Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΜΕΛΕΤΗ ΤΕΧΝΟΛΟΓΙΚΗΣ ΑΡΙΣΤΕΙΑΣ

Δράση «Συνέργειες Έρευνας και Καινοτομίας στην Περιφέρεια Αττικής»

(ΕΣΠΑ 2014-2020)

ΤΙΤΛΟΣ ΕΡΓΟΥ

«Ιχνηλασιμότητα, Συλλογή, Ανάκτηση, και Ενεργειακή Αξιοποίηση Γεωργικών Πλαστικών Αποβλήτων με τη Συνδυασμένη Χρήση της τεχνολογίας αλυσίδας κοινοποιήσεων (Blockchain) και έξυπνης εφαρμογής ασύρματης/κινητής συσκευής»

ΑΚΡΩΝΥΜΙΟ: BLOCK AGROWASTE

ΚΩΔΙΚΟΣ ΕΡΓΟΥ ΣΤΟ ΠΣΚΕ: ΑΤΤΡ4-0325411

ΑΘΗΝΑ 2024

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΤΤΙΚΗ 2014-2020

ΔΡΑΣΗ ΣΥΝΕΡΓΕΙΕΣ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ

ΕΡΓΟ: Ιχνηλασιμότητα, Συλλογή, Ανάκτηση, και Ενεργειακή Αξιοποίηση Γεωργικών Πλαστικών Αποβλήτων με τη Συνδυασμένη Χρήση της Τεχνολογίας Αλυσίδας Κοινοποιήσεων (Blockchain) και Έξυπνης Εφαρμογής Ασύρματης/ Κινητής συσκευής

ΚΩΔΙΚΟΣ ΕΡΓΟΥ: ΑΤΤΡ4-0325411

ΠΑΡΑΔΟΤΕΟ Π2: Μελέτη Τεχνολογικής Αριστείας

Διάρκεια Έργου:	**24 μήνες**
Ημερομηνία Παράδοσης:	**30/06/2024**
Υπεύθυνος Παραδοτέου:	**ΕΜΠ**
Επίπεδο Διάχυσης:	**Δημόσιο**
Τρέχουσα Κατάσταση Παραδοτέου:	**Τελικό**
Έκδοση:	**F**
Ιστοσελίδα Έργου:	www.blockagrowaste.gr

ΦΟΡΕΙΣ ΥΛΟΠΟΙΗΣΗΣ:

ΑΘΗΝΑ 2024

The present work is co-funded by the European Union and Greek national funds through the Operational Program Attica 2014-2020, under the call "RESEARCH AND INNOVATION COOPERATION ACTION IN THE ATTICA REGION" (project code: ATTP4-0325411 and Acronym: BLOCK AGROWASTE).

Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση και από εθνικούς πόρους μέσω του Επιχειρησιακού Προγράμματος Αττική 2014-2020 της Δράσης «ΣΥΝΕΡΓΕΙΕΣ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ» (Κωδικός Έργου: ΑΤΤΠ4-0325411 και ακρωνύμιο: BLOCK AGROWASTE).

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

1. Σύνοψη προς τη Διαχειριστική Αρχή (Executive Summary)

Ο βασικός σκοπός του παρόντος παραδοτέου είναι η ενδελεχής μελέτη της τεχνολογικής αριστείας που θα μπορούσε να εφαρμοστεί στο έργο **BLOCK AGROWASTE**. Πιο συγκεκριμένα, πραγματοποιείται έρευνα των πιο αξιοσημείωτων τεχνολογιών που κυριαρχούν τα τελευταία χρόνια, όπως το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT), καινοτόμοι αισθητήρες (sensors), οι οποίοι δύνανται να αξιοποιηθούν στη διαχείριση αγροπλαστικών, η υπολογιστική νέφους (cloud computing), καθώς και η τεχνολογία Blockchain που τα τελευταία χρόνια βρίσκεται στο επίκεντρο πολυάριθμων κλάδων. Ακόμα, καταγράφονται οι τομείς που εφαρμόζονται ήδη οι προαναφερθείσες τεχνολογίες και κυρίως, η συμβολή τους στον κλάδο της γεωργίας. Επομένως, ο απώτερος στόχος του παραδοτέου δεν είναι άλλος από την ανάπτυξη και μελέτη του απαραίτητου γνωσιακού υποβάθρου που σχετίζεται με τεχνολογικά ζητήματα με σκοπό την ενίσχυση των εργασιών των ακόλουθων παραδοτέων και ειδικότερα, αυτών που αφορούν την επιλογή του τεχνολογικού κράματος που θα συμβάλλει στην ανάπτυξη μίας πλατφόρμας, μέσω της οποίας θα εξασφαλίζεται απρόσκοπτη επικοινωνία μεταξύ των συμβαλλόμενων μελών που ειδικεύονται στο γεωργικό χώρο (αγρότες, υπάλληλοι θερμοκηπίων, γεωπόνοι, κλπ.) και των συλλεκτών αγροπλαστικών απορριμμάτων.

Έτσι, η δομή του παραδοτέου έχει ως εξής: Στο ***Κεφάλαιο 2***, παρουσιάζονται τα δομικά στοιχεία των συστημάτων του Διαδικτύου των Πραγμάτων και των βασικών πεδίων εφαρμογής τους, με έμφαση στην "έξυπνη" γεωργία. Έπειτα, στο ***Κεφάλαιο 3***, αναφέρονται τα πιο σημαντικά είδη αισθητήρων, καθώς και τα βασικά οφέλη που προσφέρουν. Στο ***Κεφάλαιο 4***, περιγράφονται ενδελεχώς τα δίκτυα Blockchain, καθώς και ο τρόπος λειτουργίας τους, οι μηχανισμοί συναίνεσης, ενώ μελετάται και η λειτουργία των κρυπτονομισμάτων, με απώτερο σκοπό την ανάπτυξη του ιδανικότερου token, που θα ικανοποιεί τις προδιαγραφές του έργου. Τέλος, στο ***Κεφάλαιο 5***, πραγματοποιείται μία περίληψη των πιο σημαντικών συμπερασμάτων, που θα μπορούσαν να φανούν χρήσιμα στο έργο **BLOCK AGROWASTE** και να αξιοποιηθούν σε μεταγενέστερο χρόνο, στοχεύοντας στον εντοπισμό και στην αξιολόγηση καλών πρακτικών.

2. Τεχνολογίες του Διαδικτύου των Πραγμάτων (Internet of Things – IoT)

Τα τελευταία χρόνια η τεχνολογία εξελίσσεται με εκθετικό ρυθμό, καθώς προσφέρει πολυάριθμα πλεονεκτήματα και αναβαθμίζει διαρκώς την ποιότητα της ανθρώπινης ζωής. Πλέον ένα ευρύ πλήθος εφαρμογών συναντάται στην καθημερινότητα μας, το οποίο αξιοποιεί καινοτόμες τεχνολογίες, όπως ενσωματωμένους αισθητήρες, αναπτύσσοντας έτσι, ένα ενιαίο περιβάλλον και ενισχύοντας την αλληλοεπίδραση μεταξύ των συμμετεχόντων, οι οποίοι δύνανται να ανταλλάσσουν συνεχώς πληροφορίες μεταξύ τους ή να χρησιμοποιούν κάποια υπηρεσία προστιθέμενης αξίας.

Εξέλιξη του παραπάνω οικοσυστήματος αποτελεί το Διαδίκτυο των Πραγμάτων - ΔτΠ (Internet of Things - IoT), το οποίο αναφέρεται στο δίκτυο των διασυνδεδεμένων φυσικών συσκευών ή «πραγμάτων» που είναι ενσωματωμένα με αισθητήρες, λογισμικό, ακόμα και με άλλες τεχνολογίες που τους επιτρέπουν να συλλέγουν και να ανταλλάσσουν δεδομένα μέσω του Διαδικτύου. Η πρώτη φορά που χρησιμοποιήθηκε ο συγκεκριμένος όρος ήταν από τον Kevin Ashton, ο οποίος ήταν διευθυντής του Auto-ID center στο MIT εστιάζοντας στις τεχνολογίες ραδιοσυχνικής αναγνώρισης (Radio Frequency Identification – RFID) (Ashton, 2009). Το Διαδίκτυο των Πραγμάτων δημιουργεί ένα δίκτυο «έξυπνων» συσκευών που μπορεί να ανταποκρίνεται στον περίγυρο του, οδηγώντας σε αυξημένη αποτελεσματικότητα, καθώς και στη βελτιωμένη λήψη αποφάσεων.

Το ΔτΠ επιτρέπει στα αντικείμενα να εντοπίζονται και να ελέγχονται εξ αποστάσεως σε μια υπάρχουσα υποδομή δικτύου (Islam et al., 2015), δημιουργώντας ευκαιρίες για την πιο άμεση ενσωμάτωση του φυσικού κόσμου σε συστήματα που βασίζονται σε ηλεκτρονικούς υπολογιστές οδηγώντας σε βελτιωμένη αποτελεσματικότητα, ακρίβεια και οικονομικό όφελος. Μάλιστα, όταν το ΔτΠ συμπληρώνεται με αισθητήρες (sensors) και ενεργοποιητές (actuators), κάθε αντικείμενο γίνεται μοναδικά αναγνωρίσιμο και είναι σε θέση να λειτουργεί και να αλληλοεπιδρά μέσα στην υπάρχουσα υποδομή του Διαδικτύου (Gapchup et al., 2016).

Ωστόσο, η πρώτη εφαρμογή του Διαδικτύου των Πραγμάτων αποδίδεται συχνά στον αυτόματο πωλητή της Coca-Cola στο Πανεπιστήμιο Carnegie Mellon στις αρχές της δεκαετίας του 1980. Αυτό το μηχάνημα αυτόματης πώλησης τροποποιήθηκε για να μπορεί να αναφέρει στους φοιτητές και εργαζομένους του Πανεπιστημίου το απόθεμα και τη θερμοκρασία των αναψυκτικών μέσω του Διαδικτύου, αποφεύγοντας συνεπώς, περιττές μετακινήσεις (Maxey, 2016). Αυτό το πρώιμο παράδειγμα παρουσίασε τη δυνατότητα σύνδεσης καθημερινών αντικειμένων στο διαδίκτυο για τη συλλογή δεδομένων και τη βελτίωση της λειτουργικής αποτελεσματικότητας. Έθεσε τις βάσεις για μελλοντικές εφαρμογές IoT που έκτοτε έχουν μεταμορφώσει και εξελίξει ραγδαία διάφορους κλάδους και πτυχές της καθημερινής ζωής.

Σχήμα 2-1: Η πρώτη εφαρμογή του IoT στο Πανεπιστήμιο Carnegie Mellon (Maxey, 2016)

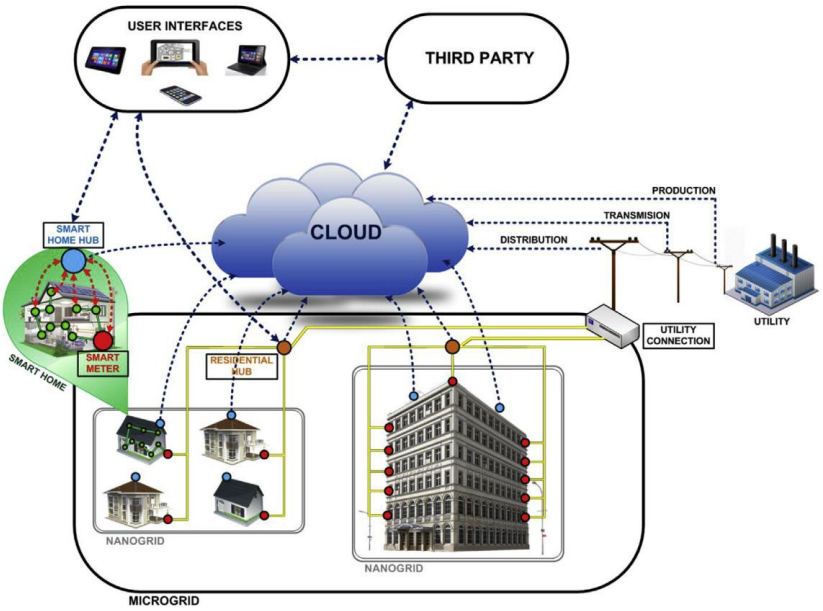
2.1. Πεδίο Ανάπτυξης εφαρμογών IoT

Λόγω της ραγδαίας ανάπτυξης των τεχνολογιών IoT, όπως ήδη έχει αναφερθεί, ένας αυξανόμενος αριθμός πρακτικών εφαρμογών μπορεί να βρεθεί σε πολλούς τομείς, όπως η ασφάλεια, η παρακολούθηση παγίων, η γεωργία, οι "έξυπνες" μετρήσεις, οι "έξυπνες" πόλεις και τα "έξυπνα" σπίτια (Ratasuk et al., 2015). Είναι αλήθεια πως πλέον ο όρος "smart" χρησιμοποιείται σαν ομπρέλα κάτω από την οποία βρίσκουν καταφύγιο όλες οι καινοτόμες τεχνολογίες που επιτυγχάνουν ένα μικρό ή και μεγαλύτερο βαθμό τεχνητής νοημοσύνης (Marikyan, 2019). Τα βασικά χαρακτηριστικά των "έξυπνων" τεχνολογιών είναι η ικανότητα κτήσης δεδομένων από το περιβάλλον και η αυτοματοποιημένη, "έξυπνη" αντίδραση με βάση τα δεδομένα αυτά. Στο ***Σχήμα 2.2*** παρουσιάζεται μια εικόνα του εύρους των εφαρμογών της τεχνολογίας IoT, οι οποίες και περιγράφονται εν συντομία στις ενότητες που ακολουθούν.

Σχήμα 2-2: Σύγχρονα Πεδία Εφαρμογής της Τεχνολογίας IoT (Raza et al., 2017)

2.1.1. "Έξυπνο" Σπίτι

Ο όρος "έξυπνο" σπίτι αναφέρεται στην κατοικία, η οποία χρησιμοποιεί ολοκληρωμένα συστήματα επικοινωνίας, προκειμένου να καταγράφει και να διαχειρίζεται τις διάφορες λειτουργίες της, όπως επίσης και να υποστηρίζει τον τρόπο ζωής των ενοίκων της. Χρησιμοποιείται ακόμα και ο όρος οικιακός αυτοματισμός, για να περιγράψει τα "έξυπνα" σπίτια, καθώς όλες οι "έξυπνες" συσκευές λειτουργούν συγχρονισμένα προκειμένου να αυτοματοποιήσουν τις οικιακές εργασίες και τα καθήκοντα. Η αυξανόμενη τάση ποικίλων ηλεκτρικών συσκευών (τηλεόραση, ψυγείο, κουζίνα, κλιματιστικό, κλπ.), οι οποίες έχουν τη δυνατότητα πρόσβασης στο Διαδίκτυο, μέσω τοπικού δικτύου WiFi, σε συνδυασμό με την ανάπτυξη των κινητών υπολογιστικών συσκευών, έχουν συνδράμει προς όφελος των "έξυπνων" σπιτιών. Παρόλο που οι πιο συνηθισμένες υπηρεσίες που παρέχονται από τα "έξυπνα" σπίτια, έχουν να κάνουν με την άνεση και τη διασκέδαση, κανείς δεν πρέπει να παραγκωνίσει τις πολλές εφαρμογές τους σε πιο ευαίσθητους τομείς, όπως π.χ. η παρακολούθηση ανθρώπων με κινητικά ή άλλα προβλήματα υγείας (με τη χρήση βιοαισθητήρων – biosensors) (Amiribesheli et al., 2015), η παροχή υπηρεσιών τηλεϊατρικής (Suresh & Sruthi, 2015), η εξοικονόμηση ενέργειας (Ahmad et al., 2016) και η τήρηση της ασφάλειας (Jose & Malekian, 2017). Οι Stojkoska και Trivodaliev (2017) προτείνουν ένα αρκετά πλήρες και γενικό πλαίσιο λειτουργίας των εφαρμογών "έξυπνου" σπιτιού, όπως φαίνεται στο ***Σχήμα*** που ακολουθεί (η ασύρματη ροή δεδομένων σημειώνεται με διακεκομμένη γραμμή).



Σχήμα 2-3: Πλαίσιο Λειτουργίας "Έξυπνου" Σπιτιού (Stojkoska & Trivodaliev, 2017)

Με βάση αυτό, όλες οι οικιακές συσκευές είναι εξοπλισμένες με interfaces ασύρματης επικοινωνίας και συνολικά όλες μαζί συνιστούν ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network). Τα δεδομένα των αισθητήρων αποστέλλονται σε έναν κεντρικό σταθμό επεξεργασίας που συναντάται στη βιβλιογραφία ως Home Hub ή 'Home Sink' και μπορεί να είναι ένας έξυπνος μετρητής ή απλά μία κινητή συσκευή (smartphone, tablet).

Όλα τα δεδομένα από τους αισθητήρες συγκεντρώνονται στο υπολογιστικό νέφος (cloud), το οποίο παρέχει **δυνατότητες αποθήκευσης μεγάλων δεδομένων και φυσικά υποδομές για την επεξεργασία τους**.

2.1.2. "Έξυπνη" Πόλη

Παρόλο που ο όρος 'Smart Cities' έχει εισαχθεί στην επιστημονική συζήτηση από το 1990, μέχρι σήμερα ***δεν υπάρχει ένας one-size-fits-all ορισμός*** για το τι είναι και το κυριότερο για το τι δεν είναι μία "έξυπνη" πόλη (O'Grady & O'Hare, 2012). Ένας πολύ πρόσφατος ορισμός, από τους Zedadra et al. (2019), αναφέρει πως '*Smart cities are complex and large distributed systems characterized by their heterogeneity, security, and reliability challenges. In addition, they are required to take into account several scalability, efficiency, safety, real-time responses, and smartness issues*'. Σε κάθε περίπτωση ο αναγνώστης μπορεί να αναζητήσει μια σειρά από ορισμούς στις εργασίες πολλών συγγραφέων, όπως οι Cretu (2012), Kourtit και Nijkamp (2012), Nam και Pardo (2011) και Komninos (2015).

Ένας –ίσως λιγότερο επιστημονικός- αλλά περισσότερο πρακτικός ορισμός/ περιγραφή του όρου 'Έξυπνη Πόλη' την ορίζει ως μια πόλη που παρακολουθεί, ελέγχει και προσπαθεί να προσαρμόσει ηλεκτρονικές διατάξεις σε υποδομές, όπως δρόμους, γέφυρες, υπόγειους ή σιδηροδρομικούς σταθμούς, αεροδρόμια, ενεργειακούς σταθμούς και άλλες σημαντικές υποδομές, με στόχο να τις καταστήσει ευφυείς και να αυξήσει την προστιθέμενη αξία των υπηρεσιών που αυτές προσφέρουν. Αντικειμενικός της σκοπός είναι, μέσα από όλη αυτή την παρακολούθηση και συλλογή δεδομένων, να μπορέσει να αξιοποιήσει αποδοτικότερα τους διαθέσιμους πόρους (φυσικούς ή μη), να παρέχει περισσότερη ασφάλεια στους πολίτες της και γενικότερα, να βελτιστοποιήσει τις υπηρεσίες που τους παρέχει. Συστήματα υψηλών προδιαγραφών που καταγράφουν τα δρώμενα σε ένα αστικό περιβάλλον και αναλύουν τα δεδομένα, διευκολύνουν το έργο της λήψης αποφάσεων από τη μεριά της διοίκησής της (Mapping Smart Cities in the EU, 2014). Σύμφωνα με την Ευρωπαϊκή Ένωση, μια "έξυπνη" πόλη ξεπερνά τη χρήση Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ) για καλύτερη χρήση των πόρων και μειωμένες εκπομπές ρύπων, όπως ίσως έχει επικρατήσει με βάση την κοινή πεποίθηση των πολιτών. Σημαίνει ***ακόμα, ευφυέστερα δίκτυα αστικών μεταφορών, αναβαθμισμένες εγκαταστάσεις παροχής νερού και διάθεσης αποβλήτων και πιο αποτελεσματικούς τρόπους φωτισμού και θέρμανσης των κτιρίων***. Τέλος, η 'Έξυπνη Πόλη'

απαιτεί μια πιο διαδραστική και ευαίσθητη διοίκηση της πόλης, ασφαλέστερους δημόσιους χώρους και κάλυψη των αναγκών της γήρανσης του πληθυσμού.

- **Χαρακτηριστικά "Έξυπνης" Πόλης**

Είναι εύκολα αντιληπτό, ότι το δυναμικό κοινωνικό-οικονομικό περιβάλλον, σε συνδυασμό με όλες τις προκλήσεις σε τεχνολογικό αλλά και ρυθμιστικό επίπεδο, αποτελεί πρόσφορο έδαφος για την ανάπτυξη μιας σειράς χαρακτηριστικών της "έξυπνης" πόλης. Η σημασία των "έξυπνων" πόλεων εντείνεται ακόμα περισσότερο αν κανείς αναλογιστεί πως σύμφωνα με τα Ηνωμένα Έθνη, πάνω από το 50% του πληθυσμού της γης κατοικούν αυτή τη στιγμή εντός ή πέριξ αστικών περιοχών. Για την Ευρώπη δε, το ποσοστό αυτό ανέρχεται στο 75%. Σύμφωνα με τους Lombardi (2011) και Lombardi et al. (2012), ***έξι (6) είναι οι βασικές διαστάσεις*** μιας "Έξυπνης" Πόλης σε αντιστοιχία με τις διαφορετικές εκφάνσεις της ζωής στα αστικά κέντρα (**βλ. Πίνακα 2.1**).

Πίνακας 2-1: Οι Βασικές Διαστάσεις της 'Έξυπνης Πόλης' (Lombardi et al., 2012)

Διάσταση	Ζωή στην Πόλη
Έξυπνη Διακυβέρνηση – Smart Governance	e-democracy
Έξυπνη Κινητικότητα – Smart Mobility	Logistics and Infrastructure
Έξυπνο Περιβάλλον – Smart Environment	Efficiency & Sustainability
Έξυπνη Οικονομία – Smart Economy	Citizens & Industry
Έξυπνους Ανθρώπους – Smart People	Training and Education
Έξυπνη Διαβίωση – Smart Living	Security and Quality of Life

2.1.3. "Έξυπνη" Διακυβέρνηση

Αφορά τη χρήση τεχνολογίας για τη διευκόλυνση και τον καλύτερο σχεδιασμό στη διαδικασία λήψης κυβερνητικών αποφάσεων ως αποτέλεσμα της αναπόφευκτης εξέλιξης των παραδοσιακών συστημάτων ηλεκτρονικής διακυβέρνησης (e-government) (Kankanhalli et al., 2019). Κεντρικοί στόχοι είναι η βελτίωση των δημοκρατικών διαδικασιών και η αποδοτικότερη παροχή των δημόσιων υπηρεσιών πάντα με κριτήρια την ***αύξηση της συμμετοχής και την ενεργοποίηση των πολιτών, τη διαφάνεια και την ενίσχυση της υπευθυνότητας*** των δημοσίων αρχών και λειτουργιών και την όσο το δυνατόν ομαλή και αφανή ***διαλειτουργικότητα των συνεργαζόμενων υπηρεσιών και των συστημάτων*** τους (Gil-Garcia et al., 2016). Οι τεχνολογίες ICT σε επίπεδο λογισμικού αλλά και υποδομής, είναι αυτές που παρέχουν την απαιτούμενη διαλειτουργικότητα και τροφοδοτούν με τα απαραίτητα δεδομένα τους αρμόδιους φορείς. Μέσω του e-governance στη δημόσια διοίκηση, οι εκάστοτε κυβερνήσεις μπορούν να παρέχουν την απαιτούμενη διαφάνεια στους πολίτες, καθώς κοινοποιούνται οι διαδικασίες λήψης κυβερνητικών αποφάσεων, προάγοντας έτσι τις δημοκρατικές διαδικασίες. Ο στόχος

είναι η μετάβαση από το γραφειοκρατικό καθεστώς διακυβέρνησης σε ένα πιο ανθρωποκεντρικό. Προς αυτήν την κατεύθυνση, συμβάλλουν τα μέσα κοινωνικής δικτύωσης, αλλά και οι πλατφόρμες ηλεκτρονικής διακυβέρνησης, όπου πολίτες και κυβερνητικοί φορείς ανταλλάσσουν απόψεις και διεκπεραιώνουν αιτήματα, κάτω από ένα άμεσο και διαδραστικό περιβάλλον.

2.1.4. "Έξυπνη" Κινητικότητα

Οι σύγχρονες πόλεις στηρίζονται σε ένα σύστημα μετακίνησης και μεταφοράς ανθρώπων και αγαθών που μοιάζει να μην είναι βιώσιμο. Έρευνες και αναλύσεις αποδεικνύουν, ότι η μαζική χρήση των αυτοκινήτων προκαλεί συμφόρηση, περιβαλλοντική μόλυνση και υψηλές εκπομπές διοξειδίου του άνθρακα. Η "Έξυπνη" Κινητικότητα παρόλο που αποτελεί μία μόνο από τις διαστάσεις μιας "έξυπνης" πόλης, έχει πολύ μεγάλο αντίκτυπο στις υπόλοιπες, καθώς επηρεάζει σημαντικά τόσο την ποιότητα της ζωής των πολιτών, όσο και το φυσικό και αστικό περιβάλλον μέσα στο οποίο αυτοί ζουν και εργάζονται. ***Η βιβλιογραφία σταχυολογεί τα οφέλη της έξυπνης κινητικότητας*** τα οποία μπορούν να ταξινομηθούν στις ακόλουθες γενικές κατηγορίες (Bencardino et al., 2014):

- Μείωση της ατμοσφαιρικής ρύπανσης
- Μείωση της κυκλοφοριακής συμφόρησης
- Αύξηση της ασφάλειας των πολιτών
- Μείωση της ηχορύπανσης
- Βελτίωση των χρόνων μεταφοράς
- Μείωση του κόστους μεταφοράς

Ειδικότερα στις αστικές μεταφορές, η μείωση της χρήσης αυτοκινήτων προς όφελος νέων και εναλλακτικών μεθόδων μεταφοράς είναι μάλλον μονόδρομος. Ενδεικτικά, αναφέρονται η χρήση ηλεκτρικών αυτοκινήτων, η αύξηση του αριθμού των συμβατικών αυτοκινήτων EURO 5, η χρήση εναλλακτικών καυσίμων (π.χ. LPG, bio-diesel, fuel cells, κ.α.) (Benevolo et al., 2016), αλλά και η ενίσχυση των νέων μοντέλων που αναδύονται μέσα από τη ραγδαία εφαρμογή της λεγόμενης οικονομίας διαμοιρασμού (sharing economy), όπως π.χ. το carpooling (Hasan et al., 2016), το bike sharing (με τη χρήση τεχνολογιών georeferencing και geotagging) (Garau et al., 2016) και το Park & Ride (Martino & Rossi, 2016). Για να επιτευχθεί όμως αυτό, θα πρέπει μια ασύγχρονη, αλλά και σε πραγματικό χρόνο πληροφόρηση να είναι διαθέσιμη στο ευρύ κοινό σε υπολογιστικά "νέφη" για τις ώρες, στάσεις και δρομολόγια των μέσων, προκειμένου να μειωθεί το κόστος, ο χρόνος και οι εκπομπές του διοξειδίου. Ακόμα, η πληροφόρηση αυτή, σε συνδυασμό με την παροχή πραγματικών δεδομένων από το επιβατικό κοινό, είναι αναγκαία για τους υπεύθυνους αρμόδιους φορείς των Μέσων Μαζικής Μεταφοράς, ώστε να προβαίνουν στη βελτίωση των παρεχόμενων υπηρεσιών. Η ***Τεχνολογία IoT αναμένεται να διαδραματίσει***

κρίσιμο ρόλο στην επιτυχία των πρωτοβουλιών "έξυπνης" κινητικότητας τα επόμενα χρόνια μέσα από τη χρήση ενσωματωμένων συσκευών και σενσόρων που θα υποστηρίξουν τις κύριες περιοχές τεχνολογικής έρευνας που απεικονίζονται στο σχήμα που ακολουθεί (Faria et al., 2017).

Σχήμα 2-4: Έξυπνη Κινητικότητα – Περιοχές Τεχνολογικής Έρευνας (Faria et al., 2017)

2.1.5. "Έξυπνη" οικονομία

Ο ρόλος των αστικών κέντρων στην ανάπτυξη και την οικονομική ευημερία των πολιτών είναι πλέον αδιαμφισβήτητος, όπως δείχνει σχετικά πρόσφατη μελέτη των Ηνωμένων Εθνών (UN-Habitat, 2010). Σύμφωνα με αυτή, ενώ ο πληθυσμός στα αστικά κέντρα ανέβηκε κατά είκοσι ποσοστιαίες μονάδες από το 1960 ως το 2010, η αύξηση του κατά κεφαλήν εισοδήματος για την ίδια περίοδο ξεπερνά το 150%. Ωστόσο, υπάρχουν εξαιρέσεις σε αυτό. Για παράδειγμα, παρά τη βραδύτερη οικονομική ανάπτυξη σε σύγκριση με άλλες περιοχές, ο αστικός πληθυσμός της Αφρικής αυξήθηκε σχεδόν εννέα φορές, χωρίς η οικονομία να ακολουθήσει, ένα φαινόμενο που είναι γνωστό ως ''Urbanization without growth'' (Kumar & Dahiya, 2017).

Είναι φανερό λοιπόν, πως η οικονομική ανάπτυξη των πόλεων (growth poles) οδηγεί σε ευεργετικά αποτελέσματα για την οικονομία και την ευημερία των πολιτών στο σύνολο τους (Parr, 1999). Παραδοσιακά, ***πέντε είναι οι βασικές διαστάσεις ανάπτυξης της έξυπνης οικονομίας:*** **α)** δημιουργία clusters παραγωγής ή/ και καινοτομίας, **β)** εμπόριο και παραγωγή, **γ)** μεταφορές και logistics, **δ)** ενέργεια και **ε)** ανάπτυξη "έξυπνων" υπηρεσιών. Οι τεχνολογίες που βασίζονται στο ΔτΠ είναι σε θέση να δημιουργήσουν μια σειρά από νέες ευκαιρίες και κανάλια οικονομικής ανάπτυξης, όπως για παράδειγμα η ***ανάπτυξη μιας community-marketplace πλατφόρμας ανοιχτού κώδικα για τα δεδομένα IoT*** που υποστηρίζονται από κοινοπραξίες κρατικών οργανισμών και ιδιωτικών επιχειρήσεων ή ***οι τεχνολογίες Blockchain που βασίζονται στο ΔτΠ και στις αρχές της οικονομίας διαμοιρασμού.*** Πράγματι, η οικονομία

διαμοιρασμού στο πλαίσιο μιας "έξυπνης" πόλης δημιουργεί πολλές ευκαιρίες για "έξυπνες" πόλεις, όπως η αξιοποίηση των περιουσιακών στοιχείων των πολιτών, η αποτελεσματική μείωση του κόστους συναλλαγών και των αποβλήτων, η εξοικονόμηση ενέργειας και η μείωση της αστικής συμφόρησης (Sun et al., 2016).

2.1.6. "Έξυπνο" Περιβάλλον

Ο όρος περιλαμβάνει τη δυνατότητα που δίνεται από ***ασύρματα δίκτυα αισθητήρων/ σενσόρων (Wireless Sensor Networks - WSN) να ανιχνεύουν, κατανοούν και μετρούν μια σειρά από περιβαντολλογικούς δείκτες*** από ευαίσθητες οικολογίες και φυσικούς πόρους σε αστικά περιβάλλοντα. Ο πολλαπλασιασμός αυτών των συσκευών σε ένα δίκτυο επικοινωνίας-ενεργοποίησης (communicate & actuate) δημιουργεί το ΔτΠ, στο οποίο οι αισθητήρες και οι ενεργοποιητές συνδυάζονται με το περιβάλλον γύρω τους και οι πληροφορίες μοιράζονται σε πλατφόρμες για να υποστηρίξουν ένα κοινό λειτουργικό πλαίσιο (Gubbi et al., 2013). Το "έξυπνο" περιβάλλον με την υποστήριξη τεχνολογιών του ΔτΠ, δεν πρέπει να συγχέεται με το αμιγώς υπολογιστικό ΔτΠ περιβάλλον που έχει πολλές και γενικότερες εφαρμογές. Περιλαμβάνει κυρίως αντικείμενα όπως:

- **η διαχείριση κτιρίων** (θερμοκρασία, κλιματισμός (HVAC), έλεγχος υγρασίας, εξαερισμός, κ.α.) (Kyriazis et al., 2013; Yu et al., 2016; Bellagente et al., 2015).
- **η διαχείριση νερού** (ποιότητα, διαρροές, χρήση, διανομή, διαχείριση λυμάτων) (Caeiro & Martins; Curry et al., 2018; Ntuli & Abu-Mahfouz, 2016; Medvedev et al., 2015; Giacobbe et al., 2016; Chen et al., 2018).
- **η διαχείριση περιβάλλοντος** (ατμοσφαιρική ρύπανση, ηχορύπανση-επίπεδα θορύβου, παρακολούθηση υδάτινων ροών και βιομηχανικές εφαρμογές) (Sheng et al., 2015).

2.1.7. "Έξυπνη" διαβίωση (περιλαμβάνει ευζωία, υγεία και ασφάλεια)

Στις μέρες μας, ένας διαρκώς αυξανόμενος αριθμός εφαρμογών για προσωπικές κινητές συσκευές παρέχει τη δυνατότητα στους χρήστες να παρακολουθούν, να ελέγχουν και να αλληλοεπιδρούν με διάφορους αισθητήρες και ενεργοποιητές, με τη χρήση του ΔτΠ. Στο πλαίσιο αυτό, οι "έξυπνες" πόλεις είναι ***ασφαλείς, καθαρές, δε δημιουργούν διακρίσεις και είναι ανθεκτικές παρέχοντας ίσες ευκαιρίες στην εκπαίδευση και ένα υψηλό επίπεδο ποιότητας ζωής*** σε όλους τους πολίτες (Wince-Smith Deborah, 2017). Πιο συγκεκριμένα, η έξυπνη διαβίωση περιλαμβάνει τις ακόλουθες διαστάσεις όπως φαίνεται και στον ***Πίνακα 2.2***.

Πίνακας 2-2: Οι Βασικές Διαστάσεις της 'Έξυπνης Διαβίωσης' (Woetzel et al., 2018)

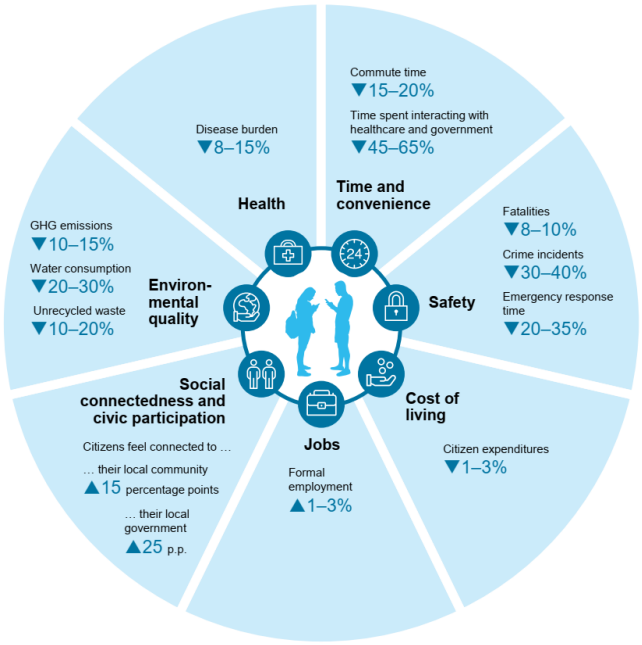
Διάσταση	Ζωή στην Πόλη
Κόστος Διαβίωσης – Cost of Living	Dynamic electricity pricing and usage tracking

	Digitized land use and permitting processes
	e-hailing and microtransit options
Ασφάλεια – Safety	Traffic Safety
	Data-driven Policing
	Optimized emergency response
Διαχείριση Χρόνου – Time Management	Public transit apps
	Intelligent Traffic Management
	New dynamic mobility options
Υγεία – Health	Improved chronic disease treatment
	Data driven public health interventions
	Digital tools for a better patient experience
Περιβάλλον – Environment	Air quality monitoring
	Energy-use optimization
	Electricity, water and waste tracking
Διασυνδεσιμότητα – Connectedness	Apps for person-2-person connections
	Apps connecting public to local government
	Apps that connect neighborhoods
Εργασία – Jobs	e-career centers, digital hiring platforms
	Digital admin processes for small businesses
	Data driven education, online retraining

Τα αποτελέσματα δείχνουν πως οι τεχνολογίες IoT και οι εφαρμογές της στο πλαίσιο μιας "έξυπνης" πόλης μπορούν να επιφέρουν σημαντικές βελτιώσεις στο επίπεδο της ποιότητας διαβίωσης των πολιτών.

2.1.8. "Έξυπνα" Συστήματα Μεταφοράς

Από τη στιγμή που τα οχήματα εξελίσσονται από απλά μέσα μεταφοράς σε "***έξυπνες" οντότητες με νέες ικανότητες αίσθησης και επικοινωνίας***, γίνονται ενεργά μέλη μιας έξυπνης πόλης. Το Ίντερνετ των Οχημάτων (Internet of Vehicles - IoV) αποτελείται από οχήματα που επικοινωνούν μεταξύ τους και με δημόσια δίκτυα μέσω των αλληλεπιδράσεων V2V (οχήματος προς οχήματα), V2I (οχήματος προς υποδομή) και V2P (οχημάτων προς πεζούς), πράγμα που επιτρέπει τόσο τη συλλογή όσο και την ανταλλαγή κρίσιμων πληροφοριών, σχετικά με την κατάσταση στο οδικό δίκτυο σε πραγματικό χρόνο (Maglaras et al., 2015). Στο ***Σχήμα 2.5*** παρουσιάζονται τα πλεονεκτήματα που προσφέρει η "έξυπνη" διαβίωση.



Σχήμα 2-5: Ωφέλειες "Έξυπνης" Διαβίωσης (Woetzel et al., 2018)

Στο πλαίσιο αυτό, ο αστικός στόλος των οχημάτων εξελίσσεται ραγδαία δημιουργώντας ένα δίκτυο αισθητήρων που παρέχουν διαρκώς πληροφορίες στους οδηγούς και μεταφέρουν δεδομένα (π.χ. θέση GPS και οδικές συνθήκες) στο νέφος του Διαδικτύου. Το δίκτυο αυτό με τη σειρά του είναι σε θέση στο μέλλον να δημιουργήσει ***ένα δίκτυο αυτόνομων οχημάτων (Autonomous Unmanned Vehicles - AUVs) που ανταλλάσσουν δεδομένα αισθητήρων μεταξύ τους,*** με στόχο τη βελτιστοποίηση της λειτουργίας τους που στην περίπτωση της εκτέλεσης μεταφορικού έργου (ιδιωτικό ή εμπορικό/ επιχειρηματικό) είναι η έγκαιρη παράδοση

επιβατών/ εμπορευμάτων σε προορισμούς με μέγιστη ασφάλεια, άνεση χωρίς καταστροφές και με την ελάχιστη δυνατή επίπτωση στο περιβάλλον (Lee et al., 2016).

Σχήμα 2-6: Το Διασυνδεδεμένο Όχημα

2.1.9. "Έξυπνες" Βιομηχανικές Εφαρμογές - Industry 4.0

Η τέταρτη βιομηχανική επανάσταση ή όπως έχει επικρατήσει να λέγεται στις μέρες μας, Industry 4.0 (αποτέλεσμα μιας γερμανικής στρατηγικής πρωτοβουλία για την εγχώρια βιομηχανία), στοχεύει στη δημιουργία ***έξυπνων εργοστασίων, όπου οι τεχνολογίες παραγωγής αναβαθμίζονται και μετασχηματίζονται ψηφιακά από κυβερνο-φυσικά συστήματα (Cyber Physical Systems), το Διαδίκτυο των πραγμάτων (IoT) και την υπολογιστική νέφους*** (Zhong et al., 2017). Στη νέα αυτή κατάσταση τα παραγωγικά συστήματα, ανάμεσα σε άλλες δυνατότητες, είναι σε θέση να παρακολουθούν τις φυσικές διεργασίες, να δημιουργούν ένα λεγόμενο «ψηφιακό δίδυμο» (Digital twin ή Twin cyber) του φυσικού κόσμου και να λαμβάνουν έξυπνες αποφάσεις μέσω επικοινωνίας και συνεργασίας σε πραγματικό χρόνο με τους ανθρώπους, τις συνδεδεμένες μηχανές και τους αισθητήρες (Wang et al., 2018). Η βιομηχανία 4.0 συνδυάζει ενσωματωμένες τεχνολογίες συστημάτων παραγωγής με έξυπνες διαδικασίες παραγωγής για να ανοίξει το δρόμο για μια νέα τεχνολογική εποχή που θα μεταβάλλει θεμελιωδώς τις αλυσίδες αξίας της βιομηχανίας, τις αλυσίδες αξίας της παραγωγής και τα επιχειρηματικά μοντέλα.

Στο πλαίσιο του Industry 4.0, τα ευφυή παραγωγικά συστήματα εκμεταλλεύονται προηγμένες τεχνολογίες πληροφοριών και παραγωγής για την επίτευξη ευέλικτων, έξυπνων και αναδιαμορφώσιμων διαδικασιών παραγωγής, προκειμένου να αντιμετωπίσουν τις προκλήσεις μιας δυναμικής και παγκόσμιας αγοράς (Shen & Norrie, 1999). Τα ευφυή παραγωγικά συστήματα κάνουν ευρεία χρήση των τεχνολογιών IoT για να μπορέσουν να φέρουν σε πέρας το παραγωγικό τους έργο οι οποίες σε αρκετές περιπτώσεις ***ενσωματώνουν δυνατότητες***

τεχνητής νοημοσύνης (AI), η οποία επιτρέπει στα συστήματα παραγωγής να μαθαίνουν από εμπειρίες προκειμένου να πραγματοποιήσουν τελικά μια συνδεδεμένη, ευφυή και πανταχού παρούσα (διάχυτη) βιομηχανική πρακτική (Liao et al., 2017). Οι βασικές τεχνολογίες που εφαρμόζονται στο πλαίσιο του Industry 4.0, στις σύγχρονες επιχειρήσεις φαίνονται στο ***Σχήμα 2.7*** και στην πλειοψηφία τους βασίζονται στη λειτουργία του ΔτΠ και της υπολογιστικής νέφους.

Σχήμα 2-7: Εφαρμογές Industry 4.0

2.1.10. "Έξυπνη" Υγεία

Η ιατρική και η υγειονομική περίθαλψη αντιπροσωπεύουν έναν από τους πιο ελκυστικούς τομείς εφαρμογής για τις τεχνολογίες IoT (Pang, 2013), οι οποίες δίνουν πλέον τη δυνατότητα ***ευρείας υιοθέτησης εφαρμογών διάχυτης υπολογιστικής, ενδυτών συστημάτων και των κινητών επικοινωνιών*** που με τη σειρά τους δημιουργούν νέες ευκαιρίες για τις κυβερνήσεις και τις επιχειρήσεις να επανεξετάσουν την ιδέα τους για την υγειονομική περίθαλψη. Ταυτόχρονα, η ***παγκόσμια διαδικασία αστικοποίησης*** αντιπροσωπεύει μια τεράστια πρόκληση και προσελκύει την προσοχή σε πόλεις που αναμένεται να συγκεντρώσουν υψηλότερους πληθυσμούς και να παρέχουν στους πολίτες υπηρεσίες με αποτελεσματικό και ανθρωποκεντρικό τρόπο (Solanas et al., 2014).

Για παράδειγμα, μία πολύ σημαντική τάση στην επιστήμη της ιατρικής, είναι η μεταφορά απλών ιατρικών ελέγχων και άλλων συνήθων υπηρεσιών υγειονομικής περίθαλψης από τα νοσοκομεία και τα ιατρεία στο σπίτι (Islam et al., 2015). Αυτό έχει σαν αποτέλεσμα ο ασθενής να λαμβάνει πιο εύκολα και πιο άμεσα φροντίδα, ειδικά στις περιπτώσεις έκτακτης ανάγκης, όπου απαιτείται άμεση δράση. Είναι πολύ σημαντικό επίσης, ότι τα νοσοκομεία μπορούν να

μειώσουν το φόρτο εργασίας τους μεταφέροντας πολλές από τις ενέργειες τους στο οικιακό περιβάλλον του ασθενή. Φυσικά, κάτι τέτοιο έχει ως επακόλουθο τη μείωση των δαπανών, τόσο για το νοσοκομείο, όσο και για τον ασθενή. Ως εκ τούτου, επείγει στο εγγύς μέλλον η εφαρμογή μιας τεχνολογίας στον κλάδο της υγείας ώστε να αναπτυχθούν προηγμένες τεχνικές και τεχνολογίες υγειονομικής περίθαλψης και να χρησιμοποιηθούν για την εύκολη παρακολούθηση των ασθενών από οπουδήποτε. Η παρακολούθηση των ασθενών περιλαμβάνει τον έλεγχο των φυσικών συνθηκών του ασθενούς και των λεπτομερειών του φαρμάκου (Gapchup et al., 2016).

Τα συστήματα υγειονομικής περίθαλψης που σχετίζονται με το Διαδίκτυο σήμερα βασίζονται στον ουσιαστικό ορισμό του Διαδικτύου ως ένα δίκτυο συσκευών που συνδέονται άμεσα μεταξύ τους για να συλλαμβάνουν και να μοιράζονται ζωτικά δεδομένα μέσω ενός ασφαλούς στρώματος υπηρεσιών (SSL) που συνδέεται με έναν κεντρικό διακομιστή εντολών και ελέγχου στο υπολογιστικό νέφος. Συνολικά, η εμφάνιση του IoT, στο οποίο οι συσκευές συνδέονται άμεσα με δεδομένα και μεταξύ τους, είναι σημαντική για δύο λόγους (Niewolny, 2013): **α)** Η πρόοδος στην τεχνολογία αισθητήρων και συνδεσιμότητας επιτρέπει στις συσκευές να συλλέγουν, να καταγράφουν και να αναλύουν δεδομένα που δεν ήταν προσιτά προηγουμένως. Στην υγειονομική περίθαλψη, αυτό σημαίνει ότι υπάρχει πια η δυνατότητα συλλογής δεδομένων ασθενών με την πάροδο του χρόνου που μπορούν να χρησιμοποιηθούν για να βοηθήσουν στην προληπτική φροντίδα, να επιτρέψουν την έγκαιρη διάγνωση οξειών επιπλοκών και να βοηθήσουν στην κατανόηση πώς μια θεραπεία (συνήθως φαρμακολογική) βοηθά στη βελτίωση των παραμέτρων του ασθενούς και **β)** Η ικανότητα των συσκευών να συλλέγουν δεδομένα από μόνα τους, καταργεί τους περιορισμούς των δεδομένων που εισάγονται από τον άνθρωπο. Πλέον, τα δεδομένα εισάγονται αυτόματα ώστε οι γιατροί να τα έχουν τη στιγμή και με τον τρόπο που τα χρειάζονται. Ο αυτοματισμός μειώνει τον κίνδυνο σφάλματος. Με τη χρήση του IoT, οι ενσωματωμένοι αισθητήρες που μπορούν να φορεθούν αποκτούν περισσότερες σαφείς λεπτομέρειες. Όπως ισχύει και για όλους τους υπόλοιπους τομείς, έτσι και στην περίπτωση αυτή, η ενσωμάτωση των τεχνολογιών IoT μπορεί να αποδώσει δραστικές αλλαγές και να φέρει μεγάλες βελτιώσεις στον τομέα της ιατρικής επιστήμης.

2.1.11. "Έξυπνη" Γεωργία

Η "έξυπνη" γεωργία αποτελεί μια μεθοδολογία που αξιοποιεί τεχνολογίες συλλογής πληροφοριών και ανάλυσης δεδομένων σε πραγματικό χρόνο με σκοπό τη βελτιστοποίηση της συνολικής γεωργικής παραγωγής. Περιλαμβάνει την ενσωμάτωση καινοτόμων τεχνολογιών όπως αισθητήρες, μη επανδρωμένα οχήματα και αλγόριθμους μηχανικής μάθησης για την παρακολούθηση και διαχείριση γεωργικών πρακτικών.

Πιο συγκεκριμένα, οι αισθητήρες χρησιμοποιούνται για τη συγκέντρωση δεδομένων σχετικά με την υγρασία του εδάφους, τα επίπεδα pH, τη θερμοκρασία, τις βροχοπτώσεις, την ταχύτητα του ανέμου, την ηλιακή ακτινοβολία και άλλες καιρικές παραμέτρους, καθώς και την περιεκτικότητα σε θρεπτικά συστατικά. Οι προαναφερθείσες πληροφορίες συμβάλλουν αισθητά στη λήψη σημαντικών αποφάσεων σχετικά με την άρδευση, έτσι ώστε να παρέχεται η κατάλληλη ποσότητα νερού στις καλλιέργειες, ενώ ταυτόχρονα εντοπίζονται και τα σημεία που απαιτείται επιπλέον νερό. Ακόμα, βάσει των δεδομένων που συλλέγονται καθορίζεται η ποσότητα λίπανσης που χρειάζεται η σοδειά, διαδραματίζοντας έτσι, καταλυτικό ρόλο στη βέλτιστη ανάπτυξη των καλλιεργειών (Jing et al., 2010).

Επιπροσθέτως, υπάρχουν αισθητήρες που αναγνωρίζουν τυχόν ασθένειες από παράσιτα και σε συνδυασμό με φασματικές κάμερες και μη επανδρωμένα οχήματα, καταγράφουν εικόνες υψηλής ανάλυσης των καλλιεργειών και παρακολουθούν ποικίλους δείκτες υγείας των φυτών (π.χ. περιεκτικότητα χλωροφύλλης) παρέχοντας πολύτιμες πληροφορίες για την κατάσταση τους και επιτρέποντας την έγκαιρη παρέμβαση των αγροτών σε περίπτωση ασθένειας των σοδειών. Ακόμη, η χρήση εξελιγμένων drones ενδέχεται να εξελιχθεί με την προσθήκη ψεκαστήρων ραντίσματος ή ποτίσματος, εξαιτίας της εμφάνισης παρασίτων και ασθενειών. Τα drones, συλλέγοντας φωτογραφίες, μπορούν να χαρτογραφήσουν τις καλλιέργειες και ύστερα από επεξεργασία των δεδομένων, να βγάλουν δείκτες βλάστησης και να αναδείξουν τα σημεία που χρειάζονται θεραπεία. Έτσι, προκύπτει ένα σχέδιο πτήσης, ενώ ταυτόχρονα έχει υπολογιστεί η ποσότητα των σπόρων που θα εφαρμοστούν στα αντίστοιχα σημεία της καλλιέργειας. Μάλιστα, τα τελευταία χρόνια το "έξυπνο" αυτό σύστημα ενισχύεται με σύγχρονες τεχνικές ανάλυσης, όπως αλγορίθμους μηχανικής μάθησης, οι οποίοι αξιοποιούν προγνωστικά μοντέλα με απώτερο στόχο τη βελτιστοποίηση των καλλιεργειών μέσω της πρόβλεψης καιρικών φαινομένων και της συχνότητας εμφάνισης ασθενειών στη σοδειά (Srivastava & Das, 2022).

Ωστόσο, αξίζει να σημειωθεί ότι αναδύονται και κάποιες προκλήσεις, που θέτουν σε κίνδυνο την ασφάλεια των δεδομένων λόγω του μεγάλου όγκου τους. Ακόμα, δεν πρέπει να παραγκωνιστεί το γεγονός ότι η πιθανότητα ασυμβατότητας των συσκευών και συστημάτων IoT είναι υψηλή, αφού ενδέχεται να προέρχονται από διαφορετικές κατασκευαστικές εταιρείες (Kumar & Sharma, 2020).

Σχήμα 2-8: "Έξυπνη" γεωργία (European Commission, 2020)

2.1.12. "Έξυπνα" Συστήματα Διαχείρισης Απορριμμάτων

Τα "έξυπνα" συστήματα διαχείρισης απορριμμάτων αξιοποιούν την τεχνολογία του ΔτΠ με σκοπό να αναβαθμίσουν αισθητά τις απαρχαιωμένες πρακτικές διαχείρισης απορριμμάτων. Αυτό επιτυγχάνεται μέσω της ενσωμάτωσης κατάλληλων αισθητήρων και της ανάλυσης δεδομένων, οδηγώντας στην real-time παρακολούθηση, τη βελτιστοποίηση και την αυτοματοποίηση των διαδικασιών συλλογής και ταξινόμησης αποβλήτων.

Ειδικότερα, υπάρχουν αισθητήρες που είναι εγκατεστημένοι σε κάδους απορριμμάτων και παρακολουθούν το επίπεδο πλήρωσης σε πραγματικό χρόνο. Τα συγκεκριμένα δεδομένα συλλέγονται και αποθηκεύονται σε μια κεντρική πλατφόρμα, συμβάλλοντας στη βελτιστοποίηση των διαδρομών των απορριμματοφόρων και ελαχιστοποιώντας έτσι, τις εκπομπές του διοξειδίου του άνθρακα (Shyam et al., 2017). Ακόμα, αισθητήρες με αλγόριθμους μηχανικής μάθησης δύνανται να βελτιώσουν τις διαδικασίες ανακύκλωσης μέσω της αυτοματοποίησης του διαχωρισμού και της ταξινόμησης των απορριμμάτων με βάση τη σύνθεση τους, ενισχύοντας την ακρίβεια και την αποτελεσματικότητα της διαδικασίας (Suvarnamma & Pradeepkiran, 2021). Αξίζει να σημειωθεί επίσης, ότι καινοτόμοι αισθητήρες, οι οποίοι είναι ενσωματωμένοι σε υγειονομικούς χώρους ταφής μπορούν να μετρήσουν περιβαλλοντικές παραμέτρους (π.χ. θερμοκρασία, υγρασία, κλπ.), με σκοπό να εντοπιστούν έγκαιρα καταστροφές, μειώνοντας έτσι, την πρόκληση ακόμα και θανατηφόρων ζημιών, ελαχιστοποιώντας τις περιβαλλοντικές επιπτώσεις και διασφαλίζοντας τη συμμόρφωση με το νομοθετικό πλαίσιο.

Συμπερασματικά, τα συστήματα "έξυπνης" διαχείρισης απορριμμάτων που βασίζονται στο Διαδίκτυο των Πραγμάτων προσφέρουν πολυάριθμα πλεονεκτήματα, όπως βελτιωμένη λειτουργική απόδοση, μειωμένο κόστος και ενισχυμένη περιβαλλοντική βιωσιμότητα.

2.2. Δομικά Στοιχεία Συστημάτων IoT

Σύμφωνα με το βαρόμετρο της Vodafone (2017), οι υφιστάμενοι χρήστες των τεχνολογιών IoT έχουν υψηλές προσδοκίες για το μέλλον της τεχνολογίας. Η πλειοψηφία θεωρεί ότι το IoT θα έχει τεράστια επίδραση στο σύνολο της οικονομίας μέσα στην επόμενη πενταετία, η οποία μάλιστα θα είναι μετρήσιμη. Ταυτόχρονα, σχεδόν το 75% των χρηστών συμφωνούν στο ότι ο ψηφιακός μετασχηματισμός (Digital transformation) που αναμένεται στο άμεσο μέλλον, θα είναι αδύνατος χωρίς τη χρήση τεχνολογιών IoT. Σε αυτή την ενότητα, θα γίνει προσπάθεια παρουσίασης των βασικών δομικών στοιχείων της αρχιτεκτονικής IoT. Στη βάση τους όλα τα συστήματα IoT χτίζονται πάνω σε **τέσσερις βασικούς πυλώνες**, οι οποίοι είναι απαραίτητοι για πετύχουν το σκοπό της χρήσης τους. Οι πυλώνες αυτοί είναι:

1. Οι Αισθητήρες/ Συσκευές (Sensors/ Devices)

Οι αισθητήρες/ συσκευές είναι ουσιαστικά τα "πράγματα" που συνθέτουν το Διαδίκτυο των Πραγμάτων. Ένας οργανισμός που θέλει να υλοποιήσει μια εφαρμογή IoT, θα χρειαστεί μια ασύρματη λύση που θα είναι σε θέση να υποστηρίξει το σύνολο των συσκευών που θα συμμετέχουν στο ασύρματο δίκτυο και να διασφαλίσει ότι οι εφαρμογές που εκτελούνται πάνω σε αυτό, "τρέχουν" απρόσκοπτα και ομαλά. Ανάλογα με το μέγεθος του οργανισμού, αλλά και το είδος της συσκευής, το δίκτυο μπορεί να περιλαμβάνει εκατοντάδες ή χιλιάδες διασυνδεδεμένους κόμβους (αισθητήρες, συσκευές) που δουλεύουν μαζί, σε ένα μόνο δίκτυο.

2. Δεδομένα και επεξεργασία τους

Μία από τις κύριες λειτουργίες του IoT είναι η συγκέντρωση τεράστιου όγκου δεδομένων για τη βελτίωση των διαδικασιών και της λειτουργίας υφιστάμενων συστημάτων ή η ανάπτυξη νέων συστημάτων και εφαρμογών. Η μορφή των δεδομένων ποικίλλει, π.χ. θα μπορούσε να αφορά ώρες streaming video για την παρακολούθηση μιας περιοχής, δεκάδες χιλιάδες βήματα και πληροφορίες τοποθεσίας από μια εφαρμογή έξυπνου ρολογιού ή στοιχεία παραγωγής από έναν αυτοματισμό παραγωγικής μονάδας. Προφανώς στην τελευταία περίπτωση η ποσότητα των προς επεξεργασία δεδομένων είναι πολύ μεγαλύτερη, το ίδιο και οι ανάγκες σε υπολογιστική ισχύ, δυναμικότητα αποθήκευσης και εργαλεία επεξεργασίας. Η δυνατότητα ανάλυσης όλων των πληροφοριών που συγκεντρώνονται είναι αυτό που κάνει τις εφαρμογές του IoT χρήσιμες και τόσο ελκυστικές. Είναι η ανάλυση δεδομένων που βοηθά στη βελτιστοποίηση της χρήσης της συσκευής και των ωφελειών των χρηστών από αυτή.

3. Συνδεσιμότητα

Η συνδεσιμότητα είναι αυτή που επιτρέπει στους δύο προηγούμενους πυλώνες να λειτουργούν in tandem. Οι συσκευές πρέπει να είναι συνδεδεμένες για τη μεταφορά δεδομένων. Τα

δεδομένα δεν μπορούν να σταλούν ή να ληφθούν χωρίς αξιόπιστη συνδεσιμότητα υψηλού εύρους ζώνης που υποστηρίζει τη ροή δεδομένων σε πραγματικό χρόνο από τις πολλές συσκευές που ζουν σε ένα δίκτυο. Χωρίς ικανοποιητικές υποδομές συνδεσιμότητας, η ανάλυση δεδομένων πάσχει, ενώ η επεκτασιμότητα της τεχνολογίας καθίσταται προβληματική.

