ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η τεχνολογία Blockchain στις σύγχρονες εφαρμογές συναλλαγών

Φοιτητής : Ματέο Μπερζάνι

Α.Μ : 711141089

Εισηγητής : Δρ. Παναγιώτης Καρκαζής, Επ. Καθηγητής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η τεχνολογία Blockchain στις σύγχρονες εφαρμογές συναλλαγών

Ματέο Μπερζάνι

Α.Μ : 711141089

Εξεταστική Επιτροπή :

Δρ. Παναγιώτης Καρκαζής, Επ. Καθηγητής Panagiotis Karkazis Digitally signed by Panagiotis Karkazis Date: 2022.03.18 08:53:01 +02'00'

Δρ. Νικόλαος Μυριδακής, Επ. Καθηγητής Nikolaos Myridakis Digitally signed by Nikolaos Myridakis Date: 2022.03.14 17:15:40 +02'00'

Δρ. Ελένη-Αικατερίνη Λελίγκου, Αν. Καθηγήτρια Eleni Aikaterini Leligkou Digitally signed by Eleni Aikaterini Leligkou Date: 2022.03.14 17:46:49 +02'00'

Ημερομηνία εξέτασης : 11/ 03 /2022

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ματέο Μπερζάνι, με αριθμό μητρώου 711141089 φοιτητής του Προγράμματος Προπτυχιακών Σπουδών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Ματέο Μπερζάνι

ΕΥΧΑΡΙΣΤΙΕΣ

Στην παρούσα διπλωματική εργασία θα ήθελα να ευχαριστήσω θερμά τον Επίκουρο καθηγητή Δρ. Παναγιώτη Καρκαζή κυρίως για την εμπιστοσύνη που μου έδειξε, και την υπομονή που έκανε κατά τη διάρκεια υλοποίησης της πτυχιακής εργασίας. Όπως επίσης και για την πολύτιμη βοήθεια και καθοδήγηση του, για την επίλυση διάφορων θεμάτων.

ΠΕΡΙΛΗΨΗ

Ο σκοπός της διπλωματικής εργασίας είναι η παρουσίαση της τεχνολογίας blockchain που είχε εμφανιστεί μαζί με το Bitcoin. Το Bitcoin ως το πρώτο και πιο επιτυχημένο παράδειγμα κρυπτονομίσματος επιτρέπει την εκτέλεση χρηματικών συναλλαγών μεταξύ αγνώστων χωρίς την ανάγκη επιβεβαίωσης της εγκυρότητας των συναλλαγών από τρίτο αξιόπιστο μέλος. Το 2013 δημιουργήθηκε, το Ethereum blockchain, μία πλατφόρμα που υποστηρίζει τη δημιουργία κατανεμημένων εφαρμογών γνωστές ως Decentralized Application. Οι κατανεμημένες εφαρμογές που αναπτύσσονται στο ethereum blockchain δεν περιορίζονται μόνο σε οικονομικές συναλλαγές όπως στο bitcoin αλλά επιτρέπει την δημιουργία ποικίλων ειδών εφαρμογών μέσω των έξυπνων συμβολαίων που αποθηκεύονται μέσα στο δίκτυο του. Τα έξυπνα συμβόλαια είναι αρχεία κώδικα που εκτελούνται, όταν κληθούν και εφόσον έχουν συναντηθεί ορισμένες συνθήκες. Μερικές περιπτώσεις οπού μπορούν να εφαρμοστούν τα έξυπνα συμβόλαια πέρα από χρηματικές συναλλαγές είναι: στην διαχείριση εφοδιαστικής αλυσίδας, σε υπηρεσίες ταυτοποίησης και στην διαδικτυακή ψηφοφορία. Τέλος αναπτύχθηκε μια εφαρμογή έξυπνου συμβολαίου για την παρουσίαση όσων αναφέρονται στην ανάπτυξη του θεωρητικού σκέλους και την παρουσίαση των εργαλείων που είναι απαραίτητα για την υλοποίηση της.

ABSTRACT

The purpose of this dissertation is to present the blockchain technology that appeared with Bitcoin. Bitcoin as the first and most successful example of cryptocurrency allows the execution of money transactions between strangers without the need of a third trusted member to validate the transactions. In 2013 Ethereum blockchain was created, a platform that supports the development of distributed applications known as Decentralized Application. Distributed applications developed in the ethereum blockchain are not limited to financial transactions such as Bitcoin but allow the creation of various types of applications through smart contracts stored within its network. Smart contracts are code files that run when called and when certain conditions are met. Some use cases of smart contracts that can be applied beyond money transactions are: supply chain management, authentication services and online voting. Finally, a smart contract application was developed to present what relates to the development of the theoretical part and the presentation of the tools that are necessary for its implementation and development.

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AES	Advanced Encryption Standard
API	Application Programming Interfaces
BFT	Byzantine Fault Tolerance
CoT	Chain of Things
DApps	Decentralized Application
DES	Data Encryption Standard
DID	Decentralized identifier
DNS	Domain Name System
DSA	Digital Signature Algorithm
DeFi	Decentralized finance
ECC	Elliptic-curve cryptography
EOA	Externally-owned accounts
ERC-20	Ethereum Request for Comments 20
ETH	Ether
EVM	Ethereum Virtual Machine
HTTP	Hypertext Transfer Protocol
IPC	International Plumbing Code
IoT	Internet of things
KYC	Know Your Customer
NFT	Non-fungible Tokens
P2P	Peer to Peer
PoS	Proof of Stake
PoW	Proof of Work
RC4	Alleged RC4
RSA	Rivest Shamir Adleman
SSI	Self-sovereign identity
SSL	Secure Sockets Layer

ZKP	Zero Knowledge Proof

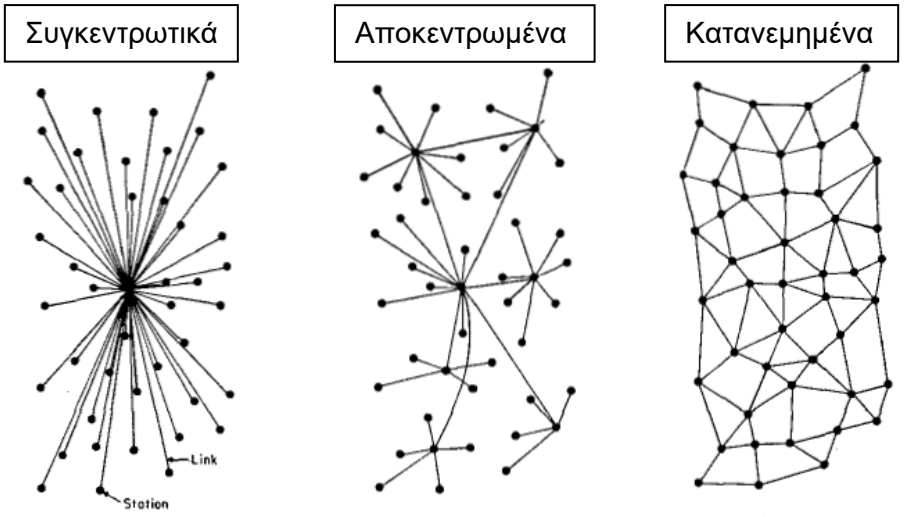
Εισαγωγή

Το blockchain [1] αποτελεί μια τεχνολογία που είναι εξαιρετικά δημοφιλής σήμερα. Η κατανόηση του τι είναι το blockchain παρουσιάζει δυσκολίες, αλλά οι πιθανές εφαρμογές της νέας αυτής τεχνολογίας είναι τόσο πολλές που έχουν δημιουργήσει ισχυρό ενδιαφέρον από διάφορους κλάδους όπως οι τράπεζες, οι ασφάλειες, η ηλεκτρονική διακυβέρνηση, ο χώρος της υγείας κ.α.. Έχει τις προδιαγραφές έτσι ώστε να προκαλέσει αναταραχή (disruption) στην καθημερινότητα πολιτών και επιχειρήσεων ανάλογη με αυτή που έχει επιφέρει το διαδίκτυο από τη δεκαετία του 1990 και μετά [2]. Οι αλλαγές που ενδέχεται να επιφέρει, εστιάζονται στην αύξηση της αποδοτικότητας των συναλλαγών, για οποιοδήποτε συναλλάσσεται, με την ταυτόχρονη διασφάλιση της εγκυρότητας των συναλλαγών. Το blockchain αποτελεί ένα ψηφιακό και αποκεντρωμένο καθολικό (digital decentralized ledger), στο οποίο καταγράφονται με ασφάλεια πληροφορίες που μπορούν να προσπελάσουν οι συμμετέχοντες σε αυτό. Βάση σχεδιασμού, οι πληροφορίες που καταγράφονται στο blockchain δεν μπορούν να αλλάξουν (immutable) από τη στιγμή που έχουν εισαχθεί σε αυτό. Μια συναλλαγή μπορεί να «ακυρωθεί», μόνο μέσω μιας άλλης συναλλαγής και σε αυτή την περίπτωση και οι δύο συναλλαγές παραμένουν ορατές στο blockchain. Αν και αυτό αρχικά φαίνεται ως περιορισμός, στην πράξη λειτουργεί ως πλεονέκτημα, καθώς προσδίδει εμπιστοσύνη και εγκυρότητα στα στοιχεία που εν τέλει εμπεριέχονται στο blockchain. Οι πληροφορίες που καταγράφονται στο blockchain μπορεί να αφορούν οτιδήποτε. Συνηθισμένες περιπτώσεις αποτελούν η καταγραφή ιδιοκτησίας (με υλική υπόσταση όπως για παράδειγμα ένα σπίτι, προϊόν, ή άυλη όπως για παράδειγμα πνευματικά δικαιώματα, πατέντες κ.α.) και η καταγραφή συναλλαγών. Το blockchain είναι συνυφασμένο στην αντίληψη πολλών με τα κρυπτονομίσματα και ιδιαίτερα με το bitcoin [3]. Πράγματι, το blockchain αποτελεί την υποδομή πάνω στην οποία λειτουργεί το bitcoin, αλλά μπορεί να αποτελέσει υποδομή και για άλλες εφαρμογές ανεξάρτητα από τον κόσμο των κρυπτονομισμάτων. Συνεπώς, το bitcoin είναι μόνο μια (και ιστορικά η πρώτη) εφαρμογή του blockchain. Οι μεγάλες εταιρείες τεχνολογίας δεν έχουν μείνει αδιάφορες σε αυτή τη νέα τεχνολογία. Η Microsoft προσφέρει εργαλεία κατασκευής εφαρμογών blockchain στην υπολογιστική υποδομή νέφους που διαθέτει, το Azure cloud. Η IBM, η Intel και άλλες εταιρείες συνεργάζονται στην δημιουργία του Hyperledger [4] που αποτελεί μια τεχνολογία blockchain με έμφαση σε επιχειρηματικές εφαρμογές. Στο ίδιο μήκος κύματος βρίσκονται και οι τράπεζες που προσπαθούν να στρέψουν την blockchain τεχνολογία προς όφελός τους. Η παρούσα πτυχιακή εξετάζει το blockchain, τα έξυπνα συμβόλαια, τα κρυπτονομίσματα, τις εφαρμογές του blockchain σε διάφορα πεδία καθώς και την υλοποίηση μιας εφαρμογής, με σκοπό να βοηθήσει στην επεξήγηση της συγγραφής και ανάπτυξης ενός έξυπνου συμβολαίου.

