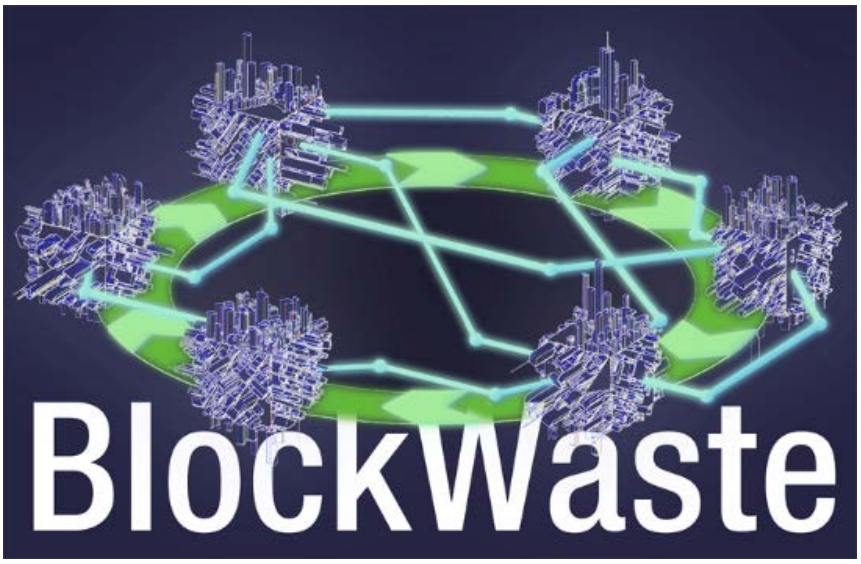
Ο1.Α3 Εγχειρίδια στρατηγικών κυκλικής οικονομίας που εφαρμόζονται στη διαχείριση δημοτικών αποβλήτων με τη χρήση τεχνολογίας Blockchain

Εγχειρίδιο ΙΙ: Blockchain



ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ΙΔΡΥΜΑ ΚΡΑΤΙΚΩΝ ΥΠΟΤΡΟΦΙΩΝ IKY

Co-funded by the Erasmus+ Programme of the European Union

Ενημερωτικό δελτίο αποτελεσμάτων:

Πρόγραμμα χρηματοδότησης	Πρόγραμμα Erasmus+ της Ευρωπαϊκής Ένωσης
ΧΡΗΜΑΤΟΔΟΤΗΣΗ	ΕΛ01 Ίδρυμα Κρατικών Υποτροφιών Ελλάδος (ΙΚΥ)
Πλήρης τίτλος του έργου	Καινοτόμος εκπαίδευση βασισμένη στην τεχνολογία Blockchain που εφαρμόζεται στη διαχείριση αποβλήτων — BlockWaste
Πεδίο	ΚΑ2 — Συνεργασία για την καινοτομία και την ανταλλαγή ορθών πρακτικών ΚΑ203 — Στρατηγικές συμπράξεις για την τριτοβάθμια εκπαίδευση
Αριθμός έργου	2020-1-EL01-KA203-079154
Διάρκεια έργου	24 μήνες
Ημερομηνία έναρξης του έργου	01-10-2020
Ημερομηνία λήξης έργου:	30-09-2022

Λεπτομέρειες παραγωγής:

Τίτλος Πνευματικού Προϊόντος: O1: Εκπαιδευτικό υλικό για διεπιστημονική Blockchain-MSW

Τίτλος Δραστηριότητας: A3. Εγχειρίδια στρατηγικών κυκλικής οικονομίας που εφαρμόζονται στη διαχείριση δημοτικών αποβλήτων με τη χρήση τεχνολογίας Blockchain

Επικεφαλής Πνευματικού Προϊόντος: ΕΜΠ

Επικεφαλής Δραστηριότητας: Saxion UAS

Συγγραφέας (-είς): Christa Barkel, c.barkel@saxion.nl, Saxion UAS, Ολλανδία, Perry Smit, Saxion UAS, p.j.smit.01@saxion.nl, Ολλανδία

Αναθεωρήθηκε από: Rainer Lenz, rlenz@fh-bielefeld.de, Bielefeld UAS, Γερμανία, Παρασκευάς Τσαγγαράτος, Εθνικό Μετσόβιο Πολυτεχνείο, ptsag@metal.ntua.gr, Ελλάδα

Έλεγχος εγγράφων

Έκδοση εγγράφου	**Η έκδοση**	**ΤΡΟΠΟΠΟΙΗΣΗ**
V0.1	11/03/2022	Τελική έκδοση — 29/04/2022

Co-funded by the Erasmus+ Programme of the European Union

ΠΕΡΙΕΧΟΜΕΝΑ

Co-funded by the Erasmus+ Programme of the European Union

Λίστα Σχημάτων

Κατάλογος συντομογραφιών

Συντομογραφία	**Ορισμός**
CBDC	Ψηφιακό νόμισμα της Κεντρικής Τράπεζας
CBDC	Ψηφιακό νόμισμα της Κεντρικής Τράπεζας
DAO	Αποκεντρωμένη Αυτόνομη Οργάνωση
DApps	Αποκεντρωμένες εφαρμογές
DLT	Κατανεμημένη τεχνολογία Ledger
ΥΠΔ	Κατ' εξουσιοδότηση απόδειξη συμμετοχής
ERC-20 (πρωτόκολλο)	Ethereum Αίτηση για Σχόλια 20 (πρωτόκολλο)
ICO	Αρχική προσφορά νομίσματος
IEO	Αρχική προσφορά ανταλλαγής
MSW	Διαχείριση αστικών στερεών αποβλήτων
NFT	Μη ανταλλάξιμο token
P2P	Peer-to-Peer
POS	Απόδειξη του πονταρίσματος
ΠΟΑ	Αποδειξη ΤΗΣ ΑΡΧΗΣ
SPOF	Μοναδικό σημείο αποτυχίας
STO	Ασφάλεια Token Προσφορά
TTP	Έμπιστος τρίτος

Συνοπτική παρουσίαση

Σε αυτό το εγχειρίδιο το Blockchain προσεγγίζεται από ένα ευρύ φάσμα προοπτικών. Η προσδοκία είναι ότι αυτό θα βοηθήσει τον αναγνώστη να αναλύσει καλύτερα τη σημασία του Blockchain και να αποκτήσει μια βαθύτερη κατανόηση των δυνατοτήτων του. Τα πρώτα βασικά στοιχεία εξηγούνται με το Bitcoin ως παράδειγμα. Το Bitcoin είναι η πρώτη εφαρμογή που χρησιμοποιεί το Blockchain. Το Bitcoin χρησιμοποιεί ένα αποκεντρωμένο δίκτυο, στο οποίο όλα τα άτομα που θέλουν να συμμετάσχουν στη διαδικασία λήψης αποφάσεων Bitcoin συμμετέχουν μαζί στη λήψη αποφάσεων. Ο κώδικας Bitcoin είναι ανοιχτός κώδικας, επιτρέποντας σε οποιονδήποτε να δει, να αντιγράψει και να επεξεργαστεί τον πηγαίο κώδικα σύμφωνα με τις προτιμήσεις του, επιτρέποντας νέα πειράματα με άλλες, ίσως καλύτερες μορφές κρυπτονομισμάτων ή άλλες εφαρμογές και άλλες μορφές συναίνεσης. Αν και το Bitcoin χρησιμοποιείται ως παράδειγμα εξήγησης, είναι σημαντικό να σημειωθεί ότι όχι μόνο το χρηματοπιστωτικό σύστημα επηρεάζεται από το Blockchain. Η υποκείμενη τεχνολογία blockchain προσφέρει νέες ευκαιρίες για τον μετασχηματισμό άλλων βιομηχανιών, συμπεριλαμβανομένης της διαχείρισης αστικών στερεών αποβλήτων.

Αυτό το εγχειρίδιο ξεκινά με μια εξήγηση του Blockchain και των χαρακτηριστικών του. Δίνεται μια σαφέστερη διάκριση μεταξύ του κρυπτονομίσματος bitcoin και του δικτύου Bitcoin και εξηγείται ο μηχανισμός συναίνεσης του Bitcoin, Proof-of-Work. Εκτός από τις βασικές αρχές Blockchain που εξηγούνται σε αυτό το εγχειρίδιο χρησιμοποιώντας το Bitcoin, η εστίαση μετατοπίζεται σε μια νεότερη γενιά Blockchains ειδικά σχεδιασμένη για να δημιουργήσει μια πληθώρα άλλων τύπων αποκεντρωμένων εφαρμογών ή dApps. Ένα συγκεκριμένο Blockchain στο οποίο επικεντρώνεται η προσοχή είναι το Ethereum, το οποίο ήταν το πρώτο που επέτρεψε τον προγραμματισμό των Έξυπνων Συμβάσεων. Ένα Έξυπνο Συμβόλαιο είναι αποκεντρωμένη αυτοματοποίηση και μπορεί να οριστεί ως μια σύμβαση με ορισμένους όρους και προϋποθέσεις που καθορίζονται σε κώδικα. Η σύμβαση είναι αυτο-εκτελέσιμη, καθώς εκτελεί κατάλληλες αντίστοιχες ενέργειες όταν πληρούνται οι όροι και οι προϋποθέσεις.

Επιπλέον, αυτό το εγχειρίδιο εξηγεί εν συντομία δύο φαινόμενα του Blockchain: αποκεντρωμένες εφαρμογές (dApps) και αποκεντρωμένοι αυτόνομοι οργανισμοί (DAO).

Το blockchain μπορεί να χωριστεί στους τύπους του από τρεις οπτικές γωνίες, το πρωτόκολλο συναίνεσης, τη διακυβέρνηση και τους τύπους συνεργασίας μεταξύ των συστημάτων Blockchain. Τα πρωτόκολλα συναίνεσης είναι απαραίτητα για τη διασφάλιση της εμπιστοσύνης μεταξύ των διαφόρων συμμετεχόντων σε ένα κατανεμημένο δίκτυο. Πρέπει να υπάρχει εμπιστοσύνη ότι οι συμμετέχοντες δεν είναι διεφθαρμένοι και ότι τα δεδομένα που μοιράζονται μεταξύ τους δεν είναι διεφθαρμένα. Στη συνέχεια, ένα Blockchain, όπως κάθε εταιρική σχέση, πρέπει να διαχειρίζεται και να ελέγχεται μέσω μιας δομής διακυβέρνησης Blockchain. Οι επιλογές μεταξύ των διαφόρων τύπων Blockchains επηρεάζουν τον έλεγχο του οργανισμού. Όσο μεγαλύτερη εμπιστοσύνη υπάρχει στον αποκεντρωμένο χαρακτήρα του Blockchain, τόσο πιο εύκολο είναι να συμμετέχετε. Όσο μεγαλύτερη είναι η βεβαιότητα ότι οι επικυρωτές μπορούν να συμμετέχουν στην οικοδόμηση συναίνεσης ως άγνωστοι, τόσο πιο διαφανές είναι το σύστημα.

Για να ολοκληρωθούν οι τρεις προοπτικές, υπάρχουν διαφορετικοί τύποι συνεργασίας μεταξύ των συστημάτων Blockchain. Blockchain όπου διαφορετικές εταιρείες και τρίτα μέρη συνεργάζονται χωρίς έναν κεντρικό χρήστη που ελέγχει αυτό το Blockchain, ονομάζεται Enterprise Blockchain. Για την κατασκευή ενός τέτοιου Enterprise Blockchain, οι εταιρείες

χρησιμοποιούν πλατφόρμες Blockchain. Αυτές οι πλατφόρμες επιτρέπουν στους χρήστες να γράφουν εφαρμογές χρησιμοποιώντας ορισμένες τεχνολογίες. Έχουν οργανωθεί διάφορες συνεργασίες γύρω από αυτές τις πλατφόρμες. Οι πλατφόρμες είναι ο τρίτος και τελευταίος τρόπος που εξετάζουμε διάφορα είδη Blockchains εδώ.

Μία από τις μεγάλες εφευρέσεις του Satoshi Nakamoto είναι ο συνδυασμός των προϋπαρχουσών τεχνολογιών με ένα σύστημα ανταμοιβής που διατηρεί ένα αποκεντρωμένο δίκτυο σε λειτουργία: τα κρυπτοοικονομικά. Η κεντρική ιδέα πίσω από τα κρυπτοοικονομικά μέσα στο Blockchain είναι ότι αναπτύσσονται πρωτόκολλα που ενθαρρύνουν τους ανθρώπους να συμμετέχουν στο δίκτυο με τέτοιο τρόπο ώστε η αξία του δικτύου να μεγιστοποιείται για τους συμμετέχοντες.

Ένα crypto token μπορεί να δημιουργηθεί σε ένα Blockchain και επίσης να αντιπροσωπεύει ένα εμπορεύσιμο περιουσιακό στοιχείο. Μερικές φορές δημιουργούνται μάρκες για τη χρηματοδότηση ενός έργου. Η διαδικασία της συμβολικής δημιουργίας ονομάζεται tokenization. Η διαπραγμάτευση αυτών των «κουπονιών» επιτρέπει τη μεταβίβαση της κυριότητας στα υποκείμενα περιουσιακά στοιχεία. Αυτό το εγχειρίδιο εξηγεί διαφορετικούς τύπους μαρκών και τη χρήση τους.

Συμπερασματικά, υπάρχουν τρία παραδείγματα χρήσης και εφαρμογής του Blockchain, συμπεριλαμβανομένης της ερμηνείας ορισμένων κρίσιμων προϋποθέσεων που απαιτούνται για την επιτυχή εφαρμογή του Blockchain.

1 Εισαγωγή

1.1 Σύντομη περιγραφή του έργου

Το έργο BlockWaste στοχεύει στην αντιμετώπιση της διαλειτουργικότητας μεταξύ της διαχείρισης αποβλήτων και της τεχνολογίας blockchain και στην προώθηση της ορθής επεξεργασίας τους μέσω της εκπαιδευτικής κατάρτισης, έτσι ώστε τα δεδομένα που συλλέγονται να μοιράζονται σε ένα ασφαλές περιβάλλον, όπου δεν υπάρχει περιθώριο αβεβαιότητας και δυσπιστίας μεταξύ όλων των εμπλεκόμενων μερών. Για το σκοπό αυτό, οι στόχοι του έργου BlockWaste είναι οι εξής:

- Διεξαγωγή έρευνας σχετικά με τα στερεά απόβλητα που παράγονται στις πόλεις και τον τρόπο διαχείρισής τους, ώστε να μπορούν να χρησιμοποιηθούν για τη δημιουργία μιας βάσης πληροφοριών ορθών πρακτικών, προκειμένου να επανεισαχθούν τα απόβλητα στην αλυσίδα αξίας, προωθώντας την ιδέα των Ευφυών Κυκλικών Πόλεων.
- Για τον προσδιορισμό των οφελών της τεχνολογίας Blockchain στο πλαίσιο της διαδικασίας διαχείρισης αστικών αποβλήτων (MSW).
- Να δημιουργήσει ένα σχέδιο σπουδών που θα επιτρέπει την κατάρτιση των εκπαιδευτικών και των επαγγελματιών των οργανισμών και των επιχειρήσεων του τομέα, στην αλληλεπικάλυψη των τομέων της διαχείρισης αποβλήτων, της κυκλικής οικονομίας και της τεχνολογίας Blockchain.
- Ανάπτυξη ενός διαδραστικού εργαλείου βασισμένου στην τεχνολογία Blockchain, το οποίο θα καταστήσει δυνατή την πρακτική εφαρμογή της διαχείρισης των δεδομένων που λαμβάνονται από τα αστικά απόβλητα, απεικονίζοντας έτσι τον τρόπο με τον οποίο εφαρμόζονται τα δεδομένα στην Blockchain και επιτρέποντας στους χρήστες να αξιολογούν τις διάφορες μορφές διαχείρισης.

Το BlockWaste στοχεύει να εφαρμόσει διακρατικά νέα εκπαιδευτικά περιεχόμενα με στόχο την κατάρτιση των μαθητών του στις χώρες εταίρους και την παροχή των απαραίτητων βασικών δεξιοτήτων που τους επιτρέπουν να ενεργούν επαγγελματικά ως μελλοντικοί εργαζόμενοι στον τομέα, προσθέτοντας ψηφιακές ικανότητες που απαιτούνται από εταιρείες που αγκαλιάζουν τη διαδικασία του ψηφιακού μετασχηματισμού. Υπό αυτή την έννοια, το έργο απευθύνεται σε:

- Επιχειρήσεις και μικρομεσαίες επιχειρήσεις, επαγγελματίες ΤΠ, πολεοδόμους και επαγγελματίες διαχείρισης αποβλήτων.
- Πανεπιστήμια (καθηγητές, φοιτητές και ερευνητές).
- Δημόσιους οργανισμούς.

Το έργο περιλαμβάνει τέσσερα πνευματικά αποτελέσματα ως εξής:

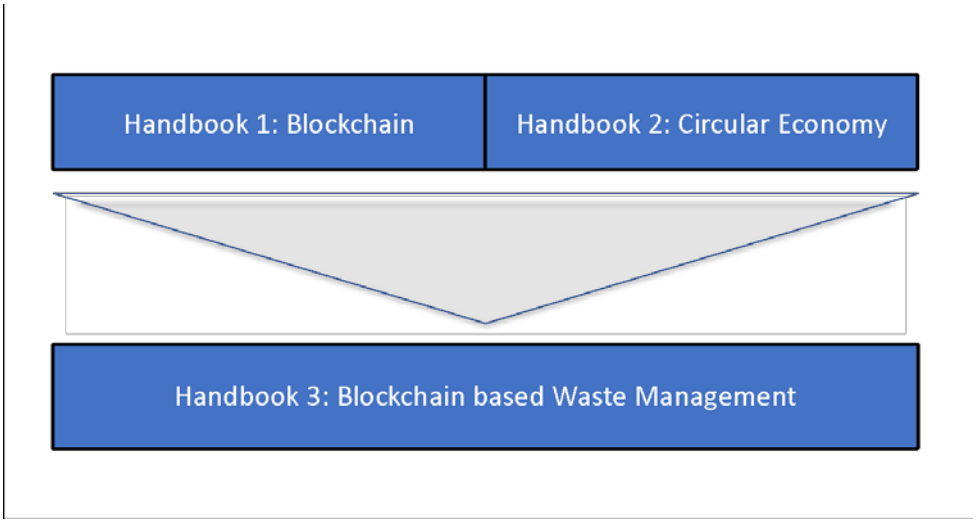
- O1. Εκπαιδευτικό υλικό για την διεπιστημονική περιοχή Blockchain-MSW
- O2. Κοινό ευρωπαϊκό πρόγραμμα σπουδών για τα MSW που εφαρμόζουν τις τεχνολογίες Blockchain στις στρατηγικές κυκλικής οικονομίας
- O3. Ψηφιακό Εργαλείο μάθησης (e-learning tool) με βάση το Blockchain-MSW επικεντρωμένο στην κυκλική οικονομία
- O4. BlockWaste Ανοιχτός Εκπαιδευτικός Πόρος (OER)

Αυτό το έγγραφο περιγράφει και εξηγεί τις βασικές αρχές του Blockchain. Περιγράφει τι είναι Blockchain, πότε μπορείτε να το χρησιμοποιήσετε, από ποια συστατικά αποτελείται ένα

Blockchain, ποιες τεχνολογίες Blockchain χρησιμοποιούνται και δίνει μια περιγραφή των διαφόρων επιτυχημένων εφαρμογών Blockchain.

1.2 Στόχοι και μεθοδολογική προσέγγιση

Στόχος αυτού του εγχειριδίου «Blockchain» είναι να καθοδηγήσει τους επαγγελματίες στον τομέα της διαχείρισης αποβλήτων σχετικά με τον τρόπο με τον οποίο θα πρέπει να εφαρμόσουν την τεχνολογία IoT και Blockchain ως στρατηγικές της κυκλικής οικονομίας. Ως εκ τούτου, απευθύνεται σε επαγγελματίες που γνωρίζουν τα πλεονεκτήματα της χρήσης της τεχνολογίας Blockchain. Τα τρία κοινά εγχειρίδια αυτού του έργου Blockwaste έχουν ως στόχο να παρέχουν στους αναγνώστες επαρκή γνώση των δυνατοτήτων της τεχνολογίας Blockchain να συμβάλουν σε μεγαλύτερη κυκλικότητα στη διαχείριση αστικών στερεών αποβλήτων. Το Εγχειρίδιο 1 (Blockchain) και το Εγχειρίδιο 2 (Κυκλική Οικονομία) πρέπει να νοούνται ως μια σύντομη σύνοψη και να παρέχουν μια επισκόπηση του ουσιαστικού περιεχομένου του Εγχειριδίου 3 (Blockchain based Waste Management) — βλ. Σχ. 1.



Σχήμα 1:Εγχειρίδια BlockWaste (οι συγγραφείς)

Η δομή του εγχειριδίου ακολουθεί μια επαγωγική λογική παρουσιάζοντας, στο πρώτο μέρος (κεφάλαιο 1 έως 4), μια σύντομη ιστορία του Blockchain μέσω του Bitcoin και των βασικών στοιχείων της τεχνολογίας Blockchain Το δεύτερο μέρος του εγχειριδίου (κεφάλαιο 5) περιέχει μια σαφή καθοδήγηση για τις χρήσεις και τις εφαρμογές της τεχνολογίας Blockchain.

2 Βασικές αρχές Blockchain

Κατανόηση των αρχών Blockchain μέσω Bitcoin

«Συγγνώμη που δεν θα είμαι αρεστός. Γράφοντας μια περιγραφή για αυτό το πράγμα για το γενικό κοινό είναι αιματηρά δύσκολο. Δεν υπάρχει τίποτα που να σχετίζεται με αυτό.» **Satoshi Nakamoto (2010)**

2.1 Εισαγωγή

Μαθησιακοί στόχοι

- Blockchain στο πιο βασικό επίπεδο εξετάζοντας το Bitcoin.
- Το blockchain είναι ουσιαστικά ένα κατανεμημένο καθολικό-μητρώο στο οποίο μπορείτε να αποθηκεύσετε δεδομένα.
- Οι διαφορές μεταξύ ενός δικτύου Blockchain και ενός κεντρικού δικτύου.

Εισαγωγή

Στις 31 Οκτωβρίου 2008, ένα μήνυμα ηλεκτρονικού ταχυδρομείου εστάλη με το όνομα Satoshi Nakamoto στη λίστα αλληλογραφίας Cryptography[1]. Το μήνυμα ηλεκτρονικού ταχυδρομείου περιελάβανε μια αναφορά σε μια **λευκή βίβλο** με τίτλο *Bitcoin: Ηλεκτρονικό σύστημα μετρητών* δικτύου ομότιμων κόμβων. Η Λευκή Βίβλος που επισυνάπτει στην ανακοίνωση είναι ένα έγγραφο μήκους 9 σελίδων, που περιγράφει τις τεχνικές λειτουργίες του Bitcoin. Το σύστημα αυτό καθιστά δυνατή την αποστολή ηλεκτρονικών πληρωμών σε άλλα μέρη, χωρίς την ανάγκη χρηματοπιστωτικού ιδρύματος.

Τα κύρια χαρακτηριστικά αυτού του συστήματος πληρωμών, σύμφωνα με τον Satoshi:

1. Οι διπλές δαπάνες αποτρέπονται με ένα δίκτυο ομότιμων κόμβων (peer-to-peer).
2. Κανένα νομισματοκοπείο ή άλλα έμπιστα χρηματοοικονομικά συστήματα.
3. Οι συμμετέχοντες μπορούν να είναι ανώνυμοι.
4. Νέα νομίσματα είναι κατασκευασμένα από «απόδειξη εργασίας» (Proof-of-Work) μορφής Hashcash.
5. Η «απόδειξη της εργασίας» για τη νέα παραγωγή νομισμάτων δίνει επίσης τη δυνατότητα στο δίκτυο να αποτρέψει τις διπλές δαπάνες.