4. Διαπροσωπεία

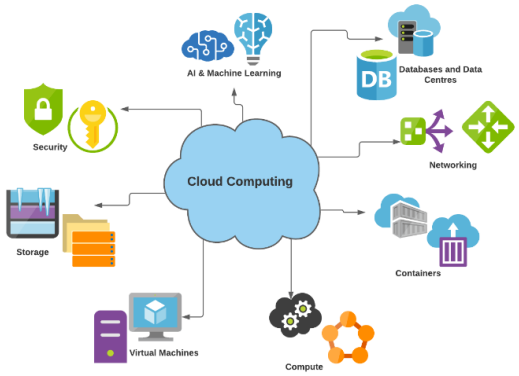
Η διεπαφή του εκάστοτε χρήστη με μια εφαρμογή IoT (user interface) είναι ένα πολύ ενδιαφέρον θέμα, καθώς η μορφή της ποικίλλει από μια απλή οθόνη γραφικών σε έξυπνες συσκευασίες προϊόντων ή πολύπλοκους και αναλυτικούς πίνακες ελέγχου (dashboards). Χαρακτηριστικό είναι το παράδειγμα της εταιρίας AdhereTech (2021), η οποία λανσάρει στην αγορά ένα "έξυπνο" μπουκάλι για χάπια. Οι ασθενείς παίρνουν το μπουκάλι που έχει προδιαμορφωθεί (χωρίς ρύθμιση) από τον φαρμακοποιό, όταν αγοράζουν τα φάρμακά τους και το απορρίπτουν όταν έχουν ολοκληρώσει την θεραπεία τους για επαναχρησιμοποίηση ή ανακύκλωση. Το μπουκάλι αυτό παρέχει στους ασθενείς ηχητικές και οπτικές υπενθυμίσεις για να παίρνουν τα φάρμακά τους. Προειδοποιεί ταυτόχρονα τους ιατρικούς επαγγελματίες όταν οι ασθενείς αμελούν να το κάνουν. Οι ασθενείς μπορούν να επιλέξουν τα μέσα που προτιμούν να λαμβάνουν ειδοποιήσεις - SMS, στο κινητό ή στο σταθερό τους τηλέφωνο ή ακόμα και στο μπουκάλι, που έτσι μετατρέπεται σε περιβάλλον διεπαφής.

Σχήμα 2-9: "Έξυπνη" συσκευή για υπενθύμιση χορήγησης φαρμάκων

2.3. Υπολογιστική Νέφους (Cloud Computing)

Η υπολογιστική νέφους (cloud computing) και το Internet of Things είναι άρρηκτα συνδεδεμένα, με σκοπό την υποστήριξη ποικίλων εφαρμογών και υπηρεσιών σε διάφορους κλάδους. Πιο συγκεκριμένα, οι συσκευές IoT, όπως είναι οι αισθητήρες και οι ενεργοποιητές, παράγουν τεράστιο όγκο δεδομένων, καθώς συλλέγουν πληροφορίες από το φυσικό κόσμο. Το cloud computing παρέχει την απαραίτητη υποδομή για την αποθήκευση, επεξεργασία και ανάλυση των συγκεκριμένων δεδομένων σε πραγματικό χρόνο (Abel et al., 2023). Ακόμα, το cloud computing προσφέρει ουσιαστικά απεριόριστη επεκτασιμότητα, επιτρέποντας στις

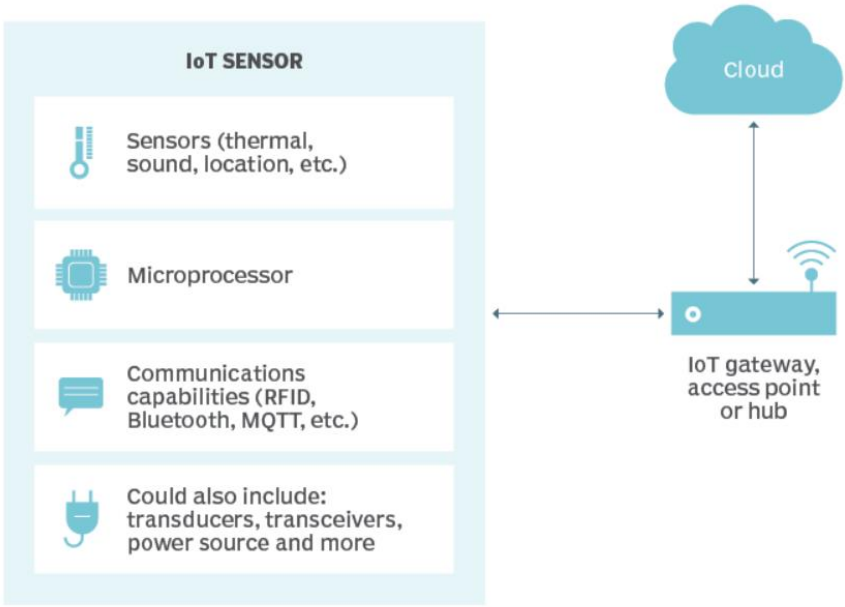
εγκαταστάσεις IoT να προσαρμόζονται στις διακυμάνσεις του όγκου δεδομένων και της συνδεσιμότητας των συσκευών. Εφόσον ο αριθμός των συσκευών IoT αυξάνεται, καθώς και η ζήτηση για επεξεργασία δεδομένων, οι πόροι του cloud μπορούν εύκολα να προσαρμοστούν ανάλογα, ώστε να ανταποκρίνονται στις απαιτήσεις, εξασφαλίζοντας βέλτιστες επιδόσεις και αξιοπιστία (Subrahmanyam et al., 2023). Ένα επιπρόσθετο πλεονέκτημα είναι ότι οι πλατφόρμες IoT που βασίζονται στο νέφος επιτρέπουν την απομακρυσμένη παρακολούθηση και διαχείριση των συνδεδεμένων συσκευών από οπουδήποτε υπάρχει σύνδεση στο διαδίκτυο. Οι χρήστες μπορούν να παρακολουθούν την κατάσταση των συσκευών, να διαμορφώνουν τις ρυθμίσεις και να ενημερώνουν από απόσταση το υλικολογισμικό, ενισχύοντας τη λειτουργική αποδοτικότητα και την ανταπόκριση (Insys Technologies, 2019). Επίσης, οι υπηρεσίες αποθήκευσης στο νέφος παρέχουν ασφαλή και αξιόπιστα αποθετήρια για την αποθήκευση δεδομένων που παράγονται από το ΔτΠ. Αξιοποιώντας την αποθήκευση στο νέφος, οι οργανισμοί μπορούν να αποφύγουν το κόστος και την πολυπλοκότητα της διατήρησης υποδομών αποθήκευσης στις εγκαταστάσεις τους, διασφαλίζοντας παράλληλα τη διάρκεια και την προσβασιμότητα των δεδομένων (AWS, n.d.). Τέλος, τα εργαλεία ανάλυσης που βασίζονται στο νέφος επιτρέπουν την προηγμένη επεξεργασία και οπτικοποίηση δεδομένων, επιτρέποντας στους οργανισμούς να αντλούν αξιοποιήσιμες πληροφορίες από τα δεδομένα IoT. Με την εφαρμογή αλγορίθμων μηχανικής μάθησης και μοντέλων προβλεπτικής ανάλυσης στο cloud, οι επιχειρήσεις μπορούν να αποκαλύψουν μοτίβα, τάσεις και ανωμαλίες που κρύβονται μέσα στις ροές δεδομένων IoT, δίνοντας τη δυνατότητα λήψης αποφάσεων και καινοτομίας βάσει δεδομένων (DataThick, 2024). Συνοπτικά, το cloud computing παρέχει την υποδομή, την αποθήκευση, την επεξεργαστική ισχύ και τις αναλυτικές δυνατότητες που απαιτούνται για την υποστήριξη της ανάπτυξης και της λειτουργίας των λύσεων IoT, επιτρέποντας στους οργανισμούς να αξιοποιήσουν το πλήρες δυναμικό των συνδεδεμένων συσκευών για την προώθηση της καινοτομίας, της αποδοτικότητας και της δημιουργίας προστιθεμένης αξίας.



Σχήμα 2-10: Υπολογιστικής νέφους (OSTECHNIX, 2022)

3. Αισθητήρες (Sensors)

Οι αισθητήρες αποτελούν το θεμέλιο λίθο οποιουδήποτε οικοσυστήματος IoT παρέχοντας δεδομένα σε πραγματικό χρόνο, τα οποία μπορούν να αξιοποιηθούν σε αναρίθμητες εφαρμογές, όπως στην παρακολούθηση ποικίλων περιβαλλοντικών παραμέτρων (π.χ. θερμοκρασία, υγρασία, ατμοσφαιρική πίεση, κλπ.), στην "έξυπνη" γεωργία, στα "έξυπνα" κτίρια, στα "έξυπνα" συστήματα διαχείρισης αποβλήτων και σε πολλές άλλες (Sehrawat & Gill, 2019). Αξίζει να σημειωθεί, ότι ένας "έξυπνος" αισθητήρας ενδέχεται να περιλαμβάνει και άλλα εξαρτήματα, όπως ενισχυτές, μορφοτροπείς, πομποδέκτες, πηγές ενέργειας (TechTarget, 2023). Ειδικότερα, σε αντίθεση με τους παραδοσιακούς αισθητήρες, οι "έξυπνοι" αισθητήρες διαθέτουν ενσωματωμένους μικροεπεξεργαστές που τους επιτρέπουν να πραγματοποιούν υπολογισμούς, να φιλτράρουν περιττά δεδομένα, ακόμη και να κάνουν βασικές επιλογές με βάση τις πληροφορίες που συγκεντρώνουν (Frank, 2000). Η τεχνολογία "έξυπνων" αισθητήρων περιλαμβάνει επίσης, ενσωματωμένες δυνατότητες επικοινωνίας που τους επιτρέπουν να συνδέονται σε ιδιωτικό περιβάλλον υπολογιστικού νέφους ή στο διαδίκτυο, επομένως και με εξωτερικές συσκευές (TechTarget, 2023). Σε γενικές γραμμές, οι αισθητήρες παίζουν καταλυτικό ρόλο στην αυτοματοποίηση οποιασδήποτε εφαρμογής πραγματοποιώντας μετρήσεις και έπειτα, την κατάλληλη επεξεργασία των δεδομένων που συλλέγονται για την ανίχνευση συγκεκριμένων αλλαγών (Sehrawat & Gill, 2019).



Σχήμα 3-1: IoT αισθητήρας (TechTarget, 2023)

3.1. Ιστορική αναδρομή

Το Διαδίκτυο των Πραγμάτων έχει αναδειχθεί ως μια τεχνολογία μετασχηματισμού, που συνδέει "έξυπνες" συσκευές, όπως είναι οι αισθητήρες και επιτρέπει την απρόσκοπτη επικοινωνία μεταξύ του φυσικού και του ψηφιακού κόσμου. Με το πέρασμα του χρόνου, το ΔτΠ έχει σημειώσει μια σημαντική εξέλιξη, μεταβαίνοντας από απλές συνδεδεμένες συσκευές σε περίπλοκα "έξυπνα" οικοσυστήματα που φέρνουν επανάσταση στις βιομηχανίες και βελτιώνουν ραγδαία την καθημερινή ζωή των πολιτών. Οι πρώτοι αισθητήρες εμφανίζονται με τη μορφή απλών θερμομέτρων και βαρομέτρων, τα οποία χρησιμοποιούνται για τη μέτρηση της θερμοκρασίας και της ατμοσφαιρικής πίεσης, αντίστοιχα. Ύστερα, εντοπίστηκαν στην ιστορία οι ηλεκτρομηχανικοί αισθητήρες, οι οποίοι χρησιμοποιούσαν ηλεκτρικά σήματα για την ανίχνευση φυσικών φαινομένων. Τα παραδείγματα περιλαμβάνουν μετρητές για τον υπολογισμό μηχανικής καταπόνησης, μορφοτροπείς πίεσης για την ανίχνευση μεταβολών πίεσης, καθώς και επιταχυνσιόμετρα (Στάμος Παναγιώτης, 2013). Ωστόσο, ο 21^{ος} αιώνας σηματοδότησε την εποχή, κατά την οποία οι αισθητήρες άρχισαν να ενσωματώνονται όλο και περισσότερο με τα ηλεκτρονικά και τη ψηφιακή τεχνολογία, επιτρέποντας βελτιωμένη λειτουργικότητα, συνδεσιμότητα και δυνατότητες επεξεργασίας δεδομένων. "Έξυπνοι" αισθητήρες εξοπλισμένοι με μικροελεγκτές, κυκλώματα επεξεργασίας σήματος και διεπαφές ασύρματης επικοινωνίας έγιναν διαδεδομένοι, επιτρέποντας την απόκτηση, ανάλυση και μετάδοση δεδομένων σε πραγματικό χρόνο. Οι πλατφόρμες IoT διευκόλυναν την ενσωμάτωση αισθητήρων σε διασυνδεδεμένα δίκτυα, επιτρέποντας την απομακρυσμένη παρακολούθηση, έλεγχο και αυτοματοποίηση διαφόρων διαδικασιών σε όλους τους κλάδους. Οι τεχνικές μηχανικής μάθησης και τεχνητής νοημοσύνης εφαρμόζονται σε δεδομένα αισθητήρων για την εξαγωγή πληροφοριών, την πρόβλεψη των τάσεων και τη βελτιστοποίηση λειτουργιών σε διάφορους τομείς. Οι μελλοντικές τάσεις στην τεχνολογία αισθητήρων είναι πιθανό να επικεντρωθούν στην ενίσχυση της ευαισθησίας, στη βελτίωση της ενεργειακής απόδοσης και στην παροχή δυνατοτήτων ανίχνευσης πολλαπλών μέσων για την αντιμετώπιση σύνθετων πραγματικών προκλήσεων σε τομείς, όπως η κλιματική αλλαγή, οι ανανεώσιμες πηγές ενέργειας και η εξατομικευμένη υγειονομική περίθαλψη.

Συνολικά, η εξέλιξη των αισθητήρων χαρακτηρίζεται από συνεχή καινοτομία και τεχνολογική πρόοδο, καθοδηγώντας την πανταχού παρούσα παρουσία τους στη σύγχρονη κοινωνία και τον απαραίτητο ρόλο τους στην προώθηση της επιστημονικής γνώσης, στη βελτίωση των βιομηχανικών διαδικασιών και στη βελτίωση της ποιότητας ζωής (Medium, 2023).

3.2. Πλεονεκτήματα αισθητήρων

Μερικά από τα πιο βασικά οφέλη εφαρμογής "έξυπνων" αισθητήρων είναι τα εξής:

- Βελτιωμένη απόδοση και παραγωγικότητα: Οι "έξυπνοι" αισθητήρες δύνανται να αυτοματοποιήσουν επαναλαμβανόμενες εργασίες, να βελτιστοποιήσουν ποικίλες διαδικασίες και να μειώσουν το ανθρώπινο λάθος. Μια μελέτη της McKinsey & Company (2018) διαπίστωσε, ότι η εφαρμογή "έξυπνων" αισθητήρων στην κατασκευή μπορεί να οδηγήσει σε κέρδη παραγωγικότητας έως και 20%. Στη γεωργία, τα "έξυπνα" συστήματα άρδευσης που χρησιμοποιούν αισθητήρες υγρασίας του εδάφους μπορούν να βελτιστοποιήσουν τη χρήση του νερού έως και 30% (ICID, 2024).

- Βελτιωμένη ασφάλεια: Οι "έξυπνοι" αισθητήρες μπορούν να παρακολουθούν συνεχώς για πιθανούς κινδύνους, όπως καπνό, διαρροές αερίου ή παραβιάσεις ασφάλειας. Μια έκθεση της NFPA (2024) υπογραμμίζει, ότι οι "έξυπνοι" ανιχνευτές καπνού μπορούν να μειώσουν τους θανάτους από πυρκαγιά έως και 50% σε σύγκριση με τα παραδοσιακά μοντέλα. Επιπλέον, οι έξυπνοι αισθητήρες θυρών και παραθύρων μπορούν να αποτρέψουν τις διαρρήξεις κατά 80%, σύμφωνα με μια μελέτη που πραγματοποιήθηκε από το Πανεπιστήμιο της Καλιφόρνια (UC Berkley, 2024).

- Λήψη αποφάσεων με γνώμονα τα δεδομένα: Ο τεράστιος όγκος δεδομένων που συλλέγονται από "έξυπνους" αισθητήρες παρέχει πολύτιμες πληροφορίες που μπορούν να βοηθήσουν στη λήψη αποφάσεων. Μια μελέτη από το Harvard Business Review (2024) διαπίστωσε, ότι οι εταιρείες που αξιοποιούν δεδομένα αισθητήρων για αναλυτικά στοιχεία παρουσιάζουν αύξηση 6% στα περιθώρια κέρδους. Στην υγειονομική περίθαλψη, οι "έξυπνοι" wearable αισθητήρες μπορούν να παρακολουθούν ζωτικά σημεία και επίπεδα δραστηριότητας, επιτρέποντας στους γιατρούς να λαμβάνουν πιο ενημερωμένες αποφάσεις θεραπείας (Deloitte, 2024).

- Απομακρυσμένη παρακολούθηση και προγνωστική συντήρηση: Οι "έξυπνοι" αισθητήρες επιτρέπουν την παρακολούθηση οικοσυστημάτων και εξοπλισμού σε πραγματικό χρόνο, ακόμη και από απομακρυσμένες τοποθεσίες. Αυτό διευκολύνει την προληπτική συντήρηση, εντοπίζοντας πιθανά ζητήματα προτού κλιμακωθούν σε δαπανηρές βλάβες. Μια έκθεση της Deloitte (2024) προτείνει, ότι η προγνωστική συντήρηση που τροφοδοτείται από "έξυπνους" αισθητήρες μπορεί να μειώσει το κόστος συντήρησης έως και 40%. Για παράδειγμα, οι "έξυπνοι" αισθητήρες στις ανεμογεννήτριες μπορούν να προβλέψουν πιθανές βλάβες εξαρτημάτων, επιτρέποντας έγκαιρες επισκευές και ελαχιστοποιώντας το χρόνο διακοπής λειτουργίας τους.

- Βιωσιμότητα και Προστασία του Περιβάλλοντος: Οι "έξυπνοι" αισθητήρες διαδραματίζουν κρίσιμο ρόλο στην προώθηση της βιωσιμότητας, βελτιστοποιώντας τη χρήση των πόρων και ελαχιστοποιώντας τις περιβαλλοντικές επιπτώσεις. Όπως αναφέρθηκε προηγουμένως, τα

"έξυπνα" συστήματα άρδευσης με αισθητήρες υγρασίας του εδάφους εξοικονομούν νερό στο τομές της γεωργίας (ICID, 2024).

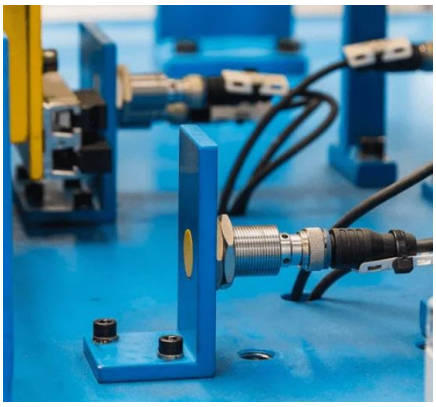
Συμπερασματικά, το μέλλον της τεχνολογίας "έξυπνων" αισθητήρων διαφαίνεται ιδιαίτερα λαμπρό, καθώς αυτές οι συσκευές γίνονται πιο προσιτές, ισχυρές και μικροσκοπικές. Αυτό έχει ως αποτέλεσμα, οι εφαρμογές τους να επεκτείνονται, μετατρέποντας τα σπίτια, τους χώρους εργασίας και τις πόλεις μας σε ακόμη πιο "έξυπνα" και πιο διασυνδεδεμένα οικοσυστήματα.

3.3. Είδη αισθητήρων

Όπως είναι κατανοητό, ο τεχνολογικός τομέας πλέον βρίθει διαφορετικών αισθητήρων, καθώς καινούργιες ανάγκες οδηγούν στη δημιουργία σύγχρονων λύσεων. Η ταξινόμηση των αισθητήρων μπορεί να γίνεται με βάση τις ιδιότητες που καταγράφει, τον τομέα που εφαρμόζεται, το υλικό κατασκευής τους, ακόμα και το φυσικό φαινόμενο που μελετά (Sehrawat & Gill, 2019). Στα επόμενα υποκεφάλαια, παρουσιάζονται οι βασικές κατηγορίες τους, καθώς και κάποια αξιοσημείωτα χαρακτηριστικά τους.

3.3.1. Αισθητήρες εγγύτητας (Proximity sensors)

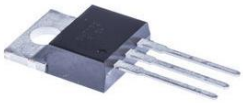
Η θέση οποιουδήποτε κοντινού αντικειμένου μπορεί εύκολα να ανιχνευθεί με αισθητήρα εγγύτητας χωρίς καμία φυσική επαφή. Αυτό επιτυγχάνεται μέσω της εκπομπής ηλεκτρομαγνητικής ακτινοβολίας, όπου διαπιστώνεται η παρουσία ενός αντικειμένου αναζητώντας απλώς οποιαδήποτε παραλλαγή στο σήμα επιστροφής. Υπάρχουν διάφοροι τέτοιοι τύποι, όπως επαγωγικοί, χωρητικοί, υπέρηχοι, φωτοηλεκτρικοί και μαγνητικοί. Οι συγκεκριμένοι αισθητήρες μπορούν να χρησιμοποιηθούν για παρακολούθηση και έλεγχο διεργασιών, μέτρηση αντικειμένων, γραμμές συναρμολόγησης και προσδιορισμό του διαθέσιμου χώρου, ενώ εφαρμόζονται σε χώρους λιανικής, βιομηχανικά συγκροτήματα και χώρους στάθμευσης (Kwaaitaal, 1993; Grattan & Sun, 2000; Zipit, 2021).



Σχήμα 3-2: Αισθητήρας εγγύτητας (Azo Sensors, 2012)

3.3.2. Αισθητήρες θερμοκρασίας (Temperature sensors)

Οι αισθητήρες θερμοκρασίας μετρούν την ποσότητα θερμότητας που παράγεται από μια περιοχή ή ένα αντικείμενο. Χρησιμοποιούνται σε διάφορους κλάδους, συμπεριλαμβανομένης της μεταποίησης, της υγειονομικής περίθαλψης, της βιομηχανίας, όπου αποτρέπεται η υπερθέρμανση του εξοπλισμού, μειώνοντας έτσι τον κίνδυνο αστοχίας του εξοπλισμού, καθώς και της γεωργίας (Zipit, 2021). Ακόμα, δύνανται να χρησιμοποιηθούν σε κάδους απορριμμάτων και σε χώρους υγειονομικής ταφής, καθώς οποιαδήποτε μεταβολή θερμοκρασίας μπορεί να υποδεικνύει τη διαδικασία αποσύνθεσης και την πιθανότητα κινδύνου πυρκαγιάς. Η έγκαιρη ανίχνευση αυξημένης θερμοκρασίας μπορεί να βοηθήσει στη λήψη προληπτικών μέτρων και στη βελτιστοποίηση των διαδικασιών διαχείρισης απορριμμάτων (VisionTIR, n.d.).



Σχήμα 3-3: Αισθητήρας θερμοκρασίας για τον τομέα της υγείας (Direct Industry, 2024)

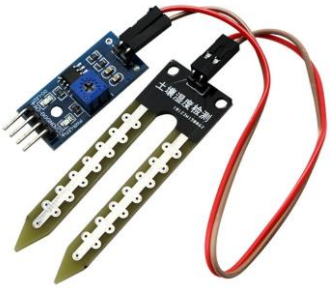
3.3.3. Αισθητήρες θέσης (Position sensors)

Ο αισθητήρας θέσης ανιχνεύει την παρουσία ανθρώπινης οντότητας ή αντικειμένων σε μια συγκεκριμένη εμβέλεια. Μπορεί να χρησιμοποιηθεί με σκοπό την ενίσχυση της ασφάλειας σπιτιού, όπου αναγνωρίζει την κίνηση και θέση πιθανών εγκληματιών. Ακόμα, δύναται να αξιοποιηθεί στην υγειονομική περίθαλψη μέσω της παρακολούθησης της θέσης ασθενών, νοσηλευτών κα γιατρών στο χώρο του νοσοκομείου (Dhar et al., 2014), καθώς και στη γεωργία για την ανίχνευση της θέσης των βοοειδών (Mekala & Viswanathan, 2017).

Σχήμα 3-4: Αισθητήρες θέσης (Eurosensor, 2019)

3.3.4. Αισθητήρες υγρασίας (Humidity sensors)

Οι συγκεκριμένοι αισθητήρες υπολογίζουν την ποσότητα του νερού που έχει εξατμιστεί στην ατμόσφαιρα, δηλαδή της υγρασίας που επικρατεί σε ένα χώρο. Εφαρμόζονται συχνά σε συστήματα εξαερισμού και κλιματισμού (Heating and Air Conditioning systems - HVAC), καθώς και για την παρακολούθηση του καιρού. Ειδικότερα σε περιβάλλοντα, όπου η υγρασία πρέπει να ελέγχεται διεξοδικά, όπως σε μουσεία, νοσοκομεία, θερμοκήπια και καλλιέργειες, παίζουν ρόλο αξιοσημείωτης σημασίας (Nayya & Puri, 2016; Zipit, 2021).



Σχήμα 3-5: Αισθητήρας υγρασίας (GROBOTRONICS, 2023)

3.3.5. Αισθητήρες κίνησης (Motion sensors)

Ένας αισθητήρας κίνησης αποτελεί μια συσκευή που χρησιμοποιείται για να ανιχνεύει οποιαδήποτε κινητική ενέργεια στο περιβάλλον. Χρησιμοποιείται συχνά σε συνδυασμό με τους αισθητήρες θέσης, με σκοπό την ενίσχυση της ασφάλειας των κατοικιών, όταν απουσιάζουν οι ιδιοκτήτες. Τη στιγμή που παρατηρείται κάποια κίνηση, πραγματοποιείται η λήψη φωτογραφιών και βίντεο, τα οποία μεταφέρονται σε έναν κεντρικό διακομιστή. Μερικές ακόμα εφαρμογές του συγκεκριμένου σένσορα είναι οι αυτοματοποιημένοι νεροχύτες, τα συστήματα διαχείρισης ενέργειας και τα αυτοματοποιημένα συστήματα στάθμευσης (Ansari et al., 2015). Αξίζει να τονιστεί, ότι οι τυπικοί αισθητήρες κίνησης ενδέχεται να λειτουργούν με υπερήχους, μικροκύματα ή παθητικά υπέρυθρα κύματα (Zipit, 2021).

Σχήμα 3-6: Αισθητήρας κίνησης εσωτερικού χώρου (emichos.gr, 2024)

3.3.6. Αισθητήρες ταχύτητας (Velocity sensors)

Οι αισθητήρες ταχύτητας είναι συσκευές που χρησιμοποιούνται για τη μέτρηση της ταχύτητας ενός αντικειμένου, συνήθως σε μηχανικές, βιομηχανικές ή επιστημονικές εφαρμογές. Είναι απαραίτητες σε διάφορους τομείς, όπως η αυτοκινητοβιομηχανία, η αεροδιαστημική, η ρομποτική και η ανάλυση κραδασμών. Ακόμα, εφαρμόζονται συχνά σε περιπτώσεις "έξυπνης" πόλης για την παρακολούθηση της ταχύτητας οχημάτων (Pendor & Tasgaonkar, 2016).

Σχήμα 3-7: Αισθητήρας ταχύτητας (Krikellas.gr, 2024)

3.3.7. Αισθητήρες πίεσης (Pressure sensors)

Αυτοί οι αισθητήρες ανιχνεύουν αλλαγές σε ένα αέριο ή υγρό. Όταν το εύρος πίεσης υπερβαίνει ένα καθορισμένο όριο, οι αισθητήρες πίεσης ειδοποιούν για το συγκεκριμένο πρόβλημα. Χρησιμοποιούνται για δοκιμές διαρροών, συστήματα νερού και αεροσκάφη. Μάλιστα, ορισμένα οχήματα χρησιμοποιούν σύστημα παρακολούθησης πίεσης ελαστικών για να ειδοποιούν όταν η πίεση των ελαστικών είναι χαμηλή και ενδεχομένως μη ασφαλής (Zipit, 2021). Ακόμα, έχουν καταγραφεί και εφαρμογές τους για την παρακολούθηση υγείας ασθενών (Zhang et al., 2012).

Σχήμα 3-8: Αισθητήρας πίεσης (bazakas.gr, 2024)

3.3.8. Αισθητήρες χημικών και αερίων (Chemical and Gas sensors)

Αυτοί οι αισθητήρες παρακολουθούν την ποιότητα του αέρα για την παρουσία τοξικών ή επικίνδυνων αερίων. Συχνά χρησιμοποιούν τεχνολογίες ημιαγωγών, ηλεκτροχημικών ή

φωτοϊοντισμού. Χρησιμοποιούνται κυρίως, σε βιομηχανικά και κατασκευαστικά περιβάλλοντα, καθώς και σε ανιχνευτές διοξειδίου του άνθρακα (Zipit, 2021).

Σχήμα 3-9: Αισθητήρας αερίων (Components, 2024)

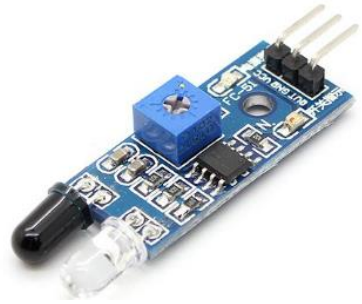
3.3.9. Αισθητήρες ποιότητας νερού (Water quality sensors)

Οι συγκεκριμένοι αισθητήρες παρακολουθούν την ποιότητα του νερού. Χρησιμοποιούνται συχνά σε συστήματα διανομής νερού, αλλά λειτουργούν και σε μια ποικιλία βιομηχανιών. Υπάρχουν διάφορα είδη αισθητήρων νερού, συμπεριλαμβανομένων των αισθητήρων υπολειμματικού χλωρίου, θολότητας, επιπέδων pH και ολικού οργανικού άνθρακα (Zipit, 2021). Οι ερευνητές Vijayakumar και Ramya (2015) παρουσίασαν ένα σύστημα χαμηλού κόστους για τη μελέτη των παραπάνω παραμέτρων και παρακολούθησαν συνολικά την ποιότητα του νερού.

Σχήμα 3-10: 3.2.9. Αισθητήρας ποιότητας νερού (rshydro, 2024)

3.3.10. Υπέρυθροι αισθητήρες (Infrared sensors)

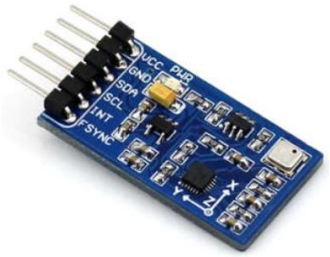
Ορισμένοι αισθητήρες είτε ανιχνεύουν είτε εκπέμπουν υπέρυθρη ακτινοβολία για να εντοπίσουν χαρακτηριστικά και αλλαγές στη γύρω περιοχή. Είναι χρήσιμα για τη μέτρηση των εκπομπών θερμότητας από ένα αντικείμενο. Οι αισθητήρες υπερύθρων χρησιμοποιούνται σε τηλεχειριστήρια, ρυθμίσεις υγειονομικής περίθαλψης, ακόμη και από ιστορικούς τέχνης που πιστοποιούν τα έργα τέχνης (Zipit, 2021).



Σχήμα 3-11: Υπέρυθρος αισθητήρας (Hellas digital, 2024)

3.3.11. Γυροσκοπικοί αισθητήρες (Gyroscope sensors)

Ένας αισθητήρας γυροσκοπίου μετρά τη γωνιακή ταχύτητα ή την ταχύτητα περιστροφής γύρω από έναν άξονα. Χρησιμοποιούνται γενικά για πλοήγηση στην αυτοκινητοβιομηχανία για συστήματα πλοήγησης και αντιολισθητικά συστήματα, καθώς και σε βιντεοπαιχνίδια και drones. Υπάρχουν τα οπτικά γυροσκόπια, τα περιστροφικά γυροσκόπια και τα γυροσκόπια δονούμενης δομής (Zipit, 2021).



Σχήμα 3-12: Γυροσκοπικός αισθητήρας (Semiconductorforu, 2024)

3.3.12. Οπτικοί αισθητήρες (Optical sensors)

Οι οπτικοί αισθητήρες μετρούν το φως και το μετατρέπουν σε ηλεκτρικά σήματα. Πολλές βιομηχανίες χρησιμοποιούν οπτικούς αισθητήρες, συμπεριλαμβανομένων των αυτοκινήτων, της ενέργειας, της υγειονομικής περίθαλψης και της αεροδιαστημικής. Οι αισθητήρες περιλαμβάνουν οπτικές ίνες, φωτοανιχνευτή και πυρόμετρο (Zipit, 2021).

Σχήμα 3-13: Οπτικός αισθητήρας (WEG, 2024)

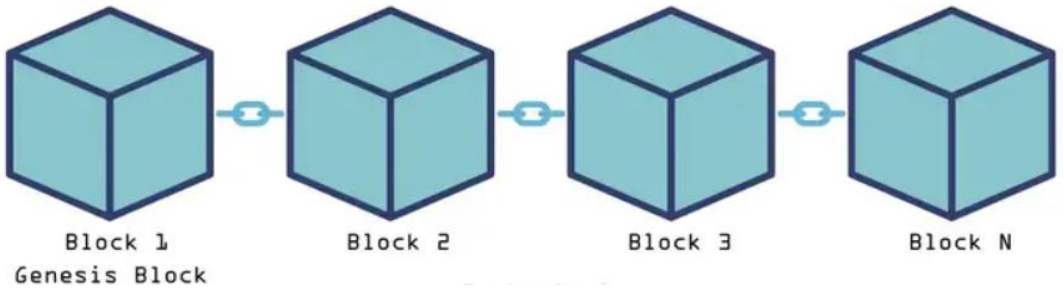
Με βάση τα παραπάνω, οι Sehrawat και Gill (2019) δημιούργησαν ένα συγκεντρωτικό πίνακα, ο οποίος περιλαμβάνει τα κατάλληλα είδη αισθητήρων ανάλογα με τον τομέα εφαρμογής τους.

Πίνακας 3-1: Χρήση κατάλληλων αισθητήρων ανάλογα με την IoT εφαρμογή (Sehrawat & Gill, 2019)

IoT εφαρμογή	**Είδη αισθητήρων**
"Έξυπνη" Πόλη	Ταχύτητας, Φωτός, Επιτάχυνσης, Θέσης, Θερμοκρασίας, Απόστασης, Υγρασίας, Πίεσης, Υπέρυθροι
"Έξυπνο" Περιβάλλον	Φωτός, Θερμοκρασίας, Υγρασίας, Χημικών, Γυροσκοπικοί, Βιολογικοί, Επιτάχυνσης, Οπτικοί
"Έξυπνη" Διαχείριση Νερού	Θερμοκρασίας, Υγρασίας, Ποιότητας Νερού, Χωρητικότητας
"Έξυπνο" Κτήριο	Φωτός, Επιτάχυνσης, Χημικών, Γυροσκοπικοί
"Έξυπνη" Υγεία	Φωτός, Επιτάχυνσης, Χημικών, Γυροσκοπικοί, Βιολογικοί, Πίεσης
"Έξυπνο" Σπίτι	Φωτός, Επιτάχυνσης, Χημικών, Γυροσκοπικοί, Βιολογικοί, Θερμοκρασίας, Απόστασης, Θέσης, Υπέρυθροι
"Έξυπνη" Μεταφορά	Γυροσκοπικοί, Πίεσης, Χημικών, Επιτάχυνσης, Θερμοκρασίας, Κίνησης, Υπέρυθροι
"Έξυπνη" Ασφάλεια	Φωτός, Γυροσκοπικοί, Χημικών, Επιτάχυνσης, Θερμοκρασίας, Κίνησης, Υπέρυθροι
"Έξυπνη" Γεωργία	Φωτός, Υγρασίας, Χημικών, Επιτάχυνσης, Θερμοκρασίας, Θέσης, Απόστασης, Ποιότητας Νερού

4. Τεχνολογία Blockchain

Η τεχνολογία Blockchain είναι μια ειδική, κατανεμημένη βάση δεδομένων, η οποία παρέχει ασφαλείς λύσεις μέσω της διαδικασίας της κρυπτογράφησης (Haber & Stornetta, 1991). Ουσιαστικά, συνιστά μία σειρά καταχωρήσεων, οι οποίες είναι χρονολογικά διατεταγμένες. Κάθε είδος καταχώρησης αποτελεί ένα block, το οποίο συνδέεται με τα προηγούμενα, σχηματίζοντας έτσι μια αλυσίδα (chain), από την οποία μάλιστα, πήρε και το όνομα της αυτή η τεχνολογία (CNN Greece, 18; Binance Academy, 2023). Το Blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό (ledger), το οποίο είναι διαμοιρασμένο σε όλα τα συμμετέχοντα μέλη, εξασφαλίζοντας αξιοπιστία και διαύγεια μεταξύ των συναλλαγών που πραγματοποιούνται (Christidis & Devetsikiotis, 2016). Η δομή του Blockchain μπορεί να παρουσιαστεί και στο ***Σχήμα 4.1***.



Σχήμα 4-1: Οπτικοποίηση της δομής Blockchain (W3schools, 2023)

Επιπροσθέτως, σύμφωνα με τους Frizzo-Barker et al. (2020): «*Το Blockchain είναι ένα αποκεντρωμένο, ψηφιακό καθολικό που διευκολύνει τις Peer-to-Peer μεταφορές αξίας όλων των ειδών, από ψηφιακά νομίσματα μέχρι εμπορεύματα και ακίνητα, χωρίς την ανάγκη μεσαζόντων όπως τράπεζες, λογιστές ή δικηγόρους*». Το Blockchain αποτελεί αναπόσπαστο κομμάτι των Τεχνολογιών Κατανεμημένης Λογιστικής (Distributed Ledger Technology – DLT), η οποία αναφέρεται σε κατανεμημένες βάσεις δεδομένων που διαχειρίζονται διάφοροι συμμετέχοντες, και όχι στην κεντρική βάση (Bigini et al., 2020; Tang et al., 2022).

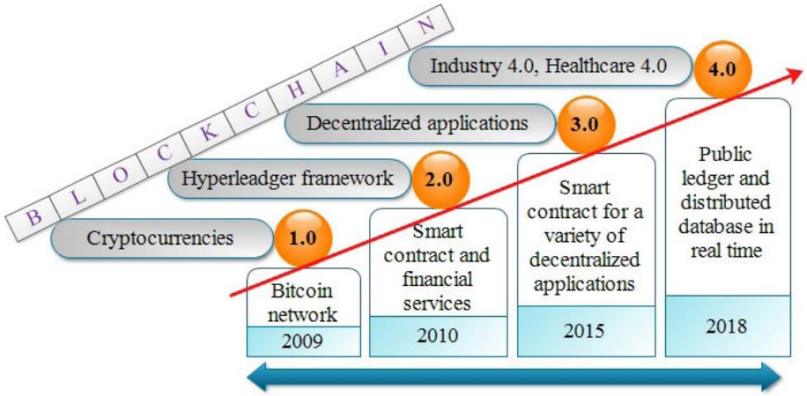
4.1. Ιστορική αναδρομή

Ο Chaum (1982), στη διδακτορική του διατριβή, πρότεινε ένα πρωτόκολλο, το οποίο μοιάζει με αυτό του Blockchain (Sherman et al., 2019). Αργότερα, οι Haber και Stornetta (1990) περιέγραψαν μία μέθοδο κρυπτογράφησης πληροφοριών με παρόμοια λειτουργία, θέλοντας να εφαρμόσουν ένα σύστημα για την ασφαλή ψηφιακή χρονική σήμανση εγγράφων, η οποία δε θα μπορούσε να παραβιαστεί. Στη συνέχεια, οι Bayer et al. (1993) ενσωμάτωσαν Merkle trees σε αυτή τη μέθοδο για να βελτιώσουν την απόδοση της και να μειώσουν τις απαιτήσεις λειτουργίας, μέσω της αποθήκευσης πολλαπλών εγγράφων σε κάθε block. Ωστόσο, το πρώτο

πλήρως αποκεντρωμένο και πλήρως λειτουργικό δίκτυο Blockchain παρουσιάστηκε από το Nakamoto (2008). Αυτή η δημοσίευση υπογράφεται από ένα άτομο με την ονομασία Satoshi Nakamoto, η ταυτότητα του οποίου είναι άγνωστη ακόμα και σήμερα ενώ πολλοί υποστηρίζουν ότι πίσω από αυτό το ψευδώνυμο βρίσκεται μία ομάδα ανθρώπων. Είναι αξιοσημείωτο ότι παρά το γεγονός ότι η συγκεκριμένη δημοσίευση με τίτλο "Bitcoin: A peer-to-peer electronic cash system", θεωρείται η πλέον καθοριστική για την αλματώδη ανάπτυξη της τεχνολογίας Blockchain τα τελευταία χρόνια, ο όρος αυτός δεν αναφέρεται στο συγκεκριμένο έγγραφο, ενώ το πιο κοντινό σε αυτό τον όρο που εμφανίζεται εντός του κειμένου της δημοσίευσης είναι το "chain of blocks".

Η συγκεκριμένη δημοσίευση προσπαθεί να προσεγγίσει την επίλυση ενός πολύπλοκου αινίγματος της θεωρίας παιγνίων με την ονομασία "Πρόβλημα των Βυζαντινών Στρατηγών" (Byzantine Generals Problem), το οποίο θα αναλυθεί εκτενέστερα στη συνέχεια. Μέσω της προτεινόμενης λύσης, εξασφαλίζεται ότι σε μια συγκεκριμένη χρονική στιγμή, ένα "block of assets" θα μπορούσε να μεταφερθεί σε ένα μόνο άλλο άτομο, χωρίς την ανάγκη ελέγχου από κάποιο τρίτο μέρος. Ένα χρόνο μετά τη δημοσίευση του Nakomoto (2008), δηλαδή το 2009, η έννοια του κατανεμημένου δικτύου Blockchain εφαρμόστηκε στην πράξη στην στο λογισμικό ανοιχτού κώδικα που αναπτύχθηκε για τη διάθεση και κυκλοφορία του κρυπτονομίσματος Bitcoin. Το πρώτο block του δικτύου Blockchain του Bitcoin δημιουργήθηκε στις 3 Ιανουαρίου 2009 (Hassan et al., 2018). Η χρήση του Blockchain για το Bitcoin το κατέστησε το πρώτο ψηφιακό νόμισμα που έλυσε το πρόβλημα των διπλών δαπανών (double spending problem), που είναι η χρήση του ίδιου asset για πολλαπλές διαφορετικές πληρωμές (Huang et al., 2021), χωρίς να απαιτείται άλλος αξιόπιστος διαχειριστής, εκτός των δύο συναλλασσόμενων μερών (Brito & Castillo, 2013). Ο όρος Blockchain άρχισε να χρησιμοποιείται ευρέως ως μία ενιαία λέξη, από το 2016.

Έχουν αναγνωριστεί 4 διαφορετικές φάσεις στην εξέλιξη της τεχνολογίας Blockchain, από τη δημιουργία της μέχρι σήμερα, οι οποίες ονομάζονται αντίστοιχα Blockchain 1.0, Blockchain 2.0, Blockchain 3.0 και Blockchain 4.0. Η περίοδος του Blockchain 1.0 αφορά την αρχική δημιουργία και χρήση των κρυπτονομισμάτων, το Blockchain 2.0 εισήγαγε τα "έξυπνα" συμβόλαια και το Blockchain 3.0 επέκτεινε τη χρήση των αποκεντρωμένων εφαρμογών σε άλλους τομείς εκτός της οικονομίας (υγεία, εφοδιαστική, "έξυπνες" πόλεις κτλ.). Η περίοδος του Blockchain 4.0, που έχει και την πιο πρόσφατη έναρξη, επικεντρώνεται στην παροχή υπηρεσιών σε πραγματικό χρόνο, κάτι το οποίο αξιοποιείται σε μεγάλο βαθμό από εφαρμογές που αφορούν την 4η Βιομηχανική Επανάσταση (Industry 4.0) (Bodkhe et al., 2020). Η εξέλιξη της τεχνολογίας Blockchain από το 2009 μέχρι σήμερα φαίνεται στο ***Σχήμα 4-2***.



Σχήμα 4-2: Εξέλιξη τεχνολογίας Blockchain (Bodkhe et al., 2020)

4.2. Το Πρόβλημα των Βυζαντινών Στρατηγών

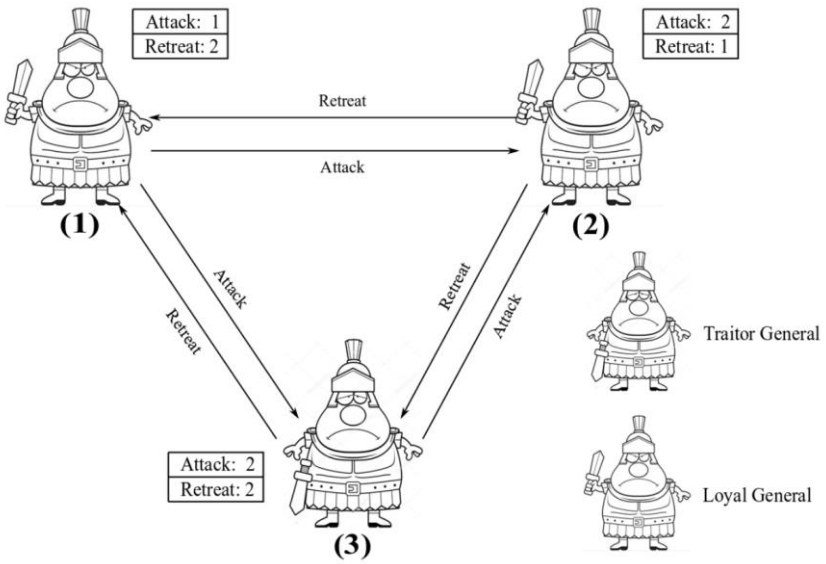
Σε αυτό το σημείο είναι η σημαντική η αναφορά στο "Πρόβλημα των Βυζαντινών Στρατηγών", καθώς αυτό αποτέλεσε την έμπνευση για τη δημιουργία και τον τρόπο λειτουργίας της τεχνολογίας Blockchain. Πρόβλημα παρόμοιο με αυτό, παρουσιάστηκε αρχικά και σε δημοσίευση των Akkoyunlu et al., (1975) και ο Gray (1978) του έδωσε την ονομασία "Two Generals Paradox" με την οποία και έγινε γνωστό. Ο Leslie Lamport ήταν αυτός που παρουσίασε για πρώτη φορά το ολοκληρωμένο πρόβλημα στις αντίστοιχες δημοσιεύσεις του (Lamport et al., 1982; Lamport & Fischer, 1982; Lamport, 1983).

Ακολουθεί σε αυτό το σημείο μία γενική περιγραφή για την κατανόηση του προβλήματος. Το πρόβλημα απεικονίζεται από δύο ή περισσότερους στρατηγούς του Βυζαντίου, οι οποίοι έχουν σταθμεύσει με τα στρατεύματα τους έξω από μία πόλη, αλλά σε διαφορετικές πλευρές. Στόχος τους είναι είτε η άμυνα της πόλης είτε η επίθεση σε αυτή και είναι απαραίτητος ο συντονισμός των ενεργειών τους για να πετύχουν το βέλτιστο δυνατό αποτέλεσμα. Οι στρατηγοί παίρνουν τις τελευταίες τους αποφάσεις για το αν θα επιτεθούν ή θα υποχωρήσουν δίνοντας διαταγές στους άλλους στρατηγούς και λαμβάνοντας διαταγές από αυτούς. Κάθε στρατηγός μπορεί να δώσει 2 διαταγές προς τους άλλους στρατηγούς πριν αντιμετωπίσει τον εχθρό: **α)** επίθεσης ή **β)** υποχώρησης. Ένας πόλεμος, είναι δυνατόν να κερδηθεί με τις λιγότερες δυνατές απώλειες μόνο όταν όλοι οι έντιμοι στρατηγοί συμφωνήσουν σε μια εντολή επίθεσης ή υποχώρησης. Ωστόσο, οι εντολές των στρατηγών αποστέλλονται από αγγελιοφόρους, καθώς δεν είναι δυνατόν να μεταφέρονται οι ίδιοι, με ή χωρίς τα στρατεύματα τους.

Εάν ο στρατηγός Α στείλει ένα μήνυμα που λέει «Επίθεση αύριο», δεν έχει ιδέα αν ο στρατηγός Β θα λάβει πραγματικά το μήνυμα και ενδεχομένως θα οδηγούταν σε μία ήττα, εάν τελικά έκανε την επίθεση χωρίς τον άλλο στρατηγό. Κατά την παραλαβή του μηνύματος, ο στρατηγός

Β δεν έχει ιδέα αν το μήνυμα είναι αυθεντικό ή αν έχει σταλεί από τον εχθρό για να τον οδηγήσει σε παγίδα. Παρ' όλα αυτά, έστω ότι επιβεβαίωνε την αυθεντικότητα, θα έπρεπε να στείλει απάντηση για να επιβεβαιώσει την επίθεση, αλλά δε θα γνώριζε αν ο στρατηγός Α την έλαβε, με αποτέλεσμα να φοβάται ότι ο άλλος στρατηγός θα σταματήσει την επίθεση, πράγμα που σημαίνει ότι ο στρατηγός Β θα είναι αυτός που θα επιτεθεί μόνος του και θα αντιμετωπίσει μία ενδεχόμενη ήττα. Ο στρατηγός Α θα μπορούσε, φυσικά, να στείλει ένα μήνυμα που να επιβεβαιώνει τη λήψη της επιβεβαίωσης του στρατηγού Β, αλλά ποτέ δεν θα μάθει πραγματικά αν έφτασε στον προορισμό του ή ακόμα και αν το μήνυμα ήταν αυθεντικό εξαρχής. Αυτό τον βάζει στο ίδιο σημείο που βρισκόταν ο στρατηγός Β.

Ένα παράδειγμα αυτής της κατάστασης με 3 στρατηγούς παρουσιάζεται στο ***Σχήμα 4-3***. Σύμφωνα με το παράδειγμα, ο Στρατηγός 3 είναι προδότης και μπορεί να εμποδίσει τους πιστούς στρατηγούς να επιτύχουν συναίνεση σε περίπτωση που έχουν διαφορετικές απόψεις, στέλνοντας τους μία διαφορετική απόφαση από τις διαταγές τους. Στην περίπτωση αυτή, ο Στρατηγός 1 θέλει να επιτεθεί ο Στρατηγός 2 θέλει να υποχωρήσει. Ο Στρατηγός 3, ο οποίος λειτουργεί με κακόβουλο τρόπο, χρησιμοποιεί την ευκαιρία που προκύπτει από τη σύγκρουση απόψεων των άλλων δύο στρατηγών και τους στέλνει δύο διαφορετικά μηνύματα που περιέχουν μία απόφαση αντίθετη από αυτή που έστειλαν οι ίδιοι, δηλαδή λέει στο Στρατηγό 1 να υποχωρήσει και στον Στρατηγό 2 να επιτεθεί. Ως εκ τούτου, με βάση τα μηνύματα του συστήματος, ο Στρατηγός 1 αποφασίζει να υποχωρήσει και ο Στρατηγός 2 αποφασίζει να επιτεθεί, θεωρώντας ο καθένας ότι έχει επιτευχθεί συναίνεση για αυτήν την απόφαση.



Σχήμα 4-3: Παράδειγμα προβλήματος Βυζαντινών Στρατηγών (Salimitari & Chatterjee, 2018)

Ουσιαστικά, υπάρχουν πολλαπλά ενδεχόμενα, είτε μερικοί από αυτούς τους στρατηγούς είτε οι αγγελιοφόροι τους να είναι προδότες. Εάν οι στρατηγοί είναι προδότες, μπορεί να στείλουν λανθασμένες ή διαφορετικές διαταγές στους άλλους στρατηγούς. Εάν οι αγγελιοφόροι είναι προδότες, θα μπορούσαν σκόπιμα να σαμποτάρουν την αποστολή παρέχοντας λάθος πληροφορίες. Ως αποτέλεσμα, αυτό θα υπονόμευε τελικά τη συνολική απόφαση των έντιμων στρατηγών και έτσι συμπεραίνεται ότι το πρόβλημα των βυζαντινών στρατηγών μπορεί να οριστεί ως το πρόβλημα της επίτευξης συναίνεσης από έντιμους στρατηγούς, όταν υπάρχει παρουσία αρκετών προδοτών. Αυτό το πρόβλημα συνεχίζεται στο διηνεκές, χωρίς κανένας στρατηγός να μπορεί ποτέ να είναι σίγουρος αν το μήνυμα του πέρασε, πόσο μάλλον αν είναι αυθεντικό. Στον κόσμο των υπολογιστών η συνθήκες του προβλήματος μετατρέπονται στο πως μεμονωμένοι χρήστες έχουν τη δυνατότητα να προστατεύουν τα δεδομένα τους από κακόβουλους χρήστες, χωρίς την ύπαρξη κάποιας κεντρικής αρχής. Ουσιαστικά, η λύση που προσφέρει το Blockchain στο πρόβλημα, είναι ότι ένας χρήστης μπορεί να αποθηκεύσει σχεδόν οτιδήποτε σε ένα "ψηφιακό κουτί". Το περιεχόμενο του κουτιού μπορεί να αλλάξει μόνο με ένα μοναδικό ιδιωτικό κλειδί, αλλά είναι κοινοποιημένο στους άλλους χρήστες, χωρίς να έχουν τη δυνατότητα τροποποίησης ή αλλαγής των δεδομένων. Αυτός ο τρόπος λειτουργίας της τεχνολογίας Blockchain θα αναλυθεί στη συνέχεια αυτού του κεφαλαίου.

4.3. Τεχνολογίες σύνθεσης Blockchain

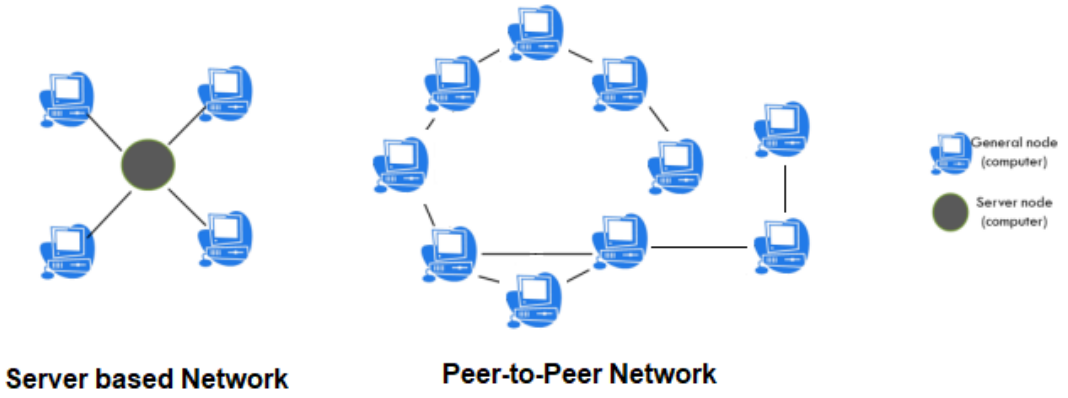
Πολλά από τα στοιχεία που αναφέρονται στις μέρες μας ως Blockchain ήταν γνωστά πριν από τη δημιουργία του Bitcoin, το 2008 (Zachariadis et al., 2019). Το Blockchain βασίζεται στο συνδυασμό πολλών προ-υπαρχουσών τεχνολογιών και εννοιών και έχει δημιουργήσει ουσιαστικά μία νέα αντίληψη για πώς αυτές οι τεχνολογίες μπορούν να συνεργαστούν. Προκειμένου να λειτουργήσει ένα δίκτυο Blockchain στο οποίο θα συναλλάσσονται assets άνευ κεντρικής αρχής, όπως π.χ. κρυπτονομίσματα, είναι απαραίτητο να έχουν καλυφθεί όλα τα ζητήματα ασφαλείας. Για αυτό το λόγο τα κύρια χαρακτηριστικά του Blockchain αποτελούν οι τεχνολογικές λύσεις που καλύπτουν αυτήν την ανάγκη, συμμετέχοντας από κοινού σε ένα ολιστικό πλαίσιο. Τα βασικά ζητήματα που πρέπει να αντιμετωπιστούν είναι η παραποίηση των δεδομένων και η αποφυγή των διπλών καταχωρίσεων, ενώ κρίσιμη είναι και η καλή επιλογή μηχανισμού συναίνεσης, ώστε να αμύνεται επαρκώς το σύστημα, απέναντι σε επιθέσεις από κακόβουλους χρήστες.

Η αρχιτεκτονική δομή των δικτύων Blockchain βασίζεται στα Peer-to-Peer δίκτυα, τα οποία αποτελούν το θεμέλιο λίθο αυτής της τεχνολογίας. Επίσης, όλες οι λειτουργίες του Blockchain, από την επαλήθευση ταυτότητας έως την προσθήκη και επαλήθευση νέων blocks, βασίζονται στην κρυπτογράφηση δεδομένων (Badev & Chen, 2014). Οι τεχνολογίες κρυπτογράφησης που χρησιμοποιούνται, είναι οι συναρτήσεις κατατεμαχισμού (hash functions), η κρυπτογράφηση

δημόσιου κλειδιού (public key cryptography) και η ψηφιακή υπογραφή (digital signature) (Zhai et al., 2019). Οι μηχανισμοί συναίνεσης, που αποτελούν επίσης βασικό χαρακτηριστικό ενός συστήματος Blockchain, θα αναλυθούν εκτενώς στο επόμενο κεφάλαιο. Συνολικά, το τεχνολογικό πλαίσιο που δημιουργείται από τη συνεργασία αυτών των τεχνολογιών καθιστά το Blockchain έναν εξαιρετικά ασφαλή τρόπο για την κατασκευή αποκεντρωμένων δικτύων ανταλλαγής πληροφοριών.

4.3.1. Peer-to-Peer Δίκτυα

Σε ένα τυπικό δίκτυο υπάρχουν δύο θέσεις για τους χρήστες. Η μία θέση είναι ο κεντρικός διακομιστής (server), ο οποίος αναλαμβάνει την αποθήκευση και σωστή διατήρηση των δεδομένων και την παροχή τους προς το υπόλοιπο δίκτυο. Η δεύτερη θέση στο δίκτυο είναι ο πελάτης (clients), ο οποίος ζητά από το server τα δεδομένα και αποκτά πρόσβαση σε αυτά. Με αυτό τον τρόπο οι ρόλοι κάθε χρήστη είναι προκαθορισμένοι και αμετάβλητοι. Αντίθετα, στα δίκτυα Peer-to-Peer, όλοι οι συμμετέχοντες κόμβοι του δικτύου είναι σε θέση τόσο να διατηρούν όσο και να ζητούν δεδομένα και δημιουργούν ένα αυτόνομο δίκτυο όπου γίνεται ανταλλαγή δεδομένων μεταξύ των κόμβων του. Σε ένα τέτοιο δίκτυο, οι ρόλοι του server και του client δεν είναι σταθεροί, αλλά εναλλάσσονται μεταξύ των κόμβων ανάλογα με την εκτελούμενη μεταφορά δεδομένων. Επίσης, παρόλο που οι κόμβοι είναι συνδεδεμένοι με τουλάχιστον έναν ακόμα κόμβο, κανένας κόμβος δεν συνδέεται απευθείας με όλους τους υπόλοιπους και άρα δεν μπορεί να ελέγχει το σύστημα (Drescher, 2017). Σύγκριση της οπτικής αποτύπωσης των δύο δικτύων παρουσιάζεται στο ***Σχήμα 4-4***.