1 Βασικές έννοιες

1.1 Πληροφορικά Συστήματα

Υπάρχουν τρία βασικά είδη πληροφοριακών συστημάτων, τα αποκεντρωμένα (decentralized [5]), τα συγκεντρωτικά (centralized [6]) και τα κατανεμημένα (distributed [7]). Στα συγκεντρωτικά συστήματα, που είναι γνωστά και ως συστήματα πελάτη-εξυπηρετητή (client-server), υπάρχει ένας κεντρικός εξυπηρετητής στον οποίο συνδέονται οι πελάτες και από το οποίο εξαρτάται η λειτουργία του συστήματος στο σύνολό του. Ένα αποκεντρωμένο σύστημα είναι ένα διασυνδεδεμένο σύστημα πληροφοριών, όπου καμία οντότητα δεν είναι η μόνη αρχή. Στο πλαίσιο της πληροφορικής και της τεχνολογίας πληροφοριών, τα αποκεντρωμένα συστήματα λαμβάνουν συνήθως τη μορφή δικτυωμένων υπολογιστών. Στα κατανεμημένα συστήματα τα επιμέρους τμήματα του συστήματος συνδέονται χωρίς να υπάρχει τμήμα που να εξυπηρετεί ή να συντονίζει τα άλλα τμήματα και από το οποίο να εξαρτάται η συνολική λειτουργία του συστήματος.



Εικόνα 1.1 Είδη κατανεμημένων συστημάτων[8]

Σε ότι αφορά τα συστήματα λογισμικού, τα κύρια πλεονεκτήματα των κατανεμημένων συστημάτων έναντι των συγκεντρωτικών είναι η υψηλότερη υπολογιστική ισχύς, το μειωμένο κόστος, η υψηλότερη διαθεσιμότητα, η αξιοπιστία και η μεγαλύτερη δυνατότητα κλιμάκωσης. Ωστόσο, τα κατανεμημένα συστήματα έχουν και μειονεκτήματα με σημαντικότερα τη μεγαλύτερη πολυπλοκότητα, τις επιβαρύνσεις συντονισμού και επικοινωνίας που δημιουργούνται, καθώς και θέματα ασφάλειας τα οποία θα πρέπει να αντιμετωπιστούν έτσι ώστε να λειτουργήσουν με αποδεκτό τρόπο.

Το blockchain μπορεί να θεωρηθεί ως ένας μηχανισμός για την επίτευξη ακεραιότητας σε κατανεμημένα συστήματα λογισμικού[9]. Η τεχνολογία blockchain μπορεί να αντικαταστήσει τον ρόλο που αυτήν την στιγμή έχουν οι θεωρούμενες ως έμπιστες οντότητες (third trust partry) (π.χ. τράπεζες, ασφαλιστικοί οργανισμοί, κυβερνητικές υπηρεσίες) στα κεντρικά συστήματα μετασχηματίζοντας τα σε αποδοτικότερα κατανεμημένα συστήματα.

1.2 Ομότιμα κατανεμημένα συστήματα

Τα ομότιμα κατανεμημένα συστήματα[10] (peer to peer – P2P) είναι μια ειδική κατηγορία κατανεμημένων συστημάτων, τα οποία αποτελούνται από επιμέρους υπολογιστές, που διαθέτουν κάποιους από τους υπολογιστικούς τους πόρους απευθείας σε όλα τα άλλα μέλη του δικτύου. Όπως δηλώνει και το όνομά τους, τα συστήματα αυτά είναι ομότιμα, δηλαδή οι επιμέρους υπολογιστές, που συχνά αναφέρονται και ως κόμβοι, λειτουργούν ταυτόχρονα ως πάροχοι αλλά και καταναλωτές πόρων στο δίκτυο.

Θα πρέπει να σημειωθεί ότι υπάρχουν πολλές παραλλαγές αρχιτεκτονικής ομότιμων συστημάτων. Για παράδειγμα υπάρχουν τα ομότιμα συστήματα με κεντρικό έλεγχο, στα οποία κάποιοι κόμβοι διατηρούν ρόλους που διευκολύνουν και καθιστούν αποδοτικότερη τη λειτουργία του συστήματος. Από την άλλη μεριά, σε ένα αμιγές ομότιμο σύστημα απουσιάζει πλήρως η έννοια του κεντρικού συντονισμού και ελέγχου.

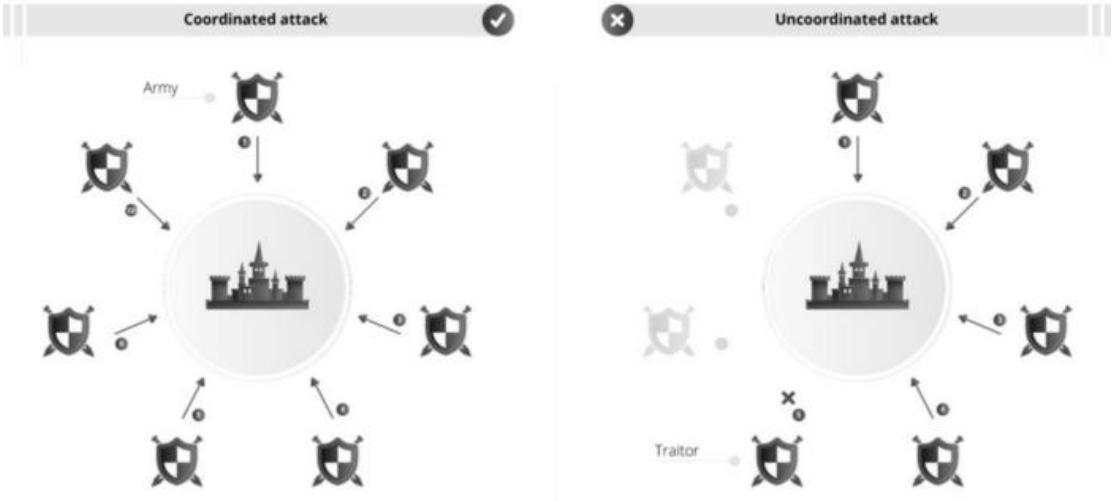
Ως προκλήσεις στην υιοθέτηση των ομότιμων συστημάτων μπορούν να αναφερθούν:

- Η ασύμμετρη ταχύτητα upload και download για τους χρήστες του διαδικτύου όπως προσφέρεται από τους παρόχους διαδικτύου σήμερα.
- Η ασφάλεια στη διάθεση του περιεχομένου που προσφέρεται.
- Η διασφάλιση ότι τα απαιτούμενα δικαιώματα διάθεσης της πληροφορίας υφίστανται.

1.3 Πρόβλημα των Βυζαντινών Στρατηγών

Το πρόβλημα των Βυζαντινών Στρατηγών [11] (Byzantine fault tolerance-BFT) αντιλήφθηκε το 1982, ως ένα λογικό δίλημμα που παρουσιάζει μια ομάδα βυζαντινών στρατηγών που προσπαθούν να αποφασίσουν την επόμενη κίνηση τους μέσο περιορισμένης επικοινωνίας.

Το δίλημμα υποθέτει ότι κάθε στρατηγός έχει το δικό του στρατό και ότι κάθε ομάδα βρίσκεται σε διαφορετικές τοποθεσίες γύρω από την πόλη που σκοπεύουν να επιτεθούν. Οι στρατηγοί πρέπει να συμφωνήσουν, είτε να επιτεθούν είτε να υποχωρήσουν. Δεν έχει σημασία αν επιτεθούν ή υποχωρήσουν, αρκεί όλοι οι στρατηγοί να επιτύχουν συναίνεση, δηλαδή να συμφωνήσουν σε μια κοινή απόφαση προκειμένου να την εκτελέσουν σε συντονισμό.



Εικόνα 1.2 Αναπαράσταση Byzantine fault tolerance[12]

Επομένως, πρέπει να λάβουμε υπόψη τις ακόλουθες απαιτήσεις:

- Κάθε στρατηγός πρέπει να αποφασίσει: επίθεση ή υποχώρηση (ναι ή όχι).
- Μετά τη λήψη της απόφασης, δεν επιτρέπονται αλλαγές.
- Όλοι οι στρατηγοί πρέπει να συμφωνήσουν για την ίδια απόφαση και να την εκτελέσουν με συγχρονισμένο τρόπο.

