονται με την αξιοπιστία των πληροφοριών, την εμπιστοσύνη (trust) των καταναλωτών, την διαφάνεια (transparency) της εφοδιαστικής αλυσίδας, την ποιότητα των προϊόντων (product quality), τις περιβαλλοντικές επιπτώσεις από την διαδικασία παραγωγής, αποθήκευσης, τυποποίησης και διανομής (πχ χρήση Ανανεώσιμων Πηγών Ενέργειας-ΑΠΕ στην όλη διαδικασία), θέματα που αφορούν τα προσωπικά δεδομένα καταναλωτών, απάτη, ασφάλεια των τροφίμων κλπ.

Οι καταναλωτές

Οι καταναλωτές ανησυχούν όλο και περισσότερο για την ασφάλεια και την αειφορία (sustainability) των τροφίμων και απαιτούν περισσότερες πληροφορίες σχετικά με τις αλυσίδες γεωργικών προϊόντων διατροφής. Ωστόσο, το μέγεθος και η πολυπλοκότητα των σύγχρονων αλυσίδων εφοδιασμού των γεωργικών προϊόντων διατροφής έχουν δημιουργήσει μια απόσταση μεταξύ των καταναλωτών και των παραγωγών, πράγμα που καθιστά ανέφικτο για τους καταναλωτές να αντιμετωπίζουν τις ανησυχίες και τις ερωτήσεις τους απευθείας στους καλλιεργητές. Η αυξανόμενη ζήτηση πληροφοριών για τα τρόφιμα αντικατοπτρίζει την ανάγκη για διαφάνεια και έλλειψη εμπιστοσύνης. Ταυτόχρονα, ολοένα και περισσότερα τρόφιμα και ποτά είναι επώνυμα και συνοδεύονται από μια ποικιλία προγραμμάτων πιστοποίησης, με συνεχώς αυξανόμενο κίνδυνο απάτης (fraud) και νοθείας (adulteration).

Στην παρούσα κατάσταση, πολλά από τα δεδομένα και οι πληροφορίες συμμόρφωσης ελέγχονται από αξιόπιστους τρίτους και αποθηκεύονται είτε σε χαρτί είτε σε κεντρική βάση δεδομένων. Σημαντικά προβλήματα είναι:

- Το υψηλό κόστος και η αναποτελεσματικότητα των διαδικασιών που βασίζονται στο χαρτί.
- Απάτη, διαφθορά, σφάλματα τόσο σε χαρτί όσο και σε συστήματα πληροφορικής.
- Ακεραιότητα ψηφιακών αρχείων (προβλήματα που οφείλονται σε ανθρώπινο σφάλμα και παραβίαση δεδομένων).
- Διάρκεια δαπανών για πιστοποιητικά.

Αυτά τα προβλήματα έχουν οδηγήσει σε χαμηλή διαφάνεια και εμπιστοσύνη στις αλυσίδες γεωργικών προϊόντων διατροφής και αποτελούν σοβαρή απειλή για την

ασφάλεια των τροφίμων, την ποιότητα των τροφίμων και τη βιωσιμότητα. Ειδικότερα, η ακεραιότητα των τροφίμων έχει γίνει ακόμη ένα λόγος μεγάλης ανησυχίας. Η ακεραιότητα των τροφίμων αναφέρεται στη δικαιοσύνη και την αυθεντικότητα των τροφίμων στις αλυσίδες αξίας των τροφίμων τόσο στο φυσικό επίπεδο όσο και στο ψηφιακό στρώμα, όπου το ψηφιακό στρώμα πρέπει να παρέχει αξιόπιστα και αξιόπιστες πληροφορίες σχετικά με την προέλευση και την προέλευση των προϊόντων διατροφής στο φυσικό στρώμα.

Η αποκέντρωση και η αξιοπιστία που εξασφαλίζει η τεχνολογία Blockchain, μπορεί να επιλύσει αυτά τα προβλήματα, παρέχοντας αξιόπιστες συναλλαγές σε περιβάλλον δυσπιστίας στον τομέα παραγωγής, διανομής και εμπορίου τροφίμων. Με την τεχνολογία Blockchain, οι εφαρμογές που θα μπορούσαν να λειτουργήσουν μόνο μέσω ενός αξιόπιστου διαμεσολαβητή μπορούν πλέον να λειτουργούν με αποκεντρωμένο τρόπο χωρίς την ανάγκη κεντρικής εξουσίας και να επιτύχουν την ίδια λειτουργικότητα με το ίδιο με βεβαιότητα. Αυτό δεν ήταν δυνατό πριν.

Τρέχουσα κατάσταση στην αγορά και παραδείγματα εφαρμογής

Σύμφωνα με την Noel (2018), βλ. σχετικά [55], υπάρχουν ήδη πολλά επιτυχημάνα παραδείγματα εφαρμογής της τεχνολογίας blockchain από επιχειρήσεις ανά τον κόσμο, Τα παραδείγματα αυτά, δίνουν μιας εικόνα της τρέχουσας κατάστασης όσον αφορά την υιοθέτηση της νέας αυτής τεχνολογίας και για αυτό το λόγο θα τα παρουσιάσουμε συνοπτικά παρακάτω.

- Η πρωτοβουλία IBM Food Trust ξεκίνησε με τη συνεργασία τους με την Walmart China και το Πανεπιστήμιο Tsinghua και έχει εξελιχθεί σε μια παγκόσμια κοινοπραξία που περιλαμβάνει μεγάλες εταιρείες όπως Dole, Driscoll, Kroger, Nestle, Tyson και Unilever. Η βελτιωμένη ιχνηλασιμότητα δεδομένων, που παρέχεται από την πλατφόρμα της IBM μείωσε το χρόνο που χρειάστηκε για να εντοπίζει ένα αγροτικό προϊόν, από το κατάστημα πίσω στην πηγή του, από επτά ημέρες σε 2,2 δευτερόλεπτα. Αυτή η μείωση του χρόνου επιτρέπει στις εταιρείες να εντοπίζουν μολυσμένες αλυσίδες εφοδιασμού και να ανακαλούν τα επηρεαζόμενα προϊόντα πριν καταναλωθούν και προκαλούν ασθένεια.

- Το OriginTrail είναι μια εταιρεία που εδρεύει στη Σλοβενία και εργάζεται πάνω στον τομέα της ιχνηλασιμότητας δεδομένων. Η επεξεργασία των συναλλαγών και η αποθήκευση δεδομένων σε ένα blockchain για την ανίχνευση προϊόντων, μπορεί να είναι δαπανηρή. Το OriginTrail βρήκε έναν τρόπο να αποθηκεύσει μόνο τα «δακτυλικά αποτυπώματα» των δεδομένων στο blockchain. Η ομάδα επίσης έχει δημιουργήσει την Trace Alliance, μια κοινοπραξία εταιρειών που χρησιμοποιούν το blockchain για την ιχνηλασιμότητα της αλυσίδας εφοδιασμού.
- Η εταιρεία Viant είναι θυγατρική της Consensys που ασχολείται με την ανάπτυξη εφαρμογών blockchain, για την αντιμετώπιση πολλών διαφορετικών προκλήσεων (αναπτύξανε πλατφόρμα για αξιόπιστη δημοσιογραφία, πλατφόρμα διαχείρισης ταυτότητας, πλατφόρμα για διαμοιρασμό μουσικών κομματιών). Η Viant έχει συνεργαστεί με τα Φίτζι, με την WWF και την Traseable Solutions, για την παρακολούθηση του πληθυσμού του λευκού τόνου που αλιεύεται από πιστοποιημένη αλιευτική εταιρεία. Οι πομποί ενός συστήματος αυτόματου εντοπισμού, εγκαταστάθηκαν στα σκάφη της αλιευτικής εταιρείας για την παρακολούθηση και την συνεχή παρακολούθηση των αλιευτικών δραστηριοτήτων. Τα ψάρια επισημαίνονται με έναν αισθητήρα όταν αλιεύονται και ο αισθητήρας αλληλεπιδρά με τον πομπό στα αλιευτικά σκάφη, για να καταγράψει τόσο το χρόνο όσο και την ακριβή θέση. Τα δεδομένα θέσης επιβεβαιώνουν ότι τα ψάρια αλιεύτηκαν σε τόπο όπου τα αποθέματα τους δεν υπερεκμεταλλεύονται.
- Το Arc-net , μια εταιρεία με βάση το Μπέλφαστ, έχει αναπτύξει μια πλατφόρμα blockchain, που αποθηκεύει πληροφορίες για DNA, για εφοδιαστικές αλυσίδες κρέατος. Ξεκινούν λαμβάνοντας ένα δείγμα ιστού ενός ζώου στις αρχές της αλυσίδας εφοδιασμού και αποθηκεύουν πληφορίες σχετικές με το DNA του δείγματος. Όταν οι εισαγωγείς και άλλοι, κατά μήκος της αλυσίδας εφοδιασμού λαμβάνουν το κρέας, μπορούν στη συνέχεια να δοκιμάσουν ένα δείγμα και να επιβεβαιώσουν ότι το DNA ταιριάζει με αυτό που περίμεναν. Αναπτύσουν επίσης για λογαριασμό ενός σκωτσέζικου αποστακτήριου ουίσκι (Ardnamurchan), ένα blockchain το οποίο περιλαμβάνει πληροφορίες για το νερό και τα σιτηρά που χρησιμοποιούνται στην παραγωγή καθώς και την ταυτότητα των οινοπνευματοποιών που έκαναν το ουίσκι.
- Η Provenance είναι μια εταιρεία με έδρα το Λονδίνο. Ο ιδρυτής της εταιρείας Jessi Baker αναγνώρισε ότι οι πελάτες θέλουν να κατανοήσουν τις κοινωνικές και

περιβαλλοντικές επιπτώσεις των αγορών τους. Η Provenance παρέχει διαφάνεια τόσο για τις εταιρείες τροφίμων όσο και για τα είδη ένδυσης, επιτρέποντας στους πελάτες όχι μόνο να μάθουν από πού προέρχονται το δείπνο τους ή το καινούργιο σακάκι τους, αλλά και να επιβεβαιώνουν ότι οι άνθρωποι που βοήθησαν να φτιάξουν το προϊόν αμοίβονταν ικανοποιητικά και ότι τα προϊόντα παράγονται με τρόπο που είναι περιβαλλοντικά υπεύθυνος.

- Η κινέζικη εμπορική εταιρεία Alibaba, χρησιμοποιεί την τεχνολογία blockchain για τη βελτίωση της εμπιστοσύνης των καταναλωτών στην αυθεντικότητα των τροφίμων σε ένα περιβάλλον όπου η ασφάλεια των τροφίμων αποτελεί καθημερινή μέριμνα για τους πελάτες.
- Η κινέζικη εμπορική εταιρεία JD.com, με έδρα το Πεκίνο, χρησιμοποιεί την τεχνολογία blockchain για την παρακολούθηση του βοείου κρέατος σε όλα τα στάδι από την παραγωγή, την επεξεργασία και τη μεταφορά του βοείου κρέατος, τόσο στην Κίνα, αλλά σε συνεργαζόμενες εταιρείς της Αυστραλίας. Επίσης, σχεδιάζουν να επεκτείνουν την εφαρμογή και σε αλυσίδα παραγωγής και εφοδιασμού premium ψαριών. Αντίστοιχη εφαρμογή, BeefChain αναπτύχθηκε και από τους κτηνοτρόφους βοοειδών του Wyoming στις ΗΠΑ, που ήθελαν να μάθουν πού πωλείται το βόειο κρέας τους. Η πλατφόρμα παρακολουθεί το βόειο κρέας κατά μήκος της αλυσίδας εφοδιασμού και δίνει τη δυνατότητα στους κτηνοτρόφους να ανακτήσουν την αξία τους από φορείς τρίτου μέρους κατά μήκος της αλυσίδας.
- Η εταιρεία ZhongAn, με έδρα τη Σαγκάη, διαθέτει μια πλατφόρμα blockchain που ονομάζεται Bubuj ithat. Τοποθετούνται αισθητήρες σε κοτόπουλα όταν φτάσουν σε ένα συγκεκριμένο μέγεθος. Οι αισθητήρες όχι μόνο παρακολουθούν τη θέση των νεοσσών, αλλά και επιτρέπουν στους πελάτες να δουν πόσο κινούνται καθημερινά.
- Το σύστημα Walimai, στην Κίνα, χρησιμοποιεί την τεχνολογία blockchain σε συνδυασμό με έναν αισθητήρα που τοποθετείται σε κουτιά συσκευασίας προϊόντων. Ο αισθητήρας ανιχνεύει αν έχει ανοίξει το κουτί και καταχωρεί σχετικές πληροφορίες σε κάρτα RFID. Ο πελάτης που θα αγοράσει το συσκευασμένο προϊόν, μπορεί να σαρώσει την κάρτα RFID, για να επιβεβαιώσει ότι δεν έχει παραβιαστεί το κουτί. Αυτό είναι ιδιαίτερα σημαντικό σε μια αγορά

όπως η Κίνα, όπου η ασφάλεια των τροφίμων αποτελεί βασικό μέλημα των καταναλωτών λόγω των πολλαπλών περιστατικών θανάτων από αλλοιωμένα και μη ασφαλή τρόφιμα.

- Η αυστραλιανή εταιρεία AgriDigitalprovides παρέχει υπηρεσίες διαχείρισης γεωργικών προϊόντων που βασίζονται σε cloud-based τεχνολογία και καταγράφονται σε ένα blockchain.
- Η Avenews-GT είναι μια εταιρεία με έδρα το Ισραήλ, που έχει δημιουργήσει μια πλατφόρμα συναλλαγών και διαχείρισης πληρωμών, για εμπόρους και παραγωγούς αγροτικών προϊόντων.
- Η εταιρεία Binkabi με έδρα το Λονδίνο, δημιούργησε μια πλατφόρμα για αγορά αγαθών και προϊόντων που μειώνει τα έξοδα συναλλάγματος και αυξάνει τα κέρδη. Επιτρέπει επίσης τη διενέργεια διμερών συναλλαγών σε τοπικά νομίσματα και στις δύο πλευρές με πολύ αποδοτικό τρόπο.
- Η VinX έχει δημιουργήσει μια πλατφόρμα συναλλαγών και διαχείρισης πληρωμών, για εμπόρους και παραγωγούς οίνου. Τα οινοποιεία μπορούν να λάβουν χρηματοδότηση απευθείας από τους καταναλωτές, επιτρέποντάς τους να αναπτύξουν σχέσεις άμεσα με τους πελάτες τους και να μειώσουν το ρίσκο μεταξύ επένδυσης και πωλήσεων.
- Το Ripe.io, είναι μια εφαρμογή που αναπτύχθηκε από μια εταιρεία με έδρα την Καλιφόρνια. Συλλέγει δεδομένα από αισθητήρες και άλλες πηγές κατά μήκος της αλυσίδας εφοδιασμού, παρέχοντας στους αγοραστές λεπτομερείς πληροφορίες σχετικά με τα χαρακτηριστικά των προϊόντων. Αποθηκεύονται δεδομένα όπως η υγρασία, η θερμοκρασία του αέρα, το χρώμα, το άλας, η περιεκτικότητα σε ζάχαρη, τα επίπεδα pH κλπ και αποθηκεύονται στο blockchain. Η παρακολούθηση αυτών των πληροφοριών βοηθά τον μεταποιητή τον έμπορο, να συλλέγει το προϊόν την κατάλληλη χρονική στιγμή, όταν έχει τα επιθυμητά χαρακτηριστικά.

