

Διοίκηση Πληροφοριακών Συστημάτων

Web 3.0 - τεχνολογίες που το χαρακτηρίζουν, χαρακτηριστικά του, υπηρεσίες που μπορεί να προσφέρει καθώς και τα πλεονεκτήματα και μειονεκτήματα ή περιορισμούς που ενέχει.



Ακαδ. Έτος 2021-2022
Νικόλαος Ρέκκας - icsd 16164

Περιεχόμενα

1. Τι είναι το Web3.0; - Τεχνολογίες και Χαρακτηριστικά
2. Υπηρεσίες και Εφαρμογές
3. Πλεονεκτήματα / Μειονεκτήματα
4. Συμπεράσματα

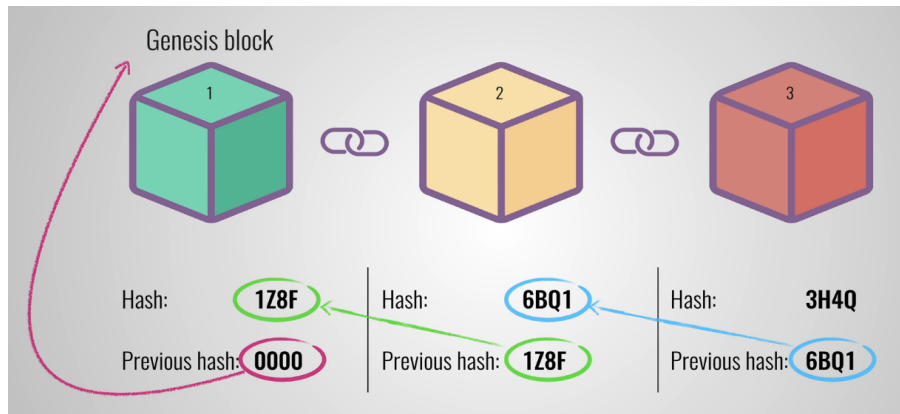
1. Τι είναι το Web3.0; - Τεχνολογίες και Χαρακτηριστικά

Όπως πολλοί αποκαλούν, το Web3.0 είναι η επόμενη φάση του διαδικτύου/παγκόσμιου ιστού. Το Web3.0 ή Web3 ονομάζεται αλλιώς και σαν Σημασιολογικός Ιστός (Semantic Web) και οι τεχνολογίες που αναπτύσσονται γύρω από αυτό είναι καινοτόμες και διαρκώς εξελίσσονται. Ο όρος Web3 επινοήθηκε από τον Gavin Wood (co-founder του Ethereum) το 2014 και αναφέρεται σε ένα online αποκεντροποιημένο οικοσύστημα το οποίο βασίζεται στην τεχνολογία του Blockchain. Για να γίνει κατανοητό το Web3 θα πρέπει πρώτα να γίνει μια σύντομη περιγραφή της ιστορίας του Παγκόσμιου Ιστού.

Η ιστορία ξεκινάει με την εφεύρεση του Παγκόσμιου Ιστού (World Wide Web) από τον Tim Berners-Lee το 1989 στο CERN όπου και δούλευε. Τα εργαλεία που ανέπτυξε για να γίνει εφικτή η χρήση του Παγκόσμιου Ιστού ήταν 1) το *HTTP* για την σωστή επικοινωνία client-server, 2) η *HTML* η οποία χρησιμοποιήθηκε για την προβολή αρχείων στους web-browsers, 3) τον πρώτο web-browser με όνομα *WorldWideWeb* και ύστερα με το όνομα *Nexus* και τέλος 4) τον πρώτο διακομιστή (server) *CERN httpd*. Οι παραπάνω τεχνολογίες έκαναν εφικτό το επονομαζόμενο και ως **Web 1.0** (1989-2004) το οποίο σε επίπεδο χρήστη ήταν μόνο "read-only", δηλαδή ο χρήστης μέσα στον browser και μέσω ενός hyperlink είχε την δυνατότητα μόνο να διαβάσει αρχεία (δλδ στατικές ιστοσελίδες).

Ο παγκόσμιος ιστός μέχρι και αυτή τη χρονική στιγμή την οποία διαβαίνουμε σήμερα (2004-2022) αναφέρεται και ως **Web 2.0** ή αλλιώς και "read-write" Ιστός. Η διαφορά με τον προκάτοχό του, τον "read-only" Ιστό είναι η δυνατότητα που έχουν πλέον οι χρήστες να δημιουργούν περιεχόμενο, δηλαδή έχουν την δυνατότητα για τροποποίηση/εισαγωγή δεδομένων (Blogs), την επικοινωνία με άλλους χρήστες (Social Media), τις ηλεκτρονικές πληρωμές (E-Banking), την ανταλλαγή εικόνας και βίντεο αλλά και εφαρμογές που διαθέτουν υπηρεσίες (π.χ cloud services) κ.α. Αυτό που έκανε εφικτό τα παραπάνω ήταν ουσιαστικά μια αναβάθμιση του Web 1.0 με καινούργιες τεχνολογίες, πρωτόκολλα, πρότυπα (π.χ. *World Wide Web Consortium (W3C)*) που εξελίχθηκαν, καθώς και καινούργιες αρχιτεκτονικές σχεδίασης (π.χ. *Web-oriented architecture (WOA)*). Κάποιες τεχνολογίες που αξίζει να σημειωθούν είναι: 1) Ajax, 2) HTML5, 3) και Web Frameworks τα οποία έχουν αυξήσει την ευκολία (high-level) και τον προγραμματισμό διαδικτυακών τόπων (Backend -> Django, Node JS, Frontend -> React, Vue κ.α).