Τα προαναφερθέντα προβλήματα επικοινωνίας σχετίζονται με το γεγονός ότι ένας στρατηγός μπορεί να επικοινωνήσει με έναν άλλο μόνο μέσω μηνυμάτων, τα οποία προωθούνται από έναν ταχυμεταφορέα. Κατά συνέπεια, η κεντρική πρόκληση του προβλήματος των Βυζαντινών στρατηγών είναι ότι τα μηνύματα μπορούν να καθυστερήσουν, να καταστραφούν ή να χαθούν.

Επιπλέον, ακόμη και αν ένα μήνυμα παραδοθεί επιτυχώς, ένας ή περισσότεροι στρατηγοί μπορούν να επιλέξουν (για οποιονδήποτε λόγο) να ενεργήσουν κακόβουλα και να στείλουν ένα δόλιο μήνυμα για να μπερδέψουν τους άλλους στρατηγούς, οδηγώντας σε πλήρη αποτυχία. Εάν εφαρμόσουμε το δίλημμα στο πλαίσιο των blockchain, κάθε στρατηγός αντιπροσωπεύει έναν κόμβο δικτύου. Οι κόμβοι πρέπει να επιτύχουν συναίνεση μεταξύ των κόμβων για την τρέχουσα κατάσταση του συστήματος. Με άλλα λόγια, η πλειοψηφία των συμμετεχόντων σε ένα κατανεμημένο δίκτυο πρέπει να συμφωνήσουν και να εκτελέσουν την ίδια ενέργεια προκειμένου να αποφευχθεί η πλήρης αποτυχία. Επομένως, ο μόνος τρόπος για να επιτευχθεί συναίνεση σε αυτούς τους τύπους κατανεμημένου συστήματος είναι τουλάχιστον τα ⅔ των κόμβων του δικτύου να είναι αξιόπιστοι και ειλικρινείς κόμβους δικτύου. Αυτό σημαίνει ότι εάν το σύστημα είναι ευαίσθητο σε αποτυχίες και επιθέσεις (όπως η επίθεση 51% [13]).

Η βυζαντινή ανοχή σφαλμάτων είναι χαρακτηριστικό ενός συστήματος, που είναι σε θέση, να αντισταθεί επιθέσεις όπως το πρόβλημα των βυζαντινών στρατηγών. Αυτό σημαίνει ότι ένα σύστημα BFT μπορεί να συνεχίσει να λειτουργεί ακόμη και αν ορισμένοι από τους κόμβους αποτύχουν ή ενεργήσουν κακόβουλα. Υπάρχουν περισσότερες από μία πιθανές λύσεις στο πρόβλημα των Βυζαντινών στρατηγών και, ως εκ τούτου, πολλοί τρόποι οικοδόμησης ενός συστήματος BFT. Ομοίως, υπάρχουν διαφορετικές προσεγγίσεις για ένα blockchain για την επίτευξη βυζαντινής ανοχής σφαλμάτων και αυτό μας οδηγεί στους λεγόμενους αλγορίθμους συναίνεσης. Μπορούμε να ορίσουμε έναν αλγόριθμο συναίνεσης ως τον μηχανισμό μέσω του οποίου ένα δίκτυο blockchain επιτυγχάνει συναίνεση. Οι πιο κοινές εφαρμογές είναι το Proof of Work (PoW)[14] και το Proof of Stake (PoS) [15].

Ας πάρουμε για παράδειγμα την περίπτωση Bitcoin. Ενώ το πρωτόκολλο που εφαρμόζεται στο Bitcoin ορίζει τους πρωταρχικούς κανόνες του συστήματος, ο αλγόριθμος συναίνεσης PoW είναι αυτό που καθορίζει πώς θα ακολουθηθούν αυτοί οι κανόνες για να επιτευχθεί συναίνεση (για παράδειγμα, κατά την επαλήθευση και την επικύρωση των συναλλαγών). Αν και η έννοια του PoW είναι παλαιότερη από αυτήν των κρυπτονομισμάτων, ο Satoshi Nakamoto[16] ανέπτυξε μια τροποποιημένη έκδοση του σαν ένα αλγόριθμο που επέτρεψε τη δημιουργία του Bitcoin ως συστήματος BFT.

Σημειώστε ότι ο αλγόριθμος PoW δεν είναι πλήρως ανεκτικός στα βυζαντινά σφάλματα, αλλά λόγω της διαδικασίας εξόρυξης υψηλής απόδοσης και των υποκείμενων κρυπτογραφικών τεχνικών, το PoW έχει αποδειχθεί ότι είναι μια από τις πιο ασφαλείς και αξιόπιστες υλοποιήσεις για δίκτυα blockchain. Υπό αυτή την έννοια, ο αλγόριθμος συναίνεσης της απόδειξης της εργασίας, που σχεδιάστηκε από τον Satoshi Nakamoto, θεωρείται ως μία από τις πιο έξυπνες λύσεις στα βυζαντινά σφάλματα.

2 Κρυπτογραφία

Κρυπτογραφία [17] ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή, με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου, ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Αντίστοιχα, η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο (cypher text) παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση.

Μέχρι και σήμερα υπάρχουν δυο κατηγορίες κρυπτογράφησης, η συμμετρική και η ασύμμετρη.

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Αυθεντικοποίηση (Authentication): Αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα.

2.1 Κατηγορίες μεθόδων κρυπτογραφίας

2.1.1 Συμμετρική κρυπτογραφία

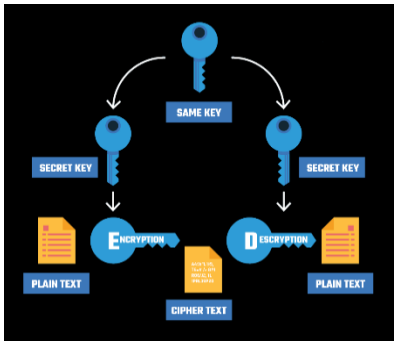
Συμμετρικό κρυπτοσύστημα [18], είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης - αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα, προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας, ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι, χωρίζονται σε τρεις κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers [19]), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- Ροής (Stream Ciphers [20]), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα.
- Αντικατάστασης (Substitution ciphers [21]), οι οποίοι αντιστοιχίζουν και στη συνέχεια αντικαθιστούν κάθε σύμβολο-γράμμα του αρχικού μηνύματος με κάποιο άλλο γράμμα ή ακολουθία γραμμάτων.

Παραδείγματα Συμμετρικών Κρυπταλγορίθμων

- Δέσμης (Block Ciphers): DES [23], 3Way [24], Blowfish [25], AES [26], Triple DES [27], Serpen t[28], Twofish [29]
- Ροής (Stream Ciphers): RC4 [30], E0 [31], ChaCha [32], A5/1 [33]
- Αντικατάστασης (substitution ciphers): Affine [34], Atbash [35], Autokey [36], Beaufor t[37], Caesar [38],



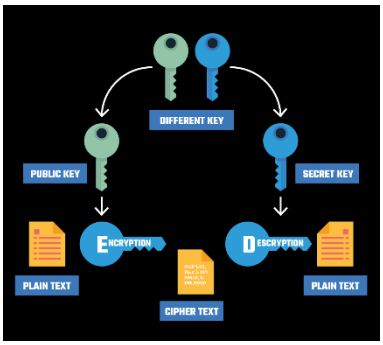
Εικόνα 2.1 Συμμετρική διαδικασία κρυπτογράφησης[22]

2.1.2 Ασύμμετρη κρυπτογραφία

Η ασύμμετρη κρυπτογραφία [39] ή Κρυπτογράφηση Δημόσιου Κλειδιού)δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσιάζουν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δύο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Παραδείγματα Ασυμμέτρων Κρυπταλγορίθμων

- RSA [40]
- Πρωτόκολλο Diffie-Hellman [41]
- DSA [42]
- Paillier [43]
- Πρότυπο ElGamal - Υπογραφή ElGamal [44]
- Κρυπτογραφία ελλειπτικών καμπυλών (Elliptic-curve cryptography-ECC) [45]



Εικόνα 2.2 Ασύμμετρη διαδικασία κρυπτογράφησης[46]