Από τα παραπάνω παραδείγματα γίνεται φανερό ότι, η τεχνολογία Blockchain ήδη αλλάζει τον τρόπο με τον οποίο γίνονται τα πράγματα, στον αγροδιατροφικό τομέα.

ΚΕΦΑΛΑΙΟ 6 - ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: BLOCKCHAIN ΚΑΙ ΕΛΑΙΟΛΑΔΟ

Σε αυτή την ενότητα θα εξετάσουμε την περίπτωση εφαρμογής της τεχνολογίας Blockchain στην περίπτωση του ελαιόλαδου (case study).

Γιατί επιλέγουμε το ελαιόλαδο σαν μελέτη περίπτωσης

Το ελαιόλαδο (olive oil), θεωρείται βασικό προϊόν της καθημερινής μας διατροφής και ξεχωρίζει από τα υπόλοιπα έλαια για την εξαιρετική του γεύση και ποιότητα, ενώ θεωρείται και πιο υγιεινό. Είναι βασικό στοιχείο της μεσογειακής δίαιτας και κορυφαίο διατροφικό προϊόν για την Ελλάδα, τόσο από πλευράς παραγωγής όσο και διατροφικών συνηθειών.

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], ο μέσος Έλληνας καταναλώνει περίπου 18 κιλά ελαιόλαδο το χρόνο, ποσότητα σχεδόν διπλάσια από την αντίστοιχη για το μέσο Ιταλό και Ισπανό καταναλωτή, και έρχεται πρώτος στην παγκόσμια κατάταξη. Η Ελλάδα είναι η 3η μεγαλύτερη ελαιοπαραγωγός χώρα της Ε.Ε. Η ετήσια παραγωγή της εκτιμάται περίπου σε 300.000 τόνους. Στη 2η θέση βρίσκεται η Ιταλία με 400.000 τόνους και στο 1ο σκαλί του βάθρου η Ισπανία με ετήσια παραγωγή που ξεπερνά το 1.000.000 τόνους, Το εξαιρετικά παρθένο ελαιόλαδο, αποτελεί από τα κυριότερα εξαγώγιμα προϊόντα μας.

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], το ελληνικό ελαιόλαδο ξεχωρίζει, τόσο για την υψηλή ποιότητα, όσο για την γεύση, το χρώμα και το άρωμά του. Το 75 - 80% περίπου του παραγόμενου ελληνικού ελαιολάδου, ανήκει στην κατηγορία έξτρα παρθένο ελαιόλαδο, ποσοστό αυξημένο σε σχέση με την παραγωγή της Ιταλίας (περίπου 50%) και της Ισπανίας (περίπου 35%). Το ελληνικό «έξτρα παρθένο ελαιόλαδο» (Extra Virgin Olive Oil - EVOO) είναι βασικό εξαγώγιμο διατροφικό προϊόν για τη χώρα μας, αφού 200 περίπου χιλιάδες τόνοι εξάγονται στην Ιταλία και την Ισπανία. Επιπλέον λόγου της εξαιρετικής του ποιότητάς, είναι ακριβότερο σε σύγκριση με αντίστοιχα EVOOs από άλλες χώρες.

Πολλά από τα ελαιόλαδα που παράγονται στην χώρα μας, είναι Προϊόντα Ονομασίας Προέλευσης (ΠΟΠ), ή Προϊόντα Γεωγραφικής Ένδειξης (ΠΓΕ).

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], ο έλεγχος και η πιστοποίηση των Προϊόντων Ονομασίας Προέλευσης (ΠΟΠ) και των Προϊόντων Γεωγραφικής Ένδειξης (ΠΓΕ), γίνεται από τον Οργανισμό Πιστοποίησης και Επίβλεψης Γεωργικών Προϊόντων (ΟΠΕΓΕΠ), σύμφωνα με τις διατάξεις της ΚΥΑ 261611/22-03-2007 (ΦΕΚ 406Β/22-03-2007) όπως έχει τροποποιηθεί και ισχύει:

- *«Ονομασία προέλευσης»: το όνομα μιας περιοχής, ενός συγκεκριμένου τόπου ή σε εξαιρετικές περιπτώσεις, μιας χώρας, το οποίο χρησιμοποιείται για την περιγραφή ενός γεωργικού προϊόντος ή ενός τροφίμου που κατάγεται από τη συγκεκριμένη περιοχή, τον συγκεκριμένο τόπο ή τη συγκεκριμένη χώρα, του οποίου η ποιότητα ή τα χαρακτηριστικά οφείλονται ουσιαστικά ή αποκλειστικά στο ιδιαίτερο γεωγραφικό περιβάλλον που περιλαμβάνει τους εγγενείς φυσικούς και ανθρώπινους παράγοντες, του οποίου η παραγωγή, η μεταποίηση και η επεξεργασία πραγματοποιούνται στην οριοθετημένη γεωγραφική περιοχή.*
- *«Γεωγραφική ένδειξη»: το όνομα μιας περιοχής, ενός συγκεκριμένου τόπου ή, σε εξαιρετικές περιπτώσεις, μιας χώρας, το οποίο χρησιμοποιείται για την περιγραφή ενός γεωργικού προϊόντος ή ενός τροφίμου: που κατάγεται από την εν λόγω περιοχή, τον συγκεκριμένο τόπο ή την εν λόγω χώρα, του οποίου η συγκεκριμένη ποιότητα, η φήμη ή άλλα χαρακτηριστικά μπορούν να αποδοθούν στην εν λόγω γεωγραφική καταγωγή , του οποίου η παραγωγή ή /και η μεταποίηση ή/και η επεξεργασία πραγματοποιούνται στην οριοθετημένη γεωγραφική περιοχή.*

Ονομασίες και κατηγοριοποίηση

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], η κατηγοριοποίηση στα ελαιόλαδα, είναι σύνθετη και δύσκολη διαδικασία, δεδομένου ότι, επικρατούν διαφορετικά διεθνή πρότυπα και προδιαγραφές.

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], στην ελληνική αγορά, στο στάδιο του λιανικού εμπορίου επιτρέπεται να διατίθενται μόνο τα ελαιόλαδο των παρακάτω ποιοτικών κατηγοριών:

- Εξαιρετικό παρθένο ελαιόλαδο

- Παρθένο ελαιόλαδο
- Ελαιόλαδο
- Πυρηνέλαιο

Προδιαγραφές - σήμανση

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], τα ελαιόλαδα που διατίθενται στο ελληνικό λιανικό εμπόριο, πρέπει να πληρούν τις παρακάτω προϋποθέσεις όσον αφορά τη συσκευασία και τη σήμανσή τους.

Υποχρεωτικές ενδείξεις σήμανσης:

- Ονομασία πώλησης
- Καθαρή Ποσότητα
- Όνομα ή εμπορική επωνυμία
- Ημερομηνία ελάχιστης διατήρησης του προϊόντος
- Παρτίδα
- Ιδιαίτερες συνθήκες διατήρησης του προϊόντος
- Συνθήκες παραγωγής του ελαιολάδου
- Οργανοληπτικά χαρακτηριστικά
- Οξύτητα
- Θρεπτική αξία
- Αναγραφή της καταγωγής του ελαιόλαδου

Όσον αφορά την Ευρωπαϊκή Ένωση, οι παραγωγοί πιέζουν για την υποχρεωτική ενσωμάτωση λεπτομερών πληροφοριών σχετικά με την προέλευση των προϊόντων στις ετικέτες τους, προκειμένου τα παραγόμενα προϊόντα να ανταποκρίνονται στην αυξανόμενη απαίτηση των καταναλωτών για ενημέρωση και διαφάνεια, σχετικά με την παραγωγή, την προέλευση, την περιβαλλοντική «ευασθησία», την ασφάλεια, την αυθεντικότητα και το περιεχόμενο των τροφίμων που τρώνε.

Από τα παραπάνω προκύπτει ότι το ελαιόλαδο, ως αγροδιατροφικό προϊόν έχει ιδιαίτερη σημασία τόσο για τον καταναλωτή αλλά και τον Έλληνα αγρότη ή έμπορο. Επίσης τα ιδιαίτερα χαρακτηριστικά και προδιαγραφές του, σε όλη την διαδικασία παραγωγής - αποθήκευσης - διακίνησης του από τον παραγωγό, στον έμπορο, τα

σημεία λιανικής πώλησης και τον τελικό καταναλωτή το καθιστούν ιδανική περίπτωση εφαρμογής της τεχνολογίας blockchain.

Στην περίπτωση της Ελλάδας, θα πρέπει να ληφθεί υπόψη και το γεγονός ότι τόσο η παραγωγή, αλλά και η επεξεργασία και μεταποίηση (ελαιοτριβεία, συσκευαστήρια) γίνεται από μικρές μονάδες, που θα μπορούσαν να επιτύχουν οικονομίες κλίμακας μέσα από συνεργατικά σχήματα, για γτα οποία η τεχνολογία blockchain θα μπορούσε να δώσει καινοτόμους τρόπους οργάνωσης και λειτουργίας.

Θα δούμε παρακάτω σε τι στάδιο βρίσκεται η υιοθέτηση της τεχνολογίας blockchain, στις βασικές ανταγωνίστριες χώρες της Ελλάδας (Ισπανία και Ιταλία), όσον αφορά την παραγωγή ελαιόλαδου.

Η περίπτωση της Ισπανίας

Η Ισπανία παράγει παγκοσμίως κορυφαία γεωργικά προϊόντα.

Η πλατφόρμα OliveTrace

Σύμφωνα με σχετικές δημοσιεύσεις, βλ. σχετικά [59], η Galpagro, μια πρωτοποριακή εταιρεία που επικεντρώνεται σε ελαιώνες υψηλής απόδοσης, σε συνεργασία με τις εταιρείες Rurapolis, OLEOCANO και IBM Ισπανίας έχουν ενώσει τις δυνάμεις τους σε ένα έργο (project) με την ονομασία OliveTrace, Πρόκειται για ένα έργο που εφαρμόζει την τεχνολογία blockchain στο ελαιόλαδο, καθιστώντας το, το τέταρτο τρόφιμο σε παγκόσμιο επίπεδο του οποίου μπορεί να εξασφαλιστεί η ιχνηλασιμότητά του με την τεχνολογία blockchain, η οποία έχει ήδη φέρει επανάσταση στα παγκόσμια οικονομικά συστήματα.

Το έργο αυτό θα εφαρμόσει την τεχνολογία Blockchain στην αλυσίδα του ποιοτικού ελαιολάδου, παρέχοντας στον καταναλωτή λεπτομερείς και επαληθευμένες πληροφορίες όλων των πλευρών οι οποίες εμπλέκονται στη διαδικασία παραγωγής, αποθήκευσης, διανομής και διάθεσης του ελαιολάδου, από την ελιά μέχρι το τελικό σημείο πώλησης.

Το OliveTrace χρησιμοποιεί τεχνολογία Blockchain για να συλλέγει και να κρυπτογραφεί όλες τις πληροφορίες που παρέχονται από κάθε κρίκο της αλυσίδας αξίας ελαιολάδου (από τον παραγωγό έως και τον διανομέα). Οι πληροφορίες αυτές συλλέγονται από αισθητήρες που διατάσσονται κατά μήκος ολόκληρης της αλυσίδας. Με αυτό τον τρόπο καταγράφει όσο το δυνατόν περισσότερα δεδομένα, με αυτοματοποιημένο τρόπο και χωρίς καμία δυνατότητα επίδρασης τρίτων σε αυτά.Αυτές οι πληροφορίες που συλλέγονται είναι πολλές: ποικιλία ελιάς, περιοχή καλλιέργειας, τεχνικές λεπτομέρειες της επεξεργασίας στο ελαιοτριβείο, θερμοκρασία αποθήκευσης, πληροφορίες συσκευασίας, εξαγωγές και εισαγωγές κατά τη διάρκεια της επεξεργασίας και του εμπορίου. Όλα όσα δηλαδή αξίζει να καταγραφούν.

Ο καταναλωτής, όταν φτάνει στο ράφι των σούπερ μάρκετ, μπορεί να δει όλη αυτή την πληροφορία μέσω του smartphone του, με μια απλή κίνηση ανάγνωσης του κώδικα QR που υπάρχει σε κάθε μπουκάλι ελαιολάδου. Έτσι, θα έχει πρόσβαση σε όλα τα δεδομένα που αφορούν όλη την αλυσίδα παραγωγής, συσκευασίας, επεξεργασίας, αποθήκευσης και διακίνησης του προϊόντος, καθώς και για τους φορείς πιστοποίησης που συμμετέχουν σε αυτήν. Κάθε φορέας που εμπλέκεται στις διαδικασίες παραγωγής και πώλησης θα είναι επίσης ορατός και διαφανής.

Το project, Olive Trace, ξεκίνησε ήδη να εφαρμόζεται πιλοτικά κατά την συγκομιδή της περιόδου 2018-2019 στο Finca El Valenciano της Σεβίλλης, όπου τμήμα της παραγωγής αποτέλεσε την πρώτη περιορισμένη παραγωγή extra virgin ελαιόλαδου.

Η πλατφόρμα Olivacoin

Σύμφωνα με σχετικές δημοσιεύσεις, βλ. σχετικά [60], το 2019 ξεκίνησε στην Ισπανία από την εταιρεία Olivacoin η εφαρμογή μιας πλατφόρμας τεχνολογίας blockchain, η οποία έχει στόχο να αποτελέσει εργαλείο ποιοτικού ελέγχου και διαχείρησης της τιμής του προϊόντος. Προσφέρει επίσης μια πλατφόρμα πληρωμών για τους αγοραστές και τους πωλητές ελαιολάδου.

Η περίπτωση της Ιταλίας

Η πλατφόρμα Devoleum

Το Devoleum αναπτύχθηκε από τους Lorenzo Zaccagnini και Elisa Romondia. Σύμφωνα με το επίσημο site του Devoleum, βλ. σχετικά [61], χρησιμοποιεί το Ethereum, μια ευέλικτη πλατφόρμα blockchain, που προσαρμόζεται σε κάθε αλυσίδα εφοδιασμού. Είναι δυνατό να εντοπιστεί το ιστορικό ενός αγροδιατροφικού προϊόντος, μέσα από δεδομένα παρακολούθησης από την παραγωγή έως την πώληση. Τα δεδομένα μπορούν να διαβαστούν εύκολα σε ένα storyboard στην πλατφόρμα web Devoleum, εύκολα προσβάσιμη από οποιαδήποτε συσκευή μόνο με τη σάρωση μιας έξυπνης ετικέτας. Υποστηρίζει την διαλειτουργικότητα και με άλλες τεχνολογίες such όπως IoT (precision farming), μοντέλα AI, Building Information Modeling (BIM) και distribution services for digital content (aggregators and streaming),.

Η πλατφόρμα Oracle Blockchain

Σύμφωνα με σχετικές δημοσιεύσεις, βλ. σχετικά [62], για την κάλυψη της ζήτησης των καταναλωτών για πιστοποιημένα προϊόντα υψηλής ποιότητας, η Certified Origins Italia χρησιμοποιεί την πλατφόρμα Oracle Blockchain για την παρακολούθηση και ανίχνευση της μάρκας Bellucci EVOO από την ιταλική μονάδα εμφιάλωσης έως το λιμάνι άφιξης στις ΗΠΑ. Αυτή η εφαρμογή της τεχνολογίας blockchain αποτελεί συνέχεια της δέσμευσης του Certified Origins για μεγαλύτερη διαφάνεια της αλυσίδας εφοδιασμού τροφίμων.

Η περίπτωση της Ελλάδας

Στην Ελλάδα, από σχετική έρευνα στο διαδίκτυο, διαπιστώθηκε ότι δεν υπάρχουν ακόμη παραδείγματα εφαρμογής της τεχνολογίας blockchain στον τομέα του ελαιόλαδου. Ειδικότερα διπιστώθηκαν τα παρακάτω.