Τεχνικοί όροι όπως διπλές δαπάνες, δίκτυο ομότιμων κόμβων (peer-to-peer), απόδειξη της εργασίας, Hashcash, χρονοσφραγίδες, hashing και ψηφιακές υπογραφές στο ηλεκτρονικό ταχυδρομείο δυσκολεύουν το ευρύ κοινό να κατανοήσει το Bitcoin ή γενικότερα το Blockchain. Ειδικά εκείνη την εποχή, όταν δεν υπήρχε τίποτα να σχετιστεί με αυτό για τους

[1] Το αρχικό μήνυμα ηλεκτρονικού ταχυδρομείου διατίθεται στη διεύθυνση: περιγραφή:Διάφορα.

Co-funded by the Erasmus+ Programme of the European Union

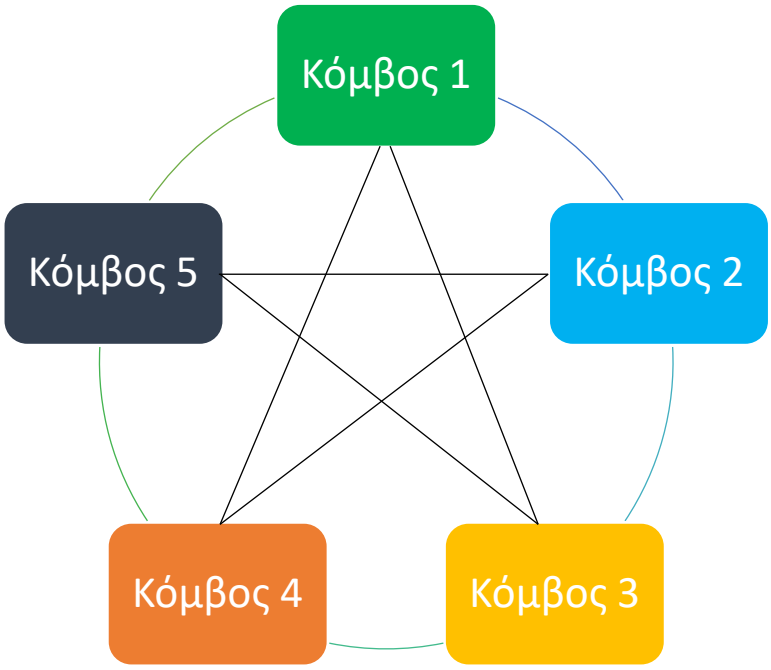
περισσότερους ανθρώπους. Σε αυτό το κεφάλαιο, συζητάμε το Bitcoin ως το μέσο για την κατανόηση των βασικών αρχών Blockchain.

2.1.1 Bitcoin vs Bitcoin

Γενικά κάνουμε μια διάκριση μεταξύ του bitcoin, το ψηφιακό χρήμα που ονομάζεται επίσης κρυπτονόμισμα, και του Bitcoin, το υποκείμενο χρηματοπιστωτικό δίκτυο που επιτρέπει τα bitcoins να αποστέλλονται και να λαμβάνονται.

2.1.2 Δίκτυο ομότιμων κόμβων peer-to-peer

Οι υπολογιστές, ονομάζονται επίσης ***κόμβοι***, που λειτουργούν αυτό το οικονομικό δίκτυο διαθέτουν και έχουν πρόσβαση σε ένα μητρώο (ledger) στο οποίο καταγράφονται όλες οι συναλλαγές bitcoin. Αυτό το μητρώο Bitcoin είναι ένα αρχείο όλων των έγκυρων συναλλαγών που έχουν ποτέ μεταδοθεί στο δίκτυο, η οποία είναι η υποκείμενη υποδομή που αποτελείται από τους κόμβους που παρακολουθούν, επικυρώνουν και χρονοσφραγίζουν όλες τις συναλλαγές bitcoin. Ονομάζουμε αυτό το δίκτυο δίκτυο ομότιμων κόμβων ***(peer-2-peer (P2P).***



Σχήμα 2: Μια αναπαράσταση ενός κατανεμημένου δικτύου, όπου το Blockchain διανέμεται σε ένα δίκτυο πλήρων κόμβων (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 1, σελίδα 14).

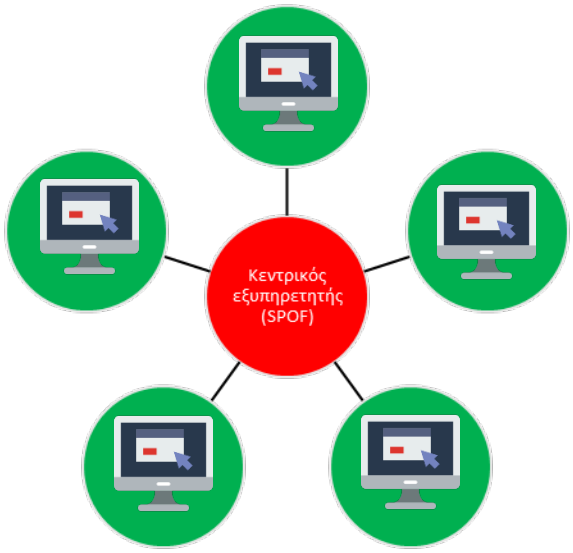
Ένα δίκτυο P2P είναι ένα δίκτυο κόμβων, συχνά ένας υπολογιστής, που είναι ισότιμα προνομιούχοι. Κάθε κόμβος μπορεί να είναι πάροχος υπηρεσιών, καθώς και καταναλωτής υπηρεσιών. Όλοι έχουν πρόσβαση στο δίκτυο Bitcoin και είναι ελεύθεροι να διαχειριστούν έναν κόμβο στο δίκτυο. Εξειδικευμένοι κόμβοι στο δίκτυο, που ονομάζονται επίσης ***πλήρεις κόμβοι***, διατηρούν ολόκληρο το ιστορικό συναλλαγών. Για να καταστρέψει ολόκληρο το

δίκτυο και το αντίστοιχο ιστορικό συναλλαγών του, θα πρέπει να κλείσουν όλοι οι κόμβοι, κάτι που είναι σχεδόν αδύνατο όταν το δίκτυο αποτελείται από πολλούς κόμβους.

Κάθε συμμετέχων στο δίκτυο ακολουθεί το πρωτόκολλο Bitcoin. Το πρωτόκολλο Bitcoin είναι οι διαδικαστικοί κανόνες που διέπουν το δίκτυο Bitcoin. Επιπλέον, δεν υπάρχει ενδιάμεσος μεταξύ δύο διαφορετικών κόμβων. Αυτό σημαίνει επίσης ότι δεν υπάρχει κεντρικός κόμβος που να μπορεί να ρυθμίσει, να ματαιώσει και να παύσει τις συναλλαγές σας. Η κατάργηση αυτών των μεσαζόντων επιτρέπει πιο αποτελεσματικές και φθηνότερες συναλλαγές.

2.1.3 Δίκτυο client-server

Το δίκτυο **P2P** έρχεται σε αντίθεση με το ***δίκτυο πελάτη – εξυπηρετητή (client-server)*** (workstation-server network).



Σχήμα 3:Απλοποιημένο δέντρο αποφάσεων είτε πρέπει να χρησιμοποιηθεί το Blockchain είτε όχι (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 1).

Ένα δίκτυο πελάτη-εξυπηρετητή χρησιμοποιεί κεντρικούς διακομιστές που παρέχουν υπηρεσίες, όπως μια υπηρεσία ηλεκτρονικού ταχυδρομείου, στους πελάτες του. Ο διακομιστής περιέχει συχνά δεδομένα και εφαρμογές. Όταν οι πελάτες χρειάζονται πρόσβαση σε αυτούς τους πόρους, μπορούν να υποβάλουν ένα αίτημα στο διακομιστή. Μια αδυναμία των δικτύων πελάτη- εξυπηρετητή είναι ότι περιέχει ένα ***Μοναδικό σημείο αποτυχίας (Single Point Of Failure, SPOF)***. Σε αυτή την περίπτωση, το SPOF είναι ο κεντρικός εξυπηρετητής. Μόλις απενεργοποιηθεί, οι πελάτες δεν θα μπορούν πλέον να έχουν πρόσβαση στις υπηρεσίες του εξυπηρετητή.

Η ανάγκη να εμπιστευτείτε ένα κεντρικό κόμβο για τα δεδομένα σας και να εμπιστευτείτε ότι το SPOF δεν θα αποτύχει καθιστά το μοντέλο ευάλωτο. Μεγάλες αξιόπιστες εταιρείες μπορούν επίσης να υποφέρουν από έναν σχεδιασμό δικτύου SPOF. Για παράδειγμα, το 2015 υπήρξε διακοπή ρεύματος σε ένα μόνο κέντρο δεδομένων PayPal. Ως αποτέλεσμα, πολλοί

χρήστες δεν μπορούσαν πλέον να έχουν πρόσβαση στον ιστότοπο PayPal, οι συναλλαγές με πιστωτικές κάρτες δεν μπορούσαν πλέον να υποβάλλονται σε επεξεργασία, οι χρήστες δεν μπορούσαν πλέον να έχουν πρόσβαση στα προσωπικά στοιχεία του λογαριασμού τους ή εμφανίστηκαν εσφαλμένοι ισολογισμοί.[2]

2.1.4 Υβριδικά δίκτυα: η περίπτωση του Napster

Υπάρχουν επίσης υβριδικά δίκτυα. Ένα διάσημο παράδειγμα είναι το Napster, μια υπηρεσία λήψης μουσικής που απέκτησε φήμη στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000.

Το 1999, μια υπηρεσία ανταλλαγής αρχείων peer-to-peer που ονομάζεται Napster ξεκίνησε από τους εφήβους Shawn Fanning και Sean Parker. Το Napster έδωσε τη δυνατότητα στους ανθρώπους να μοιράζονται εύκολα και να κατεβάζουν ψηφιακά αρχεία μουσικής από άλλους. Προκάλεσε πολλή αναστάτωση, γιατί για πρώτη φορά η μουσική μοιράστηκε, ευρέως, ο ένας με τον άλλον, δωρεάν. Το Napster επέτρεψε στους ανθρώπους να κατεβάσουν και να ακούν μεμονωμένα τραγούδια. Πριν, αν ήθελες να αποκτήσεις ένα τραγούδι, έπρεπε να αγοράσεις το πλήρες άλμπουμ. Το 2001, το Napster έκλεισε τελικά μετά από αγωγή της Recording Industry Association of America, επειδή η διανομή και η λήψη ψηφιακών μουσικών αρχείων θεωρήθηκε ότι παραβιάζει το νόμο περί πνευματικών δικαιωμάτων. Παρ' όλα αυτά, το Napster εξακολουθεί να είναι γνωστό ως μια επαναστατική υπηρεσία που έχει διαταράξει τη μουσική βιομηχανία. Στις Ηνωμένες Πολιτείες, οι πωλήσεις CD κορυφώθηκαν το 2000, ενώ την επόμενη χρονιά σημειώθηκε απότομη πτώση — εν μέρει λόγω της υπηρεσίας Napster και των επακόλουθων υπηρεσιών όπως το BitTorrent και το Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

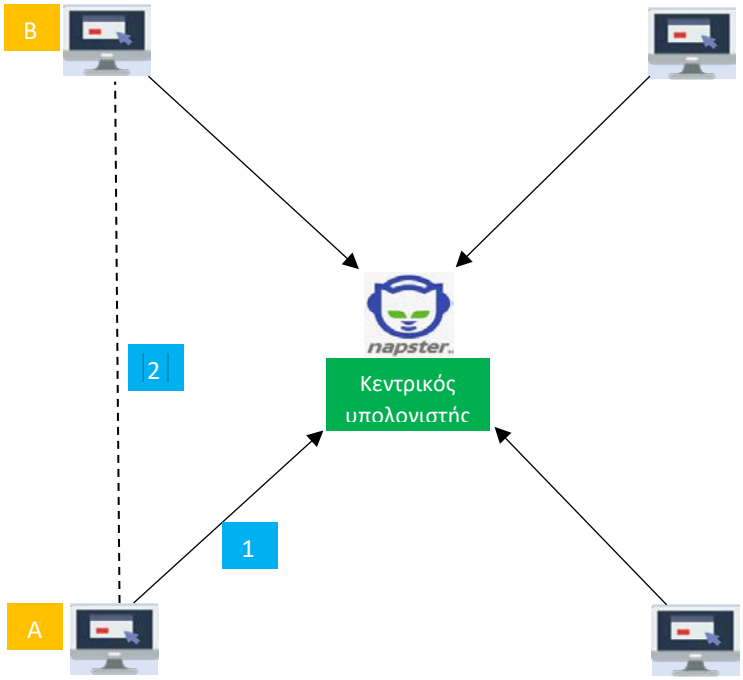
Σχήμα 4:Δελτίο ειδήσεων της ώρας της Νέας Υόρκης· Ο Napster καλείται να παραμείνει κλειστός στις 12 Ιουλίου 2001.

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Το Napster είναι γνωστό ότι χρησιμοποιεί ένα δίκτυο P2P. Πώς οι αρχές κατάφεραν να κλείσουν το Napster, κάτι που είναι σχεδόν αδύνατο με το Bitcoin;

Το Napster χρησιμοποιεί ένα κεντρικό ευρετήριο που παρακολουθεί ποιος υπολογιστής έχει ποια αρχεία για να μοιραστεί με άλλους χρήστες. Αν ένας χρήστης (υπολογιστής Α) θέλει να ψάξει για ένα τραγούδι όπως ο Michael Jackson — Billie Jean, γίνεται σύνδεση με το ευρετήριο και γίνεται αναζήτηση ποιοι υπολογιστές έχουν αυτό το τραγούδι. Εάν το ευρετήριο δείχνει ότι ο υπολογιστής Β έχει αυτό το τραγούδι, γίνεται άμεση σύνδεση μεταξύ των υπολογιστών Α και Β, επιτρέποντας στον Α να κατεβάσει απευθείας τον τραγούδι από τον υπολογιστή του Β.

Το Napster είναι ένα μικτό μοντέλο πελάτη- εξυπηρετητή και δίκτυο ομότιμων κόμβων. Το κεντρικό στοιχείο του συστήματος αποτελεί ένα client-server, αλλά τα πραγματικά αρχεία μεταφορτώνονται μέσω διαδικασίων peer-to-peer. Ο κεντρικός διακομιστής ευρετηρίου έχει αποδειχθεί ότι είναι μια σοβαρή αχίλλειος φτέρνα για το Napster επειδή μπορεί να κλείσει εύκολα, προκαλώντας το Napster να σταματήσει να λειτουργεί. Επειδή το Napster έχει μόνο έναν κεντρικό εξυπηρετητή ευρετηρίου, ο οποίος απαριθμεί τους υπολογιστές που έχουν διαθέσιμα αρχεία μουσικής, το ίδιο το Napster δεν έχει αρχεία μουσικής στον εξυπηρετητή του. Διευκολύνει τους χρήστες να κάνουν συνδέσεις peer-to-peer και να μοιραστούν μουσική μεταξύ τους.



Σχήμα 5:Δίκτυο Νάπστερ. (1) Υπολογιστής Α εκτελεί μια αναζήτηση στον κεντρικό διακομιστή του Napster για τον Michael Jackson — Billy Jean. Ο κεντρικός διακομιστής ευρετηρίου του Napster αναζητά υπολογιστές συνδεδεμένους στο δίκτυο που έχουν τον αριθμό που είναι διαθέσιμος στον σκληρό τους δίσκο. (2) Ο υπολογιστής Β έχει τον αριθμό. Τοποθέτηση υπολογιστών Α και Β απευθείας peer-to-peer σύνδεση, μετά την οποία ο υπολογιστής Α κατεβάζει το αρχείο μουσικής από τον υπολογιστή Β.

Ενώ η κοινή χρήση αρχείων μουσικής με το Napster πραγματοποιείται με διεργασίες δικτύου ομότιμων κόμβων, περιλαμβάνει επίσης ένα κεντρικό στοιχείο εξυπηρετητή, το οποίο το καθιστά επιρρεπή σε επιθέσεις. Σε αυτή την περίπτωση, έκλεισε από τις αρχές επιβολής του

νόμου. Με το δίκτυο Bitcoin, όλοι οι κόμβοι έχουν ένα ακριβές αντίγραφο του δημόσιου καθολικού Bitcoin. Το δίκτυο Bitcoin αποτελείται από πολλούς κόμβους, οι οποίοι είναι διασκορπισμένοι σε όλο τον κόσμο, καθιστώντας δύσκολο να τους εντοπίσουμε και να τους κλείσουμε όλους.

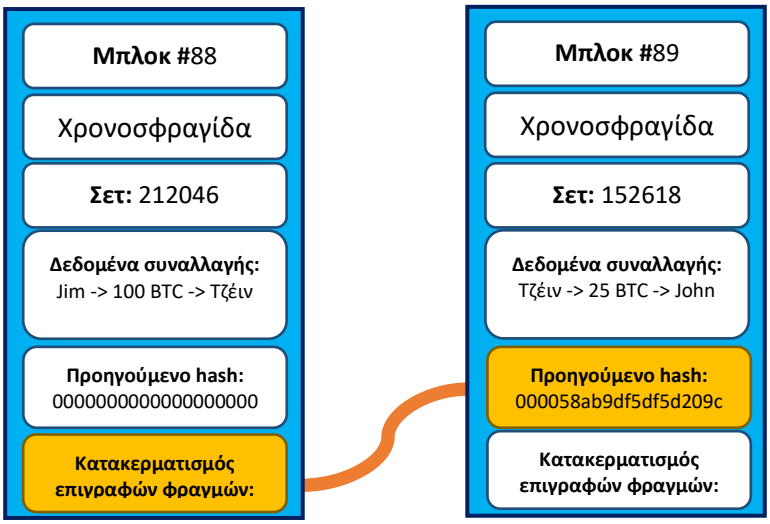
2.1.5 Blockchain

Το δημόσιο καθολικό/μητρώο Bitcoin θεωρείται αποκεντρωμένο καθώς διανέμεται σε κόμβους σε όλο τον κόσμο. Το δημόσιο καθολικό Bitcoin ονομάζεται επίσης αλυσίδα μπλοκ ή Blockchain που περιέχει τα δεδομένα συναλλαγών. Αν δούμε το Blockchain ως βάση δεδομένων που καταγράφει πληροφορίες, αυτές είναι οι βασικές εγγενείς ιδιότητες ενός Blockchain:

1. Τα δεδομένα είναι διατεταγμένα σε μπλοκ δεδομένων.
2. Τα μπλοκ ανεβαίνουν σταδιακά σε αριθμούς μπλοκ.
3. Τα δεδομένα είναι αξιόπιστα επειδή είναι κρυπτογραφικά επαληθεύσιμα.

Η αλυσίδα είναι η βάση δεδομένων συναλλαγών που κατασκευάζεται από κόμβους που συμμετέχουν στη διαδικασία εξόρυξης στο δίκτυο Bitcoin. Η αλυσίδα διατηρείται από έναν διακομιστή χρονοσφραγίδας, ο οποίος δημιουργεί μια εγγραφή ως απόδειξη της χρονολογικής σειράς των συναλλαγών. Κάθε μπλοκ περιέχει μια αναφορά (hash reference) στο μπλοκ που χτίζει, το οποίο δημιουργεί μια γραμμική ακολουθία με την πάροδο του χρόνου. Τα μπλοκ μπορούν να θεωρηθούν ως οι μεμονωμένες σελίδες ενός βιβλίου εγγραφών.

Οι «εξορύκτες» (***Miners***) επεξεργάζονται συνεχώς συναλλαγές σε μπλοκ, τα οποία προσθέτουν στο τέλος της αλυσίδας. Η διαδικασία της οποίας οι «*εξορύκτες*» προσθέτουν νέα μπλοκ στην αλυσίδα ονομάζεται επίσης ***απόδειξη εργασίας (Proof-of-Work)***. Η διαδικασία αυτή αποφεύγει τις ***διπλές δαπάνες (double-spending)***.



Σχήμα 6: Απλοποιημένη αναπαράσταση ενός έγκυρου μπλοκ γένεσης και μπλοκ #2 με τα δύο μπλοκ αλυσοδεμένα μαζί χρησιμοποιώντας το hash κεφαλίδας μπλοκ και το προηγούμενο hash. (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 3).

2.1.6 Διπλή δαπάνη

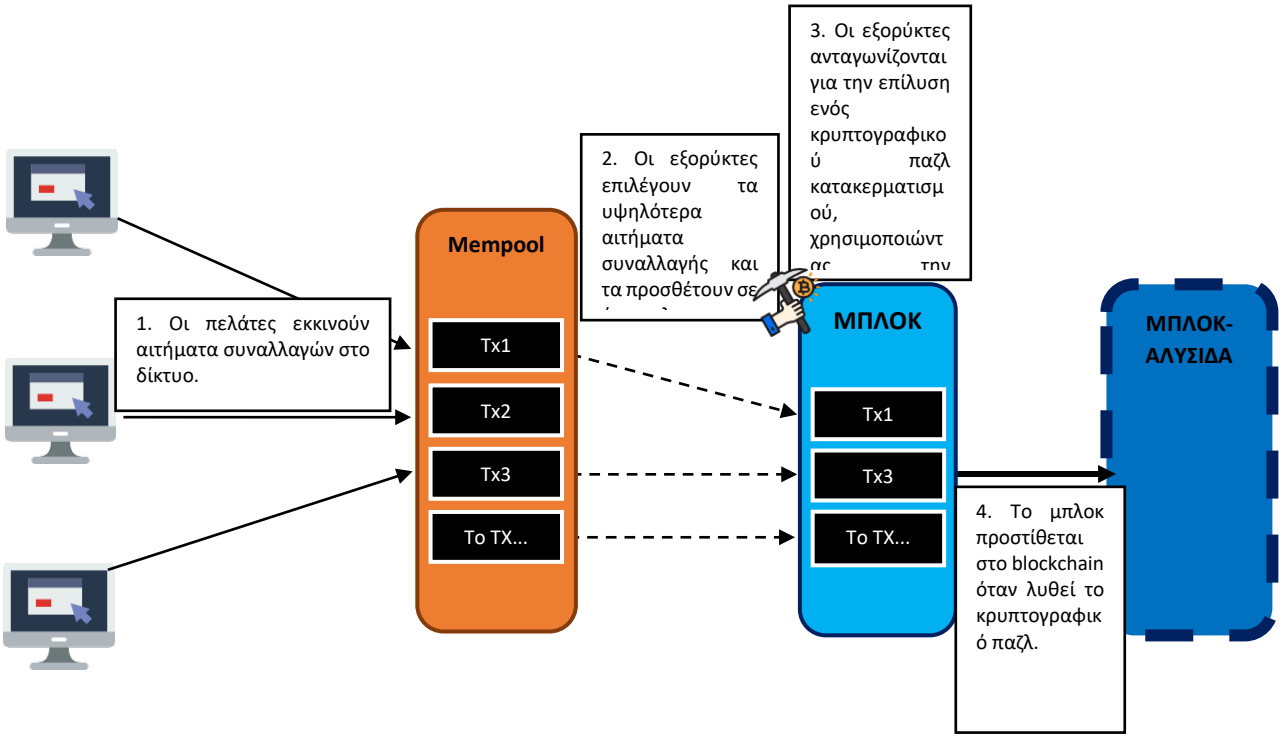
Ένα σημαντικό ζήτημα που πρέπει να επιλύσει ένα ηλεκτρονικό χρηματοπιστωτικό σύστημα peer-to-peer είναι το ζήτημα των διπλών δαπανών. Η διπλή δαπάνη είναι η πράξη της δαπάνης ενός bitcoin περισσότερες από μία φορές. Για παράδειγμα, αν έχετε 1 bitcoin και το ξοδεύετε στο άτομο Α και το άτομο Β ταυτόχρονα. Μέσα σε ένα κεντρικό οικονομικό δίκτυο, το πρόβλημα διπλής δαπάνης μπορεί να επιλυθεί από ένα ***αξιόπιστο τρίτο μέρος (TTP)*** που διατηρεί το μητρώο και ελέγχει όλες τις συναλλαγές εντός του μητρώου.