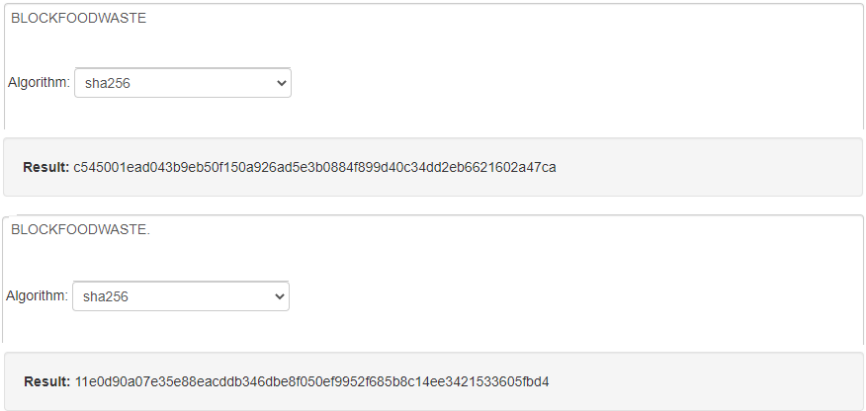
Σχήμα 4-4: Δίκτυο που βασίζεται σε διακομιστή και Peer-to Peer δίκτυο

Το Blockchain βασίζει ένα μέρος της φήμης του στην αξιοπιστία των δικτύων Peer-to-Peer, καθώς μέσω αυτών, το συνολικό καθολικό του διανέμεται και αναπαράγεται σε κάθε κόμβο, με αποτέλεσμα, εάν ένας ή περισσότεροι από αυτοί έχουν τεθούν εκτός σύνδεσης, η ακεραιότητα των δεδομένων να εξακολουθεί να διατηρείται. Για τη λειτουργία ενός Peer-to-

Peer δικτύου είναι απαραίτητο να εξετάζονται οι μέθοδοι αναζήτησης και μετάδοσης των δεδομένων. Οι μέθοδοι αναζήτησης είναι τα μέσα για τη διαχείριση των θέσεων των κόμβων και οι μέθοδοι μετάδοσης είναι τα μέσα μετάδοσης των δεδομένων μεταξύ των κόμβων. Η μετάδοση μπορεί να είναι άμεση μεταξύ δύο κόμβων ή αναμεταδιδόμενη, δηλαδή να εξελίσσεται με τη χρήση επιπλέον κόμβων εκτός του αποστολέα (server) και του παραλήπτη (client). Ένα πλεονέκτημα των Peer-to-Peer δικτύων είναι ότι μπορούν εύκολα να τροποποιηθούν, καθώς νέοι κόμβοι μπορούν να προστεθούν ή να εξαλειφθούν χωρίς μεγάλη προσπάθεια (Fridgen et al., 2019).

4.3.2. Συναρτήσεις κατατεμαχισμού (Hash functions)

Η τεχνολογία blockchain βασίζεται εκτενώς στις συναρτήσεις κατατεμαχισμού (ή κατακερματισμού), που είναι ευρέως γνωστές ως hash functions. Μία συνάρτηση κατατεμαχισμού είναι μία μη αμφίδρομη μαθηματική συνάρτηση που λαμβάνει στην είσοδο της δεδομένα και παράγει μία τιμή σταθερού μήκους, γνωστή ως τιμή κατατεμαχισμού. Ως hash περιγράφεται το αποτέλεσμα του μετασχηματισμού των αρχικών πληροφοριών που χρησιμοποιήθηκαν στην είσοδο. Η ίδια είσοδος θα αποδίδει πάντα την ίδια τιμή κατακερματισμού, επομένως η συνάρτηση είναι ντετερμινιστική (Badev & Chen, 2014). Με τη χρήση αυτών των συναρτήσεων, μπορεί να μετατραπεί ένα απροσδιόριστου μεγέθους απλό κείμενο σε ένα hash σταθερού μεγέθους (Franco, 2014). Μια μικρή αλλαγή στην είσοδο, όπως η αλλαγή ενός μόνο χαρακτήρα, θα έχει ως αποτέλεσμα μια εντελώς διαφορετική τιμή hash στην έξοδο. Όπως φαίνεται στο ***Σχήμα 4-5***, όπου χρησιμοποιήθηκε ένα ελεύθερης χρήσης online εργαλείο, η προσθήκη μίας μόνο τελείας αλλάζει ολόκληρο το hash της εξόδου. Το κύριο χαρακτηριστικό της συνάρτησης κατατεμαχισμού είναι ότι, ενώ είναι απλό να υπολογιστεί η τιμή που θα προκύψει στην έξοδο, είναι εξαιρετικά δύσκολο να αναδημιουργηθούν τα δεδομένα εισόδου από την τιμή δηλαδή που έλαβαν μετά το μετασχηματισμό τους.



Σχήμα 4-5: Παράδειγμα χρήσης συνάρτησης hash (www.tools4noobs.com/online_tools/hash)

Αξιοποιώντας αυτά τα χαρακτηριστικά, ο μηχανισμός αυτός χρησιμοποιείται για την παροχή ψηφιακού δακτυλικού αποτυπώματος δεδομένων, τη διασφάλιση της ακεραιότητας αρχείων και κωδικών πρόσβασης και την ανίχνευση της παραποίησης τους. Γνωστοί αλγόριθμοι κατατεμαχισμού είναι ο Message Digest (MD) και ο Secure Hash Algorithm (SHA). Στο παράδειγμα του ***Σχήματος 4-5***, έχει επιλεγεί η μορφή SHA256, που χρησιμοποιείται και από το Bitcoin.

4.3.3. Κρυπτογράφηση δημόσιου κλειδιού (Public key cryptography)

Η κρυπτογράφηση κλειδιών είναι μια κρυπτογραφική μέθοδος που χρησιμοποιεί κλειδιά για τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης. Υπάρχουν δύο κύρια είδη κρυπτογράφησης που χρησιμοποιούνται στο διαδίκτυο, η κρυπτογράφηση μυστικού κλειδιού (secret key cryptography) και η κρυπτογράφηση δημόσιου κλειδιού (public key cryptography). Η ονομασία των μεθόδων μπορεί να βρεθεί και ως συμμετρικού ή ασύμμετρου κλειδιού αντίστοιχα.

Στην πρώτη κατηγορία χρησιμοποιείται ένα μόνο κλειδί, δηλαδή για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων χρησιμοποιείται το ίδιο κοινόχρηστο κλειδί, τόσο από τον αποστολέα όσο και από τον παραλήπτη. Το πιο γνωστό πρότυπο κρυπτογράφησης που βασίζεται στην κρυπτογράφηση μυστικού κλειδιού είναι το Advanced Encryption Standard (AES) που αναπτύχθηκε από την κυβέρνηση των ΗΠΑ το 2001, ως εξέλιξη του Data Encryption Standard (DES) που είχε σχεδιαστεί τη δεκαετία του 1970 από την IBM (Nechvatal et al., 2001). Η πρόκληση σε αυτόν τον τύπο κρυπτογράφησης, όπου χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση, είναι ότι απαιτούνται μέτρα ασφαλείας για τη διανομή του κλειδιού μεταξύ αποστολέα και παραλήπτη, όπως η επικοινωνία μεταξύ ενός ασφαλούς καναλιού πριν από την πραγματοποίηση μίας κρυπτογραφικής μετάδοσης.

Για να αποφευχθεί η ανάγκη διαμοιρασμού κλειδιών μεταξύ χρηστών, χρησιμοποιείται η κρυπτογράφηση δημόσιου κλειδιού. Σε αυτήν την κατηγορία κρυπτογράφησης χρησιμοποιούνται δύο κλειδιά, ένα ιδιωτικό (private key) που πρέπει να διατηρείται μυστικό από τον κάτοχο του και ένα δημόσιο (public key) που μπορεί να διανεμηθεί ελεύθερα σε οποιονδήποτε (Franco, 2014). Μεταξύ των δύο κλειδιών υπάρχει μαθηματική συσχέτιση και η γνώση ενός από τα κλειδιά δεν επιτρέπει σε κάποιον να προσδιορίσει εύκολα το άλλο. Το ένα κλειδί χρησιμοποιείται για την κρυπτογράφηση και το άλλο κλειδί για την αποκρυπτογράφηση των δεδομένων, χωρίς να υπάρχει περιορισμός σχετικά με το ποιο κλειδί εφαρμόζεται πρώτο.

Η κρυπτογράφηση δημόσιου κλειδιού περιεγράφηκε για πρώτη φορά από τους Hellman & Diffie (1976) και μία εφαρμογή της είναι το σύστημα κρυπτογράφησης RSA, που πήρε το όνομα του από του δημιουργούς του (Rivest et al., 1978), και χρησιμοποιείται από πολλά προϊόντα

λογισμικού για ανταλλαγή κλειδιών, ψηφιακές υπογραφές και κρυπτογράφηση πακέτων δεδομένων. Η μέθοδος επιτρέπει την ασφαλή παράδοση και παραλαβή αρχείων, μόνο στην περίπτωση που ένας χρήστης προετοιμάσει ένα ζεύγος ιδιωτικού και δημόσιου κλειδιού και παραδώσει εκ των προτέρων το δημόσιο κλειδί στον άλλο χρήστη. Έτσι, η ασφάλεια διατηρείται ακόμη και αν άλλα άτομα χρησιμοποιούν το ίδιο δημόσιο κλειδί, αρκεί ο χρήστης να διαχειρίζεται σωστά το ιδιωτικό του κλειδί. Σε αυτή τη λογική βασίζεται και ο ασύμμετρος μηχανισμός κρυπτογράφησης για την επικύρωση του ελέγχου της ταυτότητας των συναλλαγών, που χρησιμοποιεί το Blockchain.

4.3.4. Ψηφιακή υπογραφή (Digital signature)

Είναι σύνηθες στον φυσικό κόσμο να χρησιμοποιούνται χειρόγραφες υπογραφές σε συμβατικά έγγραφα, έτσι ώστε να δεσμεύεται το άτομο που υπογράφει σε αυτά που αναφέρει το έγγραφο. Αντίστοιχα, η ψηφιακή υπογραφή είναι μία μέθοδος που συνδέει ένα άτομο με ψηφιακά δεδομένα και η δέσμευση του αντίστοιχα, μπορεί να επαληθευτεί από οποιοδήποτε άλλο μέρος έχει πρόσβαση στο ψηφιακό έγγραφο. Αποτελεί ένα μηχανισμό που χρησιμοποιείται για την απόδειξη της αυθεντικότητας των δεδομένων που αποστέλλονται μέσω ενός δικτύου χρησιμοποιώντας ένα ζεύγος κλειδιών όπως στην περίπτωση της κρυπτογράφησης δημόσιου κλειδιού.

Για ξεκινήσει η διαδικασία της ψηφιακής υπογραφής, το άτομο που θέλει να τοποθετήσει την υπογραφή μεταβιβάζει τα ψηφιακά δεδομένα σε μια συνάρτηση κατατεμαχισμού και παράγει μία τιμή hash για τα δεδομένα που θέλει να υπογράψει. Η τιμή αυτή, μεταβιβάζεται ως input στον αλγόριθμο υπογραφής μαζί με το ιδιωτικό κλειδί του ατόμου και ο αλγόριθμος δημιουργεί την ψηφιακή υπογραφή, κρυπτογραφώντας την τιμή hash που παράχθηκε. Η ψηφιακή υπογραφή επισυνάπτεται στα δεδομένα και αποστέλλεται στον παραλήπτη των υπογεγραμμένων εγγράφων, ο οποίος χρησιμοποιεί την ίδια συνάρτηση hash με τον αποστολέα για να δημιουργήσει μόνος του την τιμή hash των ψηφιακών δεδομένων. Στη συνέχεια χρησιμοποιεί την ψηφιακή υπογραφή ως input στον αλγόριθμο επαλήθευσης μαζί με το δημόσιο κλειδί του ατόμου που υπογράφει, και ο αλγόριθμος επαλήθευσης παράγει ένα output. Η επαλήθευση της γνησιότητας της υπογραφής εξαρτάται από τη σύγκριση της τιμής hash που δημιούργησε με την τιμή που λαμβάνεται μέσω της αποκρυπτογράφησης της ψηφιακής υπογραφής, οι οποίες θα πρέπει να ταυτίζονται. Αυτό έχει ως αποτέλεσμα την επιβεβαίωση ότι η ψηφιακή υπογραφή του αποστολέα είναι αυθεντική. Η ψηφιακή υπογραφή διασφαλίζει ότι το μήνυμα προέρχεται από τον αποστολέα, ο αποστολέας δεν μπορεί να αρνηθεί ότι το έστειλε και επίσης διασφαλίζει ότι δεν έχει αλλοιωθεί (Böhme et al., 2015).

Από την περιγραφή των βημάτων της διαδικασίας, είναι αντιληπτό, ότι η ψηφιακή υπογραφή δε συνδέθηκε με τα δεδομένα, αλλά δημιουργήθηκε ένα hash για αυτά, το οποίο

χρησιμοποιήθηκε στον αλγόριθμο ψηφιακής υπογραφής. Αυτό συμβαίνει για λόγους αποτελεσματικότητας, καθώς τα προς υπογραφή δεδομένα, μπορούν να αποκτήσουν αρκετά μεγάλο όγκο και η χρήση τους στον αλγόριθμο θα μπορούσε να αποδειχθεί υπολογιστικά χρονοβόρα, άρα η διαδικασία θα να είναι αργή και ακριβή. Αντίθετα, οι τιμές hash είναι μικρές και ταυτόχρονα εγγυώνται την ακεραιότητα των δεδομένων. Έτσι, η κρυπτογράφηση ενός hash είναι πολύ πιο αποτελεσματική από την κρυπτογράφηση των αρχικών δεδομένων.

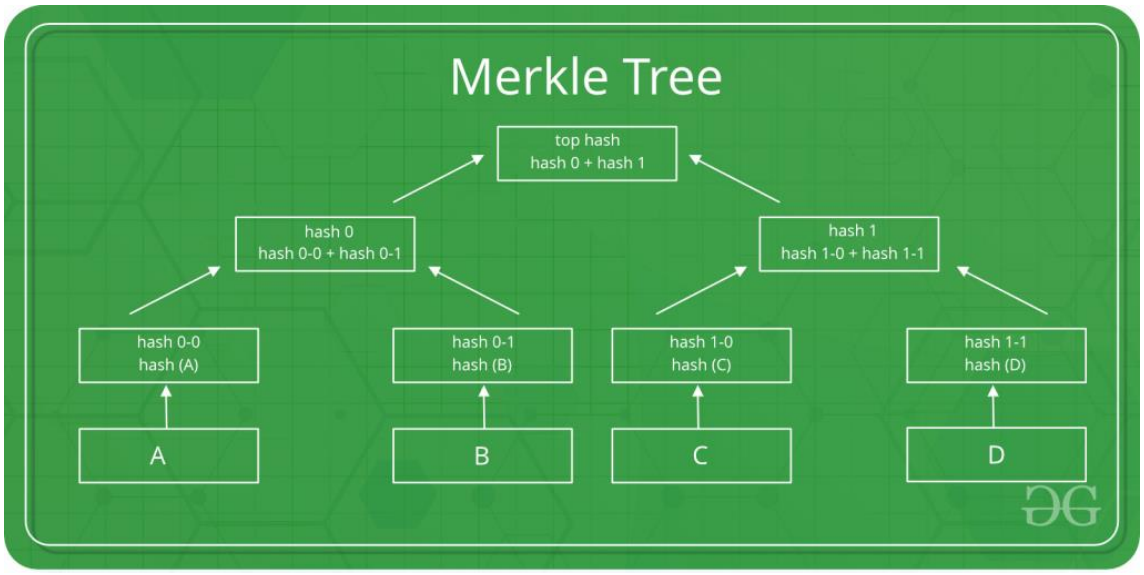
Στην τεχνολογία Blockchain μία τυπική ψηφιακή υπογραφή εμπλέκεται σε δύο φάσεις: τη φάση υπογραφής και τη φάση επαλήθευσης, που είναι ουσιαστικά οι δύο φάσεις που περιεγράφηκαν παραπάνω. Για τις ανάγκες ενός δικτύου Blockchain, μεταξύ άλλων αλγορίθμων, χρησιμοποιείται ο αλγόριθμος ψηφιακής υπογραφής Elliptic Curve Digital Signature (ECDSA). Είναι άξιο αναφοράς ότι ψηφιακή υπογραφή μπορούν να δημιουργηθούν όχι μόνο από άτομα αλλά και από άλλους συμμετέχοντες στο δίκτυο, όπως οχήματα ή μηχανήματα (Fridgen et al., 2019).

4.4. Λειτουργία Blockchain

Η τεχνολογία Blockchain παρουσιάστηκε για τη δημιουργία του κρυπτονομίσματος Bitcoin (Nakamoto, 2008), ωστόσο ένα δίκτυο Blockchain δεν απαιτεί ένα κρυπτονόμισμα για να υπάρχει και να λειτουργεί (Greenspan, 2015). Η δημοσίευση του Nakamoto καθόρισε την αρχιτεκτονική δομή του Blockchain, ως ένα δίκτυο Peer-to-Peer που υποστηρίζει τη λειτουργία ενός συστήματος ηλεκτρονικών συναλλαγών που λύνει το πρόβλημα του double spending, χωρίς να βασίζεται στην εμπιστοσύνη μεταξύ των κόμβων. Για να το πετύχει χρησιμοποιεί ψηφιακές υπογραφές μαζί με έναν μηχανισμό συναίνεσης και παρέχει κίνητρα (ανταμοιβές) στους συμμετέχοντες χρήστες. Ο τρόπος με τον οποίο το δίκτυο οδηγείται στη συναίνεση, του δίνει τη δυνατότητα να διατηρεί αποθηκευμένο και ενημερωμένο ένα έγκυρο καθολικό συναλλαγών, ιδιοκτησίας ή δικαιωμάτων για οποιοδήποτε asset και οποιαδήποτε εφαρμογή. Όλα τα δεδομένα που καταγράφονται στο Blockchain ομαδοποιούνται σε blocks με και υπάρχει πάντα χρονική σήμανση για την καταγραφή τους. Τα blocks αυτά, εκτός από το πλήθος δεδομένων (π.χ. δεδομένα συναλλαγών μεταξύ χρηστών), περιλαμβάνουν επίσης και ορισμένες ακόμα σημαντικές πληροφορίες, οι οποίες είναι απαραίτητες για την πλήρη χρήση των ειδικών χαρακτηριστικών που παρέχει η τεχνολογία, κατά τη λειτουργία της.

Για τη διαχείριση των δεδομένων συναλλαγών, το Blockchain χρησιμοποιεί τη μορφή δόμησης δεδομένων των Merkle trees, που είναι επίσης γνωστά ως hash trees (***Σχήμα 4-6***). Με τη λειτουργία των Merkle trees το Blockchain αποθηκεύει τις συναλλαγές σε μια δυαδική δεντρική μορφή και δημιουργεί μία τελική τιμή hash σε κάθε block. Κάθε κόμβος (leaf) του Merkle tree αποθηκεύει την τιμή hash των συναλλαγών που περιέχει και το leaf του επόμενο επιπέδου,

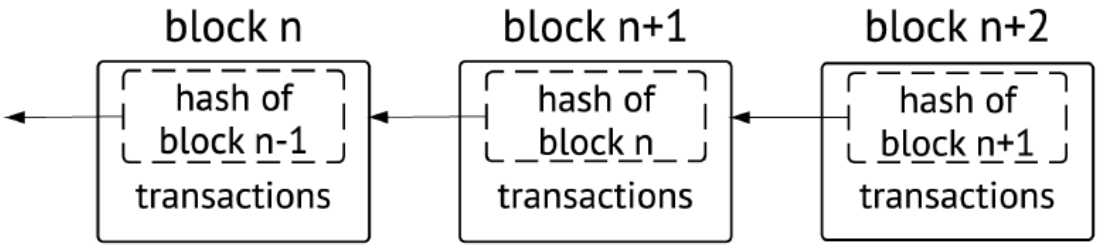
περιέχει την τιμή hash των προηγούμενων τιμών hash που παράχθηκαν, φτάνοντας έτσι στη ρίζα του δέντρου που ονομάζεται Merkle root. Συνεπώς με τη χρήση των συναρτήσεων hash, η δομή Merkle tree μπορεί να αποθηκεύσει μεγάλα σύνολα δεδομένων, τα οποία μπορούν αποτελεσματικά να συνοψιστούν και να επαληθευτούν, άρα μειώνει το κόστος μετάδοσης δεδομένων και υπολογιστικών πόρων (Bamakan et al., 2020).



Σχήμα 4-6: Αρχιτεκτονική Merkle tree (Geeksforgeeks, 2022)

4.4.1. Δομή blocks

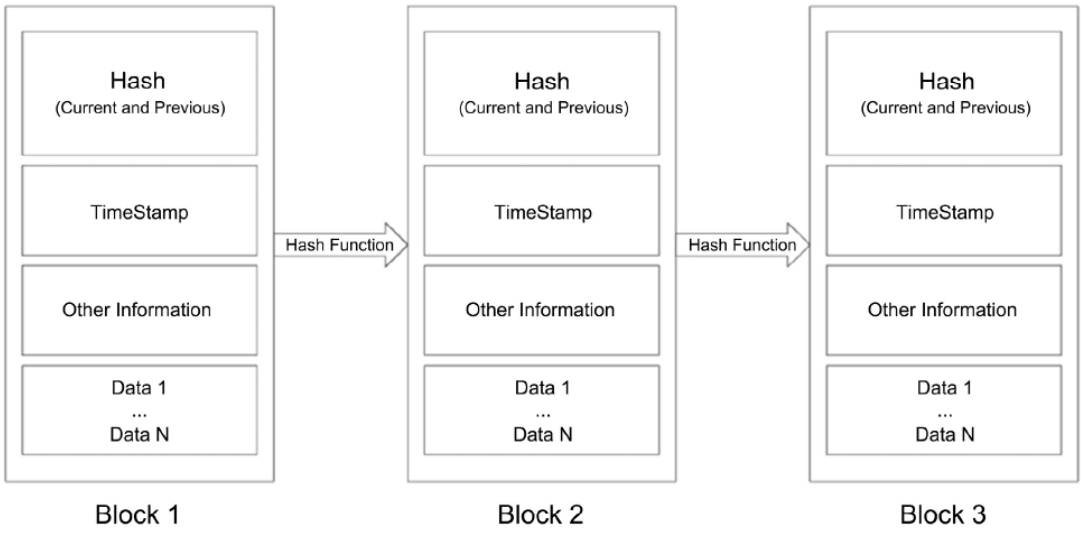
Το βασικό δομικό στοιχείο της αρχιτεκτονικής του Blockchain είναι τα blocks, τα οποία αναγνωρίζονται από την τιμή hash που διαθέτουν. Τα blocks σχηματίζουν μία ακολουθία, δηλαδή κάθε block της αλυσίδας οδηγεί στο αμέσως προηγούμενο του, μέσω της αναφοράς και της τιμής hash, του προηγούμενο block (***Σχήμα 4-7***). Το προηγούμενο block ονομάζεται "parent block", ενώ το πρώτο block της αλυσίδας, το οποίο όπως είναι φυσικό δεν έχει parent block, ονομάζεται "genesis block" και η τιμή hash πριν από αυτό είναι ίση με μηδέν. Έτσι δημιουργείται η συνδεσμολογία της αλυσιδωτής back-linked συσχέτισης μεταξύ των blocks (Antonopoulos, 2014). Οποιοσδήποτε κόμβος με πρόσβαση σε αυτήν την αλυσίδα πληροφοριών μπορεί να διαβάσει τα δεδομένα και να ανατρέξει στη σειρά των γεγονότων, έχοντας πρόσβαση έτσι στην πλήρη εικόνα των ανταλλασσόμενων πληροφοριών του δικτύου από την αρχή της ύπαρξης του, δηλαδή από το "genesis block".



Σχήμα 4-7: Σύνδεση των blocks με την τιμή hash (Christidis & Devetsikiotis, 2016)

Ο τρόπος με τον οποίο είναι δομημένο κάθε μπλοκ αντικατοπτρίζει την ακεραιότητα αυτού του τύπου αποθήκευσης δεδομένων. Ανάλογα με το σχεδιασμό του δικτύου Blockchain, οι λεπτομέρειες που περιλαμβάνει ένα block ενδέχεται να διαφέρουν. Μια γενική δομή μπορεί να απεικονιστεί στο ***Σχήμα 4-8***. Ένα block αποτελείται από δύο μέρη, την κεφαλίδα (block header) και το κυρίως σώμα (block body). Η κεφαλίδα του block αποτελείται από τις βασικές πληροφορίες, πάνω στις οποίες βασίζεται η λειτουργία της τεχνολογίας του Blockchain. Μία κεφαλίδα συνήθως αποτελείται από το "Block version" το οποίο περιέχει τους κανόνες επικύρωσης που ακολουθεί το block, το "Parent block hash" που είναι η τιμή hash μεγέθους 256-bit που υποδεικνύει το προηγούμενο block της αλυσίδας και το "Merkle tree root hash", δηλαδή την τιμή hash όλων το συναλλαγών του block, που αποτελεί το "δακτυλικό αποτύπωμα" του block. Επίσης, η κεφαλίδα περιέχει το "Timestamp", που είναι η τρέχουσα χρονοσήμανση του block με μορφή δευτερολέπτων με έναρξη την ώρα 00:00 της 01/01/1970, το "Nonce", δηλαδή ένα πεδίο μεγέθους 4 bytes, το οποίο συνήθως αρχίζει με 0 και αυξάνεται σε κάθε υπολογισμό hash και το "nBits" που είναι ο τρέχων στόχος hash σε συμπαγή μορφή.

Από την άλλη πλευρά, το κυρίως σώμα του block αποτελείται από έναν μετρητή συναλλαγών και τις καταγεγραμμένες συναλλαγές σε αυτό, που κωδικοποιούνται σε ένα Merkle tree. Ο μέγιστος αριθμός συναλλαγών που μπορεί να περιέχει ένα block εξαρτάται από το μέγεθος του block και το μέγεθος της κάθε συναλλαγής (Zheng et al., 2018). Κάθε block μπορεί να περιέχει χιλιάδες συναλλαγές που κωδικοποιούνται από συνάρτηση hash, πριν από τη μετάδοση τους στο υπόλοιπο δίκτυο (Bamakan et al., 2020). Όπως αναφέρθηκε σε προηγούμενη ενότητα, οι συναρτήσεις hash που χρησιμοποιούνται, διατηρούν την ακεραιότητα των δεδομένων διατηρώντας παράλληλα το εξαγόμενο output σε σταθερό μήκος. Οποιαδήποτε αλλαγή σε οποιοδήποτε μέρος ενός block θα είχε ως αποτέλεσμα να προκληθούν αλλαγές στην τιμή hash του και κατά συνέπεια, θα το καταστήσει άκυρο για τα επόμενα blocks και ολόκληρη την αλυσίδα (Solanki, 2021).



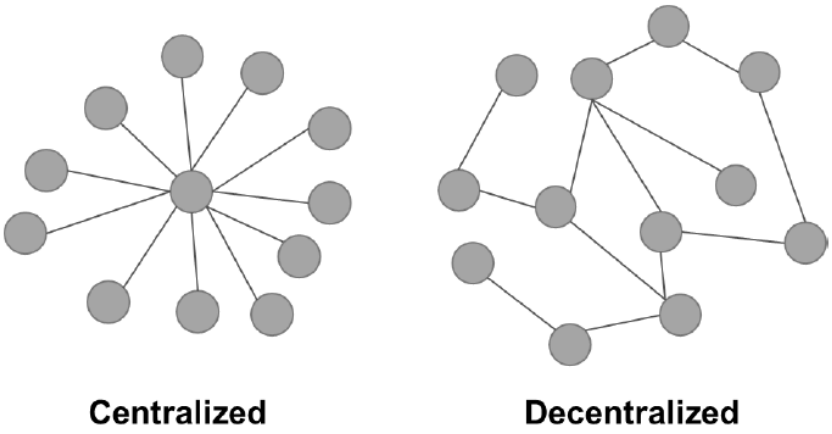
Σχήμα 4-8: Περιεχόμενα blocks στην αλυσίδα Blockchain (Joshi et al., 2018)

4.4.2. Δημιουργία blocks

Η λειτουργία του δικτύου Blockchain βασίζεται στο σύνολο χρηστών – κόμβων (nodes) που μετέχουν σε αυτό. Κάθε ένας από αυτούς διατηρεί και λειτουργεί στον τοπικό του σκληρό δίσκο ένα αντίγραφο του καθολικού του Blockchain, καθιστώντας έτσι το δίκτυο αποκεντρωμένο. Κάθε χρήστης συναλλάσσεται με το υπόλοιπο δίκτυο μέσω του δικού του κόμβου, χωρίς όμως αυτό να είναι δεσμευτικό, καθώς ένας κόμβος μπορεί να λειτουργήσει ως input πληροφοριών για περισσότερους από έναν χρήστες (Christidis & Devetsikiotis, 2016). Οι κόμβοι λοιπόν του δικτύου σχηματίζουν ένα Peer-to-Peer δίκτυο όπου, όπου χρήστες χρησιμοποιούν ένα ζεύγος ιδιωτικού και δημόσιου κλειδιού. Όπως αναφέρθηκε για τη διαδικασία κρυπτογράφησης στην προηγούμενη ενότητα, με το ιδιωτικό κλειδί υπογράφουν τις συναλλαγές τους και με τη χρήση του δημόσιου κλειδιού, οι άλλοι κόμβοι μπορούν να τις επικυρώσουν. Η χρήση ασύμμετρης κρυπτογράφησης δημόσιου κλειδιού παίζει τον καθοριστικότερο ρόλο για τη διαβεβαίωση της ακεραιότητα τους δικτύου.

Κάθε συμμετέχων κόμβος μπορεί να υποβάλει συναλλαγές στο δίκτυο Blockchain. Κάθε υπογεγραμμένη συναλλαγή μεταδίδεται από τον κόμβο του ενός χρήστη στους κοντινούς σε αυτόν (peers) που βρίσκονται σε απόσταση ενός hop, όπου hop είναι ο αριθμός πακέτων δεδομένων που πρέπει να μεταφερθούν για την ολοκληρωμένη μεταβίβαση μίας πληροφορίας από έναν κόμβο προς έναν άλλο, σε ένα Peer-to-Peer δίκτυο (Huang et al., 2021). Κάθε κόμβος επικοινωνεί άμεσα μόνο με λίγους κόμβους και έμμεσα με τους όλους υπόλοιπους, όπως αποτυπώνεται στο ***Σχήμα 4-9*** και έτσι είναι πιο εύκολο να προστατευθεί το σύστημα από διάχυση κακόβουλων ενεργειών, σε σχέση με ένα δίκτυο όπου υπάρχει μία κεντρική αρχή. Οι

γειτονικοί κόμβοι που θα λάβουν τα δεδομένα βεβαιώνουν ότι αυτή η εισερχόμενη συναλλαγή είναι έγκυρη πριν την μεταδώσουν στους υπόλοιπους κόμβους και κατανεμηθεί τελικά σε όλο το δίκτυο. Για να είναι μία συναλλαγή έγκυρη και να υπάρχει κοινή άποψη για το καθολικό του δικτύου, κάθε δίκτυο Blockchain έχει ορισμένους κανόνες και με βάση αυτούς, οι κόμβοι χρησιμοποιούν την κρυπτογράφηση δημόσιου κλειδιού και αποφασίζουν εάν μια εισερχόμενη συναλλαγή είναι έγκυρη και, κατά συνέπεια, εάν πρέπει να μεταδοθεί στο υπόλοιπο δίκτυο ή όχι. Οι κόμβοι δεν χρειάζεται να εμπιστεύονται καμία άλλη οντότητα, αντίθετα η εμπιστοσύνη επιτυγχάνεται από τις αλληλεπιδράσεις των διαφορετικών συμμετεχόντων στο σύστημα (Antonopoulos, 2014). Οι μη έγκυρες συναλλαγές, που δε θα επιβεβαιωθούν μέσω της κρυπτογράφησης δημόσιου κλειδιού, θα απορριφθούν και δε θα προχωρήσουν προς τους υπόλοιπους κόμβους.

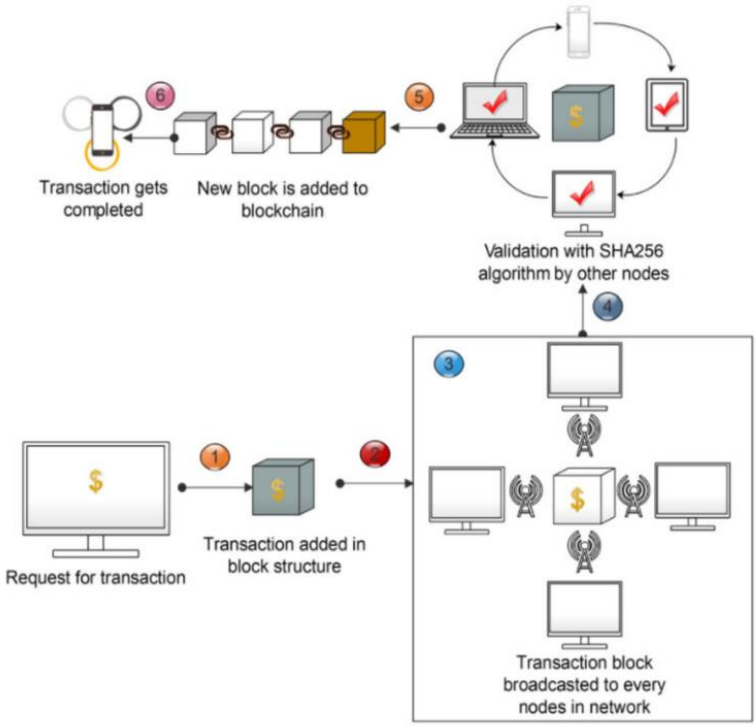


Σχήμα 4-9: Επικοινωνία κόμβων σε Centralized και Decentrilized (Peer-to-Peer) δίκτυα

Οι συναλλαγές που έχουν συλλεχθεί από το δίκτυο χρησιμοποιώντας την παραπάνω διαδικασία κατά τη διάρκεια ενός συμφωνημένου χρονικού διαστήματος, ενοποιούνται σε ένα υπό δημιουργία block με χρονική σήμανση. Σε αυτό το σημείο, ξεκινάει η διαδικασία της "εξόρυξης" (mining), όπου καθορίζεται ο κόμβος, ο οποίος θα επικυρώσει το block και θα το μεταδώσει στο υπόλοιπο δίκτυο. Το mining είναι μέρος της διαδικασίας ασφάλειας του Blockchain και δημιουργεί ένα ανταγωνιστικό περιβάλλον όπου όλοι οι κόμβοι που μετέχουν στη διαδικασία (miners) προσπαθούν να επικυρώσουν δεδομένα και να ελέγξουν ότι όλοι οι άλλοι που έχουν εξορύξει ένα block το έχουν κάνει σωστά. Για να διατηρείται αυτός ο ανταγωνισμός μεταξύ των miners, που καθιστά το δίκτυο ασφαλές, οι miners ανταμείβονται για την προσπάθεια τους, κερδίζουν δηλαδή μία επιβράβευση (reward) από το δίκτυο. Ταυτόχρονα, σε κάποιες περιπτώσεις υπάρχουν τέλη για τους κόμβους που θέλουν να καταχωρήσουν συναλλαγές στο δίκτυο, τα οποία επίσης δίνονται ως ανταμοιβή στους miners.

Συνοπτικά, προκειμένου το δίκτυο να λειτουργεί με αξιοπιστία, η διαδικασία πρέπει να δημιουργεί αρκετά κίνητρα για την προσέλκυση miners και οι παραπάνω ανταμοιβές αυτές λειτουργούν ως τέτοια, με το Blockchain να τα διανέμει χρησιμοποιώντας το υποκείμενο κρυπτονόμισμα του δικτύου (Sompolinsky & Zohar, 2017).

Η διαδικασία του mining, ο τρόπος επιλογής του κόμβου – επικυρωτή και η ανταμοιβή που λαμβάνει αυτός, διαφέρει ανάλογα το μηχανισμό συναίνεσης που χρησιμοποιεί το δίκτυο Blockchain, και αυτό θα περιγραφεί αναλυτικότερα στο επόμενο κεφάλαιο. Οι κόμβοι που θα λάβουν τη μετάδοση του επικυρωμένου block, επαληθεύουν ότι το προτεινόμενο block περιέχει έγκυρες συναλλαγές και ότι είναι έγκυρη η τιμή hash που οδηγεί στο parent block του, δηλαδή η τιμή που το ενώνει με την υπόλοιπη αλυσίδα. Εάν συμβαίνει αυτό, προσθέτουν το μπλοκ στην αλυσίδα τους και εφαρμόζουν τις συναλλαγές που περιέχει για να ενημερώσουν το καθολικό του Blockchain που διατηρούν στον τοπικό τους δίσκο. Σε αντίθετη περίπτωση, το προτεινόμενο block απορρίπτεται. Η παραπάνω διαδικασία είναι επαναλαμβανόμενη, καθώς νέα blocks παράγονται συνεχώς στο κατανεμημένο δίκτυο, και η διαδικασία ξεκινάει από την αρχή για κάθε προτεινόμενο block, που περιέχει νέες πληροφορίες. Οπτικοποίηση της παραπάνω διαδικασίας επικύρωσης συναλλαγών, παρουσιάζεται στο ***Σχήμα 4-10***.



Σχήμα 4-10: Συναλλαγή στο δίκτυο Blockchain (Bodkhe et al., 2020)

4.5. Ταξινόμηση δικτύων Blockchain

Τα δίκτυα Blockchain ταξινομούνται ανάλογα το αν δίνουν ελεύθερη δυνατότητα συμμετοχής σε όλους ή αν απαιτούνται άδειες για τη συμμετοχή των χρηστών σε αυτά. Χωρίζονται ουσιαστικά σε τρεις κατηγορίες, τα δημόσια (Public Blockchain), τα ιδιωτικά (Private Blockchain) και τα κοινοπρακτικά (Consortium Blockchain), τα οποία αποτελούν μία μίξη χαρακτηριστικών των άλλων δύο (Korpela et al., 2017). Ουσιαστικά, η έννοια του ιδιωτικών δικτύων εμφανίστηκε με τη δημιουργία του δικτύου Blockchain του Ethereum (Buterin, 2014), από το δημιουργό του Vitalik Buterin, όταν και έγινε ο διαχωρισμός μεταξύ των δημόσιων και ιδιωτικών δικτύων.

4.5.1. Public Blockchain (Δημόσιο)

Ένα δημόσιο δίκτυο Blockchain είναι πλήρως ανοιχτό καθολικό και δεν έχει περιορισμούς όσον αφορά τα δικαιώματα ανάγνωσης εγγραφής και επεξεργασίας. Οποιοσδήποτε μπορεί να συνδεθεί στο δίκτυο και να αποκτήσει πρόσβαση στα δεδομένα και έχει τη δυνατότητα να προσθέσει νέα ή να επεξεργαστεί τα ήδη υπάρχοντα. Επίσης έχει το δικαίωμα να συμμετάσχει στο πρωτόκολλο συναίνεσης, να επαληθεύσει τα blocks που προστέθηκαν πρόσφατα και να διασφαλίσει ότι δεν έρχεται σε σύγκρουση με προηγούμενα blocks στην αλυσίδα. Κάθε χρήστης μπορεί να διαβάσει τις συναλλαγές στο αναλυτικό καθολικό του συστήματος, οι οποίες συναλλαγές είναι διαφανείς, αλλά ανώνυμες.

Ένα δημόσιο δίκτυο Blockchain είναι υποχρεωμένο να λειτουργεί χωρίς την απαίτηση εμπιστοσύνης μεταξύ των χρηστών και συνεπώς είναι πλήρως αποκεντρωμένο (Korpela et al., 2017). Άρα, αυτός ο τύπος Blockchain είναι ασφαλής λόγω του είδους του μηχανισμού συναίνεσης που είναι απαραίτητο να διαθέτει (π.χ. Proof of Work, Proof of Stake κ.ά.), ο οποίος θα πρέπει να εξασφαλίζει τη συμφωνία μεταξύ των κόμβων του συστήματος, προκειμένου να λειτουργεί το δίκτυο (Yusoff et al., 2022). Τα πιο γνωστά δημόσια Blockchain είναι αυτά του Bitcoin και Ethereum.

4.5.2. Private Blockchain (Ιδιωτικό)

Ένα ιδιωτικό Blockchain έχει περιορισμούς στα δικαιώματα ανάγνωσης και εγγραφής δεδομένων και ελέγχεται πιο αυστηρά από ένα δημόσιο δίκτυο. Το δικαίωμα τροποποίησης, προσθήκης ή ανάγνωσης πληροφοριών περιορίζεται και διατηρείται συγκεντρωμένο μόνο σε μία ομάδα συμμετεχόντων, οι οποίοι μπορούν να αποτελούν π.χ. τα μέλη ενός οργανισμού. Σε ένα ιδιωτικό δίκτυο Blockchain, το πόσο ισχυρό είναι το πρωτόκολλο συναίνεσης δεν είναι καθοριστικής σημασίας λόγω της αξιοπιστίας των συμμετεχόντων κόμβων. Τα ιδιωτικά καθολικά έχουν τη δυνατότητα γρήγορης πρόσβασης σε πληροφορίες, κάνουν τις συναλλαγές φθηνότερες και έχουν καλύτερες δυνατότητες ελέγχου του επιπέδου του απορρήτου. Τα

ιδιωτικά δίκτυα Blockchain είναι χρήσιμα για την κάλυψη εσωτερικών αναγκών ενός οργανισμού (π.χ. για διαχείριση βάσεων δεδομένων, για σύστημα μισθοδοσίας, για έλεγχο ποιότητας, για ανταλλαγή εγγράφων κτλ.). Ως εκ τούτου, η αναγνωσιμότητα από ένα κοινό εκτός του οργανισμού στις περισσότερες περιπτώσεις δεν κρίνεται απαραίτητη.

Η δημιουργία και η λειτουργία ενός ιδιωτικού δικτύου Blockchain προϋποθέτει υποχρεωτικά ότι μία κεντρική αρχή αποφασίζει ποιος μπορεί να διαβάσει, να γράψει ή να συμμετάσχει σε αυτό (Yusoff et al., 2022), με αποτέλεσμα το δίκτυο να μην είναι πλήρως αποκεντρωμένο, όπως στην περίπτωση των δημόσιων δικτύων. Η ίδια κεντρική αρχή ορίζει και το μηχανισμό συναίνεσης (π.χ. Practical Byzantine Fault Tolerance, Proof of Authority κ.ά.) σύμφωνα με τον οποίο θα λαμβάνονται οι αποφάσεις (Bamakan et al., 2020). Αυτό έχει τον κίνδυνο παραβιάσεων ασφαλείας όπως σε ένα κανονικό σύστημα διαχείρισης δεδομένων, αλλά έχει πλεονεκτήματα όσον αφορά την επεκτασιμότητα και τη συμμόρφωση των κανόνων απορρήτου των δεδομένων και άλλων ρυθμιστικών ζητημάτων.

4.5.3. Consortium Blockchain (Κοινοπρακτικό)

Το κοινοπρακτικό Blockchain, το οποίο ονομάζεται και υβριδικό (hybrid) ή ομοσπονδιακό (federal), είναι ένα σύστημα που συνδυάζει τα χαρακτηριστικά ενός δημόσιου και ενός ιδιωτικού δικτύου. Ένα τέτοιο σύστημα τελεί υπό τη διαχείριση μιας προκαθορισμένης ομάδας οργανισμών ή ιδρυμάτων, δηλαδή το χειρίζονται περισσότερες από μία οντότητες χρηστών, και θεωρείται εν μέρει αποκεντρωμένο. Είναι λιγότερο αποκεντρωμένο από ένα δημόσιο δίκτυο, το οποίο είναι ανοικτό σε όλους, αλλά περισσότερο αποκεντρωμένο από ένα ιδιωτικό δίκτυο, όπου μία μόνο κεντρική αρχή αποφασίζει για τα δικαιώματα όλων των χρηστών. Στις περισσότερες περιπτώσεις, σε ένα κοινοπρακτικό Blockchain, οι άδειες ανάγνωσης είναι ανοικτές στο κοινό, ενώ σε κάποιες άλλες περιορίζονται σε μια ομάδα συμμετεχόντων. Επιπρόσθετα, τέτοιου τύπου δίκτυα, δίνουν τη δυνατότητα σε αυτούς που τα χρησιμοποιούν, να διατηρούν κάποια μέρη των δεδομένων τους δημόσια και κάποια ιδιωτικά, μεταξύ των συμμετεχόντων κόμβων.

Ο μηχανισμός συναίνεσης που χρησιμοποιεί ένα κοινοπρακτικό Blockchain (π.χ. Proof of Vote, Proof of Trust κ.ά.) είναι προκαθορισμένος και η διαδικασία συναίνεσης ελέγχεται από το σύνολο των κόμβων που ανήκουν στους προεπιλεγμένους οργανισμούς που μετέχουν στο σύστημα. Θα μπορούσε για παράδειγμα, ανάλογα με το μηχανισμό συναίνεσης, να απαιτείτε ένα ποσοστό άνω του 50% τον οργανισμών να συμφωνεί στην εγκυρότητα ώστε να θεωρείτε ένας κόμβος ελεγμένος και μία συναλλαγή επικυρωμένη. Τα κοινοπρακτικά Blockchains έχουν διάφορες εφαρμογές, αλλά χρησιμοποιούνται κυρίως στον τραπεζικό τομέα. Στην περίπτωση αυτή, στόχος είναι να κατανεμηθεί η εξουσία σε έναν αριθμό διαφορικών αρχών ελέγχου αντί

να υπάρχει μια ενιαία κεντρική αρχή για τη λήψη μιας συλλογικής και αμερόληπτης απόφασης (Dib et al., 2018).

4.6. Μηχανισμοί συναίνεσης

Ένα από τα πιο σημαντικά ζητήματα για την τεχνολογία Blockchain είναι να διασφαλιστεί ότι επιτυγχάνεται συναίνεση από το σύνολο των συμμετεχόντων στο Peer-to-Peer δίκτυο του συστήματος (Kraft, 2016). Για να ολοκληρωθεί μία συναλλαγή, είναι απαραίτητο να την επικυρώσει η πλειοψηφία των κόμβων που συμμετέχουν στο δίκτυο Blockchain (Chawla, 2020). Οι μηχανισμοί (ή αλγόριθμοι) συναίνεσης (consensus mechanisms / algorithms) φροντίζουν για αυτό και αποτελούν το πιο βασικό χαρακτηριστικό ενός συστήματος Blockchain. Απαιτούνται για τη διασφάλιση της σωστής λειτουργίας και καταγραφής όλων των συναλλαγών που γίνονται μέσα στο δίκτυο από όλους του κόμβους του και προήλθαν από το "Πρόβλημα των Βυζαντινών Στρατηγών" (Fu et al., 2021), που αναφέρθηκε στο προηγούμενο κεφάλαιο. Μέσω των μηχανισμών συναίνεσης διασφαλίζεται μεταξύ άλλων ότι οι συμμετέχοντες στο δίκτυο ακολουθούν τους κανόνες του, ότι οι συναλλαγές επικυρώνονται με τη σωστή σειρά, ότι όλες οι πληροφορίες μέσα σε ένα block είναι σωστές, ότι οι miners λαμβάνουν τη σωστή ανταμοιβή και ότι αποφεύγονται προβλήματα όπως αυτό πρόβλημα διπλής δαπάνης.

Υπάρχουν δύο κύριες κατηγορίες μοντέλων συναίνεσης. Η πρώτη προσέγγιση επιλέγει τον επικυρωτή μίας συναλλαγής μέσω κάποιας μορφής "λοταρίας" και οι πιθανότητες νίκης σε αυτή καθορίζονται με διάφορους τρόπους, ανάλογα με το μηχανισμό που χρησιμοποιείται, όπως θα δούμε και στη συνέχεια. Η δεύτερη προσέγγιση χρησιμοποιεί πολλαπλούς γύρους ψηφοφοριών για την επίτευξη της απαραίτητης συναίνεσης. Η διαφοροποίηση αυτή οδηγεί σε μία σαφή διάκριση σε proof-based και vote-based μοντέλα συναίνεσης (Nguyen & Kim, 2018). Οι πιο ευρέως διαδεδομένοι μηχανισμοί συναίνεσης είναι ο Proof-of-Work (PoW), ο Proof-of-Stake (PoS) και ο Practical Byzantine Fault Tolerance (PBFT). Παρ' όλα αυτά υπάρχει ένα μεγάλο πλήθος επιπλέον μηχανισμών συναίνεσης, η μεγάλη πλειοψηφία των οποίων είναι τροποποιημένες εκδόσεις αυτών των τριών, και διακρίνονται με βάση τον τρόπο λειτουργίας, την προστιθέμενη αξία και τους τομείς εφαρμογής τους. Στη συνέχεια αυτού του κεφαλαίου παρουσιάζεται ένας μεγάλος αριθμός μηχανισμών συναίνεσης που είτε έχουν ήδη χρησιμοποιηθεί είτε έχουν προταθεί στην παγκόσμια βιβλιογραφία.

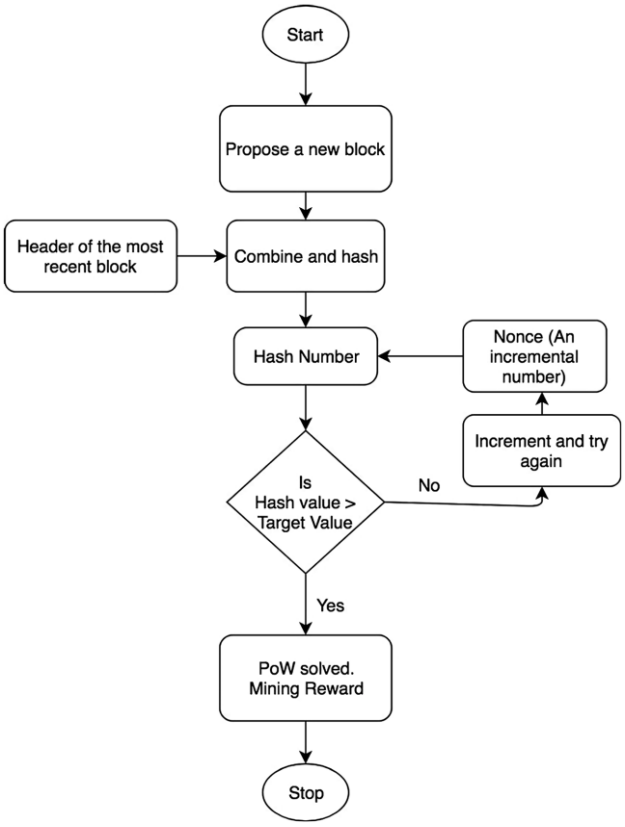
4.6.1. Proof of Work (PoW)

Ο Proof of Work είναι ο πιο διαδεδομένος μηχανισμός συναίνεσης και είναι ο πρώτος που εισήχθη σε δίκτυο Blockchain (Anwar, 2018). Χρησιμοποιείται σε πολλά κρυπτονομίσματα, συμπεριλαμβανομένου του Bitcoin και μέχρι πρόσφατα και του Ethereum (Ethereum, 2022a). Ο μηχανισμός αυτός, λειτουργεί με την παραγωγή ενός κρυπτογραφημένου hash και την έννοια

του εισήγαγαν για πρώτη φορά οι Dwork και Naor (1993). Η χρήση του Proof of Work προέρχεται ιστορικά από τη χρήση του στο "Hashcash", το οποίο σχεδιάστηκε από τον Adam Back (2002) ως ένα σύστημα για τον περιορισμό των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου και των επιθέσεων denial-of-service. Δηλαδή, ο αποστολέας των ανεπιθύμητων μηνυμάτων θα έπρεπε να δαπανήσει ένα ορισμένο ποσό υπολογιστικής ισχύος για την επίλυση ενός μαθηματικού προβλήματος πριν από την αποστολή τους, γεγονός που θα αύξανε σημαντικά το κόστος αποστολής ανεπιθύμητων μηνυμάτων, εξασφαλίζοντας έτσι την ασφάλεια του συστήματος. Ο Proof of Work εφαρμόστηκε για πρώτη φορά σε κατανεμημένα συστήματα στη δημοσίευση της δημιουργίας του Bitcoin (Nakamoto, 2008), όπου είναι επίσης η πρώτη φορά που ένας Byzantine fault-tolerant αλγόριθμος συναίνεσης χρησιμοποιείται σε ένα ανοιχτό και δημόσιο δίκτυο Blockchain.

Η βασική ιδέα του αλγορίθμου Proof of Work είναι να διασφαλίσει τη συνέπεια των δεδομένων και την ασφάλεια της συναίνεσης μέσω του ανταγωνισμού υπολογιστικής ισχύος. Ο αλγόριθμος Proof of Work λειτουργεί χρησιμοποιώντας τους κόμβους που ανήκουν στο Blockchain δίκτυο και απαιτώντας από αυτούς την επίλυση ενός μαθηματικού προβλήματος προκειμένου να δημιουργηθεί το επόμενο block και να επαληθευτεί η εγκυρότητα των συναλλαγών στο δίκτυο (Yusoff et al., 2022). Αυτή η μαθηματική επίλυση γίνεται μέσω της συνάρτησης Hash, η οποία είναι μία τυχαία και πολύπλοκη μαθηματική συνάρτηση, η οποία χρησιμοποιείται για την επιβεβαίωση των συναλλαγών που είναι αποθηκευμένες στα blocks του δικτύου (Salimitari & Chatterjee, 2018). Κάθε κόμβος του δικτύου υπολογίζει μια τυχαία τιμή nonce (number only used once), μέσω της δικής του υπολογιστικής ισχύος και η τιμή συγκρίνεται με την τιμή-στόχο της λύσης του μαθηματικού προβλήματος του συστήματος Blockchain. Όλοι οι κόμβοι ανταγωνίζονται για να είναι οι πρώτοι που θα βρουν τη λύση, κάτι το οποίο απαιτεί τεράστιο αριθμό προσπαθειών και τη κατανάλωση μεγάλης υπολογιστικής δύναμης. Όταν το nonce είναι μικρότερο από την τιμή-στόχο, ο κόμβος αποκτά το δικαίωμα της δημιουργίας του νέου block, το οποίο μεταδίδει σε ολόκληρο το δίκτυο και μόλις επαληθευτεί η ορθότητα του από τους υπόλοιπους κόμβους, θα προστεθεί στο Blockchain. Αυτή η διαδικασία ανταγωνισμού για τα λογιστικά δικαιώματα αναγνώρισης και αποδοχής νέων blocks ονομάζεται "εξόρυξη" (mining) και οι κόμβοι του δικτύου που προσπαθούν να αποκτήσουν αυτά τα δικαιώματα ονομάζονται "εξορύκτες" (miners). Μόνο ο κόμβος που επιλύει πρώτος την αξία nonce που πληροί την προϋπόθεση-στόχο μπορεί παίρνει το λογιστικό δικαίωμα και λαμβάνει τις ανταμοιβές που μπορεί να υπάρχουν π.χ., στην περίπτωση του Blockchain του Bitcoin, η ανταμοιβή για τους κόμβους είναι νέα Bitcoins. Ο μηχανισμός Proof of Work προσαρμόζει αυτόματα το στόχο λύσης του προβλήματος για να αλλάξει την υπολογιστική πολυπλοκότητα, προκειμένου να διασφαλίσει ότι οι κόμβοι του Blockchain δε θα εγκαταλείψουν την προσπάθεια λόγω πολύ μεγάλης δυσκολίας, αλλά και δε θα μονοπωλήσουν

τη δημιουργία blocks λόγω ισχυρής υπολογιστικής ισχύος και ως αποτέλεσμα, ολόκληρο το δίκτυο Blockchain παραμένει σχετικά σταθερό (Xiong et al., 2022). Στο ***Σχήμα 4-11*** απεικονίζεται η διαδικασία του μηχανισμού Proof of Work.



Σχήμα 4-11: Διαδικασία Proof of Work (Ghimire & Selvaraj, 2018)

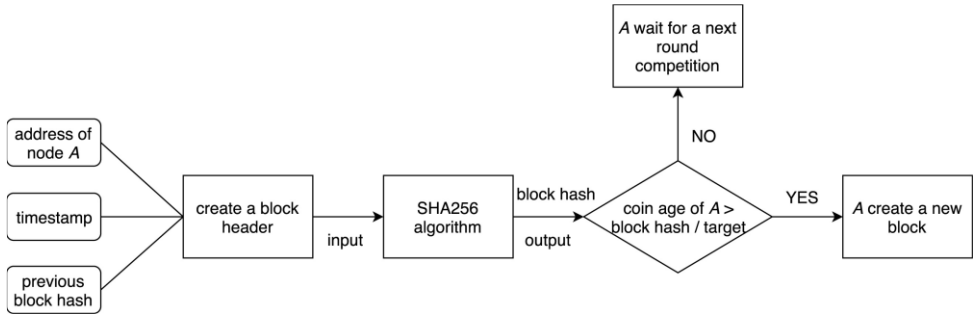
Το πλεονέκτημα του μηχανισμού Proof of Work είναι η υψηλή ασφάλεια και ο σημαντικός βαθμός αποκέντρωσης (Yusoff et al., 2022). Ο αλγόριθμος Proof of Work είναι κατάλληλος για ένα δημόσιο δίκτυο Blockchain και για τη λειτουργία του δεν απαιτείται κάποιος μηχανισμός για την επαλήθευση της ταυτότητας των χρηστών. Ο τρόπος λειτουργίας του, δηλαδή η αναζήτηση της τιμής nonce μέσω πολλών υπολογισμών, τον καθιστά εύκολο στην εφαρμογή του (Xiong et al., 2022). Ωστόσο, το κύριο μειονέκτημά του είναι η μεγάλη κατανάλωση ενέργειας και πόρων, καθώς βασίζεται σε μεγάλο βαθμό στην υπολογιστική ισχύ κατά τη διαδικασία επίλυσης του προβλήματος (De Vries, 2018). Οι κόμβοι που μετέχουν στην επίλυση της μαθηματικής συνάρτησης καταναλώνουν μεγάλη επεξεργαστική ισχύ και τεράστιους υπολογιστικούς πόρους για να καταφέρουν να λύσουν ένα πρόβλημα με δισεκατομμύρια πιθανές λύσεις. Αυτό έχει σαν αποτέλεσμα να απαιτείται η σπατάλη πολύτιμων πόρων, όπως χρήματα, ενέργεια, χώρος, υλικοτεχνική υποδομή κτλ. (Yusoff et al., 2022). Εκτός όμως αυτού, είναι μία ιδιαίτερα χρονοβόρα διαδικασία, καθώς οι κόμβοι καλούνται να εξετάσουν ένα

μεγάλο αριθμό πιθανών τιμών για να βρουν τη σωστή λύση στο πρόβλημα και είναι άγνωστο το πότε θα το καταφέρουν. Η περίοδος συμφωνίας συναίνεσης υπολογίζεται σε περίπου 10 λεπτά για την επίλυση ενός μαθηματικού προβλήματος και η απόδοση συναλλαγής είναι πολύ χαμηλή (Rosenfeld, 2014). Επομένως, αυτός ο αλγόριθμος, που χαρακτηρίζεται από χαμηλή διαμεταγωγή και υψηλό χρόνος αδράνειας και η χαμηλή απόδοση στην επίτευξη συναίνεσης (Tschorsch & Scheuermann, 2016) δεν είναι κατάλληλος για ένα μεγάλα και ταχέως αναπτυσσόμενα δίκτυα που απαιτούν τεράστιο αριθμό συναλλαγών ανά δευτερόλεπτο (Alsunaidi & Alhaidari, 2019).

4.6.2. Proof of Stake (PoS)

Ο αλγόριθμος Proof of Stake προτάθηκε το 2011, λόγω των ελλείψεων του αλγορίθμου Proof of Work που αναφέρθηκαν, όπως η σπατάλη υπολογιστικής ισχύος και η χαμηλή απόδοση στην επίτευξη συναίνεσης (Xiong et al., 2022). Αφού προτάθηκε, εφαρμόστηκε σε πρακτική εφαρμογή το επόμενο έτος (King & Nadal, 2012) στο ψηφιακό νόμισμα "Peercoin" (ή "PPCoin" όπως ήταν αρχικά γνωστό). Ο μηχανισμός αυτός αποτελεί τη βασική εναλλακτική επιλογή του Proof of Work, καθώς επιλύει το πρόβλημα της μεγάλης ενεργειακής κατανάλωσης και αυτός είναι και ο λόγος του πρόσφατου μετασχηματισμού του μηχανισμού συναίνεσης που χρησιμοποιεί το Blockchain του Ethereum από Proof of Work σε Proof of Stake (Ethereum, 2022a).