Παραγωγή - μεταποίηση - εμπόριο

Στα πλαίσια της εργασίας, έγινε τηλεφωνική επικοινωνία με εταιρείες που δραστηριοποιούνται στην τυποποίηση και εμπορία ελαιόλαδου στην περιοχή της Στερεάς Ελλάδας (Nutria Olive Oil, ΕΛΑΙΟΥΡΓΙΚΗ Μεγαπλατάνου), αλλά και με

παράγοντες του Οικονομικού Επιμελητηρίου και διαπιστώθηκε ότι δεν γνώριζαν για τις δυνατότητες από την εφαρμογή της νέας τεχνολογίας blockchain στο ελαιόλαδο.
Σε αντίστοιχη επικοινωνία με παραγωγούς (αγρότες), της περιοχής Φθιώτιδας, διαπιστώθηκε ότι δεν ήταν ενήμεροι για τις δυνατότητες της νέας τεχνολογίας.
Μετά από σύντομη ενημέρωση για τις δυνατότητες της, ήταν θετικοί στην ιδέα, αλλά κανείς δεν θα προχωρούσε άμεσα στην εφαρμογή της.

Αγορά - Κατανάλωση

Σύμφωνα με την Κολιούδη (2016), βλ. σχετικά [58], από στοιχεία έρευνας οι Έλληνες καταναλωτές δηλώνουν ότι:

- αγοράζουν ελαιόλαδο, και το χρησιμοποιούν καθημερινά στη διατροφή τους,
- είναι υγιεινό, εύγεστο και θρεπτικό,
- προτιμάνε το ελαιόλαδο έναντι άλλων προϊόντων,
- τα 2/3 προμηθεύονται το προϊόν από τα καταστήματα πώλησης
- το 1/3 προμηθεύονται το προϊόν από τον παραγωγό, διότι το θεωρούν πιο αξιόπιστο και καλύτερης ποιότητας
- το 44,4% των καταναλωτών δε χρησιμοποιεί συγκεκριμένη μάρκα, αλλά γοράζει με κριτήριο την ποιότητα καθώς επίσης και την τιμή..

Συμπεράσματα στην περίπτωση της Ελλάδας

Είναι απαραίτητο ο κλάδος να ενημερωθεί για τις εξελίξεις της νέας τεχνολογίας.

Η αγορά οδηγείται από τον ανταγωνισμό των τιμών και τα κίνητρα του πωλητή πηγαίνουν προς χαμηλής ποιότητας ελαιόλαδα. Η προσθήκη ολόκληρης αυτής της τεχνολογίας στη διαδικασία δεν είναι φθηνή. Σύμφωνα με σχετικές δημοσιεύσεις, βλ. σχετικά [59], εκτιμάται ότι η τιμή του τυποποιημένου προϊόντος θα αυξηθεί κατά περίπου 20%.

Με την πρόσβαση σε πληροφορίες σχετικά με την ασφάλεια, την ποιότητα και την προέλευση από τον καταναλωτή, η ασυμμετρία της πληροφορίας θα μειωθεί ραγδαία υπέρ των προϊόντων καλής ποιότητας σε προσιτές τιμές. Θα πρέπει επομένως, να γίνει εκστρατεία ενημέρωσης και ευαισθητοποίησης και του καταναλωτή σχετικά με τα τρόφιμα.

Ενώ οι τιμές ενδέχεται να μειωθούν στο μέλλον, το κόστος εφαρμογής της τεχνολογίας αποτελεί επί του παρόντος απαγορευτικό παράγοντα για τους περισσότερους παραγωγούς.

Τα οφέλη για τους καταναλωτές είναι προφανή, σύμφωνα με τα όσα έχουμε αναφέρει παραπάνω. Η εφαρμογή της τεχνολογίας πέραν των άλλων πλεονεκτημάτων θα βοηθούσε τους Έλληνες παραγωγούς, αλλά και όσους εμπλέκονται στην τυποποίηση, διακίνηση και εμπορία του προϊόντος να διεισδύσουν ευκολότερα σε διεθνείς αγορές (ΗΠΑ,Κίνα, Ιαπωνία, Ευρώπη), που η ζήτηση για ποιοτικά αγροδιατροφικά προϊόντα είναι μεγάλη, υλοποιώντας συνεργατικά σχήματα και καινοτόμους τρόπους οργάνωσης και λειτουργίας.

Σε κάθε περίπτωση όλοι θα πρέπει να προσαρμοστούν στα νέα δεδομένα που θα προκύψουν από την εφαρμογή της τεχνολογίας blockchain και σε αυτό τον τομέα της οικονομίας.

ΚΕΦΑΛΑΙΟ 7 - ΠΑΡΟΥΣΙΑΣΗ ΠΛΑΤΦΟΡΜΩΝ BLOCKCHAIN

Πως επιλέγω μια πλατφόρμα BlockChain

Σύμφωνα με τα όσα αναφέραμε και στην αρχή της εργασίας, σχετικά με την ακολουθούμενη μεθοδολογία, προκειμένου μια επιχείρηση να κάνει την μετάβαση στην Τεχνολογία BlockChain θα πρέπει:

1. να αξιολογήσει το επιχειρηματικό πρόβλημα και τι θέλει να βελτιώσει
2. να δει αν η τεχνολογία BlockChain έχει εφαρμογή στην περίπτωση του,
3. να επιλέξει την κατάλληλη πλατφόρμα blockchain,
4. να προχωρήσει στην σχεδίαση μιας πιλοτικής εφαρμογής (drafted application),
5. μετά την εφαρμογή να προχωρήσει αξιολόγηση της.

Επομένως η επιλογή της κατάλληλης πλατφόρμας blockchain θα πρέπει να γίνει με βάση το πρόβλημα που θέλουμε να επιλύσουμε. Η σχεδίαση της αρχικής πιλοτικής εφαρμογής θα γίνει, λαμβάνοντας υπόψη και το βαθμό δυσκολίας και πολυπλοκότητας του εγχειρήματος. Άλλοι παράγοντες που πρέπει να ληφθούν υπόψη, είναι το μέγεθος της εταιρείας και το κόστος υιοθέτησης της τεχνολογίας blockchain. Η πιλοτική εφαρμογή θα μπορούσε να είναι, στην πιο απλή περίπτωση ένα single-use application.

Δημοφιλείς πλατφόρμες blockchain

Θα δούμε στην συνέχεια, διάφορες πλατφόρμες blockchain και τα χαρακτηριστικά τους. Αυτές είναι:

- Bitcoin
- Ethereum
- Hyperledger (Sawtooth Lake)
- HydraChain
- Open Chain
- Multichain

Τα κριτήρια για την επιλογή των παραπάνω πλατφορμών Blockchain είναι κατά βάση υποκειμενικά. Έγινε προσπάθεια για μια ποιοτική ανάλυση όλων των πλατφορμών με βάση τις ακόλουθες παραμέτρους:

- Αν είναι λογισμικό ανοικτού κώδικα (open source)
- Τύπος Blockchain (public, private, permissioned)

- Υποστηριζόμενες γλώσσες προγραμματισμού
- Δυνατότητα ανάπτυξης εφαρμογών για εφοδιαστικές αλυσίδες

Bitcoin

Είναι η πλατφόρμα που δημιούργησε την τεχνολογία Blockchain. Είναι ένα κρυπτονόμισμα πλήρως αποκεντρωμένο (decentralized), ανοικτού κώδικα (open-source) και μη λογοκρινόμενο (censorship-resistant).

Η αρχική υλοποίηση του γράφτηκε σε C++. Μπορούν να γραφούν εφαρμογές (πχ για διαχείριση wallet σε οποιαδήποτε γλώσσα.

Σαν κρυπτονόμισμα δεν μπορεί να χρησιμοποιηθεί το ίδιο ως πλατφόρμα ανάπτυξης εφαρμογών διαχείρησης εφοδιαστικής αλυσίδας, μπορεί να χρησιμοποιηθεί σαν πλατφόρμα πληρωμών.

Ethereum

Το Ethereum είναι μια δημόσια πλατφόρμα blockchain ανοιχτού κώδικα. Παρόμοια με το Bitcoin Blockchain, είναι αποκεντρωμένο και επιπλέον υποστηρίζει έξυπνα συμβόλαια (smart contrcts).

Χρησιμοποιεί το Ether, γνωστό ως "προγραμματιζόμενο κρυπτονόμισμα". Η πλατφόρμα χρησιμοποιεί την Ethereum Virtual Machine (EVM). Έχει ενσωματωμένη (builtin) γλώσσα προγραμματισμού την Solidity. Υποστηρίζονται επίσης οι Python, Go , C++.

- Τύπος λογισμικού: open source.
- Υποστηριζόμενοι τύποι block chain: public.
- Υποστηριζόμενες γλώσσες προγραμματισμού: Python, Go , C++.
- Μπορεί να χρησιμοποιηθεί σαν πλατφόρμα για ανάπτυξη εφαρμογών διαχείρισης εφοδιαστικής αλυσίδας για αγροδιατροφικά προϊόντα (πχ Devoleum).

Hyperledger Sawtooth Lake

Το Hyperledger είναι ένα project ανοιχτού κώδικα , το οποίο ξεκίνησε το Δεκέμβριο του 2015 από το Ίδρυμα Linux και έλαβε συνεισφορές από την IBM, την Intel και το SAP Ariba, για να υποστηρίξει τη συνεργατική ανάπτυξη του blockchain και σχετικών εργαλείων, με ιδιαίτερη έμφαση στη βελτίωση της απόδοσης και της αξιοπιστίας

αυτών των συστημάτων . Το Hyperledger Fabric είναι μια πλατφόρμα blockchain, η οποία αναπτύχθηκε αρχικά από την IBM και την Digital Asset, παρέχοντας μια αρθρωτή (modular) αρχιτεκτονική και οριοθέτηση διαφορετικών ρόλων μεταξύ των κόμβων. Οι κόμβοι διακρίνονται σε Peer Nodes και Ordered Nodes. Οι Peer Nodes εκτελούν Smart Contracts (ονομάζονται chaincode στο Fabric) και υπηρεσίες συναίνεσης και συνδρομή. Υποστηρίζουν συναλλαγές και διεπαφή με εφαρμογές. Οι Ordered Nodes, διασφαλίζουν τη συνοχή του blockchain και παραδίδουν τις εγκριθείσες συναλλαγές (confirmed transactions) στους ομότιμους κόμβους του δικτύου και οι πάροχοι υπηρεσιών συνδρομής (MSP), γενικά υλοποιούνται ως αρχή πιστοποίησης (Certificate Authority).

Η Sawtooth Lake είναι μια modular, γραμμένη σε Python με υποστήριξη έξυπνων συμβολαίων.

- Τύπος λογισμικού: open source.
- Υποστηριζόμενοι τύποι block chain: public, private, permissioned.
- Υποστηριζόμενες γλώσσες προγραμματισμού: Python.
- Μπορεί να χρησιμοποιηθεί σαν πλατφόρμα για ανάπτυξη εφαρμογών διαχείρισης εφοδιαστικής αλυσίδας για αγροδιατροφικά προϊόντα.

HydraChain

Το HydraChain αναπτύχθηκε από κοινού από την Brainbot technologies και το Ethereum project. Είναι μια (open source) επέκταση της πλατφόρμας Ethereum, η οποία υποστηρίζει τη δημιουργία κλιμακωτών εφαρμογών που βασίζονται σε blockchain και ανταποκρίνονται σστις απαιτήσεις δημόσιων και κανονιστικών οργανισμών.

- Τύπος λογισμικού: open source.
- Υποστηριζόμενοι τύποι block chain: private, permissioned.
- Υποστηριζόμενες γλώσσες προγραμματισμού: Python.
- Μπορεί να χρησιμοποιηθεί σαν πλατφόρμα για ανάπτυξη εφαρμογών διαχείρισης εφοδιαστικής αλυσίδας για αγροδιατροφικά προϊόντα.

Openchain

Το Openchain αναπτύσσεται από την Coinprism, την εταιρεία πίσω από τα πρότυπο Open Assets (colored coins protocol).

Η Openchain ισχυρίζεται ότι είναι κατάλληλη για διαχείριση ψηφιακών περιουσιακών στοιχείων (digital assets). Έχει μια διαφορετική προσέγγιση από το Bitcoin στην υλοποίηση του Blockchain. Ακολουθεί ένα σύστημα διαχωριζόμενης συναίνεσης (partitioned consensus system). Κάθε εγγραφή του Openchain έχει μία εξουσιοδοτημένη αρχή για την επικύρωση των συναλλαγών, ανάλογα με τα στοιχεία που ανταλλάσσονται. Αυτό, με τη σειρά του, οδηγεί σε μια centralized αρχιτεκτονική (client-server) που ισχυρίζονται ότι είναι πιο αποτελεσματική και αξιόπιστη από μια αρχιτεκτονική από ομότιμους χρήστες.

- Τύπος λογισμικού: open source.
- Υποστηριζόμενοι τύποι block chain: private.
- Υποστηριζόμενες γλώσσες προγραμματισμού: Javascript.
- Μπορεί να χρησιμοποιηθεί σαν πλατφόρμα για ανάπτυξη εφαρμογών διαχείρισης εφοδιαστικής αλυσίδας για αγροδιατροφικά προϊόντα.

Multichain

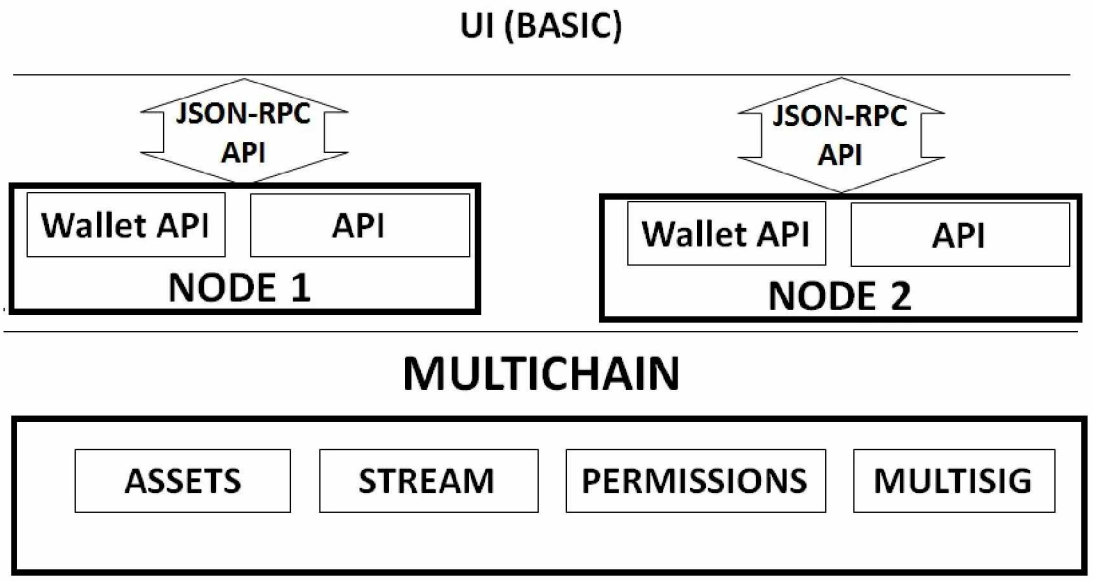
Πρόκειται για μια πλατφόρμα για τη δημιουργία και την ανάπτυξη ιδιωτικών (Private/Permissioned) Blockchains. Είναι μια πλατφόρμα ανοιχτού κώδικα, η οποία βασίζεται στο Bitcoin, αλλά είναι μια βελτιωμένη έκδοση του. Υποστηρίζει πολλά κρυπτονομίσματα. Στην περίπτωση του Multichain δίνεtai έμφαση στον τελικό χρήστη, επιτρέποντας του να ελέγχει αν η αλυσίδα είναι ιδιωτική ή δημόσια, ποιος μπορεί να συνδεθεί στο δίκτυο, το μέγιστο μέγεθος block και τα μεταδεδομένα. Όλα αυτά τα χαρακτηριστικά καλύπτονται από το Multichain και αποτελούν λύση στα προβλήματα που υπάρχουν στο Bitcoin .