Μέσα στο δίκτυο Bitcoin, αυτό το πρόβλημα λύνεται μέσω των οικονομικών κινήτρων και της χρήσης ενός εξυπηρετητή χρονοσφραγίδας. Οι εξορύκτες έχουν ισχυρό κίνητρο να μην συμπεριλάβουν αυτές τις συναλλαγές σε ένα μπλοκ επειδή κινδυνεύουν να απορρίψουν το μπλοκ τους από άλλους εξορύκτες και, επιπλέον, θα ήταν συνένοχοι στη διάπραξη ενός εγκλήματος.

2.1.7 Απόδειξη εργασίας (Proof-of-Work)

Εκτός από την αποφυγή των διπλών δαπανών, ο σκοπός της "απόδειξης εργασίας" είναι επίσης η προστασία του δικτύου από τους επιτιθέμενους και η επίτευξη συναίνεσης σχετικά με την κατάσταση του δημόσιου μητρώου. Εν ολίγοις, η απόδειξη της εργασίας είναι ένας μηχανισμός που απαιτεί από τους εξορύκτες να χρησιμοποιούν την ισχύ του υπολογιστή για να βρουν τις σωστές τιμές για ένα μπλοκ στο οποίο εργάζονται. Με την εύρεση της σωστής κατακερματισμένης τιμής (hash), τους επιτρέπεται να προσθέσουν το μπλοκ στο blockchain και να λάβουν μια ανταμοιβή σε bitcoins. Η διαδικασία εύρεσης της σωστής τιμής ονομάζεται εξόρυξη.

Οι συναλλαγές που μεταδίδονται στο δίκτυο δεν προστίθενται άμεσα σε ένα μπλοκ από τον εξορύκτη, ούτε αποθηκεύονται απευθείας στο μητρώο. Πρώτα καταλήγουν σε μια ***δεξαμενή μνήμης*** (mempool) με άλλες συναλλαγές που δεν έχουν ακόμη προστεθεί σε ένα μπλοκ από τους εξορύκτες και δεν έχουν ακόμη επιβεβαιωθεί από το δίκτυο. Μπορείτε να σκεφτείτε το mempool ως χώρο αναμονής για όλες τις εισερχόμενες συναλλαγές που δεν έχουν ακόμη επιβεβαιωθεί από το δίκτυο. Κάθε εξορύκτης έχει τη δική του mempool και είναι πιθανό ότι οι μεμονωμένες mempools διαφέρουν ανά εξορύκτη. Αυτό συμβαίνει επειδή υπάρχει πάντα καθυστέρηση δικτύου μέσα σε ένα δίκτυο υπολογιστών: χρειάζεται πάντα λίγος χρόνος για μια συναλλαγή που αποστέλλεται στο δίκτυο για να φτάσει σε όλους τους εξορύκτες στο δίκτυο.



Σχήμα 7:Σχηματική αναπαράσταση του πώς μια συναλλαγή προστίθεται στο Blockchain. Το mempool είναι όπου οι ανεπιβεβαίωτες συναλλαγές έρχονται και φυλάσσονται. Οι ανθρακωρύχοι επιλέγουν ποιες από τις συναλλαγές από το mempool που θέλουν να προσθέσουν στο μπλοκ. Στη συνέχεια, προσπαθούν να λύσουν ένα κρυπτογραφικό παζλ. Μόλις λυθούν, λαμβάνουν μια ανταμοιβή μπλοκ σε bitcoins.(Πηγή: Το βιβλίο μας: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 4).

Κάθε συναλλαγή απαιτεί τέλη συναλλαγής. Οι εξορύκτες ενθαρρύνονται οικονομικά να προσθέσουν τις υψηλότερες συναλλαγές τέλους στο μπλοκ τους, επειδή εισπράττουν αυτά τα τέλη όταν πρώτα βρουν μια έγκυρη κατακερματισμένη τιμή για το μπλοκ. Εκτός από τα τέλη συναλλαγής, οι εξορύκτες λαμβάνουν επίσης μια ανταμοιβή μπλοκ, η οποία μειώνει κατά το ήμισυ κάθε 210.000 μπλοκ.

Το σύστημα είναι ασφαλές εφόσον οι έντιμοι κόμβοι ελέγχουν συλλογικά περισσότερη υπολογιστική ισχύ από οποιαδήποτε συνεργαζόμενη ομάδα επιτιθέμενων κόμβων.

2.1.8 Αποκέντρωση

Οι όροι «αποκεντρωμένο δίκτυο και κατανεμημένο δίκτυο» χρησιμοποιούνται συχνά εναλλακτικά.[3] Η αποκέντρωση προβλέπει ένα άλλο σημαντικό χαρακτηριστικό ασφαλείας όσον αφορά την καταστροφή κάθε μεμονωμένου κόμβου που φιλοξενεί τα δεδομένα ως

[3] Επειδή το blockchain είναι μια βάση δεδομένων που διανέμεται σε διαφορετικούς διακομιστές, αυτή η τεχνολογία αναφέρεται επίσης ως ***τεχνολογία κατανεμημένου μητρώου*** (DLT). Το blockchain μπορεί να θεωρηθεί DLT, αλλά ένα DLT δεν χρειάζεται πάντα να είναι blockchain.

SPOF. Οι συνήθεις λύσεις που έχουν οι επιχειρήσεις είναι να διατηρούν πολλαπλά αντίγραφα για ολόκληρο το σύστημα/εφαρμογή τους που φιλοξενείται σε κέντρα δεδομένων σε πολλαπλές τοποθεσίες. Πρόκειται για μια τεράστια επικάλυψη κόστους που απαιτείται για την ασφάλεια των δεδομένων που επιτυγχάνει το Bitcoin μόνο από τον εγγενή αρχιτεκτονικό σχεδιασμό του.

- **Ένα αποκεντρωμένο Blockchain απαιτεί επιβεβαιώσεις νέων δεδομένων από άλλους κόμβους**

Με έναν κεντρικό διακομιστή, είναι σχετικά εύκολο να συμπεριληφθούν νέες προσθήκες δεδομένων στη βάση δεδομένων. Τα νέα δεδομένα πρέπει να προστεθούν μόνο από ένα μόνο μέρος. Αυτό είναι διαφορετικό για ένα αποκεντρωμένο δίκτυο. Εάν τα νέα δεδομένα προστεθούν σε ένα blockchain από έναν εξορύκτη, αυτά τα δεδομένα πρέπει να επαληθεύονται από άλλους πλήρεις κόμβους και στη συνέχεια να περιλαμβάνονται επίσης στα blockchains που φιλοξενούνται από άλλους κόμβους.

- **Ένα αποκεντρωμένο Blockchain απαιτεί συναίνεση**

Τι γίνεται με τις νέες ενημερώσεις του πρωτοκόλλου δικτύου; Ένα αποκεντρωμένο Blockchain απαιτεί συναίνεση για ενημερώσεις και συμφωνίες σχετικά με τη σωστή κατάσταση της Blockchain.

- **Ένα αποκεντρωμένο Blockchain είναι δύσκολο να χακαριστεί**

Δεδομένου ότι το blockchain διατηρείται σε διαφορετικούς κόμβους που μπορεί να κατοικούν σε διαφορετικά μέρη του κόσμου, είναι δύσκολο να αναλάβει τον έλεγχο του δικτύου. Για να ελέγξετε το δίκτυο, θα πρέπει να είστε σε θέση να δημιουργήσετε τη μεγαλύτερη αλυσίδα, η οποία μπορεί να επιτευχθεί μόνο αν κατέχετε την μεγαλύτερη υπολογιστική ισχύ (majority computation power). Σας επιτρέπει να βρείτε έγκυρα μπλοκ hashes γρηγορότερα από το υπόλοιπο δίκτυο σε συνδυασμό. Μια επίθεση που βασίζεται στην υπολογιστική ισχύ ονομάζεται επίσης ***επίθεση 51 %***.[4] Μια επίθεση 51 % σας επιτρέπει να αποφεύγετε τον περιορισμό της ***διπλής δαπάνης***.

- **Ένα αποκεντρωμένο Blockchain περιπλέκει τη λογοκρισία και την απάτη**

Το Blockchain, αν διανεμηθεί ευρέως και απομακρυσμένα, είναι πιο αλλοίωση απόδειξη. Ωστόσο, είναι δυνατή η αλλαγή ή η διαγραφή δεδομένων εάν υπάρχει συναίνεση εντός του δικτύου για να γίνει αυτό. Αν υποθέσουμε ότι το δίκτυο είναι καλά αποκεντρωμένο, μπορούμε να πούμε ότι η λογοκρισία του Blockchain είναι δύσκολο να επιτευχθεί.

2.1.9 Προστασία προσωπικών δεδομένων

Ο Satoshi Nakamoto δήλωσε στην πρώτη του ανακοίνωση για το δίκτυο Bitcoin ότι το bitcoin είναι ανώνυμο, αλλά αυτό δεν είναι αλήθεια. Το Bitcoin είναι «ψευδώνυμο». Αυτό σημαίνει ότι είναι ιδιωτικό, αλλά όχι ανώνυμο. Δημοσιεύει όλες τις συναλλαγές σε ένα δημόσιο blockchain σε σαφές κείμενο για οποιονδήποτε να ελέγχει και να τρέχει πράγματα όπως

[4] Ενώ η επίθεση του 51 % είναι η πιο γνωστή, πολλές άλλες επιθέσεις είναι επίσης πιθανές. Τακτικές επιθέσεις που συμβαίνουν σε κεντρικά δίκτυα, όπως διαφθορά των βασικών προγραμματιστών, σφάλματα σε λανθασμένα γραμμένο κώδικα ή κλοπή κλειδιών που δίνουν πρόσβαση σε διακομιστές συμβαίνουν επίσης με blockchains.

αλγόριθμοι μηχανικής μάθησης για την εκτέλεση αναλύσεων ανίχνευσης σε αυτό. Ωστόσο, είναι ιδιωτικό, πράγμα που σημαίνει ότι εκτός εάν υπάρχει ανάγκη να γνωρίζουμε (όπως μια δικαστική απόφαση) και αν ο χρήστης το χρησιμοποιεί με σκοπό να διατηρήσει την οικονομική του συναλλαγή ιδιωτική (με τη μη επαναχρησιμοποίηση των δημόσιων διευθύνσεών του πολλές φορές) καθώς η ιδιωτικότητα είναι ενσωματωμένη.

Η ιδιωτικότητα εξακολουθεί να διατηρείται με τη διατήρηση των δημόσιων κλειδιών και της αντίστοιχης διεύθυνσης ενός «ηλεκτρονικού πορτοφολιού». Το δημόσιο μητρώο επιτρέπει σε όλους να δουν ποια διεύθυνση έχει κάνει ποια συναλλαγή, αλλά εφόσον οι διευθύνσεις σας είναι άγνωστες και δεν συνδέονται με τα προσωπικά σας στοιχεία, μπορείτε να συναλλάσσεστε μάλλον «ανώνυμα».

Στη Λευκή Βίβλο του Bitcoin, ο Satoshi ανέφερε επίσης ότι ως πρόσθετο τείχος προστασίας για τη διατήρηση της ιδιωτικής ζωής, θα πρέπει να χρησιμοποιείται ένα νέο ζεύγος κλειδιών για κάθε συναλλαγή ώστε να μην συνδέονται με έναν κοινό ιδιοκτήτη. Ορισμένες συνδέσεις εξακολουθούν να είναι αναπόφευκτες με συναλλαγές πολλαπλών εισροών, οι οποίες αποκαλύπτουν αναγκαστικά ότι οι εισροές τους ανήκουν στον ίδιο ιδιοκτήτη. Ο κίνδυνος είναι ότι αν αποκαλυφθεί ο ιδιοκτήτης ενός κλειδιού, η σύνδεση θα μπορούσε να αποκαλύψει άλλες συναλλαγές που ανήκαν στον ίδιο ιδιοκτήτη.

Η επικρατούσα άποψη ότι το Bitcoin είναι ένα νόμισμα που είναι ανώνυμο είναι, ως εκ τούτου, εσφαλμένη. Αντίθετα, λειτουργεί ως ένα διαφανές ανοιχτό μητρώο και αυτό δημιούργησε ένα χώρο για ένα εντελώς νέο σύνολο κρυπτονομισμάτων με επίκεντρο την ανωνυμία όπως το monero, το zcash και μερικά άλλα. Πολλές χώρες εργάζονται ήδη ενεργά για τη θεσμοθέτηση σχετικής νομοθεσίας.

Το παραδοσιακό τραπεζικό μοντέλο επιτυγχάνει ένα επίπεδο ιδιωτικότητας περιορίζοντας την πρόσβαση στις πληροφορίες στα εμπλεκόμενα μέρη και στον αξιόπιστο τρίτο. Η ανάγκη να δημοσιοποιηθούν όλες οι συναλλαγές αποκλείει αυτή τη μέθοδο, αλλά η προστασία της ιδιωτικής ζωής μπορεί να διατηρηθεί διακόπτοντας τη ροή των πληροφοριών μιας άλλης διεργασίας: κρατώντας τα δημόσια κλειδιά ανώνυμα. Το κοινό μπορεί να δει ότι κάποιος στέλνει ένα ποσό σε κάποιον άλλο, αλλά χωρίς πληροφορίες που συνδέουν τη συναλλαγή με κανέναν. Αυτό είναι παρόμοιο με το επίπεδο των πληροφοριών που απελευθερώνονται από τα χρηματιστήρια, όπου ο χρόνος και το μέγεθος των μεμονωμένων συναλλαγών, η «ταινία», δημοσιοποιούνται, αλλά χωρίς να γνωρίζουν ποιοι ήταν τα μέρη.

2.1.10 ΠΕΡΙΛΗΨΗ

Αν και υπάρχουν πολλοί διαφορετικοί τύποι Blockchains και με διαφορετικά επίπεδα αποκέντρωσης, μπορούμε να συμπεράνουμε ότι γενικά ένα αποκεντρωμένο δίκτυο Blockchain έχει τα ακόλουθα χαρακτηριστικά:

1. Δεν υπάρχει μοναδικό σημείο αποτυχίας (SPOF).
2. Τα νέα δεδομένα πρέπει να επιβεβαιώνονται από άλλους κόμβους.
3. Απαιτείται κάποια μορφή συναίνεσης για να γίνουν ενημερώσεις και να συμφωνηθεί η σωστή κατάσταση του blockchain.
4. Είναι δύσκολο να δεχθεί κακόβουλη επίθεση.
5. Καθιστά πιο δύσκολη τη λογοκρισία ή την αλλαγή των δεδομένων στο blockchain.

6. Πρόκειται για ένα δίκτυο ομότιμων κόμων (peer-to-peer), το οποίο δεν απαιτεί εμπιστοσύνη σε ένα κεντρικό κόμβο.

Τελικές παρατηρήσεις

- Τα blockchain διαφέρουν από τις παραδοσιακές βάσεις δεδομένων.
- Ο λόγος που ο Napster απέτυχε είναι επειδή είχε ένα SPOF. Ένα Blockchain, από την άλλη πλευρά, δεν έχει SPOF και ως εκ τούτου είναι πιο δύσκολο να απενεργοποιηθεί.
- Το Blockchain είναι ένα peer-to-peer δίκτυο.

Εικονίδια που χρησιμοποιούνται
Εικονίδιο υπολογιστή κατασκευασμένος από Prettycons από το www.flaticon.com

Εικονίδιο ορυχείο που γίνεται από τη λουρίδα από το www.flaticon.com

2.2 Blockchain 2.0 και έξυπνα συμβόλαια

«Θέλουμε μια ολόκληρη σειρά εταιρειών: ψηφιακός τίτλος, περιουσιακά στοιχεία ψηφιακών μέσων, ψηφιακές μετοχές και ομόλογα, ψηφιακή πληθοχρηματοδότηση, ψηφιακή ασφάλιση. Εάν έχετε ηλεκτρονική εμπιστοσύνη όπως παρέχει το Blockchain, μπορείτε να επανεφεύρετε το πεδίο μετά το πεδίο μετά το πεδίο.» **Marc Andreessen (2014)**

2.2.1 Εισαγωγή

Μαθησιακοί στόχοι

- Τι είναι το Blockchain 1.0 και γιατί υπάρχει ανάγκη για Blockchain 2.0.
- Το Ethereum είναι ένα παράδειγμα του Blockchain 2.0.
- Ποια είναι τα έξυπνα συμβόλαια.
- Ποιες είναι οι αποκεντρωμένες εφαρμογές (dApps).
- Ποιες είναι οι αποκεντρωμένες αυτόνομες οργανώσεις (DAO).

Εισαγωγή

Στο προηγούμενο κεφάλαιο συζητήθηκαν κυρίως οι βασικές αρχές blockchain μέσω του Bitcoin. Σε αυτό το κεφάλαιο, στρέφουμε την προσοχή μας σε μια νεότερη γενιά blockchain που προορίζονται ειδικά για να δημιουργήσουν μια πληθώρα άλλων τύπων αποκεντρωμένων εφαρμογών ή dApps. Ένα συγκεκριμένο blockchain στο οποίο εστιάζουμε είναι το Ethereum, το οποίο επίσης διαφημίζεται ως παγκόσμιος αποκεντρωμένος υπολογιστής.

2.2.2 Blockchain 1.0 και 2.0

Η πρώτη γενιά blockchains είναι επίσης γνωστή ως ***Blockchain 1.0***, η οποία επικεντρώνεται κυρίως στο ψηφιακό χρήμα. Ο Vitalik Buterin είχε την ιδέα να αναπτύξει ένα νέο Blockchain, το Ethereum, στο οποίο θα μπορούσε κανείς να δημιουργήσει νέα νομίσματα, συμβόλαια με όρους και απαιτήσεις και ακόμη και ολοκληρωμένες ***αποκεντρωμένες εφαρμογές*** (dApps). Τα Blockchains με τέτοιες δυνατότητες είναι επίσης γνωστά ως Blockchain δεύτερης γενιάς: ***Blockchain 2.0***.[5]

2.2.3 Ethereum

Το Ethereum εισήχθη για πρώτη φορά από τον Vitalik Buterin στο «Ethereum White Paper: μια επόμενη γενιά Έξυπνων Συμβολαίων & αποκεντρωμένη πλατφόρμα εφαρμογών» (2013). Στη Λευκή Βίβλο, ο Buterin εξηγεί ότι το Bitcoin μπορεί να περιγραφεί ως ένα «σύστημα first-to-file» στο οποίο η σειρά των συναλλαγών είναι κρίσιμη. Τεχνικά, το Bitcoin μπορεί να θεωρηθεί ως ένα απλό σύστημα μετάβασης «καταστάσεων» όπου (α) η «κατάσταση» αποτελείται από το καθεστώς ιδιοκτησίας όλων των υφιστάμενων bitcoins και (β) η «λειτουργία μετάβασης κατάστασης» που παίρνει μια κατάσταση και μια συναλλαγή και παράγει μια νέα κατάσταση που είναι το αποτέλεσμα. Ωστόσο, είναι δύσκολο να εκτελεστούν οι συμβάσεις που αφορούν τη συναλλαγή, οι οποίες μπορούν να αποτυπωθούν σε πολλές καταστάσεις. Για παράδειγμα, είναι δύσκολο να ξεπεραστεί με λογική το γεγονός ότι ο Μπομπ μπορεί να στείλει τα χρήματά του στην Αλίκη, αλλά ότι η Αλίκη μπορεί να το διεκδικήσει μόνο αφού έχει παράσχει κάτι σε αντάλλαγμα. (Buterin, 2013, σ. 12)

Στόχος της Ethereum είναι να παρέχει στους προγραμματιστές τη δυνατότητα να αναπτύσσουν εφαρμογές με βάση αυθαίρετους όρους και προϋποθέσεις. Η γλώσσα προγραμματισμού που αναπτύχθηκε ειδικά για το Ethereum ονομάζεται ***Solidity***.

2.2.4 Συναλλαγές Ethereum και αιθέρας

Το υποκείμενο κρυπτονόμισμα του blockchain Ethereum είναι ο *αιθέρας* (ETH). Η πραγματοποίηση συναλλαγής στο δίκτυο Ethereum απαιτεί ***αέριο***. Το *αέριο* εκφράζεται με το κρυπτονόμισμα *Αιθέρας*. Το *αέριο* στο δίκτυο Ethereum είναι βασικά το ίδιο με το κόστος συναλλαγής. Αυτό υπολογίζεται χρησιμοποιώντας το τυποποιημένο κόστος ανά μονάδα υπολογιστικής ισχύος επί τον αριθμό των μονάδων. Μπορείτε να καθορίσετε μια συγκεκριμένη ποσότητα *αερίου* ή το κόστος συναλλαγής για κάθε συναλλαγή που εκτελείτε. Ο χρήστης πρέπει να πληρώσει την κατάλληλη ποσότητα *αερίου* για τη συναλλαγή. Εάν πληρωθεί πολύ λίγο *αέριο*, οι εξορύκτες μπορεί να μην συμπεριλάβουν τη συναλλαγή στο μπλοκ και, ως εκ τούτου, η συναλλαγή αυτή δεν θα εκτελεστεί. Εκτός από την ανταμοιβή μπλοκ, ο εξορύκτης λαμβάνει επίσης όλα τα τέλη *αερίου* που συμπεριλήφθηκαν στις συναλλαγές στο μπλοκ.

[5] Αυτά είναι blockchains που έχουν λύσει ένα σύμπλεγμα ζητημάτων που το blockchain 2.0 εξακολουθεί να αντιμετωπίζει. Παραδείγματα τέτοιων ζητημάτων είναι η επεκτασιμότητα, η διαλειτουργικότητα, η ιδιωτικότητα, η βιωσιμότητα και η διακυβέρνηση (Ackermann & Meier, σ. 1). EOS, Cosmos, Cardano, Avalanche, Terra είναι παραδείγματα blockchain που θα μπορούσαν να θεωρηθούν blockchain 3.0.

Ο κρυπτο-οικονομικός λόγος που το *αέριο* έχει εισαχθεί στο δίκτυο Ethereum είναι ότι δίνει προτεραιότητα σε σημαντικές συναλλαγές. Ένα μπλοκ έχει μόνο χώρο για περιορισμένο αριθμό συναλλαγών. Το σύστημα *αερίου* εξασφαλίζει ότι δεν σπαταλάται ενέργεια σε συναλλαγές spam ή χαμηλής αξίας.