Οι μέχρι και σήμερα υπηρεσίες, που προσφέρονται από το Web1.0 και Web2.0, είναι κεντριοποιημένες, δηλαδή όλα τα δεδομένα/περιεχόμενο που παράγονται από τους χρήστες των ιστότοπων ή και αυτό που οι ίδιες προσφέρουν ανήκει σε αυτές. Το παραπάνω, σε συνδυασμό με την συσσώρευση της παγκόσμιας πληροφορίας σε ένα μικρό αριθμό εταιρειών (Big Tech -> Apple/Google/Facebook/Twitter/Amazon), έχει δημιουργήσει μια ανασφάλεια/αναξιοπιστία των χρηστών απέναντι στον τρόπο, που αυτές οι εταιρείες επεξεργάζονται/αποθηκεύουν τα δεδομένα τους. Το Web3 έχει 'έρθει' να αλλάξει τον τρόπο με τον οποίο τα δεδομένα επεξεργάζονται και αποθηκεύονται, προσφέροντας έτσι, μεγαλύτερη ασφάλεια στα δεδομένα (data security), επεκτασιμότητα (scalability) και ιδιωτικότητα (privacy) για τους χρήστες. Όπως προαναφέρθηκε το Web3, βασίζεται στην τεχνολογία του Blockchain και των Peer-to-Peer δικτύων για να παρέχει αποκεντροποιημένες εφαρμογές (DAPPS, DAO), καθώς token-based οικονομικά μοντέλα/σχήματα (βλ. NFT, DeFi). Για να μπορέσουν να γίνουν κατανοητές αυτές οι τεχνολογίες, πρέπει να δούμε τι είναι το Blockchain, για ποιο σκοπό χρησιμοποιήθηκε (πότε; από ποιον; και γιατί;), όπως επίσης και τι είναι τα Smart Contracts.



Τεχνολογίες

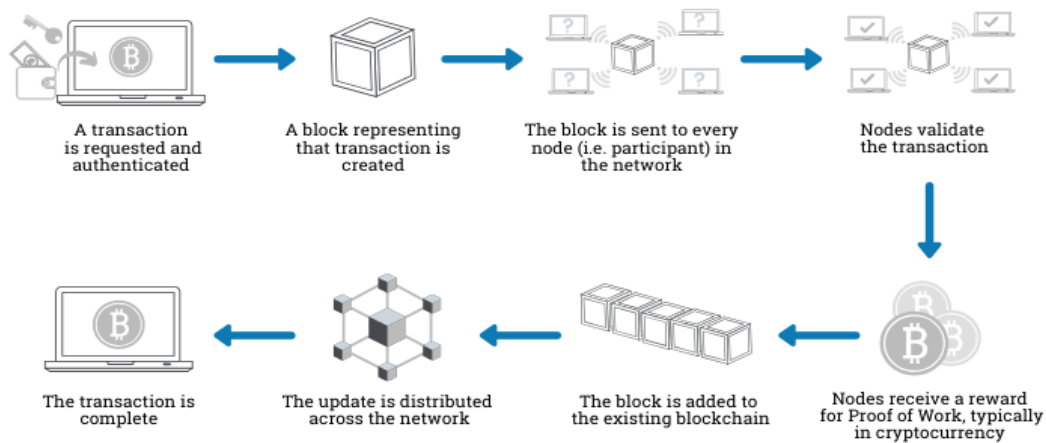
Το Blockchain όπως λέει και το όνομα είναι μια αλυσίδα από block που περιέχουν πληροφορία, θα μπορούσαμε να πούμε ότι είναι μια δημόσια βάση δεδομένων, η οποία μένει συνεχώς ανανεωμένη και διαμοιράζεται στους υπολογιστές που απαρτίζουν το δίκτυο. Η έννοια του Blockchain πρωτοεμφανίστηκε το 1991 από ένα γκρουπ ερευνητών και στην πραγματικότητα ο σκοπός του ήταν να χρονosφραγίσει (timestamps) ψηφιακά δεδομένα με κρυπτογραφικό τρόπο ώστε κανένας να μην μπορεί να αλλάξει την ημερομηνία καθώς τα ίδια τα δεδομένα. Παρόλα αυτά το Blockchain έγινε γνωστό από το White Paper που έγραψε ο 'Satoshi Nakamoto' (ψευδώνυμο) το 2009 με τίτλο "Bitcoin: A Peer-to-Peer Electronic Cash System". Όπως γίνεται κατανοητό και από τον τίτλο το paper παρουσιάζει μία peer-to-peer έκδοση ενός ηλεκτρονικού τρόπου πληρωμών, οι οποίες θα γίνονται απευθείας χωρίς την ύπαρξη κάποια ενδιάμεσου χρηματοπιστωτικού ιδρύματος.

Το Blockchain είναι καθολικά κατανεμημένο σε όλους στο δίκτυο, και οποιαδήποτε αλλαγή στις πληροφορίες που αποθηκεύονται σε κάθε block είναι πάρα πολύ δύσκολο να αλλαχτεί (υπολογιστικά αδύνατο ή τουλάχιστον οι πόροι που χρειάζονται για να γίνει αυτό είναι τεράστιοι). Αυτό συμβαίνει λόγω κάποιων ιδιοτήτων που έχουν τα block που απαρτίζουν το blockchain. Κάθε block περιέχει κάποια δεδομένα. Κάποια από τα δεδομένα που αποθηκεύονται, είναι αυτά που σχετίζονται με το ποιος στέλνει τα bitcoin, με το ποιος τα λαμβάνει καθώς και το ποσό που μεταβιβάζεται (transactions data). Ακόμα αποθηκεύεται το Hash του Block, καθώς και το Hash του προηγούμενου Block. Το hash του Block χρησιμοποιείται για να αναγνωρίζεται η μοναδικότητα που έχει το κάθε Block, μιας και κάθε Hash είναι μοναδικό. Το hash του προηγούμενου Block που αποθηκεύεται είναι αυτό που δημιουργεί την αλυσίδα των Block μιας και κάνει την σύνδεση μεταξύ τους. Αν κάποιος προσπαθήσει να αλλάξει τα δεδομένα αυτόματα θα αλλάξει και το Hash που χαρακτηρίζει το Block, με αποτέλεσμα να σπάσει η σύνδεση μεταξύ των Block, με αποτέλεσμα ο κακόβουλος χρήστης να χρειάζεται να επανα υπολογίσει όλα τα Hash των υπόλοιπων Block, για να ξαναφτιαχτεί η αλυσίδα, κάτι που είναι σχεδόν υπολογιστικά αδύνατο (τουλάχιστον τη συγκεκριμένη χρονική περίοδο).