Επιπλέον η Multichain, καλύπτει τις περισσότερες περιπτώσεις χρήσης για blockchain. Υποστηρίζει Windows, Linux and Mac servers και διαθέτει ένα εύκολο API καθώς και command-line interface. Έτσι αν είστε πρόθυμοι να αναπτύξετε DApps, τότε το Multichain είναι καλύτερο από το Ethereum.

- Τύπος λογισμικού: open source.
- Υποστηριζόμενοι τύποι block chain: private/permissioned.
- Υποστηριζόμενες γλώσσες προγραμματισμού: Python, C#, JavaScript, PHP, Ruby.
- Μπορεί να χρησιμοποιηθεί σαν πλατφόρμα για ανάπτυξη εφαρμογών διαχείρισης εφοδιαστικής αλυσίδας για αγροδιατροφικά προϊόντα.

Δημιουργία μιας private blockchain με χρήση της πλατφόρμας Multichain

Παρακάτω θα δείξουμε τα βασικά βήματα για το πως μπορούμε πως μπορούμε να στήσουμε μια private blockchain, χρησιμοποιώντας την πλατφόρμα Multichain σε Windows, σύμφωνα με σχτικό οδηγό που υπάρχει στο επίσημο site του Multichain βλ. σχετικά [70].



Εικόνα 7.1 - Αρχιτεκτονική μιας Multichain πλατφόρμας

Ο κόμβος (node) και το πορτοφόλι (wallet) είναι δύο ξεχωριστά υποσυστήματα του MultiChain. Ο κόμβος (full node) παρακολουθεί την συνολική κατάσταση του blockchain και ενημερώνει το πορτοφόλι (wallet) για τις συναλλαγές που το αφορούν. Το wallet περιέχει επιπλέον και τα κλειδιά (private, public) του χρήστη. Ο κόμβος τροφοδοτεί συχνά με πληροφορίες το πορτοφόλι.

Εγκατάσταση του MultiChain σε Windows PC

- Από το link https://www.multichain.com/download-install επιλέγουμε Installing MultiChain Community on Windows.
- Κατεβάζουμε το ZIP αρχείο.
- Εξάγουμε τα περιεχόμενα του σε ένα φάκελο που θα στήσουμε το Multichain (install directory). Μαζί με τα extracted **.exe** files, υπάρχει και ένα **README.txt** file με οδηγίες εγκατάστασης σε ένα Windows PC.

- Καταχωρούμε το multichain program directory στο PATH των Windows. Το default multichain directory στα Windows είναι: C:\Users\{UserName}\AppData\Roaming\MultiChain\

Δημιουργία ενός blockchain και σύνδεση κόμβων σε αυτό

Θα δημιουργήσουμε ένα private blockchain στο PC μας.
Θα δημιουργήσουμε 2 κόμβους στο ίδιο PC και θα εκτελέσουμε μια συναλλαγή.

Σε ένα πραγματικό σενάριο, θα είχαμε τους κόμβους (Nodes ή Servers) σε διαφορετικά PCs (συνδεδεμένα στο ίδιο δίκτυο) που θα αλληλεπιδρούσαν μεταξύ τους με τον ίδιο τρόπο. Εναλλακτικά, μπορούμε να εγκαταστήσουμε ένα VM (πχ μπορούμε να χρησιμοποιήσουμε το Oracle VM VirtualBox με το απαραίτητητο configuration) ή Docker containers αντί της virtualization μεθόδου.

Θα δημιουργήσουμε ένα blockchain με το όνομα **tutchain**. Ανοίγουμε μια κονσόλα command line στο install directory και τρέχουμε την παρακάτω εντολή:
multichain-util.exe create tutchain

Θα δείτε ένα μήνυμα που δηλώνει ότι η αλυσίδα δημιουργήθηκε (generated) με επιτυχία. Επίσης, ίσως παρατηρήσετε το μήνυμα σχετικά με το αρχείο params.dat. Αυτό το αρχείο περιέχει παραμέτρους που μπορείτε να αλλάξετε και αφορούν δικαιώματα, τη συναίνεση κλπ. Μέσα σε αυτόν τον κατάλογο θα βρείτε επίσης ένα αρχείο multichain.conf. Αυτό το αρχείο περιέχει το όνομα χρήστη και τον κωδικό πρόσβασής σας.

```
> multichain-util.exe create tutchain

MultiChain 1.0.4 Utilities (latest protocol 10010)

Blockchain parameter set was successfully generated.
You can edit it in C:\Users\ykarav\AppData\Roaming\MultiChain\tutchain\params.dat before running multicha
nd for the first time.

To generate blockchain please run "multichaind tutchain -daemon".
```

Τώρα αρχικοποιούμε (initialize) το blockchain και δημιουργούμε (mine) το block γένεσης (genesis block).

Εκτελέστε την ακόλουθη εντολή:

multichaind.exe tutchain -daemon

```
> multichaind.exe tutchain -daemon

MultiChain 1.0.4 Daemon (latest protocol 10010)

Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind tutchain@192.168.233.1:6753

This host has multiple IP addresses, so from some networks:
multichaind tutchain@192.168.136.1:6753
multichaind tutchain@172.16.212.153:6753

Listening for API requests on port 6752 (local only - see rpcallowip setting)

Node ready.
```

Θα ενημερωθείτε ότι ο κόμβος έχει ξεκινήσει και μετά από μερικά δευτερόλεπτα, ότι βρέθηκε το genesis block. Θα δείτε επίσης το IP και το PORT, δλδ τη διεύθυνση κόμβου (node address) και την θύρα που μπορούν να χρησιμοποιήσουν άλλοι κόμβοι για να συνδεθούν με αυτήν την αλυσίδα. Εφόσον δημιουργήσαμε την αλυσίδα, έχουμε τα πλήρη δικαιώματα (permissions) για αυτήν.

Για να δούμε πληροφορίες σχετικά με το tutchain, τρέχουμε την παρακάτω εντολή:

multichain-cli.exe tutchain getinfo

Θα δούμε το ακόλουθο JSON με πληροφορίες σχετικά με την αλυσίδα. Επίσης, παρατηρούμε την κλήση JSON-RPC (επισημαίνεται με κόκκινο χρώμα).

```
> multichain-cli.exe tutchain getinfo
{"method":"getinfo","params":[],"id":1,"chain_name":"tutchain"}

{
    "version" : "1.0.4",
    "nodeversion" : 10004901,
    "protocolversion" : 10010,
    "chainname" : "tutchain",
    "description" : "MultiChain tutchain",
    "protocol" : "multichain",
    "port" : 6753,
    "setupblocks" : 60,
    "nodeaddress" : "tutchain@192.168.233.1:6753",
    "burnaddress" : "1XXXXXXXDzXXXXXXfXXXXXXXQbXXXXXXWox2PK",
    "incomingpaused" : false,
    "miningpaused" : false,
    "walletversion" : 60000,
    "balance" : 0.00000000,
    "walletdbversion" : 2,
    "reindex" : false,
    "blocks" : 39,
    "timeoffset" : 0,
    "connections" : 0,
    "proxy" : "",
    "difficulty" : 0.00000006,
    "testnet" : false,
    "keypoololdest" : 1525941629,
    "keypoolsize" : 2,
    "paytxfee" : 0.00000000,
    "relayfee" : 0.00000000,
    "errors" : ""
}
```

Δίνουμε την ακόλουθη εντολή για να δούμε τα δικαιώματά (permissions) μας:

multichain-cli.exe tutchain listpermissions

```
> multichain-cli.exe tutchain listpermissions
{"method":"listpermissions","params":[],"id":1,"chain_name":"tutchain"}

[
    {
        "address" : "1Br9vA83tQjz2t751mQowKpfhz2wLrQCdRMYdX",
        "for" : null,
        "type" : "mine",
        "startblock" : 0,
        "endblock" : 4294967295
    },
```

Θα δείτε μια πλήρη λίστα των δικαιωμάτων σας, όπως:

“mine”, “create”, “admin”, “connect”, κλπ.

Μέχρι στιγμής, έχετε ένα blockchain σε λειτουργία και λειτουργεί με έναν μόνο κόμβο συνδεδεμένο σε αυτό - τον υπολογιστή σας. Ας δημιουργήσουμε έναν δεύτερο κόμβο και να τον συνδέσουμε με την αλυσίδα μας.

Η blockchchain βρίσκεται στο φάκελο:

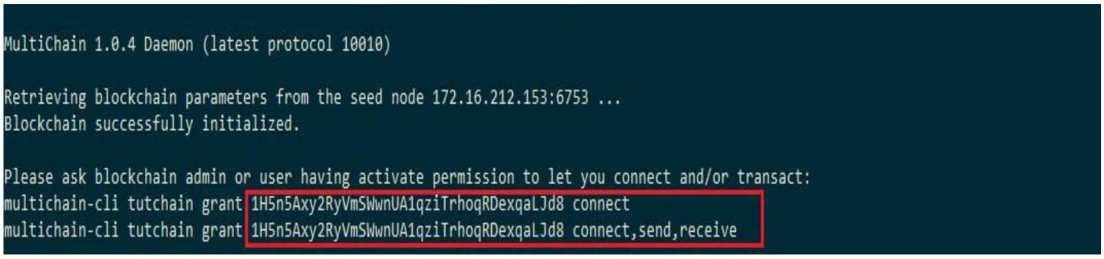
C:\Users\{UserName}\AppData\Roaming\MultiChain

Θα δημιουργήσουμε έναν δεύτερο κόμβο στο ίδιο PC.

Δημιουργούμε φάκελο με το όνομα **MultiChain_Other** μέσα στον φάκελο Roaming**.**
C:\Users\{UserName}\AppData\Roaming\MultiChain_Other

Δεδομένου ότι η αλυσίδα μας ήδη υπάρχει, κάθε νέος κόμβος δεν θα έχει πλήρη δικαιώματα.
Επομένως ο node 1 πρέπει να εκχωρήσει την άδεια "connect" στον node 2.
(σ.σ επειδή δημιουργούμε τον 2ο κόμβο στο ίδιο PC, στην εντολή θα δώσουμε παραμέτρους για να υποδείξουμε τη διαδρομή προς τον δεύτερο κόμβο και επίσης τις θύρες που θα χρησιμοποιηθούν για τη σύνδεση).

Για τον δεύτερο κόμβο, ανοίγουμε νέα κονσόλα command line στο install directory και τρέχουμε την παρακάτω εντολή:
multichaind.exe -datadir=C:\Users\user\AppData\Roaming\MultiChain_Other -port=10255 -rpcport=10254 tutchain@172.16.212.153:6753



Θα λάβουμε σαν απάντηση, ότι το blockchain ξεκίνησε με επιτυχία, αλλά δεν έχουμε δικαιώματα σύνδεσης.
(σ.σ επειδή τρέχουμε την πλατφόρμα σε Windows, όλες οι εντολές - όπως η grant - ξεκινούν με *multichain-cli tutchain*).
Θα μας δοθεί επίσης η διεύθυνση του node :
1H5n5Axy2RyVmSWwnUA1qziTrhoqRDexqaLJd8

Από την κονσόλα του πρώτου node, χορηγούμε δικαιώματα σύνδεσης (connect permission) για τη διεύθυνση του πορτοφολιού του κόμβου:
multichain-cli.exe tutchain grant 1H5n5Axy2RyVmSWwnUA1qziTrhoqRDexqaLJd8 connect

```
> multichain-cli.exe tutchain grant 1H5n5Axy2RyVmSWwnUA1qziTrhoqRDexqaLJd8 connect
{"method":"grant","params":["1H5n5Axy2RyVmSWwnUA1qziTrhoqRDexqaLJd8","connect"],"id":1,"chain_name":"tutchain"}

30109747fd4683fd47dc2fbb1367ac462b511ea03739d81b7120a989e37c019f
```

Όπως μπορείτε να δείτε, δώσαμε επιτυχώς δικαιώματα σύνδεσης στο node 2.
Επίσης αυτή η συναλλαγή δημιούργησε έναν Hash (ο αριθμός 30109747 ...).
Τώρα, ο node 2 μπορεί να συνδεθεί στον node 1.

multichaind.exe -datadir=C:\Users\user\AppData\Roaming\MultiChain_Other -port=10255 -rpcport=10254 tutchain@172.16.212.153:6753

```
> multichaind.exe -datadir=C:\Users\ykarav\AppData\Roaming\MultiChain_Other -port=10255 -rpcport=10254 tutchain@172.16.212.153:6753

MultiChain 1.0.4 Daemon (latest protocol 10010)

Chain tutchain already exists, adding 172.16.212.153:6753 to list of peers

Other nodes can connect to this node using:
multichaind tutchain@192.168.233.1:10255

This host has multiple IP addresses, so from some networks:
multichaind tutchain@192.168.136.1:10255
multichaind tutchain@172.16.212.153:10255

Listening for API requests on port 10254 (local only - see rpcallowip setting)

Node ready.
```

Πλέον έχουμε ένα blockchain που τρέχει σε ένα Windows PC με 2 κόμβους.
Γενικά, η πλατφόρμα Multichain παρέχει ένα πλήρες API και πλήρης υποστήριξη για developers στο σχετικό site. Για περισσότερες εντολές μπορούμε να ανατρέξουμε στο link https://www.multichain.com/developers/json-rpc-api/ . Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι εντολές για asset management), advanced node control, wallet control κλπ.

Ολοκληρώνονας την παρούσα ενότητα, επισημαίνουμε ότι σκοπός ήταν να δείξουμε ότι το blockchain δεν είναι κάποια «εξωτική» τεχνολογία και ότι υπάρχουν πολλές open source πλατφόρμες ανάπτυξης, που θα μπορούσε να χρησιμοποιήσει μια επιχείρηση για να κάνει την μετάβαση στη νέα τεχνολογία (ξεκινώντας από single-use εφαρμογές).