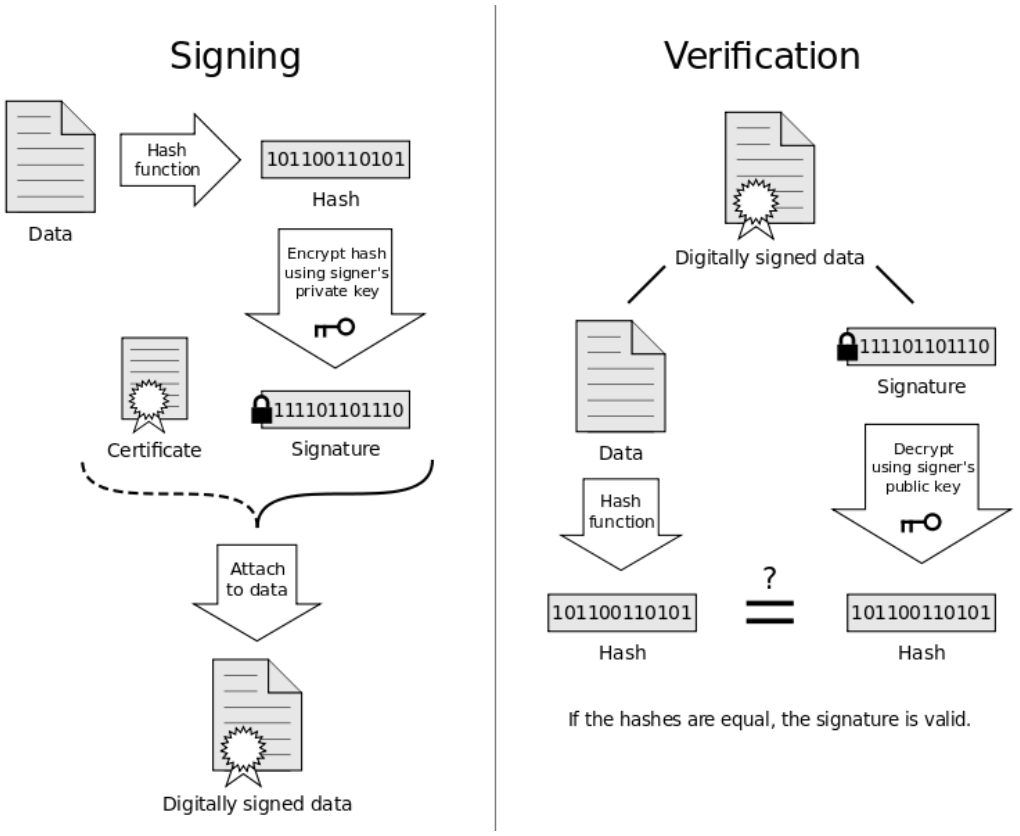
2.2 Η ασύμμετρη κρυπτογραφία στο blockchain

Η ασύμμετρη κρυπτογραφία χρησιμοποιείται για την αναγνώριση λογαριασμών και την εξουσιοδότηση συναλλαγών στο blockchain [47]. Τα δεδομένα των συναλλαγών εμπεριέχουν δημόσια κλειδιά για την ταυτοποίηση των λογαριασμών (το δημόσιο κλειδί είναι και ο αριθμός του λογαριασμού). Από την άλλη μεριά ο ιδιοκτήτης του λογαριασμού που παραδίδει την ιδιοκτησία ενός πόρου μέσω μιας συναλλαγής κρυπτογραφεί ένα κείμενο με το ιδιωτικό του κλειδί. Οι άλλοι χρήστες μπορούν να επιβεβαιώσουν την ορθότητα της συναλλαγής χρησιμοποιώντας το δημόσιο κλειδί που όπως αναφέρθηκε παραπάνω είναι ο αριθμός του λογαριασμού του ιδιοκτήτη του πόρου που μεταβιβάζεται.

2.3 Ψηφιακές υπογραφές

Η ψηφιακή υπογραφή [48] θεωρείται ως το ηλεκτρονικό ισοδύναμο της συμβατικής υπογραφής και είναι μια συμβολοσειρά που προκύπτει από το συνδυασμό των δυαδικών ψηφίων ενός μηνύματος και αυτών ενός μυστικού κλειδιού. Η χρησιμοποίηση της ψηφιακής υπογραφής σε ένα σύστημα ασφαλείας ενός δικτύου είναι απαραίτητη, καθώς παρέχει αυθεντικοποίησης του αποστολέα, εμπιστευτικότητα και ακεραιότητα του μηνύματος. Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος. Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash συνάρτηση στο μήνυμα και να δημιουργήσει ένα message digest [49]. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα. Ουσιαστικά η δουλειά της hash συνάρτησης είναι να πάρει ένα μήνυμα οποιουδήποτε μεγέθους και να το μετατρέψει σε προκαθορισμένο μέγεθος. Για να δημιουργήσει κανείς μια ψηφιακή υπογραφή κρυπτογραφεί συνήθως το message digest και όχι το ίδιο το μήνυμα (μ' άλλα λόγια το κρυπτογραφημένο message digest είναι η ψηφιακή υπογραφή του αποστολέα). Ο Α στέλνει στον Β το κρυπτογραφημένο message digest και το μήνυμα, κρυπτογραφημένο ή όχι. Προκειμένου ο Β να αυθεντικοποιήσει την υπογραφή κάνει τα εξής: Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest. Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α. Ο Β έχει τώρα στη

διάθεση του δύο message digest. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση.



Εικόνα 2.3 Διαδικασία δημιουργίας και επισύναψης ψηφιακής υπογραφής[50]

2.4 Απόδειξη μηδενικής γνώσης

Η απόδειξη μηδενικής γνώσης (Zero Knowledge Proof- ZKP) [51] είναι μια μέθοδος που επιτρέπει σε ένα άτομο (prover) να αποδείξει σε ένα άλλο άτομο (verifier) ότι ο πρώτος έχει στην κατοχή του κάποια πληροφορία χωρίς όμως ο δεύτερος να μάθει στοιχεία της ίδιας της πληροφορίας.

Μια ZKP θα πρέπει να διαθέτει τις ακόλουθες ιδιότητες:

- Πληρότητα: Σε περίπτωση που ο verifier επαληθεύσει ότι ο prover κατέχει την πληροφορία τότε όντως ο prover κατέχει την πληροφορία.
- Εγκυρότητα: Αν ο prover δεν έχει στην κατοχή του την πληροφορία που προσπαθεί να πείσει τον verifier ότι έχει, ο verifier δεν μπορεί να πειστεί (παρά μόνο με μια απειροελάχιστη πιθανότητα).
- Μηδενική γνώση: Αν ο prover κατέχει την πληροφορία που ισχυρίζεται και ο verifier το επαληθεύει, κατά τη διαδικασία επαλήθευσης ο verifier δεν μαθαίνει τίποτα για την ίδια την πληροφορία πέρα από το γεγονός ότι βρίσκεται στην κατοχή του prover. Ένα σύστημα ZKP μπορεί να χρησιμοποιηθεί για παράδειγμα έτσι ώστε να μη χρειάζεται να δίνεται ο αριθμός της πιστωτικής κάρτας από τον ιδιοκτήτη της κάρτας σε έναν έμπορο και ωστόσο ο έμπορος

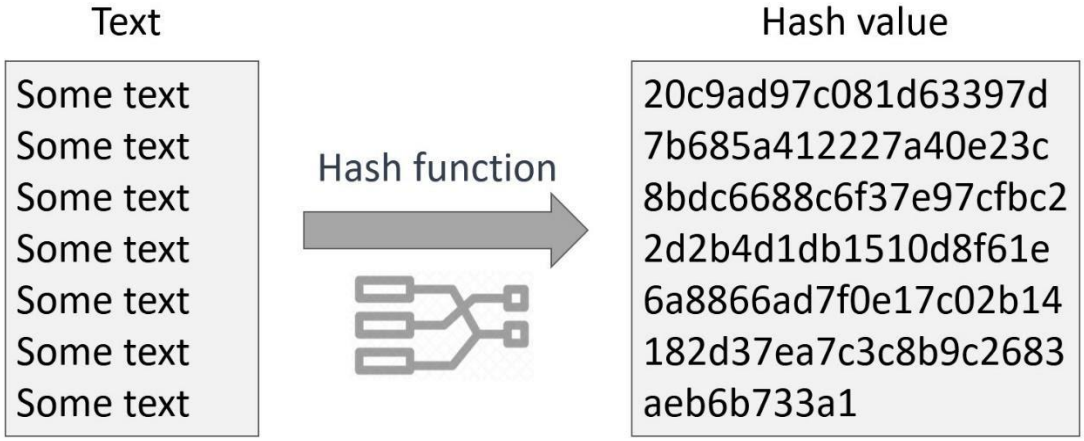
να είναι σε θέση να διαπιστώσει ότι η κάρτα ανήκει ή δεν ανήκει σε εκείνον που το ισχυρίζεται.

Εικόνα 2.3 Διαδικασία απόδειξη μηδενικής γνώσης[52]

3 Κατακερματισμός

3.1 Συναρτήσεις κατακερματισμού

Η συνάρτηση κατακερματισμού [53], είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο σταθερού μεγέθους αναπαράστασης. Το μέγεθος αυτό μπορεί να είναι μεγαλύτερο ή ίσο των 32bit, συνήθως είναι 256 bit, και είναι ανάλογο με το λόγο χρήσης της συνάρτησης. Εγγυάται την ακεραιότητα και την αυθεντικότητα των δεδομένων. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού, ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes).



Εικόνα 3.1 Διαδικασία συναρτήσεις κατακερματισμού[54]

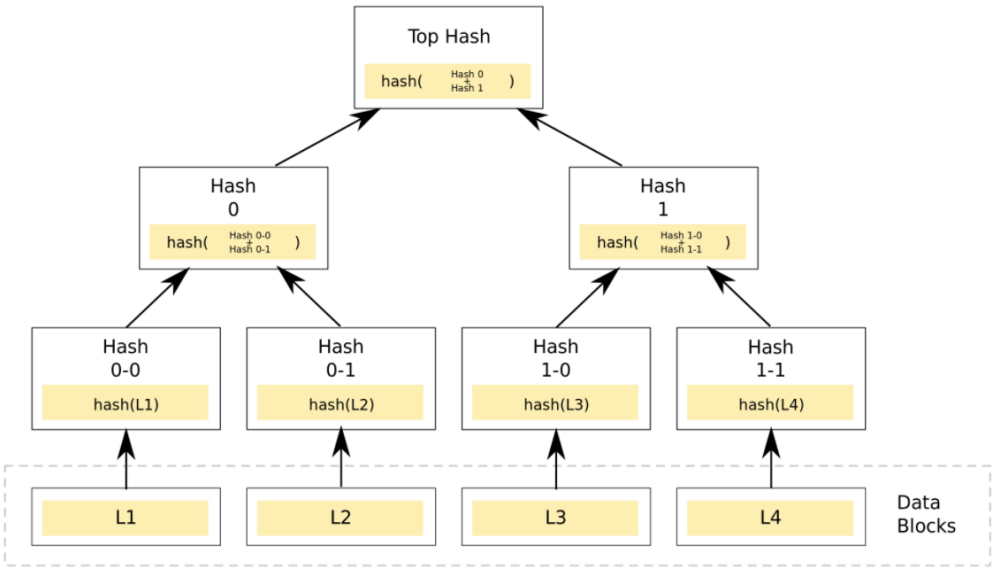
Ιδιότητες της συνάρτησης κατακερματισμού:

- Η είσοδος x είναι μια σειρά συμβόλων οποιουδήποτε μεγέθους.
- Η έξοδος h(x) είναι σταθερού μήκους, π.χ. 256 bits.
- Ο υπολογισμός της εξόδου h(x) από την είσοδο x να γίνεται εύκολα.
- Να είναι πρακτικά αδύνατο να βρεθούν συγκρούσεις, δηλαδή να βρεθούν δύο τιμές $x \neq y$ με $h(x) = h(y)$.
- Ο αντίστροφος υπολογισμός, $h-1(x)$, να είναι πρακτικά αδύνατος.