2.2.5 Έξυπνα συμβόλαια

Ένα έξυπνο συμβόλαιο αποτελεί μια αποκεντρωμένη αυτοματοποίηση και μπορεί να οριστεί ως σύμβαση με ορισμένους όρους και προϋποθέσεις που καθορίζονται από κώδικα. Η σύμβαση είναι αυτο-εκτελέσιμη, καθώς εκτελεί κατάλληλες αντίστοιχες ενέργειες όταν πληρούνται οι όροι και οι προϋποθέσεις. Για παράδειγμα, ένα έξυπνο συμβόλαιο θα μπορούσε να είναι μια σύμβαση εργασίας, όπου η Αλίκη θέλει να πληρώσει τον Μπομπ 500 EUR για την ανάπτυξη μιας ιστοσελίδας. Η σύμβαση θα μπορούσε να λειτουργήσει ως εξής:

1. Η Αλίκη βάζει 500 EUR στο συμβόλαιο και τα χρήματα είναι κλειδωμένα.
2. Όταν ο Μπομπ έχει αναπτύξει την ιστοσελίδα, ο Μπομπ στέλνει ένα μήνυμα στο συμβόλαιο για να απελευθερώσει τα χρήματα σε αυτόν.
3. Το ταμείο αποδεσμεύεται όταν συμφωνεί η Αλίκη.
4. Αν ο Μπομπ αποφασίσει να μην ολοκληρώσει την ιστοσελίδα, ο Μπομπ μπορεί να ακυρώσει τη δουλειά του στέλνοντας ένα μήνυμα στο συμβόλαιο, και το οποίο στην συνέχεια επιστρέφει αυτόματα τα χρήματα στην Αλίκη.
5. Αν ο Μπομπ ισχυρίζεται ότι έχει ολοκληρώσει την ιστοσελίδα, αλλά η Αλίκη διαφωνεί, ένας δικαστής θα μπορούσε να κληθεί μετά από μια περίοδο αναμονής 7 ημερών για να εκφράσει μια ετυμηγορία υπέρ της Αλίκης ή του Μπομπ. (Buterin, 2014)

Πλεονεκτήματα των έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια προσφέρουν πολλά πλεονεκτήματα. Το ChainTrade (2017) έχει καταγράψει τα ακόλουθα έντεκα:

1. *Ακρίβεια:* Όλοι οι όροι και οι προϋποθέσεις πρέπει να καταγράφονται λεπτομερώς σε ένα έξυπνο συμβόλαιο. Εάν παραλειφθούν ορισμένες συνθήκες, αυτό μπορεί να οδηγήσει σε ανεπιθύμητη συμπεριφορά του έξυπνου συμβολαίου.
2. *Διαφάνεια:* όλοι οι όροι και οι προϋποθέσεις είναι πλήρως ορατοί και προσβάσιμοι σε όλα τα εμπλεκόμενα μέρη. Μετά την ολοκλήρωση της σύμβασης, δεν μπορείτε πλέον να την αμφισβητήσετε.
3. *Σαφής επικοινωνία:* η ανάγκη για σχολαστικά καθορισμένες έξυπνες συμβάσεις διασφαλίζει ότι η επικοινωνία στη σύμβαση είναι σαφώς καθορισμένη, ώστε να μην υπάρχει περιθώριο για κακή επικοινωνία και παρερμηνεία.
4. *Ταχύτητα: τα* έξυπνα συμβόλαια μπορούν να αυτοματοποιήσουν και να επιταχύνουν σημαντικά τις παραδοσιακές επιχειρηματικές διαδικασίες. Δεν χρειάζεται να υποβληθούν αιτήσεις για έγκριση και δεν απαιτείται επεξεργασία ή έγκριση εγγράφων από ιδιώτες.
5. *Ασφάλεια: τα* έξυπνα συμβόλαια εκτελούνται σε πλατφόρμες blockchain και χρησιμοποιούν κρυπτογράφηση δεδομένων.
6. *Αποτελεσματικότητα:* Λόγω της ακρίβειας και της ταχύτητας, τα έξυπνα συμβόλαια εκτελούν τις επιχειρηματικές διαδικασίες πιο αποτελεσματικά ή ακόμα μπορούν να τις παραλείψουν.
7. *Χωρίς χαρτί:* δεν απαιτούνται έγγραφα για την εκτέλεση έξυπνων συμβολαίων.
8. *Αποθήκευση και δημιουργία αντιγράφων ασφαλείας: τα* έξυπνα συμβόλαια και τα στοιχεία τους αποθηκεύονται μόνιμα στο blockchain. Ως αποτέλεσμα, δεν μπορούν να χαθούν και είναι εύκολο να βρεθούν.
9. *Εξοικονόμηση κόστους: τα έξυπνα συμβόλαια* μπορούν να εξοικονομήσουν κόστος, επειδή υπάρχει λιγότερη ανάγκη για μεσάζοντες όπως δικηγόροι, μάρτυρες και τράπεζες να ερμηνεύσουν και να επιβάλουν τις συμβάσεις.
10. *Εμπιστοσύνη: τα* εμπλεκόμενα μέρη μπορούν να εμπιστεύονται ότι τα έξυπνα συμβόλαια — εάν έχουν συσταθεί σωστά — θα εκτελεστούν δίκαια, χωρίς τη δυνατότητα χειραγώγησης των δεδομένων και προκαταλήψεων.
11. *Εγγυημένα αποτελέσματα:* με τη χρήση συμβολαίων αυτοεκτέλεσης, τα συμβαλλόμενα μέρη θα συμμορφώνονται με τους κανόνες του έξυπνου συμβολαίου και θα υπάρχουν λιγότερες νομικές διαφορές.

2.2.6 Αποκεντρωμένες εφαρμογές

Ορίζουμε μια ***αποκεντρωμένη εφαρμογή*** (dApp) ως μια εφαρμογή που χρησιμοποιεί την αποκεντρωμένη αποθήκευση δεδομένων μιας τεχνολογίας Blockchain. Η εφαρμογή δεν εκτελείται μέσω κεντρικού διακομιστή, αλλά μέσω αποκεντρωμένου δικτύου κόμβων. Ακριβώς όπως μια κανονική εφαρμογή, έχει συχνά ένα μπροστινό άκρο και ένα περιβάλλον εργασίας χρήστη. Η διεπαφή προσφέρει στον χρήστη μια ευκολότερη αλληλεπίδραση με έξυπνα συμβόλαια και της τεχνολογίας Blockchain. Με την αποθήκευση και την εκτέλεση των έξυπνων συμβολαίων που αποτελούν τον βασικό κώδικα ενός dApp με αποκεντρωμένο

τρόπο, δεν υπάρχει μοναδιαίο σημείο αποτυχίας. Η λειτουργία της εφαρμογής και τα δεδομένα της αίτησης δεν μπορούν απλώς να λογοκριθούν ή να αφαιρεθούν.

2.2.7 Αποκεντρωμένη αυτόνομη οργάνωση (DAO)

Οι αποκεντρωμένοι αυτόνομοι οργανισμοί (DAO) μπορούν να οριστούν ως ένας μη ιεραρχικός οργανισμός που εκτελεί και καταχωρίζει εργασίες ρουτίνας σε ένα έργο Blockchain. Οι κανόνες που τηρεί η DAO καταγράφονται επίσης στο έργο Blockchain. Επιπλέον, η DAO εξαρτάται από τις εθελοντικές συνεισφορές των εσωτερικών ενδιαφερόμενων μερών για την καθοδήγηση του οργανισμού μέσω μιας δημοκρατικής διαδικασίας διαβούλευσης. (Hsieh et al., 2018, σ. 2)

Αυτό που κάνει μια DAO θεμελιωδώς διαφορετική από μια κεντρική οργάνωση είναι ότι δεν έχει μια ανώτατη διευθυντική ομάδα ή έναν CEO. Επίσης, δεν έχει υποκαταστήματα, υπαλλήλους ή θυγατρικές. Αντ' αυτού, υπάρχει ένα DAO σε ένα αποκεντρωμένο δίκτυο χρηστών και κόμβων που συλλέγουν, επαληθεύουν και ενημερώνουν συναλλαγές σε ένα έργο Blockchain. Οι αποφάσεις σχετικά με τις αλλαγές στον κώδικα λαμβάνονται με δημοκρατικές διαδικασίες ψηφοφορίας. Είναι ένας ριζικά διαφορετικός τρόπος δημιουργίας μιας επιχειρηματικής οργάνωσης. Λόγω του αυτόνομου χαρακτήρα του — σε τελική ανάλυση, είναι ένα αυτάρκες και αυτόνομο σύστημα — το Bitcoin μπορεί να χαρακτηριστεί ως DAO, επειδή (α) διαχειρίζεται ένα σύστημα πληρωμών, (β) απασχολεί υπεργολάβους που εργάζονται ως *εξορύκτες* και (γ) πληρώνει αυτούς τους υπεργολάβους με πρόσφατα κατανεμημένα bitcoins (Vigna & Casey, 2015, σ. 229). Επιπλέον, οι *εξορύκτες* μπορούν να ψηφίσουν προτάσεις για βελτίωση του πρωτοκόλλου μέσω της υπολογιστικής τους δύναμης. Οι DAO ελέγχονται από μια συλλογική διαδικασία λήψης αποφάσεων των ενδιαφερόμενων μερών μέσω αποκεντρωμένου πρωτοκόλλου και δεν επηρεάζονται από κεντρικό διοικητικό όργανο.

Τελικές παρατηρήσεις

- Με το Blockchain 2.0, μπορεί να αναπτυχθεί πληθώρα νέων τύπων εφαρμογών.
- Μπορείτε να αναπτύξετε έξυπνες συμβάσεις στο Ethereum όπου οι όροι και οι προϋποθέσεις είναι τόσο σαφείς ώστε σε περίπτωση παραβίασης της σύμβασης, δεν απαιτείται πλέον ερμηνεία τρίτων.
- Το Bitcoin είναι ένα σύστημα first-to-file.
- Το Bitcoin είναι ο πρώτος αποκεντρωμένος αυτόνομος οργανισμός (DAO).

3 Τύποι Blockchain

Σε αυτό το κεφάλαιο θα διαιρέσουμε το Blockchain στους τύπους του από τρεις οπτικές γωνίες, το πρωτόκολλο συναίνεσης, τη διακυβέρνηση και τους τύπους συνεργασίας μεταξύ των συστημάτων Blockchain.

3.1 Τύποι Blockchain σύμφωνα με το πρωτόκολλο συναίνεσης

Τα πρωτόκολλα συναίνεσης είναι απαραίτητα για τη διασφάλιση της εμπιστοσύνης μεταξύ των διαφόρων συμμετεχόντων σε ένα κατανεμημένο δίκτυο. Πρέπει να υπάρχει εμπιστοσύνη ότι οι συμμετέχοντες δεν είναι διεφθαρμένοι και ότι τα δεδομένα που μοιράζονται μεταξύ τους δεν είναι διεφθαρμένα. Για να διασφαλιστεί αυτή η εμπιστοσύνη, οι συμμετέχοντες κόμβοι πρέπει να επαληθεύουν τα μηνύματα ή τις συναλλαγές για την ορθότητα και να εξουδετερώνουν άλλους συμμετέχοντες που είναι διεφθαρμένοι και παραπλανητικοί: η λύση στο πρόβλημα των Βυζαντινών Στρατηγών όπως συζητήθηκε στο προηγούμενο κεφάλαιο.

Ως πρωτόκολλο συναίνεσης, επομένως, αγγίζει την ουσία ενός συστήματος blockchain, χρησιμοποιείται εδώ ως ένας τρόπος για να διακρίνουμε τους τύπους blockchain.
Στο προηγούμενο κεφάλαιο εισήχθη το πρώτο πρωτόκολλο συναίνεσης, **Proof-of-Work**, χρησιμοποιώντας το Bitcoin ως παράδειγμα. Σύμφωνα με αυτό το πρωτόκολλο, ένα μπλοκ δεδομένων μπορεί να προστεθεί στο Blockchain μόνο όταν έχει βρεθεί μια έγκυρη κατακερματισμένη τιμή του μπλοκ. Καθώς οι *εξορύκτες* Bitcoin εισήλθαν σε έναν σκληρό ανταγωνισμό για να λάβουν τις ανταμοιβές της εύρεσης μιας έγκυρης κατακερματισμένης τιμής (hash) πρώτοι, η κατανάλωση ηλεκτρικής ενέργειας από το δίκτυο Bitcoin έχει οδηγήσει σε ανησυχίες σχετικά με τις αρνητικές επιπτώσεις του Blockchain στο περιβάλλον. Η προκύπτουσα αναζήτηση πιο βιώσιμων λύσεων στο πρόβλημα των «Βυζαντινών Στρατηγών» οδήγησε σε εναλλακτικά πρωτόκολλα συναίνεσης.
Μία από τις κύριες εναλλακτικές λύσεις για την απόδειξη εργασίας είναι το **Proof-of-Stake**, το οποίο τώρα έχει υλοποιηθεί σε διάφορα έργα Blockchain με το αξιοσημείωτο παράδειγμα του Ethereum το οποίο μεταφέρεται στο **Proof-of-Stake** το 2022.

Ενώ οι *εξορύκτες* στο **Proof-of-Work** επιτρέπεται να παράγουν νέα μπλοκ όταν μπορούν να βρουν ένα έγκυρο hash, ένας παραγωγός μπλοκ στο **Proof-of-Stake** επιλέγεται με βάση (α) μια τυχαία διαδικασία επιλογής και (β) ένα **«ποντάρισμα»** όπως ο αριθμός των κερμάτων που έχει. Ως εκ τούτου, δεν χρειάζεστε υπολογιστική ισχύ για να συμμετάσχετε. Το μόνο που χρειάζεται είναι ένας τυποποιημένος υπολογιστής, μια σύνδεση στο διαδίκτυο και ένα νόμισμα. Ως εκ τούτου, ο παραγωγός μπλοκ στο **Proof-of-Stake** δεν ονομάζεται *εξορύκτης*, αλλά ***πλαστογράφος***. Επειδή ο *πλαστογράφος* λαμβάνει επίσης μια ανταμοιβή κατά την παραγωγή ενός νέου μπλοκ, μπορείτε επίσης να δείτε το **Proof-of-Stake** ως μια μέθοδο όπου κερδίζετε ένα παθητικό εισόδημα στα κέρματά σας. Όσο περισσότερο ποντάρετε, τόσο μεγαλύτερη είναι η πιθανότητα να δημιουργήσετε το επόμενο μπλοκ. Εκτός από την παραγωγή μπλοκ, οι *πλαστογράφοι* επικυρώνουν επίσης συναλλαγές, συμβάλλοντας στην ασφάλεια του δικτύου.

Δίπλα στην ενεργειακή απόδοση, τα πλεονεκτήματα του Proof-of-Stake of Proof-of-Work είναι ότι η ευκολία της παρακολούθησης επιτρέπει την καλύτερη κατανομή του Blockchain και ότι η διεξαγωγή μιας επίθεσης 51 % είναι λιγότερο ελκυστική.

Υπάρχουν διαφορετικές παραλλαγές στο **Proof-of-Stake** που έχουν τις δικές τους μοναδικές ιδιότητες. Πρώτον, στην **κατ' εξουσιοδότηση Proof-of-Stake** όποιος έχει κέρμα μπορεί να ψηφίσει για μάρτυρες και αντιπροσώπους. Οι μάρτυρες επικυρώνουν συναλλαγές και προσκομίζουν νέα μπλοκ για τα οποία λαμβάνουν ανταμοιβή. Οι αντιπρόσωποι επιβλέπουν τη δομή διακυβέρνησης του πρωτοκόλλου blockchain. Ως αποτέλεσμα, η **Proof-of-Stake** μπορεί να χειριστεί περισσότερες συναλλαγές ανά δευτερόλεπτο από τα blockchains που είναι πιο αποκεντρωμένα.
Δεύτερον, σε ένα **μισθωμένο Proof-of-Stake** ο καθένας μπορεί να μισθώσει τα κέρματά του σε κόμβους που διακυβεύονται αυξάνοντας έτσι την πιθανότητα για τους κόμβους στοιχημάτων να παράγουν ένα μπλοκ. Οι κόμβοι πονταρίσματος κατανέμουν την ανταμοιβή τους αναλογικά μεταξύ τους και των μισθωτών. Ως αποτέλεσμα, αυτό το πρωτόκολλο ενθαρρύνει τους ανθρώπους να συμμετέχουν στη διαδικασία παρακολούθησης.

Τρίτον, με τους χρήστες **της Proof-of-Stake Velocity** ανταμείβονται (α) για τον αριθμό των κερμάτων που κατέχουν και (β) πόσο ενεργά χρησιμοποιούν τα κέρματά τους. Ως εκ τούτου, η κοινότητα ενθαρρύνεται όχι μόνο να κρατήσει τα κέρματα, αλλά και να τα χρησιμοποιήσει για συναλλαγές.

Τέταρτον, με την **Proof-of-Authority**, **απόδειξη της αρχής**, οι παραγωγοί μπλοκ (κόμβοι αρχών) επικυρώνονται και εγκρίνονται με βάση την ταυτότητα και τη φήμη τους. Με τη σύνδεση της φήμης με την ταυτότητα, οι κόμβοι εξουσίας διεγείρονται επιπλέον για να δείξουν καλή συμπεριφορά και να μην συμπεριλάβουν κακόβουλες συναλλαγές στο blockchain. Αν το κάνουν, θα προκαλέσουν ζημιά στη φήμη τους. Το **Proof-of-Authority** είναι ένα παράδειγμα δημιουργίας μιας παραλλαγής του **Proof-of-Stake**, όπου η πιθανότητα δημιουργίας ενός νέου μπλοκ δεν εξαρτάται εξ ολοκλήρου από τον αριθμό των κερμάτων που ποντάρετε.
Λάβετε υπόψη ότι είναι αμφίβολο αν το **Proof-of-Authority** εμπίπτει στο **Proof-of-Stake**. Μερικές φορές θεωρείται ως μια μορφή **κατ' εξουσιοδότηση Proof-of-Stake** και πιο συχνά χρησιμοποιείται σε κλειστά, αδειοδοτημένα blockchains.

Ένα πλεονέκτημα της τυποποίησης του blockchain με τη χρήση πρωτοκόλλων συναίνεσης είναι ότι βοηθά να εξηγηθούν οι διαφορές στην **επεκτασιμότητα των blockchains**. Αυτό ως επεκτασιμότητα γενικά εξαρτάται από την επίδραση των πρωτοκόλλων συναίνεσης στον χρόνο δημιουργία των μπλοκ, το μέγεθος των μπλοκ, το επίπεδο διανομής ή αποκέντρωσης του blockchain και τον τρόπο με τον οποίο παράγονται τα μπλοκ, οι συναλλαγές αποστέλλονται στο blockchain και επαληθεύονται οι συναλλαγές. Για να βελτιωθεί αυτή η κλιμάκωση, δοκιμάζονται διάφορες λύσεις, όπως η λήψη συναλλαγών εκτός αλυσίδας. Γνωστά παραδείγματα είναι το πλάσμα (τόσο οι λεγόμενες «λύσεις επιπέδου 2») όσο και ο τεμαχισμός.

3.2 Blockchain διακυβέρνηση και ποιος μπορεί να συμμετάσχει με ποιο ρόλο

Ένα Blockchain, όπως κάθε συνεργασία, πρέπει να διοικείται και να ελέγχεται. Η προκύπτουσα δομή διακυβέρνησης Blockchain προσφέρει έναν δεύτερο τρόπο για να διακρίνουμε τους τύπους Blockchain που θα συζητηθούν εδώ.

Αξιοσημείωτα στοιχεία διακυβέρνησης είναι τα εξής:

1. **Δικαιώματα** υποβολής, εκτέλεσης και παρακολούθησης προτάσεων **απόφασης** από ομάδα ή προς όλους.
2. **Λογοδοσία** και το δικαίωμα παρακολούθησης των αποφάσεων και των συμπεριφορών και να λογοδοτούν για τις ευθύνες σας.
3. **Κίνητρα** και ενθάρρυνση των συμμετεχόντων να διατηρήσουν το Blockchain.

Ο τρόπος με τον οποίο ερμηνεύονται αυτά τα στοιχεία εξαρτάται από τους στόχους που επιδιώκει η εταιρική σχέση και, ως εκ τούτου, από το είδος της διακυβέρνησης που χρειάζεται.

Μία από τις ανάγκες διακυβέρνησης μπορεί να είναι ότι μια κεντρική ομάδα ανθρώπων ασκεί έλεγχο και υπαγορεύει όρους (**κεντρική** νοοτροπία **ελέγχου)**, σε σχέση με τις ανάγκες μιας μεγαλύτερης ομάδας να συνεργαστεί σε ισότιμη βάση χωρίς ιεραρχία ή κεντρικό έλεγχο (**αποκεντρωμένη** νοοτροπία ελέγχου).

Ο τύπος ελέγχου που ασκείται χρησιμοποιείται για να αποφασιστεί ποιος θα λάβει άδεια συμμετοχής σε ένα Blockchain ή όχι. Εάν οι κεντρικές αρχές χορηγήσουν την πρόσβαση, η Blockchain είναι ο **ιδιωτικός** τύπος Blockchain. Εάν η πρόσβαση είναι οργανωμένη για όλους, το Blockchain ονομάζεται **δημόσιο** Blockchain. Οι δημόσιοι και ιδιωτικοί τύποι Blockchain βρίσκονται συνδυασμένοι στον τύπο της **κοινοπραξίας** Blockchain, μια ενδιάμεση μορφή που είναι πιο συγκεντρωτική από μια δημόσια Blockchain και πιο αποκεντρωμένη από μια ιδιωτική Blockchain.

Σε μια κοινοπραξία, πολλοί οργανισμοί συνεργάζονται για να δημιουργήσουν ένα Blockchain και η συναίνεση διοικείται από μια επιλογή κόμβων. Η κοινοπραξία αποφασίζει για ολόκληρο το δίκτυο ποιος μπορεί να συμμετάσχει με ποιο ρόλο, ποιες συναλλαγές μπορούν να προβληθούν ανοιχτά ή να προστατευθούν από άλλους συμμετέχοντες και πώς θα πρέπει να δομηθεί η διακυβέρνηση.

Χρησιμοποιείτε κυρίως ένα δημόσιο Blockchain, όπου όλοι αντιμετωπίζονται ισότιμα, αν θέλετε μια ομάδα ομοϊδεατών ανθρώπων να συνεργαστούν. Η συνεργασία διασφαλίζεται εδώ από τον μηχανισμό συναίνεσης που λειτουργεί ως «μηχανή εμπιστοσύνης». Η «πρόσβαση σε όλους» οδηγεί σε μεγαλύτερο αριθμό κόμβων που χτίζουν εμπιστοσύνη στο σύστημα Blockchain. Ένα δημόσιο Blockchain δείχνει μικρότερο βαθμό εμπιστοσύνης στις αρχές που κυβερνούν το Blockchain στο όνομα των άλλων. Αυτή η στάση εμπιστοσύνης και εμπιστοσύνης ευνοεί την απόφαση για πρωτόκολλα συναίνεσης με πιο αποκεντρωμένο χαρακτήρα, την εμπιστοσύνη στον ανοικτό κώδικα της αλυσίδας Blockchain, καθώς και την επιθυμία για πλήρη διαφάνεια στη λήψη αποφάσεων. Επομένως, αυτή η στάση οδηγεί σε μεγαλύτερη εμπιστοσύνη στο να συμμετέχουν και να συμμετέχουν ξένοι στην εταιρική σχέση. Μετά από όλα, η εμπιστοσύνη βρίσκεται στο σύστημα και όχι στο χρήστη.

Σε γενικές γραμμές, μια εταιρεία που τείνει προς ένα ιδιωτικό Blockchain, θα θέλει να ξέρει ποιος είναι στο σύστημα Blockchain. Σκεφτείτε ένα ενδοδίκτυο στο οποίο ελέγχετε τους κόμβους, τα δεδομένα και τον πηγαίο κώδικα. Γνωρίζετε ότι όλοι και όλες οι συναλλαγές μπορούν να προβληθούν εάν αυτό είναι απαραίτητο, αλλά προστατεύετε επίσης τους ανθρώπους από την επαλήθευση ή την παρακολούθηση ορισμένων συναλλαγών. Αυτό είναι χρήσιμο όταν τα δεδομένα είναι ευαίσθητα στην εταιρεία. Σε ένα δημόσιο σύστημα είναι επίσης δυνατό να οικοδομηθεί αυτό σε τεχνικό επίπεδο, αλλά προς το παρόν στην πράξη αυτό αποδεικνύεται πρόκληση.

Έτσι, σε ένα ιδιωτικό blockchain είναι σχετικό να γνωρίζει όλους τους ρόλους που αναθέτετε στους συμμετέχοντες στους οποίους παραχωρήσατε πρόσβαση. Ένας σημαντικός ρόλος είναι η δυνατότητα **διατήρησης του μηχανισμού συναίνεσης**. Θα πρέπει αυτή η δυνατότητα να δοθεί σε όλους τους συμμετέχοντες στο blockchain ή μόνο σε μια επιλεγμένη ομάδα;

Η απάντηση σε αυτό το ερώτημα οδηγεί σε **μη αδειοδοτημένους** και **αδειοδοτημένους** τύπους blockchain.