ΚΕΦΑΛΑΙΟ 8 – ΜΕΛΕΤΗ ΕΦΑΡΜΟΓΗΣ: ΜΙΑ ΑΠΛΗ ΑΓΡΟΔΙΑΤΡΟΦΙΚΗ ΑΛΥΣΙΔΑ

Εισαγωγικές έννοιες

- **JSON file format -** Ένα αρχείο JSON είναι ένα αρχείο που αποθηκεύει απλές δομές δεδομένων (data structures) και αντικείμενα (objects), στη μορφή JavaScript Notation Object (JSON), η οποία είναι μια τυπική μορφή ανταλλαγής δεδομένων. Χρησιμοποιείται κυρίως για τη μετάδοση δεδομένων μεταξύ μιας web application και ενός server. Το JSON χρησιμοποιείται συνήθως στον προγραμματισμό Ajax Web application αλλά και από την πλατφόρμα Multichain.
- **Savoir -** Είναι ένα JSON-RPC API για την πλατφόρμα Multichain σε python .
- **Pip -** Είναι ο package installer για Python.
- **Logging -** Logging facility για την Python
- **Wget** (World Wide Web and get) - Είναι ένα sotware για να κατεβάζει αρχεία από web servers. Είναι μέρος του GNU Project.
- **Data stream network (DSN) -** Ένα δίκτυο ροής δεδομένων (DSN), είναι μια κλιμακωτή υποδομή που παρέχει μια μόνιμη και ασφαλή σύνδεση, σε μια web application, ένα κινητό, ή μια έξυπνη συσκευή IoT, επιτρέποντας την αποστολή και λήψη δεδομένων (bi-directional data streaming).
- **PubNub -** Το PubNub είναι ένα παγκόσμιο Data Stream Network (DSN) και και εταιρεία παροχής υπηρεσιών δικτύου σε πραγματικό χρόνο (realtime infrastructure-as-a-service - IaaS). Χρησιμοποιείται για την ανάπτυξη εφαρμογών σε πραγματικό χρόνο.Το PubNub μπορεί να χρησιμοποιηθεί για την γρήγορη προώθηση μικρών μηνυμάτων σε μία ή περισσότερες συσκευές (smartphones, tablet, laptops, microcontrollers κλπ.), για αμφίδρομη επικοινωνία μεταξύ συσκευών. Χρησιμοποιείται στην ανάπτυξη εφαρμογών blockchains.
- **PubNub components**
    - *publisher (sends data through a channel)*
    - *subscriber (receives data through a channel)*

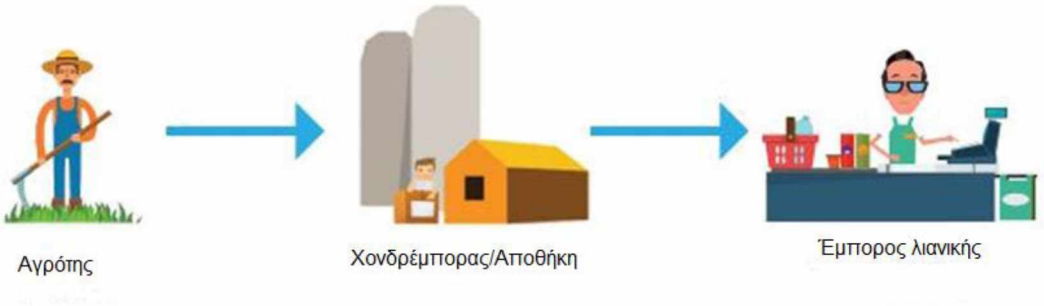
- *message (blocks of data that get published to channels - usually in JSON format)*
- *channel (Messages sent through PubNub are sent on a "channel." Channels are unique for each key set - the publish and subscribe keys).*
- *channel-group (each device can have its own channel, while also subscribing to a group channel and a global channel where all devices can receive data simultaneously)*

- **PubNub's core services**
  - *Publish/Subscribe* - As soon as data is uploaded (published), PubNub will immediately push out that data to anyone (or thing/device) that was interested in it (subscribers). Subscribers will continue to receive these data streams in realtime as more data is published.
  - *PubNub Functions* - PubNub Functions is serverless, allowing you to deploy JavaScript directly into the PubNub DSN. This enables you to run code directly inside the PubNub network, which executes on your data as it is being streamed between senders and receivers

Το απλοποιημένο σενάριο (simplistic scenario)

Όπως είδαμε σε προηγούμενη ενότητα, οι πραγματικές σχέσεις μεταξύ των φορέων/ρόλων που συμμετέχουν σε μια εφοδιαστική αλυσίδα, είναι συχνά περίπλοκες. Οι οργανισμοί έχουν κατά κανόνα πολλούς προμηθευτές σε διαφορετικές βαθμίδες που συμμετέχουν σε ένα συγκεκριμένο προϊόν και οι προμηθευτές είναι συνήθως μη αποκλειστικοί για τον οργανισμό που εξετάζεται.

Ας εξετάσουμε το πιο απλό σενάριο, όπου υποθέτουμε ότι υπάρχει μόνο ένας διανομέας στην όλη διαδικασία, ο οποίος προμηθεύεται προϊόντα από έναν αγρότη και τα διαθέτει σε ένα κατάστημα λιανικής πώλησης.



Εικόνα 8.1 – Απλοποιημένο σενάριο αγροδιατροφικής αλυσίδας

Ένας αγρότης (farmer) πωλεί το προϊόν του σε έναν διανομέα/χονδρέμπορο (distributor) ο οποίος με τη σειρά του, το αποθηκεύει στις διάφορες αποθήκες του, προκειμένου στην συνέχεια να το διαθέσει στα καταστήματα λιανικής πώλησης (retail stores).

Θεωρούμε ότι το δίκτυο της αλυσίδας εφοδιασμού, έχει τη γεωγραφική κάλυψη και εμβέλεια, καθώς και την ικανότητα κλιμάκωσης, προκειμένου να ανταποκριθεί σε οποιαδήποτε διακύμανση (αυξομείωση) της προσφοράς και της ζήτησης.
Επίσης θεωρούμε ότι τόσο ο αγρότης όσο και ο λιανοπωλητής δεν έχουν την δυνατότητα ή τα μέσα, για να συναλλάσσονται άμεσα μεταξύ τους. Επιπλέον, θεωρούμε ότι όλη η διαδικασία, λειτουργεί στην λογική μιας κοινοπραξίας ή συνεταιρισμού (με την έννοια ότι θέλουμε όλες οι πλευρές να επωφελούνται ισότιμα και δίκαια από την συμμετοχή τους σε αυτήν). Η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί σε αυτή την περίπτωση, καθώς μπορεί να εξασφαλίσει την τήρηση της βασικής αρχής της ανταλλαγής πληροφοριών και της διαφάνειας.

Όπως είπαμε σε προηγούμενη ενότητα, προκειμένου μια επιχείρηση να κάνει την μετάβαση στην Τεχνολογία BlockChain, θα πρέπει πρώτα να αξιολογήσει το επιχειρηματικό πρόβλημα, να δει αν η τεχνολογία έχει εφαρμογή στην περίπτωση του, να επιλέξει την κατάλληλη πλατφόρμα blockchain και στη συνέχεια να προχωρήσει στην σχεδίαση μιας πιλοτικής εφαρμογής (drafted application).

Πρέπει να λοιπόν αρχικά να θέσουμε την ερώτηση:
Τι θέλουμε να βελτιστοποιήσουμε με την σχεδιαζόμενη εφαρμογή;

Σε μια τυπική εφοδιασμού αγροτικών προϊόντων, θα μπορούσαμε να εντοπίσουμε κακές πρακτικές και μονοπώλια. Είναι γνωστό το γεγονός ότι τις περισσότερες φορές, οι αγρότες συνήθως δεν πετυχαίνουν να πωλήσουν το προϊόν τους στους διανομείς (χονδρέμπορους) σε μια δίκαιη τιμή. Τις περισσότερες φορές οι διανομείς «ρίχνουν» τις τιμές στις οποίες αγοράζουν ένα προϊόν, μειώνοντας τεχνητά τη ζήτηση σε σχέση με την προσφορά. Στην συνέχεια καρπώνονται οι ίδιοι το μεγαλύτερο ποσοστό κέρδους, διανέμοντας σε αρκετά υψηλότερες τιμές στα καταστήματα λιανικής πώλησης, τα προϊόντα που αγοράσανε σε χαμηλότερη τιμή από τον παραγωγό/αγρότη. Στο τέλος και ο τελικός καταναλωτής (consumer), αγοράζει το προϊόν σε πολύ υψηλότερη τιμή, από την τιμή που εισπράττει ο αγρότης/παραγωγός.

Σε μια τέτοια κατάσταση, ο καλύτερος τρόπος για να διορθωθεί η στρέβλωση στην όλη αλυσίδα, είναι να υπάρχει διαφάνεια (transparency), σε όλα τα ενδιάμεσα στάδια παραγωγής και διάθεσης των προϊόντων. Εάν διασφαλιστεί η διαφάνεια, τότε οποιαδήποτε αύξηση της ζήτησης λόγω πραγματικών εξωτερικών παραγόντων μπορεί να κεφαλαιοποιηθεί από όλα τα μέρη, αντί μόνο από λίγους που θα προσπαθήσουν να εκμεταλλευτούν το σύστημα παραγωγής και διάθεσης, προς όφελός τους. Επίσης οποιαδήποτε πραγματική μείωση της ζήτησης (από πλευράς τελικού καταναλωτή), θα οδηγούσε σε αυτορρύθμιση του συστήματος, είτε με μείωση των τιμών, είτε με μείωση της παραγωγής.

Ένα σύστημα με διαφανείς επιχειρηματικές διαδικασίες, θα λειτουργούσε αποτελεσματικά και θα μπορούσε να ωφελήσει όλα τα μέρη με πολλούς τρόπους. Εξασφαλίζοντας την ισότιμη δυνατότητα παροχής υπηρεσιών/προϊόντων και την δίκαιη τιμολόγηση για όλα τα μέρη που εμπλέκονται στην όλη διαδικασία, αυξάνεται σίγουρα ο ανταγωνισμός, προς όφελος του τελικού καταναλωτή που θα απολαμβάνει υψηλότερη ποιότητα προϊόντων και καλύτερες τιμές. Από την άλλη οι παραγωγοί μπορούν να αυξήσουν το μέγεθος της παραγωγής τους και οι διανομείς/πωλητές, μπορούν να επεκτείνουν το δίκτυο σε μεγαλύτερες αγορές, μεγιστοποιώντας έτσι το κέρδος τους.

Η τεχνολογία Blockchain επιβάλλει εγγενώς ένα επίπεδο ασφάλειας που απαγορεύει σε οποιονδήποτε να μεταβάλλει τις συναλλαγές (transactions) από την στιγμή που θα εισαχθούν στην αλυσίδα. Παρέχει δηλαδή στο σύστημα που περιγράψαμε παραπάνω, έναν τρόπο εντοπισμού και ελέγχου κάθε συναλλαγής έτσι ώστε να μπορεί να αντιμετωπιστεί οποιαδήποτε παρατυπία/ανωμαλία(irregularity), όπως προβλήματα ποιότητας, εκπλήρωσης παραγγελίας ή αδικαιολόγητες διακυμάνσεις της τιμής. Επιπλέον δίνει την δυνατότητα παρακολούθησης της ποσότητας των προϊόντων (assets quantity) που παραμένουν στο σύστημα μετά από κάθε συναλλαγή. Άρα η τεχνολογία Blockchain έχει εφαρμογή στην περίπτωση και αποτελεί λύση στο πρόβλημα.

Στην συνέχεια θα πρέπει να επιλέξουμε την κατάλληλη πλατφόρμα blockchain και να σχεδιάσουμε την πιλοτική εφαρμογή (drafted application).

Υπάρχουν πολλές πλατφόρμες Blockchain και η κάθε μια ισχυρίζεται ότι είναι καλύτερη από την άλλη. Σε προηγούμενη ενότητα είδαμε κάποια βασικά χαρακτηριστικά της Multichain, η οποία είναι open source, υποστηρίζει private blockchains, έχει άριστο assets management, μπορεί να υποστηρίξει διάφορα κρυπτονομίσματα ενώ ταυτόχρονα είναι και BitCoin compatible.

Οντότητες/μέρη (entities) στην αλυσίδα

Σε αυτό το σενάριο αλυσίδας εφοδιασμού, μιλάμε για τρεις οντότητες ή μέρη που αποτελούν μέρος του συστήματος. Έχουμε έναν αγρότη, ο οποίος είναι ιδιοκτήτης της γεωργικής γης (Farm Land).

Έχουμε έναν διανομέα ο οποίος έχει στην ιδιοκτησία του μια αποθήκη (Warehouse) και έναν ιδιοκτήτη καταστήματος λιανικής πώλησης (Retail Store).

Στόχος μας είναι να επεξεργαστούμε τις συναλλαγές (αγοραπωλησίες) μεταξύ αυτών των τριών μερών/οντοτήτων για να ολοκληρώσουμε το στόχο του συστήματος, δηλαδή να φέρουμε τα αγροτικά προϊόντα από τον αγρότη μέχρι το σημείο λιανικής πώλησης και να τα καταστήσουμε προσιτά στους τελικούς καταναλωτές.

Αντιστοίχιση οντοτήτων (entities) με έννοιες του blockchain στο σενάριο μας

- Node - Κάθε οντότητα που εμπλέκεται σε transactions συνδέεται σε έναν υπολογιστή (συνδεδεμένο στο internet) για να ξεκινήσει η transaction. Αυτός ο υπολογιστής αποτελεί ένα κόμβο.
- Address – Σε κάθε κόμβο αντιστοιχεί μια μοναδική διεύθυνση, η οποία εκχωρείται στον node όταν συνδέεται στο blockchain.
- Asset - Οτιδήποτε έχει αξία και εμπλέκεται σε μια συναλλαγή θεωρείται ως πάγιο (asset). Έτσι τόσο τα προϊόντα, όσο και τα χρήματα είναι assets. Κάθε asset μπορεί να έχει σχετικές παραμέτρους (attributes). Αυτές οι πρόσθετες παράμετροι μπορούν να χρησιμοποιηθούν για την μέτρηση της αποτελεσματικότητας του συστήματος και για να εξασφαλιστεί υψηλότερη ποιότητα, σε μια δίκαιη τιμή. Κάθε τέτοια εγγραφή (record) ακολουθεί την πορεία του asset στο σύστημα και σχηματίζει μια αλυσίδα με άλλα αρχεία εγγραφών, έως ότου το asset εγκαταλείψει το σύστημα.
- Transaction - Κάθε πράξη στο blockchain είναι μια συναλλαγή. Δημιουργία ενός asset, έναρξη μιας διαδικασίας ανταλλαγή assets ή επιβεβαίωση μιας διαδικασίας ανταλλαγής assets. Κάθε μία από αυτές είναι μια ξεχωριστή συναλλαγή. Ο αγρότης που πωλεί την καλλιέργεια του, καθορισμένης ποσότητας, στον διανομέα και παίρνει χρήματα ισοδύναμης και προκαθορισμένης αξίας είναι ένα παράδειγμα ανταλλαγής. Στο Blockchain, ξεκινάει μια ανταλλαγή και αφού ολοκληρωθεί και επαληθευτεί, προστίθεται στην αλυσίδα. Η συναλλαγή περιέχει που σχετίζονται με assets.
- Ledger - Είναι η λίστα όλων των συναλλαγών σε ολόκληρη την αλυσίδα. Όλοι οι κόμβοι στην αλυσίδα έχουν ένα αντίγραφο του. Έτσι οι συναλλαγές είναι αμετάβλητες.
- Exchange – Σαν ανταλλαγή θεωρούμε κάθε αγοραπωλησία (buy/sell) μεταξύ οντοτήτων. Σε μια ανταλλαγή, η μια οντότητα θα δίνει ένα asset σε μια άλλη και θα λαμβάνει το ισοδύναμο της αξίας του από την άλλη.

Σχεδιάζοντας την εφαρμογή

1. Αρχίζουμε με την δημιουργία Node instances στο Multichain για τα τρία μέρη, τον αγρότη, τον διανομέα και το κατάστημα λιανικής πώλησης. Υποθέτουμε ότι έχουν

όλοι έναν υπολογιστή που συνδέεται με το σύστημα της αλυσίδας εφοδιασμού και είναι ενεργοπος κόμβος στο Blockchain.