Η διαδικασία που χρειάζεται για να φτιαχτεί ένα νέο Block λέγεται Proof-of-Work, είναι πολύ ενεργοβόρα και χρονοβόρα μιας και κάθε block χρειάζεται περίπου 10 λεπτά για να μπει στην αλυσίδα (στο δίκτυο του Bitcoin). Ο λόγος για τον οποίο, ο χρόνος που χρειάζεται είναι μεγάλος είναι, γιατί κάθε φορά επιλύεται ένα 'δύσκολο μαθηματικό puzzle' το οποίο χρησιμοποιεί αρκετούς υπολογιστικούς πόρους (κατάλληλο Hardware για mining) και αυτό είναι που ονομάζεται Mining. Το Blockchain χρησιμοποιεί P2P δίκτυα και οποιοσδήποτε

επιτρέπεται να είναι σε αυτό το δίκτυο (Public Blockchain). Όταν εισέρχεται κάποιος στο δίκτυο αυτός γίνεται κόμβος και λαμβάνει ένα πλήρες αντίγραφο του Blockchain, έτσι κάθε κόμβος μπορεί να επιβεβαιώσει ότι η αλυσίδα είναι σωστή και ότι κανένας δεν έχει προσπαθήσει να αλλάξει κάτι. Στην πραγματικότητα για κάθε νέο Block που είναι να προστεθεί στην αλυσίδα στέλνεται broadcast σε όλους τους κόμβους του δικτύου, γίνεται έλεγχος και επαλήθευση από όλους και τέλος όλοι ανανεώνουν τη κατάσταση του Blockchain.

How does a transaction get into the blockchain?



© Euromoney Learning 2020

Μια τεχνολογία που είναι αρκετά πρώιμη ακόμα είναι τα Smart Contracts ή Έξυπνα Συμβόλαια. Τα έξυπνα συμβόλαια είναι εκτελέσιμος κώδικας ο οποίος αποθηκεύεται στο Blockchain. Ο όρος έξυπνα συμβόλαια χρησιμοποιήθηκε πρώτη φορά από τον Nick Szabo, το 1997 και ο στόχος του ήταν να χρησιμοποιήσει τη τεχνολογία κατακεντρωμένου καθολικού (δλδ, Distributed Ledger Technology) όπου θα αποθηκεύονται συμβόλαια. Τα έξυπνα συμβόλαια, όπως προαναφέρθηκε είναι προγράμματα/εκτελέσιμος κώδικας, ο οποίος ενεργοποιείται και εκτελείται, όταν ικανοποιηθούν συγκεκριμένες συνθήκες και οι κινήσεις καταγράφονται στο blockchain καθιστώντας την πληροφορία αμετάβλητη και αδιαμφισβήτητη. Αξίζει να σημειωθεί πως τα smart contracts μπορούν να εκτελέσουν και να επεξεργαστούν δεδομένα πάνω στο Blockchain εκτελούμενα είτε αυτόματα είτε έπειτα από κάποιο ερέθισμα το οποίο μπορεί να έρθει από μια συσκευή IoT ή από ένα εξωτερικό ERP πρόγραμμα. Ένα παράδειγμα έξυπνου συμβολαίου είναι το εξής, “Ένα φορτηγό μεταφέρει ευπαθή προϊόντα από το μέρος Α στο Β. Το συμβόλαιο μεταφοράς λέει ότι η θερμοκρασία δεν πρέπει να ανέβει πάνω από τους -10 βαθμούς κελσίου. Αν για κάποιο λόγο η θερμοκρασία αυτή ανέβει και γίνει -8 βαθμοί κελσίου τότε αυτόματα ένας αισθητήρας ενημερώνει το Blockchain και ένα έξυπνο συμβόλαιο “ξυπνάει” και καταγράφει την κίνηση αυτή. Ο τελικός παραλήπτης γνωρίζει ότι η θερμοκρασία μεταβλήθηκε και μπορεί να ασκήσει ποινικές ρήτρες όπως ορίζει το συμβόλαιο που έχει συμφωνήσει.”.

Η κατακεντρωμένη δομή του προγράμματος και η ταυτόχρονη εκτέλεση αυτού σε όλους τους κόμβους του δικτύου αποτρέπει την εκτέλεση του από ένα κόμβο ο οποίος μπορεί να έχει πέσει θύμα κυβερνοεπίθεσης και αυτός είναι ο λόγος που η παραποίηση της πληροφορίας είναι αδύνατη. Ωστόσο, ένα αρνητικό που προκύπτει από τα παραπάνω, είναι πως χρειάζεται πολύ προσεκτική

μελέτη της αρχιτεκτονικής της εφαρμογής που θα υλοποιηθεί σε έξυπνα συμβόλαια και αυτό γιατί οι μεταγενέστερες αλλαγές στο κώδικα είναι αδύνατες.