Υπάρχουν διάφοροι μηχανισμοί έτσι ώστε οι συναρτήσεις κατακερματισμού να μπορούν να εφαρμοστούν και σε δεδομένα που αποτελούν σύνθεση άλλων ανεξάρτητων τμημάτων δεδομένων και επιστρέφουν μια hash τιμή για το σύνολο αυτών. Ένας αποδοτικός μηχανισμός για να επιτευχθεί αυτό είναι τα Merkle Trees [55].

3.2 Merkle Tree

Ένα Merkle tree είναι ένα δέντρο στο οποίο κάθε φύλλο (leaf node) χαρακτηρίζεται με τον κρυπτογραφικό κατακερματισμό ενός μπλοκ δεδομένων. Κάθε κόμβος χωρίς φύλλα (non-leaf node) χαρακτηρίζεται με τον κρυπτογραφικό κατακερματισμό των ετικετών των απογόνων του (child nodes). Τα Merkle tree επιτρέπουν την αποδοτική και ασφαλή επαλήθευση του περιεχομένου των μεγάλων δομών δεδομένων. Τα Merkle tree είναι μια γενίκευση καταλόγων κατακερματισμού και αλυσίδων κατακερματισμού.



Εικόνα 3.2 Παράδειγμα Merkle tree[56]

Για παράδειγμα, στην εικόνα hash 0 είναι αποτέλεσμα κατακερματισμού της συνένωσης hash 0-0 και hash 0-1. Δηλαδή, hash 0 = hash (hash (0-0) + hash (0-1)) όπου + δηλώνει συνένωση. Η απόδειξη ότι ένας κόμβος φύλλων είναι μέρος ενός δεδομένου δυαδικού Merkle tree απαιτεί τον υπολογισμό ενός αριθμού κατακερματισμών ανάλογων με τον λογάριθμο του αριθμού των κόμβων φύλλων του δέντρου. Αυτό έρχεται σε αντίθεση με τις λίστες κατακερματισμού, όπου ο αριθμός είναι ανάλογος με το αριθμός των ίδιων των κόμβων φύλλων.

Η έννοια των Merkle trees πήρε το όνομά της από τον Ralph Merkle[57], ο οποίος το κατοχύρωσε με δίπλωμα ευρεσιτεχνίας το 1979. Τα Merkle trees μπορούν να χρησιμοποιηθούν για την επαλήθευση οποιουδήποτε είδους δεδομένων που αποθηκεύονται, διαχειρίζονται και μεταφέρονται εντός και μεταξύ υπολογιστών. Μπορούν να βοηθήσουν για να διασφαλιστεί ότι τα μπλοκ δεδομένων τα οποία λαμβάνονται από άλλους peer, σε ένα δίκτυο P2P, λαμβάνονται άθικτα, αμετάβλητα και για να ελέγξουν ότι τα άλλα peer δεν ψεύδονται στέλνοντας ψεύτικα μπλοκ. Στο bitcoin και σε άλλα κρυπτονομίσματα, τα Merkle trees χρησιμεύουν για την αποτελεσματική και ασφαλή κωδικοποίηση δεδομένων blockchain.

Η αρχική εφαρμογή των δέντρων Merkle στο Bitcoin από τον Satoshi Nakamoto πραγματοποιεί το βήμα συμπίεσης της συνάρτησης κατακερματισμού σε υπερβολικό βαθμό, το οποίο μετριάζεται με τη χρήση fast Merkle Trees. Οι περισσότερες εφαρμογές κατακερματισμού είναι δυαδικές (δύο κόμβοι παιδία κάτω από κάθε κόμβο), αλλά μπορούν εξίσου να χρησιμοποιούν πολύ περισσότερους κόμβους παιδία κάτω από κάθε κόμβο. Συνήθως, μια κρυπτογραφική συνάρτηση κατακερματισμού όπως το SHA-2 χρησιμοποιείται για τον κατακερματισμό. Εάν το δέντρο κατακερματισμού χρειάζεται μόνο προστασία από ακούσια ζημιά, μπορούν να χρησιμοποιηθούν μη ασφαλή αθροίσματα ελέγχου.

Στην κορυφή ενός Merkle tree υπάρχει ένα root hash (ή master hash). Πριν από τη λήψη ενός αρχείου σε ένα δίκτυο P2P, στις περισσότερες περιπτώσεις το root hash αποκτάται από μια αξιόπιστη πηγή, για παράδειγμα έναν φίλο ή έναν ιστότοπο που είναι γνωστό ότι έχει καλές προτάσεις για λήψη αρχείων. Όταν το root hash είναι διαθέσιμο, το δέντρο κατακερματισμού μπορεί να ληφθεί από οποιαδήποτε μη αξιόπιστη πηγή, όπως κάθε κόμβο στο δίκτυο P2P. Στη συνέχεια, το ληφθέν Merkle tree ελέγχεται έναντι του αξιόπιστου root hash και εάν το Merkel tree είναι

κατεστραμμένο ή ψεύτικο, θα δοκιμαστεί ένα άλλο Merkle tree από άλλη πηγή έως ότου το πρόγραμμα εντοπίσει ένα που ταιριάζει με το root hash.

Η κύρια διαφορά από μια hash list είναι ότι, μια διακλάδωση του Merkle tree μπορεί να ληφθεί τι φορά και η ακεραιότητα κάθε διακλάδωσης μπορεί να ελεγχθεί αμέσως, παρόλο που ολόκληρο το δέντρο δεν είναι ακόμη διαθέσιμο. Για παράδειγμα, στην εικόνα, η ακεραιότητα του μπλοκ δεδομένων L2 μπορεί να επαληθευτεί αμέσως εάν το δέντρο περιέχει ήδη hash 0-0 και hash 1 με κατακερματισμό του μπλοκ δεδομένων και συνδυάζοντας επαναληπτικά το αποτέλεσμα με hash 0-0 και στη συνέχεια με το hash 1 και τέλος σύγκριση του αποτελέσματος με το root hash. Παρομοίως, η ακεραιότητα του μπλοκ δεδομένων L3 μπορεί να επαληθευτεί εάν το δέντρο έχει ήδη hash 1-1 και hash 0. Αυτό μπορεί να είναι ένα πλεονέκτημα δεδομένου ότι είναι αποτελεσματικό να χωριστούν τα αρχεία σε πολύ μικρά μπλοκ δεδομένων, έτσι ώστε να πρέπει να επαναλάβετε τη λήψη εάν υποστούν ζημιά. Το μέγεθος του hash tree ή hash list είναι ανάλογο με το μέγεθος των κατακερματισμένων αρχείων. Στην περίπτωση ενός hash tree, μπορεί να γίνει γρήγορη λήψη ενός μικρού κλάδου, να ελεγχθεί η ακεραιότητα του κλάδου και, στη συνέχεια, να ξεκινήσει η λήψη των μπλοκ δεδομένων.

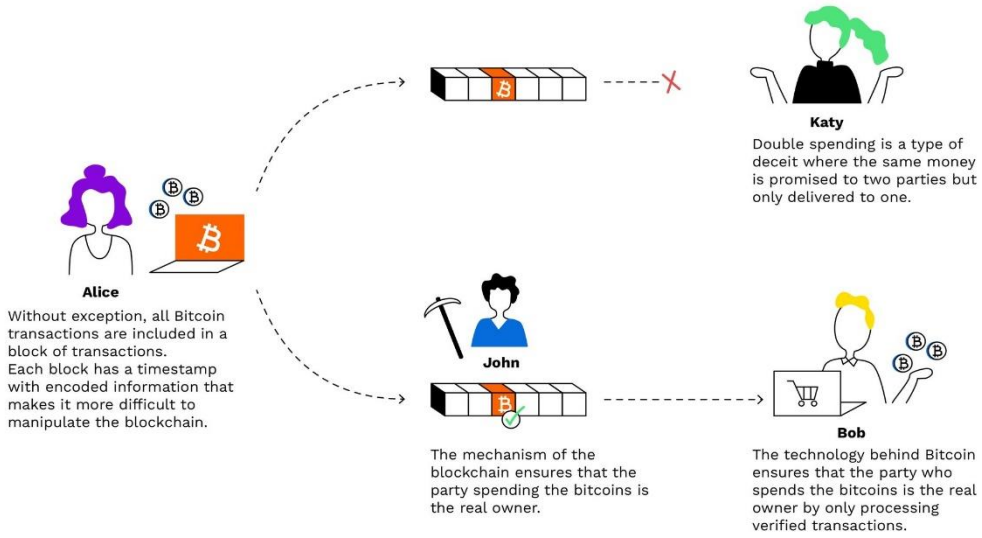
4 Τεχνολογία Blockchain

Σε αυτό το κεφάλαιο θα εξηγούμε την έννοια του blockchain αναλύοντας πώς λειτουργεί το Bitcoin, καθώς είναι εγγενώς συνδεδεμένο με το Bitcoin. Ωστόσο, η τεχνολογία blockchain μπορεί να εφαρμοστεί για οποιαδήποτε διαδικτυακή συναλλαγή ψηφιακών περιουσιακών στοιχείων.