2. Το σύστημα εκδίδει περιουσιακά στοιχεία (issue assets) στις αντίστοιχες οντότητες, τα οποία θα τους επιτρέψουν να συμμετάσχουν στη διαδικασία αγοραπωλησίας (exchanges) στο πλαίσιο αυτού του συστήματος αλυσίδας εφοδιασμού. Για τον αγρότη, το περιουσιακό στοιχείο (asset) είναι το αγροτικό προϊόν, (συγκομιδή καλλιέργειας). Για τον διανομέα/χονδρέμπορο και το κατάστημα λιανικής πώλησης, περιουσιακό στοιχείο (asset) είναι τα χρήματα. Από την άποψη του blockchain, αυτό είναι ένα είδος συναλλαγής (transaction).
3. Ξεκινάμε μια αγοραπωλησία (exchange) μεταξύ του αγρότη και του διανομέα που κατέχει μια αποθήκη. Αυτό στον πραγματικό κόσμο, είναι το αποτέλεσμα μιας σύμβασής, για ανταλλαγή περιουσιακών στοιχείων. Αυτή είναι η πρώτη φυσική συναλλαγή στη διαδικασία.
4. Μετά την έναρξη της αγοραπωλησίας, ζητάμε από το σύστημα να ενημερώσει το υπόλοιπο του ενεργητικού (asset balance) και στα δύο μέρη. Ως αποτέλεσμα, μπορούμε να δούμε το επικαιροποιημένο υπόλοιπο, που αντανακλά ότι μια συγκεκριμένη περιουσιακού στοιχείου του αγρότη (προϊόν) τώρα ανήκει στην αποθήκη, σε αντάλλαγμα περιουσιακού στοιχείου της αποθήκης (χρήματα).
5. Το ακατέργαστο περιουσιακό στοιχείο, αλλάζει σε ένα μεταποιημένο περιουσιακό στοιχείο. Στην αποθήκη, το αγαθό που παραδίδει ο αγρότης είναι η ακατέργαστη σοδειά. Δεδομένου ότι ο διανομέας θα το πουλήσει στην λιανική κατανάλωση, θα πρέπει να το συσκευάσει σε πακέτα που είναι κατάλληλα για λιανική πώληση και κατανάλωση. Αυτό είναι ένα προαιρετικό βήμα και εξαρτάται από το πώς ο ιδιοκτήτης αποθήκης/διανομέας, θέλει να εμπορεύεται το προϊόν του περαιτέρω. Ο μετασχηματισμός του περιουσιακού στοιχείου είναι επίσης ένα είδος συναλλαγής για το Blockchain.
6. Η αποθήκη είναι τώρα εφοδιασμένη με συσκευασμένα πρϊόντα και ο διανομέας που είναι ιδιοκτήτης της αποθήκης, θέλει να πουλήσει στον ιδιοκτήτη του καταστήματος λιανικής πώλησης. Ως εκ τούτου, το σύστημα εκκινεί τώρα μια ακόμη ανταλλαγή μεταξύ της αποθήκης και του καταστήματος λιανικής πώλησης. Αυτή είναι η δεύτερη φυσική συναλλαγή στη διαδικασία.
7. Και πάλι, μετά την έναρξη της αγοραπωλησίας, ζητάμε από το σύστημα να ενημερώσει το υπόλοιπο του ενεργητικού. Μόλις γίνει αυτό, μπορούμε να δούμε ότι assets της αποθήκης (συσκευασμένα προϊόντα) μεταφέρονται στο κατάστημα

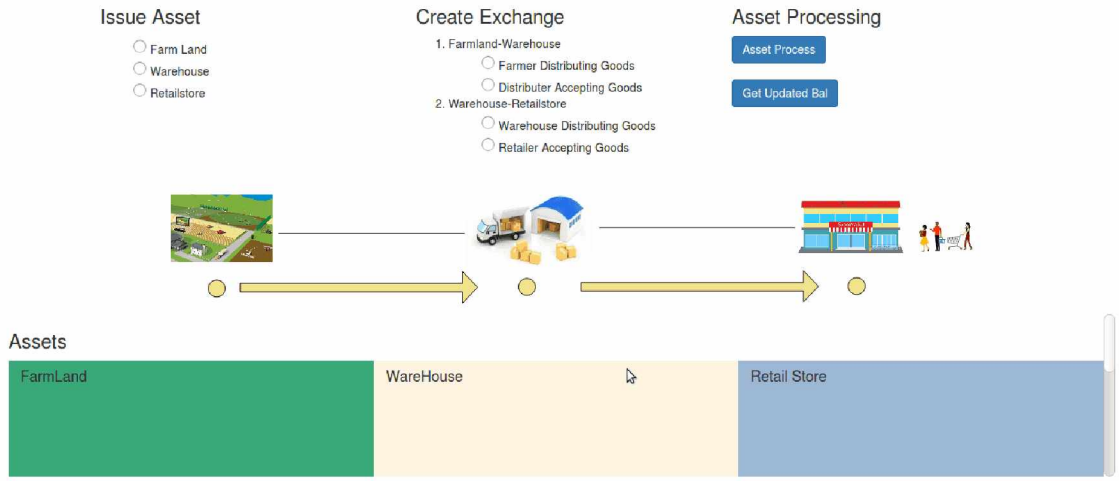
λιανικής πώλησης. Σε αντάλλαγμα, η αποθήκη δέχεται assets (χρήματα) από τον ιδιοκτήτη.Με αυτόν τον τρόπο, ακατέργαστα προϊόντα μεταφέρονται σε όλο το σύστημα και καταλήγουν ως συσκευασμένα προϊόντα στο κατάστημα λιανικής πώλησης.

8. Το κατάστημα λιανικής πώλησης μπορεί τώρα να πουλήσει αυτό το απόθεμα στον τελικό καταναλωτή σε υψηλότερη τιμή, προκειμένου να εξασφαλίσει το κέρδος του. Εάν αυτή η συναλλαγή περιλαμβάνεται στο Blockchain τότε όλα τα μέρη μπορούν να δουν το κέρδος του τελικού πωλητή προς τον καταναλωτή.

Σε ένα «συνεταιριστικό» σύστημα με διαφάνεια και δίκαιη πολιτική κατανομής των κερδών, η προσέγγιση αυτή μπορεί να εξασφαλίσει ότι τυχόν πλεόνασμα κερδών θα επιστρέψει στο σύστημα, ωφελόντας τόσο τον αγρότη/παραγωγό όσο και τον διανομέα/χονδρέμπορα.

Διεπαφή με χρήστες (Users Interface)

Το user interface (UI) των χρηστών και των συναλλαγών που περιγράψαμε παραπάνω, με το blockchain μπορεί να γίνεται μέσω ενός web application στην παρακάτω μορφή:



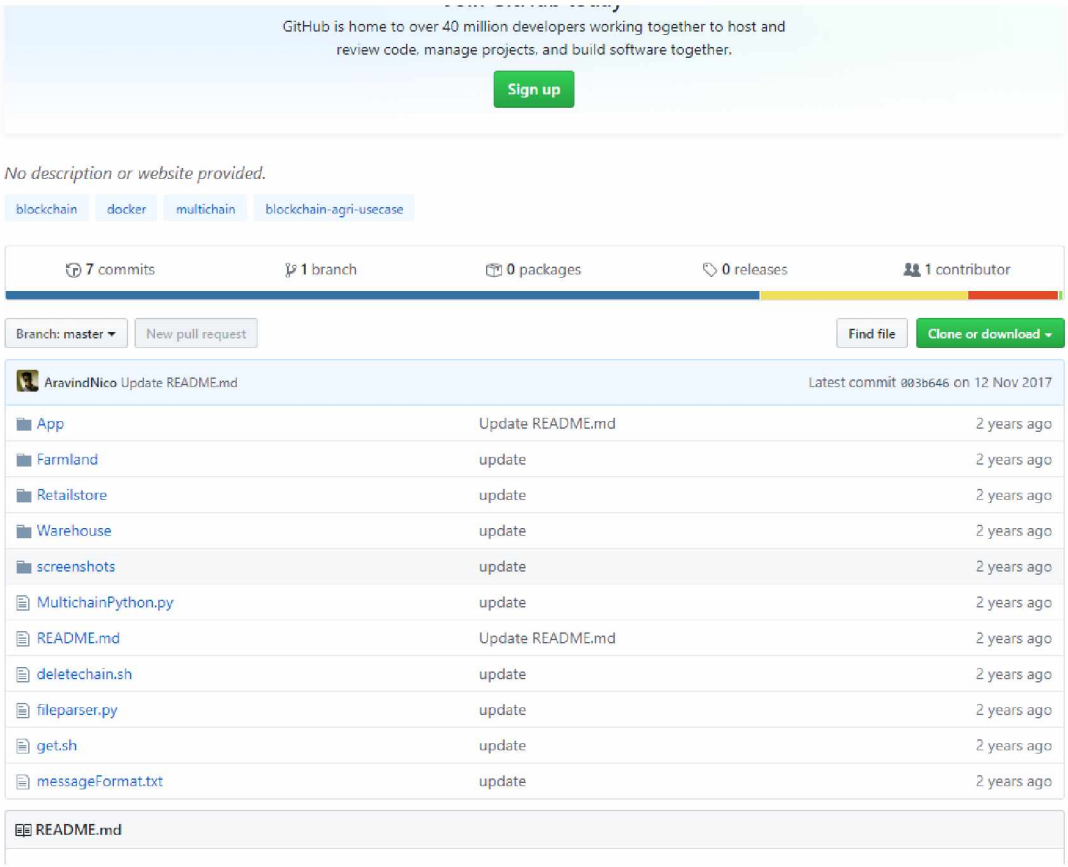
Εικόνα 8.2 – UI της web application για την εφαρμογή

Παρουσίαση σχετικού open-source code στο Github

Θα παρουσιάσουμε ένα demo source που υλοποιεί το παραπάνω σενάριο μιας απλής αγροδιατροφικής αλυσίδας. Ολόκληρο το πακέτο κώδικα της εφαρμογής υπάρχει στο Github:

AravindNico, “Blockchain. Agri_usecase”,

https://github.com/AravindNico/blockchain_agri_usecase



Εικόνα 8.3 – open source code στο GiHub

Η εφαρμογή μπορεί να τρέξει σε Linux και απαιτεί την εγκατάσταση των παρακάτω:

- pip
- wget
- multichain (http://www.multichain.com/download-install/)
- Savoir (https://github.com/DXMarkets/Savoir)
- Pubnub==3.8.3 (https://www.pubnub.com/docs/python/pubnub-python-sdk)
- logging
- git

MultichainPython.py
Υλοποιεί λειτουργικότητα του blockchain
Κάνει χρήση API calls (στην πλατφόρμα Multichain) με χρήση Savoir wrapper.

App folder
Υλοποιεί το UI της web application
blockchainui.html
index.js
Τα βήματα της διαδικασίας στην αλυσίδας εφοδιασμού που περιγράψαμε νωρίτερα είναι:
Βήμα 1: IssueAsset procedure
1.Click on the radio button under IssueAsset to issue FARMLAND asset
2.Click on the radio button under IssueAsset to issue WAREHOUSE asset
3.Click on the radio button under IssueAsset to issue RETAILSTORE asset
Βήμα 2: Create Exchange procedure (FARMLAND-WAREHOUSE)
Click on the radio button Create Exchange to issue FARMLAND-WAREHOUSE asset
Βήμα 3: Decode Exchange procedure (FARMLAND-WAREHOUSE)
Click on the radio button Decode Exchange to issue FARMLAND-WAREHOUSE asset
Βήμα 4: Getting updated asset balances
Click on the "Get Updated Bal" button to get the upated balances of each asset
Βήμα 5: Asset Processing
Click on the AssetProcess button to process the raw farmland asset to processed warehouse asset.
Βήμα 6: Create Exchange procedure (WAREHOUSE-RETAILSTORE)
Click on the radio button Exchange heading to issue WAREHOUSE-RETAILSTORE asset
Βήμα 7: Decode Exchange procedure (WAREHOUSE-RETAILSTORE)
Click on the radio button to issue WAREHOUSE-RETAILSTORE asset
Βήμα 8: Getting updated asset balances
Click on the "Get Updated Bal" to get the upated balances of each asset

Farmland folder
Υλοποιεί λειτουργικότητα της οντότητας FARMLAND.
farmland.py

Retailstore folder
Υλοποιεί λειτουργικότητα της οντότητας RETAILSTORE.
retailstore.py

Warehouse folder
Υλοποιεί λειτουργικότητα της οντότητας WAREHOUSE.
warehouse.py

Η επικοινωνία μεταξύ των modules του κώδικα έχει όπως παρακάτω:

```
Pubnub Channels Used
==============
1.farmland
2.warehouse
3.retailstore

Channel Description
====================
1.Farmland - Send/Receive data regarding farmland asset issue, updated asset
balances and create exchange procedure
2.Warehouse - Send/Receive data regarding warehouse asset issue, updated
asset balances , create/decode exchange procedure and asset conversion
3.Retailstore - Send/Receive data regarding retailstore asset issue, updated
asset balances and decode exchange procedure

Request From UI to Blockchain Nodes
====================================
       1.IssueAsset
       =============
              1.Issue Farmland Asset
              2.Issue Warehouse Asset
              3.Issue Retailstore Asset
       2.Create Exchange
       ==================
              1.createExchange-farm-warehouse
              2.createExchange-warehouse-retailstore
       3.Decode-Exchange
       ==================
              1.Decode-Exchange-farm-warehouse
              2.Decode-Exchange-warehouse-retailstore
       4.Convert Asset
       ================
              1.Convert asset
       5.Get Updated Balances
       ======================
              1.Fetch Updates

Response From BlockChain nodes to UI
====================================
       1.Issue Asset
       ==============
              1.Issue Farmland Asset
              2.Issue Warehouse Asset
              3.Issue Reailstore Asset
       2.Create Exchange
       ==================
              1.createExchange-farm-warehouse
              2.createExchange-warehouse-retailstore
       3.Decode-Exchange
       ==================
              1.Decode-Exchange-farm-warehouse
              2.Decode-Exchange-warehouse-retailstore
       4.Convert Asset
       ================
              1.Convert asset
```

```
        5.Get Updated Balances
        ======================
                1.Fetch Updates

Response From BlockChain nodes to UI
====================================
        1.Issue Asset
        ==============
                1.Issue Farmland Asset
                2.Issue Warehouse Asset
                3.Issue Reailstore Asset
        2.Create Exchange
        ==================
                1.createExchange-farm-warehouse
                2.createExchange-warehouse-retailstore
        3.Decode-Exchange
        ==================
                1.Decode-Exchange-farm-warehouse
                2.Decode-Exchange-warehouse-retailstore
        4.Get Updated Balances
        ======================
                1.Fetch Farmland Updates
                2.Fetch Warehouse Updates
                3.Fetch retailstore Updates

Error message from blockchain node
==================================
1.Error Handling Type 1 (Top level error in Multichain class)
2.Error Handling Type 2 (Top level error in each node)
3.Error Handling Type 3 (API level error)
```

Όλα τα σχετικά αρχεία υπάρχουν και στο συνοδευτικό CD.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατ' αρχήν θα πρέπει να διαχωρίσουμε, σαν έννοιες, τα «κρυπτονομίσματα» από την τεχνολογία blockchain που χρησιμοποιούν. Η τεχνολογία Blockchain, μπορεί να είναι πολλαπλά χρήσιμη σε πολλούς τομείς της οικονομίας και σίγουρα έχει πολλά πλεονεκτήματα η χρήση της για ανάπτυξη εφαρμογών στον αγροδιατροφικό τομέα.