Οι αποκεντρωποιημένες εφαρμογές ή αλλιώς και DAPP's που απαρτίζουν το Web3, βασίζονται στις παραπάνω τεχνολογίες. Αποκεντροποιημένη εφαρμογή (dapp) είναι μια εφαρμογή που έχει 'χτιστεί πάνω' σε P2P δίκτυα και συνδυάζει τα έξυπνα συμβόλαια αλλά και κάποια διεπαφή για τον χρήστη. Ουσιαστικά, ο backend κώδικας τρέχει σε αποκεντρωποιημένο peer-to-peer δίκτυο, σε αντίθεση με τις συμβατικές αρχιτεκτονικές όπου ο backend κώδικας τρέχει σε κεντροποιημένους servers. Η διεπαφή (frontend) μπορεί και αυτή με τη σειρά να υλοποιηθεί και να γίνει hosted σε κάποια αποκεντρωποιημένη βάση δεδομένων (π.χ στο [IPFS](#)). Κάποια χαρακτηριστικά αυτών των εφαρμογών, είναι:

1. η *αποκεντρωμένη φύση* που τις χαρακτηρίζει, αφού δεν υλοποιούνται και τρέχουν σε κάποιο κεντροποιημένο σύστημα
2. *ντετερμινιστικές*, αφού εκτελούν τις ίδιες λειτουργίες ανεξάρτητα του περιβάλλοντος στο οποίο εκτελούνται
3. *Turing complete*, δηλαδή μπορούν να εκτελέσουν οποιαδήποτε λειτουργία (ανεξάρτητα πολυπλοκότητας), έχοντας τους κατάλληλους πόρους
4. *απομονωμένες*, επειδή εκτελούνται σε εικονικά περιβάλλοντα - στην περίπτωση του Ethereum, εκτελούνται στο EVM (Ethereum Virtual Machine) - και σε περίπτωση εμφάνισης προβλήματος ενός smart contract, δεν επηρεάζεται το δίκτυο blockchain.

Ωστόσο, πριν από τις τεχνολογίες που αναφέρονται παραπάνω, δηλαδή τα blockchain, smart contracts, οι οποίες καθορίζουν το Web3, υπήρχε είδη το όραμα της τρίτης γενιάς του παγκόσμιου ιστού με όνομα Web3.0 ή αλλιώς και Σημασιολογικό Ιστό. Τον όρο, τον εισήγαγε πρώτος, ο Tim Berners-Lee το 1999 και το όραμα που είχε ήταν τα διαδικτυακά δεδομένα να μπορούσαν να γίνουν κατανοητά από τους υπολογιστές (machine-readable data). Ο τρόπος με τον οποίο μπορεί να γίνει αυτό είναι μέσω των 'μεταδεδομένων', επεκτείνοντας τα δεδομένα έτσι σημασιολογικά. Οι τεχνολογίες που χρησιμοποιούνται για αυτή τη διαδικασία είναι η XML, RDF (Resource Description Framework), OWL (Web Ontology Language) και JSON-LD. Μέσω των σημασιολογικών δεδομένων αποκτούν νόημα τα δεδομένα των οντοτήτων που αποθηκεύονται στις βάσεις δεδομένων, έτσι η αφαιρετικότητα που τα καθορίζει τους δίνει ένα τρόπο συσχέτισης με τον πραγματικό κόσμο. Τα σημασιολογικά μοντέλα - σε αντίθεση με τα αντικειμενοστραφή (object-oriented)- είναι προσανατολισμένα στα γεγονότα (fact-oriented). Τα γεγονότα εκφράζονται συνήθως με δυαδικές σχέσεις μεταξύ στοιχείων των δεδομένων, ενώ οι σχέσεις υψηλότερης τάξης εκφράζονται ως συλλογές δυαδικών σχέσεων. Οι

δυναμικές σχέσεις έχουν τη μορφή τριπλέτων: Αντικείμενο - Τύπος Σχέσης - Αντικείμενο, π.χ Ο πύργος του Άιφελ <βρίσκεται> στο Παρίσι.

Η διασύνδεση μεταξύ διαφορετικών δεδομένων, με τρόπο που είναι κατανοητός, όχι μόνο από τους ανθρώπους αλλά και από τις μηχανές, γίνεται εφικτός με αυτό που ονομάζεται Linked Data. Τα Linked Data ή αλλιώς και συνδεδεμένα δεδομένα είναι ένα σύνολο με σχεδιαστικές αρχές για να μοιράζονται machine-readable διασυνδεδεμένα δεδομένα στον Παγκόσμιο Ιστό. Οι τέσσερις σχεδιαστικές αρχές που προτάθηκαν από τον Tim Berners-Lee για τα διασυνδεδεμένα δεδομένα το 2006 είναι οι εξής:

1. χρήση των URIs για ονοματοδοσία στο Web
2. χρήση του HTTP για τα URIs ώστε οι άνθρωποι να μπορούν να ψάξουν για δεδομένα
3. παροχή χρήσιμων πληροφοριών, χρησιμοποιώντας standards όπως RDF, SPARQL, όταν κάποιος αναζητάει ένα URI
4. χρήση ενσωματωμένων link μέσα σε URIs ώστε να γίνεται εύκολη η ανακάλυψη νέας πληροφορίας

Τέλος, αξίζει να σημειωθεί, ότι εκτός από τα διασυνδεδεμένα δεδομένα υπάρχουν και τα ανοιχτά δεδομένα (Open Data). Τα ανοιχτά δεδομένα, είναι δεδομένα τα οποία μοιράζονται ελεύθερα και καταναμημένα από τον οποιονδήποτε. Ο συνδυασμός αυτών των δύο τύπων δεδομένων είναι τα ανοιχτά διασυνδεδεμένα δεδομένα (Linked Open Data).



Χαρακτηριστικά

Κάποια από τα χαρακτηριστικά που διακρίνονται από την ανάλυση των παραπάνω τεχνολογιών είναι τα παρακάτω:

Trustless and permissionless: τα αποκεντρωμένα δίκτυα και ο ανοιχτός κώδικας (open source), επιτρέπει στους χρήστες που απαρτίζουν το Web3.0, να μπορούν να επικοινωνούν απευθείας χωρίς να χρειάζεται να εμπιστεύονται κάποιον ενδιάμεσο. Επίσης, δίνεται η συμμετοχική δυνατότητα των χρηστών, χωρίς να χρειάζεται η εξουσιοδότηση κάποιας κεντροποιημένης υπηρεσίας.