4.1 Συναλλαγές στο Blockchain

Ορίζουμε ένα ηλεκτρονικό νόμισμα [58] ως μια αλυσίδα ψηφιακών υπογραφών. Κάθε κάτοχος μεταφέρει το νόμισμα στον επόμενο, υπογράφοντας ψηφιακά ένα κατακερματισμό της προηγούμενης συναλλαγής και μαζί με το δημόσιο κλειδί του επόμενου κατόχου προστίθενται στο τέλος του νομίσματος. Ο απολαβών μπορεί να επαληθεύσει τις υπογραφές για να επαληθεύσει την αλυσίδα ιδιοκτησίας.

Το πρόβλημα φυσικά είναι ότι ο απολαβών δεν μπορεί να επαληθεύσει ότι ένας από τους ιδιοκτήτες δεν ξόδεψε δυο φορές το ίδιο νόμισμα. Μια κοινή λύση είναι να εισαγάγετε μια αξιόπιστη κεντρική αρχή ή νομισματοκοπείο, η οποία ελέγχει κάθε συναλλαγή για διπλές δαπάνες (double spending [59]). Μετά από κάθε συναλλαγή, το νόμισμα πρέπει να επιστραφεί στο νομισματοκοπείο για να εκδώσει ένα νέο νόμισμα, διότι μόνο τα νομίσματα που εκδίδονται απευθείας από το νομισματοκοπείο δεν θεωρούνται διπλά. Το πρόβλημα με αυτήν τη λύση είναι ότι η τύχη ολόκληρου του χρηματικού συστήματος εξαρτάται από την οντότητα που διαχειρίζεται το νομισματοκοπείο, με κάθε συναλλαγή να πρέπει να επιβεβαιωθεί από εκείνη, όπως σε μια τράπεζα.



Εικόνα 4.1 Παράδειγμα double spending[60]

Χρειαζόμαστε έναν τρόπο ώστε ο απολαβών να γνωρίζει ότι οι προηγούμενοι κάτοχοι δεν υπέγραψαν προηγούμενες συναλλαγές. Για τους σκοπούς μας, η παλαιότερη συναλλαγή είναι αυτή που μετράει, επομένως δεν ενδιαφερόμαστε για μεταγενέστερες προσπάθειες διπλασιασμού. Ο μόνος τρόπος επιβεβαίωσης της απουσίας μιας συναλλαγής είναι να γνωρίζετε όλες τις συναλλαγές. Στο μοντέλο με βάση το νομισματοκοπείο, το νομισματοκοπείο γνώριζε όλες τις συναλλαγές και αποφάσισε ποια έφτασε πρώτη. Για να το πετύχουμε αυτό χωρίς τρίτο αξιόπιστο μέρος, οι συναλλαγές πρέπει να ανακοινώνονται δημόσια και χρειαζόμαστε ένα σύστημα στο οποίο οι συμμετέχοντες να συμφωνήσουν σε ένα μόνο ιστορικό της σειράς παραλαβής των συναλλαγών. Ο απολαβών χρειάζεται απόδειξη ότι κατά τη στιγμή κάθε συναλλαγής, η πλειοψηφία των κόμβων συμφώνησε ότι ήταν η πρώτη που ελήφθη.

Το Bitcoin χρησιμοποιεί κρυπτογραφική απόδειξη, αντί της επικύρωσης μιας αξιόπιστη κεντρικής αρχής, για τα δύο πρόθυμα μέρη να πραγματοποιήσουν μια συναλλαγή μέσω Διαδικτύου. Κάθε συναλλαγή προστατεύεται μέσω ψηφιακής υπογραφής.

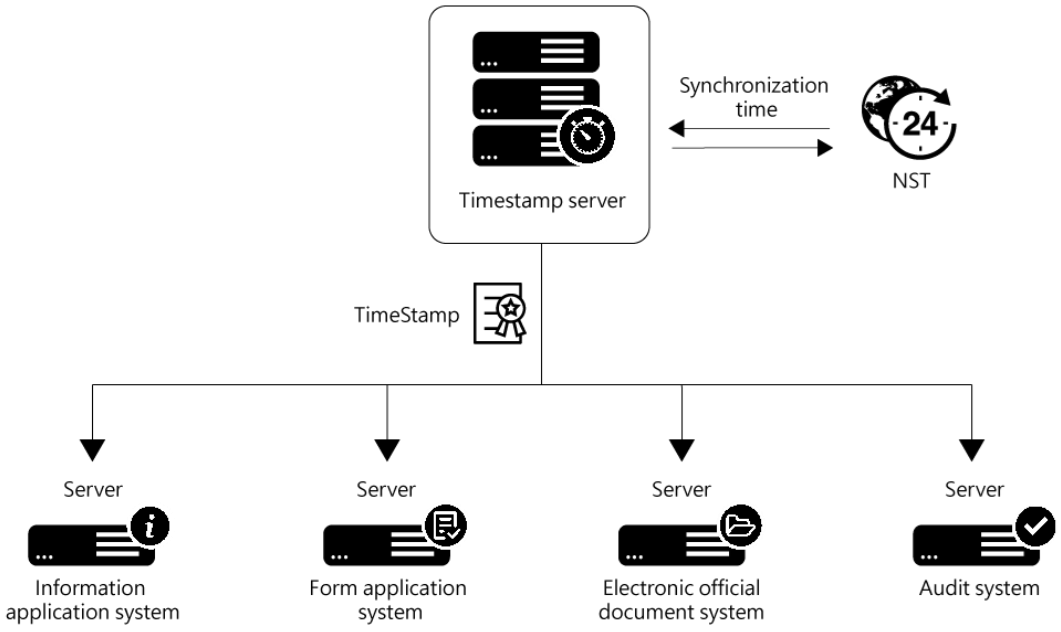
4.2 Blockchain

Το Bitcoin έλυσε αυτό το πρόβλημα με έναν μηχανισμό που είναι πλέον γνωστός ως τεχνολογία Blockchain. Το σύστημα Bitcoin ταξινομεί συναλλαγές τοποθετώντας τις σε ομάδες που ονομάζονται μπλοκ και στη συνέχεια συνδέοντας αυτά τα μπλοκ μέσω αυτού που ονομάζεται Blockchain. Οι συναλλαγές σε ένα μπλοκ θεωρείται ότι έχουν συμβεί ταυτόχρονα. Αυτά τα μπλοκ συνδέονται μεταξύ τους (όπως μια αλυσίδα) με μια σωστή γραμμική, χρονολογική σειρά με κάθε μπλοκ να περιέχει το hash του προηγούμενου μπλοκ.

Παραμένει όμως ένα ακόμα πρόβλημα. Οποιοσδήποτε κόμβος στο δίκτυο μπορεί να συλλέξει μη επιβεβαιωμένες συναλλαγές και να δημιουργήσει ένα μπλοκ και στη συνέχεια να το μεταδίδει στο υπόλοιπο δίκτυο ως πρόταση για το ποιο μπλοκ πρέπει να είναι το επόμενο στο blockchain. Το δίκτυο πρέπει να αποφασίσει ποιο μπλοκ είναι το σωστό για να το ενώσει πάνω στο blockchain. Μπορεί να υπάρχουν πολλά μπλοκ που δημιουργούνται από διαφορετικούς κόμβους ταυτόχρονα. Δεν μπορεί λοιπόν να πάρει την εξής απόφαση με βάση τη σειρά λήψης, καθώς τα μπλοκ μπορούν να φτάσουν με διαφορετική σειρά σε διαφορετικά σημεία του δικτύου.

4.3 Διακομιστής χρονικής σήμανσης

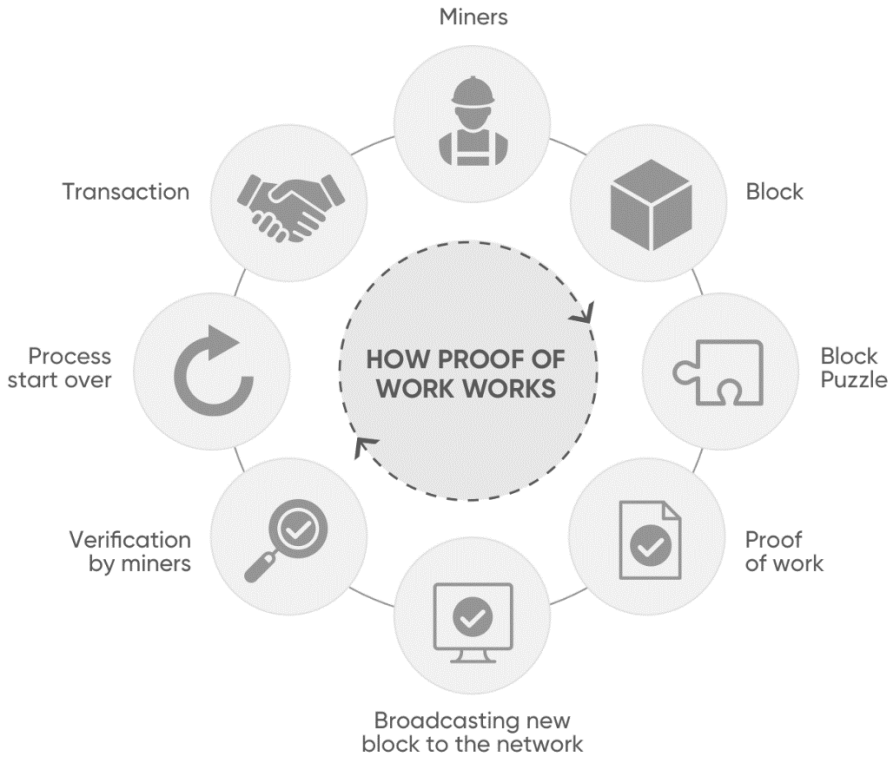
Η λύση που προτείνεται στο πρόβλημα του προηγούμενου κεφαλαίου ξεκινά με έναν διακομιστή χρονικής σήμανσης [61] σε βάση P2P. Ένας διακομιστής χρονικής σήμανσης λειτουργεί λαμβάνοντας ένα κατακερματισμό ενός μπλοκ αντικειμένων για χρονική σήμανση και δημοσιεύει ευρέως τον κατακερματισμό. Η χρονική σήμανση αποδεικνύει ότι τα δεδομένα πρέπει να υπήρχαν εκείνη τη στιγμή, προφανώς, για να μπουν στο κατακερματισμό. Κάθε χρονική σήμανση περιλαμβάνει την προηγούμενη χρονική σήμανση στο κατακερματισμό της, σχηματίζοντας μια αλυσίδα, με κάθε πρόσθετη χρονική σήμανση να ενισχύει αυτές που προηγούνται.