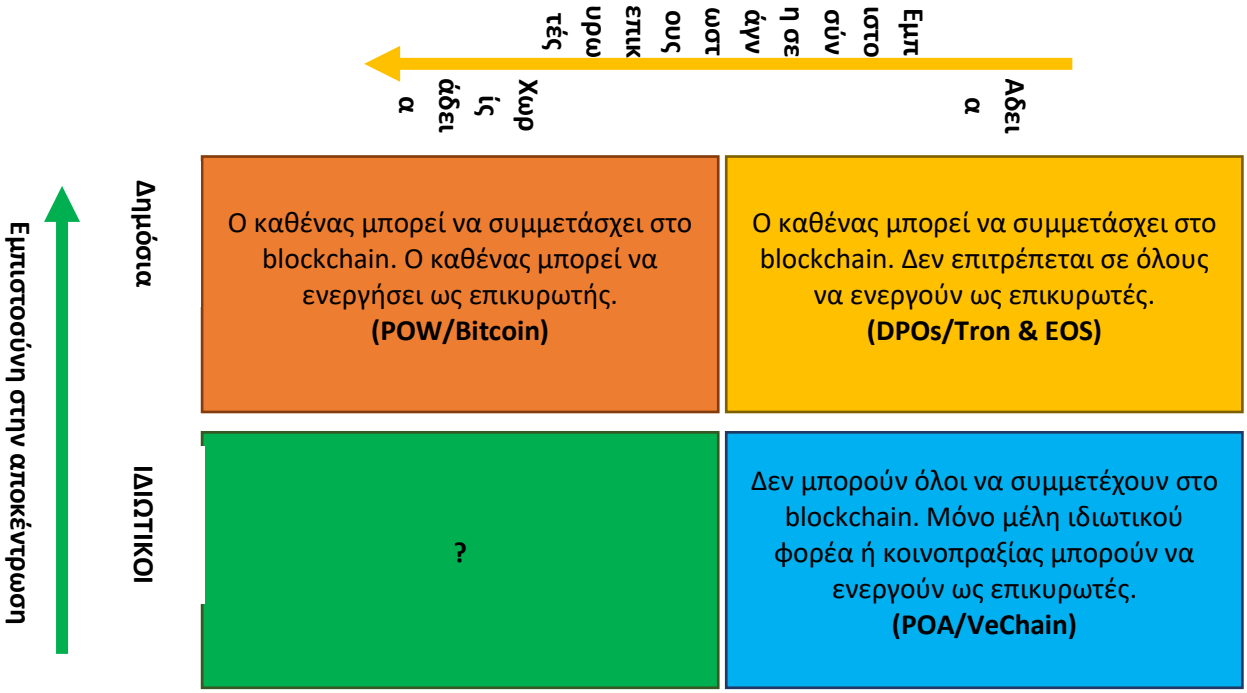
Εάν κάθε συμμετέχων στο blockchain επιτρέπεται να διατηρήσει τον μηχανισμό συναίνεσης, πρόκειται για έναν τύπο **blockchain** χωρίς άδεια. Εάν ο ρόλος για τη διατήρηση του μηχανισμού συναίνεσης προορίζεται για μια επιλεγμένη ομάδα, μιλάμε για έναν **εγκεκριμένο** τύπο blockchain.

Εκτός από τη διατήρηση της συναίνεσης, υπάρχουν ρόλοι που σας επιτρέπουν να εκτελείτε, να βλέπετε και να προσαρμόζετε τις συναλλαγές στο blockchain, να διατηρείτε τεχνικά το blockchain ή να συμμετέχετε στην ψηφοφορία επί ιδέων. Αυτοί οι ρόλοι δεν σχετίζονται με την επιλογή μεταξύ ενός συστήματος χωρίς άδεια ή ενός συστήματος με άδεια. Ωστόσο, οι ρόλοι αυτοί έχουν σημασία για τη φύση των εταιρικών σχέσεων. Αυτό έχει σημασία, διότι εάν οι αρχές δεν ενδιαφέρονται για το ποιος έχει πρόσβαση στο σύστημα και εμπιστεύεται το ίδιο το σύστημα, είναι πιθανότερο να τείνει να χορηγήσει ανωνυμία στους συμμετέχοντες. Επί του παρόντος, οι εταιρείες που χρησιμοποιούν συστήματα ελέγχου διαχείρισης θα επέλεγαν να γνωρίζουν τους ανθρώπους στους οποίους παραχωρούν πρόσβαση, καθώς επίσης θα επέλεγαν να γνωρίζουν σε ποιους ρόλους υπάρχουν και σε ποιον συμμετέχοντα μπορούν να αναθέσουν ποιον ρόλο.

Με τον διαχωρισμό των ρόλων, αυτές οι εταιρείες μπορούν να συνεχίσουν να χρησιμοποιούν την υποκείμενη οργανωτική δομή τους. Έτσι, μπορούν να επιβάλουν την εταιρική τους ταυτότητα μέσα στο blockchain τους, καθώς ελέγχουν το προφίλ των προσώπων καθώς και τους ρόλους τους. Επιπλέον, εκτός από τη μερική μεταφορά εμπιστοσύνης στο σύστημα, μπορούν να συνεχίσουν να διαχειρίζονται την οργάνωσή τους το σύστημα ελέγχου διαχείρισης, όπως συγκεκριμένη τη διαχείριση προσωπικού.

Αυτό βοηθά να εξηγηθεί γιατί μέσα σε ένα σύστημα χωρίς άδεια, τα κρυπτονομίσματα είναι διαθέσιμα για να ενθαρρύνουν τη συνεργασία.

Οι διαφορετικοί τύποι Blockchain χρησιμοποιούνται σε συνδυασμό στις σημερινές εφαρμογές Blockchains:



Σχήμα 8: Μια επισκόπηση των διαφόρων τύπων Blockchain, εκφρασμένη σε άδεια, άδεια, ιδιωτικά και δημόσια (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 9).

Η εμπιστοσύνη που υπάρχει στο σύστημα με τα δημόσια blockchains, το «ποιος γράφει δεδομένα στο blockchain», «ποιος διαβάζει δεδομένα από το blockchain» και «ποιος επιτρέπεται να διατηρήσει το blockchain» θεωρείται μικρότερης σημασίας. Αυτό με τη σειρά του οδηγεί στο γεγονός ότι τα περισσότερα δημόσια blockchains δεν έχουν άδεια. Λόγω του χαμηλού φραγμού για την ένταξή τους στο δίκτυο, τέτοια blockchains είναι τα πιο αποκεντρωμένα.

Οι συμμετέχοντες καθορίζουν τη λειτουργία του blockchain σύμφωνα με τα κίνητρα της ομάδας, όπως το άνοιγμα, η ουδετερότητα και η ελευθερία. Στο πλαίσιο του δημόσιου blockchain, ο καθένας μπορεί επίσης να συμμετάσχει στη λήψη αποφάσεων για όλα τα ζητήματα διακυβέρνησης.

Ένα **δημόσιο** blockchain δεν είναι πάντα επιθυμητό για τις εταιρείες, ειδικά σε ένα πιο ρυθμιζόμενο περιβάλλον στο οποίο αναμένεται, μεταξύ άλλων, ότι γνωρίζουν την ταυτότητα όλων των μερών που γράφουν δεδομένα στο blockchain.

Αυτός ο κεντρικός κόμβος έχει συχνά δημιουργήσει έναν αριθμό κόμβων που διαχειρίζονται τον εαυτό τους και που διατηρούν το blockchain λειτουργούντας όλα μαζί. Στην πιο ακραία περίπτωση, ο κεντρικός κόμβος αποτελεί ένα μοναδικό κόμβο στον οποίο τρέχει το blockchain. Ωστόσο, αυτό δεν προσφέρει κανένα πλεονέκτημα σε σχέση με ένα κεντρικό δίκτυο που είναι επίσης ένα SPOF.

Οι επιλογές μεταξύ των διαφόρων τύπων blockchain επηρεάζουν τον έλεγχο του οργανισμού. Όσο μεγαλύτερη εμπιστοσύνη υπάρχει στον αποκεντρωμένο χαρακτήρα του blockchain, τόσο πιο εύκολη είναι η συμμετοχή. Όσο μεγαλύτερη είναι η βεβαιότητα ότι

οι επικυρωτές μπορούν να συμμετέχουν στην οικοδόμηση συναίνεσης ως άγνωστοι, τόσο πιο διαφανές είναι το σύστημα. Μετά από όλα, όλοι μπορούν στη συνέχεια να εκτελέσουν έναν πλήρη κόμβο και να βοηθήσουν στην επικύρωση όλων των δεδομένων. Λόγω του αποκεντρωμένου χαρακτήρα, τα συστήματα αυτά έχουν συχνά πολλούς επικυρωτές και, εν μέρει λόγω αυτού, εξακολουθούν να έχουν προβλήματα επεκτασιμότητας. Επίσης, τέτοια blockchains είναι σχετικά πιο ακριβά από τις λιγότερο αποκεντρωμένες και αδειοδοτημένες παραλλαγές.

Μακροπρόθεσμα, ωστόσο, ένα δημόσιο blockchain χωρίς άδεια αναμένεται να γίνει όλο και πιο αποτελεσματικό, έτσι ώστε περισσότερα επαγγελματικά μέρη θα επιλέξουν τέτοια blockchains. Αυτά τα blockchains πρέπει στη συνέχεια να οργανωθούν με τέτοιο τρόπο ώστε οι ρόλοι που μπορούν να αναλάβουν οι συμμετέχοντες για επιχειρηματικές εφαρμογές να είναι καλά καθορισμένοι και να πληρούν τις επιχειρηματικές απαιτήσεις. Για παράδειγμα, οι εταιρείες σε δημόσια blockchain χωρίς άδεια μπορούν να ανωνυμοποιήσουν τα δεδομένα μέσω Zero-Knowledge Proofs και οι συμμετέχοντες σε επίπεδο εφαρμογής μπορούν να κληθούν να δείξουν την ταυτότητά τους.

3.3 Πλατφόρμες και κοινοπραξίες

Ένα έργο blockchain όπου συνεργάζονται διαφορετικές εταιρείες και τρίτα μέρη χωρίς έναν κεντρικό χρήστη να έχει τον έλεγχο, ονομάζεται blockchain επιχειρήσεων. Για την κατασκευή ενός τέτοιου Enterprise Blockchain, οι εταιρείες χρησιμοποιούν πλατφόρμες blockchain. Αυτές οι **πλατφόρμες** σας επιτρέπουν να γράφετε εφαρμογές χρησιμοποιώντας ορισμένες τεχνολογίες. Έχουν σχεδιαστεί διάφορες συνεργασίες γύρω από αυτές τις πλατφόρμες, οι οποίες θα αποτελέσουν και την τελευταία διαφοροποίση ως προς τα είδη blockchain.

Οι **πλατφόρμες** blockchain επιτρέπουν στην εφαρμογή σας να συνεργάζεται με άλλες εφαρμογές, για παράδειγμα, στη δική της ή κοινή γλώσσα προγραμματισμού, τα έγγραφα αποθηκεύονται ή μοιράζονται και αποκτάται πρόσβαση σε ένα συγκεκριμένο δίκτυο. Οι δύο πιο σημαντικές πλατφόρμες είναι σήμερα το Ethereum και το Hyperledger, με την Corda να είναι η τρίτη πιο σημαντική.

Κάθε πλατφόρμα έχει τα δικά της μοναδικά χαρακτηριστικά. Το Ethereum είναι, γενικά, ένα δημόσιο blockchain, το Hyperledger προσφέρει plug-and-play modules χρησιμοποιώντας διάφορες τεχνολογίες και η Corda είναι η αποκεντρωμένη τεχνολογία Ledger που είναι πιο εξειδικευμένη στις χρηματοπιστωτικές υπηρεσίες. Τα μέλη που έχουν προσχωρήσει σε μια εταιρική σχέση γύρω από μία πλατφόρμα είναι συχνά επίσης μέλη εταιρικών σχέσεων γύρω από τις άλλες πλατφόρμες. Οι ίδιες οι πλατφόρμες είναι ανοιχτού κώδικα. Η Ethereum και η Hyperledger αγωνίζονται για μεγαλύτερη ενοποίηση μεταξύ τους τα τελευταία χρόνια στον αμοιβαίο στόχο τους να εφαρμόσουν συστήματα blockchain σε εταιρείες παντού.

Όταν οι εταιρικές σχέσεις αφορούν μια μορφή συνεργασίας των blockchains στην οποία οι νεοεισερχόμενοι είναι γνωστοί και αναλαμβάνουν συγκεκριμένους ρόλους, εργάζονται σε δομές που ονομάζονται επίσης κοινοπραξίες (βλέπε παραπάνω παράγραφο 3.2), αλλά από άλλη οπτική γωνία, στη συνέχεια, αναμιγνύουν χαρακτηριστικά δημόσιων και ιδιωτικών blockchain μόνο. Τα συνεργαζόμενα μέρη μπορούν να διαφέρουν από κρατικούς φορείς, ομάδες συμφερόντων και άγνωστους, έως προμηθευτές, πελάτες και άμεσους ανταγωνιστές.

Επιπλέον, οι κοινοπραξίες εδώ βοηθούν τα μέρη να ξεπεράσουν τέσσερις βασικές προκλήσεις που αντιμετωπίζουν οι οργανισμοί κατά την εφαρμογή του blockchain. Πρώτον,

οι κοινοπραξίες ανταλλάσσουν γνώσεις και διατηρούν ενεργό επαφή με (υπερ) εθνικούς εποπτικούς φορείς. Στη συνέχεια, οι κοινοπραξίες βοηθούν στην αποσαφήνιση των νόμων και των κανονισμών, μεταξύ άλλων.

Δεύτερον, οι κοινοπραξίες βοηθούν τους οργανισμούς να κατανείμουν τους κινδύνους σε διάφορα μέρη μέσω της ανταλλαγής πόρων για την ανάπτυξη συστημάτων blockchain.

Τρίτον, μέσω της συνεργασίας, οι κοινοπραξίες παρέχουν κρίσιμη μάζα για να υιοθετήσουν ένα σταθερό σύστημα επιδόσεων.

Και τέταρτον, οι κοινοπραξίες δίνουν την ευκαιρία να δημιουργήσουν νέες αποκεντρωμένες εταιρικές σχέσεις με έμπιστα και αναξιόπιστα μέρη, χωρίς οι συμμετέχοντες οργανισμοί να χάνουν υπερβολικά μεγάλο μέρος της αυτονομίας τους. Αυτό προσφέρει στους ανταγωνιστές, για παράδειγμα, τυποποιημένες διαδικασίες για τη δημιουργία και την ανταλλαγή δεδομένων μεταξύ τους, ή τη συνεργασία με τους πελάτες και τους προμηθευτές του άλλου. Ωστόσο, καθώς τα συμμετέχοντα μέρη θα πρέπει να εμπιστεύονται το ένα το άλλο για να συνεργαστούν, συνήθως επιβάλλουν την εμπιστοσύνη τους με συμβόλαια σχετικά με τους κοινούς πόρους, τη λήψη αποφάσεων, τις κυρώσεις, τις ευαίσθητες πληροφορίες και την αμοιβαία ανταλλαγή δεδομένων. Αυτά τα συμβόλαια ταυτόχρονα τείνουν να αυξήσουν τα εμπόδια για ένταξη σε μια κοινοπραξία, καθώς αύξηση των εμποδίων για αποχώρηση από μια κοινοπραξία. Είναι πιθανό να συνυπάρχουν διάφορες κοινοπραξίες. Η διαλειτουργικότητα εντός και μεταξύ κοινοπραξιών διαδραματίζει σημαντικό ρόλο σε αυτό.

4 Κρυπτονομίσματα και κουπόνια

Μία από τις μεγάλες εφευρέσεις του Satoshi Nakamoto είναι ο συνδυασμός των προϋπαρχουσών τεχνολογιών με ένα σύστημα ανταμοιβής που διατηρεί ένα αποκεντρωμένο δίκτυο σε λειτουργία. Όπως αναφέρθηκε προηγουμένως, η ανταμοιβή στα Bitcoins καταβάλλεται στον εξορύκτη που παράγει ένα μπλοκ.

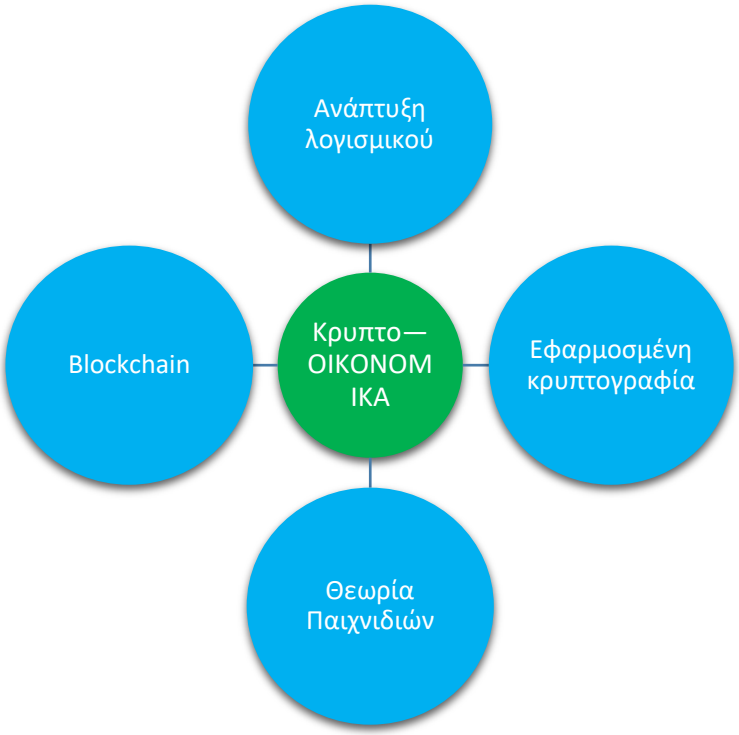
Tokens στην τωρινή κοινωνία μας είναι γνωστά ως «κουπόνια» και νομίσματα — για παράδειγμα, πόντους επιβράβευσης, νομίσματα καζίνο και κάρτες δώρων. Γνωρίζουμε επίσης «μάρκες» στην πληροφορική που παρέχουν δικαιώματα πρόσβασης σε ένα δίκτυο για την εκτέλεση μιας εργασίας ή ως αναπαραστάσεις δικαιωμάτων σε υποκείμενα περιουσιακά στοιχεία. Ένα Bitcoin, το οποίο θα μπορούσατε επίσης να δείτε ως κρυπτογραφικό διακριτικό, διαφέρει από τα προαναφερθέντα μέσα συναλλαγής με την έννοια ότι αντιπροσωπεύει αξία. Τα κρυπτογραφικά μέσα συναλλαγής μάρκες μπορούν να χρησιμοποιηθούν για πολλούς λόγους. Στην τεχνολογία blockchain, εξυπηρετούν κυρίως ένα **Διαδίκτυο της Αξίας,** όπου οι αξίες μπορούν να ανταλλάσσονται μέσω ενός αποκεντρωμένου διαδικτύου με αξιόπιστο τρόπο.

Με κρυπτογραφικά μέσα συναλλαγής όπως το Bitcoin, μπορείτε να πληρώσετε ή να αποθηκεύσετε, αλλά μπορείτε επίσης να το πάτε ένα βήμα παραπέρα. Το Bitcoin, για παράδειγμα, μπορεί να κερδηθεί με την παροχή ηλεκτρικής ενέργειας στον υπολογιστή για την παραγωγή νέων μπλοκ. Έτσι, δημιουργεί μια οικονομία όπου πολλοί συμμετέχοντες ενθαρρύνονται να βοηθήσουν στην ασφάλεια του δικτύου με αντάλλαγμα κρυπτονομίσματα. Η χρήση κρυπτογραφικών μαρκών για την τόνωση ορισμένων συμπεριφορών των συμμετεχόντων και την τιμωρία της λανθασμένης συμπεριφοράς μέσω ενός πρωτοκόλλου συναίνεσης αποτελεί μέρος της οικονομίας των **κρυπτονομισμάτων**.

Σε αυτό το κεφάλαιο, το 4.1 περιγράφει **πρώτα τα** κρυπτοοικονομικά ως την έννοια της βάσης στην οποία τα tokens αποδεικνύονται ότι παίζουν χρήσιμο ρόλο. Στη συνέχεια, 4.2. περιγράφει **τι είναι τα μέσα συναλλαγής (tokens)** και τα **ταξινομεί**. Αυτή η ταξινόμηση περιλαμβάνει dApp tokens και κρυπτονομίσματα, αλλά και τη διαφορά μεταξύ ανταλλάξιμο και μη-ανταλλάξιμου token και πώς υποστηρίζουν την οικονομία των κρυπτονομισμάτων. Το κεφάλαιο συνεχίζεται στην ενότητα 4.3 με επισκόπηση του τρόπου με τον οποίο τα **tokens** μπορούν να χρησιμοποιηθούν για τη συγκέντρωση κεφαλαίων με αρχική προσφορά νομισμάτων, προσφορά σημείων ασφαλείας και αρχική προσφορά ανταλλαγής.

4.1 Crypto Economics

Τα κρυπτογραφικά νομίσματα εξυπηρετούν διαφορετικούς σκοπούς, όπως η πρόσβαση σε ένα σύστημα ή η αναπαράσταση πληροφοριών από ένα φυσικό αντικείμενο. Αυτό παρέχει στα tokens αξία και τη δυνατότητα να ανταλλάσσονται μεταξύ διαφορετικών φορέων μέσα σε ένα Blockchain. Αυτή η νέα επιστήμη που μελετά τη μεταφορά πλούτου μέσω των δικτύων των υπολογιστών, την κρυπτογραφία, την θεωρία παιγνίων και την ανάπτυξη λογισμικού, μαζί με τη δημιουργία πλούτου και την κατανάλωση, ονομάζεται κρυπτο-οικονομία, crypto economics.



Σχήμα 9:Διεπιστημονικές πτυχές της κρυπτοοικονομικής. (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 10).

Τα δίκτυα υπολογιστών σχεδιάζονται με ορισμένους κανόνες που λειτουργούν ως ένα είδος νόμου για όλους όσους συμμετέχουν. Αυτοί οι νόμοι, ωστόσο, σχεδιάζονται από ιδιωτικούς φορείς/κοινότητες και εν μέρει επιβάλλονται από το λογισμικό και όχι από τις κυβερνήσεις. Στο πλαίσιο αυτών των νόμων, γίνονται υποθέσεις σχετικά με το πώς οι συμμετέχοντες μπορούν να συμπεριφέρονται και να συμπεριφέρονται εσφαλμένα μέσα στο δίκτυο.

Η κεντρική ιδέα πίσω από την κρυπτο-οικονομία μέσα στο **blockchain** είναι ότι αναπτύσσονται πρωτόκολλα που ενθαρρύνουν τους ανθρώπους να συμμετέχουν στο δίκτυο με τέτοιο τρόπο ώστε η **αξία** του δικτύου **να μεγιστοποιείται** για τους συμμετέχοντες. Η αξία δικτύου μπορεί να μεγιστοποιηθεί μόνο εάν το δίκτυο και οι συναλλαγές που πραγματοποιούνται σε αυτό είναι επίσης **εξασφαλισμένες**. Για να επιτευχθεί αυτό, η **κρυπτογραφία** χρησιμοποιείται για την εξασφάλιση συναλλαγών εντός του δικτύου μέσω **λογισμικού** όπως π.χ. λειτουργίες κατακερματισμού και ψηφιακές υπογραφές. Επιπλέον, οι ανταμοιβές καταβάλλονται σε συμμετέχοντες που βοηθούν στην ασφάλεια του δικτύου μέσω π.χ. εξόρυξης ή παρακολούθησης. Ο συνδυασμός αυτής της σκέψης είναι παράδειγμα στο ρόλο του Bitcoin ως ένα διακριτικό που διεγείρει τους ανθρώπους να συνεργαστούν και έτσι να βοηθήσει στη διατήρηση ενός αυτο-οργανωμένου κρυπτοοικονομικού συστήματος. Η οικονομία των κρυπτονομισμάτων είναι μια σημαντική προϋπόθεση για την υποστήριξη της ιδέας ενός βιώσιμου και κατά προτίμηση αυτο-οργανωτικού συστήματος, χωρίς τα κεντρικά κόμματα να παροτρύνουν τους ανθρώπους να δράσουν με έναν συγκεκριμένο τρόπο. Σημαντική για αυτή την υπόθεση είναι **η *Θεωρία Παιχνιδιών,*** μια μελέτη σχετικά με το πώς να δημιουργηθούν οι βέλτιστες συνθήκες σε ένα ανταγωνιστικό περιβάλλον, προκειμένου οι συμμετέχοντες να επιλέγουν πάντα να επιδεικνύουν καλή συμπεριφορά στις επιλογές τους, καθώς αυτό οδηγεί σε περισσότερο κέρδος από την κακή συμπεριφορά. Ένας

τρόπος για να ενθαρρύνετε τους συμμετέχοντες σχετικά με την καλή συμπεριφορά είναι μέσω crypto token ανταμοιβών.