Artificial intelligence (AI) and machine learning: στο Web3.0, ο συνδυασμός των σημασιολογικών διασυνδεδεμένων δεδομένων - τα οποία είναι machine-readable δεδομένα - και η χρήση της τεχνητής νοημοσύνης, θα δώσει την δυνατότητα καλύτερης κατανόησης των δεδομένων που υπάρχουν στο Παγκόσμιο Ιστό. Με αυτό το τρόπο οι υπολογιστές θα μπορούν να παράγουν πιο γρήγορα και αξιόπιστα αποτελέσματα, με εφαρμογές που ξεκινούν από την καλύτερη παραγωγή χημικών ενώσεων για φάρμακα μέχρι την κατασκευή καινούργιων υλικών.

Connectivity and ubiquity: με την διασύνδεση των δεδομένων και του περιεχομένου των ιστοσελίδων του διαδικτύου, τα δεδομένα γίνονται πιο ανοιχτά και συνδεδεμένα και με την αύξηση των εφαρμογών αλλά και των καθημερινών συσκευών που συνδέονται στο διαδίκτυο (π.χ Internet of Things) γίνονται πιο προσβάσιμα.

2. Υπηρεσίες και Εφαρμογές

Οι παραπάνω τεχνολογίες έκαναν εφικτή την ανάπτυξη πολλών διαφορετικών Blockchain, κρυπτονομισμάτων αλλά και δικτυακών πρωτοκόλλων που αυτά με την σειρά τους αρχίζουν και συνθέτουν ένα οικοσύστημα από αποκεντροποιημένες εφαρμογές. Το πρώτο κρυπτονόμισμα το οποίο έκανε εφικτή την χρήση των έξυπνων συμβολαίων (Application Logic -> Backend Code), για την ανάπτυξη αποκεντρωποιημένων εφαρμογών ήταν το Ethereum. Η *Solidity* είναι μια αντικειμενοστραφής, υψηλού επιπέδου γλώσσα προγραμματισμού, η οποία χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων και σχεδιάστηκε για να τρέχει στο Ethereum Virtual Machine (EVM). Ένα ακόμα κρυπτονόμισμα το οποίο αξίζει να αναφερθούμε, είναι το Solana. Το Solana, είναι ένα από τα πιο ταχέως αναπτυσσόμενα blockchain αφού και αυτό με τη σειρά του δίνει την δυνατότητα για ανάπτυξη αποκεντρωποιημένων εφαρμογών. Ένα εγχείρημα το οποίο φαίνεται να αλλάζει και αυτό με τη σειρά του τη δομή του σύγχρονου παγκόσμιου ιστού είναι το IPFS (InterPlanetary File System). Το IPFS είναι ένα peer-to-peer hypermedia πρωτόκολλο, το οποίο σχεδιάστηκε από την ομάδα Protocol Labs, η οποία αναπτύσσει ανοικτού κώδικα πρωτόκολλα, εργαλεία αλλά και υπηρεσίες. Το IPFS σκοπεύει να αντικαταστήσει το HTTP πρωτόκολλο, προσφέροντας ένα αποκεντρωποιημένο τρόπο αποθήκευσης αλλά και ανάκτησης πληροφορίας, η οποία είναι προσανατολισμένη στο περιεχόμενο (content-addressable).

Παρακάτω παρουσιάζονται κάποιες από τις ήδη υπάρχουσες αποκεντροποιημένες εφαρμογές και υπηρεσίες που βασίζονται στις τεχνολογίες που αναλύθηκαν:

MetaMask: η συγκεκριμένη εφαρμογή είναι ένα plug-in για web browsers, το οποίο ενεργοποιεί την πρόσβαση στο δίκτυο του Ethereum. Έτσι η χρήση τους ως πορτοφόλι για κρυπτονομίσματα στους

browsers δίνει την δυνατότητα χρήσης του σαν εργαλείο αυθεντικοποίησης για άλλες αποκεντρωποιημένες εφαρμογές.

Moralis: είναι μια υπηρεσία η οποία προσφέρει μια ενιαία ροή εργασίας για την ανάπτυξη εφαρμογών στο web3, συγκεκριμένα προσφέρει εύκολη αυθεντικοποίηση χρηστών, ιστορική και πραγματικού-χρόνου παρακολούθηση των συναλλαγών, SDKs (Web, Game, Backend) για ανάπτυξη σε διαφορετικές πλατφόρμες αλλά και διάφορα plug-in, είδη υπάρχων web3 εφαρμογών.

Ethereum Name System: χρησιμοποιείται για την ονοματοδοσία ethereum πορτοφολιών, ιστοσελίδων (παρόμοια με το DNS) κ.α.

OpenSea: είναι μια peer-to-peer πλατφόρμα αγοράς ψηφιακών έργων ή αλλιώς και NFTs.

Gitcoin: είναι ένα ethereum token, το οποίο δίνει την δυνατότητα, συντονισμού και χρηματοδότησης open-source έργων. Δυνατότητες είναι η 1) ευέλικτη εργασία για ανάπτυξη λογισμικού για το web3, με πληρωμή σε κρυπτονομίσματα, 2) η ενημέρωση και η μάθηση για τα blockchain, 3) σύνδεση με άλλους developer, 4) χρηματοδότηση ανοικτού-κώδικα έργων και 5) τέλος η ενασχόληση με την GitcoinDAO κοινότητα.

Fleek: είναι μια υπηρεσία 'χτισμένη πάνω' στο IPFS και σκοπός της είναι το εύκολο hosting ιστοσελίδων στο IPFS. Κάποια από τα στοιχεία τα οποία καθιστούν προσιτή την επιλογή hosting στο IPFS μέσω του fleek είναι: 1) Git Integration, 2) Auto Deploy, ευκολία εγκατάστασης εφαρμογής (χρήση Docker), 3) Auto SSL, αυτόματη εισαγωγή κατάλληλων πιστοποιητικών από την Let's Encrypt (NonProfit Certificate Authority providing TLS certificates), 4) Collaborative, αλλαγές στο git/github ανανεώνουν την ιστοσελίδα αυτόματα.