Εικόνα 4.2 Λειτουργεία διακομιστή χρονικής σήμανσης[62]

4.4 Απόδειξη εργασίας

Η απόδειξη εργασίας (PoW) είναι μια μορφή κρυπτογραφικής απόδειξης μηδενικής γνώσης στην οποία ένα μέρος (ο πάροχος) αποδεικνύει σε άλλους (τους επαληθευτές) ότι έχει χρησιμοποιήσει ορισμένη ποσότητα υπολογιστικής ισχύ για κάποιο σκοπό. Οι επαληθευτές μπορούν στη συνέχεια να επιβεβαιώσουν αυτές τις δαπάνες με ελάχιστη προσπάθεια εκ μέρους τους.



Εικόνα 4.3 Παραδείγματα proof-of-work[63]

Για να εφαρμόσουμε έναν Timestamp Server με βάση P2P, θα χρειαστεί να χρησιμοποιήσουμε ένα σύστημα PoW. Το PoW περιλαμβάνει σάρωση για μια τιμή που όταν κατακερματιστεί, όπως με το SHA-256, ο κατακερματισμός ξεκινά με έναν συγκεκριμένο αριθμό μηδέν bit. Η μέση απαιτούμενη εργασία είναι εκθετική στον αριθμό των μηδενικών bit που απαιτούνται και μπορεί να επαληθευτεί εκτελώντας ένα μόνο κατακερματισμό.

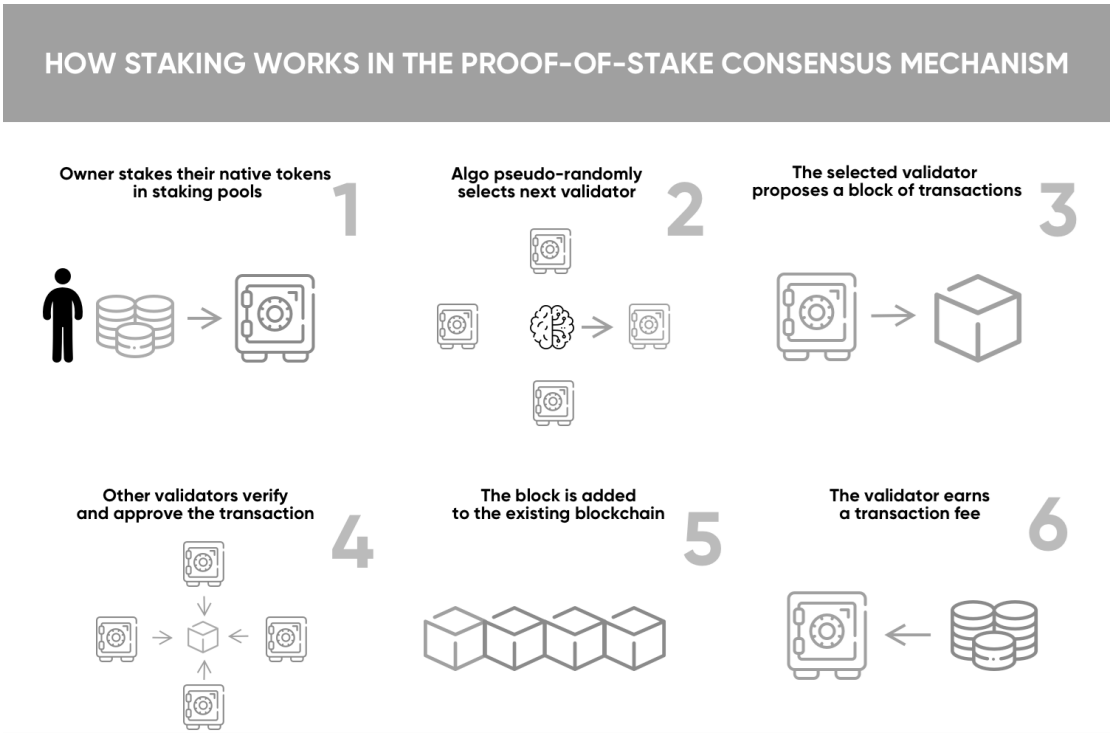
Για το δίκτυο χρονικής σήμανσης, εφαρμόζουμε το PoW αυξάνοντας το nonce στο μπλοκ μέχρι να βρεθεί μια τιμή που δίνει στο hash του μπλοκ τα απαιτούμενα μηδενικά bit. Μόλις δαπανηθεί η προσπάθεια της CPU για να ικανοποιήσει το PoW, το μπλοκ δεν μπορεί να αλλάξει χωρίς να επαναληφθεί η εργασία. Καθώς τα επόμενα μπλοκ είναι συνδεδεμένα μετά από αυτό, η εργασία για την αλλαγή του μπλοκ θα απαιτεί να ξαναγίνουν όλα τα μπλοκ μετά από αυτό.

Το PoW, επιλύει επίσης το πρόβλημα του καθορισμού της εκπροσώπησης στη λήψη αποφάσεων κατά πλειοψηφία. Εάν η πλειοψηφία βασίστηκε σε one-IP-address-one-vote, θα μπορούσε να ανατραπεί από οποιονδήποτε μπορεί να εκχωρήσει πολλές IP. Το PoW είναι ουσιαστικά one-CPU-one-vote. Η πλειοψηφική απόφαση αντιπροσωπεύεται από τη μεγαλύτερη αλυσίδα, η οποία έχει τη μεγαλύτερη προσπάθεια PoW που επενδύεται σε αυτήν. Εάν η πλειονότητα της ισχύος της CPU ελέγχεται από έντιμους κόμβους, η έντιμη αλυσίδα θα αναπτυχθεί ταχύτερα και ξεπερνά τις ανταγωνιστικές αλυσίδες. Για να τροποποιήσει ένα παλαιότερο μπλοκ, ένας εισβολέας θα πρέπει να επαναλάβει το PoW του μπλοκ και όλων των μπλοκ μετά από αυτό και στη συνέχεια να προλάβει και να ξεπεράσει το έργο των έντιμων κόμβων.

Για να αντισταθμιστεί η αύξηση της ταχύτητας υπολογισμού του υλικού και το ενδιαφέρον για τον υπολογισμό κόμβων με την πάροδο του χρόνου, η δυσκολία του PoW καθορίζεται από έναν κινούμενο μέσο όρο που στοχεύει έναν μέσο αριθμό μπλοκ ανά ώρα. Εάν δημιουργούνται πολύ γρήγορα, η δυσκολία αυξάνεται.

4.5 Απόδειξη συμμετοχής

Το PoS είναι ένας άλλος τύπος μηχανισμού συναίνεσης που χρησιμοποιείται από τα δίκτυα blockchain για την επίτευξη κατανεμημένης συναίνεσης. Απαιτεί από τους χρήστες να καταθέσουν (stake) όλο το κεφάλαιο τους για να γίνουν επικυρωτές στο δίκτυο. Οι επικυρωτές είναι υπεύθυνοι για το ίδιο πράγμα με τους miners στο PoW: να επιβλέπουν συναλλαγές και να δημιουργούν νέα μπλοκ, έτσι ώστε όλοι οι κόμβοι να μπορούν να συμφωνήσουν για την κατάσταση του δικτύου.