4.2 Ταξινόμηση των μέσων συναλλαγής μαρκών token Blockchain

Το διαδίκτυο δημιουργήθηκε αρχικά για την ανταλλαγή πληροφοριών. Αυτό είναι επίσης γνωστό ως **Internet of Information**. Στο πλαίσιο αυτό, είναι δύσκολο να αποθηκευτεί και να μετακινηθεί αξία χωρίς έναν αξιόπιστο διαμεσολαβητή (Tapscott, 2016), ο οποίος ελέγχει κυρίως αν μια αξία, όπως το ευρώ, δεν δαπανάται δύο φορές (Satoshi, 2008, σ. 2). Με την έλευση του blockchain, μπορείτε να παρακάμψετε την ανάγκη για μεσάζοντες και να εμπορευτείτε αξία peer-to-peer άμεσα. Αυτό είναι επίσης γνωστό ως το **Διαδίκτυο της Αξίας**. Τα κρυπτονομίσματα διαδραματίζουν κεντρικό ρόλο στη συμβολή σε αυτό το κρυπτο-οικονομικό σύστημα. Ένα crypto token μπορεί να δημιουργηθεί σε ένα blockchain και επίσης να αντιπροσωπεύει ένα εμπορεύσιμο περιουσιακό στοιχείο. Μερικές φορές δημιουργούνται **token** σε ένα ICO ή ένα STO για τη χρηματοδότηση ενός έργου. Η διαδικασία της δημιουργίας **token** ονομάζεται **tokenization**. Η διαπραγμάτευση αυτών των **token** σας επιτρέπει να μεταβιβάσετε την ιδιοκτησία στα υποκείμενα περιουσιακά στοιχεία.

Υπάρχουν διαφορετικές προοπτικές για το πώς να κοιτάξετε τα κρυπτονομίσματα. Η ακόλουθη μορφή ενσωματώνει όλες τις διαφορετικές μάρκες με το πρόσθετο πλεονέκτημα της αντιμετώπισης του μελλοντικού ρόλου των μαρκών σε ένα Διαδίκτυο Αξίας:

Εφαρμογή	Token προς όφελος της εφαρμογής	Token ως περιουσιακά στοιχεία
Ανταλλάξιμα Tokens	ΔΙΕΥΘΥΝΣΗ: Αιθέρας το DApp: Augur	Το περιουσιακό στοιχείο: χρυσός Η ασφάλεια: μέρος Shell Κρυπτονόμισμα: Bitcoin
Μη ανταλλάξιμες μάρκες		Το περιουσιακό στοιχείο: πιστοποιητικό γέννησης Η ασφάλεια: προσωπικό δάνειο

Σχήμα 10: Διπλή μορφή των μαρκών. Από τη μία πλευρά, να διακρίνει μάρκες που χρησιμοποιούνται στο δίκτυο Blockchain για να διατηρήσει vs για να αποδείξει και να μεταβιβάσει την κυριότητα. Από την άλλη πλευρά, να διακρίνει μάρκες που ανταλλάσσονται vs δεν είναι ανταλλάξιμο. (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021, κεφάλαιο 10).

Θα πρέπει να λάβετε υπόψη ότι τα tokens μπορούν να έχουν μια διπλή συμβολική δομή στην οποία εξυπηρετούν πολλαπλούς σκοπούς ταυτόχρονα. Για παράδειγμα, το Bitcoin χρησιμοποιείται ως δίκτυο ή εφαρμογή συναλλαγής ή ως περιουσιακό στοιχείο.

Tokens προς όφελος της εφαρμογής χρησιμοποιούνται στο πιο βασικό επίπεδο για να ενθαρρύνουν τους ανθρώπους να συμμετάσχουν σε μια εφαρμογή blockchain και να κρατήσει αυτό το δίκτυο σε λειτουργία. Αυτό το δίκτυο μπορεί να χρησιμεύσει ως πλατφόρμα στην οποία εκτελούνται αποκεντρωμένες εφαρμογές, dApps. Εδώ τα **token δικτύου** χρησιμοποιούνται για να **επιβραβεύσουν** τους συμμετέχοντες για το έργο που κάνουν για να βοηθήσουν στη διατήρηση του δικτύου. Αυτά τα token καταλαμβάνουν μια κεντρική θέση μέσα σε ένα blockchain, επειδή ως οργανωτική ιδέα υποστηρίζουν ένα κατανεμημένο αξιόπιστο δίκτυο και έτσι διαμορφώνουν το κρυπτο-οικονομικό σύστημα ενός blockchain. Εκτός από μια εφαρμογή, ένα δίκτυο μπορεί επίσης να είναι μια **πλατφόρμα** στην οποία οι εφαρμογές τρέχουν όπως στο Ethereum ή το Cardano με τα κρυοπτονομίσματα ETH και ADA για να επιτευχθεί συναίνεση και να επιβραβευθεί το σύστημα συναλλαγών. Κάνοντας τη σκέψη ένα βήμα παραπέρα μπορείτε να δείτε ότι μέσα σε ένα blockchain υπάρχει η επιλογή να χρησιμοποιήσετε ένα token, ή να αγνοήσετε τη χρήση τους.

Τα dApp tokens ή τα **tokens χρησιμότητας** είναι χρήσιμα μόνο στο πλαίσιο της δικής τους εφαρμογής και χρησιμοποιούνται για την πρόσβαση σε αυτό το βοηθητικό πρόγραμμα. Δεν έχουν καμία χρησιμότητα εκτός της εφαρμογής αυτής. Μπορείτε ακόμα να τα ανταλλάξετε έξω από την εφαρμογή. Ωστόσο, δεν είναι πάντα προγραμματισμένα ως νόμισμα ή μερίδιο σε ένα δίκτυο. Για παράδειγμα, Siacoin (SC) όπου οι άνθρωποι μπορούν να κερδίσουν SC όταν κάνουν τον ελεύθερο χώρο στο δίσκο τους διαθέσιμο σε άλλους στο δίκτυο.

Τα dApp tokens στο Ethereum γίνονται σύμφωνα με το πρωτόκολλο **Ethereum Request for Comments 20** (ERC-20). Το πρωτόκολλο καθορίζει ορισμένους κανόνες και πρότυπα σχετικά με την έκδοση ψηφιακών κρυπτονομισμάτων στο δίκτυο Ethereum. Όλα τα dApp token που γίνονται σύμφωνα με το ERC-20 είναι μοναδικά για την εφαρμογή τους και μπορούν να αποτελέσουν αντικείμενο συναλλαγών στο δίκτυο Ethereum.

Τα tokens προς όφελος των εφαρμογών διαφέρουν από τα token που περιστρέφονται γύρω από τη δέσμευση και την ανταλλαγή αξίας εντός των εφαρμογών blockchain με τις οποίες αποδεικνύουν την κατοχή αυτής της αξίας και επιτρέπουν τη μεταφορά του δικαιώματος σε αυτή την αξία, **token ως περιουσιακά στοιχεία**. Αυτό μπορεί να υποδιαιρεθεί σε token περιουσιακών στοιχείων, token ασφαλείας και crypto valuta.

Τα tokens περιουσιακών στοιχείων αντιπροσωπεύουν αρχεία δικαιωμάτων και υποχρεώσεων στο υποκείμενο περιουσιακό στοιχείο, όπως ο χρυσός ή το πετρέλαιο, αλλά και σε ένα σπίτι, ένα χάρτινο κλιπ ή κρυπτοσυλλεκτικά, όπως τα avatars παιχνιδιών ή τα ψηφιακά έργα τέχνης. Αυτές τα tokens μπορεί να αντιπροσωπεύουν αμελητέες έως πολύ μεγάλες υποκείμενες αξίες. Μια σημαντική προϋπόθεση για τα ψηφιακά μέσα συναλλαγής περιουσιακών στοιχείων είναι ότι μπορεί να τεκμηριωθεί η ταυτότητα του ιδιοκτήτη. Τα κρυπτονομίσματα περιουσιακών στοιχείων μπορούν να αποφέρουν οφέλη λόγω της δυνατότητας προγραμματισμού τους (**έξυπνων token**) και εμπορίου τους με χαμηλή φθορά και υψηλή ασφάλεια:

1. Μπορείτε εύκολα να διαιρέσετε τα περιουσιακά στοιχεία και να τα διαθέσετε σε μικρές μονάδες. Ένα παράδειγμα αυτής της **διάσπασης** αντιπροσωπεύει την ιδιοκτησία της Mona Lisa σε 1.000 tokens για πώληση/μίσθωση.
2. Μπορείτε να προγραμματίσετε τα δικαιώματα στο κρυπτογραφικό token και να τα επιβάλετε μέσω έξυπνων συμβολαίων. Για παράδειγμα, ορίστε το token Mona Lisa να πωλείται μόνο σε μη κερδοσκοπικούς οργανισμούς ή το πρόγραμμα που μια μεταπώληση περιλαμβάνει αυτόματα προμήθεια 2 % στον αρχικό πωλητή.

3. Μειώνετε την τριβή στην αγορά και την πώληση, εν μέρει λόγω των γρήγορων και φθηνών μικροσυναλλαγών. Για παράδειγμα, ένα έξυπνο ψυγείο σαρώνει τη φθηνότερη ηλεκτρική ενέργεια για ορισμένα χρονικά διαστήματα.
4. Μπορείτε να καταγράψετε όλες τις σχετικές πληροφορίες για τα υποκείμενα περιουσιακά στοιχεία στο token. Για παράδειγμα, ελέγξτε τους προηγούμενους ιδιοκτήτες του μεταχειρισμένου μηχανήματός σας, βελτιώνοντας έτσι την οικονομία του διαμοιρασμού.
5. Μπορείτε εύκολα να δημιουργήσετε ένα περιουσιακό στοιχείο μόνοι σας, όπως ένα εισιτήριο εισόδου σε μια συναυλία στο σπίτι.

Εν ολίγοις, τα έξυπνα ψηφιακά μέσα συναλλαγής μεταφέρουν εύκολα αξία, πληροφορίες, ιδέες, δικαιώματα και υποχρεώσεις μέσω έξυπνων συμβολαίων.

Τα **tokens ασφαλείας** αντιπροσωπεύουν ομόλογα, μετοχές, δάνεια, συμβόλαια μελλοντικής εκπλήρωσης, δικαιώματα προαίρεσης και άλλα διαπραγματεύσιμα χρηματοοικονομικά περιουσιακά στοιχεία. Αν και ανήκουν στα μέσα συναλλαγής περιουσιακών στοιχείων, αναφέρονται ξεχωριστά. Όλα τα είδη δικαιωμάτων μπορούν να δοθούν σε tokens ασφαλείας. Για παράδειγμα, το δικαίωμα να μην μεταπωλήσετε την ασφάλεια σε όλους ή να είστε σε θέση να δανείσετε προσωρινά τα δικαιώματα ψήφου σας σχετικά με την κατεύθυνση της εταιρείας σε κάποιον.

Τα ψηφιακά **κρυπτονομισμάτα** ανήκουν επίσης σε μέσα συναλλαγής περιουσιακών στοιχείων και αντιμετωπίζονται χωριστά λόγω του σημαντικού αναμενόμενου χρηματοοικονομικού αντικτύπου τους. Το Bitcoin είναι το πιο γνωστό παράδειγμα ενός κρυπτονομίσματος. Σε αυτή την περίπτωση, το token προορίζεται να λειτουργήσει ως χρήμα. Αργά αλλά **σταθερά νομίσματα** συγκεντρώνουν την προσοχή καθώς δείχνουν πιθανούς τρόπους σταθεροποίησης της αξίας των κρυπτονομισμάτων και ως εκ τούτου, μεταξύ άλλων, δυνητικά να χρησιμεύσουν ως αποκεντρωμένες εναλλακτικές λύσεις ή αναπαραστάσεις των νομισμάτων μορφής fiat. Τα σταθερά νομίσματα μπορούν να ασφαλιστούν με διάφορα περιουσιακά στοιχεία, όπως νόμισμα μορφής fiat ή χρυσό ή κρυπτονομίσματα, ή να μην είναι καθόλου εξασφαλισμένα.

Ορισμένες κεντρικές τράπεζες δοκιμάζουν σταθερά νομίσματα σε αυτό που ονομάζεται ψηφιακό νόμισμα **της Κεντρικής Τράπεζας (CBDC**). Ενώ η CBDC μπορεί να χρησιμοποιήσει στοιχεία του blockchain, δεν είναι απαραίτητα μια εφαρμογή blockchain. Τα CBDC είναι διαμετρικά αντίθετα με την αποκεντρωμένη προέλευση του Bitcoin, καθώς ένα CDBC είναι ένα κεντρικά ρυθμιζόμενο νόμισμα.

Υπάρχει το ζήτημα του τρόπου εφαρμογής των κρυπτονομισμάτων σε ένα οικονομικό σύστημα όπου πραγματοποιείται η ανταλλαγή. Ένας τρόπος για να γίνει αυτό είναι να εξετάσουμε την **ανταλλαξιμότητα των token**. Ορισμένα token μπορούν να ανταλλάσσονται ευκολότερα από άλλα. Για παράδειγμα, ένα πακέτο 1 κιλού αλεύρου μπορεί να ανταλλαχθεί με άλλο 1 κιλό αλεύρι. Ένα τραπεζογραμμάτιο των 10 EUR μπορεί επίσης να ανταλλαχθεί με δύο τραπεζογραμμάτια των 5 EUR. Το ίδιο ισχύει και για τις **ανταλλάξιμα token**: οι μεμονωμένες μονάδες είναι δυσδιάκριτες μεταξύ τους και μπορούν να ανταλλάσσονται μεταξύ τους. Ένα παράδειγμα είναι το Polkadot: 1 Polkadot token μπορεί να ανταλλαχθεί με ένα άλλο και δύο μισά Polkadot token μπορούν να ανταλλαγούν με 1 ολόκληρο Polkadot.

Αντίθετα από τα προηγούμενα είναι τα **μη-ανταλλάξιμα token** όπου τα token είναι μοναδικά από μόνα τους και ως εκ τούτου σπάνια. Σκεφτείτε για παράδειγμα τα άτομα, τη χώρα και τα

Co-funded by the Erasmus+ Programme of the European Union

πιστοποιητικά γέννησης που δεν μπορούν να ανταλλάσσονται με άλλα άτομα, άλλη χώρα και άλλα πιστοποιητικά γέννησης.

Ειδικότερα, το blockchain είναι κατάλληλο για την αποτελεσματική καταγραφή και εμπορία αυτών των token, ακόμη και αν τα token αντιπροσωπεύουν μόνο μια μικρή αξία και/ή είναι μοναδικά στο είδος τους. Αυτό είναι σημαντικό, όπως σε έναν ψηφιακό κόσμο, είναι εύκολο να δημιουργήσετε ένα αντίγραφο ενός ψηφιακού αγαθού. Έτσι, έχοντας ένα μέσο συναλλαγής ως αναπαράσταση, δεν υπάρχει μόνο μια ευκαιρία για εύκολη εμπορία αγαθών από τον πραγματικό κόσμο. Σας δίνει επίσης την ευκαιρία να δώσετε σε κάθε φυσικό αγαθό μια αυθεντική ψηφιακή αναπαράσταση, όσο μικρή ή ανόητη μπορεί να είναι η καλή και να την ανταλλάξετε. Επιπλέον, η δημιουργία ενός σπάνιου token είναι οικονομικά ενδιαφέρουσα αν θέλετε να διατηρήσετε την τιμή που σας δίνεται το adagio: «όσο χαμηλότερη είναι η προσφορά token, τόσο μεγαλύτερη είναι η σπανιότητα και, κατά συνέπεια, η πιθανότητα υψηλότερης τιμής».
Μια σειρά από τα πλεονεκτήματα που αναφέρθηκαν νωρίτερα για τα κρυπτονομίσματα περιουσιακών στοιχείων, όπως ο κατακερματισμός και η δημιουργία έξυπνων token, υποστηρίζουν την περίπτωση του χρήστη για μη ανταλλάξιμα token, δεδομένου ότι μπορούν να γίνουν ιδιαίτερα ατομικές αναπαραστάσεις οποιουδήποτε αντικειμένου (που πρόκειται να ψηφιοποιηθεί) που δημιουργείται και ανταλλάσσεται μέσω ενός χαμηλού επιπέδου ταυτοποίησης (όλοι μπορούν να εισέλθουν, όλοι μπορούν να συμμετάσχουν) ασφαλές δίκτυο, το Διαδίκτυο της Αξίας. Ένα διαδίκτυο που μπορεί να χρησιμοποιηθεί για να μετρήσει με διαφάνεια τον αντίκτυπό σας στο περιβάλλον και σας ωθεί να υποστηρίξετε τους στόχους μιας ευρύτερης κοινότητας. Είτε είστε ιδιοκτήτης ηλιακών συλλεκτών, χρήστης ηλεκτρικής ενέργειας ή επενδυτής δικτύου.

Στο μέλλον, θα μπορούσατε θεωρητικά να χρησιμοποιήσετε οποιοδήποτε περιουσιακό στοιχείο που σας ανήκει, να κάνετε token και να χρησιμοποιήσετε αυτά τα token τμηματικά ή με άλλο τρόπο ως μέσο πληρωμής ή χρηματοδότησης.

4.3 Μέσα συναλλαγής – μάρκες απόκτησης κεφαλαίων

Στη συνέχεια, όλα αυτά τα ξεχωριστά μέσα συναλλαγής (token) μπορούν να χρησιμοποιηθούν με διάφορους τρόπους για την απόκτηση κεφαλαίων: από τις αρχικές προσφορές νομισμάτων (Iinitial Coin Offering), προσφορές ασφαλείας μέσων συναλλαγής (Security Token Offering) και των αρχικών προσφορών ανταλλαγής (Intial Exhange Offering) έως τις αρχικές προσφορές DEX (Initial DEX Offering).

Η **αρχική προσφορά νομισμάτων** (ICO) χρησιμοποιήθηκε κυρίως στο παρελθόν για την άντληση κεφαλαίων στο διαδίκτυο για έργα blockchain. Το Ethereum ειδικότερα ήταν το κύριο blockchain για τη δημιουργία και την πώληση μέσων συναλλαγής. Ένας σημαντικός αριθμός περιπτώσεων κατάχρησης προέκυψαν στην αρχή της εφαρμογής του ICO, που εξαιτίας του γεγονότος ότι η ICO έλαβε χώρα εκτός της προστασίας των εθνικών νόμων και κανονισμών. Ως αποτέλεσμα, η **ασφάλεια Token Offering** (STO) σχεδιάστηκε για να εξυπηρετεί τον ίδιο σκοπό με ένα ICO, ωστόσο τώρα με το να θεωρεί ένα διακριτικό ως ασφάλεια με τυποποιημένα πρωτόκολλα, δικαιώματα ψήφου και πολλά άλλα σύμφωνα, ανκαι όχι πλήρως, με διάφορους εθνικούς νόμους και κανονισμούς ανταλλαγής. Η STO δεν έχει αποδειχθεί ιδιαίτερα επιτυχημένη στον δημόσιο χώρο μέχρι σήμερα. Επίσης, ως νέες πιο ρυθμισμένες, αλλά ακόμα «ανοικτές» εναλλακτικές λύσεις, σχεδιάστηκαν όπως η **αρχική**

προσφορά ανταλλαγής (IEO) και η **αρχική προσφορά DEX** (IDO). Εδώ συγκεντρωτικές ή αποκεντρωμένες ανταλλαγές, όπως Binance ή Uniswap χέρι start-ups μια ευκαιρία να αποκτήσουν crowdfunding μέσω της ενδιάμεσης πλατφόρμας τους, η οποία συνήθως αναλαμβάνει τους ελέγχους KYC και AML.

Η τάση διαμόρφωσης ενός αποκεντρωμένου Διαδικτύου της Αξίας από την κοινότητα φαίνεται να συνεχίζεται σε ένα ανεμοστρόβιλο συγκρουόμενων ιδανικών, ιδεών, τεχνικών δυνατοτήτων, λαθών, θαυμαστών ατυχημάτων και επιμονών.

5 Χρήσεις και εφαρμογές του Blockchain

Σε αυτό το κεφάλαιο δίνονται τρία παραδείγματα χρήσης και εφαρμογών του blockchain. Πριν από αυτό, δίνεται μια εισαγωγή για το πώς οι οργανισμοί μπορούν να σκεφτούν στρατηγικά τα σχετικά στοιχεία του επιχειρηματικού τους μοντέλου και τις ευκαιρίες που προσφέρει το blockchain. Το κεφάλαιο τελειώνει με συγκεκριμένα σημεία που μια εταιρεία δίνει προσοχή μόλις εφαρμόσει το blockchain.

5.1 Επιχειρηματικά μοντέλα

Το blockchain συνήθως προσφέρει αξία στο πλαίσιο των επιχειρηματικών μοντέλων και των επιχειρηματικών οικοσυστημάτων, όπου τα ψηφιακά δεδομένα και η τεχνολογία μπορούν να δημιουργηθούν και να μοιραστούν μεταξύ των εταίρων. Η τεχνολογία blockchain είναι μια ψηφιακή τεχνολογία που ταιριάζει με αυτά τα ψηφιακά δεδομένα που βασίζονται σε επιχειρηματικά μοντέλα και επιτρέπει στους εταίρους να συνεργαστούν εκεί που δεν θα μπορούσαν πριν. Αυτοί οι εταίροι μπορούν τώρα να εμπιστευτούν «στο σύστημα» όπου πριν από το blockchain δεν εμπιστεύονταν ο ένας τον άλλον για να συνεργαστούν από την αρχή. Υπό την έννοια αυτή, η τεχνολογία blockchain είναι μια ευκαιρία ανάπτυξης και ψηφιοποίησης οικοσυστημάτων που χρησιμοποιούν **επιχειρηματικά μοντέλα που βασίζονται σε ψηφιακά δεδομένα**.

Όσον αφορά τα επιχειρηματικά μοντέλα, το **αποκεντρωμένο Business Model Canvas** [6][7] είναι σχετικό, ενώ η αποκέντρωση είναι ουσιαστική για τις δημόσιες προσαρμογές blockchain χωρίς άδεια. Οι κάτοχοι των μέσων συναλλαγής (token) έχουν κεντρική θέση καθώς έχουν πολλαπλούς ρόλους, όπως χρήστης, επικυρωτής, υπάλληλος ή/και ιδιοκτήτης. Τα παραπάνω δίνουν μια ιδέα για τις πιθανές νέες ευκαιρίες που προσφέρει το δημόσιο blockchain χωρίς άδεια καθώς φορείς που δεν γνωρίζουν ο ένας τον άλλον, έχουν μια εναλλακτική λύση να εγκαταστήσουν και να χρησιμοποιήσουν ένα σχετικά χαμηλού επιπέδου συστήματος ασφαλείας για να μοιραστούν και να επαληθεύσουν τα δεδομένα, ενώ δεν γνωρίζονται μεταξύ τους.

Στη συνέχεια, η διακυβέρνηση δημιουργείται με αποκεντρωμένο τρόπο από το κοινό, τα δεδομένα αποθηκεύονται με αποκεντρωμένο τρόπο και η επικοινωνία μεταξύ των διαφόρων μερών πραγματοποιείται με τη μέθοδο peer-to-peer. Αυτή είναι η πιο ανοιχτή μορφή ενός blockchain. Μια εταιρεία είναι ελεύθερη να προσαρμόσει τα δομικά μπλοκ του ίδιου του blockchain. Με ένα συγκεντρωτικό σύστημα, ένας κεντρικός οργανισμός παίρνει τις αποφάσεις.

Σε ένα αποκεντρωμένο επιχειρηματικό μοντέλο, οι πωλήσεις συχνά μοιράζονται μεταξύ εκείνων που συνεισφέρουν περισσότερο στο δίκτυο και το κόστος χρήσης της πλατφόρμας είναι πολύ χαμηλό — για παράδειγμα, με την πλατφόρμα blockchain κοινωνικής blogging Steemit.