Η διαδικασία λειτουργίας του μηχανισμού συναίνεσης Proof of Stake είναι διαφορετική από αυτή του Proof of Work, καθώς δεν απαιτείται από τους κόμβους που μετέχουν στο σύστημα, η επίλυση κάποιου μαθηματικού προβλήματος για να επιτευχθεί η συναίνεση. Οι χρήστες χρησιμοποιούν μόνο το υποκείμενο asset του blockchain (π.χ. κρυπτονόμισμα) ως "μερίδιο" (stake) για να επιτύχουν τη ζητούμενη συναίνεση. Με αυτόν τον τρόπο ο μηχανισμός Proof of Stake εισαγάγει την έννοια του token, το οποίο αποτελεί αυτό το asset. Στην περίπτωση λοιπόν αυτού του μηχανισμού, επιλέγεται από το σύστημα ως κόμβος με δικαίωμα λογιστικής εγγραφής ενός νέου block, αυτός με το υψηλότερο "μερίδιο" (stake) στο σύστημα. Το "μερίδιο" ενός κόμβου υπολογίζεται με βάση τον αριθμό των tokens που κατέχει και το χρόνο που τα κατέχει. Όσο περισσότερα tokens κατέχει ένας κόμβος και όσο περισσότερο τα κατέχει, τόσο υψηλότερο είναι το "μερίδιο" του, τόσο μικρότερη η δυσκολία του "mining" και τόσο μεγαλύτερη η απόδοση στην εύρεση της τιμής στόχου του τυχαίου αριθμού (Xiong et al., 2022) και τόσο αυξάνονται και οι πιθανότητες για ένα χρήστη του συστήματος να αποκτήσει το δικαίωμα εγγραφής ου νέου block (Eigelshoven et al., 2020). Για παράδειγμα, εάν το μερίδιο σε συγκεκριμένο κρυπτονόμισμα είναι στο 1%, οι χρήστες μπορούν να κόψουν έως και το 1% των συναλλαγών (Jain et al., 2018). Στο ***Σχήμα 4-12*** απεικονίζεται η διαδικασία του μηχανισμού Proof of Stake.



Σχήμα 4-12: Διαδικασία Proof of Stake (Zhang & Lee, 2020)

Αφού ένας από τους κόμβους αποκτήσει με επιτυχία το λογιστικό δικαίωμα για τη δημιουργία του block, το "μερίδιο" του θα εκκαθαριστεί και θα ξεκινήσει ο επόμενος γύρος για την επανάληψη αυτής της διαδικασίας (staking). Υπάρχουν δύο τρόποι συμμετοχής στο "staking" (Yusoff et al., 2022). Ο πρώτος είναι ότι ο χρήστης μπορεί να δανείσει τα tokens του σε άλλο χρήστη που μετέχει σε μία μεγαλύτερη ομάδα χρηστών (pool) και στη συνέχεια να μοιραστεί το κέρδος μαζί του. Ωστόσο, σε αυτήν την περίπτωση, ο χρήστης θα πρέπει να βρει ένα αξιόπιστο άτομο για να δανείσει τα tokens του. Ο δεύτερος τρόπος είναι ο χρήστης να μετέχει ο ίδιος, σε μία μεγαλύτερη ομάδα χρηστών. Όλοι όσοι συμμετέχουν στη συγκεκριμένη ομάδα θα λάβουν κέρδος αντίστοιχο με το ποσό του μεριδίου που παραχώρησαν. Ο δημιουργός του νέου block επιλέγεται από μία από τις ομάδες χρηστών έχει ποντάρει ένα συγκεκριμένο ποσό νομισμάτων και κανένας χρήστης δεν μπορεί να προβλέψει εκ των προτέρων τον αριθμό nonce.

Όπως είναι φανερό, η επιλογή του Proof of Stake ως μηχανισμού συναίνεσης σε Blockchains κρυπτονομισμάτων ενθαρρύνει τους κατόχους των νομισμάτων να αυξήσουν το χρόνο διακράτησης τους (Mingxiao et al., 2017). Σε αυτήν την περίπτωση το Blockchain δεν εξαρτάται πλέον από την εντατική χρήση υπολογιστικής ισχύος, χάρη στην ανάγκη διακράτησης των νομισμάτων για την μεγαλύτερη πιθανότητα κέρδους νέων και αυτό λύνει αποτελεσματικά το πρόβλημα της σπατάλης των πόρων (Yusoff et al., 2022). Αυτό με τη σειρά του μειώνει το χρόνο μπλοκ και τον χρόνο επεξεργασίας των συναλλαγών και εξοικονομεί σημαντικά χρόνο για την επίτευξη συναίνεσης και η αποτελεσματικότητα της συναίνεσης βελτιώνεται σημαντικά (Saleh, 2021). Επίσης, η χρήση του μηχανισμού Proof of Stake βελτιώνει την ασφάλεια του συστήματος, καθώς οι κακόβουλοι χρήστες πρέπει να συγκεντρώσουν μεγάλο αριθμό νομισμάτων και να τα κρατήσουν για μεγάλο χρονικό διάστημα για να επιτεθούν στο δίκτυο, κάτι το οποίο αυξάνει σημαντικά τη δυσκολία της επίθεσης, σε σχέση με τον αλγόριθμο Proof of Work. Εκτός αυτού όμως, μία επίθεση στα μερίδια του συνολικού συστήματος, θα επηρεάσει και την αξία των μεριδίων που κατέχει ο κακόβουλος χρήστης (Xiong et al., 2022).

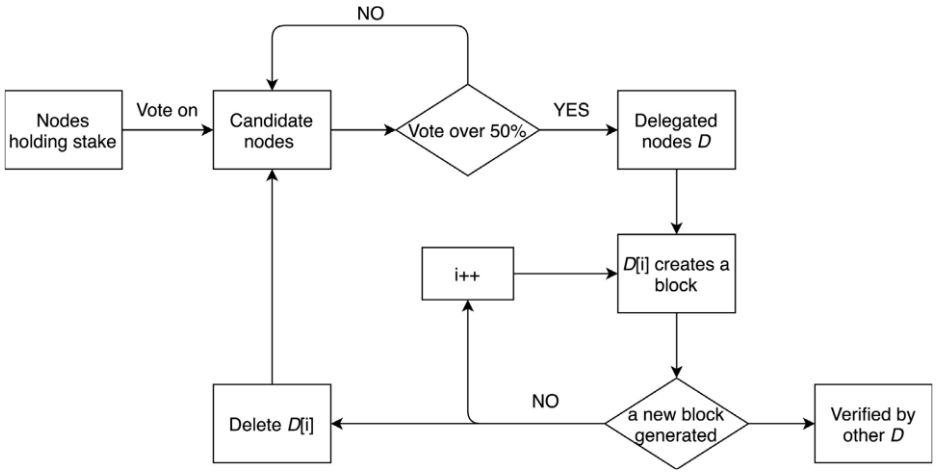
Όμως, ο τρόπος λειτουργίας του αλγορίθμου, ο οποίος αυξάνει την ασφάλεια του δικτύου από κακόβουλους χρήστες, αυξάνει ταυτόχρονα και τον κίνδυνο μονοπωλίου, καθώς οδηγεί σε

τάσεις συγκέντρωσης assets από κόμβους του συστήματος (Fu et al., 2021), επιτρέποντας παράλληλα στους κακόβουλους επιτιθέμενους να έχουν ένα ξεκάθαρο στόχο για να βλάψουν, προκαλώντας τη μέγιστη δυνατή ζημιά. Επίσης, επειδή οι κόμβοι με υψηλότερο μετοχικό κεφάλαιο τείνουν να αποκτούν περισσότερα δικαιώματα δημιουργίας blocks, μειώνεται ο ενθουσιασμός των χρηστών με χαμηλότερα μερίδια να συμμετάσχουν, μειώνοντας έτσι την ενεργή κοινότητα ολόκληρου του Blockchain (Xiong et al., 2022).

4.6.3. Delegated Proof of Stake (DPoS)

Ο αλγόριθμος Delegated Proof of Stake εισήχθη από τον Larimer (2014) και ο τρόπος λειτουργίας του παρομοιάζεται με τη λειτουργία του αντιπροσωπευτικού εκλογικού συστήματος (Xiong et al., 2022) ή με τη διαδικασία ψηφοφορίας σε ένα διοικητικό συμβούλιου μίας εταιρείας (Wang et al., 2020). Ο αλγόριθμος προτάθηκε σαν μία βελτίωση του αλγορίθμου Proof of Stake, μέσω της εκλογής αντιπροσώπων μεταξύ των κόμβων, οι οποίοι λειτουργούν ως υπεύθυνοι για τη λήψη των αποφάσεων. Ο αριθμός των νομισμάτων που κατέχει κάθε κόμβος στο σύστημα αποτελεί τον αριθμό των ψήφων που έχει στη διάθεση του. Μέσω ψηφοφορίας, κόμβοι που θεωρούνται πιο αξιόπιστοι, εκλέγονται ως υπεύθυνοι για να λάβουν αποφάσεις κατά τη διαδικασία της συναίνεσης. Η επιλογή του τελικού αριθμού των αντιπροσώπων γίνεται με τέτοιο τρόπο, ώστε τουλάχιστον το 50% των κόμβων που ψηφίζουν να πιστεύουν ότι υπάρχει επαρκής αποκέντρωση για το δίκτυο. Οι κόμβοι που έλαβαν τις περισσότερες ψήφους αποτελούν τους υπεύθυνους λήψης αποφάσεων, οι οποίοι ελέγχουν ολόκληρο το δίκτυο και ανταμείβονται με τη δυνατότητα δημιουργίας των νέων block της αλυσίδας, εναλλάσσοντας με τη σειρά τα λογιστικά δικαιώματα για τη δημιουργία τους.

Κάθε κόμβος του συστήματος μπορεί να βρεθεί στη θέση του αντιπροσώπου αρκεί να λάβει τον απαραίτητο αριθμό ψήφων. Όσοι επιθυμούν να εκλεγούν οφείλουν να εξασφαλίζουν ότι θα βρίσκονται online κατά τον απαιτούμενο χρόνο ώστε να λειτουργεί σωστά το δίκτυο. Εάν ένας υπεύθυνος λήψης αποφάσεων παραβιάσει το πρωτόκολλο του blockchain, η δραστηριότητα της δημιουργίας νέου block θα μεταφερθεί στο επόμενο block και οι ενδιαφερόμενοι κόμβοι του συστήματος θα τον αντικαταστήσουν, εκλέγοντας νέο αντιπρόσωπο για να πάρει τη θέση του. Μέσω του μηχανισμού της εκλογής πολλαπλών φορέων λήψης αποφάσεων, δεν θα υπάρξει υπερβολική συγκέντρωση των λογιστικών δικαιωμάτων σε έναν μόνο κόμβο, γεγονός που μπορεί να αποτρέψει τον υπερβολικό συγκεντρωτισμό. Στόχος του αλγορίθμου DPoS είναι να αξιοποιεί στο έπακρο τις ψήφους των ενδιαφερόμενων κόμβων, ώστε η επίτευξη της συναίνεσης να είναι δίκαιη και δημοκρατική (Zhang & Lee, 2020). Στο ***Σχήμα 4-13*** απεικονίζεται η διαδικασία του μηχανισμού Delegated Proof of Stake.



Σχήμα 4-13: Διαδικασία Delegated Proof of Stake (Zhang & Lee, 2020)

Ο αλγόριθμος DPoS συνδυάζει έως ένα βαθμό τα πλεονεκτήματα των αλγορίθμων Proof of Work και Proof of Stake, παρέχοντας εξοικονόμηση ενέργειας, όχι μόνο σε σχέση με τον πρώτο, αλλά και με το δεύτερο (Yusoff et al., 2022). Ο μηχανισμός είναι απλός και αποτελεσματικός, καθώς δεν απαιτεί "εξόρυξη" ή πλήρη επαλήθευση των κόμβων, αλλά αντ' αυτού, η διαδικασία εκτελείται από περιορισμένο αριθμό κόμβων, μέσω του συστήματος εκλογής. Έτσι, η ταχύτητα επικοινωνίας μεταξύ των κόμβων κατά τη συναίνεση είναι ταχύτερη και οι κόμβοι μπορούν να ολοκληρώσουν γρήγορα τη λογιστική εγγραφή, τη μετάδοση και την επαλήθευση των blocks και να βελτιώσουν σημαντικά την απόδοση συναλλαγών του συστήματος (Xiong et al., 2022). Ταυτόχρονα, μπορεί να φιλοξενηθεί μεγάλο αριθμό κόμβων με ελεύθερη είσοδο και έξοδο από το σύστημα, καθώς η αλλαγή του αριθμού του κόμβων είτε δεν επηρεάζει την απόδοση του συστήματος είτε ο αντίκτυπος είναι μικρός, άρα και η επεκτασιμότητα ισχυρή (iBid).

Ωστόσο, αυτός ο περιορισμένος αριθμός υπευθύνων για τη λήψη αποφάσεων καθιστά το δίκτυο πιο συγκεντρωτικό (Salimitari & Chatterjee, 2018), ενώ και οι κανόνες ψηφοφορίας παίζουν σημαντικό ρόλο, ώστε να διατηρείται το αίσθημα δικαιοσύνης μεταξύ των κόμβων που θέλουν να μετέχουν συμβάλλοντας επαρκώς στην αποκέντρωση του συνολικού συστήματος. Επιπλέον, λόγω του μηχανισμού που κάθε εκλεγμένος αντιπρόσωπος δημιουργεί εναλλάξ τα blocks, η ταυτότητα του κόμβου αυτού είναι ήδη γνωστή και πάντα σταθερή, γεγονός που καθιστά το blockchain πιο ευάλωτο σε επιθέσεις συμπαιγνίας (Yang et al., 2019).

4.6.4. Leased Proof of Stake (LPoS)

Ο Leased Proof of Stake είναι ένας ακόμα μηχανισμός που βασίζεται στον PoS και διαφοροποιείται ώστε να βελτιώσει τις αδυναμίες του. Σύμφωνα με την πλατφόρμα Waves (n.d.), που βασίζει τη λειτουργία της σε αυτό το μηχανισμό, οι κόμβοι μπορούν να συμμετέχουν στη διαδικασία χρησιμοποιώντας κεφάλαια που ανήκουν σε άλλους κόμβους. Επιτρέπει

δηλαδή στους κόμβους με μικρό κεφάλαιο να συμμετέχουν στην διαδικασία δημιουργία νέων blocks, μέσω μίας επιλογής "μίσθωσης" (leasing). Η μίσθωση επιτρέπει στους κόμβους που κατέχουν μεγάλα "μερίδια" να εκμισθώνουν τα κεφάλαιά τους, για συγκεκριμένο χρονικό διάστημα, σε κόμβους με μικρά "μερίδια" που λειτουργούν ως μισθωτές. Κατά τη διάρκεια της μίσθωσης, το μισθωμένο ποσό διατηρείται στο υπόλοιπο του εκμισθωτή, ωστόσο, αυξάνει κανονικά την πιθανότητα δημιουργίας κάποιου block από τον μισθωτή, δηλαδή αυτόν με το μικρό υπόλοιπο. Όταν αυτό συμβεί, τα δύο συμβαλλόμενα μέρη θα μοιραστούν αναλογικά την ανταμοιβή. Αυτή η προσέγγιση εφαρμόζεται ώστε το Blockchain ναι είναι πιο ασφαλές σε σχέση με τις εκδοχές των μηχανισμών PoS και DPoS, καθώς αντιμετωπίζεται σε σημαντικό βαθμό η μειωμένη αποκέντρωση, η οποία είναι ένα σημαντικό μειονέκτημα των άλλων δύο μηχανισμών (Salimitari & Chatterjee, 2018).

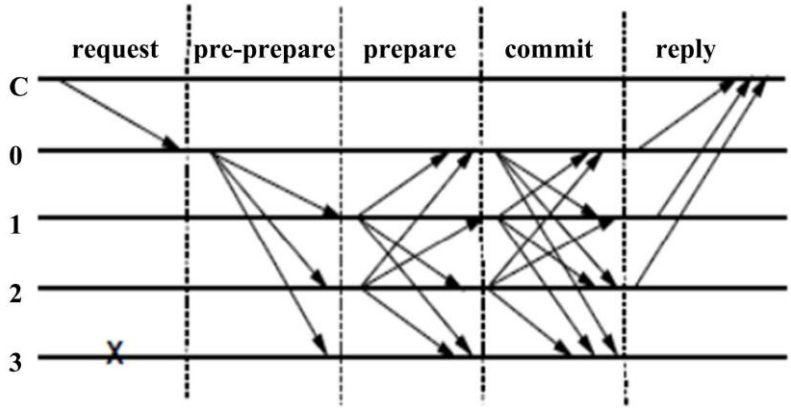
4.6.5. Practical Byzantine Fault Tolerance (PBFT)

Ο Practical Byzantine Fault Tolerance είναι ο κύριος αλγόριθμος μίας κατηγορίας αλγορίθμων που εντάσσονται στην κατηγορία Byzantine Agreement. Οι αλγόριθμοι αυτής της κατηγορίας έχουν ως στόχο την ομοφωνία μέσα σε ένα περιβάλλον που περιλαμβάνει σφάλματα και χωρίζονται σε αυτούς που λειτουργούν με ανεκτικότητα στα σφάλματα (Byzantine Fault Tolerance) και σε αυτούς που δεν είναι ικανοί να λειτουργήσουν σε περιβάλλον με σφάλματα (Non-Byzantine Fault-Tolerance). Ένα αλγόριθμος Byzantine Fault Tolerance μπορεί να επιλύσει οποιοδήποτε είδος σφάλματος στο κατανεμημένο σύστημα έως κάποιο βαθμό και να αντιμετωπίσει την παρουσία κακόβουλων κόμβων, εξασφαλίζοντας την ασφάλεια και τη σταθερότητα του κατανεμημένου συστήματος (Schneider, 1990). Αντίθετα ένας αλγόριθμος Non-Byzantine Fault-Tolerance δεν μπορεί να εγγυηθεί την ασφάλεια των δεδομένων και τη σταθερότητα του συστήματος, όταν εκτελούνται κακόβουλες δραστηριότητες από κόμβους (π.χ. παραποίηση δεδομένων) και ως εκ τούτου είναι δύσκολο να εφαρμοστεί σε ένα δημόσιο δίκτυο (Xiong et al., 2022).

Ο αλγόριθμος Practical Byzantine Fault Tolerance προτάθηκε από τους Castro και Liskov (1999) ως μία προσέγγιση για την επίλυση του προβλήματος των Βυζαντινών στρατηγών και είναι εμπνευσμένος από την πρόταση των Lamport et al. (1982). Ο αλγόριθμος επικεντρώνεται στην επίλυση του προβλήματος της επικύρωση συναλλαγών σε κόμβους κατανεμημένων συστημάτων που μπορεί να αντιμετωπίζουν σφάλματα του προβλήματος των Βυζαντινών στρατηγών, παρέχοντας έναν τρόπο για την ανοχή σε αυτά (Alsunaidi & Alhaidari, 2019). Μειώνει την πολυπλοκότητα και αυξάνει την απόδοση ανοχής των σφαλμάτων, με την προϋπόθεση της διατήρησης της σταθερότητας και της ασφάλειας του αρχικού αλγορίθμου, καθιστώντας τον έτσι λειτουργικό σε πρακτικές εφαρμογές (Zhang et al., 2019). Για τη λειτουργία του PBFT, ο μέγιστος αριθμός κακόβουλων κόμβων δεν μπορεί να υπερβαίνει το

1/3 του συνολικού αριθμού κόμβων, με αποτέλεσμα μέχρι εντός αυτού του ορίου, ο αλγόριθμος να μπορεί να λειτουργήσει σωστά και να διασφαλίσει την αξιοπιστία του συστήματος, βελτιώνοντας έτσι σημαντικά την απόδοση ασφαλείας (Xiong et al., 2022).

Οι κόμβοι του μηχανισμού αποτελούνται από τον κύριο κόμβο (leader node) και τους υπόλοιπους κόμβους (validating nodes) του δικτύου και οι συναλλαγές επικυρώνονται αφού περάσουν από μία διαδικασία ψηφοφορίας που απαρτίζεται από πολλούς γύρους. Ο κύριος κόμβος επιλέγεται από το σύστημα και είναι υπεύθυνος για τη διανομή και επεξεργασία των πληροφοριών στους άλλους κόμβους, καθώς και για τον έλεγχο της εγκυρότητας τους. Αφού υπόλοιποι κόμβοι λάβουν τις πληροφορίες που αποστέλλονται από τον κύριο κόμβο, θα επαληθεύσουν τις πληροφορίες. Η διαδικασία του αλγορίθμου PBFT χωρίζεται σε 3 φάσεις: α) pre-prepare, β) prepare και γ) commit (Castro & Liskov, 1999). Στη φάση "pre-prepare", ο κύριος κόμβος στέλνει τον εκχωρημένο αριθμό ακολουθίας και πληροφορίες στους άλλους κόμβους. Αφού οι άλλοι κόμβοι λάβουν τις πληροφορίες που αποστέλλονται από τον κύριο κόμβο και επιβεβαιώσουν, αρχίζει η φάση "prepare". Σε αυτή τη φάση ο κάθε κόμβος στέλνει τις πληροφορίες σε όλους τους κόμβους εκτός από τον εαυτό του όταν αυτό ολοκληρωθεί όλοι οι κόμβοι θεωρούνται έτοιμοι. Στη φάση "commit" όλοι οι υπόλοιποι κόμβοι θα μεταδώσουν ένα μήνυμα επιβεβαίωσης σε ολόκληρο το δίκτυο και οι πληροφορίες καταγράφονται στο Blockchain Σε κάθε φάση, ένας κόμβος προχωρά στην επόμενη φάση εάν λάβει ψήφους από περισσότερα από τα δύο τρίτα όλων των κόμβων, ενώ ο κύριος κόμβος συντονίζει τις ενέργειες της διαδικασίας (Mingxiao et al., 2017). Στο ***Σχήμα 4-14*** απεικονίζεται η διαδικασία του μηχανισμού Practical Byzantine Fault Tolerance.



Σχήμα 4-14: Διαδικασία Practical Byzantine Fault Tolerance (Mingxiao et al., 2017)

Ο τρόπος επίτευξης της ομοφωνίας στον αλγόριθμο PBFT δεν απαιτεί υψηλή ενεργειακή κατανάλωση, ενώ η εμπιστοσύνη μεταξύ των κόμβων που απαιτείται για να λειτουργεί σωστά το δίκτυο, το κάνει ιδιαίτερα αποδοτικό στην επικύρωση των συναλλαγών (Vukolić, 2016). Ωστόσο, ο αλγόριθμος έχει επίσης ορισμένους περιορισμούς. Η πολυπλοκότητα της

επικοινωνίας καθιστά την επεκτασιμότητα του δικτύου πολύ δύσκολη, ενώ κάποιες φορές εμφανίζονται και χρονικές καθυστερήσεις, καθώς το δίκτυο θα πρέπει να περιμένει τις ψήφους όλων των κόμβων του (Bamakan et al., 2020). Επιπλέον σε περίπτωση που υπάρχουν προβλήματα επικοινωνίας εντός του δικτύου, θα εμφανιστεί υψηλή καθυστέρηση επεξεργασίας των πληροφοριών (Xiong et al., 2022). Επομένως, με βάση τα χαρακτηριστικά του, ο PBFT είναι ένα ιδανικό μοντέλο ομοφωνίας για χρήση σε Blockchain με περιορισμένο αριθμό κόμβων και εφαρμόζεται κυρίως είτε σε ιδιωτικά δίκτυα είτε σε δίκτυα κοινοπραξίας και δεν είναι ένας κατάλληλος αλγόριθμος για δημόσια δίκτυα Blockchain.

4.6.6. Delegated Byzantine Fault Tolerance (DBFT)

Ο αλγόριθμος Delegated Byzantine Fault Tolerance ακολουθεί τους ίδιους κανόνες με τον PBFT, αλλά δεν απαιτεί την καθολική συμμετοχή όλων των κόμβων για την επίτευξη της ομοφωνίας και την προσθήκη ενός block. Αυτό είναι ουσιαστικά η διαφορά του, η οποία του δίνει δυνατότητες πολύ μεγαλύτερης επεκτασιμότητας (Salimitari & Chatterjee, 2018). Όπως και στην περίπτωση του DPoS, ορισμένοι κόμβοι του δικτύου επιλέγονται ως αντιπρόσωποι άλλων κόμβων και ακολουθούν μία διαδικασία συναίνεσης παρόμοια με του PBFT (Zheng et al., 2018).

Τον αλγόριθμο αυτό χρησιμοποιεί η πλατφόρμα του κρυπτονομίσματος με την ονομασία "NEO", όπου οι κόμβοι χωρίζονται στους κανονικούς κόμβους και στους "Bookkeepers". Η δεύτερη κατηγορία είναι οι αντιπρόσωποι όλων των υπολοίπων κόμβων του δικτύου και για να προχωρήσουν στα διαδοχικά στάδια της ψηφοφορίας θα πρέπει να έχουν την αποδοχή τουλάχιστον των 2/3 του συνολικού δικτύου. Ο DBFT έχει χαμηλή ενεργειακή κατανάλωση και κάθε νέο block δημιουργείται ανά περίπου 15 δευτερόλεπτα (Salimitari & Chatterjee, 2018).

4.6.7. Proof of Importance (PoI)

Ο Proof of Importance είναι ένας μηχανισμός ομοφωνίας, ο οποίος είναι μία παραλλαγή του PoS, και αναπτύχθηκε από την ομάδα του δικτύου NEM (nemproject.github.io) για τη λειτουργία του κρυπτονομίσματος με την ονομασία XEM. Κάθε λογαριασμός εντός του δικτύου NEM έχει ένα υπόλοιπο κρυπτονομισμάτων XEM που χωρίζεται σε δύο μέρη: α) στο κατοχυρωμένο υπόλοιπο (vested balance) και β) στο μη κατοχυρωμένο υπόλοιπο (unvested balance). Κατά την πραγματοποίηση μίας συναλλαγής, τα δύο μέρη μεταβάλλονται με στόχο να διατηρείται η μία σχετική αναλογία μεταξύ τους. Ο κανόνας για τη διατήρηση αυτής της ισορροπίας είναι όταν ένας λογαριασμός λαμβάνει XEM, αυτά να προστίθενται στο μη κατοχυρωμένο υπόλοιπο του, ενώ το 1/10 δέκατο του μη κατοχυρωμένου υπολοίπου κάθε λογαριασμού να μετακινείται στο κατοχυρωμένο ανά τη δημιουργία 1440 blocks στο Blockchain. Αντίστοιχα, όταν ένας λογαριασμός στέλνει XEM, αυτά χρεώνονται τόσο στο

κατοχυρωμένο όσο και στο μη κατοχυρωμένο υπόλοιπο του, προκειμένου να διατηρηθεί η ίδια αναλογία (Bach et al., 2018).

Το "Importance Score" κάθε κόμβου είναι αυτό με το οποίο καθορίζεται ο δημιουργός των νέων blocks. Η διαδικασία αυτή δεν ονομάζεται "εξόρυξη", όπως στην περίπτωση του PoW, αλλά "συγκομιδή" (harvesting) και παρέχει τις αντίστοιχες ανταμοιβές (τέλη συναλλαγών) στους κόμβους με βάση το "Importance Score" που διαθέτουν (Janowicz et al., 2018). Για να μπορεί ένας κόμβος να διεκδικήσει το δικαίωμα συμμετοχής στη "συγκομιδή", θα πρέπει να διαθέτει τουλάχιστον 10.000 XEM στο κατοχυρωμένο υπόλοιπο του (Bach et al., 2018). Το "Importance Score" μετράει τη συνολική συνεισφορά ενός κόμβου στο δίκτυο συνυπολογίζοντας πολλές παραμέτρους όπως το κατοχυρωμένο υπόλοιπο, τη φήμη του, την τοπολογία του (ακραίος κόμβος ή μέρος συμπλέγματος κόμβων), το πλήθος των συναλλαγών που έχει επικυρώσει κ.ά. (iBid).

4.6.8. Proof of Activity (PoA)

Το Proof of Activity είναι ένα υβριδικό σύστημα μηχανισμού συναίνεσης που συνδυάζει τους αλγορίθμους Proof of Work και Proof of Stake (Zheng et al., 2018). Στόχος του είναι η μείωση της ενεργειακής κατανάλωσης της δημοφιλέστερης αλυσίδας blockchain δηλαδή του Bitcoin (Nguyen & Kim, 2018). Για να το πετύχει αυτό, η προτεινόμενη διαδικασία αποτελείται από δύο φάσεις οι οποίες εκτελούνται σειριακά, το "mining" και το "voting". Το πρώτο μέρος ταυτίζεται με το mining του Proof of Work, ωστόσο το block που θα δημιουργηθεί θα περιέχει μόνο μία κεφαλίδα και τη διεύθυνση του miner που το δημιούργησε, χωρίς καμία συναλλαγή. Οι συναλλαγές προστίθενται στο μπλοκ, στο δεύτερο μέρος της διαδικασίας, όπου κόμβοι που ανήκουν στην κατηγορία των "επικυρωτών" (validators), κερδίζουν το λογιστικό δικαίωμα της εγγραφής των συναλλαγών στο νέο block, μία διαδικασία η οποία εφαρμόζεται όπως στην περίπτωση του Proof of Stake. Η διαδικασία επιλογής κόμβων για τη συναίνεση στηρίζεται στο "coinage", δηλαδή στο γινόμενο των νομισμάτων ενός κόμβου και του χρόνου διακράτησης αυτών από τον ίδιο κόμβο (Bentov et al, 2014).

Ο αλγόριθμος Proof of Activity προσφέρει ασφάλεια απέναντι σε απειλές, όπως το "51% Attack" και το "Double spending", ενώ παρέχει μεγαλύτερη διασπορά των αμοιβών στους κόμβους που μετέχουν στη διαδικασία. Λόγω όμως της ανάγκης για τη χρήση του μηχανισμού Proof of Work στη φάση του mining, η κατανάλωση ενέργειας και πόρων παραμένει σχετικά υψηλή (Salimitari & Chatterjee, 2018). Επιπλέον, η υβριδική μορφή απαιτεί περισσότερο χρόνο για την επίτευξη συναίνεσης και μπορεί να αντιμετωπίσει χρονικές καθυστερήσεις στην επικύρωση των συναλλαγών (Debus, 2017).

4.6.9. **Proof of Authority (PoA)**

Ο αλγόριθμος Proof of Authority (PoA) προτάθηκε από τον Wood (2016) και είναι ουσιαστικά μία εκδοχή του κλασσικού Proof of Stake και μπορεί να εφαρμοστεί τόσο σε δημόσια όσο και σε ιδιωτικά δίκτυα Blockchain. Η διαφορά μεταξύ τους είναι ότι ο Proof of Authority, για την επίτευξη της συναίνεσης, αξιοποιεί την ταυτότητα του χρήστη αντί για το πλήθος των ψηφιακών περιουσιακών στοιχείων που διαθέτει, όπως στην περίπτωση του Proof of Stake. Αυτό σημαίνει ότι βασίζεται στη φήμη των αξιόπιστων κόμβων (authorities) του δικτύου Blockchain, οι οποίοι είναι οι προ-εγκεκριμένοι υπεύθυνοι για την επικύρωση των συναλλαγών και τη συνολική ασφάλεια του συστήματος. Σύμφωνα με το μοντέλο λειτουργίας αυτού του αλγορίθμου, για να μπορεί κάποιος κόμβος να διεκδικήσει αυτή την εξουσιοδοτημένη θέση μέσα στο σύστημα, δεν είναι εύκολο και θα πρέπει να ακολουθήσει ένα σύνολο κανόνων. Κατ' αρχήν θα πρέπει να είναι πρόθυμος να αποκαλύψει με επίσημα έγγραφα την ταυτότητα του και να εγγραφεί με την ίδια ταυτότητα σε ξεχωριστή "συμβολαιογραφική" βάση δεδομένων (Yusoff et al., 2022). Στη συνέχεια κατά τη διαδικασία επιλογής, οι κόμβοι εκλέγονται σε μέσω διαδικασίας πολλαπλών βημάτων (De Angelis et al., 2018), κατά την οποία πρέπει να αποδείξουν τη μακροπρόθεσμη δέσμευσή τους στο δίκτυο Blockchain και να είναι πρόθυμοι να επενδύσουν χρήματα και να διακινδυνεύσουν τη φήμη τους για αυτό το σκοπό. Σε κάθε περίπτωση η διαδικασία θα πρέπει να ακολουθεί συγκεκριμένες κατευθυντήριες γραμμές για να διασφαλιστεί ότι όλοι οι υποψήφιοι έχουν ίσες ευκαιρίες να γίνουν εξουσιοδοτημένοι κόμβοι, θέση η οποία τους παρέχει αντίστοιχες ανταμοιβές και δύναμη μέσα στο δίκτυο.

Βασικό ζητούμενο για το μηχανισμό Proof of Authority σε σύγκριση με άλλους, είναι να είναι ταχύτερος και με καλύτερη απόδοση, θυσιάζοντας όμως έτσι τη συνεκτικότητα των δεδομένων και την έννοια της εμπιστοσύνης στο δίκτυο (De Angelis et al., 2018), το οποίο σημαίνει ότι σε περιπτώσεις που η ακεραιότητα των δεδομένων είναι κρίσιμη για τους κόμβους του δικτύου, δεν αποτελεί καλή επιλογή ως μηχανισμός συναίνεσης. Όπως είναι αντιληπτό, δεν απαιτεί υλικοτεχνική υποδομή υψηλής απόδοσης επειδή οι κόμβοι δεν χρειάζεται να χρησιμοποιούν υπολογιστικούς πόρους και καταγράφει μεγαλύτερο ποσοστό συναλλαγών σε σχέση με τους PoW και PoS, καθώς η επικύρωση γίνεται με προκαθορισμένη ακολουθία από τους εξουσιοδοτημένους κόμβους και σε προκαθορισμένο χρονικό διάστημα (Yusoff et al., 2022). Ωστόσο, οι ταυτότητες των εξουσιοδοτημένων κόμβων είναι ορατές σε οποιονδήποτε και αυτό θα μπορούσε ενδεχομένως να οδηγήσει σε χειραγώγηση από τρίτους.

4.6.10. **Proof of Capacity (PoC)/ Proof of Space (PoSpace)**

Ο μηχανισμός συναίνεσης Proof of Capacity, ο οποίος είναι γνωστός και ως Proof of Space, είναι μία μορφή του PoW, με τη διαφορά ότι αντί να βασίζεται στην υπολογιστική δύναμη που διαθέτει κάθε κόμβος, λειτουργεί με βάση το διαθέσιμο χώρο που έχει κάθε κόμβος στο σκληρό

του δίσκο. Ο μηχανισμός αυτός έχει ήδη βρει εφαρμογή σε κρυπτονομίσματα (Gauld et al., 2017). Για τη λειτουργία του μηχανισμού, οι miners υπολογίζουν εξ' αρχής μεγάλο όγκο δεδομένων, τα οποία κρατούν αποθηκευμένα στο σκληρό τους δίσκο σε μορφή πακέτων που ονομάζονται "plots" και οι κόμβοι διεκδικούν το λογιστικό δημιουργίας νέων blocks, με τις πιθανότητες τους να αυξάνονται αναλογικά με την ποσότητα πακέτων που έχουν αποθηκευμένα στο δίσκο τους (Nguyen & Kim, 2018). Με τον τρόπο αυτό οι miners δεν είναι υποχρεωμένοι να εκτελούν συνεχώς νέους υπολογισμούς όπως στην περίπτωση του PoW, με αποτέλεσμα ο μηχανισμός συναίνεσής να απαιτεί μικρότερη κατανάλωση ενέργειας. Στην περίπτωση που ένας κόμβος του συστήματος δεν έχει αρκετό αποθηκευτικό χώρο αποκλείεται από τη διαδικασία της συναίνεσης (Gupta & Sadoghi, 2021). Αν και ο σχεδιασμός του αλγορίθμου είναι ανθεκτικός στις κακόβουλες επιθέσεις, ο τρόπος επίτευξης της ομοφωνίας ευνοεί τους κόμβους με το μεγαλύτερο διαθέσιμο αποθηκευτικό χώρο, κάτι το οποίο δημιουργεί προβλήματα στο στόχο της αποκέντρωσης του δικτύου.

4.6.11. **Proof of Burn (PoB)**

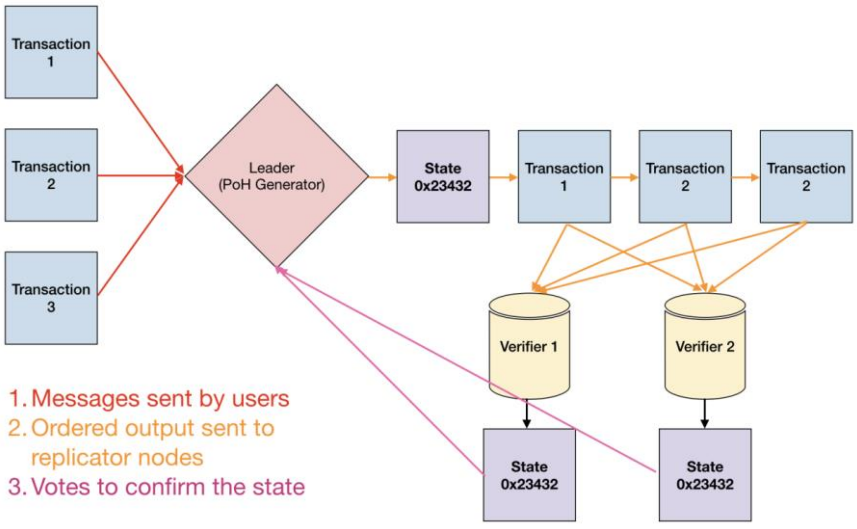
Ο αλγόριθμος Proof of Burn προτάθηκε από τον Iain Stewart το 2012 (Karantias et al., 2020) και έχει χρησιμοποιηθεί για την παραγωγή του κρυπτονομίσματος Slimcoin (P4Titan, 2014). Είναι ένας αλγόριθμος που προσπαθεί να αντιμετωπίσει το ζήτημα της υψηλής κατανάλωσης ενέργειας και της χαμηλής απόδοσης που προκύπτει από τη διαδικασία "εξόρυξης" του μηχανισμού PoW. Οι κόμβοι που μετέχουν στη διαδικασία της "εξόρυξης" στέλνουν νομίσματα σε μια διεύθυνση με την ονομασία "eater address" με σκοπό αυτά να ''καούν'' (coin burning). Όταν φτάσουν σε αυτή τη διεύθυνση δεν μπορούν πλέον να ξαναχρησιμοποιηθούν για κανένα σκοπό, καθώς καταγράφονται σε ένα καθολικό, καθιστώντας τα πραγματικά αχρησιμοποίητα. Επιπλέον, μία τέτοια διεύθυνση δημιουργείται τυχαία και δε διαθέτει ιδιωτικό κλειδί, με αποτέλεσμα κανένας χρήστης να μη μπορεί ποτέ να έχει πρόσβαση στα "καμένα" νομίσματα. Η λειτουργία αυτού του μηχανισμού είναι φαινομενικά μία δαπανηρή διαδικασία για τον χρήστη, αφού αναγκάζεται να καταστρέψει τα assets του, αλλά δεν καταναλώνει πόρους και ενέργεια, κόστη τα οποία επωμίζεται ο ίδιος στην περίπτωση του PoW. Κάθε κόμβος αποκτά το λογιστικό δικαίωμα να δημιουργήσει blocks ανάλογα με το πόσα νομίσματα έχει θυσιάσει στη διαδικασία του "καψίματος" και λαμβάνει αντίστοιχες αμοιβές από το δίκτυο.

Αυτός ο αλγόριθμος δημιουργεί μεγαλύτερη σταθερότητα καθώς οι κόμβοι επιλέγουν να επενδύσουν στο δίκτυο ρισκάροντας νομίσματα και διακινδυνεύοντας μία βραχυπρόθεσμη απώλεια, άρα θα πρέπει να παραμείνουν στο δίκτυο για μεγαλύτερο χρονικό διάστημα για να αποκομίσουν οφέλη. Αυτό ενισχύει την αποκέντρωση και οδηγεί σε ένα καλύτερα κατανεμημένο δίκτυο, κάτι το οποίο σημαίνει ότι ο Proof of Burn είναι μία βελτιωμένη έκδοση του Proof of Work, παρέχοντας περιορισμό των δαπανών που καταβάλουν οι κόμβοι αλλά και

βελτιωμένο τρόπο διανομής των αμοιβών. Ωστόσο, δεν έχει αποδειχθεί ότι μπορεί να λειτουργήσει σε μεγαλύτερες κλίμακες (Yusoff et al., 2022).

4.6.12. **Proof of History (PoH)**

Ο αλγόριθμος Proof of History προτάθηκε από τον Yakovenko (2018) για να χρησιμοποιηθεί στο κρυπτονόμισμα "Solana". Ο αλγόριθμος αυτός λειτουργεί με στόχο την επαλήθευση της χρονικής σειράς των γεγονότων στο δίκτυο, δηλαδή μπορεί να δημιουργήσει ένα ιστορικό από το οποίο μπορεί οι κόμβοι του δικτύου να αποδείξουν πότε συνέβη κάθε γεγονός. Η διαφορά σε σχέση με άλλους μηχανισμούς είναι ότι δεν απαιτεί από τους κόμβους που επικυρώνουν τις συναλλαγές να επικοινωνούν μεταξύ τους, αλλά αντίθετα στην περίπτωση του Proof of History, κάθε επικυρωτής διατηρεί το δικό του τοπικό ρολόι και μέσω κωδικοποίησης η δομή του δικτύου συνδέει όλα τα μηνύματα μεταξύ τους. Αυτή η διαδικασία παρέχει την κρυπτογραφημένη απόδειξη για την πραγματική σειρά των γεγονότων στο δίκτυο, καθώς το δίκτυο είναι σε θέση να αντιμετωπίσει όποιες καθυστερήσεις εμφανίζονται και τα δεδομένα του δικτύου να βρίσκονται πάντα στη σωστή σειρά. Η δομή του δικτύου είναι ικανή να μειώσει το χρόνο επιβεβαίωσης των συναλλαγών, προσφέροντας στο δίκτυο αντικειμενικότητα. Η ροή των δεδομένων σε έναν αλγόριθμο Proof of History αποτυπώνεται στο ***Σχήμα 4-15***. Σύμφωνα με τους Pierro και Tonelli (2022), τα Blockchains που χρησιμοποιούν αυτόν τον μηχανισμό έχουν μεγαλύτερες δυνατότητες επεκτασιμότητας σε σχέση με άλλους PoS μηχανισμούς, έχουν δυνατότητες για επικύρωση χιλιάδων συναλλαγών ανά δευτερόλεπτο και λειτουργούν με χαμηλότερο κόστος.



Σχήμα 4-15: Ροή συναλλαγών στο Blockchain του Solana (Yakovenko, 2018)

4.6.13. **Proof of Exercise (PoX)**

Ο Proof of Exercise είναι ένας μηχανισμός που προσπαθεί να δώσει αξία στην μεγάλη κατανάλωση ενέργειας του μηχανισμού PoW, ανακατευθύνοντας την υπολογιστική ισχύ στην επίλυση πραγματικών επιστημονικών προβλημάτων. Το μηχανισμό αυτό εμπνεύστηκε ο Shoker (2017), ο οποίος περιγράφει ένα σύστημα στο οποίο οι "εργοδότες" (employers) παρέχουν προβλήματα πινάκων (matrix-based) και οι miners αναλαμβάνουν να τα λύσουν. Επειδή τα απαιτούμενα δεδομένα για αυτά τα προβλήματα πρέπει να αποθηκεύονται και να είναι άμεσα διαθέσιμα, ενεργοποιείται ένα "hostage credit" σύστημα συναλλαγών. Αυτό σημαίνει ότι και τα δύο μέρη δεσμεύουν ένα ποσό από τα assets τους, για την εξασφάλιση της βιωσιμότητας του συστήματος, το οποίο λαμβάνουν πίσω με την ολοκλήρωση της διαδικασίας (Bach et al., 2018). Ο employer πρέπει να καταθέσει ένα ποσό, το οποίο να είναι μεγαλύτερο από το κόστος αποθήκευσης των δεδομένων του προβλήματος. Ομοίως, για να λάβει ένας miner ένα πρόβλημα προς επίλυση, πρέπει πρώτα να πλειοδοτήσει για αυτό, καταθέτοντας μια προκαταβολή που θα του επιστραφεί μετά την επιτυχή ολοκλήρωση της επίλυσης. Εάν πολλοί miners κερδίσουν την προσφορά για την επίλυση του ίδιου προβλήματος, η ανταμοιβή για τη λύση θα μοιραστεί μεταξύ τους.

Στη συνέχεια, μετά την ολοκλήρωση της επίλυσης του προβλήματος, η λύση των miners αποστέλλεται στους "ελεγκτές" (verifiers) του συστήματος, οι οποίοι επαληθεύουν τα δεδομένα πριν αυτά καταγραφούν στο blockchain. Για να αποφευχθεί πιθανή συμπαιγνία μεταξύ των συμβαλλόμενων κόμβων (employers, miners, verifiers), τα δεδομένα αποστέλλονται μεταξύ των μερών με τυχαίο τρόπο μέσω αντίστοιχης υπηρεσίας (shuffling service), τόσο κατά τη δημοσίευση των δεδομένων του προβλήματος από τον employer, όσο και κατά την αποστολή των δεδομένων της λύσης προς το verifier. Μειονέκτημα του μηχανισμού Proof of Exercise είναι η μεγάλη του πολυπλοκότητα, που δημιουργεί αρκετές δυσκολίες στην βέλτιστη και εντός χρόνου επίλυση των προβλημάτων που τίθενται από τους employers.

4.6.14. **Proof of Luck (PoL)**

Ο μηχανισμός συναίνεσης Proof of Luck αναπτύχθηκε με στόχο να ξεπεραστούν προβλήματα άλλων μηχανισμών, όπως η μειωμένη απόδοση, η χρήση ενέργειας και η κατανάλωση χρόνου. Είναι ένας μηχανισμός ομοφωνίας που χρησιμοποιεί μία πλατφόρμα TEE (Trusted Execution Environment), όπως η SGX (Software Guard Extensions) της Intel (n.d.), για την παραγωγή ενός αξιόπιστου τυχαίου αριθμού που θα οδηγήσει στην επιλογή ενός ηγέτη για το δίκτυο (Sabt et al., 2015). Ο αλγόριθμος Proof of Luck λειτουργεί με τη χρήση δύο συναρτήσεων, οι οποίες είναι η PoLRound και PoLMine (Milutinovic et al., 2016). Στην αρχή κάθε γύρου, ο συμμετέχων καλεί τη συνάρτηση PoLRound και μεταβιβάζει το πιο πρόσφατο block σε μια συγκεκριμένη αλυσίδα.

Όταν λήξει ο χρόνος του γύρου (round time), ο συμμετέχων καλεί τη συνάρτηση PoLMine για να δημιουργήσει ένα νέο block και να συνδεθεί με το προηγούμενο και η συνάρτηση επιλέγει μία τυχαία τιμή από το εύρος 0 έως 1 (luck value), χρησιμοποιώντας την ομοιόμορφη κατανομή. Η χρήση αυτής της κατανομής διασφαλίζει τον χαρακτήρα "τυχαιότητας" του μηχανισμού. Η τυχαία τιμή που επιλέχθηκε από τη συνάρτηση χρησιμοποιείται για τον προσδιορισμό του νικητή του γύρου. Πιο "τυχερή" άρα και νικήτρια θεωρείται η αλυσίδα με το υψηλότερο άθροισμα "luck values", ξεκινώντας από το πρώτο block (genesis) μέχρι το τελευταίο. Επιπλέον, ο μηχανισμός καθυστερεί την τελική έκδοση κάθε επόμενου block, με την καθυστέρηση αυτή να είναι μικρότερη για τα πιο τυχερά blocks, ώστε να βελτιστοποιείται η επικοινωνία στο δίκτυο.

Ο αλγόριθμος Proof of Luck παρέχει μικρό χρόνο επικύρωσης συναλλαγών (περίπου 15 δευτερόλεπτα), χρησιμοποιεί μικρή υπολογιστική ισχύ και έχει υψηλή ανοσία έναντι της επίθεσης διπλής δαπάνης (double-spending) επειδή ο επιτιθέμενος πρέπει να είναι πολύ τυχερός για να καταφέρει να εκτελέσει μία τέτοια επίθεση (Milutinovic et al., 2016). Ωστόσο, το κύριο πρόβλημα αυτού του πρωτοκόλλου είναι η εξάρτησή του από την Intel, η οποία εξάρτηση είναι τελείως αντίθετη με την αρχή της αποκέντρωσης που πρεσβεύει η τεχνολογία Blockchain (Yusoff et al., 2022). Ένα ακόμα πρόβλημα που αφορά τη λειτουργία του αλγορίθμου είναι ότι το ρολόι του κόμβου θα πρέπει να είναι συγχρονισμένο με το ρολόι του δικτύου, ώστε να συμμετέχει ο κόμβος στο σύνολο του γύρου και να έχει καλύτερες πιθανότητες να κερδίσει.

4.6.15. **Proof of Elapsed Time (PoET)**

Ο Proof of Elapsed Time είναι ακόμα ένα μηχανισμός συναίνεσης που χρησιμοποιεί για τη λειτουργία του μία πλατφόρμα TEE (Trusted Execution Environment), όπως η SGX (Software Guard Extensions) της Intel (n.d.). Ο αλγόριθμος αυτός λειτουργεί παρόμοια με τον Proof of Work, αλλά με χαμηλότερη κατανάλωση ενέργειας (Salimitari & Chatterjee, 2018). Οι miners καλούνται να λύσουν ένα πρόβλημα κατακερματισμού (hash), ωστόσο, αντί για έναν ανταγωνισμό μεταξύ τους για την επίλυση του προβλήματος, ο νικητής επιλέγεται με βάση έναν τυχαίο χρόνο αναμονής. Πιο συγκεκριμένα, ένας χρόνος έχει οριστεί σε κάθε κόμβο για το δικαίωμα της δημιουργίας του επόμενου block και ο νικητής είναι εκείνος του οποίου ο χρόνος θα τελειώσει πρώτος. Αυτή η εξάρτηση από το χρόνο μειώνει τον ανταγωνισμό υπολογιστικής ισχύος μεταξύ των συμμετεχόντων. Όταν η δημιουργία του νέου block ολοκληρωθεί, για να εγκριθεί από το υπόλοιπο δίκτυο, ο κόμβος που το δημιούργησε καλείτε να αποδείξει ότι αυτό δε συνέβη πρόωρα, μέσω εξωτερικής υπηρεσίας πιστοποιήσεων (της Intel), κάτι το οποίο καθιστά το μηχανισμό Proof of Elapsed Time μερικώς και όχι πλήρως αποκεντρωμένο. Η διαδικασία λειτουργίας του μηχανισμού αυτού παρέχει στους κόμβους μία μορφή δικαιοσύνης και ισότητας.

Τα όρια ασφαλείας του μηχανισμού έχουν ελεγχθεί από τους Chen et al. (2017) και στη μελέτη τους αποδείχθηκε ότι το σύστημα είναι ευάλωτο αν οι κακόβουλοι κόμβοι ξεπεράσουν ένα ποσοστό που μεταβάλλεται ανάλογα με το σύνολο των κόμβων, με λογαριθμική συσχέτιση. Άμυνα απέναντι στους κακόβουλους κόμβους αποτελεί το ότι το ίδιο το σύστημα κάνει καταμέτρηση των νικών κάθε κόμβου, οπότε είναι εύκολο ο εντοπισμός ενεργειών χειραγώγησης. Το κύριο μειονέκτημα της προσέγγισης του Proof of Elapsed Time είναι η εξάρτησή του από την πλατφόρμα της Intel, η οποία έρχεται σε σύγκρουση με τη βασική φιλοσοφία της πλήρους αποκέντρωσης του Blockchain (Salimitari & Chatterjee, 2018).

4.6.16. **Proof of Trust (PoT)**

Ο Proof of Trust είναι ένας αλγόριθμος συναίνεσης που στηρίζεται στον εκλογικό αλγόριθμο με την ονομασία "Raft" (Bakhoff, 2010). Για να επιτευχθεί η απαιτούμενη συναίνεση, ο μηχανισμός λειτουργεί σε ένα δημόσιο δίκτυο blockchain, ενσωματώνοντας μέσα σε αυτό ένα δίκτυο blockchain κοινοπραξίας, το οποίο ελέγχει τις διαδικασίες του μηχανισμού (Zou et al., 2018). Ο αλγόριθμος λαμβάνει εντολή από έναν πελάτη (client) και η εντολή αυτή εκτελείται μόνο αν υπάρξει συναίνεση μεταξύ του μεγαλύτερου μέρους των κόμβων του συστήματος.

Κάθε γύρος της διαδικασίας συναίνεσης απαιτεί την εκτέλεση τεσσάρων φάσεων (Ongaro & Ousterhout, 2015). Στην πρώτη φάση θα πρέπει η ομάδα διαχείρισης του blockchain κοινοπραξίας, να εκλέξει έναν κόμβο, ο οποίος θα είναι ο μοναδικός "Ηγέτης" (Leader) της ομάδας. Εκτός από τον ηγέτη, που είναι υπεύθυνος για την επίβλεψη και τη διαχείριση όλων των αλληλεπιδράσεων του συστήματος, υπάρχουν ακόμα οι "Υποψήφιοι" (Candidates), που αναμένουν την εκλογή για να γίνουν ηγέτες και οι "Ακόλουθοι" (Followers), οι οποίοι είναι παθητικοί χρήστες και αναμένουν από τους Leader κλήσεις με την ονομασία "Remote Procedure Calls", με τις οποίες ο ηγέτης επικοινωνεί με το υπόλοιπο δίκτυο. Στη δεύτερη φάση του μηχανισμού Proof of Trust, ο ηγέτης φτιάχνει μία λίστα από κόμβους, με βάση κριτήρια όπως π.χ. τον βαθμό εμπιστοσύνης (trust value) του δικτύου σε αυτούς και από αυτή τη λίστα διαλέγει κάποιους ως ομάδα επικυρωτών (service transaction validation group). Στην τρίτη φάση η ομάδα επικυρωτών καλείται να επιλέξει τις συναλλαγές που θα αποτελέσουν το επόμενο block. Τέλος, στην τέταρτη φάση, η ομάδα εκλέγει εκ νέου τις συναλλαγές και ο ηγέτης αναλαμβάνει την αξιολόγηση και την εγκατάσταση του νέου block. Κάθε γύρος συναίνεσης ξεκινάει με την εκλογή του ηγέτη και τελειώνει με την εκτέλεση της εντολής αυτού.

Ο μηχανισμός συναίνεσης Proof of Trust μπορεί να αξιοποιηθεί σε ένα ιδιωτικό δίκτυο, καθώς απαιτεί για την αποδοτική λειτουργία του, εμπιστοσύνη μεταξύ των συμμετεχόντων. Έχει καλύτερες δυνατότητες επεκτασιμότητας σε σχέση με άλλους μηχανσιμούς και παρέχει τη δυνατότητα διανεμημένης διακυβέρνησης (Zou et al., 2018).

4.6.17. **Proof of Authentication (PoAh)**

Ο Proof of Authentication είναι ακόμα ένας μηχανισμός συναίνεσης που προσπαθεί να βελτιώσει την ενεργειακή κατανάλωση του PoW, με τη χρήση μίας διαδικασίας επαλήθευσης. Παρουσιάστηκε από τους Puthal et al. (2019) και διαχωρίζει τους συμμετέχοντες κόμβους του συστήματος σε δύο κατηγορίες: α) individual και β) trusted. Οι κόμβοι που ανήκουν στην πρώτη κατηγορία δημιουργούν τα blocks των συναλλαγών, τα οποία στη συνέχεια αποστέλλουν στους κόμβους της δεύτερης κατηγορίας προς αξιολόγηση. Οι trusted κόμβοι του συστήματος κάνουν την αξιολόγηση και με βάση το επίπεδο "εμπιστοσύνης" που τους παρέχεται από όλο το δίκτυο ολοκληρώνουν τη διαδικασία επαλήθευσης στέλνοντας πίσω στους κόμβους την τελική έκδοση των blocks. Σύμφωνα με τους Maitra et al. (2020) ο Proof of Authentication βελτιώνει σημαντικά το χρόνο αναμονής και την κατανάλωση ενέργειας, ωστόσο θα πρέπει να δοκιμαστεί και σε Blockchains με πολύ μεγαλύτερο αριθμό κόμβων.

4.6.18. **Proof of Vote (PoV)**

Ο μηχανισμός συναίνεσης Proof of Vote, αποτελεί μία μορφή του μηχανισμού Proof of Work, προτάθηκε από τους Li et al. (2017) και εφαρμόζεται αποκλειστικά σε δίκτυα κοινοπραξίας (consortium Blockchains). Σύμφωνα με τους δημιουργούς του, αναπτύχθηκε με γνώμονα την υψηλή ασφάλεια και απόδοση και τη χαμηλή κατανάλωση ενέργειας. Η διαδικασία συναίνεσης του συστήματος βασίζεται σε ένα μηχανισμό ψηφοφορίας, για τις ανάγκες του οποίου, οι κόμβοι του συστήματος χωρίζονται σε 4 κατηγορίες με τις αντίστοιχες αρμοδιότητες: α) απλός χρήστης (ordinary user), β) υποψήφιος βοηθός (butler candidate), γ) βοηθός (butler) και δ) επίτροπος (commissioner). Ο αλγόριθμος Proof of Vote απαιτεί μόλις μία επιβεβαίωση για την επικύρωση των νέων blocks, άρα το μεγάλο του πλεονέκτημα είναι η άμεση λειτουργία του συστήματος, καθώς απαιτούνται 15 δευτερόλεπτα για τη δημιουργία κάθε νέου block, χρόνος κατά πολύ ταχύτερος από αυτόν που παρέχει ο PoW.

4.6.19. **Proof of Humanity (PoH)**

Ο αλγόριθμος Proof of Humanity είναι επίσης μία νέα πρόταση αλγορίθμου και αφορά τη συγκέντρωση συνεισφορών για την επίλυση προβλημάτων που σχετίζονται με την κοινωνία (Arjomandi-Nezhad et al., 2021). Στη διαδικασία συναίνεσης που έχει σχεδιαστεί, η πιθανότητα ένας κόμβος να αποκτήσει το λογιστικό δικαίωμα για τη δημιουργία νέων blocks εξαρτάται από το ποσό της δωρεάς του κόμβου στο δίκτυο. Επιπλέον, οι κόμβοι μπορούν να συνάψουν "έξυπνα" συμβόλαια και να εκτελέσουν συναλλαγές, με αντίστοιχα τέλη συναλλαγής. Κατά τη διάρκεια της διαδικασίας του αλγορίθμου, δημιουργείται ένα "έξυπνο" συμβόλαιο που περιέχει: α) μία διεύθυνση πληρωμής, η οποία είναι η διεύθυνση στην οποία οι συμμετέχοντες κόμβοι μπορούν να κάνουν δωρεές σε ολόκληρο το δίκτυο, και β) μία βαθμολογία φήμης

(reputation score), η οποία αντιπροσωπεύει την εμπιστοσύνη του κοινού σε ολόκληρο το δίκτυο. Η πιθανότητα ένας κόμβος να αποκτήσει το λογιστικό δικαίωμα στο δίκτυο είναι ίση με το κλάσμα των συνολικών δωρεών του προς τις συνολικές δωρεές που έλαβε το δίκτυο. Προκειμένου να διατηρηθεί η ασφαλής και σταθερή λειτουργία του δικτύου Blockchain, ο αλγόριθμος Proof of Humanity χρησιμοποιεί έναν κατανεμημένο αλγόριθμο τυχαίων μεταβλητών για να διασφαλίσει ότι ο κόμβος επιλέγεται τυχαία και δεν μπορεί να προβλεφθεί από κανέναν. Αυτός ο αλγόριθμος είναι πιο κατάλληλος για σενάρια κοινωνικής φορολογίας, όπως π.χ. για την κάλυψη αναγκών φιλανθρωπικών οργανώσεων (Xiong et al., 2022).