LivePeer: είναι μια αποκεντρωποιημένη εφαρμογή η οποία προσφέρει video streaming δίκτυο, βασισμένο στο ethereum blockchain.

AKASHA: είναι μια social media πλατφόρμα, προέρχεται από το 'Advanced Knowledge Architecture for Social Human Advocacy' και είναι μια εφαρμογή βασισμένη στο IPFS και το Ethereum Blockchain.

Odyssey: είναι μια πλατφόρμα στην οποία δημιουργείται περιεχόμενο και οδηγοί για θέματα που αφορούν το Web3 όπως : 1) DeFi, 2) DAOs, 3) NFTs κτλ.

Infura: υπηρεσία η οποία παρέχει APIs και εργαλεία για developers, προσφέροντας εύκολη διαλειτουργικότητα αλλά και επεκτασιμότητα μέσω του Ethereum και του IPFS δικτύου.

Deeper Network: παρέχει αποκεντρωποιημένο VPN μέσω κατάλληλου υλικού, εξασφαλίζοντας την ανωνυμία στο Web3. Επίσης δίνει την δυνατότητα στους χρήστες να κάνουν mine όσο είναι στο διαδίκτυο, προσφέροντας bandwidth που δεν χρησιμοποιούν.

Filecoin: είναι ένα αποκεντρωποιημένο δίκτυο το οποίο δίνει την δυνατότητα στους χρήστες να αποθηκεύουν αλλά και να ανακτούν πληροφορία, χωρίς την ύπαρξη κάποιας κεντρικοποιημένης δομής.

Helium: είναι μια προσπάθεια για να αποκεντρωποιηθεί η ασύρματη δικτυακή υποδομή, παρέχοντας συσκευές κάλυψης (Proof-of-Coverage) στους χρήστες που θέλουν να πληρώνονται με HNT κάνοντας mine, ανάλογα με το πόσα δεδομένα περνάνε από το Helium Gateway. Επίσης το μέχρι πρότινος δίκτυο κάλυψης, αφορούσε το LoRaWAN πρωτόκολλο, για κάλυψη IoT συσκευών (πλέον και 5G).

Εφαρμογές Σημασιολογικού Ιστού

DBpedia: είναι μια εφαρμογή με σκοπό την ανάδειξη του σημασιολογικού ιστού. Η εφαρμογή βασίζεται στα δεδομένα που αναρτούν οι χρήστες. Τα δεδομένα αυτά εξορύσσονται από Wikimedia έργα και δομούνται με κατάλληλο τρόπο (Open Knowledge Graph -> OKG). Αυτά τα δεδομένα τελικά μπορούν να ανακτηθούν σαν διασυνδεδεμένα δεδομένα.

IPLD ή Interplanetary Linked Data: είναι ένα επίπεδο κάτω από αυτό που τρέχει το IPFS και ονομάζεται επίπεδο δεδομένων. Σε αυτό το επίπεδο τα δεδομένα ή αλλιώς block πληροφορίας συνδέονται μεταξύ τους.

3. Πλεονεκτήματα / Μειονεκτήματα

Η ανάπτυξη αποκεντρωποιημένων εφαρμογών, φαίνεται να κερδίζει όλο και περισσότερο χώρο στο τομέα της ανάπτυξης λογισμικού για τον Παγκόσμιο Ιστό. Η τεχνολογίες που το απαρτίζουν, καθώς και οι προοπτικές των εφαρμογών του Web3 φαίνεται να ενέχουν, θετικά αλλά και αρνητικά χαρακτηριστικά. Ένα από τα πιο σημαντικά μειονεκτήματα είναι δυσκολία που έχουν τα κράτη να νομοθετήσουν το αποκεντρωποιημένο διαδίκτυο και τις εφαρμογές που το απαρτίζουν. Η αδυναμία αυτή έχει αφήσει χώρο για μια διαφορετική οικονομία - οικονομικό μοντέλο στο οποίο τα χρήματα που διακινούνται είναι αφορολόγητα. Επίσης αρκετοί έχουν χαρακτηρίσει τα κρυπτονομίσματα σαν την οικονομική 'φούσκα' του αιώνα, ενώ άλλοι βλέπουν μέσα σε αυτό μια οικονομική πυραμίδα ή αλλιώς σχήμα Ponzi. Ένα αρνητικό το οποίο προκύπτει από την ανωνυμία που προσφέρουν τα πρωτόκολλα που απαρτίζουν τα αποκεντρωμένα δίκτυα είναι η δυσκολία που θα υπάρχει για την ανίχνευση κυβερνοεγκλημάτων αλλά και ρητορικής μίσους. Τέλος, ένα ακόμα πρόβλημα που ανιχνεύεται στα Blockchain που βασίζονται στην αρχιτεκτονική του Proof-of-Work, είναι η μεγάλη κατανάλωση ενέργειας η οποία χρειάζεται για την επικύρωση συναλλαγών, με αποτέλεσμα να ενισχύει την περιβαλλοντική κρίση και την κλιματική αλλαγή.

Παρόλα τα αρνητικά/μειονεκτήματα που αναφέρθηκαν το αποκεντρωποιημένο διαδίκτυο έχει αρκετά πλεονεκτήματα. Ένα σημαντικό πλεονέκτημα, είναι η κατοχή των δεδομένων των χρηστών από τους ίδιους και από το δίκτυο. Η κατοχή των δεδομένων των χρηστών είναι ένα μείζον θέμα που έχει προκύψει τα τελευταία χρόνια με την συσσώρευση των δεδομένων από τις FAANG (facebook, amazon, apple, netflix, google), μετατρέποντας τους χρήστες σε προϊόντα. Ένα ακόμα πλεονέκτημα είναι τα ακριβή και σχετικά αποτελέσματα από τις αναζητήσεις των χρηστών στον σημασιολογικό ιστό. Επίσης στις αποκεντρωποιημένες εφαρμογές δεν υπάρχει κεντρικό σημείο ελέγχου, με αποτέλεσμα να είναι αδύνατον να σταματήσει να λειτουργεί κάποια υπηρεσία.