Το κίνητρο για την μετάβαση στην νέα τεχνολογία

Το κίνητρο που οδηγεί επιχειρήσεις του αγροδιατροφικού τομέα να επενδύσουν στην τεχνολογία blockchain, είναι η απαίτηση των σημερινών καταναλωτών, για αυξημένη ιχνηλασιμότητα, διαφάνεια και ασφάλεια, τόσο στις διαδικασία παραγωγής, όσο και αποθήκευσης και διανομής των αγροδιατροφικών προϊόντων. Στα τρόφιμα, οι σημερινοί καταναλωτές επιθυμούν να ξέρουν την προέλευση, τον τρόπο παραγωγής και την αειφορία ή το περιβαλλοντικό αποτύπωμα - με λίγα λόγια, θέλουν να γνωρίζουν την πλήρη ιστορία των προϊόντων διατροφής που επιλέγουν. Οι επιχειρήσεις του κλάδου, όλο και περισσότερο, θα απευθύνονται σε καταναλωτές που γνωρίζουν από θέματα τεχνολογίας και τους αρέσει να είναι πληροφορημένοι για ό,τι αγοράζουν, ιδιαίτερα για προϊόντα διατροφής.

Η τεχνολογία blockchain επιτρέπει, όπως είπαμε, να εξασφαλίσουμε την ιχνηλασιμότητα των αγροτικών προϊόντων, από το αγρόκτημα έως και τα ράφια των σούπερ μάρκετ, εξασφαλίζοντας έτσι την ασφάλεια και την διαφάνεια που ζητάει ο καταναλωτής. Επιπλέον, σε αυτή τη διαδικασία επαλήθευσης πληροφοριών μπορούν να παρέμβουν οργανισμοί πιστοποίησης (για παράδειγμα οι οργανισμοί που διαχειρίζονται την επικύρωση του σήματος του βιολογικού προϊόντος). Όλες οι πληροφορίες που καταχωρούνται σε αυτό το εργαλείο είναι κρυπτογραφημένες και επαληθεύσιμες.

Κίνδυνοι και ευκαιρίες της νέας τεχνολογίας

Το Blockchain είναι μια πολλά υποσχόμενη τεχνολογία. Υπάρχει πληθώρα εφαρμογών ή προβλημάτων που μπορούν να λυθούν χρησιμοποιώντας την τεχνολογία Blockchain. Οι περισσότερες από αυτές είναι ριζικές καινοτομίες και επομένως υπάρχουν κίνδυνοι και ευκαιρίες.

Αλλαγή συμπεριφοράς (Behavior change)

Η αλλαγή είναι σταθερή, αλλά σε κάθε αλλαγή υπάρχει αντίσταση. Οι χρήστες της νέας τεχνολογίας πρέπει να συνηθίσουν στο γεγονός ότι οι ηλεκτρονικές συναλλαγές είναι ασφαλείς. Οι σημερινοί μεσάζοντες (χρηματοπιστωτικά/τραπεζικά ιδρύματα) θα περάσουν επίσης από μια αλλαγή ρόλων και ευθυνών .

Θεωρούμε ότι οι εταιρείες θα επενδύσουν στο Blockchain, προκειμένου να διατηρήσουν την πελατεία τους.

Κλιμάκωση (Scaling)

Η κλιμάκωση των σημερινών υπηρεσιών που δημιουργούνται με βάση το Blockchain αποτελεί πρόκληση. Φανταστείτε κάποιον που εκτελεί μια συναλλαγή Blockchain για πρώτη φορά. Θα χρειαστεί να κατεβάσει ολόκληρο το Blockchain πριν εκτελέσει την πρώτη συναλλαγή. Αυτό μπορεί να διαρκέσει ώρες ή και περισσότερο, καθώς ο αριθμός των blocks αυξάνεται εκθετικά.

Θεωρούμε ότι όπως έγινε και με την εισαγωγή άλλων τεχνολογιών (interenet, web, smartphones), οι τελικοί χρήστες και ειδικά η νεότερη γενιά, θα υιοθετήσουν στην πλειοψηφία τους την νέα τεχνολογία.

Αρχική μετάπτωση στη νέα τεχνολογία (Bootstrapping)

Η μετακίνηση των υφιστάμενων συμβάσεων ή επιχειρηματικών εγγράφων στη νέα μεθοδολογία βασισμένη στο Blockchain απαιτεί «μεταβατικές ενέργειες» που πρέπει να εκτελεστούν. Για παράδειγμα, στην περίπτωση ιδιοκτησίας ακίνητης περιουσίας, τα υπάρχοντα έγγραφα που βρίσκονται σε εταιρείες ή δημόσιους οργανισμούς και μητρώα πρέπει να μεταφερθούν στην αντίστοιχη πλατφόρμα Blockchain. Αυτό σημαίνει χρόνο και κόστος.

Θεωρούμε ότι όπως έγινε και με την εισαγωγή άλλων τεχνολογιών (interenet, web, smartphones), οι εταιρείες και οι δημόσιοι φορείς/οργανισμοί, θα υιοθετήσουν σταδιακά την νέα τεχνολογία.

Κυβερνητικοί κανονισμοί (Government Regulations)

Στον νέο κόσμο των συναλλαγών που βασίζονται στο Blockchain, τα κράτη και οι διεθνείς οργανισμοί, πρέπει να υλοποιήσουν τις απαραίτητες αλλαγές και προσαρμογές στο θεσμικό τους πλαίσιο. Η εισαγωγή νέων νόμων και κανονισμών για την παρακολούθηση και τη ρύθμιση της νέας τεχνολογίας, μπορεί να βοηθήσει ή να επιβραδύνει την υιοθέτηση της νέας τεχνολογίας στην οικονομία και την κοινωνία.

Θεωρούμε ότι όπως έγινε και με την εισαγωγή άλλων τεχνολογιών (internet, web, smartphones), τα κράτη και οι διεθνείς οργανισμοί, θα υλοποιήσουν τις απαραίτητες αλλαγές και προσαρμογές στο θεσμικό πλαίσιο και θα υιοθετήσουν σταδιακά την νέα τεχνολογία.

(σ.σ Η Ευρώπη προσπαθεί να είναι μπροστά στις εξελίξεις, να δημιουργήσει σύγχρονες πλατφόρμες, οργανισμούς και καινοτόμους μηχανισμούς, για να καταστούν mainstream οι τεχνολογίες του blockchain, ώστε να είναι ανταγωνιστική απέναντι στις ΗΠΑ και την Ασία και κυρίως απέναντι στην Κίνα (που κατέχει το 72% της υπολογιστικής ισχύος - mining power- για το Bitcoin, αλλά και το 25% παγκοσμίως όλων των blockchain projects), σύμφωνα με στοιχεία σχετικής έρευνας, βλ. σχετικά [63]. Οι ΗΠΑ δίνουν μεγαλύτερη έμφαση στην Τεχνητή Νοημοσύνη, ενώ δεν φαίνεται να θέλουν να επενδύσουν όσα η Ευρώπη ή η Κίνα στο blockchain. Στο πλαίσιο της κοινοτικής αυτής προσπάθειας, το 2009, ξεκίνησε η λειτουργία τού Διεθνούς Συνδέσμου Αξιόπιστων Εφαρμογών Blockchain (International Association for Trusted Blockchain Applications, IATBA), στην οποία μετέχουν εταιρείες (όχι μόνο ευρωπαϊκές) όπως οι Deutsche Telecom, Telefonika, Fujitsu, IBM, SAP και L'oreal. Επίσης, υπάρχει από το 2018 ο μηχανισμός European Blockchain Partnership (EBP), στον οποίο μετέχουν συνολικά 26 κράτη-μέλη της ΕΕ (μεταξύ των οποίων και η Ελλάδα) και η Νορβηγία και το Λίχτενσταϊν. Οι χώρες που υπέγραψαν τη διακήρυξη για τη δημιουργία του EBP έχουν ως στόχο να τεθεί σε λειτουργία η Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain (EBSI), μια πλατφόρμα, που αναμένεται να λειτουργήσει σε κάποια τμήματά της μέχρι το τέλος του 2019, με προοπτική να ολοκληρωθεί και να τεθεί σε πλήρη λειτουργία το 2020).

Κακόβουλες Δραστηριότητες/Απάτη (Fraudulent Activities)

Δεδομένου του χαρακτήρα των συναλλαγών Blockchain, σε συνδυασμό με την ευκολία που προσφέρουν, κάποιοι μπορούν να καταχραστούν την τεχνολογία για κακόβουλες δραστηριότητες όπως η διακίνηση χρημάτων. Όμως το ίδιο συμβαίνει με κάθε νέα τεχνολογία. Η χρήση της εξαρτάται από τον άνθρωπο.

Θεωρούμε ότι με επαρκείς νόμους, κανονισμούς και υποστήριξη τεχνολογίας, οι υπηρεσίες επιβολής του νόμου θα είναι σε θέση να ελέγξουν, να αποτρέψουν ή να διώκουν αυτά τα άτομα.

Τεχνολογικές εξελίξεις (Technological advances)

Η βάση της τεχνολογίας Blockchain στηρίζεται στο ίδιο το γεγονός ότι είναι μαθηματικά αδύνατο για ένα μόνο χρήστη, να «ξεγελάσει» το σύστημα λόγω έλλειψης της απαιτούμενης υπολογιστικής ισχύος. Αλλά με τη μελλοντική εμφάνιση των κβαντικών υπολογιστών (Quantum Computers), τα κρυπτογραφικά κλειδιά μπορεί να είναι αρκετά εύκολα για να σπάσουν εντός εύλογου χρονικού διαστήματος (με χρήση αλγορίθμων brute-force). Ήδη η Google ανακοίνωσε επίσημα ότι πέτυχε την αποκαλούμενη «κβαντική υπεροχή» (quantum supremacy).

Θεωρούμε ότι η λύση θα ήταν τα κλειδιά να γίνουν ακόμη πιο δυνατά ώστε να μην είναι εύκολο να σπάσουν.

Συμπεράσματα και προτάσεις για την περίπτωση της Ελλάδας

Τόσο ο πρωτογενής, όσο και τομέας μεταποίησης και παρεχόμενων υπηρεσιών αλλάζει ραγδαία παγκοσμίως, ωθούμενος από παράγοντες, όπως η εισαγωγή καινοτόμων τεχνολογικών λύσεων. Σε αυτό το ρευστό τοπίο, ωστόσο, η χώρα μας παραμένει στάσιμη και απροετοίμαστη.

Η ανάπτυξη νέων, αποτελεσματικών συνεργατικών σχημάτων και η χρήση καινοτόμων τεχνολογιών, είναι προϋπόθεση για να μπορέσει η Ελλάδα να παρακολουθήσει τις εξελίξεις και για να διεκδικήσει μια καλύτερη θέση στην παγκόσμια αγροδιατροφική αγορά. Η τεχνολογία blockchain μπορεί να παίξει καταλυτικό ρόλο και στα δύο.

Θα πρέπει, μέσα στα επόμενα χρόνια το σύνολο των εμπλεκόμενων φορέων, τόσο σε επιχειρηματικό όσο και πολιτικό και κανονιστικό επίπεδο, να συνεργαστούν για να διαμορφώσουν το απαραίτητο θεσμικό, νομικό και οικονομικό πλαίσιο, ώστε να απελευθερώσουν και να εκμεταλευτούν το συνολικό δυναμικό αυτής της τεχνολογίας.

Η χρήση της καινοτόμου αυτής τεχνολογίας θα μπορούσε να οδηγήσει σε περαιτέρω ανάπτυξη του αγροδιατροφικού κλάδου και σε δημιουργία νέων θέσεων εργασίας, τόσο στην έρευνα και ανάπτυξη εφαρμογών της, όσο και από την εφαρμογή της στην παραγωγική διαδικασία.

Οι νέες δυνατότητες της τεχνολογίας blockchain στις οικονομικές συναλλαγές (ταυτοποίηση του καταναλωτή, έγκριση πληρωμής, ευκολία συναλλαγής, ασφάλεια, πρόσβαση στο ιστορικό των συναλλαγών), μπορούν να οδηγήσουν σε σημαντική μείωση του κόστους των συναλλαγών, αφού δεν θα απαιτείται πλέον η ύπαρξη των ενδιάμεσων που υφίστανται σήμερα.

Χρειάζεται ψηφιακός εγγραμματισμός όχι μόνο των καταναλωτών αλλά και των λοιπών εμπλεκόμενων φορέων (τράπεζες, κανονιστικοί και ρυθμιστικοί οργανισμοί).

Είναι απαραίτητο να υπάρχει ενημέρωση σχετικά με την ασφάλεια και τη διαφάνεια στα τρόφιμα, έτσι ώστε η κοινωνία να κατανοήσει σε τι συμβάλλει η τεχνολογία blockchain στον κλάδο.

Η αγορά οδηγείται από τον ανταγωνισμό των τιμών και τα κίνητρα του πωλητή πηγαίνουν προς χαμηλής ποιότητας προϊόντα. Η προσθήκη ολόκληρης αυτής της τεχνολογίας στη διαδικασία δεν είναι δωρεάν και πιθανά να οδηγήσει σε αύξηση τιμών των αγροδιατροφικών προϊόντων. Η αύξηση των τιμών, μπορεί να είναι ένα πρόβλημα για την υιοθέτηση της νέας τεχνολογίας αλλά αν η τεχνολογία εισαχθεί σταδιακά, η αγορά θα προσαρμοστεί ομαλά. Με την πρόσβαση σε πληροφορίες σχετικά με την ασφάλεια, την ποιότητα και την προέλευση από τον καταναλωτή, η ασυμμετρία της πληροφορίας θα μειωθεί υπέρ των προϊόντων καλής ποιότητας σε προσιτές τιμές. Ενώ οι τιμές ενδέχεται να μειωθούν στο μέλλον, το κόστος εφαρμογής της τεχνολογίας

αποτελεί επί του παρόντος απαγορευτικό παράγοντα, ιδίως στην περίπτωση της Ελλάδας.

Η πολυπλοκότητα του εγχειρήματος και οι προσαρμογές που πρέπει να γίνουν σε θεσμικό και νομικό επίπεδο, είναι ανασταλτικός παράγοντας για την μετάβαση στην νέα τεχνολογία blockchain.

Μια σταδιακή υιοθέτηση της τεχνολογίας blockchain (ξεκινώντας από single-use εφαρμογές και χρήση open source platforms) θα ήταν ένα καλό πρώτο βήμα για κάθε επιχείρηση σήμερα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Κ. Στεφάνου, «Δημιουργία Εφαρμογής Blockchain Ethereum και Κρυπτονομίσματος», *Μεταπτυχιακή Διατριβή*, Πανεπιστήμιο Πειραιώς, 2018. Available: http://dione.lib.unipi.gr/xmlui/handle/unipi/11083 . [Accessed Dec 12, 2019].

[2] "Global Glossary of Blockchain Terms". Available: https://blockchaintrainingalliance.com/pages/glossary-of-blockchain-terms . [Accessed Dec 12, 2019].

[3]. "Guide to blockchain", Investopedia. Available: https://www.investopedia.com/blockchain-4689765 . [Accessed Dec 12, 2019].

[4] «Τι είναι η τεχνολογία Blockchain: Ένας πλήρης οδηγός για αρχάριους». Available: https://www.dreamweaver.gr/blockchain.php . [Accessed Dec 12, 2019].

[5] Tapscott, D. & Tapscott, A. (2016). «Blockchain Revolution». Great Britain: Clays Ltd, St Ives plc.

[6] "Blockchain". Available: https://el.wikipedia.org/wiki/Blockchain . [Accessed Dec 12, 2019].

[7] "Blockchain revolution in mutual fund trades", *The Times*. 2018-12-03. Available: https://www.thetimes.co.uk/article/blockchain-revolution-in-mutual-fund-trades-jcldstwt6 . [Accessed Dec 12, 2019].

[8] Laurence, T. (2017). "Blockchain". Canada: John Wiley & Sons, Inc.