4.6.20. Άλλοι μηχανισμοί συναίνεσης

Οι παραπάνω μηχανισμοί συναίνεσης είναι μόνο ένα μικρό δείγμα από το σύνολο των μηχανισμών που έχουν προταθεί στην παγκόσμια βιβλιογραφία και ο αριθμός αυξάνεται συνεχώς. Όμως μόνο ένα πάρα πολύ μικρό ποσοστό των μηχανισμών συναίνεσης που υπάρχουν, έχουν βρει τη θέση τους σε κάποια πρακτική εφαρμογή μέχρι τώρα. Έως τώρα, οι τρεις κυρίως χρησιμοποιούμενοι μηχανισμοί συναίνεσης είναι ο Proof of Work, ο Proof of Stake και ο Practical Byzantine Fault Tolerance και ουσιαστικά όλοι οι υπόλοιποι είναι τροποποιημένες μορφές αυτών. Στη συνέχεια ακολουθεί η ενδεικτική καταγραφή μερικών ακόμη σύγχρονων και παλαιότερων μηχανισμών, που είναι ένα μόνο ένα μικρό μέρος από αυτούς που αναφέρονται στην παγκόσμια βιβλιογραφία.

- Proof of Useful Work: Χρησιμοποιεί πόρους των miners για την εκπαίδευση μοντέλων μηχανικής μάθησης (Baldominos & Saez, 2019)
- Tendermint: Παρόμοια διαδικασία συναίνεσης με τον PBFT, αλλά οι κόμβοι πρέπει να κλειδώσουν τα νομίσματά τους για να γίνουν επικυρωτές (Kwon, 2014).
- Proof of Familiarity: Σχεδιάστηκε για εφαρμογή στην ιατρική περίθαλψη για την καταγραφή ιατρικών αποφάσεων (Yang et al., 2019).
- Proof of Familiarity and Existence: Συνδυάζει τις δυνατότητες των δύο αντίστοιχων αλγορίθμων (Sheela & Priya, 2022).
- Proof of Learning: Παραλλαγή του Proof of Useful Work, όπου κάθε κόμβος δεν χρειάζεται να εκτελεί την ίδια εργασία (Bravo-Marquez et al., 2019)
- Proof of Participation: Χρησιμοποιεί μία τεχνητή δυσκολία για την εύρεση της τιμής hash, η οποία είναι μικρότερη από του PoW και μεγαλύτερη από του PoS (Nandwani et al., 2019).
- Proof of Contribution: Ποσοτικοποιεί τις συμπεριφορές χρηστών ως τιμές συνεισφοράς στο δίκτυο (Song et al., 2021).
- Proof of Solution: Εξέλιξη του Proof of Useful Work που μειώνει στο μισό την εκπαίδευση μοντέλων μέσω πολλαπλών κόμβων (Kiran et al., 2021).

- Proof of Distance: Συνδυάζει τους Proof of Stake και Proof of Importance (Zhang et al., 2020).
- Ouroboros: Μηχανισμός PoS με αυστηρότερες εγγυήσεις ασφάλειας (Kiayias et al., 2016)
- Proof of Interaction: Βελτίωση του PoW, που λειτουργεί μόνο στην περίπτωση που οι κόμβοι του συστήματος δεν είναι ανώνυμοι (Abegg et al., 2021).
- Proof of Credit: Ειδική μορφή PoS, όπου ποσοτικοποιείται η αξία της δραστηριότητας του κόμβου στο σύστημα (Han et al., 2019).
- Proof of Believability: Αξιολογεί συνολικά την αξιοπιστία των κόμβων, λαμβάνοντας υπόψιν την ποσότητα των assets, τη συμμετοχή στην κοινότητα και τη συμπεριφορά στο δίκτυο (Send, 2017).
- Ripple: Προτάθηκε για χρήση σε οικονομικές συναλλαγές με τη χρήση αξιόπιστων υπο-δικτύων μέσα σε ένα μεγαλύτερο δίκτυο Blockchain (Schwartz et al., 2014).
- Proof of Existence: Διασφαλίζει ότι ένα ψηφιακό έγγραφο υπάρχει πραγματικά σε μία δεδομένη χρονικής στιγμή (Chopra et al., 2019)
- Proof of Replication: Χρησιμοποιείται σε συστήματα Blockchain, με στόχο να διασφαλιστεί ότι τα αποθηκευμένα δεδομένα δεν έχουν αλλοιωθεί (Benet, 2017).
- GHOST: Αντικαθιστά τον κανόνα της μακρύτερης αλυσίδας, προτείνοντας ένα νέο τρόπο δημιουργίας block (Sompolinsky & Zohar, 2015)
- HoneyBadgerBFT: Λύνει το πρόβλημα χρονικού ορίου που προκαλείται από την καθυστέρηση δικτύου (Miller et al., 2016).
- Simplified Byzantine Fault Tolerance: Στηρίζει τη λειτουργία του αποκλειστικά στην εμπιστοσύνη μεταξύ των κόμβων (Kiayias & Russell, 2018).
- Stellar (SCP): Βυζαντινό πρωτόκολλο, όπου ο κάθε κόμβος επιλέγει ο ίδιος ποιους κόμβους θα εμπιστευτεί (Mazieres, 2015).
- CW-PoW (Compute and Wait): Μορφή του PoW που λειτουργεί με διαφορετικούς γύρους επίλυσης (Kara et al., 2021).
- Bitcoin-NG: Μορφή του PoW που χρησιμοποιεί μικρότερα blocks για να βελτιώσει την απόδοση του συστήματος (Eyal et al., 2016).
- Byzcoin: Βασίζεται στον Bitcoin-NG και συνδυάζει τον PoW με τον PBFT (Karkhanis, 2019).
- VRF (Verifiable Random Function): Βασίζεται στο DPoS και προσθέτει εικονικούς κόμβους για να αυξήσει την αβεβαιότητα στην εκλογική διαδικασία (Bitansky, 2020).
- LaKSA (Large-scale Known-committee Stake-based Agreement): Μορφή του PoS που βελτιώνει την ταχύτητα συναλλαγής και μειώνει τον κίνδυνο επιθέσεων μεγάλης εμβέλειας (Reijsbergen et al., 2020).
- Proof of Stake Velocity: Είναι μία εναλλακτική των PoW και PoS, που ασφαλίζει το Peer-to-Peer δίκτυο (Ren, 2014).

- Casper: Συνδυάζει τον PoW και τον PoS για να εξασφαλίσει ασφάλεια και να μειώσει την κατανάλωση ενέργειας (Buterin & Griffith, 2017).
- Algorand: Μορφή του PoS με υψηλή αποκέντρωση και μειωμένο χρόνο συναλλαγών (Gilad et al., 2017).
- SBFT: Λύνει προβλήματα επεκτασιμότητας (scalability) των βυζαντινών αλγορίθμων (Gueta et al., 2019).
- Thunderella: Αναπαράγει τις λειτουργίες των έντιμων κόμβων του συστήματος, μειώνοντας την επαναλαμβανόμενη εργασία (Pass & Shi, 2018).
- SG-PBFT: Αναδιαμόρφωση της λειτουργίας του PBFT με μηχανισμό κλασματικής ομαδοποίησης (Xu et al., 2022)

4.7. Smart Contracts

"Έξυπνο" συμβόλαιο (smart contract) ονομάζεται ένα αυτοεκτελούμενο συμβόλαιο που χρησιμοποιεί την τεχνολογία Blockchain για την ψηφιακή εφαρμογή και επαλήθευση των όρων του. Η ιδέα για την δημιουργία των "έξυπνων" συμβολαίων εμφανίστηκε για πρώτη φόρα από τον Nick Szabo τη δεκαετία του 1990 (Szabo, 1994), ο οποίος οραματίστηκε συμβόλαια γραμμένα σε κώδικα υπολογιστή, όπου με την χρήση ψηφιακών τεχνολογιών, θα ήταν αξιόπιστα και αυτοεκτελούμενα (self-executing), έτσι ώστε να ελαχιστοποιηθεί η ανάγκη για αξιόπιστους μεσάζοντες μεταξύ των συναλλασσόμενων μερών (Szabo, 1997). Στόχος αυτού του τρόπου επιβολής συμφωνιών, είναι η ενίσχυση της αποτελεσματικότητα τους και η εξάλειψη των διχογνωμιών και των κακόβουλων ενεργειών που απορρέουν από τα συμβατικά συμβόλαια (De Filippi et al., 2021). Ο Szabo χρησιμοποιούσε ως παράδειγμα τη χρήση "έξυπνου" συμβολαίου για την ενοικίαση ενός αυτοκινήτου, το δικαίωμα χρήσης του οποίου θα επέστρεφε αυτόματα πίσω στον ιδιοκτήτη του, όταν ένας ενοικιαστής ολοκλήρωνε τις πληρωμές. Η υλοποίηση της ιδέας του Szabo υπήρξε ουσιαστικά αδύνατη και δεν ωρίμασε ποτέ, έως και την εμφάνιση της τεχνολογίας Blockchain, καθώς δεν μπορούσε να αντιμετωπίσει το πρόβλημα του "double-spending". Μέσω του Blockchain παρέχεται ουσιαστικά η ευκαιρία για την υλοποίηση των smart contracts στην πράξη, καθώς μέσω των τεχνολογικών δυνατοτήτων που προσφέρει, ένα "έξυπνο" συμβόλαιο είναι σε θέση να εκτελεί αυτόματα τις συμφωνίες που έχουν προκαθοριστεί εκ των προτέρων, όταν πληρούνται ορισμένες συνθήκες ενεργοποίησης (Peng et al., 2021).

Ένας ορισμός για τα "έξυπνα" συμβόλαια που μπορεί να βρεθεί στη βιβλιογραφία, είναι ότι αποτελούν ψηφιακά συμβόλαια που επιτρέπουν όρους, οι οποίοι εξαρτώνται από αποκεντρωμένη συναίνεση, είναι απαραβίαστοι και συνήθως επιβάλλονται μέσω αυτοματοποιημένης εκτέλεσης (Cong & He, 2019). Το κύριο χαρακτηριστικό των έξυπνων

συμβολαίων είναι ότι λόγω της χρήσης της τεχνολογίας Blockchain, λειτουργούν μέσω δικτύων Peer-to-Peer, χωρίς την παρέμβαση ενός τρίτου μέρους και χωρίς καμία κεντρική εξάρτηση (Hewa et al., 2021). Αποτελούν αυτόνομα προγράμματα λογισμικού που όταν ενεργοποιούνται, εκτελούν αυτόματα και υποχρεωτικά τους κανόνες και τις συνθήκες που τίθενται κατά την εφαρμογή τους. Μπορεί να στοχεύουν στην επιβολή μιας συμφωνίας, στην εκπλήρωση μιας νομικής σύμβασης, στην εκτέλεση μιας συναλλαγής ή στην επαλήθευση μίας διαδικασίας. Μέσω της ασφάλειας και του αποκεντρωμένου συστήματος, που παρέχει η τεχνολογία Blockchain, τα "έξυπνα" συμβόλαια μπορούν να ενισχύσουν την αξιοπιστία των συναλλαγών μεταξύ συμβαλλομένων μερών χωρίς την ανάγκη διαμεσολαβητών, οι οποίοι είναι απαραίτητοι για τη σύναψη συμβατικών συμβολαίων ή συμβάσεων (Christidis & Devetsikiotis, 2016). Μπορούν λοιπόν να αντικαταστήσουν τις παραδοσιακές αυτές μορφές καταγραφής των συμφωνιών σε μια προσπάθεια να μειωθεί σημαντικά το κόστος τους και ταυτόχρονα να προωθηθεί η ασφάλεια των συναλλαγών, η αποτελεσματικότητα και η μείωση των παραβιάσεων των ορών των συμβολαίων (Swan, 2015; Zheng et al., 2020).

Σύμφωνα τους Hewa et al. (2021) τα βασικά χαρακτηριστικά των "έξυπνων" συμβολαίων μπορούν να κατηγοριοποιηθούν ως εξής:

- Κατάργηση της ανάγκης για αξιόπιστο τρίτο μέρος: Επιτρέπεται η αυτόνομη εκτέλεση των προκαθορισμένων όρων και η αποκεντρωμένη λειτουργία του δικτύου αποδεσμεύει την ανάγκη για τη διαμεσολάβηση ενός αξιόπιστου τρίτου μέρος, ενώ εξαλείφει και τις καθυστερήσεις.
- Προστασία κατά της πλαστογραφίας: Η ακεραιότητα της κάθε συναλλαγής και του κάθε block στο κατανεμημένο καθολικό επαληθεύεται με τις ψηφιακές υπογραφές. Το αρχείο συναλλαγών και η υπολογιστική λογική της εκτέλεσης, επαληθεύονται κρυπτογραφικά και παραμένουν μόνιμα στο δίκτυο, με αποτέλεσμα να αποτρέπεται η πλαστογραφία.
- Διαφάνεια: Η διαφάνεια των συναλλαγών είναι δεδομένη, καθώς το καθολικό του δικτύου και η λογική των "έξυπνων" συμβολαίων είναι ορατή σε όλα τα μέρη του συστήματος Blockchain.
- Αυτόνομη εκτέλεση: Η προγραμματισμένη συνθήκη και η ροή των γεγονότων που ορίζονται από το "έξυπνο" συμβόλαιο, εκτελούνται με επιτυχία μόλις το σύστημα φτάσει στην κατάσταση ενεργοποίησης, όπως αυτή έχει οριστεί κατά συμφωνία όλων των μερών.
- Ακρίβεια: Οι προγραμματισμένοι όροι στα "έξυπνα" συμβόλαια είναι αμετάβλητοι και επαληθεύονται πριν από το διαμοιρασμό τους στους κόμβους του δικτύου. Η ακρίβεια κατά την εκτέλεση τους είναι εγγυημένη, χωρίς ανθρώπινο ή άλλο σφάλμα, με αποτέλεσμα να εκλείπουν τα μεροληπτικά φαινόμενα και να βελτιώνεται η εμπιστοσύνη.

Τα "έξυπνα" συμβόλαια μπορούν να χρησιμοποιηθούν σε διάφορες εφαρμογές, όπως στις χρηματοοικονομικές συναλλαγές, στην ιχνηλασιμότητα των προϊόντων και στην προστασία της πνευματικής ιδιοκτησίας και για αυτό το λόγο αυξάνεται συνεχώς ο αριθμός των εταιρειών που τα χρησιμοποιούν, ενώ εντοπίζονται και νέες δυνατότητες χρήσης. Ωστόσο, για την ικανοποίηση των υψηλών απαιτήσεων απόδοσης και ασφάλειας, οι πλατφόρμες οι οποίες αναπτύσσουν την τεχνολογία Blockchain, πάνω στην οποία λειτουργούν αυτά, θα πρέπει να είναι καλά σχεδιασμένες και να έχουν δοκιμαστεί διεξοδικά (Destefanis et al., 2018). Κύριο όφελος της ανάπτυξης "έξυπνων" συμβολαίων μέσω του Blockchain είναι ότι το ίδιο το Peer-to-Peer δίκτυο εγγυάται στις δύο πλευρές, ότι οι συμβατικοί όροι της συμφωνίας δεν μπορούν να τροποποιηθούν. Το Blockchain καθιστά αδύνατη την παραβίαση των συμβατικών όρων και για αυτό το λόγο τα "έξυπνα" συμβόλαια αναμένεται να επιφέρουν μείωση του κόστους επαλήθευσης, εκτέλεσης και διαμεσολάβησης των συμβολαίων, καθώς και του κόστους πρόληψης απάτης για αυτά. Για παράδειγμα, τα "έξυπνα" συμβόλαια μπορούν να είναι χρήσιμα για την αντιμετώπιση του προβλήματος του "ηθικού κινδύνου", ο οποίος εμφανίζεται σε περιπτώσεις ασφάλειας υγείας σε βάρος των ασφαλιστικών εταιρειών (Sangeetha et al., 2020).

4.7.1. Λειτουργία Smart Contracts

Τα "έξυπνα" συμβόλαια λειτουργούν ως μηχανογραφημένα προγράμματα που επιτρέπουν την αυτοματοποιημένη εκτέλεση μίας συγκεκριμένης ενέργειας, με την προϋπόθεση ότι πληρούνται ορισμένες προϋποθέσεις (Dutta et al., 2020; Lu, 2019). Είναι μία ψηφιακά υπογεγραμμένη συμφωνία μεταξύ δύο ή περισσότερων μερών, όπου ένα λογισμικό χωρίς καμία προκατάληψη, μπορεί να εκτελέσει και να επιβάλει τους όρους της συμφωνίας στα αντισυμβαλλόμενα μέρη. Θεωρούνται ως ένα από τα πιο κρίσιμα στοιχεία στο σχεδιασμό και την εφαρμογή των συστημάτων Blockchain (Chang et al., 2019) και αποτελούν έναν αυτόματο μηχανισμό εγγύησης για τον χρήστη (Lu, 2019).

Το Blockchain μόνο του, υποστηρίζει συναλλαγές επιτρέποντας τη μεταφορά assets μεταξύ αντισυμβαλλομένων που δεν εμπιστεύονται ο ένας τον άλλον. Ωστόσο, ένα Blockchain που υποστηρίζει τη δυνατότητα ανάπτυξης "έξυπνων" συμβολαίων προχωρά ένα βήμα περισσότερο και επιτρέπει την πραγματοποίηση διαδικασιών πολλαπλών βημάτων ή αλληλεπιδράσεων, μεταξύ αμοιβαία δύσπιστων αντισυμβαλλομένων. Οι συναλλασσόμενες οντότητες μπορούν να επιθεωρήσουν τον κώδικα και να προσδιορίσουν τα αποτελέσματά του πριν αποφασίσουν να συμμετάσχουν στη συμφωνία, να είναι σίγουροι ότι λόγω της αποκεντρωμένης, άρα αμερόληπτης φύσης του δικτύου, το συμβόλαιο το συμβόλαιο θα εκτελεστεί κανονικά και τέλος να επαληθεύουν όλες τις διαδικασίες, καθώς όλες οι αλληλεπιδράσεις είναι ψηφιακά υπογεγραμμένες. Οι συναλλαγές που γίνονται μέσω των

"έξυπνων" συμβολαίων λειτουργούν ως δομές δεδομένων που υποδεικνύουν μία μεταφορά assets από μία οντότητα σε άλλη (Antonopoulos, 2014).

Στο πλαίσιο του Blockchain, ένα "έξυπνο" συμβόλαιο είναι ένα πρόγραμμα που καθοδηγείται από τα γεγονότα των επικυρώσεων των συναλλαγών του δικτύου και λειτουργεί πάνω στο ίδιο κοινόχρηστο καθολικό στο οποίο καταγράφονται τα assets που αφορούν το συμβόλαιο. Ουσιαστικά, είναι ένα σενάριο που αποθηκεύεται στο Blockchain και έχει μία διεύθυνση μέσα σε αυτό. Η εκτέλεση κάθε συμβολαίου καταγράφεται ως αμετάβλητη συναλλαγή και αποθηκεύεται στο Blockchain. Όλες οι πληροφορίες των συναλλαγών που υπάρχουν σε ένα "έξυπνο" συμβόλαιο αποθηκεύονται στην αποκεντρωμένη βάση δεδομένων που διατηρείται δημόσια με ασφαλή τρόπο, και αυτό έχει σαν αποτέλεσμα τα "έξυπνα" συμβόλαια να είναι ανιχνεύσιμα και μη αναστρέψιμα (Mohanta et. al, 2018). Ένα "έξυπνο" συμβόλαιο ενεργοποιείται όταν αποσταλεί μία συναλλαγή στη διεύθυνση του, και στη συνέχεια εκτελείται ανεξάρτητα και αυτόματα με τον τρόπο που έχει προκαθοριστεί, και πάντα σύμφωνα με τα δεδομένα που συμπεριλήφθηκαν στη συναλλαγή ενεργοποίησης (Christidis & Devetsikiotis, 2016). Με αυτό τον τρόπο, δίνει στο Blockchain τη δυνατότητα να διαχειρίζεται αλληλεπιδράσεις μεταξύ οντοτήτων, βάσει των πραγματικών δεδομένων που βρίσκονται στο δίκτυο.

Τα κύρια μέρη που περιλαμβάνει ένα "έξυπνο" συμβόλαιο, είναι οι μεταβλητές κατάστασης (state variables), οι λειτουργίες (functions) και τα συμβάντα (events), με σκοπό να εκτελεί ενέργειες και να ελέγχει σχετικά γεγονότα σύμφωνα με τους όρους του συμβολαίου (Frantz & Nowostawski, 2016). Συμφώνα με τον Buterin (2014) διακρίνονται δύο τύποι μεταβλητών κατάστασης: α) οι σταθερές μεταβλητές κατάστασης, οι οποίες ποτέ δεν μπορούν να αλλάξουν, και β) οι μεταβλητές κατάστασης με δυνατότητα εγγραφής στο δίκτυο του Blockchain. Οι λειτουργίες διακρίνονται σε λειτουργίες ανάγνωσης, οι οποίες εκτελούνται ελεύθερα, και σε λειτουργίες εγγραφής, οι οποίες συνήθως απαιτούν την καταβολή κάποιου είδους φόρου (ανάλογα με το δίκτυο) επειδή επιφέρουν αλλαγές των μεταβλητών κατάστασης, άρα πρέπει να επικυρωθούν σε ένα νέο block του Blockchain. Η διαδικασία κατασκευής ενός "έξυπνου" συμβολαίου ξεκινάει με την ανάρτηση (host) του στο δίκτυο του Blockchain, η οποία ενεργοποιείται με την κλήση της κατασκευαστικής λειτουργίας μέσω μιας συναλλαγής (transaction). Ο αποστολέας αυτής της συναλλαγής, γίνεται ο ιδιοκτήτης του "έξυπνου" συμβολαίου και λαμβάνει τις επιστρεφόμενες παραμέτρους, όπως την μοναδική διεύθυνση συμβολαίου. Στη συνέχεια οι χρήστες μπορούν να επικαλεστούν οποιαδήποτε διαθέσιμη λειτουργία του έξυπνου συμβολαίου στέλνοντας μία συναλλαγή. Υπάρχει ακόμα η δυνατότητα της λειτουργίας αυτοκαταστροφής, την οποία συνήθως μπορεί να χρησιμοποιήσει μόνο ο

ιδιοκτήτης του "έξυπνου" συμβολαίου, άρα να καταστρέψει το συμβόλαιο με την κλήση αυτής της λειτουργίας.

Οι βασικές λειτουργίες συναλλαγής που παρέχει ένα "έξυπνο" συμβόλαιο στους χρήστες, είναι η κατάθεση (deposit), η ανταλλαγή (trade) και η ανάληψη (withdrawal) (Christidis & Devetsikiotis, 2016). Η λειτουργία της κατάθεσης δίνει στο χρήστη τη δυνατότητα να μεταφέρει μία ποσότητα ενός asset που διαθέτει, προς τη διεύθυνση ενός συμβολαίου, δηλαδή να δεσμεύσει κάτι σε αυτό, και η λειτουργία της ανάληψης του επιτρέπει να λάβει μία ποσότητα ενός asset από ένα συμβόλαιο, δηλαδή να αποδεσμεύσει κάτι από αυτό. Η λειτουργία της ανταλλαγής είναι η πιο κρίσιμη λειτουργία, η οποία εκτελείται αυτόματα δεσμεύοντας και αποδεσμεύοντας assets από και προς χρήστες, ανάλογα με τις συναλλαγές που εκτελούνται και καταγράφονται στο καθολικό. Η λειτουργία της ανταλλαγής, παρέχει τη δυνατότητα στον προγραμματιστή να εκφράσει μία επιχειρηματική λογική, κατά το σχεδιασμό του συμβολαίου, το οποίο και αποτελεί το λόγο της μεγάλης χρησιμότητας των "έξυπνων" συμβολαίων για το Blockchain. Για τις λειτουργίες κατάθεσης και ανάληψης μπορεί να έχει γραφτεί στον κώδικα, είτε ότι ένας χρήστης είναι ο μόνος που μπορεί να τις ενεργοποιήσει μέσω του κλειδιού του, είτε ότι υπάρχει η δυνατότητα να μπορούν να ενεργοποιηθούν και από όποιον άλλο χρήστη επιθυμεί ο συντάκτης του συμβολαίου. Οι κινήσεις που εκτελούνται σε όλες τις λειτουργίες ενός "έξυπνου" συμβολαίου καταγράφονται στο Blockchain και όλοι οι συμμετέχοντες στο δίκτυο λαμβάνουν ένα κρυπτογραφικά επαληθεύσιμο ίχνος των λειτουργιών του. Αντίστοιχα, στο Blockchain είναι καταγεγραμμένος και ο κώδικας του συμβολαίου, οπότε μπορεί να επιθεωρηθεί από κάθε συμμετέχοντα στο δίκτυο.

Οι παραπάνω γενικοί κανόνες του τρόπου λειτουργίας ενός "έξυπνου" συμβολαίου, δείχνουν ότι ένα συμβόλαιο αποτελεί μία οντότητα μέσα στο Blockchain, όπως και οι κανονικοί κόμβοι του δικτύου, και ως οντότητα, το συμβόλαιο έχει τη δυνατότητα να έχει στην κατοχή του assets (Christidis & Devetsikiotis, 2016). Ένα σωστά γραμμένο "έξυπνο" συμβόλαιο θα πρέπει να περιγράφει όλα τα πιθανά αποτελέσματα των συμφωνηθέντων, για να είναι σε θέση να λαμβάνει αποφάσεις, ακόμα και για συναλλαγές που δεν εκπληρώνουν όρους της συμφωνίας, και να επιστρέφει assets, μερικώς ή ολικώς, πίσω στους χρήστες. Όταν λοιπόν λαμβάνονται υπόψη όλα τα πιθανά αποτελέσματα, η πιθανότητα διαφωνίας εξαλείφεται, καθώς οι συμμετέχοντες δεν μπορούν να διαφωνήσουν σχετικά με το τελικό αποτέλεσμα αυτής της επαληθεύσιμης διαδικασίας στην οποία συμμετείχαν. Επίσης θα πρέπει το συμβόλαιο να είναι ντετερμινιστικό, δηλαδή η ίδια είσοδος να παράγει πάντα την ίδια έξοδο. Εάν κάποιος γράψει ένα μη ντετερμινιστικό συμβόλαιο, όταν αυτό ενεργοποιηθεί θα εκτελεστεί σε κάθε κόμβο του δικτύου και μπορεί να επιστρέψει διαφορετικά αποτελέσματα, εμποδίζοντας έτσι το δίκτυο να καταλήξει σε συναίνεση σχετικά με το αποτέλεσμα εκτέλεσής του. Σε μια σωστά

κατασκευασμένη πλατφόρμα Blockchain, η σύνταξη μη ντετερμινιστικών "έξυπνων" συμβολαίων είναι συνήθως αδύνατη, λόγω της γλώσσας προγραμματισμού που χρησιμοποιείται, αλλά ακόμα και αν είναι δυνατή, μία προσπάθεια ανάπτυξης μιας τέτοιας συμφωνίας θα απορριφθεί από το υπόλοιπο δίκτυο (Cachin et al., 2016).

Oracles

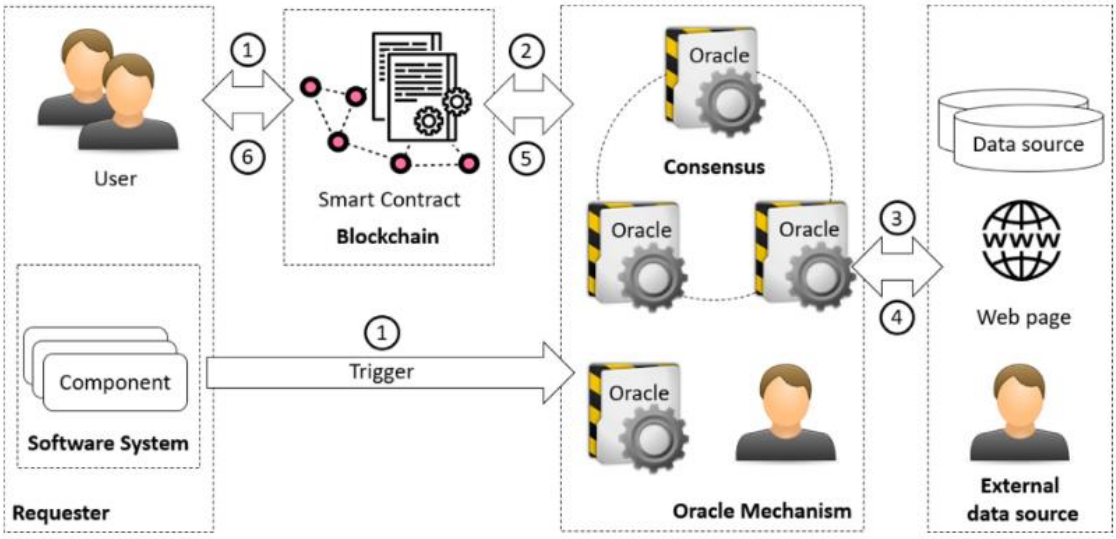
Η συμπεριφορά των "έξυπνων" συμβολαίων είναι απολύτως προβλέψιμη. Ως εκ τούτου, οι χρήστες μπορούν να τα εμπιστεύονται για την προώθηση οποιασδήποτε λογικής εντός του Blockchain που μπορεί να εκφραστεί ως συνάρτηση των εισαγόμενων σε αυτό δεδομένων, υπό την προϋπόθεση ότι τα δεδομένα αυτά να είναι εντός της εμβέλειας του δικτύου. Με αυτόν τον τρόπο διατηρείται η ντετερμινιστική επικύρωση των συναλλαγών, καθώς τα "έξυπνα συμβόλαια" μπορούν να έχουν πρόσβαση μόνο σε δεδομένα που είναι αποθηκευμένα στο Blockchain και δεν μπορούν να χρησιμοποιήσουν εξωτερικά δεδομένα. Σε πολλές περιπτώσεις όμως, εφαρμογές "έξυπνων" συμβολαίων πρέπει να αλληλοεπιδρούν με άλλα εξωτερικά συστήματα, που δεν ελέγχονται από το Blockchain. Αυτή η κατάσταση περιορίζει δραματικά την ικανότητα των "έξυπνων" συμβολαίων να χειρίζονται πραγματικά προβλήματα, καθώς οι πληροφορίες για την επικύρωση των συναλλαγών δε βρίσκονται πια εντός της εμβέλειας του δικτύου και απαιτείται ένας τρόπος ώστε ξεπεραστεί αυτό το εμπόδιο, χωρίς να μειώνεται η αξιοπιστία των δεδομένων. Για αυτόν ακριβώς το σκοπό χρησιμοποιούνται τα oracles, τα οποία μεταδίδουν τα απαιτούμενα δεδομένα από εξωτερικά συστήματα στο Blockchain, με κύριο σκοπό τη χρήση τους για τις ανάγκες των "έξυπνων" συμβολαίων. Η χρήση των oracles καθιστά δυνατή την επικοινωνία του Blockchain με τον εξωτερικό κόσμο, καταγράφοντας δεδομένα από αυτόν, στο Blockchain (Lo et al., 2020).

Τα oracles αποτελούν ουσιαστικά μία υπηρεσία για τη μεταφορά αξιόπιστων πληροφοριών στο Blockchain. Η οντότητα τους τοποθετείται ανάμεσα στα δεδομένα εξωτερικού κόσμου και το "έξυπνο" συμβόλαιο που εξυπηρετούν. Γεφυρώνουν το χάσμα μεταξύ του εικονικού συστήματος του Blockchain και του εξωτερικού κόσμου, εισάγοντας στο δίκτυο σε πραγματικό χρόνο γεγονότα και δεδομένα από τον πραγματικό κόσμο. Τέτοια δεδομένα θα μπορούσαν να είναι π.χ. η τιμή της θερμοκρασία, η τιμή μίας μετοχής, το ποσοστό του πληθωρισμού κτλ. Η πρωταρχική ευθύνη των oracles είναι να παρέχουν αυτό το είδος δεδομένων σε "έξυπνα" συμβόλαια με ασφαλή και αξιόπιστο τρόπο.

Ένας μηχανισμός oracle ενεργοποιείται με τη δημιουργία ενός "έξυπνου" συμβολαίου, του οποίου οι όροι απαιτούν δεδομένα εκτός του συστήματος. Η οντότητα του oracle μπορεί να συσταθεί με διάφορους τρόπους σύμφωνα με τον Kehrli (2016), όπως π.χ. με προσδιορισμό αξιόπιστου τρίτου μέρους εξ' αρχής από τους αντισυμβαλλόμενους του συμβολαίου, με αναφορά σε αξιόπιστη βάση δεδομένων ή με χρήση αποκεντρωμένης υπηρεσίας oracles. Στην

τελευταία περίπτωση ομάδα χρηστών που λειτουργεί με αποκεντρωμένο τρόπο, ψηφίζει για το αποτέλεσμα που θεωρεί ακριβές και ο προκαθορισμένος μηχανισμός συναίνεσης μεταξύ των συμμετεχόντων καθορίζει το τελικό αποτέλεσμα που θα αποσταλεί στο Blockchain. Το ρόλο ενός oracle μπορεί να παίξει και ένας άνθρωπος, με το πλεονέκτημα ότι μπορεί να απαντήσει σε πιο ασαφή ερωτήματα, κάτι το οποίο δεν μπορούν να κάνουν άλλοι μηχανισμοί (Mammadzada et al., 2020). Με τη χρήση ενός αποκεντρωμένου δικτύου από oracles, η επιρροή του κάθε oracle στο σύστημα περιορίζεται (Breidenbach et al., 2021).

Μόλις αναπτυχθεί ένα αυτοματοποιημένο oracle, θα επικοινωνήσει με την εξωτερική πηγή δεδομένων του, όπως ένα φυσικό αισθητήρα ή μία web υπηρεσία, για τη συλλογή των δεδομένων και θα τα εισάγει στο Blockchain ώστε να εκτελεστεί το "έξυπνο" συμβόλαιο. Απεικόνιση του αρχιτεκτονικού σχεδιασμού των αλληλεπιδράσεων ενός oracle παρουσιάζεται στο **Σχήμα 4-16**.



Σχήμα 4-16: Αρχιτεκτονικός σχεδιασμός μηχανισμού Oracle στο Blockchain (Lo et al., 2020)

Οι μηχανισμοί των oracles ταξινομούνται στις παρακάτω κατηγορίες (Beniiche, 2020):

- Software oracles: Αλληλοεπιδρούν με βάσεις δεδομένων του διαδικτύου και έχουν τη δυνατότητα να το κάνουν σε πραγματικό χρόνο.
- Hardware oracles: Αποτελούν αισθητήρες που βρίσκονται στο φυσικό κόσμο και μεταφέρουν τις μετρήσεις τους (π.χ. θερμόμετρα, scanners, trackers κτλ.)
- Human oracles: Είναι οι άνθρωποι που τους έχει ανατεθεί να τροφοδοτούν το Blockchain με συγκεκριμένα δεδομένα.
- Computational oracles: Μπορούν να κάνουν υπολογισμούς με τα δεδομένα πριν τα μεταδώσουν.

- Consensus based oracles: Βασίζονται στη συναίνεση μεταξύ πλήθους χρηστών – κόμβων.
- Centralized oracles: Ελέγχονται από μία μοναδική κεντρική αρχή.
- Decentralized oracles: Βασίζονται τη συναίνεση πλήθους άλλων oracles.

Τα oracles ταξινομούνται επίσης με βάση την κατεύθυνση των πληροφοριών, καθώς μπορούν είτε να μεταδίδουν πληροφορίες από εξωτερικές πηγές στο Blockchain (inbound oracles), είτε να στείλουν πληροφορίες από "έξυπνα" συμβόλαια σε εξωτερικές διεπαφές (outbound oracles). Η χρήση ενός oracle όμως, εισάγει και ορισμένα ζητήματα (Lo et al., 2020), τα οποία είναι η ανάγκη εμπιστοσύνης όλων των συμμετεχόντων προς το oracle και η μεταβλητότητα των εξωτερικών δεδομένων που θα χρησιμοποιηθούν.

4.7.2. Προγραμματισμός smart contracts

Τα "έξυπνα" συμβόλαια στο Blockchain δημιουργούνται από προγραμματιστές υπολογιστών και είναι εξ' ολοκλήρου ψηφιακά και γραμμένα με γλώσσες προγραμματισμού. Ο κώδικας τους ορίζει τους κανόνες και τις συνέπειες με τον ίδιο τρόπο που θα όριζε ένα παραδοσιακό νομικό έγγραφο. Η μεγάλη διαφορά με τα παραδοσιακά συμβόλαια είναι ότι λόγω του κώδικα, το συμβόλαιο εκτελείται αυτόματα (self-executing) από ένα κατανεμημένο σύστημα, χωρίς τη δυνατότητα παρεμβάσεων και κακόβουλων αλλαγών. Όπως και στα παραδοσιακά συμβόλαια, περιέχουν κανόνες, κυρώσεις και ενέργειες που αφορούν τα αντισυμβαλλόμενα μέρη που εμπλέκονται στη συναλλαγή και εκτελούνται μόλις εκπληρωθεί ο όρος του συμβολαίου (Dutta et al., 2020). Με βάση της προκαθορισμένες λειτουργίες του, ένα "έξυπνο" συμβόλαιο αποθηκεύει πληροφορίες, επεξεργάζεται εισερχόμενα δεδομένα (inputs) και δημιουργεί εξερχόμενα δεδομένα (outputs) (Buterin, 2014). Τα έξυπνα συμβόλαια λειτουργούν με δύο τύπους δεδομένων, οι οποίοι είναι τα εσωτερικά δεδομένα που αφορούν το συμβόλαιο και τα εξωτερικά δεδομένα που προέχονται από τις συναλλαγές.

Ένα "έξυπνο" συμβόλαιο αναλύεται σε δύο ξεχωριστά στοιχεία: α) τον κώδικα του συμβολαίου που αποθηκεύεται, επαληθεύεται και εκτελείται σε ένα Blockchain και β) νομικό κομμάτι του συμβολαίου που μπορεί να χρησιμοποιηθεί ως συμπλήρωμα ή υποκατάστατο για νομικές συμβάσεις. Ο τρόπος λειτουργίας ενός "έξυπνου" συμβολαίου μπορεί να διακριθεί κατά σειρά σε input, process και output (Kehrli, 2016). Επειδή τα "έξυπνα" συμβόλαια λειτουργούν όπως τα προγράμματα των υπολογιστών, είναι πολύ σημαντικό να κάνουν ακριβώς αυτό που έχει συμφωνηθεί μεταξύ των μερών. Αυτό επιτυγχάνεται με την εισαγωγή της σωστής λογικής κατά τη σύνταξη τους, ώστε ο κώδικας του συμβολαίου να συμπεριφέρεται με προκαθορισμένους τρόπους, έτσι ώστε να λειτουργεί απολύτως αυτοματοποιημένα μόλις καταγραφεί γεγονός στο Blockchain που θα πρέπει ενεργοποιήσει δράση από το συμβόλαιο. Ο κώδικας αφού γραφεί, κρυπτογραφείται και αποστέλλεται σε άλλους κόμβους μέσω του δικτύου Blockchain που πάνω

στο οποίο βασίζεται η λειτουργία του. Μόλις οι κόμβοι στο δίκτυο Blockchain λάβουν τον κώδικα, ενεργοποιείται η διαδικασία συναίνεσης σχετικά με τα αποτελέσματα της εκτέλεσης του κώδικα. Στη συνέχεια, το δίκτυο ενημερώνει το καθολικό για να καταγραφεί η εκτέλεση της συμβολαίου και στη συνέχεια το σύστημα παρακολουθεί τη συμμόρφωση των μερών με τους όρους του "έξυπνου" συμβολαίου. Σε αυτόν τον τύπο συστήματος, η χειραγώγηση ενός μέρους αποφεύγεται επειδή ο έλεγχος της εκτέλεσης του "έξυπνου" συμβολαίου δεν είναι πλέον δυνατός, δεδομένου ότι η εκτέλεση αυτή δεν βρίσκεται στα χέρια ενός μόνο μέρους.

Υπάρχουν διάφορες γλώσσες προγραμματισμού που μπορούν να χρησιμοποιηθούν για τη δημιουργία "έξυπνων" συμβολαίων. Μερικές από αυτές αναπτύχθηκαν ειδικά για τη συγγραφή τέτοιων συμβολαίων. Μερικές από τις δημοφιλέστερες γλώσσες είναι οι εξής:

- Solidity: Είναι μία high-level γλώσσα προγραμματισμού που αναπτύχθηκε για να είναι προσανατολισμένη στην συγγραφή "έξυπνων" συμβολαίων. Η φιλοσοφία της έχει επηρεαστεί από τη C++, την Python και τη JavaScript και έχει σχεδιαστεί για να λειτουργεί με το Ethereum Virtual Machine (EVM) (Solidity, n.d.). Είναι η πιο συχνά χρησιμοποιούμενη γλώσσα για την ανάπτυξη κώδικα συμβολαίων στο Blockchain του Ethereum, αλλά χρησιμοποιείτε και από άλλες πλατφόρμες Blockchain, όπως την Polkadot, την Binance κ.ά. Είναι μία στατική γλώσσα, το οποίο σημαίνει ότι πρέπει να καθοριστεί ο τύπος κάθε μίας από τις μεταβλητές που θα χρησιμοποιηθούν. Επίσης υποστηρίζει τη χρήση βιβλιοθηκών και δίνει τη δυνατότητα ανάπτυξης πολύπλοκων τύπων μεταβλητών από το χρήστη.
- Vyper: Είναι μια γλώσσα προγραμματισμού με έντονη επιρροή από την Python, ειδικά προσαρμοσμένη για την ανάπτυξη "έξυπνων" συμβολαίων. Οι τρεις θεμελιώδεις σχεδιαστικές αρχές και στόχοι της Vyper είναι η δυνατότητα ανάγνωσης του κώδικα από τον άνθρωπο, η ασφάλεια και η ευκολία στην χρήση.
- Rust: Είναι μια γλώσσα προγραμματισμού που έχει σχεδιαστεί δίνοντας μεγάλη έμφαση στην ασφάλεια και την απόδοση. Χρησιμοποιείτε για την κατασκευή συστημάτων υψηλών επιδόσεων, συμπεριλαμβανομένων web servers και λειτουργικών συστημάτων. Μέσω αυτής γίνεται η δημιουργία ενός "έξυπνου" συμβολαίου στο Blockchain Solana.
- JavaScript: είναι μια γλώσσα προγραμματισμού που χρησιμοποιείτε ευρέως σε διάφορες εφαρμογές και αξιοποιείτε από αρκετές πλατφόρμες Blockchain. Επειδή η JavaScript είναι μία entry-level γλώσσα, οι περισσότερες πλατφόρμες Blockchain τείνουν να δημιουργούν μια βιβλιοθήκη ή ένα wrapper JavaScript για να επιτρέπουν στους προγραμματιστές να μεταβούν με ευκολία στο οικοσύστημα και να αρχίζουν να δημιουργούν "έξυπνα" συμβόλαιο το συντομότερο δυνατό.

Στο επόμενο κεφάλαιο θα αναλυθούν πλατφόρμες για την ανάπτυξη "έξυπνων" συμβολαίων, με πιο σημαντική αυτή του Ethereum.

4.7.3. Ταξινόμηση smart contracts

Υπάρχουν πέντε διαφορετικές κατηγορίες για την ταξινόμηση των "έξυπνων" συμβολαίων με βάση το σκοπό της χρήσης τους (Bartoletti & Pompianu, 2017). Η πρώτη κατηγορία είναι τα συμβόλαια οικονομικού περιεχομένου. Το κύριο χαρακτηριστικό αυτού του τύπου συμβολαίων είναι η διαχείριση συγκεκριμένου χρηματικού ποσού ή η επαλήθευση της ιδιοκτησίας αγαθών. Σε άλλες περιπτώσεις, μπορεί να χρησιμοποιούνται για τη συγκέντρωση χρημάτων συμμετοχικής χρηματοδότησης (crowdfunding) με σκοπό τη χρηματοδότηση νέων έργων, επιχειρήσεων ή δράσεων. Επίσης χρησιμοποιούνται σε συμβόλαια επενδυτικών προγραμμάτων υψηλής απόδοσης που περιλαμβάνουν υψηλό κίνδυνο και υπόσχονται υψηλό επιτόκιο στους νέους επενδυτές που ενταχθούν στο πρόγραμμα. Τέλος, ορισμένα συμβόλαια παρέχουν ασφάλιση σε περιπτώσεις που η ζημία μπορεί να είναι ψηφιακά αποδείξιμη, ενώ υπάρχουν και συμβόλαια που ασχολούνται με τις διαφημίσεις.

Η δεύτερη κατηγορία είναι τα συμβολαιογραφικά συμβόλαια. Σε αυτή την κατηγορία τα συμβόλαια εκμεταλλεύονται την αμετάβλητη φύση του Blockchain για την αποθήκευση των πληροφοριών και των δεδομένων, την πιστοποίηση της ιδιοκτησίας τους και της προέλευσης τους. Στο ίδιο συμβολαιογραφικό πλαίσιο, τα "έξυπνα" συμβόλαια επιτρέπουν στους χρήστες να εκμεταλλευθούν την εφαρμογή των συναρτήσεων hash σε να έγγραφο στο Blockchain, έτσι ώστε να μπορούν να αποδείξουν την ύπαρξη και την ακεραιότητα του εγγράφου. Με παρόμοιο τρόπο, επιτρέπεται και η δήλωση πνευματικών δικαιωμάτων σε ψηφιακά μέσα όπως φωτογραφίες και μουσική, ενώ σε αυτήν κατηγορία χρήσης υπάρχουν επίσης συμβόλαια που συνδέουν τους χρήστες με διευθύνσεις και άλλα έγγραφα, προκειμένου να πιστοποιήσουν την ταυτότητα τους, όταν π.χ. απαιτείται κάτι τέτοιο από το μηχανισμό συναίνεσης που χρησιμοποιείται.

Μία ακόμα σημαντική κατηγορία της χρήσης των "έξυπνων" συμβολαίων αφορά τη διαχείριση πορτοφολιών (wallets) στο Blockchain. Ένα wallet είναι λογισμικό που δίνει πρόσβαση στα κρυπτονομίσματα κάποιου χρήστη, μέσω της αποθήκευσης των διευθύνσεων του Blockchain και των κλειδιών του χρήστη (Antonopoulos, 2014). Τα "έξυπνα" συμβόλαια χειρίζονται δημόσια και ιδιωτικά κλειδιά και διαχειρίζονται συναλλαγές μεταφοράς χρημάτων, καθιστώντας εφικτή την αλληλεπίδραση μεταξύ των χρηστών του δικτύου. Τα πορτοφόλια μπορούν να τα διαχειριστούν ένας ή και περισσότεροι ιδιοκτήτες, χρησιμοποιώντας πολλαπλές εξουσιοδοτήσεις. Η τέταρτη κατηγορία, αφορά την εφαρμογή τους σε τυχερά παιχνίδια και παιχνίδια δεξιοτήτων, καθώς καθορίζουν τη συμφωνία των κανόνων τους και τη διευθέτηση τους, μεταξύ των παικτών. Η τελευταία κατηγορία έχει τη μορφή βιβλιοθήκης "έξυπνων"

συμβολαίων και αφορά συμβόλαια που χρησιμοποιούνται για την υλοποίηση κοινών και γενικού σκοπού πράξεων, οι οποίες χρησιμοποιούνται από άλλες συμβάσεις.

4.7.4. Ιδιότητες και απαιτήσεις smart contracts

Σε αυτό το σημείο παρουσιάζονται βασικές ιδιότητες και απαιτήσεις που πρέπει να εκπληρώνονται κατά την ανάπτυξη "έξυπνων συμβολαίων" σύμφωνα με τους Capocasale και Perboli (2022), που ουσιαστικά αποτελούν κατευθυντήριες γραμμές για την τυποποίηση τους.

Τα "έξυπνα" συμβόλαια είναι λειτουργίες μεταβολής της κατάστασης του συστήματος: Ένα σύστημα Blockchain μπορεί να περιγραφεί ως μια μηχανή πεπερασμένων καταστάσεων (Buterin, 2014) και υπό αυτό το πρίσμα, τα "έξυπνα" συμβόλαια είναι οι λειτουργίες μετάβασης, που αλλάζουν την κατάσταση του συστήματος. Ουσιαστικά τα "έξυπνα" συμβόλαια λειτουργούν σε δύο τύπους δεδομένων: τα εσωτερικά (internal) δεδομένα του καθολικού, τα οποία είναι αξιόπιστα, και τα εξωτερικά (external) δεδομένα των συναλλαγών, των οποίων η ορθότητα πρέπει να επαληθευτεί. Ανάλογα με την περίπτωση χρήσης, τα εσωτερικά δεδομένα ενδέχεται να μην επαρκούν για την επαλήθευση των εξωτερικών. Αυτό δημιουργεί ένα όριο στη χρήση των συμβολαίων, του οποίου η υπέρβαση είναι μεν δυνατή, αλλά γίνεται με την αποδοχή αναξιόπιστων δεδομένων συναλλαγών, κάτι που μπορεί να έχει και τις αντίστοιχες συνέπειες στα outputs του συμβολαίου.

Τα "έξυπνα" συμβόλαια πρέπει να αλλάζουν την κατάσταση του συστήματος: Εάν ένα "έξυπνο" συμβόλαιο διαβάζει μόνο κάποια δεδομένα, ή κάνει μόνο κάποια επεξεργασία δεδομένων χωρίς να μεταβάλλει την κατάσταση του συστήματος, καθίσταται αδύνατο να ελεγχθεί η ορθότητα της εκτέλεσης του. Επομένως, ένα "έξυπνο" συμβόλαιο πρέπει υποχρεωτικά να μεταβάλλει την κατάσταση του συστήματος. Το πρωτόκολλο του Ethereum επιτρέπει τον ορισμό λειτουργιών ανάγνωσης (Chapman et al., 2019), που όταν καλούνται, η εκτέλεση τους λαμβάνει χώρα σε ένα μόνο κόμβο. Η θεώρηση ότι οι λειτουργίες ανάγνωσης αποτελούν "έξυπνα" συμβόλαια αποτελεί κοινή παρανόηση (Saetran et al., 2021; Vashistha et al.,2021), καθώς είναι μόνο συναρτήσεις για την ανάκτηση δεδομένων από το Blockchain ή για την εκτέλεση υπολογισμών από τα δεδομένα των συναλλαγών. Άλλα συστήματα Blockchain δεν κάνουν ρητή διάκριση μεταξύ των λειτουργιών με βάση την αλληλεπίδρασή τους με το ledger, αλλά η γενική έννοια εξακολουθεί να ισχύει. Δηλαδή το μόνο επαληθεύσιμο output ενός έξυπνου συμβολαίου είναι η αυτό που αλλάζει την κατάσταση του συστήματος και κατά συνέπεια αποθηκεύεται στο Blockchain.

Τα "έξυπνα" συμβόλαια πρέπει να είναι επαληθεύσιμα: Θα πρέπει να είναι δυνατή η επαλήθευση του output ενός "έξυπνου" συμβολαίου σε οποιαδήποτε μελλοντική χρονική στιγμή. Αν αυτή η απαίτηση δεν ικανοποιείται, το σύστημα μπορεί να διχαστεί και η συναίνεση

μεταξύ των κόμβων μπορεί να μην μπορεί να επιτευχθεί. Ειδικότερα, ο χρόνος επαλήθευσης μπορεί να είναι πολύ διαφορετικός από το χρόνο εκτέλεσης ενός "έξυπνου" συμβολαίου, γεγονός που εισάγει έναν περιορισμό στη χρήση των language primitives που σχετίζονται με το χρόνο (Abdelhamid & Hassan, 2019). Ακόμη και αν όλοι οι κόμβοι του συστήματος μοιράζονται το ίδιο ατομικό ρολόι, αυτό θα τους επέτρεπε μόνο να συγχρονίσουν την εκτέλεση ενός "έξυπνου" συμβολαίου, αλλά όχι την επαλήθευση του. Ένας τέτοιος περιορισμός δεν εμποδίζει τα "έξυπνα" συμβόλαια να αξιοποιήσουν τα primitives που σχετίζονται με τον χρόνο, αλλά η εισαγωγή τους θα πρέπει να μελετηθεί προσεκτικά. Τα "έξυπνα" συμβόλαια θα πρέπει να βασίζονται μόνο στα δεδομένα που είναι ήδη αποθηκευμένα στο δίκτυο του Blockchain ή που παρέχονται στο input τους. Δε θα πρέπει να στηρίζονται σε οποιοδήποτε άλλο δεδομένο, όπως ο χρονισμός του κόμβου που εκτελεί το "έξυπνο" συμβόλαιο.

Τα "έξυπνα" συμβόλαια πρέπει να είναι ντετερμινιστικά: Όπως έχει ήδη αναφερθεί παραπάνω, αυτό είναι μία βασική απαίτηση στο σχεδιασμό των "έξυπνων" συμβολαίων, καθώς πρέπει να παράγει το ίδιο αποτέλεσμα σε όλους τους κόμβους που το εκτελούν. Η συγκεκριμένη απαίτηση συχνά υποτιμάται και το πρόβλημα αυτό ερευνάται ενεργά, και μερικές από τις κύριες τεχνικές για την αντιμετώπισή του, βασίζονται σε υπολογισμό πολλαπλών μερών (multi-party computation) (Du et al.,2019).

Τα "έξυπνα" συμβόλαια είναι κλάσεις ισοδύναμης κατάστασης: Άλλη μία κοινή παρανόηση είναι ότι ένα "έξυπνο" συμβόλαιο είναι μοναδικό (Hassan et al., 2021). Σε ένα σύστημα Blockchain, ένας κόμβος δεν μπορεί να ελέγξει ποιοι υπολογισμοί εκτελούνται από τους άλλους, αλλά μόνο εάν φτάσουν στην ίδια κατάσταση μετά τον υπολογισμό. Έτσι, ένα "έξυπνο" συμβόλαιο είναι μία κλάση συναρτήσεων μετάβασης ισοδύναμης κατάστασης που, όταν τους παρέχεται το ίδιο input, παράγουν το ίδιο output, ανεξαρτήτως του τρόπου που φτάνουν σε αυτό. Ένα σύστημα Blockchain λειτουργεί χωρίς προβλήματα, ακόμη και αν ορισμένοι κόμβοι χρησιμοποιούν διαφορετική κλάση του συμβολαίου. Αυτό θα πρέπει να διευκρινίζεται αναλυτικότερα σε "έξυπνα" συμβόλαια που έχουν έχουν νομική αξία, καθώς θα πρέπει να είναι ξεκάθαρο ότι είναι σημαντικό το τι πρέπει να κάνουν και όχι πώς να το κάνουν (Governatori et al., 2018).

Τα έξυπνα συμβόλαια δεν χρειάζεται να αποθηκεύονται στην αλυσίδα: Μία ακόμη παρανόηση είναι ότι τα "έξυπνα" συμβόλαια πρέπει να αποθηκεύονται στην αλυσίδα (Rouhani & Deters, 2019; Schär, 2021). Η αποθήκευση του κώδικα ενός "έξυπνου" συμβολαίου στην αλυσίδα είναι μόνο ένας απλός τρόπος διανομής του κώδικα του συμβολαίου σε όλους τους κόμβους του Blockchain. Δημόσια δίκτυα Blockchain, όπως το Ethereum, χρησιμοποιούν αυτή την προσέγγιση για την αυτόματη ενημέρωση του σύνολο των "έξυπνων" συμβολαίων που αναπτύσσονται σε κάθε κόμβο. Άλλες πλατφόρμες, όπως το Sawtooth (Olson et al., 2018) δεν

αποθηκεύουν τον κώδικα στην αλυσίδα και κάθε συμβαλλόμενος (peer) είναι υπεύθυνος για την εγκατάσταση των απαιτούμενων "έξυπνων" συμβολαίων στον κόμβο του. Η βασική ιδέα είναι ότι κάθε κόμβος δεν χρειάζεται να γνωρίζει τι κώδικα εκτελούν οι άλλοι, αλλά μόνο ποια είναι η κατάσταση στην οποία καταλήγουν στο τέλος και υποθέτοντας ότι η πλειοψηφία είναι ειλικρινής, θα επιτευχθεί μια κοινή κατάσταση. Η αποθήκευση του κώδικα ενός "έξυπνου" συμβολαίου στην αλυσίδα είναι πολύτιμη σε άλλα πλαίσια όπως σε περιπτώσεις που είναι απαραίτητη η διαφάνεια ή το συμβόλαιο έχει νομική αξία.

Τα "έξυπνα" συμβόλαια δεν είναι αμετάβλητα: Αν ένα σύστημα Blockchain είναι αμετάβλητο και ένα έξυπνο συμβόλαιο αποθηκεύεται στην αλυσίδα, τότε το έξυπνο συμβόλαιο είναι αμετάβλητο (Sergey et al., 2019; Kongmanee et al., 2019), ωστόσο, ο όρος αμετάβλητος είναι παραπλανητικός. Πιο σωστά, ένα Blockchain μπορεί να οριστεί ως ένα σύστημα που υπάρχει η δυνατότητα, μόνο να προστίθενται νέες πληροφορίες. Κατά συνέπεια, ακόμη και αν αυτό που είναι αποθηκευμένο σε ένα Blockchain δεν μπορεί να τροποποιηθεί, μία νεότερη έκδοση του μπορεί πάντα να ενσωματωθεί στο καθολικό του. Έτσι, ακόμη και όταν τα "έξυπνα" συμβόλαια αποθηκεύονται στην αλυσίδα, μπορούν να ενημερωθούν. Επιπλέον, στο δίκτυο Ethereum, η πλειοψηφία των κόμβων μπορεί πάντα να αποφασίσει για την αντικατάσταση ενός συγκεκριμένου συμβολαίου. Επομένως, τα "έξυπνα" συμβόλαια είναι αμετάβλητα μόνο εάν δεν εφαρμόζουν μηχανισμό ενημέρωσης και η πλειοψηφία δεν είναι πρόθυμη να τα αλλάξει. Άλλες πλατφόρμες, όπως η EOSIO, επιτρέπουν την ενημέρωση των έξυπνων συμβολαίων με αντικατάσταση του παλαιού κώδικα με τον νέο (Kemmoe et al., 2020), όμως όλοι οι κόμβοι θα πρέπει να αρχίσουν να χρησιμοποιούν ταυτόχρονα τη νεότερη έκδοση. Κάθε κόμβος ενεργεί ανεξάρτητα από τους άλλους, οπότε οι ενημερώσεις των "έξυπνων" συμβολαίων δεν μπορούν να επιβληθούν όπως στα συστήματα κεντρικής αρχής, αλλά πρέπει να προταθούν και να γίνουν αποδεκτές από τους συμβαλλομένους. Συνεπώς, η διαχείριση "έξυπνων" συμβολαίων είναι δύσκολη, καθώς απαιτεί τη συνεργασία και το συντονισμό της πλειοψηφίας των κόμβων.