Παρακάτω παρουσιάζονται τα πλεονεκτήματα καθώς και τα μειονεκτήματα της ανάπτυξης αποκεντρωμένων εφαρμογών.

Πλεονεκτήματα ανάπτυξης DAPPs

- **Μηδενικός χρόνος διακοπής λειτουργίας** - Αφότου γίνει η ανάπτυξη και η εγκατάσταση ενός έξυπνου συμβολαίου στο blockchain, το δίκτυο φροντίζει για την ομαλή λειτουργία της εφαρμογής εξυπηρετώντας μόνιμα του χρήστες.

- **Ιδιωτικότητα** – Οι χρήστες που αλληλεπιδρούν με κάποια αποκεντρωμένη εφαρμογή δεν χρειάζεται να αυθεντικοποιηθούν με τα πραγματικά τους στοιχεία, αντ' αυτού χρειάζεται κάποιου τύπου εφαρμογή όπως το MetaMask.
- **Αντίσταση στην λογοκρισία** - Καμία οντότητα δεν μπορεί να μπλοκάρει χρήστες του δικτύου από το να κάνουν συναλλαγές, υλοποιήσουν αποκεντροποιημένες εφαρμογές ή να διαβάσουν δεδομένα που αποθηκεύονται στο blockchain.
- **Ακεραιότητα των δεδομένων**– Τα δεδομένα που αποθηκεύονται στο blockchain είναι αμετάβλητα και αδιαμφισβήτητα ως προς την ακεραιότητα τους χάρη στα κρυπτογραφικά πρωτόκολλα και τις συναρτήσεις κατακερματισμού. Έτσι κανένας κακόβουλος χρήστης δεν μπορεί να παραποιήσει δεδομένα που υπάρχουν είδη δημόσια στο blockchain.
- **Υπολογισμός χωρίς εμπιστοσύνη** (καλύτερα Computation Trustless)– Τα έξυπνα συμβόλαια εκτελούνται με τρόπο ο οποίος είναι αναμενόμενος, χωρίς να χρειάζεται εμπιστοσύνη όπως γίνεται στην περίπτωση κάποιας κεντροποιημένης αρχής. Ένα παράδειγμα είναι αυτό των τραπεζικών συστημάτων, όπου οι χρήστες εμπιστεύονται για την ακεραιότητα των δεδομένων (π.χ. τραπεζικό υπόλοιπο), ή για το ότι έγινε κάποια συναλλαγή ή στο ότι δεν θα πειράξουν τα αρχεία τους.

Μειονεκτήματα ανάπτυξης DAPPs

- **Συντήρηση** – Οι αποκεντρωποιημένες εφαρμογές είναι δύσκολο να συντηρηθούν και αυτό συμβαίνει διότι ο κώδικας που γίνεται deploy και τα δεδομένα που αποθηκεύονται στο blockchain δεν γίνεται να τροποποιηθούν. Με αυτό τον τρόπο γίνεται δύσκολη η δουλειά των προγραμματιστών που θέλουν να κάνουν αλλαγές και updates στις εφαρμογές. Ένα μειονέκτημα εδώ είναι πως και κενά ασφαλείας να υπάρχουν δεν μπορεί να γίνει καμία αλλαγή.
- **Προβλήματα απόδοσης**– Το πρόβλημα που αντιμετωπίζουν τα proof-of-work blockchain είναι αυτό της απόδοσης και της επεκτασιμότητας, μετρικών που είναι πολύ σημαντικές για τα Πληροφοριακά Συστήματα. Έτσι για να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας, ακεραιότητας, διαφάνειας και αξιοπιστίας θα πρέπει κάθε κόμβος να εκτελεί και να αποθηκεύει κάθε συναλλαγή.
- **Δικτυακή συμφόρηση**– Οι αποκεντρωμένες εφαρμογές χρησιμοποιούν πάρα πολλούς πόρους. Αυτό συμβαίνει γιατί στην πραγματικότητα γίνεται backup της πληροφορίας σε όλο το δίκτυο(κόμβοι). Αν αθροίσουμε στην εξίσωση, ότι το δίκτυο μπορεί να επεξεργαστεί 10-15 συναλλαγές το δευτερόλεπτο, τότε μπορούμε εύκολα να συμπεράνουμε ότι μεγαλύτερος αριθμός συναλλαγών μπορεί να προκαλέσει συμφόρηση στο δίκτυο
- **Διαλειτουργικότητα χρήστη** – Για το τελικό χρήστη που θέλει να χρησιμοποιήσει τις αποκεντρωποιημένες εφαρμογές, μπορεί να γίνει δύσκολο να επιλέξει την κατάλληλη στοίβα εργαλείων που χρειάζεται, για να αλληλεπιδράσει με το blockchain με έναν ασφαλή τρόπο
- **Κεντροποίηση** – Φιλικές προς το χρήστη αλλά και προς τον προγραμματιστή λύσεις (που αναπτύσει εφαρμογές πάνω από το Ethereum), μπορεί τελικά να μοιάζουν με κάποια κεντροποιημένη υπηρεσία. Για παράδειγμα μπορεί να χρειαστεί η αποθήκευση κλειδιών (απαραίτητα για κρυπτογραφικά συστήματα), ή η διεπαφή να τρέχει σε κάποιον κεντροποιημένο server. Με αυτό το τρόπο αναιρούνται κάποια από τα χαρακτηριστικά και πλεονεκτήματα που έχει το Blockchain σε αντίθεση με το παραδοσιακό μοντέλο/αρχιτεκτονική.