[9] Gupta, M. (2017). "Blockchain IBM Limited Edition". United States of America: John Wiley & Sons, Inc.

[10] Antonopoulos, A.M. (2017). "Mastering Bitcoin (2nd Edition)". United States of America: O,Reilly Media Inc.

[11] "How blockchain architecture works?" *Basic Understanding of Blockchain and its Architecture*. Available: https://www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture . [Accessed Dec 12, 2019].

[12] Vincenzo Morabito (2017). "Business Innovation Through Blockchain". Cham, Switzerland Springer International Publishing AG.

[13] Σταμπέρνας, Σ., «Τεχνολογίες αλυσίδας συστοιχιών και έξυπνα συμβόλαια στο πλαίσιο του Διαδικτύου των Πραγμάτων», *Μεταπτυχιακή Διατριβή*, Πανεπιστήμιο Πειραιώς, 2018. Available: http://dione.lib.unipi.gr/xmlui/handle/unipi/11201 . [Accessed Dec 12, 2019].

[14] Buchman, E (2016). Tendermint: "Byzantine fault tolerance in the age of blockchains". University of Guelph (Master Thesis).

[15] Mayank Pratap,"Blockchain Technology Explained: Introduction, Meaning, and Applications Replenish your fears against Blockchain", Jul 2018 .

[16] Curtis Miles, "Blockchain security: What keeps your transaction data safe" . 2017. Available: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe . [Accessed Dec 12, 2019].

[17] «Τεχνολογία Αλυσίδας Κοινοποιήσεων και Εφαρμογές». Πανεπιστήμιο Πειραιώς. Available: https://mscdss.ds.unipi.gr/metaptixiako/proigmena-pliroforiaka-sistimata/texnologia-alisidas-koinopoihsewn-efarmoges/ . [Accessed Dec 12, 2019].

[18] «Πώς μπορεί η νέα τεχνολογία να μεταμορφώσει τις χρηματοπιστωτικές αγορές;» ΕΚΤ. Available: https://www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.el.html . [Accessed Dec 12, 2019].

[19] «Πώς η τεχνολογία στηρίζει το παγκόσμιο εμπόριο», naftemporiki.gr. Available: https://www.naftemporiki.gr/finance/story/1398466/poe-pos-i-texnologia-stirizei-to-pagkosmio-emporio . [Accessed Dec 12, 2019].

[20] "Blockchain Enhances Privacy, Security and Conveyance of Data", SCIENTIFIC AMERICAN.,2016. Available: https://www.scientificamerican.com/article/blockchain-enhances-privacy-security-and-conveyance-of-data . [Accessed Dec 12, 2019].

[21] "Decentralized autonomous organization". Available:https://www.sec.gov/news/press-release/2017-131 .[Accessed Dec 12, 2019].

[22] "Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015". Available:. http://www.gartner.com/newsroom/id/3165317 . [Accessed Dec 12, 2019].

[23] "Is Blockchain The Answer To Election Tampering?", *Forbes,* 2018. Available:https://www.forbes.com/sites/forbestechcouncil/2018/11/02/is-blockchain-the-answer-to-election-tampering . [Accessed Dec 12, 2019].

[24] "A secure online voting system using blockchain", BusinessTech.,2018. Available:https://businesstech.co.za/news/it-services/237547/a-secure-online-voting-system-using-blockchain . [Accessed Dec 12, 2019].

[25] «Blockchain: Η τεχνολογία που αλλάζει για πάντα οικονομία και διαδίκτυο»,. insider.gr, 2018. Available: https://www.insider.gr/epiheiriseis/tehnologia/69555/blockchain-i-tehnologia-poy-allazei-gia-panta-oikonomia-kai-diadiktyo . [Accessed Dec 12, 2019].

[26] "Cryptography & Blockchain". Available: https://blockchainhub.net/blog/blog/cryptography-blockchain-part-1 . [Accessed Dec 12, 2019].

[27] Μαρκουλής, Δ., «ΝΟΜΙΚΟ & ΤΕΧΝΟΛΟΓΙΚΟ ΚΑΘΕΣΤΩΣ ΨΗΦΙΑΚΩΝ ΝΟΜΙΣΜΑΤΩΝ», Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς, 2019. Available:http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12043/Markoulis_1711.pdf.pdf?sequence=1&isAllowed=y . [Accessed Dec 12, 2019].

[28] Λαγαράς, Κ., «Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της».Available: https://www.lawspot.gr/nomika-nea/h-tehnologia-blockchain-oi-efarmoges-kai-oi-nomikes-ptyhes-tis [Accessed Dec 12, 2019].

[29] "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities". Available: https://www.sec.gov/news/press-release/2017-131 . [Accessed Dec 12, 2019].

[30] ΔικΕΕ, υπόθεση C-264/14, σκέψη 24

[31] ΔικΕΕ, υπόθεση C-264/14, σκέψη 49

[32] "Virtual currency schemes – a further analysis". EKT. Available:https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf . [Accessed Dec 12, 2019].

[32] GEO. L. TECH. REV. 305, 2017. Available: https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf . [Accessed Dec 12, 2019].

[33] "BLP wins in disputed UK predictive coding case David Brown v BCA". Available:https://www.legaltechnology.com/latest-news/blp-wins-in-disputed-uk-predictive-coding-case-david-brown-v-bca . [Accessed Dec 12, 2019].

[34] International Telecommunication Union, «Measuring the Information Society Report»,International Telecommunication Union (ITU), Report, 2015. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-E.pdf . [Accessed Dec 12, 2019].

[35] Iansiti, Marco, and Karim R. Lakhani. "The Truth about Blockchain". Harvard Business Review 95, no. 1 (January–February 2017): 118–127. Available: https://hbr.org/2017/01/the-truth-about-blockchain . [Accessed Dec 12, 2019].

[36] "Blockchain Technology: preparing for change". Accenture 2015. Available:

https://www.accenture.com/t20160608T052656Z__w__/us-en/_acnmedia/PDF-5/Accenture-2016-Top-10-Challenges-04-Blockchain-Technology.pdfla=en . [Accessed Dec 12, 2019].

[37] Bozarth, Cecil C., Handfield, Robert B., (2006). "Introduction to Operations and Supply Chain Management", New Jersey, USA: Pearson Education.

[38] Fredrik Jansson and Oskar Petersen (2017). "Blockchain Technology in Supply Chain Traceability Systems.Developing a Framework for Evaluating the Applicability". *Industrial Engineering and Management, Lund University (Master Thesis)* Available:. http://lup.lub.lu.se/student-papers/record/8918347/file/8919918.pdf . [Accessed Dec 12, 2019].

[39] Aung, M. M., Chang, Y. S., 2014. "Traceability in a food supply chain: Safety and quality perspectives". Food Control, Vol. 39, pp. 172-184.

[40] Moe, T. 1998. "Perspectives on traceability in food manufacture". Trends in Food Science & Technology, Vol. 9, No. 1, pp. 211-214.

[41] GS1, 2012. "GS1 Standard Document: GS1 Global Traceability Standard". http://www.gs1.org/sites/default/files/docs/traceability/Global_Traceability_Standard.pdf . [Accessed Dec 12, 2019].

[42] European Commission, 2002, chapter 1, article 3, no. 15. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1488202332570&uri=CELEX:32002R0178 . [Accessed Dec 12, 2019].

[43] Kalogianni, E. P., Tektonidis, D., Salampasis, M., (2012). "TraceALL: a semantic web framework for food traceability systems". *Journal of Systems and Information Technology*, Vol. 14 Iss. 4, pp. 302-317.

[44] Bechini, A., Cimino, M., Marcelloni, F., Tomasi, A., (2008). "Patterns and technologies for enabling supply chain traceability through collaborative e-business. Information and Software Technology", Vol. 50, Iss. 5, pp. 342-359.

[45] Golan, E., Krissoff, B., Kuchler, F., Calvin, L., Nelson, K., Price, G., 2004. "Traceability in the US food supply: economic theory and industry studies". *Agricultural Economic Report*, Iss. 830, No. 3, pp. 1-56.

[46] Kumari, L.; Narsaiah, K.; Grewal, M.K.; Anurag, R.K. "Application of rfid in agri-food sector".Trends Food Sci. Technol. 2015, 43, 144–161..

[47] Olsen, P., Borit, M., 2013. How to define traceability. Trends in Food Science & Technology, Vol. 23, pp. 142-150.

[48] GS1, 2017b. How GDSN Works. Available: http://www.gs1.org/how-gdsn-works . [Accessed Dec 12, 2019].

[49] GS1, 2017c. "EPCIS and Core Business Vocabulary". Available: http://www.gs1.org/epcis . [Accessed Dec 12, 2019].

[50] Marucheck, A., Greis, N., Mena, C., Cai, L., (2011). "Product safety and security in the global supply chain: Issues, challenges and research opportunities". *Journal of Operations Management,* Vol. 29, Iss. 7-8, pp. 707-720.

[51] Trienekens, J. H., P. M. Wognum, A. J. M. Beulens and J. G. A. J. van der Vorst (2012). "Transparency in complex dynamic food supply chain"s. *Advanced Engineering Informatics* 26(1): 55-65.

[52] Dianhui Mao, Zhihao Hao,Fan Wang and Haisheng Li (2018). "Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province", China. Ανακτήθηκε από https://www.mdpi.com . [Accessed Dec 12, 2019].

[53] Minarelli, F.; Galioto, F.; Raggi, M.; Viaggi, D. "Asymmetric Information along the Food Supply Chain: A Review of the Literature", 2016. Available: http://www.sufisa.eu/userfiles/update%2011122016/minarelli%20et%20al%20(2016).pdf . [Accessed Dec 12, 2019].

[54] "COMMISSION STAFF WORKING DOCUMENT STAKEHOLDER CONSULTATION - SYNOPSIS REPORT" , Accompanying the Document Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on Unfair Trading Practices in Business-to-Business Relationships in the Food Supply Chain. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:091:FIN . [Accessed Dec 12, 2019].

[55] Alicia Noel , "Six Ways Blockchain is Being Used in Food and Agriculture Supply Chains", 2018. Available: https://medium.com/cultivati/six-ways-blockchain-is-being-used-in-food-and-agriculture-supply-chains-68a7305fd533 . [Accessed Dec 12, 2019].

[56] Σαρτζετάκη, Κ. (2013). «Logistics και Εφοδιαστική Αλυσίδα σε μια επιχείρηση», *Πτυχιακή Εργασία*, ΤΕΙ Κρήτης, 2013. Available: http://nefeli.lib.teicrete.gr/browse/sdo/log/2013/SartzetakiKalliopi/attached-document-1381859641-980321-4729/SartzetakiKalliopi2013.pdf . [Accessed Dec 12, 2019].

[57] Michael, Crosby (Google), Nachiappan (Yahoo), Pradan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor), 2016. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review. Issue No2 June 2016.

[58] ΚΟΥΛΙΟΥΔΗ, Ε., «ΜΕΛΕΤΗ ΤΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ ΤΩΝ ΚΑΤΑΝΑΛΩΤΩΝ ΩΣ ΠΡΟΣ ΤΟ ΕΛΑΙΟΛΑΔΟ», *Πτυχιακή Εργασία*, ΑΠΘ, 2016. Available: http://ikee.lib.auth.gr/record/287549/files/GRI-2017-18434.pdf . [Accessed Dec 12, 2019].

[59] «OliveTrace: Ιχνηλασιμότητα ελαιολάδου». Available: https://www.olivenews.gr/el/9888/episthmh/poiotita/olivetrace-ixnhlasimothta-elaioladou/ . [Accessed Dec 12, 2019].

[60] «Η τεχνολογία Blockchain προσθέτει διαφάνεια στη βιομηχανία ελαιολάδου της Ισπανίας». Available: https://www.oliveoiltimes.com/el/business/blockchain-technology-adds-transparency-to-spains-olive-oil-industry/66559 . [Accessed Dec 12, 2019].

[61] "Devoleum". Available: https://www.devoleum.com [Accessed Dec 12, 2019].

[62] "Certified Origins Italia Transforms Supply Chain with Oracle Blockchain". Available: https://www.oracle.com/it/customers/certified-origins-1-blockchain-story.html . [Accessed Dec 12, 2019].

[63] «Έρευνα: Είναι το blockchain τόσο επαναστατικό;» . Available: https://www.euractiv.gr/section/oikonomia/news/ereyna-einai-to-blockchain-toso-epanastatiko .[Accessed Dec 12, 2019].

[64] "Compare eight Blockchain platforms to kick start your next project". Available: http://radiostud.io/eight-blockchain-platforms-comparison . [Accessed Dec 12, 2019].

[65] Rivera, J., "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor." Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. N.p., 18 Aug. 2015. Web. 03 May 2016.

[66] «Terra: Εφοδιαστική Αλυσίδα». Available: https://www.terra.gr/el/home/ . [Accessed Dec 12, 2019].

[67] "Agriculture and Agri-Food Canada". Available: http://allaboutfood.aitc.ca/article/faqs-about-agri-food.php . [Accessed Dec 12, 2019].

[68] "Multichain:Getting Started". Available: https://www.multichain.com/getting-started/ . [Accessed Dec 12, 2019].

[69] "A Step-by-Step Guide to Building and Deploying MultiChain Private Blockchains". Available:

https://medium.com/coinmonks/a-step-by-step-guide-to-building-and-deploying-multichain-private-blockchains-d3b27b5cf2b2 . [Accessed Dec 12, 2019].

[70] "Get Started With MultiChain on Windows PC". Available:

https://dzone.com/articles/how-to-get-started-with-multichain-blockchain-on-w . [Accessed Dec 12, 2019].

[71] "How Blockchain Can Revolutionize Agricultural Supply Chain". Available:

https://radiostud.io/blockchain-can-revolutionize-agricultural-supply-chain-part-2/ . [Accessed Dec 12, 2019].

[72] AravindNico, "Blockchain. Agri_usecase", GitHub. Available:

https://github.com/AravindNico/blockchain_agri_usecase . [Accessed Dec 12, 2019].

[73] Τριαντόπουλος Χρ. και Φιλίνης Κ., «Σημειώσεις για το Εισαγωγικό Σεμινάριο στην Οικονομική Θεωρία», Πανεπιστήμιο Θεσσαλίας, Δεκ 2019.

[74] «Χάρτης Εξόδου Από Την Κρίση: Ένα Νέο Παραγωγικό Μοντέλο Για Την Ελλάδα (2016)», ΔΙΑΝΕΟΣΙΣ. Available: https://www.dianeosis.org/product/xartis-eksodou-apo-tin-krisi/. [Accessed Dec 12, 2019].

[75] «Τα δεδομένα για το ΑΕΠ στην χώρα μας», 2017.Available: https://www.xrysoselladas.gr/blog/2017/10/xrysoselladas-tiparagoume. [Accessed Dec 12, 2019].

[76] Alessandro Chiesa, "Blockchain Fundamentals DeCal", 2018.Available: https://www2.eecs.berkeley.edu/Scheduling/CS/schedule.html. [Accessed Dec 12, 2019].

[77] Lamport, L. (1978). "Time, clocks, and the ordering of events in a distributed system" (PDF). Communications of the ACM . 21 (7): 558–565. CiteSeerX 10.1.1.142.3682. doi:10.1145/359545.359563.

[78] «Alpha Bank: Η αύξηση του ΑΕΠ της Ελλάδας», 2018.Available: https://www.bankingnews.gr/index.php?id=396584 [Accessed Dec 12, 2019].

[79] Γκέκας, Γ., «Τα χαρακτηριστικά του αγροτικού τομέα σήμερα», 2017.epixeiro.gr. Available: https://www.epixeiro.gr/article/2564 [Accessed Dec 12, 2019].