Τα "έξυπνα" συμβόλαια δεν είναι νομικά συμβόλαια: Παρά την ονομασία τους, τα "έξυπνα" συμβόλαια είναι προγράμματα υπολογιστών και όχι συμβόλαια, με τη δεσμευτική σημασία του όρου (Dell'Erba, 2018). Κατά συνέπεια, έχουν ένα τεράστιο φάσμα πιθανών εφαρμογών και μπορούν να αντιπροσωπεύουν πολύ περισσότερα από μία συμφωνία, με αποτέλεσμα είναι κάτι περισσότερο από απλά νομικά συμβόλαια. Οι χρήστες τα υπογράφουν ψηφιακά τα συμβόλαια, αλλά τις συναλλαγές που αλληλοεπιδρούν με αυτά. Συνεπώς, δεν επαρκούν ως νομικά συμβόλαια, και η νομική τους αξία πρέπει να νομιμοποιηθεί από τα υπάρχοντα νομικά εργαλεία. Σε κάθε περίπτωση, τα "έξυπνα" συμβόλαια μπορούν εν μέρει, να αυτοματοποιήσουν τα νομικά (Mik, 2017). Μπορούν να τυποποιήσουν και να απλοποιήσουν

την ανταλλαγή δεδομένων μεταξύ πολλαπλών εταιρειών, αλλά η νομική τους νομιμοποίηση είναι μόνο δυνητική και εξαρτάται από την εκάστοτε δικαιοδοσία.

Τα "έξυπνα" συμβόλαια δεν αποδίδουν νόημα: Όπως αναφέρθηκε, τα "έξυπνα" συμβόλαια είναι προγράμματα υπολογιστών, άρα επεξεργάζονται ακολουθίες από bits και παράγουν άλλες ακολουθίες από bits, χωρίς να περιγράφουν λεπτομερώς το νόημα και τη σωστή ερμηνεία των ακολουθιών που παράγουν. Επομένως, τα "έξυπνα" συμβόλαια δεν αρκούν από μόνα τους και χρειάζονται εξωτερικά πρότυπα για τον καθορισμό του τρόπου κωδικοποίησης των δεδομένων και του πώς θα πρέπει να ερμηνεύονται. Σε κάποιο βαθμό, όλα τα συστήματα Blockchain, παρέχουν πρότυπα κωδικοποίησης και αποκωδικοποίησης δεδομένων. Ωστόσο, δεν παρέχουν αρκετές λεπτομέρειες για να εγγυηθούν μία μονοσήμαντη και ουσιαστική ερμηνεία των αποθηκευμένων δεδομένων, η οποία είναι απαιτητή για τη νομιμοποίηση των "έξυπνων" συμβολαίων από νομική άποψη.

Τα "έξυπνα" συμβόλαια θα πρέπει να κωδικοποιούνται και να αναπτύσσονται ανεξάρτητα (κατά προτίμηση): Σε αντίθεση με ότι συμβαίνει σήμερα σε πολλά δίκτυα Blockchain, τα "έξυπνα" συμβόλαια δε θα πρέπει να κωδικοποιούνται και να αναπτύσσονται σε όλους τους κόμβους του συστήματος, καθώς εξ' ορισμού, δεν είναι δεδομένη η εμπιστοσύνη μεταξύ των κόμβων του συστήματος. Κατά συνέπεια, ένας κόμβος δε θα πρέπει να ποτέ να δέχεται να εκτελέσει μία υλοποίηση που παρέχεται από άλλους αναξιόπιστους κόμβους. Αντ' αυτού, κάθε κόμβος θα πρέπει να εκτελεί αυτόνομα και να υλοποιεί όλα τα "έξυπνα" συμβόλαια για να είναι σίγουρος για την ορθότητά τους. Όμως, οι κόμβοι συνήθως χρησιμοποιούν μόνο ένα μέρος του συνόλου των διαθέσιμων συμβολαίων και επιπλέον, δε διαθέτουν τις κατάλληλες ικανότητες και πόρους για τη δημιουργία ανεξάρτητων υλοποιήσεων. Σε τέτοιες καταστάσεις, η απαίτηση να κωδικοποιεί κάθε κόμβος ανεξάρτητα όλα τα "έξυπνα" συμβόλαια (ακόμη και αυτά που δεν χρησιμοποιεί) είναι υπερβολική και συνήθως ανέφικτη, παρ' όλα αυτά, η κακόβουλη εκμετάλλευση ενός σφάλματος θα γινόταν σχεδόν αδύνατη, σε αυτήν την περίπτωση.

Τα "έξυπνα" συμβόλαια θα πρέπει να ελέγχονται και να δοκιμάζονται ανεξάρτητα (κατά προτίμηση): Όπως και στην προηγούμενη περίπτωση, κι αυτό είναι δύσκολο να συμβεί, δηλαδή, τα "έξυπνα" συμβόλαια να ελέγχονται και να δοκιμάζονται από τους κόμβους πριν από την εφαρμογή τους. Ωστόσο, αυτή η κατευθυντήρια γραμμή είναι πιο πιθανό να βρει εφαρμογή, καθώς η δοκιμή ενός "έξυπνου" συμβολαίου είναι ευκολότερη από την κωδικοποίησή του. Προκειμένου να απλοποιηθεί η διαδικασία δοκιμών, η δημοσίευση του πηγαίου κώδικα των συμβολαίων είναι η βέλτιστη πρακτική, καθώς απλοποιεί τον έλεγχο του κώδικα.

Τα "έξυπνα" συμβόλαια μπορούν να αξιοποιήσουν τις αποδείξεις εκτέλεσης τους: Σε ορισμένες περιπτώσεις, η εκτέλεση μεγάλων υπολογιστικά "έξυπνων" συμβολαίων μπορεί να είναι πολύ απαιτητική και θα ήταν προτιμότερη η μόχλευση μιας μεμονωμένης εκτέλεσης και η απόδειξη της ορθότητάς της. Αυτή η προσέγγιση, εξακολουθεί να απαιτεί την εκτέλεση ενός μέρους του του "έξυπνου" συμβολαίου, δηλαδή την επαλήθευση και την αποθήκευση της λύσης. Έτσι, τα "έξυπνα" συμβόλαια έχουν μία σταθερή βάση, καθώς τα βήματα επαλήθευσης και αποθήκευσης πρέπει πάντα να εκτελούνται με αποκεντρωμένο τρόπο. Πολλές πλατφόρμες Blockchain υιοθετούν αυτήν την προσέγγιση για να βελτιώσουν την επεκτασιμότητα τους και η έννοια των zero-knowledge proofs είναι ιδιαίτερα χρήσιμη για την υλοποίηση της προσέγγισης (He et al., 2022).

Τα "έξυπνα" συμβόλαια δεν χρειάζεται να είναι πιστοποιημένα: Ανεξάρτητα από την περίπτωση εφαρμογής, τα "έξυπνα" συμβόλαια δε χρειάζεται να πιστοποιηθούν. Εξ' ορισμού, οι φορείς πιστοποίησης είναι αξιόπιστα τρίτα μέρη, και η τεχνολογία Blockchain προσπαθεί να εξαλείψει όλα αυτά τα μέρη. Φυσικά είναι προς το συμφέρον των κόμβων να ελέγχουν ορθά τις υλοποιήσεις των "έξυπνων" συμβολαίων τους (Almakhour et al., 2020), και μπορούν αν θέλουν να αξιοποιούν και εξωτερικές υπηρεσίες για αυτό. Η ορθότητα των "έξυπνων" συμβολαίων θα πρέπει να είναι εγγυημένη μόνο από το γεγονός ότι οι κόμβοι μπορούν να φτάσουν στην ίδια κατάσταση του συστήματος μετά την εκτέλεση τους. Σε περίπτωση, εάν το σύστημα το επιθυμεί, μπορεί να βασίζεται σε κάποιες εξωτερικές αρχές για την πιστοποίηση των συμβολαίων του. Από μια ευρύτερη οπτική γωνία, οποιαδήποτε μορφή συγκεντρωτισμού υπονομεύει την αξία των "έξυπνων" συμβολαίων που βασίζονται στην τεχνολογία Blockchain. Σε πολλές περιπτώσεις όμως, η έλλειψη πρακτικότητας των αποκεντρωμένων λύσεων μπορεί να οδηγήσει τους υπεύθυνους λήψης αποφάσεων στο να αποδεχτούν συμβιβασμούς στα συστήματα τους.

Τα "έξυπνα" συμβόλαια δεν θα πρέπει να βασίζονται σε oracles (κατά προτίμηση): Δεν πρέπει πότε να υπάρχει πλήρη εμπιστοσύνη σε δεδομένα που παρέχονται από τους τρίτα μέρη, καθώς μειώνουν το βαθμό αποκέντρωσης του συστήματος (Mik, 2017). Η εξάλειψη όμως των oracles από ένα σύστημα Blockchain είναι σπάνια εφικτή, παρ' όλα αυτά τα "έξυπνα" συμβόλαια θα πρέπει να σχεδιάζονται με τέτοιο τρόπο ώστε να βασίζονται όσο το δυνατόν λιγότερο, στα δεδομένα που τους παρέχουν αυτά. Επιπλέον, θα πρέπει να εφαρμόζονται στρατηγικές που αποθαρρύνουν την αθέμιτη συμπεριφορά των oracles. Για το σκοπό αυτό, δίκτυα όπως το Chainlink, χρησιμοποιούν οικονομικά κίνητρα και πολλαπλή τροφοδοσία δεδομένων για να μειώσουν τις απόπειρες χειραγώγησης (Breidenbach et al., 2021).

Τα έξυπνα συμβόλαια δεν έχουν σφάλματα (πιθανότατα): Υπό την υπόθεση ότι ένα "έξυπνο" συμβόλαιο έχει κωδικοποιηθεί ανεξάρτητα από πολλούς κόμβους, είναι απίθανο όλες οι

υλοποιήσεις να μοιράζονται το ίδιο σφάλμα. Φυσικά, όλες οι υλοποιήσεις μπορεί να βασίζονται στην ίδια βιβλιοθήκη. Σε τέτοιες περιπτώσεις, τα σφάλματα που επηρεάζουν τη βιβλιοθήκη, θα επηρεάσουν το ίδιο όλες τις υλοποιήσεις. Ωστόσο, η γενική ιδέα πίσω από την επεκτασιμότητα εξακολουθεί να ισχύει, δηλαδή η αύξηση του αριθμού των ανεξάρτητων υλοποιήσεων αυξάνει την προσπάθεια που απαιτείται για την κωδικοποίηση τους και την πιθανότητα απόκτησης ενός έξυπνου συμβολαίου χωρίς σφάλματα (Altarawneh et al., 2020). Παρά το αυξημένο, κόστος τα έξυπνα συμβόλαια που διαχειρίζονται πολύτιμα περιουσιακά στοιχεία, αξίζει να εξετάσουν αυτή τη στρατηγική ως έναν τρόπο αντιστάθμισης του κινδύνου μίας επίθεσης.

Τα έξυπνα συμβόλαια είναι απαραβίαστα (πιθανότατα): Ένα "έξυπνο" συμβόλαιο επαληθεύεται ανεξάρτητα από πολλαπλούς κόμβους, άρα η αλλοίωση της εκτέλεσης του είναι ανέφικτη. Κατά συνέπεια, τα "έξυπνα" συμβόλαια είναι απαραβίαστα, όμως η ανθεκτικότητα τους είναι ανάλογη του βαθμού αποκέντρωσης του δικτύου Blockchain. Δεν προσφέρουν καμία εγγύηση αν ένας μόνο κόμβος μπορεί να επηρεάσει τους άλλους ή αν ορισμένοι κόμβοι έχουν ισχυρό κίνητρο για να εκτελέσουν μαζί κακόβουλη ενέργεια. Συνεπώς, οι υπεύθυνοι λήψης αποφάσεων θα πρέπει να αναλύουν τις σχέσεις μεταξύ των κόμβων πριν από την ένταξή τους σε ένα δίκτυο Blockchain, καθώς οι συμβαλλόμενοι πρέπει να εξακολουθούν να εμπιστεύονται, ότι η πλειοψηφία είναι ειλικρινής, για να μπορεί να λειτουργεί το δίκτυο.

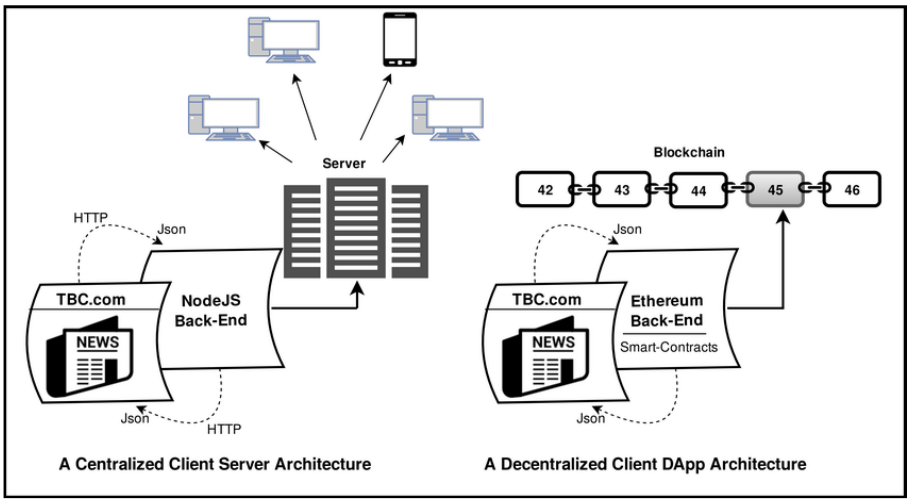
Τα έξυπνα συμβόλαια ανήκουν στο σύστημα του Blockchain: Ο ιδιοκτήτης ενός "έξυπνου" συμβολαίου είναι συχνά ο δημιουργός του. Σε κάθε περίπτωση ωστόσο, το "έξυπνο" συμβόλαιο διαχειρίζεται και εκτελείται από τους κόμβους του δικτύου Blockchain. Εάν η πλειοψηφία του δικτύου, αποφασίσει να τροποποιήσει το συμβόλαιο, ο ιδιοκτήτης του δεν έχει καμία εξουσία ή δικαίωμα να τους σταματήσει. Έτσι, ο πραγματικός ιδιοκτήτης ενός "έξυπνου" συμβολαίου είναι το ίδιο το Blockchain.

4.7.5. Decentralized applications (dApp)

Η θεωρία των "έξυπνων" συμβολαίων έθεσε τα θεμέλια της ανάπτυξης λογισμικού στο Blockchain και με αυτόν τον τρόπο έχει κάνει πραγματικότητα τη δυνατότητα ανάπτυξης αποκεντρωμένων εφαρμογών σε αυτό. Αποκεντρωμένες εφαρμογές υπήρχαν και πριν από το Blockchain, αλλά με περιορισμένες δυνατότητες (π.χ. διαμοιρασμός αρχείων). Αυτό κατέστη εφικτό, διότι όπως έχει αναφερθεί, τα "έξυπνα" συμβόλαια μετατρέπουν το στατικό καθολικό του Blockchain σε ένα δυναμικό σύστημα, ικανό να εκτελεί επιχειρηματική λογική.

Οι συνηθισμένες online εφαρμογές (webapps) αποτελούνται από το Front-End, δηλαδή το περιβάλλον με το οποίο αλληλοεπιδρά ο χρήστης της εφαρμογής, και το Back-End που είναι το κομμάτι του κώδικα που ελέγχει την εφαρμογή και τροποποιεί το interface του χρήστη ανάλογα

με τις ενέργειες του. Αντίθετα, μία αποκεντρωμένη εφαρμογή βασίζεται, όπως φανερώνει και το όνομα της, σε ένα αποκεντρωμένο δίκτυο που συνδυάζει ένα "έξυπνο" συμβόλαιο με ένα Front-End. Η εκτέλεση των λειτουργικών διαδικασιών του Back-End μίας dApp, δε βασίζεται σε ένα διακομιστή ή σε έναν υπολογιστή, αλλά στους κόμβους ενός Peer-to-Peer δικτύου και η διαφορά αυτή απεικονίζεται στο ***Σχήμα 4-17***.



Σχήμα 4-17: Αρχιτεκτονική dApp και σε σύγκριση με αρχιτεκτονική κεντρικού server (Sayeed et al., 2020)

Οι dApps είναι εφαρμογές ανοιχτού κώδικα και ο πηγαίος κώδικας τους είναι διαθέσιμος για εξέταση από όλους, καθώς η εφαρμογή αποθηκεύεται στο Blockchain για να διασφαλιστεί η εμπιστοσύνη και η διαφάνεια (Sayeed et al., 2020). Οι miners είναι υπεύθυνοι για την εκτέλεση των διαδικασιών της εφαρμογής και ανταμείβονται για την επικύρωση των λειτουργιών της dApp. Το κομμάτι αυτό της dApp συνδέεται κανονικά με το Front-End της εφαρμογής, ανεξαρτήτως με το ποια γλώσσα προγραμματισμού έχει χρησιμοποιηθεί για την ανάπτυξη του. Οι dApps αντλούν τη φύση τους από τα στοιχεία backend. Η λειτουργία μίας τέτοιας εφαρμογής βασίζεται αποκλειστικά στη λογική πάνω στην οποία έχει γραφτεί το "έξυπνο" συμβόλαιο που την καθορίζει.

Λόγω του γεγονότος ότι το Back-End των dApps βασίζεται στα "έξυπνα" συμβόλαια και το Blockchain, αποκτούν από αυτά τα χαρακτηριστικά τους. Δηλαδή δεν ελέγχονται από άτομο, αλλά από το σύνολο των κόμβων του δικτύου, είναι ντετερμινιστικά ανεξαρτήτως του περιβάλλοντος που εκτελούνται, είναι σε θέση να εκτελέσουν οποιαδήποτε ενέργεια μπορεί να εκτελέσει μια σύγχρονη γλώσσα προγραμματισμού εκτελούνται στο εικονικό περιβάλλον του Blockchain, άρα είναι ανεκτικές σε σφάλματα, χωρίς να εμποδίζουν την κανονική λειτουργία του δικτύου (Ethereum, 2022b). Με βάση αυτά, προκύπτουν κάποια οφέλη από τη χρήση των dApps, σε σχέση με τις παραδοσιακές εφαρμογές. Οι αποκεντρωμένες εφαρμογές προσφέρουν μηδενικό χρόνο διακοπής λειτουργίας, λόγω του ότι λειτουργούν σε κάθε κόμβο,

οπότε το δίκτυο θα είναι πάντα σε θέση να ανταποκρίνεται στους χρήστες που θέλουν να αλληλοεπιδράσουν με αυτό. Λόγω του Peer-to-Peer δικτύου, οι denial-of-service επιθέσεις είναι πολύ αδύναμες και οι συναλλαγές χωρίς την ανάγκη εμπιστοσύνης μεταξύ των χρηστών είναι εφικτές. Το ίδιο ισχύει και για την εκτέλεση των "έξυπνων" συμβολαίων πάνω στα οποία βασίζεται η εφαρμογή, όπου δεν απαιτείται αξιόπιστος ενδιάμεσος. Παρέχεται πλήρη ακεραιότητα των δεδομένων, επομένως δεν μπορούν να πλαστογραφηθούν και ταυτόχρονα οι dApps είναι ανοικτού κώδικα και οι κόμβοι του δικτύου μπορούν εύκολα να εντοπίσουν και να αποτρέψουν σφάλματα και προσπάθειες για κακόβουλες ενέργειες. Τέλος, οι dApps παρέχουν απόλυτη ελευθερία ενεργειών και απόρρητο στο χρήστη, ο οποίος δε χρειάζεται να παράσχει την πραγματική του ταυτότητα.

Αντίστοιχα όμως, υπάρχουν και κάποια μειονεκτήματα. Οι dApps αποθηκεύονται στο Blockchain και αυτό καθιστά δύσκολη την τροποποίησή τους με τους προγραμματιστές να αντιμετωπίζουν δυσκολίες στη δημοσίευση ενημερώσεων των εφαρμογών τους. Επίσης η αποκέντρωση έχει έξοδα για την καλή της απόδοσης, καθώς απαιτεί κάθε κόμβος στο δίκτυο να εκτελεί και να αποθηκεύει κάθε συναλλαγή, με αποτέλεσμα να αντιμετωπίζονται προβλήματα κατά την κλιμάκωση της χρήσης μία τέτοιας εφαρμογής. Επιπλέον, αν οι συναλλαγές παράγονται ταχύτερα από τη χωρητικότητα του δικτύου, η δεξαμενή των μη επιβεβαιωμένων συναλλαγών μπορεί να αυξηθεί σημαντικά, οδηγώντας σε καθυστερήσεις. Προς το χρήστη, οι dApps στερούνται φιλικής εμπειρίας, ενώ αν ο χρήστης απωλέσει το κλειδί του ο λογαριασμός του στην εφαρμογή θα είναι μη ανακτήσιμος. Τέλος, οι dApps δεν μπορούν να χειριστούν εύκολα το KYC (Know-Your-Customer), λόγω του απορρήτου του Blockchain, με αποτέλεσμα η επαλήθευση της ταυτότητας να είναι δύσκολη έως αδύνατη, σε τομείς εφαρμογών που το απαιτούν.

4.7.6. Πλατφόρμες Blockchain για Smart Contracts

Σε αυτό σημείο θα παρουσιαστούν πλατφόρμες Blockchain για τη ανάπτυξη "έξυπνων" συμβολαίων, που αποτελούν και πιθανές επιλογές του έργου BLOCK AGROWASTE όσον αφορά την επιλογή εργαλείου για ανάπτυξη του συστήματος Blockchain. Όλες οι επιλογές που θα παρουσιαστούν είναι πλατφόρμες ανοικτού κώδικα και έχουν κοινά βασικά χαρακτηριστικά, δηλαδή είναι ασφαλείς κρυπτογραφικά για τη χρήση συναρτήσεων κατατεμαχισμού, χρησιμοποιούν ασύμμετρα κλειδιά και ψηφιακές υπογραφές, ενώ υποστηρίζουν και τη χρήση των smart contracts. Ωστόσο, οι τομείς εφαρμογής τους ποικίλλουν σημαντικά.

Ethereum

Η πλατφόρμα του Ethereum (ethereum.org), όπως έχει αναφερθεί, δημιουργήθηκε από το Vitalik Buterin με τη δημοσίευση ενός white paper (Buterin, 2014) και η κυκλοφορία του έγινε

το 2015. Για τη δημιουργία του Ethereum, ο Buterin είχε επηρεαστεί από το Satoshi Nakamoto και το σύστημα Blockchain του Bitcoin, και αποφάσισε προσπαθήσει να το συνδυάσει με τις ιδέες του Nick Szabo, περί αυτοματοποιημένων ψηφιακών συμφωνιών χωρίς διαμεσολαβητές. Αναγνώρισε ότι το δίκτυο του Bitcoin μπορεί να υποστηρίξει την ανάπτυξη κάποιων σεναρίων που θα μπορούσαν να συσχετιστούν με "έξυπνα" συμβόλαια, αλλά έχει σημαντικούς περιορισμούς, όπως ότι του λείπουν οι δομές ελέγχου για να είναι Turing-complete. Έτσι αποφάσισε να προτείνει ένα νέο πρωτόκολλο για τη δημιουργία αποκεντρωμένων εφαρμογών, το οποίο είναι Turing-complete (Swan, 2015) και μπορεί να αναπτύξει κάθε ζητούμενο σενάριο. Έτσι μετασχημάτισε την τεχνολογία Blockchain με την εισαγωγή της έννοια των "έξυπνων" συμβολαίων και έχει καταφέρει σήμερα, να είναι η δεύτερη πιο χρησιμοποιούμενη πλατφόρμα κρυπτονομισμάτων (μετά το Bitcoin) και να οδηγεί τη αγορά των "έξυπνων" συμβολαίων. Σύμφωνα με τη μελέτη των Sigaki et al. (2019), η πλατφόρμα του Ethereum είναι πιο αποτελεσματική από αυτή του Bitcoin.

Η ανάπτυξη του Ethereum από το 2015, υποστηρίζεται από το Ίδρυμα Ethereum, έναν ελβετικό μη κερδοσκοπικό οργανισμό, που ιδρύθηκε από τους τον Buterin και τους συνεργάτες του (Emeç et al, 2020). Για να χρηματοδοτήσουν την ανάπτυξη του Ethereum, ο Buterin μαζί με τους υπόλοιπους συνιδρυτές της πλατφόρμας, ξεκίνησαν μία εκστρατεία τύπου crowdfunding, για να πουλήσουν στους συμμετέχοντες το Ether, το εγγενές κρυπτονόμισμα του Blockchain του Ethereum. Η υποδιαίρεση του Ether ονομάζεται Wei (πήρε το όνομα της από τον επιστήμονα υπολογιστών Wei Dai) και η αντιστοιχία τους είναι ότι 1 Ether ισούται με 1018 Wei. Ο γύρος δημόσιας χρηματοδότησης ήταν πολύ επιτυχημένος, με το Ίδρυμα Ethereum να συγκεντρώνει αρκετά εκατομμύρια για να ξεκινήσει τις δραστηριότητές του. Από τότε, η πλατφόρμα έχει εξελιχθεί κατά πολύ, με εκατοντάδες προγραμματιστές να συμμετέχουν παγκοσμίως.

Ο Buterin (2014) αναφέρει στο white paper του Ethereum ότι το Ether, εξυπηρετεί το διπλό σκοπό της παροχής ενός πρωτογενούς επιπέδου ρευστότητας που επιτρέπει την αποτελεσματική ανταλλαγή μεταξύ διαφόρων τύπων ψηφιακών περιουσιακών στοιχείων και την παροχή ενός μηχανισμού για την πληρωμή τελών συναλλαγής, που είναι και το πιο σημαντικό. Έτσι, όπως και το Bitcoin, το Ether προσφέρεται στους miners από το δίκτυο, ως κίνητρο για την προστασία της ασφάλειας του δικτύου, και επιπλέον χρησιμεύει ως μηχανισμός για την πληρωμή τελών ανά συναλλαγή για σκοπούς α) επίσης κινήτρων και β) anti-spam. Από τη μία, όπως και στο Bitcoin, τα τέλη συναλλαγής αποτελούν μέρος του μηχανισμού κινήτρων στο Ethereum, ωστόσο υπάρχει μια διαφορά στον τρόπο αναπαράστασης και υπολογισμού τους. Στο Bitcoin, το τέλος συναλλαγής είναι η διαφορά αξίας μεταξύ του input και του output μίας συναλλαγής, ενώ από την άλλη, οι χρεώσεις στο Ethereum δεν είναι σταθερές καθώς εξαρτώνται από τον κώδικα που θα εκτελεστεί ως μέρος της συναλλαγής. Από την άλλη, τα τέλη

στο Ethereum υπάρχουν για την πρόληψη τυχαίων ή μη επαναλαμβανόμενων βρόχων ή άλλης υπολογιστικής σπατάλης κώδικα (iBid). Άρα η ύπαρξη τους εισάγει ένα όριο στην Turing-complete φύση της γλώσσας προγραμματισμού του Ethereum, καθώς έτσι περιορίζεται ο αριθμός των βημάτων που μπορεί να εισαγάγει στην υλοποίηση ενός κώδικα, ο προγραμματιστής του. Οι συναλλαγές εκτελούνται σε κάθε κόμβο στο Blockchain και μια υπολογιστικά βαριά συναλλαγή, θα τους επιβαρύνει όλους, και με αυτόν τον τρόπο, τα τέλη λειτουργούν επίσης ως μέτρο κατά του spamming.

Το Ethereum εκτός από το πρώτο, είναι και το πιο δημοφιλές Blockchain, που έχει την δυνατότητα να λειτουργεί ένα "έξυπνο" συμβόλαιο (Rocha et al., 2018). Είναι ένα δημόσιο Blockchain με μία ενσωματωμένη γλώσσα προγραμματισμού (Solidity) που είναι Turing-complete, και επιτρέπει σε οποιονδήποτε να γράφει "έξυπνα" συμβόλαια και αποκεντρωμένες εφαρμογές (dApps). Ο προγραμματιστής του "έξυπνου" συμβολαίου μπορεί να δημιουργήσει τους κανόνες που επιθυμεί για ότι αφορά το συμβόλαιο, δηλαδή την ιδιοκτησία, τις συναλλαγές και τις λειτουργίες διαχείρισης κατάστασης. Όπως το Bitcoin, έτσι και το Ethereum χρησιμοποιούσε μηχανισμό συναίνεσης μορφής PoW, γνωστό ως Ethash, αντί του SHA256 του Bitcoin. Λόγω του Ethash, το Ethereum είναι πολύ γρήγορο και μπορεί να απαιτηθεί χρόνος μεταξύ 10 και 20 δευτερολέπτων για την παραγωγή ενός block (Christidis & Devetsikiotis, 2016). Ενώ ο Ethash είναι ικανός να αποτρέπει τις καταχρήσεις από πιθανό εξειδικευμένο υλικό, δεν βελτιώνει απαραίτητα την ανοχή σφαλμάτων και η αποθήκευση παρουσιάζει επίσης άλλο ένα πρόβλημα, καθώς το Ethereum απαιτεί από όλους τους κόμβους να αποθηκεύουν ένα Blockchain που είναι πολύ μεγαλύτερο από άλλα δίκτυα. Πλέον το Ethereum βρίσκεται σε φάση μετασχηματισμού για την υιοθέτηση ενός μηχανισμού συναίνεσης PoS, γνωστού ως Πρωτόκολλο Casper (Rosic, 2017a), η οποία φάση οδηγεί στη μετάβαση στο Ethereum 2.0 (Zanelatto Gavião Mascarenhas et al., 2020).

Το Ethereum, όπως έχει αναφερθεί, είναι το πρώτο σύστημα Blockchain που εφάρμοσε ένα Turing-complete πρωτόκολλο για την ανάπτυξη "έξυπνων" συμβολαίων και για τη λειτουργία του πρωτοκόλλου, είναι απαραίτητη η ύπαρξη των Ethereum Virtual Machines (EVMs). Το EVM περιγράφεται στο yellow paper του Ethereum (Wood, 2014), ως μία υπολογιστική μηχανή που λειτουργεί σαν αποκεντρωμένος υπολογιστής, η οποία διαχειρίζεται την κατάσταση του Blockchain και επιτρέπει την εκτέλεση και τη λειτουργικότητα των "έξυπνων" συμβολαίων. Ένα EVM υπάρχει σε κάθε κόμβο που συμμετέχει στο δίκτυο και βασίζεται σε 256 bits words, που σημαίνει ότι κάθε χώρος αποθήκευσης είναι 256 bit. Ένα συμβόλαιο γράφεται σε μία high-level γλώσσα προγραμματισμού και μεταγλωττίζεται σε ένα δυαδικό string, που ονομάζεται bytecode. Δηλαδή, όλα τα "έξυπνα" συμβόλαια είναι σύνολα εντολών, όπου το EVM τις μετατρέπει σε δυαδικό κώδικα μηχανής (binary machine code) και οι οποίες εκτελούνται σε

ακολουθία (Chen et al., 2017). Ένα "έξυπνο" συμβόλαιο προσδιορίζεται από μία διεύθυνση στο δίκτυο και ενεργοποιείται, όταν η διεύθυνση του αναφέρεται ως προορισμός από μια συναλλαγή. Οι διευθύνσεις των συμβολαίων ορίζονται τη στιγμή της δημιουργίας τους και είναι ικανά να εκτελούν διάφορες λειτουργίες, εκτός από τη μεταφορά Ether μεταξύ λογαριασμών. Μόλις ενεργοποιηθεί, το "έξυπνο" συμβόλαιο εκτελείται αυτόματα στο EVM κάθε κόμβου του δικτύου (Christidis & Devetsikiotis, 2016).

Στο Ethereum υπάρχουν ειδικά αντικείμενα κατάστασης (λογαριασμοί) και οι μεταβάσεις κατάστασης σημαίνουν μεταφορά assets μεταξύ λογαριασμών. Υπάρχουν δύο τύποι λογαριασμών, οι οποίοι είναι: α) Λογαριασμός εξωτερικής ιδιοκτησίας (Externally Owned Account - EOA), που ελέγχεται από το ιδιωτικό κλειδί του χρήστη, και β) Λογαριασμός συμβολαίου (Contract Account), που ελέγχεται από τον κώδικα του συμβολαίου του (Zanelatto Gavião Mascarenhas et al., 2020). Οι λογαριασμοί διακρίνονται με τη σειρά τους από το ότι μπορούν να ανήκουν σε δύο τύπους χρηστών: α) miners και β) traders, δηλαδή απλούς χρήστες. Ένας miner στοχεύει στο οικονομικό κέρδος από τη διαδικασία του mining και λαμβάνει μία αμοιβή λόγω της υπολογιστικής του εργασίας σε ένα block (όσο το Ethereum λειτουργεί με PoW). Ωστόσο, αυτή η αμοιβή μεταφέρεται μόνο μετά την εγγραφή του block στο Blockchain. Οι traders, από την άλλη πλευρά, χρησιμοποιούν την πλατφόρμα κυρίως για την εκτέλεση συμβολαίων ή για τη μεταφορά assets μεταξύ λογαριασμών. Ωστόσο και οι δύο, miners και traders, μπορούν να αλλάζουν ρόλους ανάλογα με το τι θέλουν τους (iBid).

Στη γλώσσα Solidity, όταν ένα έξυπνο συμβόλαιο μεταγλωττίζεται (compiled), για να εκτελεστεί από το EVM, μετατρέπεται σε μια ακολουθία από "operation codes" (οδηγίες λειτουργίας του κώδικα), επίσης γνωστές ως opcodes (Marchesi et al., 2020). Οι opcodes προσδιορίζονται με συντομογραφίες, για παράδειγμα ADD για την πρόσθεση, DIV για διαίρεση, κ.λπ. . Όλοι οι opcodes και η περιγραφή τους είναι διαθέσιμοι στο yellow paper του Ethereum (Wood, 2014). Το Ethereum χρησιμοποιεί το Gas, ως μονάδα μέτρησης για τον προσδιορισμό της μέγιστης υπολογιστικής εργασίας που θα δαπανηθεί για την επικύρωση μίας συναλλαγής (Zanelatto Gavião Mascarenhas et al., 2020). Κάθε opcode έχει μία προκαθορισμένη ποσότητα Gas που του έχει ανατεθεί, η οποία είναι μέτρο της υπολογιστικής προσπάθειας (ισχύος), που απαιτείται για την εκτέλεση της συγκεκριμένης λειτουργίας (Chen et al., 2017). Δηλαδή, το Gas είναι η χρέωση (fee) για την εκτέλεση του υπολογισμού, η οποία πληρώνεται από τον αποστολέα της συναλλαγής και ενεργοποιεί την λειτουργία. Σε γενικές γραμμές, η χρέωση είναι αναλογική της υπολογιστικής ισχύς που καταναλώνεται (Werner et al., 2020), αλλά όχι πάντα. Στον ***Πίνακα 4-1*** αναλύονται οι ποσότητες του Gas που απαιτούνται για διάφορες λειτουργίες στο Ethereum. Για παράδειγμα, η εφαρμογή της λειτουργίας call απαιτεί 20.000 Gas, ενώ η λειτουργία ADD απαιτεί 3 μονάδες Gas. Αξίζει να σημειωθεί ότι ένα "έξυπνο" συμβόλαιο

αποτελείται από πολυάριθμες πράξεις, ορισμένες από τις οποίες καταναλώνουν πολύ περισσότερο Gas από μια απλή αριθμητική πράξη. Οι λειτουργίες ανάγνωσης δεν απαιτούν Gas για να εκτελεστούν, ενώ οι λειτουργίες εγγραφής απαιτούν, επειδή επιφέρουν αλλαγές των μεταβλητών κατάστασης, οι οποίες πρέπει να κωδικοποιηθούν σε ένα νέο block του Blockchain.

Πίνακας 4-1: Ποσότητα Gas ανά opcodes (Chen et al., 2017)

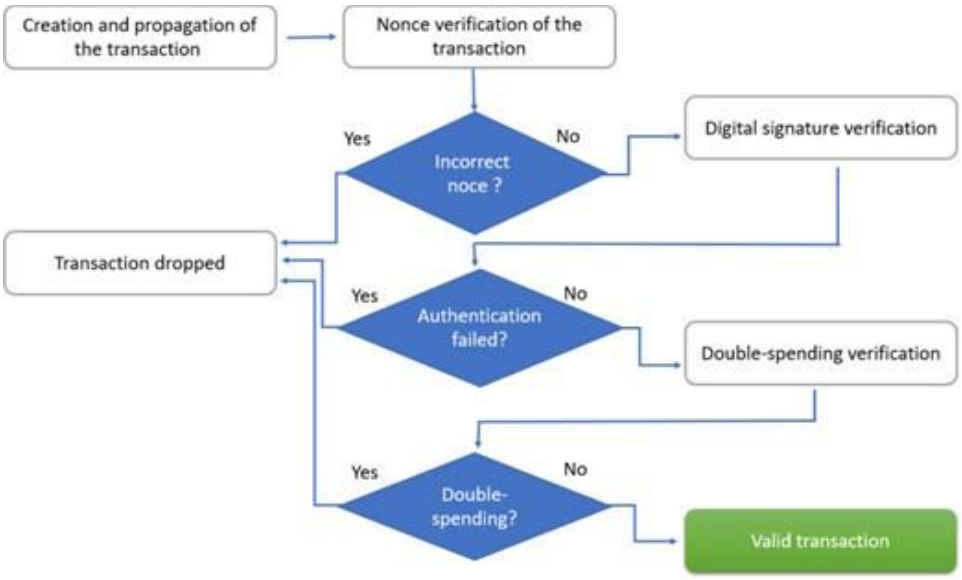
Operation	Gas	Description
ADD/SUB	3	Arithmetic operation
MUL/DIV	5	
ADDMOD/MULMOD	8	
AND/OR/XOR	3	Bitwise logic operation
LT/GT/SLT/SGT/EQ	3	Comparison operation
POP	2	Stack operation
PUSH/DUP/SWAP	3	
MLOAD/MSTORE	3	Memory operation
JUMP	8	Unconditional jump
JUMPI	10	Conditional jump
SLOAD	200	Storage operation
SSTORE	5,000/ 20,000	
BALANCE	400	Get balance of an account
CREATE	32,000	Create a new account using CREATE
CALL	25,000	Create a new account using CALL

Μια συναλλαγή στο Ethereum αναφέρεται σε μία ενέργεια που ξεκινάει από έναν λογαριασμό που διαχειρίζεται ένας άνθρωπος και όχι ένα συμβόλαιο, δηλαδή θα πρέπει να ξεκινάει από Externally Owned Account, και όχι από Contract Account. Όταν ένας χρήστης στείλει σε έναν άλλο χρήστη 1 ETH, ο λογαριασμός του αποστολέα πρέπει να χρεωθεί και ο λογαριασμός του παραλήπτη να πιστωθεί, και με την έναρξη αυτής της συναλλαγής από τον αποστολέα ξεκινάει η διαδικασία για τη ενημέρωση της κατάστασης του δικτύου Ethereum (Cook, 2022), για την ενημέρωση του Blockchain. Κάθε συναλλαγή Ethereum περιλαμβάνει δύο πεδία που ονομάζονται StartGas και GasPrice. Το StartGas είναι η μέγιστη ποσότητα Gas που διαθέτει η συναλλαγή για χρήση, ενώ το GasPrice είναι το τέλος που ο αποστολέας είναι πρόθυμος να πληρώσει ανά μονάδα Gas που καταναλώνεται. Το συνολικό τέλος υπολογίζεται πολλαπλασιάζοντας το συνολικό Gas που χρησιμοποιήθηκε για την εκτέλεση της συναλλαγής, με την τιμή GasPrice. Δηλαδή το γινόμενο των μονάδων Gas που απαιτούνται και της τιμή ανά μονάδα Gas (σε Ether), αντιπροσωπεύει τη μέγιστη ποσότητα Ether που σκοπεύει να ξοδέψει ένας χρήστης για την εξόρυξη της συναλλαγής του.

Με το να παρέχει τα ξεχωριστά πεδία για το Gas, το Ethereum καταφέρνει να αποσυνδέσει το κόστος εκτέλεσης και τη διακύμανση της τιμής του Ether, από τα συμβατικά χρήματα (δολάριο κτλ.). Αυτή η προσέγγιση είναι απαραίτητη εάν, για παράδειγμα, η τιμή του Ether αυξάνεται εκθετικά στην αγορά κρυπτονομισμάτων, καθώς μία συναλλαγή με σταθερή τιμή ανά

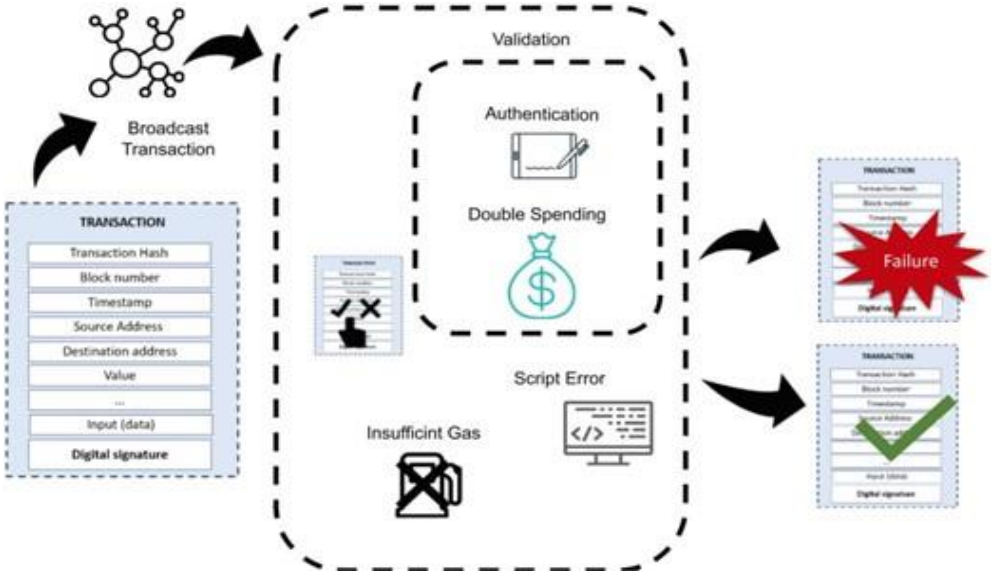
υπολογισμό θα μπορούσε να καταστεί απαγορευτική. Αυτό μετριάζεται με τη χρήση του GasPrice, καθώς το επιλέγει ο χρήστης για κάθε συναλλαγή. Στο προηγούμενο σενάριο, ακόμη και αν η ποσότητα Gas που καταναλώνεται από μία συγκεκριμένη συναλλαγή παραμένει σταθερή, η τιμή του Gas μπορεί να μειωθεί ώστε να επιτρέψει στο δίκτυο να λειτουργεί με λογικό κόστος.

Οι συναλλαγές στο Ethereum περνούν από διάφορα βήματα για να επικυρωθούν (***Σχήμα 4-18***). Αυτά τα βήματα περιλαμβάνουν την επαλήθευση: α) της ψηφιακής υπογραφής των χρηστών, β) του nonce της συναλλαγής, γ) του StartGas που δεν πρέπει να είναι μικρότερο από την ποσότητα Gas που απαιτείται για την εκτέλεση της συναλλαγής και δ) την επαλήθευση του υπολοίπου του λογαριασμού του αποστολέα που πρέπει να διαθέτει τουλάχιστον το κόστος συναλλαγής.



Σχήμα 4-18: Διάγραμμα ροής διαδικασίας επαλήθευσης συναλλαγών (Zanelatto Gavião Mascarenhas et al., 2020)

Εάν το συνολικό Gas υπερβαίνει την ποσότητα StartGas που παρέχεται, τότε η συναλλαγή δεν επικυρώνεται (Zanelatto Gavião Mascarenhas et al., 2020). Στο ***Σχήμα 4-19***, παρουσιάζεται η κατάσταση συναλλαγής στο Ethereum.



Σχήμα 4-19: Κατάσταση συναλλαγής στο Ethereum (Zanelatto Gavião Mascarenhas et al., 2020)

Μόλις επικυρωθεί μία συναλλαγή, είναι διαθέσιμη για την εισαγωγή της σε ένα block από έναν miner. Αυτή η διαδικασία είναι παρόμοια με αυτή που συμβαίνει στο Bitcoin, όπου οι συναλλαγές εξορύσσονται πριν εισαχθούν στο Blockchain. Ωστόσο, το Ethereum έχει κάποιες διαφορές σε σύγκριση με το Bitcoin, όπως για παράδειγμα ανταμείβει τους miners που δεν εξόρυξαν με επιτυχία τη συναλλαγή.

Hyperledger Fabric

Η πλατφόρμα Hyperledger Fabric (hyperledger.org) αποτελεί ένα δίκτυο Blockchain με έλεγχο πρόσβασης (permissioned) που εφαρμόζει "έξυπνα" συμβόλαια βασισμένα σε μηχανισμό συναίνεσης Practical Byzantine Fault Tolerance (PBFT) και περιλαμβάνει συστήματα βελτίωσης της ασύμμετρης κρυπτογράφησης και ψηφιακές υπογραφές SHA3 και ECDSA (Cachin, 2016). Ο έλεγχος πρόσβασης της Hyperledger Fabric ενισχύει την ασφάλεια του δικτύου μέσω της αποτροπής επιθέσεων, όπως οι επιθέσεις Sybil. Επιπλέον, η εφαρμογή "έξυπνων" συμβολαίων στην Hyperledger Fabric περιλαμβάνει κώδικα, ο οποίος μπορεί να εκτελέσει μόνος του κινήσεις, όπως μεταβίβαση περιουσιακών στοιχείων ή μεταφορές πόρων μεταξύ κόμβων σε χιλιοστά του δευτερολέπτου (Samaniego & Deters, 2016; Smith & Christidis, 2016). Αυτός ο χρόνος είναι ιδιαίτερα χαμηλός μεταξύ των ανταγωνιστικών συστημάτων Blockchain και είναι το πλεονέκτημα της πλατφόρμας. Η υιοθέτηση του PBFT αποτρέπει το υπολογιστικά δαπανηρό mining, ωστόσο, υπάρχει μία αντιστάθμιση των άμεσων υπολογιστικών γενικών εξόδων με τη χρήση του δικτύου.

Counterparty

Η πλατφόρμα Counterparty (counterparty.io) δε διαθέτει δικό της Blockchain, αλλά αντίθετα ενσωματώνει τα δεδομένα της σε συναλλαγές του Bitcoin. Ενώ οι κόμβοι του δικτύου Blockchain του Bitcoin είναι αδιάφοροι για τα δεδομένα που είναι ενσωματωμένα σε αυτές τις συναλλαγές, οι κόμβοι του Counterparty τα αναγνωρίζουν και τα ερμηνεύουν. Τα "έξυπνα" συμβόλαια της πλατφόρμας μπορούν να γραφτούν στην ίδια γλώσσα που χρησιμοποιεί και το Ethereum (solidity), ωστόσο κανένα πρωτόκολλο συναίνεσης δεν χρησιμοποιείται για την επικύρωση των αποτελεσμάτων των υπολογισμών. Ο αντισυμβαλλόμενος έχει το δικό του κρυπτονόμισμα, το οποίο μπορεί να μεταφερθεί μεταξύ των χρηστών και να δαπανηθεί για την εκτέλεση των συμβολαίων. Οι κόμβοι δεν λαμβάνουν τέλη για την εκτέλεση των συμβολαίων, αλλά αντίθετα χρησιμοποιείται ο μηχανισμός Proof of Burn, που αναλύθηκε σε προηγούμενο κεφάλαιο. Τα τέλη που πληρώνουν οι πελάτες καταστρέφονται και οι κόμβοι ανταμείβονται έμμεσα, από τον πληθωρισμό του νομίσματος (Bartoletti & Pompianu, 2017).

Monax

Η πλατφόρμα Monax (monax.io) δεν έχει δικό της κρυπτονόμισμα, αλλά υποστηρίζει την εκτέλεση "έξυπνων" συμβολαίων μέσω του Blockchain του Ethereum. Η πλατφόρμα στους χρήστες να δημιουργούν ιδιωτικά Blockchain και να καθορίζουν τις πολιτικές εξουσιοδότησης που επιθυμούν, για την πρόσβαση σε αυτά. Ως μηχανισμό συναίνεσης χρησιμοποιεί το Tendermint (tendermint.com), το οποίο όπως είδαμε σε προηγούμενο κεφάλαιο, είναι μορφή του Practical Byzantine Fault Tolerance (PBFT). Μέσω του Tendermint οργανώνεται ψηφοφορία σε γύρους, όπου ένας συμμετέχων προτείνει ένα νέο block συναλλαγών και οι άλλοι το ψηφίζουν. Όταν ένα block δεν εγκριθεί, το πρωτόκολλο μετακινείται στον επόμενο γύρο ψηφοφορίας, όπου ένας άλλος συμμετέχων θα είναι υπεύθυνος να προτείνει ένα νέο block. Όπως συμβαίνει και στον PBFT, ένα block επιβεβαιώνεται όταν εγκριθεί από πάνω από τα 2/3 των συνολικών κόμβων (Bartoletti & Pompianu, 2017).

Stellar

Η πλατφόρμα Stellar (stellar.org) διαθέτει ένα δημόσιο Blockchain με το δικό της κρυπτονόμισμα και λειτουργεί με αλγόριθμο συναίνεσης εμπνευσμένο από την κατηγορία των Βυζαντινών συμφωνιών (Mazieres, 2015). Ένας κόμβος συμφωνεί σε μια συναλλαγή, αν συμφωνούν και οι κόμβοι κοντά του, τους οποίους θεωρεί πιο αξιόπιστους από τους άλλους. Όταν η συναλλαγή γίνει αποδεκτή από αρκετούς κόμβους του δικτύου θεωρείται επιβεβαιωμένη και είναι ανέφικτο για έναν κακόβουλο χρήστη να την ακυρώσει. Για την ανάπτυξη των "έξυπνων" συμβολαίων σε αυτήν την πλατφόρμα, δεν υπάρχει συγκεκριμένη γλώσσα προγραμματισμού. Ωστόσο, είναι δυνατό να συγκεντρωθούν ορισμένες συναλλαγές

που βρίσκονται στο Blockchain, οι οποίες περιλαμβάνουν διαφορετικές διευθύνσεις, και να χρησιμοποιηθούν για την υλοποίηση "έξυπνων" συμβολαίων για απλές συναλλαγές μεταξύ χρηστών, όπως και στο Bitcoin. Η πλατφόρμα Stellar διαθέτει ειδικούς λογαριασμούς, που ονομάζονται "multisignature", τους οποίους μπορούν να χειριστούν αρκετοί κάτοχοι. Για την εκτέλεση λειτουργιών σε αυτούς τους λογαριασμούς, πρέπει να επιτευχθεί ένα όριο συναίνεσης μεταξύ των ιδιοκτητών και μπορούν να συνδυαστούν για τη δημιουργία πιο σύνθετων συμβολαίων (Bartoletti & Pompianu, 2017).

Lisk

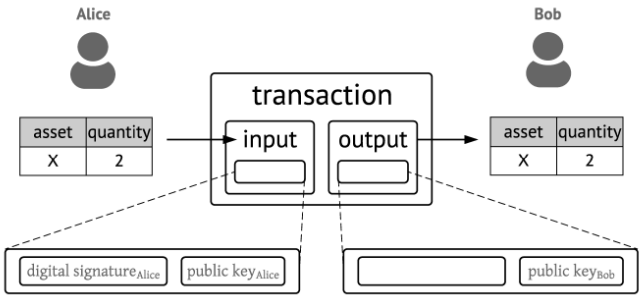
Η πλατφόρμα Lisk (lisk.io) έχει το δικό της κρυπτονόμισμα και είναι ένα δημόσιο Blockchain, που χρησιμοποιεί ως μηχανισμό συναίνεσης το Delegated Proof of Stake (DPoS). Συνολικά 101 ενεργοί αντιπρόσωποι, οι οποίοι εκλέγονται από τους χρήστες του συστήματος, είναι αυτοί που έχουν την εξουσία να δημιουργούν νέα blocks. Οι χρήστες του συστήματος, εκτός της δυνατότητα να ψηφίσουν, μπορούν να θέσουν οι ίδιοι υποψηφιότητα. Η πλατφόρμα Lisk υποστηρίζει την εκτέλεση "έξυπνων" συμβολαίων γραμμένων είτε σε JavaScript είτε σε Node.js. Σε αντίθεση με το Ethereum, ο ντετερμινισμός των εκτελέσεων δεν διασφαλίζεται από τη γλώσσα προγραμματισμού, αλλά πρέπει οι ίδιοι οι προγραμματιστές να φροντίζουν για αυτό (π.χ. να μην χρησιμοποιούν συναρτήσεις όπως το Math.random). Παρ' όλο που όπως αναφέρθηκε, η πλατφόρμα Lisk έχει ένα κύριο δημόσιο Blockchain, κάθε "έξυπνο" συμβόλαιο εκτελείται σε ξεχωριστό. Οι χρήστες μπορούν να μεταφέρουν κρυπτονομίσματα από ένα συμβόλαιο προς την κύρια αλυσίδα και αντίστροφα, αποφεύγοντας το "double spending". Οι κάτοχοι συμβολαίων μπορούν να προσαρμόσουν το Blockchain τους πριν τα δημοσιεύσουν, επιλέγοντας ποιοι κόμβοι μπορούν να συμμετάσχουν στο μηχανισμό συναίνεσης των συμβολαίων τους (Bartoletti & Pompianu, 2017).

4.8. Κρυπτονομίσματα και Tokens

Τα κρυπτονομίσματα και τα tokens είναι παράγωγα των συστημάτων Blockchain. Όπως αναφέρθηκε στην αρχή αυτού του παραδοτέου, ένα δίκτυο Blockchain μπορεί να λειτουργήσει χωρίς να έχει κάποιο υποκείμενο κρυπτονόμισμα. Όμως δεν μπορεί να συμβεί το αντίθετο, δηλαδή για την ύπαρξη ενός κρυπτονομίσματος, είναι απαραίτητο ένα δίκτυο Blockchain. Τα κρυπτονομίσματα είναι πάντα εγγενή με κάποιο Blockchain, γεννιούνται δηλαδή μαζί με ένα δίκτυο Blockchain και χρησιμοποιούνται ως μέσο συναλλαγών σε αυτό. Αντίστοιχα για να δημιουργηθεί ένα token, αυτό θα πρέπει να είναι εξαρτημένο από υπάρχον κρυπτονόμισμα και επίσης απαιτείται ένα "έξυπνο" συμβόλαιο μέσα στο ήδη υφιστάμενο Blockchain, που λειτουργεί αυτό το κρυπτονόμισμα. Αυτή είναι η μεγαλύτερη διαφορά μεταξύ ενός κρυπτονομίσματος και ενός token, ότι δηλαδή τα κρυπτονομίσματα είναι το εγγενές

περιουσιακό στοιχείο ενός δικτύου Blockchain (όπως το Bitcoin), ενώ τα tokens είναι το περιουσιακό στοιχείο ενός "έξυπνου" συμβολαίου, που έχει φτιαχτεί για τη δημιουργία αυτού το token. Τα κρυπτονομίσματα και τα tokens μοιράζονται πολλές ομοιότητες, αλλά τα κρυπτονομίσματα είναι τα μόνα που χρησιμοποιούνται αποκλειστικά ως οικονομικά μέσα για ανταλλαγές, πληρωμές κτλ. Ένα token είναι μία αναπαράσταση ενός περιουσιακού στοιχείου ή υπηρεσίας που έχει γίνει tokenized σε ένα Blockchain κρυπτονομίσματος, αλλά δεν είναι ενσωματωμένο νόμισμα. Παρ' όλα αυτά μπορεί να δημιουργηθεί και να ανήκει σε κάποιον χρήστη, αλλά και να μεταφερθεί σε άλλους, δημιουργώντας έτσι και αυτό οικονομικά συστήματα (Chen et al., 2020). Το token εξαρτάται πάντα από το κρυπτονόμισμα, αλλά είναι ευκολότερο να τεθεί σε κυκλοφορία στην αγορά, καθώς πρακτικά δεν απαιτείται κόστος συντήρησης του δικτύου Blockchain. Άλλη μία βασική διαφορά μεταξύ κρυπτονομισμάτων και tokens είναι ότι οι miners λαμβάνουν κρυπτονομίσματα ως επιβράβευση, για τις υπηρεσίες που παρέχουν στο δίκτυο μέσω της επικύρωσης συναλλαγών και της δημιουργίας νέων blocks, αλλά αυτό δεν ισχύει για τα tokens (Freni et al., 2022), τα οποία μπορούν να συλλεχθούν μόνο με βάση τους τρόπους που έχουν αποφασιστεί από τη συγγραφή του "έξυπνου" συμβολαίου τους.

Ένα κρυπτονόμισμα, ή ένα token, λειτουργεί ουσιαστικά σαν μία βάση δεδομένων με ορισμένους περιορισμούς. Η βάση αυτή μπορεί να εκτελέσει μία μόνο λειτουργία που προσομοιώνει μία συναλλαγή. Μία συναλλαγή πραγματοποιείται αφαιρώντας κάποιες μονάδες ενός asset από το υπόλοιπο ενός χρήστη και προσθέτοντάς τις στο υπόλοιπο ενός άλλου χρήστη. Οι περιορισμοί επιβάλλουν ότι το υπόλοιπο του πρώτου χρήστη είχε τουλάχιστον τις ζητούμενες μονάδες πριν από τη συναλλαγή και προφανώς ο χρήστης πρέπει να εγκρίνει τη συναλλαγή. Για να γίνει tokenization, το μόνο που χρειάζεται είναι να εφαρμοστεί αυτή η λογική σε ένα έξυπνο συμβόλαιο. (Lesavre et al., 2021).Στο ***Σχήμα 4-20*** αποτυπώνεται ένα παράδειγμα μεταφοράς κρυπτονομισμάτων ή tokenized assets από έναν χρήστη σε έναν άλλο, στο Blockchain. Ο αποστολέας υπογράφει το input και δημιουργεί ένα output για το δημόσιο κλειδί του παραλήπτη, ώστε μόνο αυτός να μπορεί να το ξοδέψει.



Σχήμα 4-20: Παράδειγμα μεταφοράς assets στο Blockchain (Christidis & Devetsikiotis, 2016)

4.8.1. Κρυπτονομίσματα

Το Bitcoin, η εφαρμογή με την οποία γεννήθηκε η τεχνολογία Blockchain (Nakamoto, 2008), είναι το πρώτο και πιο γνωστό κρυπτονόμισμα παγκοσμίως, αλλά και το πιο επιτυχημένο σενάριο εφαρμογής του Blockchain μέχρι στιγμής. Πριν όμως από αυτό είχαν γίνει και άλλες προσπάθειες εφαρμογής κατανεμημένων συστημάτων για τη δημιουργία ψηφιακού χρήματος, καθώς αναπτύχθηκαν διάφορες εφαρμογές με παρόμοια χαρακτηριστικά, που μπορούν να αναγνωριστούν ως προκάτοχοι του Bitcoin και άλλων κρυπτονομισμάτων (Arslanian & Fischer, 2019). Αξιοσημείωτο παράδειγμα είναι το "B-money" (Dai, 1998), που προτάθηκε από τον Wei Dai. Η πρόταση του αφορούσε ένα ανώνυμο και κατανεμημένο τρόπο, που έδινε τη δυνατότητα σε ομάδα χρηστών με μη ανιχνεύσιμα ψηφιακά ψευδώνυμα, να πληρώνουν ο ένας τον άλλον με χρήματα και να επιβάλλουν συμβάσεις μεταξύ τους, χωρίς εξωτερικό διαμεσολαβητή. Την ίδια περίπου περίοδο ο Nick Szabo δημιούργησε το "bit gold" (Szabo, 1998). Το bit gold, όπως και το Bitcoin, ήταν ένα σύστημα ηλεκτρονικού νομίσματος που επέβαλε στους χρήστες να λύσουν προβλήματα με PoW με αντίστοιχα κρυπτογραφικά χαρακτηριστικά, με το Blockchain. Αργότερα, ο Hal Finney ακολούθησε το έργο των Dai και Szabo, και δημιούργησε ένα νομισματικό σύστημα βασισμένο σε ένα επαναχρησιμοποιήσιμο PoW (Finney, 2004). Είναι αξιοσημείωτο, ότι ο Finney ήταν ο παραλήπτης της πρώτης συναλλαγής που έγινε ποτέ στο Blockchain του Bitcoin, το 2009.