4. Συμπεράσματα

Η ανάγκη των ανθρώπων για αποκεντροποιημένα συστήματα γίνεται εμφανής στο πέρασμα των χρόνων, από το τέλος των φεουδαρχικών καθεστώτων μέχρι και σήμερα. Κάποιες πρώιμες εφαρμογές οι οποίες έκαναν εφικτή την ανταλλαγή αρχείων μέσω των peer-to-peer δικτύων ήταν το Napster και το μTorrent. Οι τεχνολογίες που αφορούν το Web3.0 φαίνεται να είναι ακόμα πρώιμες, χωρίς αυτό να σημαίνει πως δεν χρειάζεται να γίνεται συζήτηση για αυτές. Η απαρχή φαίνεται να είναι το Bitcoin, το οποίο είναι ένα ψηφιακό νόμισμα που έδωσε την δυνατότητα αγοράς και πώλησης χωρίς να είναι αναγκαία η ύπαρξη κάποιου ενδιάμεσου χρηματοπιστωτικού ιδρύματος, εξασφαλίζοντας την ανωνυμία και την ασφάλεια στις συναλλαγές μεταξύ των χρηστών.

Ανακεφαλαιώνοντας, οι τεχνολογίες που βασίστηκαν στην αρχιτεκτονική του Blockchain και των peer-to-peer δικτύων, ξεκλείδωσαν προοπτικές για την ανάπτυξη και δημιουργία εφαρμογών που δεν μπορούσαμε πριν καν να φανταστούμε. Κάποιες από αυτές θα μπορούσαν εξαλείψουν την διαφθορά σε κρατικούς μηχανισμούς και ενισχύσουν την διαφάνεια μεταξύ κράτους και πολιτών. Ο τρόπος με τον οποίο θα εκδημοκρατίζονταν κάποιες διαδικασίες όπως αυτή της ψηφοφορίας, των δημοψηφισμάτων είναι μέσω των smart contracts. Ακόμα θα μπορούσαν δημόσια έγγραφα να αποθηκεύονται στο blockchain ώστε να είναι εξασφαλίζεται η ακεραιότητα τους. Εκτός από τις παραπάνω διαδικασίες που θα μπορούσαν να βοηθήσουν το Κράτος, ενδιαφέρον είναι και η χρήση των DAO (Decentralized Autonomous Organization) για τις επιχειρήσεις και τους συνεταιρισμούς. Με την χρήση των DAO γίνεται εύκολη η λήψη αποφάσεων μέσα στις επιχειρήσεις και του οργανισμού.

Κάποιες ακόμα εφαρμογές, που δεν αναφέρθηκαν στις προηγούμενες ενότητες, είναι η διασφάλιση ποιότητας των προϊόντων στο Cold Chain και γενικότερα στο Supply Chain εξασφαλίζοντας την ανιχνευσιμότητα των προϊόντων και όχι μόνο (Shipping Quality, Consistency Checks, Item Identification, Quality Assessment). Ακόμα η χρήση των smart contracts θα μπορούσε να βοηθήσει αρκετές λειτουργίες που σχετίζονται με τους δικηγόρους, όπως αυτή της διαθήκης (μια από τις πάρα πολλές χρήσεις που θα μπορούσαν να έχουν τα έξυπνα συμβόλαια). Τα NFTs με τη σειρά τους, ξεκλείδωσαν τη χρήση αυτών από δημιουργούς ψηφιακών έργων και όχι μόνο, εξασφαλίζοντας την μοναδικότητα αυτών.

Τα πιο βασικά προβλήματα που υπάρχουν μέχρι στιγμής είναι η ανικανότητα νομοθέτησης των κρυπτονομισμάτων και γενικά των εφαρμογών που προκύπτουν από τις τεχνολογίες που απαρτίζουν το Web3, επιτρέποντας μέχρι στιγμής την ύπαρξη μεγάλων χρηματικών ποσών που δεν φορολογούνται. Ακόμα ένα πρόβλημα είναι αυτό της συντήρησης, αφού όπως προαναφέρθηκε οι εφαρμογές που αναπτύσσονται δεν μπορούν να τροποποιηθούν, έτσι οποιοδήποτε λάθος στις λειτουργικές απαιτήσεις, στην αρχιτεκτονική ή σε κενά ασφαλείας είναι μη αντιστρέψιμο (καθόλου χρήσιμο για ανάπτυξη λογισμικού που βασίζεται στο Agile Development).

Εν κατακλείδι, μπορεί να γίνει εμφανές πως, από τη μια οι παραπάνω τεχνολογίες που αναλύθηκαν μπορούν να χρησιμοποιηθούν για να λύσουν σημαντικά προβλήματα του οικονομικού, κρατικού, επιχειρησιακού συστήματος. Από την άλλη ενέχει ο κίνδυνος για την περιθωριοποίηση των τεχνολογιών αυτών λόγω της χρηματιστηριακής υπόστασης που τους έχει δοθεί, αφού ο περισσότερος κόσμος τα αντιμετωπίζει σαν μετοχές.

Πηγές

1. [The father of Web3 Wants You to Trust Less](#)
2. [Web3.0 & Privacy - Computerphile](#)
3. [Stanford Seminar - IPFS and the Permanent Web](#)
4. [Web3](#)
5. [Bitcoin: A Peer-to-Peer Electronic Cash System](#)
6. [Fleek](#)
7. [Formalizing and Securing Relationships on Public Networks, by Nick Sazbo](#)
8. [Web 3.0, Linked Data, and the Semantic Web: What's this all about?](#)
9. [Tim Berners-Lee: The next Web of open, linked data](#)
10. [Web 3.0: The Future Architecture of the Internet?](#)
11. [Introduction to Smart Contracts](#)
12. [World Wide Web Consortium: Web3.0 Emerging](#)
13. [Host a single-page website on IPFS](#)
14. [Solidity](#)
15. [Odyssey - Learning Paths](#)
16. [Decentralization at Work: Cooperatives on the Blockchain](#)
17. [Blockchain Democracy: Digital Governance in the EU and the US](#)