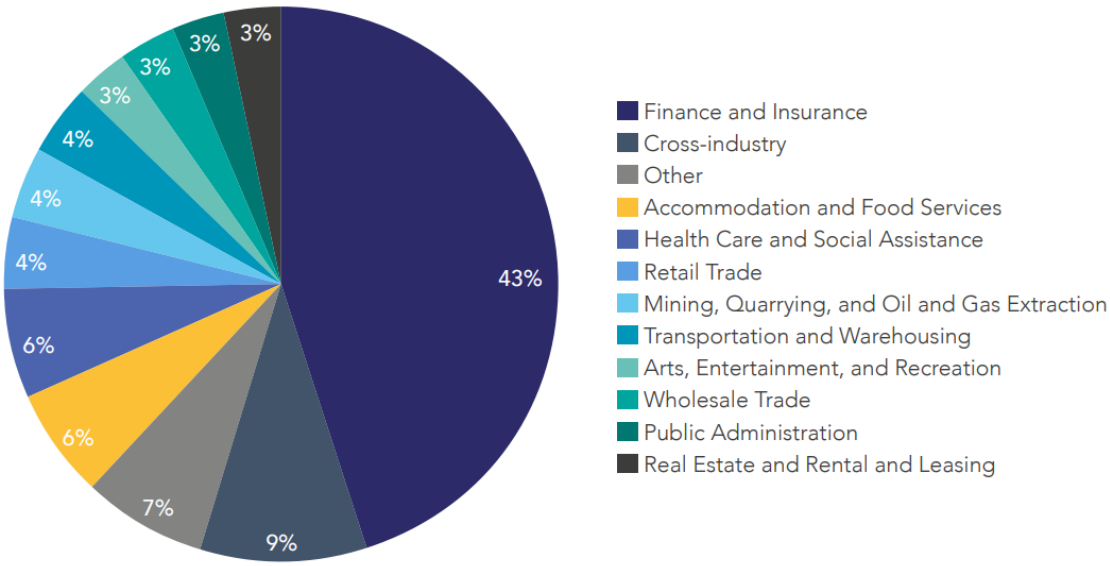
[6] https://canvanizer.com/new/decentralized-business-model-canvas
[7] https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

5.2 Εφαρμογές Blockchain επιχειρήσεων

Αυτή η παράγραφος περιγράφει τρεις εφαρμογές που αναπτύχθηκαν σε τρεις διαφορετικούς κλάδους και τις συγκρίνει χρησιμοποιώντας τα συγκριτικά πλεονεκτήματα που προσφέρει το blockchain σε αυτές τις εφαρμογές. Οι τρεις εφαρμογές είναι:

1. Κυβέρνηση και δημόσια αγαθά από την Lantmäteriet.
2. Κατασκευή από την BMW.
3. Ψηφιακό πορτοφόλι από την Singapore Airlines.

Μια χρήσιμη επισκόπηση εδώ για να σας βοηθήσει να καταλάβετε πόσοι πολλοί τομείς blockchain εφαρμόζουν blockchain είναι από την παρακάτω έρευνα που διεξήχθη μεταξύ 67 δικτύων blockchain επιχειρήσεων και τους τομείς στους οποίους εμπίπτουν αυτές οι εφαρμογές (Rauchs, Blandin, Bear, McKeon, 2019).



Σχήμα 11: Επισκόπηση 67 ζωντανών επιχειρηματικών δικτύων Blockchain και σε ποιους τομείς εμπίπτουν (Πηγή: Rauchs, Blandin, αρκούδα, McKeon, 2019).

Το πρώτο παράδειγμα αφορά τον **τομέα της κυβέρνησης και των δημόσιων αγαθών**. Το σουηδικό **Lantmäteriet** έχει το καθήκον να διατηρεί το Κτηματολόγιο, να παρέχει γεωδεδομένα και να εκτελεί την κτηματογράφηση. Υπάρχει ανάγκη για μεγαλύτερη διαφάνεια και μεγαλύτερη αποτελεσματικότητα του έργου, καθώς διάφοροι εταίροι συνεργάζονται χρησιμοποιώντας χειρόγραφες διαδικασίες που φαίνονται αναποτελεσματικές και επιρρεπείς σε σφάλματα.

Η Lantmäteriet δοκίμασε μια λύση για να δει πώς οι παράγοντες όπως οι αγοραστές ακινήτων, οι πωλητές, οι μεσίτες, οι χρηματοπιστωτικές υπηρεσίες, οι δικηγόροι, τα συνταξιοδοτικά ταμεία και το Lantmäteriet μπορούν να συνεργαστούν σε μια αποτελεσματική διαδικτυακή πλατφόρμα που παρέχει άμεση διαφάνεια ενός αιτήματος μέσω ψηφιακών συσκευών. Το έργο δημιουργήθηκε (2015-2019) υπό μια ελεγχόμενη κατάσταση με αξιόπιστους εταίρους, χωρίς υπερβολικές φιλοδοξίες για μεγαλύτερη αποκέντρωση σε βραχυπρόθεσμο ορίζοντα. Υπήρξε σαφής εστίαση σε άμεσα εφικτούς

στόχους όπως είναι η δημιουργία του μητρώο των τίτλων γης, δημιουργώντας παράλληλα ένα πρότυπο για μελλοντικές υπηρεσίες.

Κατά τη διάρκεια του έργου προέκυψαν νομικά ζητήματα που έπρεπε να ξεπεραστούν. Για ένα από αυτά, η Lantmäteriet έπρεπε να εξετάσει τον τρόπο αντιμετώπισης του δικαιώματος των φυσικών προσώπων να ελέγχουν τα δικά τους δεδομένα (γενικός κανονισμός της ΕΕ για την προστασία δεδομένων — GDPR), συμπεριλαμβανομένης της δυνατότητας να τα προστατεύουν και να τα διαγράφουν όπου αυτό είναι επιθυμητό και εφικτό. Καθώς και σχετικά με τον τρόπο με τον οποίο οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν ως νομικά δεσμευτικές υπογραφές εντός της ΕΕ (κατευθυντήρια γραμμή eIDAS) ή το καθεστώς των ψηφιακά υπογεγραμμένων (ηλεκτρονικών) συμβάσεων που βασίζονται σε blockchain.

Η πώληση των τίτλων γης ήταν φιλόδοξη, δεδομένου ότι διάφορα μέρη δημιούργησαν μια νέα διαδικασία και ένα παιχνίδι με μια νέα τεχνολογική λύση. Οι λύσεις blockchain περιλάμβαναν τόσο ιδιωτικά, κλειστά, αδειοδοτημένα συστήματα blockchain όσο και ένα κατανεμημένο δημόσιο δίκτυο. Το ιδιωτικό blockchain ανήκει στην κυβέρνηση, διοικείται από περιορισμένο αριθμό κόμβων από αξιόπιστους μεσάζοντες και υπό την εποπτεία της σουηδικής δημόσιας κυβέρνησης. Το σύστημα αυτό συνεργάζεται με την ChromaWay και το ιδιωτικό δίκτυο των ενδιαφερομένων. Χρησιμοποιεί έξυπνα συμβόλαια, την πρακτική Practical Byzantine Fault Tolerance και μηχανισμούς συναίνεσης απόδειξης της εργασίας, off-chain και on-chain ψηφιακές ταυτότητες μέσω μιας εφαρμογής κινητού τηλεφώνου και χωρίς μέσου συναλλαγής (token).

Η πράξη παραμένει καταχωρημένη στο Lantmäteriet και δεν μεταφέρεται σε δημόσιο blockchain με δεδομένο τα προηγούμενα προβλημάτα σχετικά με την προστασία προσωπικών δεδομένων - GDPR. Οι συμβάσεις υπογράφονται χειρόγραφα και τοποθετούνται στο blockchain μέσω hashes. Οι αρχικές συμβάσεις είναι στο διακομιστή με άλλα μέρη, ενώ οι πληροφορίες αυτές έχουν αντίγραφα ασφαλείας. Η Telia προσφέρει μια λύση αναγνώρισης για κινητά που επιτρέπει στους χρήστες να εγγραφούν χωρίς να δημοσιεύουν τον ατομικό τους Σουηδικό Αριθμό Δημόσιας Διοίκησης (Swedish Civil Service Number). Αυτές οι εγγραφές αποθηκεύονται στο blockchain του Bitcoin μέσω μπολκ hash και επαληθεύονται. Οι ψηφιακές προσωπικές πληροφορίες μπορούν να αφαιρεθούν εάν ένα άτομο το επιθυμεί και δεν απαιτείται από το νόμο να είναι δημόσιες πληροφορίες.

Τα κύρια πλεονεκτήματα ήταν η ασφάλεια της χρήσης τεχνολογίας blockchain, καθώς και η λειτουργικότητα. Όσον αφορά το τελευταίο, καθώς το χρονικό πλαίσιο της καταχώρισης ενός τίτλου γης μειώθηκε από 4-6 μήνες σε λίγες ημέρες. Επίσης, προβλέπεται εξοικονόμηση 100 εκατ. EUR/έτος κυρίως εξαιτίας λιγότερων σφαλμάτων και κόστους συντήρησης (Kairos Future, 2017). Αυτό στη συνέχεια μειώνει τους κινδύνους μιας σύμβασης με διφορούμενα χαρακτηριστικά, δόλια δεδομένα ή πιθανότητες κλοπής περιουσιακών στοιχείων. Εξαιτίας της ύπαρξης μιας διαδρομής ελέγχου και προς τους δύο πελάτες, ο ελεγκτής ως νομοθέτης έγινε επίσης ποιο διαφανής. Επίσης, το οικοσύστημα ενίσχυσε τις αμοιβαίες διαδικασίες και την ανταλλαγή δεδομένων χωρίς υπερβολική αναστάτωση των κεντρικών υπηρεσιών και του επιχειρηματικού του μοντέλου. Και, τέλος, η δημόσια προσβασιμότητα αύξησε την εμπιστοσύνη στη διαδικασία και σε όλα τα εμπλεκόμενα μέρη. Μετά τη δοκιμή, το σύστημα θα μπορούσε να επεκταθεί σε άλλους τομείς όπως οι ασφαλιστές, οι συμβολαιογράφοι και άλλες τοπικές δημόσιες αρχές.

Το έργο ολοκληρώθηκε το 2019, δείχνοντας ότι η αρχιτεκτονική της πλατφόρμας αποδείχθηκε δυνατή, ωστόσο, σύμφωνα με τον Mats Snäll, Chief Innovation Officer της

Lantmäteriet, «Ποτέ δεν ενσωματώθηκε στο σύστημα παραγωγής του κτηματολογίου», καθώς θα χρειαζόταν μια αλλαγή στη νομοθεσία πριν το σύστημα μπορέσει να επεκταθεί στο μέλλον (Baraniuk, 2020). Πιθανότατα αυτό δείχνει την πρόκληση της δημοσίευσης δεδομένων ταυτότητας χρήστη στο δημόσιο blockchain.

Άλλες έρευνες δείχνουν επίσης την κατεύθυνση μιας «θεμελιώδους αλλαγής στη δομή διακυβέρνησης, όπως ο ρόλος του Lantmäteriet», η οποία θα μπορούσε να αποτελέσει ένα υποκείμενο κίνητρο να παγώσουν την περαιτέρω πρόοδο του έργου ειδικά για τα οικοσυστήματα ακινήτων (Schnuer, 2020).

Εν τω μεταξύ, η Lantmäteriet αξιοποιεί την εμπειρία της και συνεχίσει τον πειραματισμό με το blockchain. Για παράδειγμα, η κοινή κυβερνητική ανάθεση με τη DIGG ενός έργου στο πλαίσιο του οποίου πρόκειται να βρεθεί «ένα μοντέλο ή μια εννοιολογική λύση για τον τρόπο οικοδόμησης εμπιστοσύνης στην αυτοματοποίηση με την τεχνητή νοημοσύνη και με άλλες νέες τεχνολογίες, όπως η τεχνολογία blockchain» (AI Sweden, Lantmäteriet, 2020).

Το δεύτερο παράδειγμα εφαρμογής blockchain αφορά τη BMW στον τομέα **της μεταποίησης. Τα επιχειρηματικά μοντέλα της αυτοκινητοβιομηχανίας πρέπει να αντιμετωπίσουν τις** τεχνολογίες της 4ης βιομηχανικής επανάστασης, όπως η ηλεκτροκίνηση και τα αυτόνομα συστήματα υπό συνεχώς αυξανόμενες περιβαλλοντικές συνειδητές συνθήκες.

Η **BMW** σε αυτό το παράδειγμα προσπαθεί να κατανοήσει πώς μπορεί να χρησιμοποιηθεί μια ψηφιακή ταυτότητα για τα αυτοκίνητα, ώστε να μπορεί να επιτρέψει τη χρήση άλλων τεχνολογιών και εννοιών της 4ης Βιομηχανικής Επανάστασης. Ειδικότερα, τα ζητήματα ιδιωτικότητας/ασφάλειας της συνεχούς σύνδεσης του αυτοκινήτου και του χρήστη στο διαδίκτυο, καθώς και η ανάγκη ασφαλούς αποθήκευσης των δεδομένων αυτών. Αυτή η ασφαλής ανταλλαγή δεδομένων μεταξύ συσκευών που εγγυώνται ασφαλείς ψηφιακές ταυτότητες είναι αυτό που το blockchain μπορεί να φέρει στο τραπέζι, προσφέροντας έτσι μια είσοδο στην αγορά της οικονομίας διαμοιρασμού αυτοκινήτων για την BMW.

Η BMW έχει δοκιμάσει μια σειρά από εφαρμογές κοινής χρήσης αυτοκινήτων, όπως το Share Now, όπου μπορεί να εμπλέκεται η ψηφιακή ταυτότητα και των δύο αυτοκινήτων ως χρήστη. Αυτές οι συνδυασμένες ψηφιακές ταυτότητες αυτοκινήτων μπορούν, για παράδειγμα, να εγγράφουν πότε βάζει ο χρήστης βενζίνη ή που είναι το αυτοκίνητο σταθμευμένο. Αυτού του είδους πληροφορίας στη συνέχεια μπορεί να χρησιμοποιηθεί σε επιχειρηματικά μοντέλα όπου οι κατασκευαστές αυτοκινήτων, μαζί με ή χωρίς μεσάζοντες, προσφέρουν εξατομικευμένες υπηρεσίες όπως ασφάλιση ζημιών, αυτόνομες διαδρομές αυτοκινήτων ή βελτιώνουν την εμπειρία του αυτοκινήτου γενικότερα.

Σε αυτό το συγκεκριμένο παράδειγμα, ωστόσο, η BMW πειραματίστηκε με ένα απλούστερο project με αποκλειστική εστίαση στην ταυτότητα του αυτοκινήτου και στα αποθηκευμένα δεδομένα του, οπότε δεν εστιάζει στον χρήστη. Η ιδέα είναι ότι οι πιθανοί αγοραστές χρησιμοποιημένων BMW θα ενδιαφέρονταν για αξιόπιστα δεδομένα σχετικά με τα χιλιόμετρα, το ιστορικό ατυχημάτων, το ιστορικό σέρβις και άλλες πληροφορίες του αυτοκινήτου. Ένας μελλοντικός πωλητής θα μπορούσε να μοιραστεί αυτά τα δεδομένα με έναν υποψήφιο πωλητή ή τον ασφαλιστή του, η BMW θα μπορούσε να χρησιμοποιήσει τις πληροφορίες για να βελτιώσει το επιχειρηματικό της μοντέλο, όπως τη χρήση τους για την καλύτερη εξυπηρέτηση των πελατών της.

Για να δημιουργηθεί αυτή η λύση, το **BMW's Startup Garage** της BMW συνεργάστηκε με τις νεοσύστατες επιχειρήσεις blockchain, σε αυτή την περίπτωση τη VeChain. Επίσης, η BMW χρησιμοποιεί τα αποτελέσματα για να αναπτύξει το ID ενός αυτοκινήτου, ένα πρώτο βήμα για μια ταυτότητα οχήματος (VID) που τα μέλη της Πρωτοβουλίας Κινητικότητας Open Blockchain (MOBI) μπορούν να χρησιμοποιήσουν μαζί. Η Mobi είναι μια κοινοπραξία blockchain που αναπτύσσει μαζί τα πρότυπα blockchain.

Η συνεργασία με την VeChain οδήγησε στην **εφαρμογή** VerifyCar. Το VeChain είναι ένας Αποκεντρωμένος Αυτόνομος Οργανισμός με ένα κεντρικό διοικητικό όργανο που χρησιμοποιεί τη μέθοδο **Proof-of-Authority** και διαφορετικά μέσα συναλλαγής στο δημόσιο blockchain VeChain.

Το VID έχει ένα μοναδικό αναγνωριστικό σε αυτό το blockchain. Περιοδικά η εφαρμογή συλλαμβάνει δεδομένα (μέσω των καρτών SIM εντός του αυτοκινήτου και της επικοινωνίας Machine-to-Machine), τα οποία επαληθεύονται στο blockchain VeChain: Η VeChain αποθηκεύει μόνο την αναφορά στα δεδομένα, τα δεδομένα παραμένουν στο ίδιο το όχημα. Τα δεδομένα του αυτοκινήτου περιέχουν τόσο στατικές πληροφορίες, όπως ο τύπος και η ημερομηνία παραγωγής του αυτοκινήτου, όσο και δυναμικές πληροφορίες, όπως ο αριθμός των χιλιομέτρων οδήγησης. Κάθε φορά που ένας ιδιοκτήτης αυτοκινήτου θέλει να μοιραστεί δεδομένα με άλλο μέρος, χρησιμοποιεί την εφαρμογή VerifyCar για να δείξει τα δεδομένα, συμπεριλαμβανομένων των αναφορών στο blockchain, για να δείξει ότι αυτά είναι τα πραγματικά δεδομένα που είναι αποθηκευμένα στο όχημα.

Η πρόθεση της BMW να μην έχει κανέναν έλεγχο στη διακυβέρνηση της VeChain ή στον κώδικα. Τις αρχές του 2022 η εφαρμογή ακόμη δεν έχει εφαρμοστεί.

Κατά την πιλοτική εφαρμογή αυτής της λύσης, η BMW κάνει ένα ελεγχόμενο πρώτο βήμα προς την σταδιακή ενσωμάτωση της αποκεντρωμένης τεχνολογίας blockchain. Επίσης, εάν το VerifyCar μπορεί να χρησιμοποιηθεί για αυτοκίνητα, τότε γιατί να μην έχετε ένα VID όπως την ψηφιακή ταυτότητα για να βεβαιωθείτε ότι τα εξαρτήματα αυτοκινήτων δεν είναι παραποιημένα, από που αγοράζονται οι πρώτες ύλες που μπορεί να βρεθούν στη γραμμή παραγωγής ή να κατανοήσετε τους όρους κατασκευής ή μεταφοράς ορισμένων μηχανημάτων παραγωγής που έχετε παραγγείλει; Σύμφωνα με αυτή τη σκέψη, η BMW πειραματίζεται με το blockchain προς όφελος **μιας διαφανούς εφοδιαστικής αλυσίδας**.

Για παράδειγμα, το 2019 **το** πιλοτικό PartChain για την αγορά εμπρόσθιων φώτων χρησιμοποιώντας υπηρεσίες ιστού Amazon, Microsoft Azure και Hyperledger Fabric blockchain (Ledger Insights (2020, 31 Μαρτίου) επεκτάθηκε και σε άλλους προμηθευτές. Αυτό επέτρεψε στην BWM να είναι σε θέση να ανιχνεύει τα συστατικά της και, μακροπρόθεσμα, τις κρίσιμες πρώτες ύλες «από το ορυχείο έως το μεταλλουργείο». (BMW Pressclub Global, 2020). Και επιπλέον να εξασφαλιστεί «ευκολότερη πιστοποίηση και συντομότερες τελωνειακές διαδικασίες» (BMW, 2019).

Ένα **τελευταίο παράδειγμα είναι το ψηφιακό πορτοφόλι της Singapore Airlines, KrisPay**. Η Singapore Airlines επιδίωκε να αυξήσει περαιτέρω την αφοσίωση των πελατών της με τη χρήση του blockchain. Αυτό είχε ως αποτέλεσμα την ενίσχυση του προγράμματος συχνών επιβατών KrisFlyer με το ψηφιακό blockchain πορτοφόλι KrisPay το 2018.

Με το KrisPay οι πελάτες μπορούν να ανταλλάξουν τα αεροπορικά μίλια KrisFlyer για μίλια KrisPay, που αποτελούν κρυπτονομισμάτων. Αυτά τα κρυπτονομίσματα KrisPay μπορούν να αποθηκευτούν ή να ανταλλαχθούν σε διάφορους εμπορικούς φορείς όπως οι τράπεζες, τα πρατήρια βενζίνης και άλλα εμπορικά καταστήματα. Επίσης, ο πελάτης μπορεί να

αποθηκεύσει και να ανταλλάξει άλλες ανταμοιβές, όπως χρησιμοποιώντας την πιστωτική κάρτα της DBS (Development Bank of Singapore Limited), ή να κερδίσει, να αγοράσει ή να ξοδέψει μίλια της Singapore Airlines, όπως για αναβαθμίσεις θέσεων σε πτήσεις. Η νομισματική αξία του ίδιου του κρυπτονομίσματος KrisPay υπαγορεύεται από την Singapore Airlines. Έτσι, η λύση που προσφέρει η KrisPay εδώ είναι να δώσει στους πελάτες έναν εύκολο τρόπο να εξαργυρώσουν τις ανταμοιβές τους για να αποτρέψουν μίλια από το να πάνε χαμένα μαζί με την εξοικονόμηση αυτών των κρυπτονομισμάτων στο εμπορικό δίκτυο. Κατά κάποιο τρόπο, οι πελάτες λαμβάνουν μια ψηφιακή προσθήκη/εναλλακτική στα νομίσματα που υποστηρίζονται από «χαρτονομίσματα χωρίς μεταλλική βάση» (fiat money).

Η λειτουργικότητα του KrisPay είναι απλή στη χρήση μέσω μιας εφαρμογής στην κινητή συσκευή σας και των άμεσων συναλλαγών στο σημείο πώλησης. Για να ενισχυθεί η περαιτέρω χρηστικότητα, τα μίλια KrisFlyer μπορούν να μεταφερθούν εντός της οικογένειας ή σε εξουσιοδοτημένους χρήστες.

Συνδυάζοντας τα πορτοφόλια blockchain και τα κρυπτονομίσματα, η KrisPay χρησιμοποιεί τα δυνατά στοιχεία της τεχνολογίας blockchain, όπως είναι η ασφάλεια σε όλους τους χρήστες, καθώς η καταχώριση των συναλλαγών πραγματοποιείται χωρίς τη δυνατότητα παραποίησης. Οι έμποροι έχουν αμέσως τις συναλλαγές τους εγκεκριμένες, χωρίς τη χρήση ενός πιο αργού ακριβότερου μεσάζοντος. Αυτό υποστηρίζει της πληρωμές μεταξύ των εμπόρων (και των οικονομικών τους διοικήσεων) και τους παρέχει επικαιροποιημένες πληροφορίες για τους πελάτες.

Το KrisPay αναπτύχθηκε από την KPMG Digital Village και τη Microsoft. Η KrisPay είναι μια ιδιωτική εταιρεία που ανήκει στην Singapore Airlines και «τρέχει» σε ένα περιβάλλον που συνδυάζει το Microsoft Azure (αρχικά βασισμένο στο πρωτόκολλο Ethereum) με την εφαρμογή Azure και λειτουργίες βάσης δεδομένων. Διαφορετικοί συνεργάτες διατηρούν και επαληθεύουν τη βάση δεδομένων blockchain έτσι ώστε ο καθένας να έχει τις πληροφορίες πελάτη/συναλλαγής διαθέσιμες ταυτόχρονα.

Η Microsoft ανακοίνωσε ότι θα αποσύρει το blockchain Azure το 2021 και θα υποστηρίξει τη μετάβαση των πελατών στην Quorum Blockchain Service, μια άλλη παραλλαγή του πρωτοκόλλου Ethereum (Microsoft, 2021).