Το κρυπτονόμισμα Bitcoin ήταν η πρώτη μορφή ψηφιακού νομίσματος που προσέλκυσε τη μεγάλη προσοχή του κοινού και των επενδυτών. Κατά την έναρξή του, υπήρχαν μόνο 50 Bitcoins σε κυκλοφορία στην αγορά, και μόνο άνθρωποι με γνώσεις τεχνολογίας έδειχναν ενδιαφέρον για αυτό. Το 2010, η ιαπωνική εταιρεία MT.GOX (mtgox.com) ξεκίνησε μία πλατφόρμα με μέσο συναλλαγών το Bitcoin, με μία ισοτιμία, όπου 1$ ΗΠΑ αντιστοιχούσε σε περίπου 20 Bitcoins (Fauzi, et al., 2020). Πλέον, καθώς η χρήση και η αναγνωσιμότητα του Bitcoin έχε αυξηθεί κατά πολύ, η τιμή του επίσης έχει κλιμακωθεί σε τεράστιο βαθμό με 1 Bitcoin να αντιστοιχεί σε δεκάδες χιλιάδες δολάρια ΗΠΑ. Ήδη, πριν τη μεγάλη οικονομική έκρηξη της αξίας των κρυπτονομισμάτων, το World Economic Forum (2015), είχε κάνει την πρόβλεψη ότι το 10% του παγκόσμιου ΑΕΠ θα είναι αποθηκευμένο σε Blockchain. Όλα αυτά είχαν σαν αποτέλεσμα να δημιουργηθεί ο νόμος περί κρυπτονομισμάτων του 2020 στις ΗΠΑ, ο οποίος αναγνώρισε επίσημα και νομιμοποίησε τη χρήση των κρυπτονομισμάτων ως μέσα πληρωμής, κάτι το οποίο αποτέλεσε ένα βήμα προς την αναγνώριση τους από το παγκόσμιο οικονομικό σύστημα (Mikhaylov, 2020). Παρ' όλα αυτά, η τεχνολογία Blockchain για την ανάπτυξη κρυπτονομισμάτων, έχει προκαλέσει πολλές επικρίσεις από τις κυβερνήσεις και τον οικονομικό τομέα, λόγω της ανωνυμίας που παρέχει στους χρήστες (van Erp, 2017).

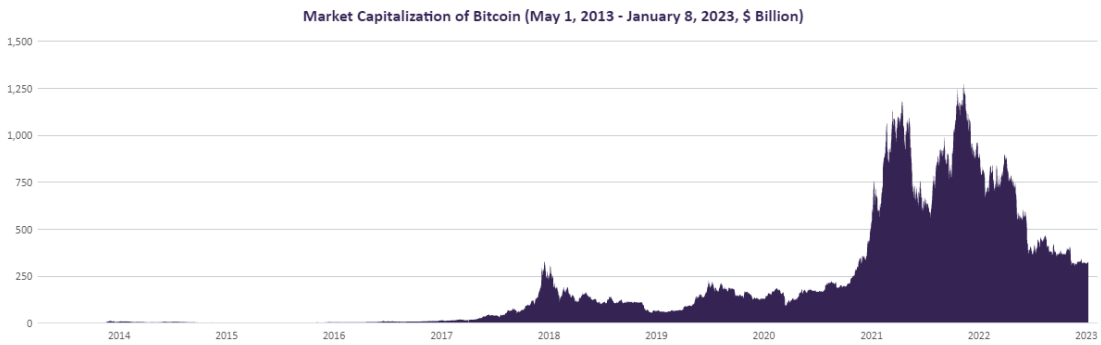
Μετά το Bitcoin, ακολούθησε το 2011 το Namecoin (namecoin.org), που αναπτύχθηκε ως μια προσπάθεια δημιουργίας ενός αποκεντρωμένου DNS (Domain Name System), καθιστώντας πολύ δύσκολη τη λογοκρισία στο διαδίκτυο. Λίγο αργότερα την ίδια χρονιά, κυκλοφόρησε το Litecoin (litecoin.org), που ήταν το πρώτο επιτυχημένο κρυπτονόμισμα που δε χρησιμοποίησε SHA-256 ως hash function. Επίσης αξιοσημείωτο είναι το Peercoin (peercoin.net), το οποίο έχει ήδη αναφερθεί στην ανάλυση του μηχανισμού Proof of Stake, καθώς ήταν το πρώτο που χρησιμοποίησε έναν υβριδικό μηχανισμό PoW-PoS. Από τότε έχουν αναπτυχθεί πάρα πολλά κρυπτονομίσματα, αλλά μόνο λίγα έχουν πετύχει.

Τα κρυπτονομίσματα έχουν σημαντικά χαρακτηριστικά που τα διαφοροποιούν από τα παραδοσιακά χρήματα, με τα πιο σημαντικά από αυτά να είναι η διαφάνεια, η ασφάλεια και το απόρρητο του κατόχου (Chang et al., 2018), έχοντας όμως προφανώς άλλα μειονεκτήματα. Διαφέρουν από το ηλεκτρονικό χρήμα, που διακινείται μέσω των παραδοσιακών τραπεζών ή σύγχρονων ψηφιακών πορτοφολιών (π.χ. Revolut) για τους παρακάτω πέντε λόγους (Yuan et al., 2018):

1. Το Bitcoin είναι πλήρως αποκεντρωμένο, χωρίς κεντρικό έλεγχο ή ιεραρχική δομή, ενώ τα ηλεκτρονικό χρήμα χρειάζεται παρόχους υπηρεσιών, και επομένως ελέγχεται κεντρικά από κυβερνήσεις ή εταιρείες.
2. Το Bitcoin είναι ψευδο-ανώνυμο, δηλαδή κάποιος μπορεί να γνωρίζει τη διεύθυνση ενός χρήστη Bitcoin, αλλά δεν μπορεί να γνωρίζει ακριβώς ποιος είναι. Αντίθετα, στην περίπτωση του ηλεκτρονικού χρήματος, οι ταυτότητες των χρηστών καταγράφονται από τους κεντρικούς παρόχους υπηρεσιών, καθώς η υπηρεσία Know-you-customer (KYC) είναι νομικά απαραίτητη.
3. Τα νομίσματα του Bitcoin δεν μπορούν ξεπεράσουν ένα συγκεκριμένο όριο, δηλαδή τα 21.000.000. Αντίθετα η έκδοση του ηλεκτρονικού χρήματος εξαρτάται από του κεντρικούς παρόχους (π.χ. κεντρικές τράπεζες), οι οποίοι μπορούν να λάβουν την απόφασή του να αυξήσουν ή να μειώσουν την προσφορά, κάτι που προκαλεί πληθωρισμό ή αποπληθωρισμό.
4. Το Bitcoin είναι ανοιχτού κώδικα για το κοινό και ο καθένας μπορεί να ελέγξει τον πηγαίο κώδικα και να κατανοήσει τους υποκείμενους μηχανισμούς της έκδοσης Bitcoin, σε αντίθεση με το ηλεκτρονικό χρήμα, του οποίου η επιχειρηματική λογική δεν είναι γνωστή στους χρήστες.
5. Το Bitcoin από μόνο του, είναι μόνο μια ακολουθία κώδικα, χωρίς αξία. Ωστόσο, μπορεί να αποκτήσει αξία αυξάνοντας αυτούς που το εμπιστεύονται και το χρησιμοποιούν.

Σύμφωνα με το coinmarketcap.com, μέχρι τον Ιανουάριο του 2023, έχουν εκδοθεί 19,3 εκατομμύρια Bitcoin, με περίπου 1,7 εκατομμύρια Bitcoin να μην έχουν ακόμη κυκλοφορήσει.

Όπως έχει αναφερθεί, το genesis block του Bitcoin, δημιουργήθηκε τον Ιανουάριο του 2009 και χρησιμοποιεί τη βασική μορφή του μηχανισμού PoW, με τη διαδικασία του mining για την εγγραφή του νέου block στην αλυσίδα. Όταν αυτό συμβεί, το σύστημα του Bitcoin δημιουργεί μία συγκεκριμένη ποσότητα από το κρυπτονόμισμα, η οποία λειτουργεί ως ανταμοιβή για το miner και ως κίνητρο για τους υπόλοιπους κόμβους, ώστε να συνεχίσουν να συνεισφέρουν την υπολογιστική τους ισχύ. Ο αριθμός των Bitcoin που δίνονται ως ανταμοιβή στους miners για κάθε συναλλαγή μειώνεται κατά 50%, μετά από κάθε 210.000 blocks, ή περίπου μία φορά κάθε τέσσερα χρόνια (Baker, 2022). Η ανταμοιβή εκφράζεται σε satoshis, όπου ένα Satoshi είναι ίσο με 0,00000001 Bitcoins. Η αξία οποιουδήποτε κρυπτονομίσματος καθορίζεται πολλαπλασιάζοντας την τρέχουσα τιμή του με τον συνολικό αριθμό νομισμάτων που βρίσκονται σε κυκλοφορία. Το Bitcoin έφτασε την υψηλότερη κεφαλαιοποίηση της ιστορίας του, στις 9 Νοεμβρίου 2021, στα 1,28 τρισεκατομμύρια δολάρια ΗΠΑ, όπως φαίνεται στο ***Σχήμα 4-21***.

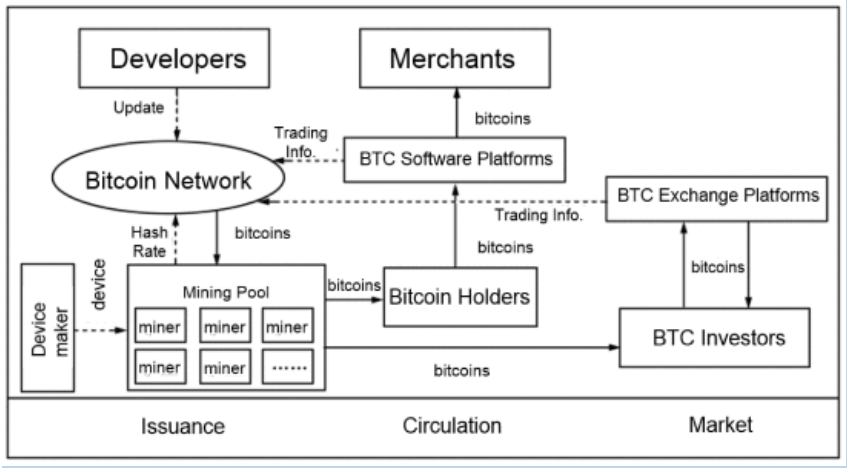


Σχήμα 4-21: Κεφαλαιοποίηση του Bitcoin ανά ημέρα (GlobalData, 2023)

Η ιδιοκτησία των κρυπτονομισμάτων καταγράφεται στο αποκεντρωμένο καθολικό του Blockchain, όπου τα δεδομένα διατηρούνται δημόσια. Οι κάτοχοι των κρυπτονομισμάτων μπορούν να τα αποθηκεύσουν, χρησιμοποιώντας μία εφαρμογή λογισμικού που ονομάζεται wallet (πορτοφόλι) και να τα αποστείλουν σε άλλους χρήστες, κάνοντας συναλλαγές στο Blockchain. (Hinzen et al., 2019). Εάν κάποιος θέλει να στείλει Bitcoin, ο αποστολέας δημιουργεί ένα μήνυμα που περιέχει, μεταξύ άλλων, τις πληροφορίες σχετικά με τη διεύθυνση του wallet του παραλήπτη και το ποσό των Bitcoin (Xu, 2016). Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί, με αλγόριθμο ψηφιακής υπογραφής (Franco, 2014). Αυτό το υπογεγραμμένο μήνυμα αποστέλλεται στο δίκτυο. Οι κόμβοι στο δίκτυο μπορούν στη συνέχεια να χρησιμοποιήσουν το δημόσιο κλειδί του αποστολέα για να επαληθεύσουν εάν το μήνυμα (και επομένως η συναλλαγή) είναι έγκυρο και κατά συνέπεια γίνεται αποδεκτό ή απορρίπτεται (Badev & Chen, 2014). Σε αυτό το βήμα, το Blockchain χρησιμοποιείται επίσης για να ελέγξει

εάν αυτό το ποσό Bitcoin είναι πραγματικά διαθέσιμο στον αποστολέα (Xu, 2016). Εάν το μήνυμα γίνει αποδεκτό, η συναλλαγή εκτελείται και επισυνάπτεται στο Blockchain σε ένα block με άλλες αποδεκτές συναλλαγές. Οι συναλλαγές του Bitcoin μπορούν να προγραμματιστούν και να ελεγχθούν από σενάρια που βασίζονται σε αλγόριθμους και "έξυπνα" συμβόλαια, που όμως δεν είναι Turing-complete, έτσι ώστε να πραγματοποιείται η αυτόματη κυκλοφορία του κρυπτονομίσματος (Nakamoto, 2017).

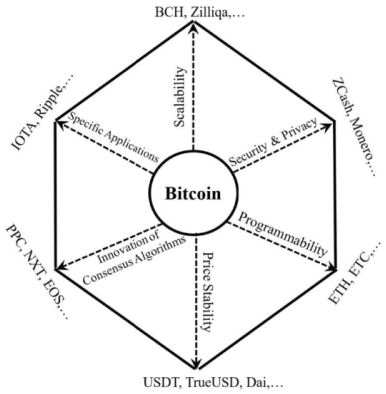
Το Bitcoin, όπως και τα περισσότερα κρυπτονομίσματα, είναι ένα αυτόνομο σύστημα που αποτελείται από την έκδοση, την κυκλοφορία και την αγορά του κρυπτονομίσματος (Yuan et al., 2018), όπως απεικονίζεται στο ***Σχήμα 4-22***. Στο επίπεδο της έκδοσης, το δίκτυο διατηρείται και ενημερώνεται από τους προγραμματιστές και λαμβάνει υπολογιστική ισχύ από τους miners ώστε να παράξει Bitcoins ως ανταμοιβή προς τους miners. Οι miners μπορούν να συμμετάσχουν στη διαδικασία μεμονωμένα ή να συνεργαστούν μπαίνοντας σε κάποιο mining pool, ώστε να αυξηθεί η πιθανότητα επιτυχούς δημιουργίας ενός block. Για την κυκλοφορία του Bitcoin, οι κάτοχοι του κρυπτονομίσματος Bitcoin αγοράζουν τύπους αγαθών ή υπηρεσιών από εμπόρους μέσω λογισμικού, όπως τα wallets. Τέλος, στο επίπεδο της αγοράς, η τιμή του Bitcoin παρουσιάζει ανοδικές τάσεις, αλλά και συχνές διακυμάνσεις, γεγονός που το έχει μετατρέψει σε επενδυτικό προϊόν, μέσα από πλατφόρμες ανταλλακτηρίων. Προφανώς, όλες οι συναλλαγές, και στο επίπεδο της κυκλοφορίας και στο επίπεδο της αγοράς, καταγράφονται στο Blockchain του Bitcoin.



Σχήμα 4-22: Πλαίσιο έκδοσης, κυκλοφορίας και αγοράς Bitcoin (Yuan et al., 2018)

Εμπνευσμένα από τη μεγάλη επιτυχία του Bitcoin, πάρα πολλά ακόμα εγγενή κρυπτονομίσματα δικτύων Blockchain εμφανίζονται στην αγορά. Τα περισσότερα από αυτά τα κρυπτονομίσματα, γνωστά και ως altcoins, επινοούνται με στόχο τη βελτίωση της απόδοσης του Bitcoin. Επί του παρόντος, έχουν αναγνωριστεί έξι κύριες κατευθύνσεις για τη δημιουργία κρυπτονομισμάτων

(Yuan et al, 2018), όπως φαίνεται στο ***Σχήμα 4-23***. Η πρώτη κατεύθυνση εστιάζει στην επεκτασιμότητα, όπου για παράδειγμα το Bitcoin cash (BCH), το οποίο διαχωρίζεται από την αλυσίδα του Bitcoin, επεκτείνει το μέγεθος ενός block από 1MB σε 8MB. Αυτό επιτρέπει περισσότερες συναλλαγές να συσκευάζονται σε ένα ενιαίο block σε κάθε γύρο mining, έχοντας έτσι βελτιωμένη ικανότητα επεξεργασίας συναλλαγών και μειωμένο χρόνο επιβεβαίωσης συναλλαγών. Στην ίδια κατεύθυνση, το Zilliqa (ZIL) βελτιώνει την απόδοση χρησιμοποιώντας την τεχνική κοινής χρήσης δικτύου, η οποία μπορεί να χωρίσει αυτόματα το δίκτυο Blockchain σε πολλά μικρότερα κομμάτια που επικυρώνουν τις συναλλαγές παράλληλα. Η δεύτερη κατεύθυνση στοχεύει στη βελτίωση της ασφάλειας και της προστασίας της ιδιωτικής ζωής με κρυπτογραφικές τεχνικές, όπως το ZCash (ZEC) και το Monero (XMR). Η τρίτη κατεύθυνση ενισχύει τη δυνατότητα προγραμματισμού των συστημάτων Blockchain και το πιο γνωστό παράδειγμα είναι το Ether (ETH) (το οποίο έχει ήδη αναφερθεί εκτενώς), που υποστηρίζει Turing-complete "έξυπνα" συμβόλαια και dApps. Η τέταρτη κατεύθυνση στοχεύει στη σταθερότητα των τιμών, όπως για παράδειγμα το Tether (USDT) που είναι ισοδύναμο σε αξία με το δολάριο ΗΠΑ (ισοτιμία 1 προ 1) και μπορεί να βοηθήσει στη μεταφοράς συμβατικών νομισμάτων και να παράσχει στους χρήστες μια σταθερή εναλλακτική λύση στο Bitcoin. Η πέμπτη κατεύθυνση βασίζεται σε καινοτομίες των αλγορίθμων συναίνεσης, όπως το PeerCoin (PPC) και το EOS. Τέλος, η έκτη κατεύθυνση στην καινοτομία των κρυπτονομισμάτων είναι αφιερωμένη σε συγκεκριμένα σενάρια εφαρμογών, όπως το IOTA (προσανατολισμένο στην τεχνολογία του Internet of Things), το Ripple (χρησιμοποιείται για χρηματοοικονομικούς διακανονισμούς) και το Augur (δημιουργήθηκε για εφαρμογές στην που κάνουν προβλέψεις των αγορών).



Σχήμα 4-23: Έξι κατευθύνσεις στην καινοτομία κρυπτονομισμάτων (Yuan et al., 2018)

Στη συνέχεια, θα γίνει αναφορά σε γνωστά κρυπτονομίσματα, εκτός του Bitcoin και του Ether, που έχουν ήδη αναλυθεί.

Litecoin

Το Litecoin (LTC) είναι ένα κρυπτονόμισμα ανοιχτού κώδικα και είναι ένα από τα πρώτα που δημιουργήθηκαν, τον Οκτώβριο του 2011. Ο μηχανισμός συναίνεσης στο Litecoin βασίζεται στον αλγόριθμο Scrypt PoW, με τη χρήση του αλγόριθμου κρυπτογράφησης SHA-256 που χρησιμοποιείται και από το Bitcoin (Rosic, 2017b). Διαφέρει από το Bitcoin για δύο λόγους. Πρώτον, η χρήση του μηχανισμού Scrypt PoW στο Litecoin είναι πολύ πιο γρήγορη από το Bitcoin, καθώς στο Litecoin χρειάζονται κατά μέσο όρο 2,5 λεπτά για την παραγωγή ενός block στο Blockchain (Emeç et al, 2020), ενώ αντίστοιχα στο Bitcoin χρειάζονται 10 λεπτά. Δεύτερον, είναι διαφορετική η συνολική προσφορά, καθώς για το Litecoin αντιστοιχεί σε 84 εκατομμύρια νομίσματα (Bhosale & Mavale, 2018), ενώ για το Bitcoin είναι 21 εκατομμύρια.

Ripple

Το Ripple (XRP) κυκλοφόρησε το 2012 από τη Ripple Labs. Η πλατφόρμα της Ripple μπορεί να επεξεργαστεί περισσότερες από 1500 λειτουργίες ανά δευτερόλεπτο. Το Ripple χρησιμοποιεί τη δική του ιδιωτική συναίνεση για την επικύρωση συναλλαγών αντί για PoW ή PoS. Στο Ripple, η ψηφιακή υπογραφή αποδεικνύει ότι μια συναλλαγή είναι εξουσιοδοτημένη να ορίσει ένα συγκεκριμένο σύνολο ενεργειών. Μόνο υπογεγραμμένες συναλλαγές αποστέλλονται στο δίκτυο και εγκρίνονται. Κάθε ψηφιακή υπογραφή βασίζεται σε ένα κρυπτογραφημένο ζεύγος κλειδιών που σχετίζεται με τον λογαριασμό αποστολής. Ένα ζεύγος κλειδιών μπορεί να δημιουργηθεί χρησιμοποιώντας έναν από τους υποστηριζόμενους αλγόριθμους υπογραφής κρυπτογράφησης του XRP Ledger (Emeç et al, 2020). Τα αντικείμενα του καθολικού έχουν ένα μοναδικό αναγνωριστικό και η ταυτότητα τους προκύπτει από την ανάμειξη του περιεχομένου του αντικειμένου με ένα αναγνωριστικό χώρου ονομάτων. Ο τύπος αντικειμένου καθολικού καθορίζει το αναγνωριστικό χώρου ονομάτων που θα χρησιμοποιηθεί και το περιεχόμενο που θα συμπεριληφθεί στο μικτό περιεχόμενο. Με αυτόν τον τρόπο, κάθε ταυτότητα γίνεται μοναδική.

Dash

Το Dash (DASH), κυκλοφόρησε για πρώτη φορά τον Ιανουάριο του 2014 και χρησιμοποιεί τον αλγόριθμο συναίνεσης X11 PoW. Εκτός από το PoW, το Dash χρησιμοποιεί επίσης υποδομή Masternode, το οποίο είναι ένας διακομιστής συνδεδεμένος στο δίκτυο Dash, ο οποίος εγγυάται ελάχιστες επιδόσεις για την εκτέλεση εργασιών που γίνονται για τον έλεγχο την εγκυρότητα μιας συναλλαγής που αποστέλλεται στο δίκτυο. Αυτό σημαίνει ότι το Dash μπορεί να επεξεργαστεί συναλλαγές άμεσα, όπως συναλλαγές μία πιστωτική κάρτα. Ο αλγόριθμος X11 έχει σχεδιαστεί και αναπτυχθεί για να κάνει τη δημιουργία ολοκληρωμένων κυκλωμάτων για συγκεκριμένες εφαρμογές (ASIC) πιο δύσκολη. Είναι εμπνευσμένος από την προσέγγιση του

Quark, με περισσότερη πολυπλοκότητα και αυξάνοντας τον αριθμό των κατατεμαχισμών. Ωστόσο, σε αντίθεση με το Quark, δεν επιλέγονται τυχαία ορισμένοι κατατεμαχισμοί, καθιστώντας το έτσι, ένα από τα ασφαλέστερα και πιο σύνθετα μείγματα κρυπτογράφησης που χρησιμοποιούνται σήμερα (Emeç et al, 2020).

Monero

Το Monero (XMR) κυκλοφόρησε τον Απρίλιο του 2014 και έχει αναπτυχθεί κρυπτογραφικά για να διατηρεί τις λειτουργίες με απόλυτη ασφάλεια. Οι διευθύνσεις αποστολής και λήψης των δεδομένων και το ποσό των συναλλαγών που εκτελούνται, κωδικοποιούνται για λόγους ασφαλείας. Ο μηχανισμός συναίνεσης του Monero βασίζεται στον αλγόριθμο CryptoNote PoW. Το Monero, σε αντίθεση με τον ασφαλή αλγόριθμο κατατεμαχισμού SHA-256, που χρησιμοποιείται από το Bitcoin, αποτρέπει την ανάπτυξη ASIC χρησιμοποιώντας έναν αλγόριθμο σκληρής μνήμης (CryptoNight) που κάνει την ανάπτυξη ASIC πιο δύσκολη από. Χρησιμοποιεί μικτές, που είναι εργαλεία κρυπτογράφησης που μπορούν να δημιουργήσουν έναν μοναδικό αριθμό για κάθε καταχώρηση, για να ενισχύσουν την ασφάλεια του. Το Monero έχει δισεκατομμύρια διαθέσιμες συσκευές με δυνατότητα εξόρυξης, καθώς είναι δυνατή η εξόρυξη του από οποιοδήποτε τηλέφωνο ή υπολογιστή με πρόγραμμα περιήγησης ιστού (Emeç et al, 2020).

NEO

Το NEO (NEO) κυκλοφόρησε αρχικά το Φεβρουάριο του 2014 με άλλη ονομασία και τον Ιούνιο του 2017, κυκλοφόρησε ως NEO. Το NEO, μερικές φορές αναφέρεται ως το "Κινεζικό Ethereum" (Moskov, 2018). Το NEO είναι ένα έργο που δημιουργήθηκε με σκοπό μια "έξυπνη" οικονομία που τεχνικά δεν είναι κρυπτονόμισμα. Όπως το Ethereum και το Cardano, είναι μία πλατφόρμα στην οποία πραγματοποιούνται "έξυπνα" συμβόλαια και αποκεντρωμένες συναλλαγές και μπορεί να υποστηρίξει έως και 10.000 συναλλαγές ανά δευτερόλεπτο. Ως μηχανισμός συναίνεσης, χρησιμοποιεί το Delegated Byzantine Fault Tolerance (Vukolić, 2015). Οι δημιουργοί του NEO επέλεξαν το dBFT, επειδή έχει καλή επεκτασιμότητα και η επεκτασιμότητα (Emeç et al, 2020).

Cardano

Το Cardano (ADA) κυκλοφόρησε τον Σεπτέμβριο του 2015 και αναπτύχθηκε ως μία πλατφόρμα για "έξυπνα" συμβόλαια και αποκεντρωμένες εφαρμογές, όπως δηλαδή το Ethereum και το NEO. Με βάση την προϋπάρχουσα εμπειρία από το Bitcoin και το Ethereum, το Cardano στόχευσε στην ασφάλεια, την επεκτασιμότητα και τη διαλειτουργικότητα. Με το Cardano μπορεί να πραγματοποιηθεί αποστολή και η λήψη συναλλαγών ψηφιακών κεφαλαίων και είναι

το πρώτο Blockchain που σχεδιάστηκε από ομάδα, με επικεφαλείς ακαδημαϊκούς και μηχανικούς. Ο μηχανισμός συναίνεσης του Cardano βασίζεται σε μία μορφή του αλγορίθμου PoS, και πιο συγκεκριμένα στον Ouroboros. Στο πρωτόκολλο Ouroboros, κάθε ενότητα περιέχει ένα σύνολο εγκρίσεων. Οι διαδικασίες που πρέπει να περιλαμβάνονται σε αυτά τα τμήματα πρέπει να εγκρίνονται από τον κατάλληλο αριθμό κόμβων. Για τη δημιουργία ισορροπίας, οι επικυρωτές ανταμείβονται ανά ορισμένες περιόδους (Emeç et al, 2020).

4.8.2. **Tokens**

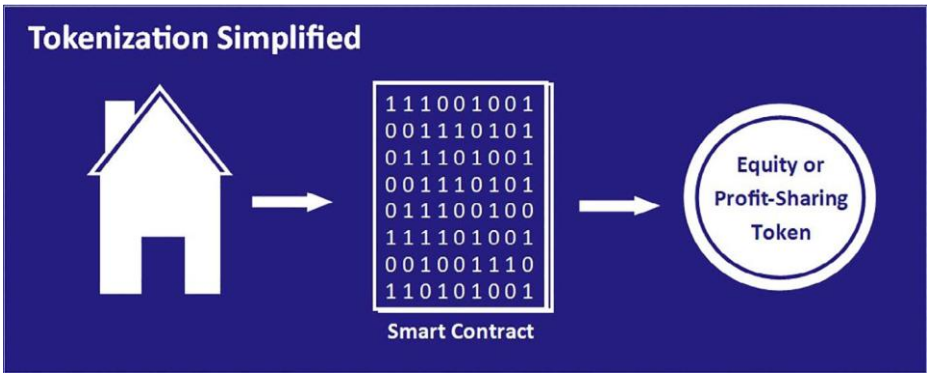
Με τη ραγδαία εξέλιξη της τεχνολογίας Blockchain τα τελευταία χρόνια και την αυξημένη κεφαλαιοποίηση των κρυπτονομισμάτων, η έννοια του tokenization έχει κεντρίσει το ενδιαφέρον πολλών ερευνητών. Ένα token είναι η ψηφιακή αναπαράσταση ενός περιουσιακού στοιχείου (asset) στο Blockchain. Αυτό το περιουσιακό στοιχείο που αντιπροσωπεύει το token, μπορεί να είναι τόσο ψηφιακό ή φυσικό όσο και υλικό ή άυλο. Με τη διαδικασία του tokenization, κάθε είδους asset μπορεί να διαχειριστεί πλέον ως ψηφιακό περιουσιακό στοιχείο, του οποίου η λογιστική μονάδα είναι ένα αποκλειστικό token του Blockchain. Τέτοια tokens μπορούν να δημιουργηθούν από οποιοδήποτε οντότητα (μεμονωμένο άτομο ή οργανισμό), η οποία θα καθορίσει και το σύνολο των κανόνων που θα διέπει τη λειτουργία του οικονομικού τους συστήματος (Freni et al., 2022).

Τεχνικά, ένα token είναι ένας αλγόριθμος που υλοποιείται ως ένα "έξυπνο" συμβόλαιο μέσα σε ένα Blockchain. Το "έξυπνο" συμβόλαιο εμπεριέχει μία λίστα με όλες τις διευθύνσεις των κατόχων και το υπόλοιπο των token που διαθέτουν, η οποία ανανεώνεται σε πραγματικό χρόνο όσο γίνονται συναλλαγές με αυτό. Ο τρόπος προγραμματισμού του "έξυπνου" συμβολαίου καθορίζει όλα τα χαρακτηριστικά του token, όπως την αξία του, το πώς δημιουργούνται, το πόσα βρίσκονται σε κυκλοφορία στην αγορά, ποιες ονομαστικές αξίες επιτρέπουν, πώς δαπανώνται και με ποια διεύθυνση στο Blockchain μπορούν να χρησιμοποιηθούν. Μπορούν να εφαρμοστούν και πιο πολύπλοκες λειτουργίες από τους κατόχους του ίδιου token, όπως π.χ. μία διαδικασία ψηφοφορίας. Ο χρήστης αποκτά πρόσβαση στα tokens του μέσω της διεύθυνσης που έχει στο Blockchain. Τα wallets, όπως και στην περίπτωση των κρυπτονομισμάτων, απλοποιούν τη χρήση καθώς κατέχουν τα ιδιωτικά κλειδιά της διεύθυνσης χρήστη και τη διεύθυνση του συμβολαίου των tokens.

Η σύνδεση ενός token με ένα ψηφιακό περιουσιακό στοιχείο μπορεί να χαρτογραφηθεί μέσω του κώδικα ενός "έξυπνου" συμβολαίου και έτσι η συσχέτιση τους είναι ξεκάθαρη και βασίζεται αποκλειστικά στο Blockchain. Ο αλγόριθμος του "έξυπνου" συμβολαίου καθορίζει τη σπανιότητα και τη μοναδικότητα των ψηφιακών περιουσιακών στοιχείων που αντιπροσωπεύουν τα tokens, καθώς δεν επιτρέπει αντίγραφα και περιορίζει τον μέγιστο αριθμό διαθέσιμων tokens, διαμορφώνοντας την αξία τους (Weingärtner, 2019).

Αντίθετα, στην περίπτωση των φυσικών περιουσιακών στοιχείων, η κατάσταση γίνεται πολύ πιο περίπλοκη. Η σύνδεση μεταξύ ενός token και ενός φυσικού περιουσιακού στοιχείου δεν μπορεί να λειτουργήσει αποκλειστικά σε ένα αποκεντρωμένο περιβάλλον με άγνωστους κόμβους. Για τη σύνδεση περιουσιακών στοιχείων του πραγματικού κόσμου με tokens, π.χ. για το tokenization ενός ακινήτου, η απόδειξη της μοναδικότητας και της αμεταβλητότητας βασίζεται πάντα σε δεδομένα εκτός του Blockchain, άρα και απαιτούνται oracles για τη λήψη πληροφοριών από τον πραγματικό κόσμο. Στην περίπτωση που γίνεται tokenization ενός asset του πραγματικού κόσμου, τα tokens αντιπροσωπεύουν το φυσικό αντικείμενο στον ψηφιακό κόσμο. Αυτό επιτρέπει στα "έξυπνα" συμβόλαια να έχουν πρόσβαση σε συγκεκριμένα αντικείμενα και έτσι ο ψηφιακός κόσμος μπορεί να "διαχειριστεί" το φυσικό κόσμο. Για παράδειγμα μπορεί να αυξήσει τη διαφάνεια στη διαχείριση των φυσικών αγαθών (Garner, 2018).

Ο όρος tokenization προέρχεται από τη γλωσσολογία, όπου το tokenization είναι μία διαδικασία επεξεργασίας κειμένου, με την οποίο κείμενο διασπάται μικρότερες μονάδες κειμένου, τα "tokens" (Matulionyte, 2019). Αυτό περιγράφει και τη σημαντικότερη ιδιότητα των tokens μέσα στο Blockchain, που είναι ότι επιτρέπουν τη διαίρεση μεγάλων τιμών σε μικρότερες μονάδες, δημιουργώντας υποδιαιρέσεις της αξίας τους. Με αυτόν τον τρόπο, μεγάλα και δύσκολο να ρευστοποιηθούν περιουσιακά στοιχεία, όπως π.χ. ακίνητα ή έργα τέχνης, αναλύονται σε κομμάτια μικρότερης αξίας, που είναι πιο εύκολο να πωληθούν. Αυτό απλοποιεί την επένδυση σε τέτοια περιουσιακά στοιχεία, αλλά και τις αντίστοιχες συναλλαγές για αυτά. Ένα απλοποιημένο παράδειγμα μίας τέτοιας διαίρεσης παρουσιάζεται στο ***Σχήμα 4-24***.



Σχήμα 4-24: Μετατροπή physical asset σε token (Sazandrishvili, 2020)

Η πιο διαδεδομένη πλατφόρμα Blockchain για την ανάπτυξη tokens και εφαρμογών tokenization είναι η πλατφόρμα του Ethereum, λόγω των δυνατοτήτων της γλώσσας προγραμματισμού Solidity, της μεγάλης κοινότητας χρηστών που διαθέτει, των υπαρχόντων παραδειγμάτων κώδικα προγραμματισμού, της εύκολης σύνδεσης με το κρυπτονόμισμα Ether

και των εύκολων λειτουργικών υλοποιήσεων (Weingärtner, 2019). Και άλλες πλατφόρμες ανάπτυξης Blockchain δίνουν τη δυνατότητα tokenization, όπως π.χ. το Hyperledger Fabric (Androulaki et al., 2018), ωστόσο καμία άλλη πλατφόρμα εκτός του Ethereum δεν χρησιμοποιείται ακόμη ευρέως για εφαρμογές tokenization.

Στο περιβάλλον του Ethereum έχουν δημιουργηθεί από την κοινότητα του, ορισμένα πρότυπα για τη δημιουργία tokens με το πιο γνωστό να είναι το ERC-20, το οποίο χρησιμοποιείται ως για την υλοποίηση "έξυπνων" συμβολαίων, παρέχοντας έναν κατάλογο κανόνων για τη λειτουργία της διαδικασίας του tokenization (Chen et al., 2020). Το ERC-20 αποτελείται από έξι βασικές λειτουργίες (Frumkin, 2018):

1. Καθορίζει το συνολικό αριθμό tokens που θα δημιουργηθούν.
2. Καθορίζει την αρχική διανομή tokens στα πορτοφόλια των χρηστών.
3. Επιτρέπει στους κατόχους των tokens να συναλλάσσονται με αυτά μετά την αρχική διανομή.
4. Παρακολουθεί το υπόλοιπο των tokens στο πορτοφόλι κάθε χρήστη.
5. Εγγυάται ότι η συνολική προσφορά tokens εντός του συστήματος διατηρείται σταθερή και ίση με αυτά που δημιουργήθηκαν.
6. Διασφαλίζει την εγκυρότητα των συναλλαγών πριν αυτές προστεθούν στο Blockchain.

Με αυτές τις έξι λειτουργίες, η ανάπτυξη νέων tokens από οποιονδήποτε είναι εξαιρετικά απλή. Το πρότυπο ERC-20 έχει χρησιμοποιηθεί στις περισσότερες και στα σημαντικότερες εφαρμογές tokenization, ενώ είναι ιδιαίτερα δημοφιλές σε περιπτώσεις ICO, λόγω της αποτελεσματικότητας της δεύτερης λειτουργίας του που εκτελεί την αρχική διανομή.

Μέσω των tokens, ο ψηφιακός κόσμος του Blockchain διαχειρίζεται assets μεγάλης συνολικής αξίας, η οποία συνεχώς αυξάνεται. Λόγω αυτού του γεγονότος, η ρύθμιση της αγοράς αποκτά μεγαλύτερη σημασία, αφενός για την πρόληψη της απάτης και της φοροδιαφυγής, αφετέρου για την προστασία των επενδυτών. Από κανονιστική άποψη λοιπόν, τα tokens χωρίζονται στις ακόλουθες κατηγορίες (Weingärtner, 2019):

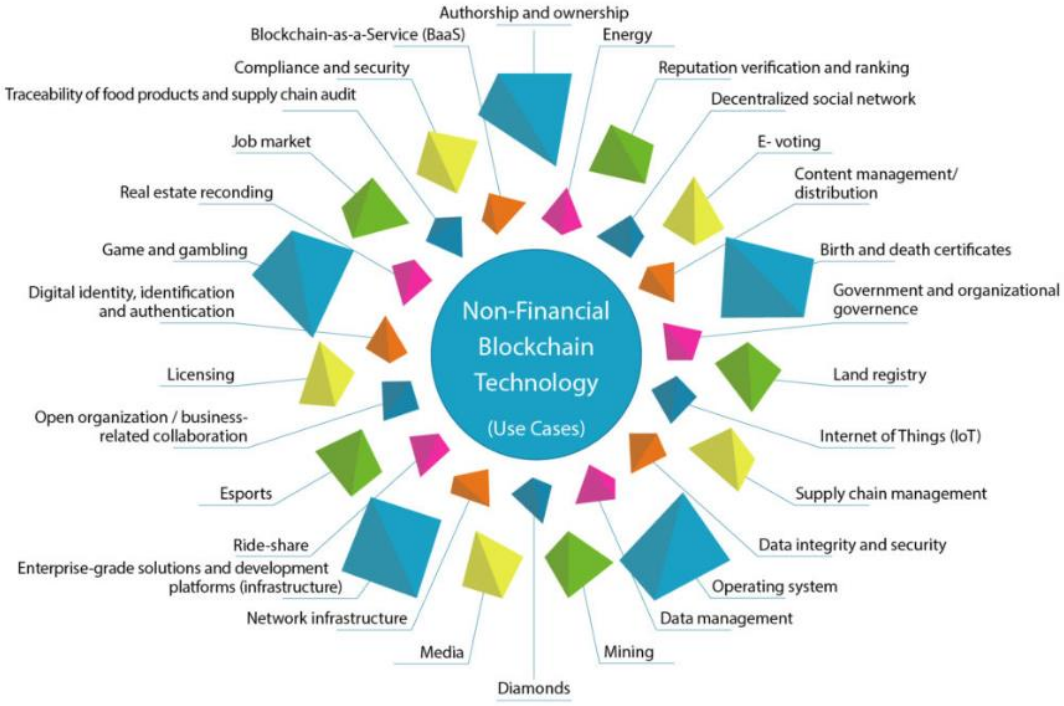
- Payment Tokens: Έχουν νομισματικό χαρακτήρα.
- Utility Tokens: Αντιπροσωπεύουν ένα δικαίωμα ή μια υπηρεσία.
- Asset or Security Tokens: Αντιπροσωπεύουν μερίδιο ενός περιουσιακού στοιχείου.

4.9. Εφαρμογές Blockchain εκτός Κρυπτονομισμάτων

Η τεχνολογία Blockchain είναι μια έννοια που εξελίσσεται συνεχώς. Είναι άρρηκτα συνδεδεμένη με τα κρυπτονομίσματα και την ψηφιακή οικονομία, όμως τα τελευταία χρόνια έχει βρει εφαρμογές σε πάρα πολλούς άλλους τομείς, στους οποίους φαίνεται ότι μπορεί να

προσδώσει αξία και για αυτό το λόγο, έχει προσελκύσει το ενδιαφέρον των ερευνητών (Javaid et al., 2021). Ήδη από το Blockchain 3.0 οι ερευνητές είχαν ξεκινήσει να ψάχνουν για εφαρμογές της τεχνολογίας σε τομείς εκτός της ανταλλαγής οικονομικών αγαθών, και πλέον στην εποχή του Blockchain 4.0, οι προσπάθειες έχουν επικεντρωθεί στη χρήση της τεχνολογίας σε βιομηχανικές εφαρμογές και πολλές φορές σε συνδυασμό με την Τεχνολογία των Πραγμάτων (internet of Things - IoT) (Bodkhe et al., 2020).

Στο ***Σχήμα 4-25*** αποτυπώνονται πλήθος τομέων εκτός της οικονομικών, στους οποίους η τεχνολογία Blockchain μπορεί να βρει πρακτική εφαρμογή και να λύσει προβλήματα.

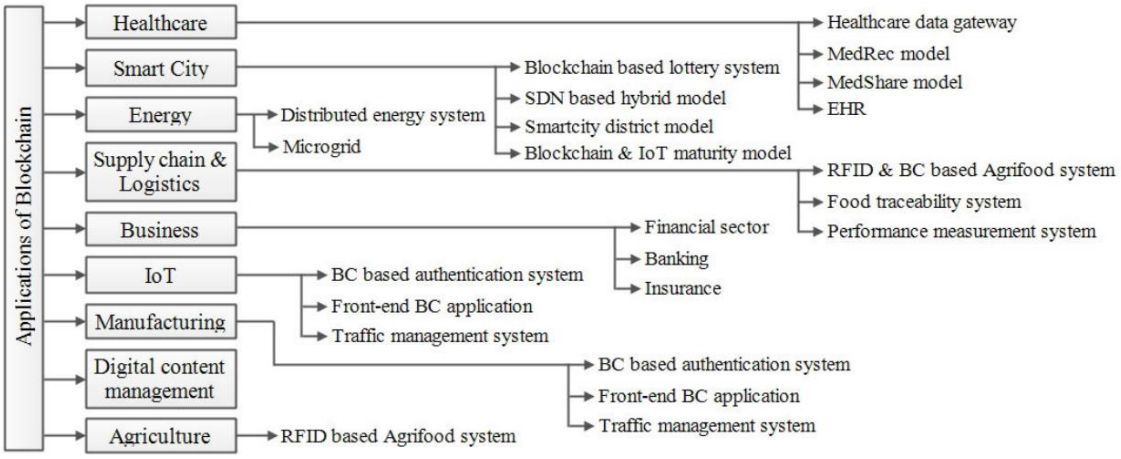


Σχήμα 4-25: Τομείς εφαρμογών Blockchain εκτός οικονομικών (Hellenic Blockchain Hub, n.d.)

Το Blockchain είναι κατάλληλο για εφαρμογές στην αποθήκευση, ασφάλεια και διατήρηση δεδομένων (Berdik et al., 2021; Cai et al., 2021) σε όλους τους τομείς τους οικονομίας και της επιχειρηματικότητας. Μπορεί να τα προβλήματα παραποίησης και απώλειας δεδομένων, καθώς και την αναποτελεσματικότητα της επεξεργασίας συναλλαγών (Pu et al., 2017; Belchior et al., 2021) και να βοηθήσει στην ανάγκη χρηματοδότησης οργανισμών (Chen et al., 2021). Έχει τη δυνατότητα να προσφέρει λύσεις στην ιατρική (Haleem et al., 2021) και τη βιοϊατρική (Solanki, 2021), στην παρακολούθηση των αγορών και στην εφοδιαστική αλυσίδα (Xu et al., 2019), καθώς και στην παρακολούθηση της ασφάλειας των τροφίμων (Alkhateeb et al., 2022). Με βάση τα χαρακτηριστικά της, η τεχνολογία μπορεί λύσει προβλήματα και στο χώρο της πνευματικής ιδιοκτησίας, όπως η παράνομη αντιγραφή, η πλαστογραφία και η παραποίηση

στο περιβάλλον εμπορίας ψηφιακού περιεχομένου, τα οποία έχουν επιδεινωθεί πολύ στην εποχή της πληροφορίας (Heo et al, 2021; Jing et al., 2021). Η παραπάνω λίστα μπορεί να επεκταθεί σε τομείς όπως η ενέργεια (Andoni et al., 2019), η εκπαίδευση (Raimundo & Rosário, 2021), οι κυβερνητικές υπηρεσίες (Ølnes et al., 2017), οι τράπεζες (Garg et al., 2021) και πολλές ακόμα κατηγορίες.

Το Blockchain 4.0 έχει ανοίξει το δρόμο για τη μαζική είσοδο της τεχνολογίας Blockchain σε όλα τα "έξυπνα" συστήματα που αναπτύσσονται τα τελευταία χρόνια. Το Industry 4.0 παρέχει τεχνολογίες σε επιχειρήσεις, βιομηχανίες και οργανισμούς, όπως το Διαδίκτυο των Πραγμάτων (IoT), η Τεχνητή νοημοσύνη (AI), η Επαυξημένη Πραγματικότητα και πολλές ακόμα. Το Blockchain έχει μπει και αυτό στο στόχαστρο των ερευνητών της 4ης Βιομηχανικής Επανάστασης (Bodkhe et al., 2020), καθώς μπορεί να λειτουργήσει πολλαπλασιαστικά ως προς το όφελος, από την εφαρμογή αυτών των σύγχρονων τεχνολογιών, αν δηλαδή αναπτυχθεί σε συνεργασία με αυτές, σε όλους τους τομείς, όπως φαίνεται στο ***Σχήμα 4-26***.



Σχήμα 4-26: Εφαρμογές Blockchain στο φάσμα του Industry 4.0 (Bodkhe et al., 2020)

Στη συνέχεια αναφέρονται ενδεικτικά, σενάρια χρήσης του Blockchain σε κάποιους τομείς, για να καταδειχθεί το εύρος των δυνατοτήτων της τεχνολογίας Blockchain.

4.9.1. Εφαρμογές στον τομέα της γεωργίας και των τροφίμων

Ο τομέας της γεωργίας και των τροφίμων είναι πιο ίσως αυτός με τον οποίο έχουν ασχοληθεί περισσότερο οι ερευνητές, που αναζητούν τρόπους εφαρμογής της τεχνολογίας Blockchain, πέραν των κρυπτονομισμάτων. Το Blockchain ενδέχεται να εφαρμοστεί σε σημαντικές υποκατηγορίες του τομέα της γεωργίας και των τροφίμων, όπως στην αγροτική ασφάλιση, στην "έξυπνη" γεωργία, στην εφοδιαστική αλυσίδα, στη συναλλαγή γεωργικών προϊόντων κ.ά. (Xiong et al., 2020).

Σχετικά με την αγροτική ασφάλιση, οι δυσμενείς καιρικές συνθήκες αποτελούν απειλή για τη σοδειά ποικίλων γεωργικών προϊόντων, αφήνοντας εκτεθειμένους τους γεωργούς και για αυτό το λόγο, η αγροτική ασφάλιση αποτελεί ένα ευρέως αναγνωρισμένο εργαλείο διαχείρισης των κινδύνων που σχετίζονται με τις καιρικές συνθήκες. Πολλές φορές οι αγρότες πληρώνουν ασφάλιστρα, πριν ξεκινήσει ο κύκλος καλλιέργειας και λαμβάνουν ένα ποσό πληρωμής κάθε φορά που αντιμετωπίζουν κάποιου είδους απώλειας στο αγρόκτημά τους (Miranda et al., 1997). Ο συνδυασμός αυτής της δυνατότητας ασφάλισης με την τεχνολογία του Blockchain, βελτιώνει τη διαδικασία ασφάλισης σε δύο διαστάσεις (Gatteschi et al., 2018). Πρώτον, οι πληρωμές μπορούν να γίνουν έγκαιρα και αυτοματοποιημένα, με βάση τα καιρικά δεδομένα που ενεργοποιούν την πληρωμή, όπως ορίζεται από ένα "έξυπνο" συμβόλαιο. Δεύτερον, πληροφορίες για τον καιρό και άλλες πηγές δεδομένων, όπως δεδομένα που συλλέγονται από γεωργικά μηχανήματα, μπορούν να ενσωματωθούν αυτόματα μέσω μιας βάσης πρόγνωσης του κινδύνου, καθιστώντας έτσι την πληρωμή πιο αποτελεσματική.

Η "έξυπνη" γεωργία χαρακτηρίζεται από την αξιοποίηση των τεχνολογιών Industry 4.0, όπως το διαδίκτυο των πραγμάτων (IoT), διάφορες σύγχρονες τεχνολογίες συλλογής και ανάλυσης δεδομένων, συμπεριλαμβανομένων των μη επανδρωμένων εναέριων οχημάτων (UAV), των αισθητήρων και της μηχανικής μάθησης. Ένα βασικό χαρακτηριστικό της "έξυπνης" γεωργίας είναι η ανάπτυξη ενός ολοκληρωμένου συστήματος ασφάλειας που διευκολύνει τη χρήση και διαχείριση δεδομένων, η οποία με τη βοήθεια παραδοσιακών τρόπων εγκυμονεί πλήθος κινδύνων (Xiong et al., 2020). Ειδικότερα, ενδέχεται να οδηγήσει σε ανακριβή δεδομένα, στη διαστρέβλωση δεδομένων, στην εσφαλμένη χρήση δεδομένων, καθώς και στις διαδικτυακές επιθέσεις. Για την αντιμετώπιση αυτών των προβλημάτων, η αξιοποίηση της τεχνολογίας Blockchain δίνει τη δυνατότητα αποθήκευσης δεδομένων και πληροφοριών που παράγονται από διαφορετικές οντότητες και καταγράφονται από την αρχή της παραγωγικής διαδικασίας του αγροτικού προϊόντος, για την επιβεβαίωση της διαύγειας και της αμετάβλητης κατάστασης των προϊόντων σε όλα τα ενδιαφερόμενα μέρη. Μία άλλη μορφή "έξυπνης" γεωργίας αποτελεί η πρόταση των Patil et al. (2018) για μία αρχιτεκτονική ανάπτυξης θερμοκηπίων βασισμένη σε ιδιωτικό Blockchain για τον έλεγχο αισθητήρων IoT, ενώ αντίστοιχη πρόταση έχει υπάρξει και από τους Lin et al. (2018)

Από την πλευρά των παραγωγών, η χρήση της τεχνολογίας Blockchain βοηθά στην ενίσχυση εμπιστοσύνης μεταξύ των καταναλωτών και στο "χτίσιμο" της φήμης των προϊόντων τους, παρέχοντας πληροφορίες των προϊόντων μέσω του Blockchain, εξασφαλίζοντας έτσι την αναγκαία διαύγεια. Οι επιχειρήσεις πώλησης των προϊόντων, θα μπορούν να αντιληφθούν την αντιληφθούν με μεγαλύτερη προσέγγιση την οικονομική τους αξία, αυξάνοντας με αυτόν τον τρόπο, την ανταγωνιστικότητά τους. Αυτό θα καθιστούσε δύσκολο για τους προμηθευτές να

προβούν σε απάτη, αναγκάζοντας τους να βελτιώσουν την ποιότητα των προϊόντων του κλάδου της γεωργίας και των τροφίμων. Από την πλευρά των καταναλωτών, το Blockchain παράγει αξιόπιστες πληροφορίες σχετικά με τον τρόπο παραγωγής των τροφίμων, εξασφαλίζοντας την ασφάλεια, την ποιότητα και την οικολογική παραγωγή τους (Ge et al., 2017). Επιπροσθέτως, συμβάλλει στην αλληλεπίδραση των καταναλωτών με τους παραγωγούς, έτσι ώστε να κατανοούν ενδελεχώς τις ιδιαιτερότητες της παραγωγικής διαδικασία των τροφίμων. Από την πλευρά των ρυθμιστικών αρχών, η τεχνολογία Blockchain καθιστά διαθέσιμες τις απαραίτητες για αυτές πληροφορίες, με σκοπό να συνεχίσουν να νομοθετούν με αποτελεσματικότητα (Zhou et al., 2016; Chen, 2018). Τέλος, σε επίπεδο συναλλαγών, η τεχνολογία Blockchain προσφέρει μια αξιόπιστη προσέγγιση για συναλλαγές μεταξύ ανώνυμων μερών. Η απάτη και οι δυσλειτουργίες μπορούν έτσι να εντοπιστούν γρήγορα και επιπλέον, τα προβλήματα μπορούν να αναφερθούν σε πραγματικό χρόνο μέσω της ενσωμάτωσης "έξυπνων" συμβολαίων (Haveson et al., 2017; Sylvester, 2019).

4.9.2. Εφαρμογές στην εφοδιαστική αλυσίδα

Η τεχνολογία Blockchain είναι μία πολλά υποσχόμενη τεχνολογία στον κλάδο της εφοδιαστικής αλυσίδας, καθώς δίνει τη δυνατότητα της σύναψης "έξυπνων" συμβολαίων, εδραιώνοντας έτσι την εμπιστοσύνη μεταξύ των συμβαλλόμενων μερών, ενώ παράλληλα διασφαλίζει την αξιοπιστία, την καταπολέμηση των απομιμήσεων, τη διαφάνεια και την ιχνηλασιμότητα (Azzi et al., 2019; Saberi et al., 2019). Μια πιθανή περίπτωση χρήσης "έξυπνων" συμβολαίων στις αλυσίδες εφοδιασμού είναι η διαχείριση των προμηθειών, όπου το διαχειριστικό σύστημα μπορεί να ενημερωθεί αυτόματα σε πραγματικό χρόνο σχετικά με το ποια αγαθά έχουν αγοραστεί, πωληθεί και παραδοθεί (Saberi et al., 2019).

Άλλο ένα πρόσθετο όφελος είναι η διαφάνεια που παρέχει το Blockchain στις αλυσίδες εφοδιασμού, επιτρέποντας την ορατότητα και την ιχνηλασιμότητα σε όλους του κόμβους του δικτύου. Δηλαδή, με τη χρήση της τεχνολογίας Blockchain μπορεί να δημιουργηθεί ένα block για κάθε ένα γεγονός στην παραγωγική διαδικασία από την κατασκευή έως τη διανομή, τα οποία θα ήταν ορατά σε όλους, επιτρέποντας έτσι στα μέλη του κατανεμημένου δικτύου να ελέγχουν την πρόοδο των διαδικασιών (Wang et al., 2019). Η διαφάνεια αυτή δεν αφορά μόνο τον παραγωγό αλλά μπορεί να προσφέρει οφέλη και στον καταναλωτή, ενισχύοντας σημαντικά την εμπιστοσύνη του στο προϊόν και στον κατασκευαστή του (Saberi et al., 2019), με τη δημιουργία ενός συνολικού αποτυπώματος του κύκλου ζωής του προϊόντος, το οποίο μπορεί να ελεγχθεί (Wang et al., 2019). Η τεχνολογία του Blockchain παρέχει επίσης της δυνατότητα για επίτευξη επιτυχούς "απομεσαζοντοποίησης" των μεγάλων παραδοσιακών εφοδιαστικών αλυσίδων που λειτουργούν κατ' ανάγκη με τη χρήση μεγάλου πλήθους διαμεσολαβητών και εγγράφων (Dutta et al., 2020; Wang et al., 2019).

Γενικότερα, υπάρχουν διάφορες πιθανές εφαρμογές του Blockchain στην εφοδιαστική αλυσίδα, ανάλογα τον τομέα που αυτή εξυπηρετεί. Πέρα από εφαρμογές στην εφοδιαστική αλυσίδα του τομέα της γεωργίας (Kamble et al., 2019), υπάρχουν προσπάθειες για την εφαρμογή της τεχνολογίας Blockchain σε όλο το φάσμα της εφοδιαστικής αλυσίδας, όπως στο κομμάτι των μεταφορών (Batta et al., 2021), στη βιωσιμότητα (Caldarelli et al., 2021), στο κομμάτι των κατασκευών (Wang et al., 2017). Όσο αφορά την ιχνηλασιμότητα είναι άξιο αναφοράς το παράδειγμα της Walmart για την παρακολούθηση προϊόντων κατά μήκος της αλυσίδας εφοδιασμού τροφίμων, όπου σύμφωνα με τους Chang et al. (2019), χρησιμοποίησε ένα σύστημα Blockchain της IBM, με το οποίο σε μία πιλοτική εφαρμογή, μείωσε τον χρόνο αναμονής για φρούτα (μάνγκο) στα σύνορα ΗΠΑ-Μεξικού από επτά ημέρες σε 2,2 δευτερόλεπτα.

4.9.3. Εφαρμογές στον τραπεζικό τομέα

Η τεχνολογία Blockchain ενδέχεται να εφαρμοστεί στον τραπεζικό κλάδο, καθώς εμφανίζει πολυάριθμες προοπτικές. Πιο συγκεκριμένα, το Blockchain έχει λάβει ιδιαίτερη προσοχή στη χρηματοοικονομική τεχνολογία (FinTech), καθώς συνδυάζει πολλές τεχνολογίες υπολογιστών, συμπεριλαμβανομένης της κατανεμημένης αποθήκευσης δεδομένων, της peer-to-peer μετάδοσης δεδομένων, των μηχανισμών συναίνεσης, καθώς και των αλγορίθμων κρυπτογράφησης (Qi-Guo, 2016). Αυτά τα χαρακτηριστικά του, καθιστούν το μέλλον του Blockchain ιδιαίτερα αισιόδοξο, όσον αφορά την εφαρμογή του στον τραπεζικό κλάδο και ήδη παλαιότερη έρευνα υποδεικνύει ότι η τεχνολογία του Blockchain θα εφαρμοστεί εκτενώς από το 15% των τραπεζών (Guo & Liang, 2016). Αυτό οφείλεται στο γεγονός ότι η τεχνολογία Blockchain δύναται να προσφέρει πολλαπλά οφέλη στον τραπεζικό τομέα. Μπορεί για παράδειγμα, σύμφωνα με τη McKinsey (Higgison et al., 2019) να λύσει το προβλήματα απάτης ταυτότητας διαδικασιών KYC (Know Your Customer), τα οποία στοιχίζουν στις τράπεζες 15 με 20 δισεκατομμύρια δολάρια ετησίως. Επίσης σύμφωνα με τους Guo & Liang (2016), μπορεί να δημιουργήσει έναν πιστωτικό μηχανισμό σε μια κατάσταση που επικρατεί έλλειψη αμοιβαίας εμπιστοσύνης μεταξύ των συνεργαζόμενων μερών, επιλύοντας έτσι το υψηλό κόστος που προκαλείται από τις μη τεχνικές πτυχές του συγκεντρωτισμό του τραπεζικού συστήματος. Ακόμα, οι διαδικασίες των χρηματοπιστωτικών υπηρεσιών ελλοχεύουν πολλούς κινδύνους, όπως μείωση της αποτελεσματικότητας, καθυστέρηση των συναλλαγών, αυξημένη πιθανότητα απάτης και κίνδυνοι λειτουργίας. Αυτά είναι κάποια από τα παραδείγματα προβλημάτων που μπορούν να επιλυθούν με την εφαρμογή της τεχνολογίας Blockchain, η οποία παρέχει εξατομικευμένη εξυπηρέτηση και υψηλή ασφάλεια.

4.9.4. Εφαρμογές στον τομέα της υγείας

Μολονότι έχουν πραγματοποιηθεί ήδη έρευνες σχετικά με τα οφέλη της τεχνολογίας του Blockchain σε ικανό αριθμό κλάδων, κλάδος της υγειονομικής περίθαλψης δεν έχει λάβει την ίδια προσοχή από τους ερευνητές, με αποτέλεσμα να λαμβάνει προσοχή με καθυστέρηση ετών σε σχέση με άλλους κλάδους (Au et al., 2017; Beninger & Ibara, 2016; Yüksel et al., 2017). Γενικά, η υγειονομική περίθαλψη ως κλάδος έχει υψηλές απαιτήσεις που σχετίζονται με την ασφάλεια και ιδιωτικότητα των χρηστών, εξαιτίας των πρόσθετων νομικών απαιτήσεων για την προστασία των ιατρικών πληροφοριών των ασθενών. Ειδικότερα, στην εποχή που διανύουμε, κατά την οποία η κοινή χρήση αρχείων και δεδομένων, καθώς και η αποθήκευση τους στο cloud, σε συνδυασμό με την υιοθέτηση φορητών συσκευών υγείας γίνεται ολοένα και πιο διαδεδομένη, αυξάνοντας ωστόσο το ρίσκο κακόβουλων επιθέσεων και τον κίνδυνο παραβίασης προσωπικών πληροφοριών. Καθημερινά παράγονται και αποθηκεύονται πολυάριθμα αρχεία σε διάφορα νοσοκομεία (Khan & Hoque, 2016), τα οποία είναι διάσπαρτα, με αποτέλεσμα να είναι εύκολο να χαθούν και να μην υπάρχει προσβασιμότητα στους ενδιαφερόμενους ασθενείς (Azaria et al., 2016). Επομένως, οι βασικές απαιτήσεις της υγειονομικής περίθαλψης σχετίζονται με την επιβεβαίωση της γνησιότητας, τη διαλειτουργικότητα, την κοινή χρήση δεδομένων, αλλά και τη μεταφορά των ιατρικών αρχείων (McGhin et al., 2019).

Το Blockchain έχει τη δυνατότητα να αντιμετωπίσει τα προαναφερθέντα εμπόδια. Μερικές από τις πιο ισχυρές δυνατότητες που προσφέρει η τεχνολογία Blockchain στο τομέα της υγείας και της περίθαλψης είναι: ασφάλεια, αποκεντρωμένη φύση, ακεραιότητα, διαθεσιμότητα και αρχές γνησιότητας. Μέσω της αποκεντρωμένης δομής του, εξασφαλίζεται η γνησιότητα των στοιχείων ή άλλων προσωπικών πληροφοριών που είναι αποθηκευμένα στο δίκτυο του (Sullivan & Burger, 2017). Η βιομηχανία της περίθαλψης αντιμετωπίζει γενικότερα προβλήματα σχετικά με την προσαρμογή της στις αναδυόμενες τεχνολογίες, όπως το Διαδίκτυο των Πραγμάτων (IoT) και οι "έξυπνες" συσκευές με ενσωματωμένους αισθητήρες. Μολονότι, οι παραπάνω τεχνολογίες συμβάλλουν στη βέλτιστη εξυπηρέτηση των ασθενών, οδηγούν και στην εμφάνιση παθογενειών που εμποδίζουν την αξιόπιστη μεταφορά δεδομένων μεταξύ των διαφορετικών νοσοκομείων και γιατρών. Αυτό μπορεί να έχει ως αποτέλεσμα τη λανθασμένη διάγνωση, οδηγώντας ενδεχομένως στην επιδείνωση της υπάρχουσας κατάστασης υγείας του ασθενή. Έτσι, ο στόχος είναι οι ασθενείς μέσω της τεχνολογίας Blockchain να ελέγχουν τα ιατρικά τους δεδομένα, τα οποία διακινούνται και αποθηκεύονται σε ένα πλήρως ασφαλές περιβάλλον (McGhin et al., 2019). Ως εκ τούτου, η από κοινού χρήση των δύο τεχνολογιών (IoT και Blockchain) μπορεί να γίνει μία λογική επιλογή για το σχεδιασμό ενός αποκεντρωμένου συστήματος ηλεκτρονικής φροντίδας (Ray et al., 2020).

4.9.5. Εφαρμογές στον τομέα της εκπαίδευσης

Σύμφωνα με έρευνα που διεξήχθη από τους Alammary et al. (2019) η τεχνολογία Blockchain μπορεί να προσφέρει πολυάριθμα σημαντικά οφέλη στον τομέα της εκπαίδευσης. Το πρώτο όφελος είναι η παροχή ασφάλειας στους χρήστες, η οποία περιλαμβάνει την προστασία δεδομένων, την ιδιωτικότητα και την ακεραιότητα. Ένα επιπρόσθετο πλεονέκτημα της ένταξης της τεχνολογίας Blockchain στον εκπαιδευτικό τομέα, αποτελεί ο έλεγχος σχετικά με την πρόσβαση των μαθητών στα δεδομένα, ενώ τονίζεται και ο ρόλος που διαδραματίζει η "διαφάνεια", καθώς και η ανάληψη ευθυνών. Ακόμα, το Blockchain έχει τη δυνατότητα να βελτιώσει την εμπιστοσύνη μεταξύ των συμμετεχόντων, διευκολύνοντας τη διαδικασία επικοινωνίας μεταξύ τους, αλλά και να μειωθεί το συνολικό κόστος της εκπαίδευσης.

Ειδικότερα, στον τομέα της τριτοβάθμιας εκπαίδευσης, οι παραβιάσεις της ιδιωτικότητας και της ασφάλειας αυξάνονται συνεχώς. Το Blockchain έχει προταθεί ως ένας τρόπος επίλυσης κρίσιμων προκλήσεων που αντιμετωπίζει η τριτοβάθμια εκπαίδευση, όπως η τήρηση αρχείων των διπλωμάτων (Kamišalić et al., 2019). Μπορεί να διαδραματίσει καταλυτικό ρόλο στη διασφάλιση της αυθεντικότητας τους και στην τήρηση αρχείων με απόλυτη ακρίβεια (Vidal et al., 2019). Επίσης, η αυξανόμενη ψηφιοποίηση της τριτοβάθμιας εκπαίδευσης οδήγησε στην περαιτέρω αναγνώριση των ανησυχιών που σχετίζονται με την ασφαλή αποθήκευση των δεδομένων. Για την αντιμετώπιση αυτού του προβλήματος, μέσω της τεχνολογίας Blockchain δίνεται η δυνατότητα χρήσης των δεδομένων με αποκεντρωμένο τρόπο, μείωσης της πιθανότητας απάτης, ασφαλούς αποθήκευσης των πληροφοριών και μείωσης των εξόδων συναλλαγών που σχετίζονται με τον ακαδημαϊκό έλεγχο δεδομένων (Fedorova & Skobleva, 2020).

5. Συμπεράσματα

Η παρούσα μελέτη τεχνολογικής αριστείας προσφέρει μια ολοκληρωμένη εικόνα των διαθέσιμων τεχνολογιών που μπορούν να αξιοποιηθούν στο πλαίσιο του έργου **BLOCK AGROWASTE** για την αποτελεσματική διαχείριση των αγροτικών πλαστικών αποβλήτων. Μέσα από την ανάλυση σύγχρονων τεχνολογιών, όπως το Διαδίκτυο των Πραγμάτων (IoT), η υπολογιστική νέφους (Cloud Computing) και η τεχνολογία Blockchain, αναδείχθηκαν τα εργαλεία και οι μέθοδοι που μπορούν να διαμορφώσουν μια αποδοτική λύση για την ιχνηλασιμότητα, τη συλλογή και την ενεργειακή αξιοποίηση των αγροπλαστικών. Πρώτα απ' όλα, η τεχνολογία IoT παρουσιάστηκε ως βασικό συστατικό του συστήματος διαχείρισης αποβλήτων. Με τη χρήση αισθητήρων, τα δεδομένα που αφορούν τα αγροπλαστικά απορρίμματα μπορούν να συλλέγονται σε πραγματικό χρόνο, ενισχύοντας την παρακολούθηση της κατάστασης των πλαστικών κατά την απόρριψη και τη μεταφορά τους. Αυτό επιτρέπει στους αγρότες και στους συλλέκτες να έχουν πρόσβαση σε κρίσιμες πληροφορίες σχετικά με τον όγκο των αποβλήτων, τη γεωγραφική θέση και την κατάσταση τους, διευκολύνοντας την ορθολογική διαχείριση των πόρων. Η ανάλυση των αισθητήρων στο Κεφάλαιο 3 παρέχει σαφή καθοδήγηση για την επιλογή του κατάλληλου εξοπλισμού που θα εφαρμοστεί στο πλαίσιο του έργου. Αισθητήρες θερμοκρασίας, υγρασίας, βάρους και θέσης θα μπορούσαν να χρησιμοποιηθούν για την καταγραφή της φυσικής κατάστασης των αποβλήτων και για την παρακολούθηση της μεταφοράς τους προς τις μονάδες επεξεργασίας. Τα δεδομένα αυτά θα συνεισφέρουν στην ακριβή αποτύπωση της ροής των αποβλήτων, ενώ η αποθήκευσή τους σε υποδομές υπολογιστικού νέφους θα εξασφαλίσει την επεκτασιμότητα και την ασφαλή διαχείριση μεγάλων όγκων δεδομένων. Επιπρόσθετα, η ενσωμάτωση της τεχνολογίας Blockchain εξασφαλίζει την ακεραιότητα και τη διαφάνεια σε όλες τις συναλλαγές που αφορούν τη διαχείριση των αγροπλαστικών. Μέσω της τεχνολογίας αυτής, κάθε κρίσιμο σημείο στη διαδικασία συλλογής, απόρριψης και ενεργειακής αξιοποίησης των πλαστικών θα καταγράφεται σε ένα αποκεντρωμένο μητρώο, παρέχοντας ασφάλεια, αλλά και ενισχύοντας την εμπιστοσύνη μεταξύ των εμπλεκόμενων μερών, δηλαδή των αγροτών, των συλλεκτών και των μονάδων ανακύκλωσης ή αξιοποίησης. Επιπλέον, η δυνατότητα εφαρμογής έξυπνων συμβολαίων (Smart Contracts) θα διευκολύνει την αυτοματοποίηση κρίσιμων διαδικασιών, όπως την αποπληρωμή των υπηρεσιών συλλογής ή την επιβεβαίωση της παράδοσης των αποβλήτων στις μονάδες επεξεργασίας. Τέλος, η έρευνα κατέδειξε πως η χρήση εργαλείων αναλυτικής δεδομένων και αλγορίθμων μηχανικής μάθησης θα μπορούσε να παίξει καθοριστικό ρόλο στην ανάλυση των δεδομένων που θα προκύπτουν από την πλατφόρμα IoT. Οι αλγόριθμοι αυτοί θα μπορούν να προβλέπουν τη ζήτηση για τη συλλογή των αποβλήτων, αλλά και να βελτιστοποιούν τις διαδρομές συλλογής, μειώνοντας τα λειτουργικά κόστη και την περιβαλλοντική επιβάρυνση. Παράλληλα, η χρήση τεχνολογιών υπολογιστικού νέφους

εξασφαλίζει την αποθήκευση μεγάλων όγκων δεδομένων και την παροχή υποδομών για την απομακρυσμένη πρόσβαση και επεξεργασία τους.

Εν κατακλείδι, η μελέτη τεχνολογικής αριστείας υποδεικνύει τις τεχνολογικές λύσεις που μπορούν να εφαρμοστούν στο έργο BLOCK AGROWASTE με τρόπο που να ενισχύει την αποδοτικότητα, την ακρίβεια και τη διαφάνεια της διαχείρισης των αγροπλαστικών αποβλήτων. Η βιβλιογραφική ανασκόπηση αποδεικνύει ότι ο συνδυασμός τεχνολογιών IoT, Blockchain και υπολογιστικού νέφους μπορεί να αποτελέσει τη βάση για την ανάπτυξη μιας πλατφόρμας που όχι μόνο θα βελτιστοποιεί τις διαδικασίες διαχείρισης των αποβλήτων, αλλά θα συμβάλει και στην εναρμόνιση της γεωργίας με τις αρχές της αειφορίας και της κυκλικής οικονομίας.

6. Βιβλιογραφικές Αναφορές

Abdelhamid, M., & Hassan, G. (2019, April). Blockchain and smart contracts. In Proceedings of the 8th International Conference on Software and Information Engineering (pp. 91-95).

Abegg, J. P., Bramas, Q., & Noël, T. (2021). Blockchain Using Proof-of-Interaction. In Networked Systems: 9th International Conference, NETYS 2021, Virtual Event, May 19–21, 2021, Proceedings (pp. 129-143). Springer International Publishing.

Abel, E. E., Abd Latiff, M. S., & Chan, W. H. (2023). IoT data analytic algorithms on edge-cloud infrastructure: A review. Digital Communications and Networks.

Adheretech, 2021. Retrieved from: https://adheretech.com/

Ahmad, M. W., Mourshed, M., Mundow, D., Sisinni, M., & Rezgui, Y. (2016). Building energy metering and environmental monitoring–A state-of-the-art review and directions for future research. Energy and Buildings, 120, 85-102.

Akkoyunlu, E. A., Ekanadham, K., & Huber, R. V. (1975, November). Some constraints and tradeoffs in the design of network communications. In Proceedings of the fifth ACM symposium on Operating systems principles (pp. 67-74).

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. Sensors, 22(4), 1304.

Almakhour, M., Sliman, L., Samhat, A. E., & Mellouk, A. (2020). Verification of smart contracts: A survey. Pervasive and Mobile Computing, 67, 101227.

Alsunaidi, S. J., & Alhaidari, F. A. (2019, April). A survey of consensus algorithms for blockchain technology. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

Altarawneh, A., Herschberg, T., Medury, S., Kandah, F., & Skjellum, A. (2020). Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0727-0736). IEEE.

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. Journal of Ambient Intelligence and Humanized Computing, 6(4), 495-517.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and sustainable energy reviews, 100, 143-174.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

Ansari, A. N., Sedky, M., Sharma, N., & Tyagi, A. (2015, January). An Internet of things approach for motion detection using Raspberry Pi. In Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things (pp. 131-134). IEEE.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.".

Anwar, H. (2018). Consensus Algorithms: The Root Of Blockchain Technology, 2018.

Arjomandi-Nezhad, A., Fotuhi-Firuzabad, M., Dorri, A., & Dehghanian, P. (2021). Proof of humanity: A tax-aware society-centric consensus algorithm for Blockchains. Peer-to-Peer Networking and Applications, 14(6), 3634-3646.

Arslanian, H., & Fischer, F. (2019). The basics of cryptography and encryption. The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services, 89-93.

Ashton, K. (2009). That 'internet of things' thing. *RFID journal*, *22*(7), 97-114.

Au, M. H., Yuen, T. H., Liu, J. K., Susilo, W., Huang, X., Xiang, Y., & Jiang, Z. L. (2017). A general framework for secure sharing of personal health records in cloud system. Journal of computer and system sciences, 90, 46-62.

AWS, n.d. What is Cloud Storage? Retrieved from: https://aws.amazon.com/what-is/cloud-storage/

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD) (pp. 25-30). IEEE.

Azo Sensors, 2012. Retrieved from: https://www.azosensors.com/article.aspx?ArticleID=57

Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. Computers & industrial engineering, 135, 582-592.

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). Ieee.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Badev, A. I., & Chen, M. (2014). Bitcoin: Technical background and data analysis.

Baker, B. (2022). What is Bitcoin mining and how does it work?. Retrieved from: https://www.bankrate.com/investing/what-is-bitcoin-mining (Accessed December 30, 2022)

Bakhoff, M. (2010). Consensus algorithms for distributed systems. In 2010 Free. Annu. Conf (pp. 222-225).

Baldominos, A., & Saez, Y. (2019). Coin. AI: A proof-of-useful-work scheme for blockchain-based distributed deep learning. Entropy, 21(8), 723.

Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications, 154, 113385.

Bartoletti, M., & Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. In Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21 (pp. 494-509). Springer International Publishing.

Batta, A., Gandhi, M., Kar, A. K., Loganayagam, N., & Ilavarasan, V. (2021). Diffusion of blockchain in logistics and transportation industry: an analysis through the synthesis of academic and trade literature. Journal of Science and Technology Policy Management, 12(3), 378-398.

Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In Sequences II: Methods in Communication, Security, and Computer Science (pp. 329-334). Springer New York.

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys (CSUR), 54(8), 1-41.

Bellagente, P., Ferrari, P., Flammini, A., & Rinaldi, S. (2015, September). Adopting IoT framework for Energy Management of Smart Building: A real test-case. In 2015 IEEE 1st International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI) (pp. 138-143). IEEE.

Bencardino, M., & Greco, I. (2014). Smart communities. Social innovation at the service of the smart cities. Tema. Journal of Land Use, Mobility and Environment.

Benet, J., Dalrymple, D., & Greco, N. (2017). Proof of replication. Protocol Labs, July, 27, 20.

Benevolo, C., Dameri, R. P., & D'Auria, B. (2016). Smart mobility in smart city. In Empowering Organizations (pp. 13-28). Springer, Cham.

Beniiche, A. (2020). A study of blockchain oracles. arXiv preprint arXiv:2004.07140.

Beninger, P., & Ibara, M. A. (2016). Pharmacovigilance and biomedical informatics: a model for future development. Clinical therapeutics, 38(12), 2514-2525.

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review, 42(3), 34-37.

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1), 102397.

Bhosale, J., & Mavale, S. (2018). Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin. Annu. Res. J. SCMS, Pune, 6.

Bigini, G., Freschi, V., & Lattanzi, E. (2020). A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. Future Internet, 12(12), 208.

Binance Academy, 2023. Τι είναι το blockchain και πώς λειτουργεί; Retrieved from: https://academy.binance.com/el/articles/what-is-blockchain-and-how-does-it-work

Bitansky, N. (2020). Verifiable random functions from non-interactive witness-indistinguishable proofs. Journal of Cryptology, 33(2), 459-493.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. IEEE Access, 8, 79764-79800.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2), 213-238.

Bravo-Marquez, F., Reeves, S., & Ugarte, M. (2019, April). Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions. In 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON) (pp. 119-124). IEEE.

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., ... & Zhang, F. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. Chainlink Labs, 1.

Brito, J., & Castillo, A. (2013). Bitcoin: A primer for policymakers. Mercatus Center at George Mason University.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437.

Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, No. 4, pp. 1-4).

Cachin, C., Schubert, S., & Vukolić, M. (2016). Non-determinism in byzantine fault-tolerant replication. arXiv preprint arXiv:1603.07351.

Caeiro, J. J., & Martins, J. C. (2019). Water Management for Rural Environments and IoT. In Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities (pp. 83-99). IGI Global.

Cai, X. Q., Deng, Y., Zhang, L., Shi, J. C., Chen, Q., Zhen, W. L., ... & Guo, M. Y. (2021). The principle and core technology of blockchain. Chinese journal of computers, 44(1), 84-131.

Caldarelli, G., Zardini, A., & Rossignoli, C. (2021). Blockchain adoption in the fashion sustainable supply chain: Pragmatically addressing barriers. Journal of Organizational Change Management.

Capocasale, V., & Perboli, G. (2022). Standardizing smart contracts. IEEE Access, 10, 91203-91212.

Castro, M., & Liskov, B. (1999, February). Practical byzantine fault tolerance. In OsDI (Vol. 99, No. 1999, pp. 173-186).

Chang, J., Katehakis, M. N., Melamed, B., & Shi, J. J. (2018). Blockchain design for supply chain management. Available at SSRN 3295440.

Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. Technological Forecasting and Social Change, 144, 1-11.

Chapman, P., Xu, D., Deng, L., & Xiong, Y. (2019, July). Deviant: A mutation testing tool for solidity smart contracts. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 319-324). IEEE.

Chaum, D. L. (1982). Computer Systems established, maintained and trusted by mutually suspicious groups. Ph.D. dissertation, Computer Science Department, University of California, Berkeley

Chawla, C. (2020). Trust in blockchains: Algorithmic and organizational. Journal of Business Venturing Insights, 14, e00203.

Chen, L., Cong, L. W., & Xiao, Y. (2021). A brief introduction to blockchain economics. In Information for Efficient Decision Making: Big Data, Blockchain and Relevance (pp. 1-40).

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). In Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19 (pp. 282-297). Springer International Publishing.

Chen, T., Li, X., Luo, X., & Zhang, X. (2017, February). Under-optimized smart contracts devour your money. In 2017 IEEE 24th international conference on software analysis, evolution and reengineering (SANER) (pp. 442-446). IEEE.

Chen, W. (2018). Administrative rules and regulations for the introduction of food information traceability in blockchain (Doctoral dissertation, Ph. D. thesis, Shanghai Normal University, Shanghai).

Chen, W. E., Wang, Y. H., Huang, P. C., Huang, Y. Y., & Tsai, M. Y. (2018, August). A Smart IoT System for Waste Management. In 2018 1st International Cognitive Cities Conference (IC3) (pp. 202-203). IEEE.

Chen, W., Zhang, T., Chen, Z., Zheng, Z., & Lu, Y. (2020, April). Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In Proceedings of The Web Conference 2020 (pp. 1411-1421).

Chopra, K., Gupta, K., & Lambora, A. (2019, February). Proof of existence using blockchain. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 429-431). IEEE.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

CNN, 2018. Τι είναι το blockchain και γιατί είναι τόσο σημαντικό. Retrieved from: https://www.cnn.gr/oikonomia/story/117710/ti-einai-to-blockchain-kai-giati-einai-toso-simantiko

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. The Review of Financial Studies, 32(5), 1754-1797.

Cretu, L. G. (2012). Smart cities design using event-driven paradigm and semantic web. Informatica Economica, 16(4), 57.

Curry, E., Hasan, S., Kouroupetroglou, C., Fabritius, W., ul Hassan, U., & Derguech, W. (2018). Internet of Things Enhanced User Experience for Smart Water and Energy Management. IEEE Internet Computing, 22(1), 18-28.

Dai, W. (1998). B-money. Retrieved from: http://www.weidai.com (Accessed: November 14, 2022)

DataThick, 2024. What is Cloud analytics? | AI-centric cloud platform and Emerging Trends in AI Cloud Analytics | Future of Data Analysis with AI Cloud Analytics

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain.

De Filippi, P., Wray, C., & Sileno, G. (2021). Smart contracts. Internet Policy Review, 10(2).

De Vries, A. (2018). Bitcoin's growing energy problem. Joule, 2(5), 801-805.

Debus, J. (2017). Consensus methods in blockchain systems. Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep.

Dell'Erba, M. (2018). Demystifying Technology. Do smart contracts require a new legal framework? Regulatory fragmentation, self-regulation, public regulation. Do Smart Contracts Require a New Legal Framework.

Deloitte, (2024), The Internet of Things: Potential Impact on Life and Business. Retrieved from: https://www2.deloitte.com/us/en/pages/consulting/topics/the-internet-of-things.html

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018, March). Smart contracts vulnerabilities: a call for blockchain software engineering?. In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 19-25). IEEE.

Dhar, S. K., Bhunia, S. S., & Mukherjee, N. (2014, December). Interference aware scheduling of sensors in IoT enabled health-care monitoring system. In 2014 Fourth International Conference of Emerging Applications of Information Technology (pp. 152-157). IEEE.

Di Martino, S., & Rossi, S. (2016). An architecture for a mobility recommender system in smart cities. Procedia Computer Science, 98, 425-430.

Dib, O., Brousmiche, K. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. Int. J. Adv. Telecommun, 11(1), 51-64.

Direct Industry, 2024. Retrieved from: https://www.directindustry.com/industrial-manufacturer/temperature-sensor-medical-applications-199357.html

Drescher, D. (2017). Blockchain basics: a non-technical introduction in 25 steps: Apress, 2017, 255 pp, ISBN: 978-1-4842-2603-2.

Du, M., Chen, Q., Liu, L., & Ma, X. (2019). A blockchain-based random number generation algorithm and the application in blockchain games. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 3498-3503). IEEE.

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067.

Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In Advances in Cryptology—CRYPTO'92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992 Proceedings 12 (pp. 139-147). Springer Berlin Heidelberg.

Eigelshoven, F., Ullrich, A., & Bender, B. (2020). Public blockchain–a systematic literature review on the sustainability of consensus algorithms.

Emeç, M., Karatay, M., Dalkılıç, G., & Alkım, E. (2020). Consensus Approaches of High-Value Crypto Currencies and Application in SHA-3. In Artificial Intelligence and Applied Mathematics in Engineering Problems: Proceedings of the International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ICAIAME 2019) (pp. 572-583). Springer International Publishing.

Ethereum (2022a). Proof-of-work (POW). Retrieved from: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/ (Accessed: October 30, 2022)

Ethereum. (2022b). INTRODUCTION TO DAPPS. Retrieved from: https://ethereum.org/el/developers/docs/dapps (Accessed: September 28, 2022)

European Commission, 2020. Unleashing the full potential of smart agriculture. Retrieved from: https://cordis.europa.eu/article/id/413531-unleashing-the-full-potential-of-smart-agriculture

Eurosensor, 2019. What is a Position Sensor? Retrieved from: https://www.variohm.com/news-media/technical-blog-archive/what-is-a-position-sensor-

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16) (pp. 45-59).

Faria, R., Brito, L., Baras, K., & Silva, J. (2017, July). Smart mobility: A survey. In 2017 International Conference on Internet of Things for the Global Community (IoTGC) (pp. 1-8). IEEE.

Fauzi, M. A., Paiman, N., & Othman, Z. (2020). Bitcoin and cryptocurrency: Challenges, opportunities and future works. The Journal of Asian Finance, Economics and Business, 7(8), 695-704.

Fedorova, E. P., & Skobleva, E. I. (2020). Application of blockchain technology in higher education. European Journal of Contemporary Education, 9(3), 552-571.

Finney, H. (2004). Reusable proofs of work (rpow). URL: http://web. archive. org/web/20071222072154/http://rpow. net/, Abruf am, 11(01), 2019.

Franco, P. (2014). Understanding Bitcoin: Cryptography, engineering and economics. John Wiley & Sons.

Frank, 2000. Understanding smart sensors. Retrieved from: http://www.nomads.usp.br/pesquisas/design/dos/Capacitacao/arquivos/Understand

Frantz, C. K., & Nowostawski, M. (2016). From institutions to code: Towards automated generation of smart contracts. In 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 210-215). IEEE.

Freni, P., Ferro, E., & Moncada, R. (2022). Tokenomics and blockchain tokens: A design-oriented morphological framework. Blockchain: Research and Applications, 3(1), 100069.

Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W., Urbach, N., Baur, J., ... & Wederhake, L. (2019). Opportunities and challenges of DLT (Blockchain) in mobility and logistics.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. International Journal of Information Management, 51, 102029

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. International Journal of Information Management, 51, 102029.

Frumkin, D. (2018) What Are Ethereum Tokens? ERC-20, ERC-223, ERC-721, And ERC-777 Tokens Explained. Retrieved from: https://www.investinblockchain.com/what-are-ethereum-tokens (Accessed: December 25, 2022)

Fu, X., Wang, H., & Shi, P. (2021). A survey of Blockchain consensus algorithms: mechanism, design and applications. Science China Information Sciences, 64, 1-15.

Gapchup, A., Wani, A., Gapchup, D., & Jadhav, S. (2016). Health Care Systems Using Internet of Things. IJIRCCE, 4(12).

Garau, C., Masala, F., & Pinna, F. (2016). Cagliari and smart urban mobility: Analysis and comparison. Cities, 56, 35-46.

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological Forecasting and Social Change, 163, 120407.

Garner, B. (2018). Physical assets on the blockchain: Why bother.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. Future internet, 10(2), 20.

Gauld, S., Von Ancoina, F., & Stadler, R. (2017). The burst dymaxion: An arbitrary scalable, energy efficient and anonymous transaction network based on colored tangles. Proc. CryptoGuru PoC SIG.

Ge, L., Brewster, C., Spek, J., Smeenk, A., Top, J., van Diepen, F., ... & de Wildt, M. D. R. (2017). Blockchain for agriculture and food: Findings from the pilot study (No. 2017-112). Wageningen Economic Research.

Geeksforgeeks. (2022). Introduction to Merkle Tree. Retrieved from: https://www.geeksforgeeks.org/introduction-to-merkle-tree (Accessed: December 10, 2022)

Ghimire, S., & Selvaraj, H. (2018, December). A survey on bitcoin cryptocurrency and its mining. In 2018 26th International Conference on Systems Engineering (ICSEng) (pp. 1-6). IEEE.

Giacobbe, M., Puliafito, C., & Scarpa, M. (2016, September). The big bucket: An iot cloud solution for smart waste management in smart cities. In European Conference on Service-Oriented and Cloud Computing (pp. 43-58). Springer, Cham.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017, October). Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th symposium on operating systems principles (pp. 51-68).

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. Government Information Quarterly, 33(3), 524-534.

GlobalData. (2023). Bitcoin's Market Capitalization History (2013 – 2023, $ Billion). Retrieved from: https://www.globaldata.com/data-insights/financial-services/bitcoins-market-capitalization-history (Accessed 30 January, 2023)

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artificial Intelligence and Law, 26, 377-409.

Grattan, K. T., & Sun, T. (2000). Fiber optic sensor technology: an overview. Sensors and Actuators A: Physical, 82(1-3), 40-61.

Gray, J. Notes on Data Base Operating Systems. 1978. IBM Research Laboratory, San Jose, CA.

Greenspan, G. (2015). Ending the bitcoin vs blockchain debate. MultiChain. Retrieved from: https://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate (Accessed: July 11, 2022).

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660

Gueta, G. G., Abraham, I., Grossman, S., Malkhi, D., Pinkas, B., Reiter, M., ... & Tomescu, A. (2019, June). Sbft: a scalable and decentralized trust infrastructure. In 2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN) (pp. 568-580). IEEE.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial innovation, 2, 1-12.

Gupta, S., & Sadoghi, M. (2021). Blockchain transaction processing. arXiv preprint arXiv:2107.11592.

Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document (pp. 437-455). Springer Berlin Heidelberg.

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2, 130-139.

Han, X., Yuan, Y., & Wang, F. Y. (2019). A fair blockchain based on proof of credit. IEEE Transactions on Computational Social Systems, 6(5), 922-931.

Han, X., Yuan, Y., & Wang, F. Y. (2019). A fair blockchain based on proof of credit. IEEE Transactions on Computational Social Systems, 6(5), 922-931.

Harvard Business Review, (2024). The Rise of Analytics: How Big Data Is Transforming Businesses. Retrieved from: https://hbr.org/video/3633937151001/the-explainer-big-data-and-analytics

Hasan, R., Bhatti, A. H., Hayat, M. S., Gebreyohannes, H. M., Ali, S. I., & Syed, A. J. (2016, March). Smart peer car pooling system. In 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC) (pp. 1-6). IEEE.

Hassan, A., Ali, M. I., Ahammed, R., Khan, M. M., Alsufyani, N., & Alsufyani, A. (2021). Secured insurance framework using blockchain and smart contract. Scientific Programming, 2021, 1-11.

Hassan, N., Jain, N., & Chandna, V. K. (2018, April). Blockchain, cryptocurrency and bitcoin. In International Conference on Information Technology & Digital Applications.

Haveson, S., Lau, A., & Wong, V. (2017). Protecting farmers in emerging markets with blockchain. Newyork, NY: Cornell Tech.

He, M., Wang, H., Sun, Y., Bie, R., Lan, T., Song, Q., ... & Qiu, Z. (2022). T2L: A traceable and trustable consortium blockchain for logistics. Digital Communications and Networks.

Hellenic Blockchain Hub. (n.d.) About Blockchain Technology. Retrieved from: https://www.blockchain.org.gr/home/en/about-blockchain-technology (Accessed: April 25, 2022)

Hellman, M., & Diffie W. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

Heo, G., Yang, D., Doh, I., & Chae, K. (2021). Efficient and secure blockchain system for digital content trading. IEEE Access, 9, 77438-77450.

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857.

Higginson, M., Hilal A., & Yugac, E. (2019). Blockchain and retail banking: Making the connection. Retrieved from: https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection (Accessed: December 10, 2022)

Hinzen, F. J., Irresberger, F., John, K., & Saleh, F. (2019). The public blockchain ecosystem: An empirical analysis. SSRN Electronic Journal.

Huang, J., Tan, L., Mao, S., & Yu, K. (2021). Blockchain Network Propagation Mechanism Based on P4P Architecture. Security and Communication Networks, 2021, 1-12.

ICID, 2024. Improving Irrigation Efficiency. Retrieved from: https://icid-ciid.org/home

Insys Technologies, 2019. Benefits Of Cloud Computing. Retrieved from: https://www.insystechnologies.in/benefits-of-cloud-computing.html

Intel. (n.d.). Intel® Software Guard Extensions. Retrieved from: https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html (Accessed: November 30, 2022)

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE Access, 3, 678-708.

Jain, A., Arora, S., Shukla, Y., Patil, T., & Sawant-Patil, S. (2018). Proof of stake with casper the friendly finality gadget protocol for fair validation consensus in ethereum. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(3), 291-298.

Janowicz, K., Regalia, B., Hitzler, P., Mai, G., Delbecque, S., Fröhlich, M., ... & Lazarus, T. (2018). On the prospects of blockchain and distributed ledger technologies for open science and academic publishing. Semantic web, 9(5), 545-555.

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain: Research and Applications, 2(4), 100027.

Jing, N., Liu, Q., & Sugumaran, V. (2021). A blockchain-based code copyright management system. Information Processing & Management, 58(3), 102518.

Jing, T., Shengwei, Y., Bing, Y., & Shilong, M. (2010, October). Study on wireless sensor networks. In 2010 International Conference on Intelligent System Design and Engineering Application (Vol. 2, pp. 510-521). IEEE.

Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. Mathematical foundations of computing, 1(2), 121.

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. International Journal of Production Research, 57(7), 2009-2033.

Kamišalić, A., Turkanović, M., Mrdović, S., & Heričko, M. (2019). A preliminary review of blockchain-based solutions in higher education. In Learning Technology for Education Challenges: 8th International Workshop, LTEC 2019, Zamora, Spain, July 15–18, 2019, Proceedings 8 (pp. 114-124). Springer International Publishing.

Kankanhalli, A., Charalabidis, Y., & Mellouli, S. (2019). IoT and AI for Smart Government: A Research Agenda.

Kara, M., Laouid, A., AlShaikh, M., Hammoudeh, M., Bounceur, A., Euler, R., ... & Laouid, B. (2021). A compute and wait in pow (cw-pow) consensus algorithm for preserving energy consumption. Applied Sciences, 11(15), 6750.

Karantias, K., Kiayias, A., & Zindros, D. (2020). Proof-of-burn. In Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24 (pp. 523-540). Springer International Publishing.

Karkhanis, S. (2019). Evaluation of using pairing-based cryptography in byzcoin.

Kehrli, J. (2016). Blockchain 2.0-from bitcoin transactions to smart contract applications. Niceideas, November.

Kemmoe, V. Y., Stone, W., Kim, J., Kim, D., & Son, J. (2020). Recent advances in smart contracts: A technical overview and state of the art. IEEE Access, 8, 117782-117801.

Khan, S. I., & Hoque, A. S. L. (2016, January). Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In 2016 International Conference on Networking Systems and Security (NSysS) (pp. 1-6). IEEE.

Kiayias, A., & Russell, A. (2018). Ouroboros-bft: A simple byzantine fault tolerant consensus protocol. Cryptology ePrint Archive.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2016). Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive.

Kim, J. W. (2020). Blockchain technology and its applications: case studies. Journal of System and Management Sciences, 10(1), 83-93.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

Kiran, M. H. M., Patil, A. P., Premkumar, H., Hegde, P., & Kumar, P. R. (2021, December). Proof of Solution: Implementation of Work History as Stake in Blockchain Applications. In 2021 IEEE 18th India Council International Conference (INDICON) (pp. 1-6). IEEE.

Komninos, N. (2015). Intelligent cities: Variable geometries of spatial intelligence. In From Intelligent to Smart Cities (pp. 46-62). Routledge.

Kongmanee, J., Kijsanayothin, P., & Hewett, R. (2019, November). Securing smart contracts in blockchain. In 2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW) (pp. 69-76). IEEE.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration.

Kourtit, K., & Nijkamp, P. (2012). Smart cities in the innovation age. Innovation: The European Journal of Social Science Research, 25(2), 93-95.

Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. Peer-to-peer Networking and Applications, 9, 397-413.

Kumar, N., & Sharma, B. (2020). Opportunities and challenges with WSN's in smart technologies: A smart agriculture perspective. Handbook of wireless Sensor Networks: Issues and Challenges in Current Scenario's, 441-463.

Kumar, T. V., & Dahiya, B. (2017). Smart economy in smart cities. In Smart Economy in Smart Cities (pp. 3-76). Springer, Singapore.

Kwaaitaal, T. (1993). The fundamentals of sensors. Sensors and Actuators A: Physical, 39(2), 103-110.

Kwon, J. (2014). Tendermint: Consensus without mining. Draft v. 0.6, fall, 1(11).

Kyriazis, D., Varvarigou, T., White, D., Rossi, A., & Cooper, J. (2013, June). Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. In 2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 1-5). IEEE.

Lamport, L. (1983). The weak Byzantine generals problem. Journal of the ACM (JACM), 30(3), 668-676.

Lamport, L., & Fischer, M. (1982). Byzantine generals and transaction commit protocols.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401.

Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper, 81, 85.

Lee, E. K., Gerla, M., Pau, G., Lee, U., & Lim, J. H. (2016). Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. International Journal of Distributed Sensor Networks, 12(9), 1550147716665500.

Lesavre, L., Varin, P., & Yaga, D. (2021). Blockchain networks: Token design and management overview (No. NIST Internal or Interagency Report (NISTIR) 8301). National Institute of Standards and Technology.

Li, K., Li, H., Hou, H., Li, K., & Chen, Y. (2017, December). Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th

International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 466-473). IEEE.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future generation computer systems, 107, 841-853.

Liao, Y., Deschamps, F., Loures, E. D. F. R., & Ramos, L. F. P. (2017). Past, present and future of Industry 4.0-a systematic literature review and research agenda proposal. International journal of production research, 55(12), 3609-3629.

Lim, Y. G., Hong, K. H., Kim, K. K., Shin, J. H., Lee, S. M., Chung, G. S., ... & Park, K. S. (2011). Monitoring physiological signals using nonintrusive sensors installed in daily life equipment. *Biomedical engineering letters*, *1*, 11-20.

Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2018, July). Blockchain and IoT based food traceability for smart agriculture. In Proceedings of the 3rd international conference on crowd science and engineering (pp. 1-6).

Lo, S. K., Xu, X., Staples, M., & Yao, L. (2020). Reliability analysis for blockchain oracles. Computers & Electrical Engineering, 83, 106582.

Lombardi, P. (2011). New challenges in the evaluation of Smart Cities. Network Industries Quarterly, vol. 13 n. 3, pp. 8-10.

Lombardi, P., Giordano, S., Farouh, H., & Yousef, W. (2012). Modelling the smart city performance. Innovation: The European Journal of Social Science Research, 25(2), 137-149.

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90.

Maglaras, L., Al-Bayatti, A., He, Y., Wagner, I., & Janicke, H. (2016). Social internet of vehicles for smart cities. Journal of Sensor and Actuator Networks, 5(1), 3.

Maitra, S., Yanambaka, V. P., Abdelgawad, A., Puthal, D., & Yelamarthi, K. (2020, June). Proof-of-authentication consensus algorithm: Blockchain-based IoT implementation. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-2). IEEE.

Mammadzada, K., Iqbal, M., Milani, F., García-Bañuelos, L., & Matulevičius, R. (2020). Blockchain oracles: a framework for blockchain-based applications. In Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings 18 (pp. 19-34). Springer International Publishing.

Mapping Smart Cities in the EU. (2014). European parliament. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf (Last accessed 15 December 2018)

Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., & Tigano, D. (2020, February). Design patterns for gas optimization in ethereum. In 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 9-15). IEEE.

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change, 138, 139-154.

Masai, K., Sugiura, Y., Ogata, M., Kunze, K., Inami, M., & Sugimoto, M. (2016, March). Facial expression recognition in daily life by embedded photo reflective sensors on smart eyewear. In Proceedings of the 21st International Conference on Intelligent User Interfaces (pp. 317-326).

Matulionyte, R. (2019). Can copyright be tokenized?. Available at SSRN 3475214.

Maxey, K. (2016). Retrieved from: https://www.engineersrule.com/how-a-coke-machine-and-the-industrial-internet-of-things-can-give-birth-to-a-planetary-computer

Mazieres, D. (2015). The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation, 32, 1-45.

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.

McKinsey & Company, 2018. Skill shift: Automation and the future of the workforce. Retrieved from: https://www.mckinsey.com/featured-insights/future-of-work/skill-shift-automation-and-the-future-of-the-workforce

Medium, 2023. The Evolution of Sensor Technology: From Analog to Digital. Retrieved from: https://eelectronics.medium.com/the-evolution-of-sensor-technology-from-analog-to-digital-3857b6f37629

Medvedev, A., Fedchenkov, P., Zaslavsky, A., Anagnostopoulos, T., & Khoruzhnikov, S. (2015). Waste management as an IoT-enabled service in smart cities. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems (pp. 104-115). Springer, Cham.

Mekala, M. S., & Viswanathan, P. (2017, February). A novel technology for smart agriculture based on IoT with cloud computing. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 75-82). IEEE.

Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. Law, innovation and technology, 9(2), 269-300.

Mikhaylov, A. (2020). Cryptocurrency market analysis from the open innovation perspective. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 197.

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016, October). The honey badger of BFT protocols. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 31-42).

Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016, December). Proof of luck: An efficient blockchain consensus protocol. In proceedings of the 1st Workshop on System Software for Trusted Execution (pp. 1-6).

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In 2017 IEEE international conference on systems, man, and cybernetics (SMC) (pp. 2567-2572). IEEE.

Miranda, M. J., & Joseph, W. Glauber. 1997.". Systemic Risk, Reinsurance, and the Failure of Crop Insurance Markets.

Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In 2018 9th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-4). IEEE.

Moskov, A. (2018). Cryptocurrency Industry Spotlight: Who is NEO's Da Hongfei?.

Nakamoto, N. (2017). Centralised bitcoin: a secure and high performance electronic cash system. Available at SSRN 3065723.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 21260.

Nam, T., & Pardo, T. A. (2011, June). Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times (pp. 282-291). ACM.

Nandwani, A., Gupta, M., & Thakur, N. (2019). Proof-of-participation: Implementation of proof-of-stake through proof-of-work. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1 (pp. 17-24). Springer Singapore.

National Fire Protection Association (NFPA), 2024. Home Fire Deaths, Injuries, Property Loss, and Costs. Retrieved from: https://www.nfpa.org/education-and-research/research/nfpa-research/fire-statistical-

reports#aq=%40culture%3D%22en%22&cq=%40taglistingpage%3D%3D(%22Fire%20Statistics%22)%20%20&numberOfResults=12&sortCriteria=%40publicationdate%20descending

Nayyar, A., & Puri, V. (2016, September). Smart farming: IoT based smart sensors agriculture stick for live temperature and moisture monitoring using Arduino, cloud computing & solar technology. In Proc. of The International Conference on Communication and Computing Systems (ICCCS-2016) (pp. 9781315364094-121).

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). Journal of research of the National Institute of Standards and Technology, 106(3), 511.

Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. Journal of Information processing systems, 14(1), 101-128.

Niewolny, D. (2013). How the internet of things is revolutionizing healthcare. White paper, 1-8.

Ntuli, N., & Abu-Mahfouz, A. (2016). A simple security architecture for smart water management system. Procedia Computer Science, 83, 1164-1169.

O'grady, M., & O'hare, G. (2012). How smart is your city?. Science, 335(6076), 1581-1582.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355-364.

Olson, K., Bowman, M., Mitchell, J., Amundson, S., Middleton, D., & Montgomery, C. (2018). Sawtooth: an introduction. The Linux Foundation.

Ongaro, D., & Ousterhout, J. (2015). The raft consensus algorithm. Lecture Notes CS, 190, 2022.

P4Titan. (2014). Slimcoin: A Peer-To-Peer Crypto-Currency with Proof-of-Burn.

Pang, Z. (2013). Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being (Doctoral dissertation, KTH Royal Institute of Technology).

Parr, J. B. (1999). Growth-pole strategies in regional economic planning: A retrospective view: Part 1. Origins and advocacy. Urban studies, 36(7), 1195-1215.

Pass, R., & Shi, E. (2018). Thunderella: Blockchains with optimistic instant confirmation. In Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37 (pp. 3-33). Springer International Publishing.

Patil, A. S., Tama, B. A., Park, Y., & Rhee, K. H. (2018). A framework for blockchain based secure smart green house farming. In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17 (pp. 1162-1167). Springer Singapore.

Pendor, R. B., & Tasgaonkar, P. P. (2016, April). An IoT framework for intelligent vehicle monitoring system. In 2016 International Conference on Communication and Signal Processing (ICCSP) (pp. 1694-1696). IEEE.

Peng, K., Li, M., Huang, H., Wang, C., Wan, S., & Choo, K. K. R. (2021). Security challenges and opportunities for smart contracts in Internet of Things: A survey. IEEE Internet of Things Journal, 8(15), 12004-12020.

Pierro, G. A., & Tonelli, R. (2022, March). Can solana be the solution to the blockchain scalability problem?. In 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 1219-1226). IEEE.

Pu, H., Ge, Y., Yan-Feng, Z., & Yu-Bin, B. (2017). Survey on blockchain technology and its application prospect. Computer science, 44(4), 1-7.

Puthal, D., Mohanty, S. P., Nanda, P., Kougianos, E., & Das, G. (2019, January). Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-5). IEEE.

Qi-Guo, M. (2016). First Report on Survey of Blockchain Technology: Potential to Disrupt All Industries [J]. Report by Chuancai Securities Co., Ltd.

Raimundo, R., & Rosário, A. (2021). Blockchain system in the higher education. European Journal of Investigation in Health, Psychology and Education, 11(1), 276-293.

Ratasuk, R., N. Mangalvedhe, A. Ghosh, Overview of LTE enhancements for cellular IoT, in: Proc. of PIMRC, Hong Kong, China, 2015, pp. 2293– 2297.

Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Systems Journal, 15(1), 85-94.

Raza, U., P. Kulkarni, M. Sooriyabandara, Low power wide area networks: An overview, IEEE J. Commun. Surv. Tuto. 19 (2) (2017) 855–873.

Reijsbergen, D., Szalachowski, P., Ke, J., Li, Z., & Zhou, J. (2020). LaKSA: A probabilistic proof-of-stake protocol. arXiv preprint arXiv:2006.01427.

Ren, L. (2014). Proof of stake velocity: Building the social currency of the digital age. Self-published white paper.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

Rocha, H., & Ducasse, S. (2018, May). Preliminary steps towards modeling blockchain oriented software. In 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (pp. 52-57).

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009.

Rosic, A. (2017a). What is Ethereum Casper Protocol? Crash Course. Retrieved from: https://blockgeeks.com/guides/ethereum-casper (Accessed: December 12, 2022)

Rosic, A. (2017b). What is Litecoin? A Basic Beginners Guide Retrieved from: https://blockgeeks.com/guides/litecoin (Accessed: December 14, 2022)

Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. IEEE Access, 7, 50759-50779.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135.

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: what it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/Ispa (Vol. 1, pp. 57-64). IEEE.

Saetran, M., Seo, J., & Park, S. (2021). Leverage sidechains to reduce the workload of smart contracts through parallelization. Journal of Computing Science and Engineering, 15(3), 125-133.

Saleh, F. (2021). Blockchain without waste: Proof-of-stake. The Review of financial studies, 34(3), 1156-1190.

Salimitari, M., & Chatterjee, M. (2018). A survey on consensus protocols in blockchain for IoT networks. arXiv preprint arXiv:1809.05613.

Samaniego, M., & Deters, R. (2016, December). Hosting virtual iot resources on edge-hosts with blockchain. In 2016 IEEE International conference on computer and information technology (CIT) (pp. 116-119). IEEE.

Sangeetha, M., Manisankar, M. S., Mahalingam, M. G., & Mythreyan, M. S. (2020). Blockchain based Information Architecture for Medical Product Supply Chain.

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart contract: Attacks and protections. IEEE Access, 8, 24416-24427.

Sazandrishvili, G. (2020). Asset tokenization in plain English. Journal of Corporate Accounting & Finance, 31(2), 68-73.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review.

Schneider, F. B. (1990). Implementing fault-tolerant services using the state machine approach: A tutorial. ACM Computing Surveys (CSUR), 22(4), 299-319.

Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5(8), 151.

Sehrawat, D., & Gill, N. S. (2019, April). Smart sensors: Analysis of different types of IoT sensors. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 523-528). IEEE.

Send, D. (2017). Internet of Services: The Next-generation, Secure, Highly Scalable Ecosystem for Online Services.

Sergey, I., Nagaraj, V., Johannsen, J., Kumar, A., Trunov, A., & Hao, K. C. G. (2019). Safer smart contract programming with Scilla. Proceedings of the ACM on Programming Languages, 3(OOPSLA), 1-30.

Sheela, K., & Priya, C. (2022, October). A Research on the Perspective of Exploring Restricted Decentralized Blockchain by Applying PoFE: Proof of Familiarity and Existence to Reinforce Multiple Domains. In 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 794-798). IEEE.

Shen, W., & Norrie, D. H. (1999). Agent-based systems for intelligent manufacturing: a state-of-the-art survey. Knowledge and information systems, 1(2), 129-156.

Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C. (2015). Recent advances in industrial wireless sensor networks toward efficient management in IoT. IEEE access, 3, 622-637.

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. IEEE Security & Privacy, 17(1), 72-77.

Shoker, A. (2017, October). Sustainable blockchain through proof of exercise. In 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 1-9). IEEE.

Shyam, G. K., Manvi, S. S., & Bharti, P. (2017, February). Smart waste management using Internet-of-Things (IoT). In 2017 2nd international conference on computing and communications technologies (ICCCT) (pp. 199-203). IEEE.

Sigaki, H. Y., Perc, M., & Ribeiro, H. V. (2019). Clustering patterns in efficiency and the coming-of-age of the cryptocurrency market. Scientific reports, 9(1), 1440.

Smith, B., & Christidis, K. (2016, June). IBM Blockchain: An enterprise deployment of a distributed consensus-based transaction log. In Proc. Fourth International IBM Cloud Academy Conference (Vol. 210).

Solanas, A., Patsakis, C., Conti, M., Vlachos, I. S., Ramos, V., Falcone, F., ... & Martinez-Balleste, A. (2014). Smart health: a context-aware health paradigm within smart cities. IEEE Communications Magazine, 52(8), 74-81.

Solanki, M., 2021. Overview of Blockchain Technology: Consensus, Architecture, and Its Future Trends. International Journal of Innovative Research in Computer Science & Technology, pp.47-51.

Solidity. (n.d.) Solidity. Retrieved from: https://docs.soliditylang.org/en/v0.7.0/index.html (Accessed: July 12, 2022)

Sompolinsky, Y., & Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers 19 (pp. 507-527). Springer Berlin Heidelberg.

Sompolinsky, Y., & Zohar, A. (2017). Bitcoin's Underlying Incentives: The unseen economic forces that govern the Bitcoin protocol. Queue, 15(5), 29-52.

Song, H., Zhu, N., Xue, R., He, J., Zhang, K., & Wang, J. (2021). Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. Information processing & management, 58(3), 102507.

Srivastava, A., & Das, D. K. (2022). A comprehensive review on the application of Internet of Thing (IoT) in smart agriculture. Wireless Personal Communications, 122(2), 1807-1837.

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464.

Subrahmanyam, V., Kumar, S., Srivastava, S., Bist, A. S., Sah, B., Pani, N. K., & Bhambu, P. (2023). Optimizing horizontal scalability in cloud computing using simulated annealing for Internet of Things. Measurement: Sensors, 28, 100829.

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. computer law & security review, 33(4), 470-481.

Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 26.

Suresh, S., & Sruthi, P. V. (2015, November). A review on smart home technology. In 2015 Online International Conference on Green Engineering and Technologies (IC-GET) (pp. 1-3). IEEE.

Suvarnamma, A., & Pradeepkiran, J. A. (2021). SmartBin system with waste tracking and sorting mechanism using IoT. Cleaner Engineering and Technology, 5, 100348.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, Inc.

Sylvester, G. (2019). E-agriculture in action: blockchain for agriculture, opportunities and challenges. FAO.

Szabo, N. (1994). Smart Contracts. Retrieved from: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (Accessed: September 01, 2022)

Szabo, N. (1997). Formalizing and securing relationships on public networks. First monday.

Szabo, N. (1998). Bit Gold proposal. Decentralized Business Review, 21449.

Tang, S., Wang, Z., Jiang, J., Ge, S., & Tan, G. (2022). Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain. Scientific Reports, 12(1), 4426.

Tang, S., Wang, Z., Jiang, J., Ge, S., & Tan, G. (2022). Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain. Scientific Reports, 12(1), 4426.

TechTarget, 2023. Smart Sensor. Retrieved from: https://www.techtarget.com/iotagenda/definition/smart-sensor

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

UC Berkeley, 2024. New Study Shows Smart Home Security Systems Can Deter 80% of Break-Ins. Retrieved from: https://ucpd.berkeley.edu/safety/enhancing-safety-campus-and-community

UN-HABITAT (2010) The State of Asian Cities 2010/11, UN-HABITAT, Fukuoka. Unmanned Systems Technology, 2022. Retrieved from: https://www.unmannedsystemstechnology.com/expo/unmanned-ground-vehicle-ugv-manufacturers/

van Erp, S. (2017). Land registration systems: public, private or privately public?. European Property Law Journal, 6(1), 1-3.

Vashistha, N., Hossain, M. M., Shahriar, M. R., Farahmandi, F., Rahman, F., & Tehranipoor, M. M. (2021). eChain: a blockchain-enabled ecosystem for electronic device authenticity verification. IEEE Transactions on Consumer Electronics, 68(1), 23-37.

Vidal, F., Gouveia, F., & Soares, C. (2019, October). Analysis of blockchain technology for higher education. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 28-33). IEEE.

Vijayakumar, N., & Ramya, A. R. (2015, March). The real time monitoring of water quality in IoT environment. In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-5). IEEE.

VisionTIR, n.d. Retrieved from: https://visiontir.com/early-fire-detection-in-waste-to-energy-and-waste-management-plants/

Vodafone IoT Barometer. (2017). from https://www.vodafone.com/business/news-and-insights/white-paper/vodafone-iot-barometer-2017

Vukolić, M. (2016). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers (pp. 112-125). Springer International Publishing.

W3schools, 2023. Blockchain – Introduction. Retrieved from: https://www.w3schools.in/blockchain/introduction-to-blockchain-technology?utm_content=cmp-true

Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management.

Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P., & He, L. (2020). A comparative study of blockchain consensus algorithms. In Journal of Physics: Conference Series (Vol. 1437, No. 1, p. 012007). IOP Publishing.

Wang, Y., Cai, S., Lin, C., Chen, Z., Wang, T., Gao, Z., & Zhou, C. (2019). Study of blockchains's consensus mechanism based on credit. IEEE Access, 7, 10224-10231.

Wang, Y., Kung, L., Wang, W. Y. C., & Cegielski, C. G. (2018). An integrated big data analytics-enabled transformation model: Application to health care. Information & Management, 55(1), 64-79.

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains?. International Journal of Production Economics, 211, 221-236.

Ward, V. (2016). Police to use drones to aid criminal investigations. The Telegraph.

Waves. (n.d.). Leased Proof of Stake. Retrieved from: https://docs.waves.tech/en/blockchain/leasing#leasing-benefits-for-the-node-owner (Accessed: November 13, 2022)

Weingärtner, T. (2019, January). Tokenization of physical assets and the impact of IoT and AI. In European Union Blockchain Observatory and Forum (Vol. 10, pp. 1-16).

Werner, S. M., Pritz, P. J., & Perez, D. (2020). Step on the gas? A better approach for recommending the ethereum gas price. In Mathematical Research for Blockchain Economy (pp. 161-177). Springer, Cham.

Wince-Smith Deborah (2017). Smart Living in Smart Cities: Leading Cities Into the Future, Global Federation of Competitiveness Council, https://blog.thegfcc.org/smart-living-in-smart-cities-leading-cities-into-the-future-4c0d11669660

Woetzel, J., Remes, J., Boland, B., Lv, K., Sinha, S., Strube, G., ... & von der Tann, V. (2018). Smart cities: Digital solutions for a more livable future. McKinsey Global Inst., New York, NY, USA, Tech. Rep.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.

World Economic Forum. (2015). Deep Shift Technology Tipping Points and Societal Impact. Retrieved from: https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (Accessed: August 12, 2022)

Xiong, H., Dalhaus, T., Wang, P., & Huang, J. (2020). Blockchain technology for agriculture: applications and rationale. frontiers in Blockchain, 3, 7.

Xu, G., Bai, H., Xing, J., Luo, T., Xiong, N. N., Cheng, X., ... & Zheng, X. (2022). SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles. Journal of Parallel and Distributed Computing, 164, 1-11.

Xu, J. J. (2016). Are blockchains immune to all malicious attacks?. Financial Innovation, 2(1), 1-9.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.

Yakovenko, A. (2018). Solana: A new architecture for a high performance blockchain v0. 8.13. Whitepaper.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access, 7, 118541-118555.

Yu, J., Kim, M., Bang, H. C., Bae, S. H., & Kim, S. J. (2016). IoT as a applications: cloud-based building management systems for the internet of things. Multimedia Tools and Applications, 75(22), 14583-14596.

Yuan, Y., & Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48(9), 1421-1428.

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68, 1-13.

Yusoff, J., Mohamad, Z., & Anuar, M. (2022). A Review: Consensus Algorithms on Blockchain. Journal of Computer and Communications, 10(9), 37-50.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization, 29(2), 105-117.

Zanelatto Gavião Mascarenhas, J., Ziviani, A., Wehmuth, K., & Vieira, A. B. (2020). On the transaction dynamics of the Ethereum-based cryptocurrency. Journal of Complex Networks, 8(4), cnaa042.

Zedadra, O., Guerrieri, A., Jouandeau, N., Spezzano, G., Seridi, H., & Fortino, G. (2019). Swarm Intelligence and IoT-Based Smart Cities: A Review. In The Internet of Things for Smart Urban Ecosystems (pp. 177-200). Springer, Cham.

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In Journal of Physics: Conference Series (Vol. 1168, No. 3, p. 032077). IOP Publishing.

Zhang, C., Wang, R., Tsai, W. T., He, J., Liu, C., & Li, Q. (2019, May). Actor-based Model for Concurrent Byzantine Fault-tolerant Algorithm. In 2019 International Conference on Computer, Network, Communication and Information Systems (CNCI 2019) (pp. 552-558). Atlantis Press.

Zhang, C., Wu, C., & Wang, X. (2020, May). Overview of Blockchain consensus mechanism. In Proceedings of the 2020 2nd International Conference on Big Data Engineering (pp. 7-12).

Zhang, G., Li, C., Zhang, Y., Xing, C., & Yang, J. (2012, October). SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors. In 2012 IEEE 14th international conference on e-health networking, applications and services (Healthcom) (pp. 238-243). IEEE.

Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. ICT express, 6(2), 93-97.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. Engineering, 3(5), 616-630.

Zhou, Q., Wang, Y., & Fu, X. (2016). Information asymmetry, blockchain and food safety. Res. China Mark. Superv, 11(1), 53-56.

Zipit, 2021. What Are IoT Sensors? Types, Uses, and Examples. Retrieved from: https://www.zipitwireless.com/blog/what-are-iot-sensors-types-uses-and-examples

Zou, J., Ye, B., Qu, L., Wang, Y., Orgun, M. A., & Li, L. (2018). A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. IEEE Transactions on Services Computing, 12(3), 429-445.

Στάμος Παναγιώτης, 2013. Σχεδιασμός και υλοποίηση δικτύου αισθητήρων για εφαρμογή σε έξυπνο δωμάτιο με τη χρήση του Opnet