Το κρυπτονόμισμα KrisPay και το πορτοφόλι συνδυάστηκαν σε μια νέα εφαρμογή το 2020, Kris+. Αυτή η εφαρμογή χρησιμοποιεί περαιτέρω δεδομένα πελατών προκειμένου η Singapore Airlines να εξυπηρετήσει καλύτερα τον πελάτη της, καθώς και να προσφέρει εξατομικευμένες προσφορές, ακόμη και με βάση τη γεωγραφική θέση από το κινητό τηλέφωνο.

Ενδεχομένως το πορτοφόλι KrisPay μπορεί να χρησιμοποιηθεί για την έκδοση εισιτηρίων, την απόδειξη της ψηφιακής σας ταυτότητας ή ως ένα περαιτέρω γενικό διακριτικό που μπορεί να χρησιμοποιηθεί για ανταλλαγή έναντι νομισμάτων τύπου fiat money, ή άλλων πόντων επιβράβευσης.

Συμπερασματικά, **όλες αυτές** οι **εφαρμογές** είναι διαχειρίσιμες σαφώς καθορισμένες περιπτώσεις blockchain που εφαρμόζονται προσεκτικά ως μέρος ενός ευρύτερου οράματος μέσα σε ένα περιβάλλον που οι εμπνευστές εμπιστεύονται και ελέγχουν. Οι περιπτώσεις δείχνουν σαφήνεια σχετικά με τα στοιχεία που θεωρούν ως ευκαιρία ή καμία ευκαιρία και

χρησιμοποιούν μια διαδικασία σταδιακής αλλαγής κατά την οποία εντείνουν την προσπάθεια από τα πρώτα προσεκτικά βήματα έως την πλήρη εφαρμογή.

Το περιβάλλον τους αποτελείται από σταθερές διαδικασίες, ένα γνωστό επιχειρηματικό μοντέλο και αξιόπιστους συνεργάτες για να πειραματιστούν με τις πιο δοκιμασμένες πτυχές της τεχνολογίας και τις αποκεντρωμένες επιχειρηματικές επιπτώσεις της.

Δεν υπήρχε χώρος για να γίνει επίδειξη ενός πλήρους αποκεντρωμένου επιχειρηματικού μοντέλου, αν θέλετε ένα παράδειγμα διαβάσετε το παράδειγμα της Augur Predication market στο Κεφάλαιο 16.5. (Lin Lim, Janse, 2021).

5.3 Πότε έχει νόημα η εφαρμογή του Blockchain;

Από τα προηγούμενα παραδείγματα είναι σαφές ότι πρέπει να υπάρχουν ορισμένες προϋποθέσεις για την επιτυχή εφαρμογή του blockchain.

Υπάρχουν ορισμένα κριτήρια που μπορείτε να εξετάσετε για να αποφασίσετε αν το blockchain είναι μια σημαντική υπόθεση για την επιχείρησή σας. Τα κριτήρια αυτά αποσκοπούν στην εξάλειψη των τριβών με τα δεδομένα ή την ροή των δεδομένων ή στη δημιουργία ευκαιριών με τα δεδομένα και την ροή δεδομένων μεταξύ των διαφόρων μερών. Κατά κανόνα, τα κριτήρια μπορούν να συνοψιστούν ως ακολούθως:

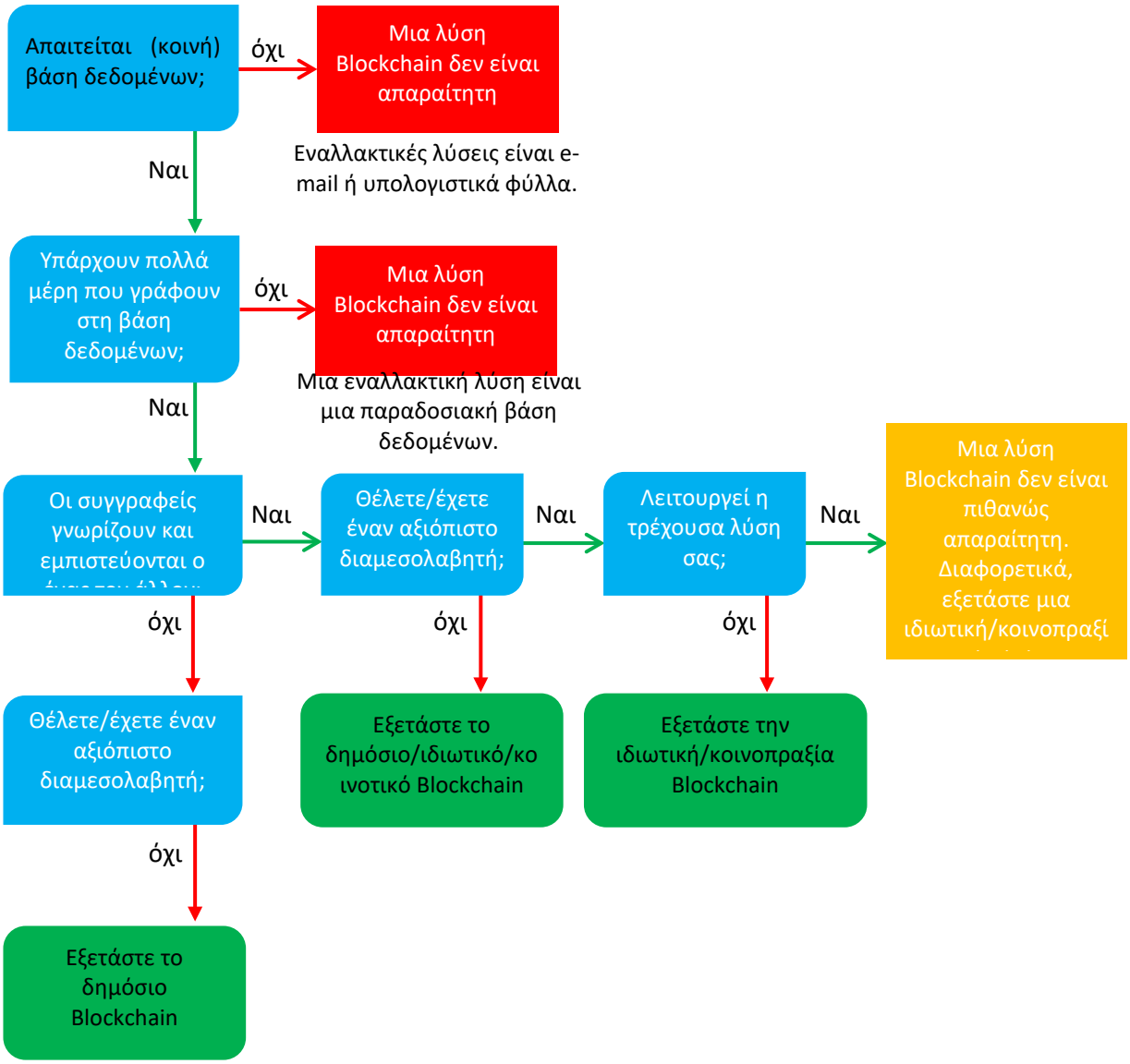
1. **Η ψηφιακή καινοτομία** αποτελεί μέρος της στρατηγικής.
2. Τα διάφορα μέρη **ανταλλάσσουν δεδομένα**.
3. Τα δεδομένα αυτά και οι συναλλαγές τους αφορούν **νομισματική αξία**.
4. Τα δεδομένα είναι **εμπιστευτικά**.
5. Διαφορετικά μέρη επεξεργάζονται δεδομένα.
6. Τα δεδομένα πρέπει να επαληθευθούν.
7. Υπάρχει **σαφής και επαρκής απόδοση της επένδυσης που** πρέπει να υπολογιστεί.
8. Η επαλήθευση είναι **πολύπλοκη, κοστίζει και ή απαιτεί χρόνο**.
9. Η λύση της επιλογής της τεχνολογίας blockchain είναι η **απλούστερη λύση** για να ξεπεραστεί το πρόβλημα.
10. Η λύση επηρεάζει την υπάρχουσα οργανωτική δομή.
11. Η λύση επηρεάζει την υπάρχουσα ροή εργασιών.
12. Η λύση επηρεάζει το υπάρχον οικοσύστημα.
13. Η τεχνική λύση είναι κοντά σε αυτή που δινόταν από υπάρχοντα συστήματα ή μπορεί να ενσωματωθεί σε υπάρχοντα συστήματα.
14. Η λύση είναι εντατική αλλά κλιμακούμενη. Σκεφτείτε τις διαφορές ανάμεσα σε 1k, 10k, 100k, 1 εκατομμύριο ή> 10 εκατομμύρια συναλλαγές ανά ώρα.

Μόλις δείτε την ευκαιρία να εφαρμόσετε την τεχνολογία blockchain με βάση αυτά τα κριτήρια, μπορείτε να προχωρήσετε στην κατανόηση των υποκείμενων υπηρεσιών κοινής ωφέλειας χρηστών που απαιτούνται καθώς και των δομικών μπλοκ που συνθέτουν αυτές τις υπηρεσίες κοινής ωφέλειας. Για παράδειγμα, το δομικό μπλοκ «μέσο πληρωμής» έχει αντίκτυπο στην ευκολία, την ταχύτητα και τη διαφάνεια των πράξεων πληρωμής. Άλλα παραδείγματα δομικών μπλοκ είναι τα «πορτοφόλια», τα έξυπνα συμβόλαια, dApps, τύποι μπλοκ, oracles, και ούτω καθεξής.

Επί του παρόντος, ο αντίκτυπος του blockchain στις εταιρείες επικεντρώνεται κυρίως στην αποτελεσματικότητα, την αποδιαμεσολάβηση και την καταχώριση. Και ο αντίκτυπος είναι

υψηλότερος εκεί όπου τα συνεργαζόμενα μέρη ξεκλειδώνουν και δημιουργούν νέα δεδομένα. Στο μέλλον, ωστόσο, οι πολύπλοκες εφαρμογές blockchain που οδηγούν στην αποκέντρωση και την ολοκλήρωση των οικοσυστημάτων αναμένεται να δουν τα μεγαλύτερα οφέλη του blockchain.

Μπορείτε να χρησιμοποιήσετε το ακόλουθο απλοποιημένο δέντρο αποφάσεων για να εκτιμήσετε τη χρήση ενός έργου Blockchain:



Σχήμα 12: Απλοποιημένο δέντρο αποφάσεων είτε πρέπει να χρησιμοποιηθεί το Blockchain είτε όχι (Πηγή: Lin Lim, C., Janse, A., Blockchain Basics, 2021).

6 Αναφορές και πηγές για περαιτέρω ανάγνωση

Ackermann, J. & Meier, M. (2018). *Blockchain 3.0: Η επόμενη γενιά συστημάτων Blockchain.*

Προηγμένο σεμινάριο Blockchain Technologies, Θερινός Όρος 2018, Πολυτεχνείο Munch.

PAI Sweden, Lantmäteriet (2020, Νοέμβριος). *Δημιουργία ενός μοντέλου εμπιστοσύνης TN για τον δημόσιο τομέα,*

Συμβουλευθείτε από τη διεύθυνση https://www.ai.se/en/node/85154

Αντωνόπουλος, Α. Μ. (2016). *Το Διαδίκτυο των Χρημάτων: μιλάτε από τον*. Merkle Bloom Llc.

Ο Ογκούρ. (n.d.). Η*Επισκόπηση*. Ζητήθηκε η γνώμη της στις 23 Δεκεμβρίου 2019, από τη διεύθυνση https://docs.augur.net/#overview

Ο Ογκούρ. (2018, 9 Ιουλίου). *Προγνωστικό Ίδρυμα ΟΥ Πολιτική Προστασίας Προσωπικών Δεδομένων*. Ζητήθηκε η γνώμη του στις 23 Δεκεμβρίου 2019, από τον ιστότοπο Augur.net: https://www.augur.net/privacy-policy/

Baraniuk, C. (2020, 11 Φεβρουαρίου). Το*Blockchain: Η επανάσταση που δεν έχει συμβεί*. Συμβουλευθείτε από τη διεύθυνση https://www.bbc.com/news/business-51281233

Bitcoin Block Ανταμοιβή κατά το ήμισυ Αντίστροφη μέτρηση. (2019). Ζητήθηκε η γνώμη τους στις 23 Δεκεμβρίου 2019, από

Bitcoinblockhalf.com ιστοσελίδα: http://www.bitcoinblockhalf.com

BMW, (2019, 14 Οκτωβρίου). Πώς οι λύσεις Blockchain μπορούν να βοηθήσουν τον οδηγό Συμβουλευθείτε από τη διεύθυνση https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW Pressclub Global (2020, 31 Μαρτίου). *Το BMW Group χρησιμοποιεί το Blockchain για να προωθήσει τη διαφάνεια της εφοδιαστικής αλυσίδας.* Ζητήθηκε η γνώμη της διεύθυνσης https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency.

Buterin, V. (2013). Λευκή Βίβλος*Ethereum: ένα έξυπνο συμβόλαιο επόμενης γενιάς και μια αποκεντρωμένη πλατφόρμα εφαρμογών* [Λευκή Βίβλος]. Ζητήθηκε η γνώμη της Blockchainlab στις 27 Δεκεμβρίου 2019: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, 6 Μαΐου). *DAOs, DACs, DAs και άλλα: Ένας ατελής οδηγός ορολογίας.*

Ζητήθηκε η γνώμη του στις 27 Δεκεμβρίου 2019, από τον ιστότοπο του Ethereum.org: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Το ChainTrade. (2017, 27 Δεκεμβρίου*). 10 Πλεονεκτήματα από τη χρήση έξυπνων συμβάσεων*. Διαβούλευση σχετικά με

27 Δεκεμβρίου 2019, από την ιστοσελίδα Medium: κατηγορία:Πλεονεκτήματα χρήσης-έξυπνες συμβάσεις-bc29c508691a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Το Bitcoin και η άνοδος

αποκεντρωμένων αυτόνομων οργανισμών. Journal of Organization Design, 7(1).

https://doi.org/10.1186/s41469-018-0038-1

Το μέλλον του Kaoris. (2017) *The Land Registry in the blockchain — testbed*. Συμβουλευθείτε από τη διεύθυνση https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Μέλλον. (2016). *Το κτηματολόγιο στο blockchain.* Συμβουλευθείτε από τη διεύθυνση http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Καθολικό Insights (2020, 31 Μαρτίου). H*BMW επεκτείνει το blockchain της εφοδιαστικής αλυσίδας για την ιχνηλασιμότητα εξαρτημάτων.* Συμβουλευθείτε από τη διεύθυνση https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, 15 Οκτωβρίου), η *Singapore Airlines επεκτείνει το ψηφιακό πορτοφόλι ανταμοιβής που βασίζεται σε blockchain*. Διαβούλευση στη διεύθυνση https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook*, Σεπτέμβριος 2021, κεφάλαιο 10. Εκδότης: De boekdrukker Άμστερνταμ. ΤΟ NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

Microsoft, 2021, 14 Μαΐου). H*δράση που απαιτείται: Μεταναστεύστε τα δεδομένα της υπηρεσίας Azure Blockchain έως τις 10 Σεπτεμβρίου 2021*. Διαβούλευση στη διεύθυνση https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, Μάιος 2), *Singapore Airlines μεταμορφώνει την αφοσίωση των πελατών με blockchain στο Azure*. Διαβούλευση στις 4

ΤΟ ΜΌΜΠΙ. (2019). *Πρότυπο ταυτότητας οχήματος*. Συμβουλευθείτε από τη διεύθυνση https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Νακαμότο, Σ. (2008). *Bitcoin P2P e-cash χαρτί.* Ζητήθηκε η γνώμη τους στις 23 Δεκεμβρίου 2019, από

Ιστοσελίδα του Metzdowd.com: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, 30 Σεπτεμβρίου). *Σχετικά με: Έσπασα το πορτοφόλι μου, δεν το επιβεβαιώνω ποτέ.* [Online]

σχόλιο του φόρουμ]. Το μήνυμα δημοσιεύτηκε στο https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, Νοέμβριος 1). H*πρόσφατη διακοπή ρεύματος του PayPal οδηγεί την υιοθέτηση bitcoin*.

Ζητήθηκε η γνώμη του στις 23 Δεκεμβρίου 2019, από τον ιστότοπο Bravenewcoin.com: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Bear, K., McKeon, S. (2019). 2η *μελέτη συγκριτικής αξιολόγησης Global Enterprise Blockchain*. Συμβουλευθείτε από τη διεύθυνση https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, 7 Δεκεμβρίου). *Αλλαγή της αγοράς ακινήτων μέσω blockchain*. Συμβουλευθείτε από τη διεύθυνση https://delano.lu/article/delano_changing-property-market-through-blockchain

Ο Στρατηγός. (n.d.) *Επιχειρηματικό μοντέλο καμβά*. Ζητήθηκε η γνώμη της στις 23 Δεκεμβρίου 2019, από τη διεύθυνση https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U., & Lakhani, R. (2018). *Εννοιολογικά Blockchains: Χαρακτηριστικά & Τις εφαρμογές*. 11ο Διεθνές Συνέδριο Πληροφοριακών Συστημάτων IADIS 2018, 49-57

Vigna, P., & Casey, M. (2015). *Η ηλικία του cryptocurrency: πώς είναι το Bitcoin και το blockchain αμφισβήτηση της παγκόσμιας οικονομικής τάξης*. Νέα Υόρκη, N.Y.: Picador/St. Martin's Press.

Young, S. (2018). *Επιβολή των Συνταγματικών Δικαιωμάτων μέσω του Κώδικα Ηλεκτρονικών Υπολογιστών.* Γνωμοδοτήθηκε από Cua Law Scholarship Repository Δικτυακός τόπος: https://scholarship.law.edu/jlt/vol26/iss1/5/

Παράρτημα Ι — Γλωσσάριο όρων

51 % επίθεση: Μια επίθεση στο blockchain που επιτυγχάνεται κερδίζοντας περισσότερο από το 51 % της υπολογιστικής ισχύος του δικτύου.

Πρότυπο πελάτη-εξυπηρετητών: Το μοντέλο όπου οι πελάτες (χρήστης) είναι συνδεδεμένοι σε έναν εξυπηρετητή. Ο εξυπερητητής περιέχει δεδομένα σχετικά με τους πελάτες. Οι πελάτες συνδέονται με το εξυπερητητή για να έχουν πρόσβαση σε αυτά τα δεδομένα. Αυτό κάνει τους πελάτες να εξαρτώνται από το εξυπηρετητή.

Τεχνολογία κατανεμημένου μητρώου (DLT): Τεχνολογία κατανεμημένου μητρώου.

Διπλές δαπάνες: Ξοδεύουμε δύο φορές ένα Bitcoin. Για παράδειγμα, κατέχετε ακριβώς ένα Bitcoin, αλλά στέλνετε ένα Bitcoin στο άτομο Α και ένα Bitcoin στο άτομο Β.

Πλήρης κόμβος: Ένας κόμβος που έχει ένα πλήρες αντίγραφο του blockchain.

Εξορύκτης: Ένας υπολογιστής που παρέχει υπολογιστική ισχύ για την παραγωγή ενός έγκυρου μπλοκ. Ένα μπλοκ είναι έγκυρο μόνο αν βρει ένα nonce που οδηγεί σε μια έγκυρη κατακερματισμένη τιμή (hash value).

Κόμβος: Συσκευή που είναι συνδεδεμένη σε δίκτυο υπολογιστών.

P2P: Δείτε peer-to-peer.

Peer-to-peer (δίκτυο ομότιμων κόμβων) : Ένα δίκτυο υπολογιστών όπου οι υπολογιστές είναι ισότιμοι μεταξύ τους και μπορούν να προσφέρουν ο ένας στον άλλον υπηρεσίες.

Απόδειξη εργασίας (Proof-of-Work): Ένας μηχανισμός συναίνεσης που απαιτεί από τους εξορύκτες να χρησιμοποιούν την ισχύ του υπολογιστή για να βρουν τη έγγυρη κατακερματισμένη τιμή για ένα νέο μπλοκ. Με την εύρεση της σωστής κατακερματισμένης τιμής, τους επιτρέπεται να προσθέσουν το μπλοκ στο blockchain και να λάβουν μια ανταμοιβή.

Μοναδικό σημείο αποτυχίας (SPOF): Το τμήμα ενός δικτύου που σταματά τη λειτουργία ολόκληρου του δικτύου σε περίπτωση βλάβης.

SPOF: Δείτε το μοναδικό σημείο αποτυχίας.

Αξιόπιστο τρίτο μέρος (TTP): Έμπιστος διαμεσολαβητής.

ΤΟ TTP: Δείτε τα έμπιστα τρίτα μέρη.

Λευκή Βίβλος: Ένα έγγραφο που περιγράφει τον τρόπο επίλυσης ενός συγκεκριμένου προβλήματος. Ο Satoshi Nakamoto έγραψε στη Λευκή Βίβλο του Bitcoin πώς το Bitcoin λύνει το πρόβλημα της διπλής δαπάνης σε ένα κατανεμημένο δίκτυο.

Blockchain 1.0: Η πρώτη γενιά blockchains που έχουν χρησιμοποιηθεί κυρίως για τη διευκόλυνση της αποθήκευσης και της μεταφοράς κρυπτονομισμάτων.

Blockchain 2.0: Η δεύτερη γενιά blockchains που επικεντρώνεται περισσότερο στην ενεργοποίηση έξυπνων συμβολαίων, dApps και DAOs.

Blockchain 3.0: Η τρίτη γενιά των blockchains που έχουν λύσει ένα σύμπλεγμα ζητημάτων που το blockchain 2.0 εξακολουθεί να έχει να αντιμετωπίσει. Παραδείγματα τέτοιων ζητημάτων είναι η επεκτασιμότητα, η διαλειτουργικότητα, η ιδιωτικότητα, η βιωσιμότητα και η διακυβέρνηση.

Αέριο: Κόστος συναλλαγής για την εκτέλεση μιας συναλλαγής στο blockchain Ethereum.

Αποκεντρωμένη εφαρμογή (dApp): Μια εφαρμογή που χρησιμοποιεί την αποκεντρωμένη αποθήκευση δεδομένων ενός έργου blockchain. Η εφαρμογή δεν εκτελείται μέσω κεντρικού εξυπηρετητή, αλλά μέσω αποκεντρωμένου δικτύου κόμβων. Ακριβώς όπως μια κανονική εφαρμογή, έχει συχνά μια διεπαφή και μια διεπαφή χρήστη.

Αποκεντρωμένη Αυτόνομη Οργάνωση (DAO): Μια αυτόνομη οντότητα που βασίζεται επίσης στην πρόσληψη ατόμων. Αυτά τα άτομα μπορούν να εκτελέσουν ορισμένα απαραίτητα καθήκοντα που η οντότητα δεν μπορεί. Το DAO έχει στη διάθεσή του εσωτερικό κεφάλαιο για το σκοπό αυτό, με το οποίο ορισμένες δραστηριότητες αυτών των ατόμων μπορούν να ανταμειφθούν. Αυτό που κάνει μια DAO θεμελιωδώς διαφορετική από μια κεντρική οργάνωση είναι ότι δεν έχει μια ανώτατη διευθυντική ομάδα ή έναν CEO. Είναι μια μη ιεραρχική οργάνωση.

Έξυπνο συμβόλαιο: Συμβόλαιο με ορισμένους όρους και προϋποθέσεις που καθορίζονται στον κώδικα. Το συμβόλαιο αυτοεκτελείται, δηλαδή εκτελεί το ίδιο τις κατάλληλες αντίστοιχες ενέργειες όταν πληρούνται οι όροι και οι προϋποθέσεις. Ωστόσο, το συμβόλαιο πρέπει να περιέχει επαρκείς πληροφορίες από κάθε συμβαλλόμενο μέρος που συμμετέχει στο συμβόλαιο, ώστε να στερεί τα μέρη από τη δυνατότητά τους να καταγγείλουν το συμβόλαιο. Υπάρχουν δύο τύποι έξυπνων συμβολαίων: ντετερμινιστικό και μη ντετερμινιστικό.

Solidity: Η γλώσσα προγραμματισμού αναπτύχθηκε ειδικά για το Ethereum για να γράψει έξυπνα συμβόλαια.