Εικόνα 4.4 Proof-of-Stake[63]

Το PoS συνοδεύεται από μια σειρά βελτιώσεων στο σύστημα PoW:

- Καλύτερη ενεργειακή απόδοση
- Χαμηλότερα εμπόδια εισόδου, μειωμένες απαιτήσεις υλικού: Όλοι έχουν την ευκαιρία να δημιουργήσουν νέα μπλοκ όχι μόνο εκείνοι με τεραστία υπολογιστική ισχύει
- Ισχυρότερη αντίσταση στο συγκεντρωτισμό: το PoS θα πρέπει να οδηγήσει σε περισσότερους κόμβους στο δίκτυο
- Ισχυρότερη υποστήριξη σε shard chains: μια βασική αναβάθμιση στην κλιμάκωση του δικτύου Ethereum

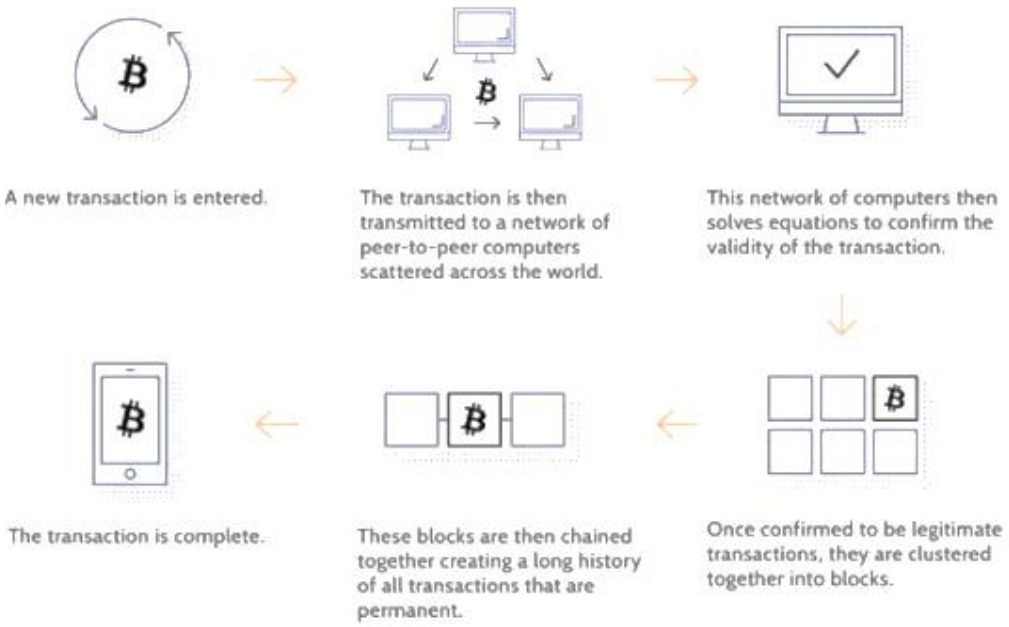
Σε αντίθεση με την απόδειξη εργασίας, οι επικυρωτές δεν χρειάζεται να χρησιμοποιούν σημαντικά ποσά υπολογιστικής ισχύος επειδή επιλέγονται τυχαία και δεν ανταγωνίζονται. Δεν χρειάζεται να εξορύξουν μπλοκ. Απλώς πρέπει να δημιουργούν μπλοκ όταν επιλέγονται και να επικυρώνουν τα προτεινόμενα μπλοκ όταν δεν είναι. Αυτή η επικύρωση είναι γνωστή ως attesting. Οι επικυρωτές λαμβάνουν ανταμοιβές για την πρόταση νέων μπλοκ και για τη βεβαίωση αυτών που έχουν δει. Εάν βεβαιώσουν ότι υπάρχουν κακόβουλα μπλοκ, χάνονται οι καταθέσεις τους.

Η απειλή μιας επίθεσης 51% εξακολουθεί να υπάρχει στο PoS, αλλά είναι ακόμη πιο επικίνδυνο για τους επιτιθέμενους. Για να συμβεί αυτό, θα πρέπει, ο επιτιθέμενους να κατέχει το 51% των κρυπτονομισμάτων που έχουν κατατεθεί. Όχι μόνο είναι πολλά χρήματα, αλλά πιθανότατα μια τέτοια κίνηση να προκαλούσε πτώση της αξίας του νομίσματος. Υπάρχουν πολύ λίγα κίνητρα για την καταστροφή την αξία ενός νομίσματος στο οποίο έχουν πλειοψηφικό μερίδιο. Υπάρχουν ισχυρότερα κίνητρα για την διατήρηση του δίκτυο ασφαλές και υγιές.

4.6 Δίκτυο Blockchain

Τα βήματα για την εκτέλεση συναλλαγών μέσα στο δίκτυο blockchain [64] είναι τα εξής:

- Νέες συναλλαγές μεταδίδονται σε όλους τους κόμβους
- Κάθε κόμβος συλλέγει νέες συναλλαγές σε ένα μπλοκ.
- Κάθε κόμβος εργάζεται για την εύρεση μιας απόδειξης PoW για το μπλοκ του.
- Όταν ένας κόμβος βρίσκει μια απόδειξη εργασίας, μεταδίδει το μπλοκ σε όλους τους κόμβους.
- Οι κόμβοι δέχονται το μπλοκ μόνο εάν όλες οι συναλλαγές σε αυτό είναι έγκυρες και δεν έχουν ήδη δαπανηθεί.
- Οι κόμβοι εκφράζουν την αποδοχή του μπλοκ δουλεύοντας στη δημιουργία του επόμενου μπλοκ στην αλυσίδα, χρησιμοποιώντας το κατακερματισμό του αποδεκτού μπλοκ ως το προηγούμενο κατακερματισμό.



Εικόνα 4.5 Τρόπος λειτουργείας Blockchain[65]

Κάθε συναλλαγή μεταδίδεται σε κάθε κόμβο στο δίκτυο Bitcoin και στη συνέχεια καταγράφεται σε δημόσιο καθολικό μετά την επαλήθευση. Κάθε συναλλαγή πρέπει να επαληθευτεί για εγκυρότητα προτού καταγραφεί στο δημόσιο καθολικό. Οι κόμβοι επαλήθευσης πρέπει να διασφαλίσουν δύο πράγματα πριν από την καταγραφή οποιασδήποτε συναλλαγής:

- Επαλήθευση ψηφιακής υπογραφής στη συναλλαγή (ο αποστολέας να έχει στην κατοχή του το κρυπτονόμισμα).
- Επαλήθευση επαρκές υπολοίπου (έλεγχος κάθε συναλλαγής απέναντι στον λογαριασμό του αποστολέα ("δημόσιο κλειδί") στο καθολικό).

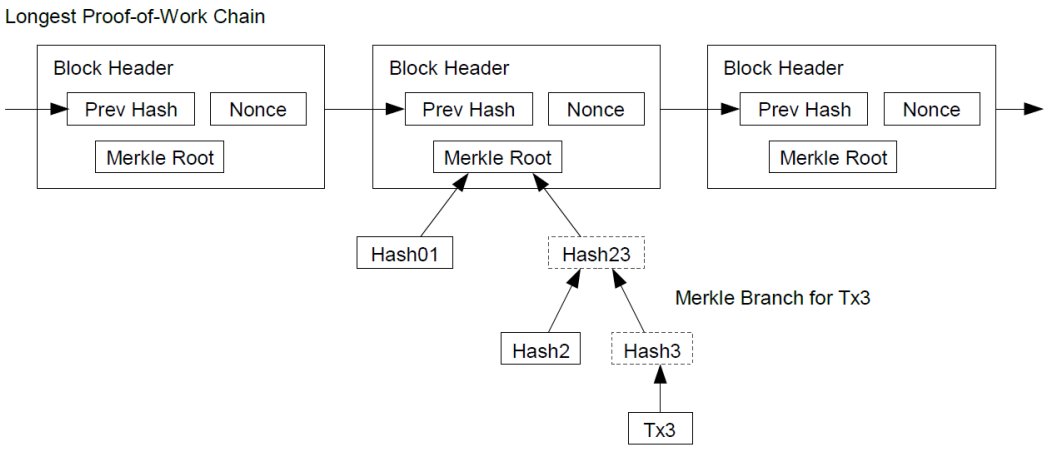
Οι κόμβοι, θεωρούν πάντα τη μεγαλύτερη αλυσίδα ως τη σωστή και θα συνεχίσουν να εργάζονται για την επέκτασή της. Υπάρχει πολύ μικρή πιθανότητα να δημιουργηθούν περισσότερα από ένα block στο σύστημα σε μια δεδομένη στιγμή. Ο πρώτος κόμβος που θα βρει το nonce, μεταδίδει το μπλοκ στο υπόλοιπο δίκτυο. Παρόλα αυτά εάν δύο κόμβοι μεταδίδουν ταυτόχρονα διαφορετικές εκδόσεις του επόμενου μπλοκ, ορισμένοι κόμβοι θα λάβουν τη μια έκδοση και ορισμένο την άλλη. Σε αυτήν την περίπτωση, οι κόμβοι ενημερώνονται με το πρώτο που έλαβαν, αλλά αποθηκεύουν και την άλλη έκδοση, ως διακλάδωση, σε περίπτωση που αυτή γίνει μεγαλύτερη. Η ισοδυναμία θα σπάσει όταν βρεθεί το επόμενο PoW και μια διακλάδωση γίνει μεγαλύτερη από την άλλη. Σε αυτή την περίπτωση οι κόμβοι που είχαν ενημερωθεί με την μικρότερη θα αλλάξουν και θα ενημερωθούν με αυτούς της μεγαλύτερης διακλάδωσης.

Οι μεταδόσεις νέων συναλλαγών δεν χρειάζεται απαραίτητα να φτάσουν σε όλους τους κόμβους, αρκεί να φτάσουν σε αρκετούς κόμβους, ώστε να μπουν σε ένα μπλοκ σύντομα. Η μετάδοση των μπλοκ είναι επίσης ανεκτική σε απώλειες μηνυμάτων. Εάν ένας κόμβος δεν λάβει ένα μπλοκ, θα το ζητήσει όταν παραλάβει το επόμενο μπλοκ και θα συνειδητοποιήσει την έλλειψη του.

4.7 Λόγοι υποστήριξης αλυσίδας

Κατά κανόνα, η πρώτη συναλλαγή σε κάποιο blockchain είναι μια ειδική συναλλαγή που ξεκινά ένα νέο νόμισμα που ανήκει στον δημιουργό του blockchain και ονομάζεται Genesis Block[66]. Αυτό προσθέτει ένα κίνητρο για τους κόμβους να υποστηρίξουν το δίκτυο και παρέχει έναν τρόπο για την αρχική διανομή κερμάτων σε κυκλοφορία, καθώς δεν υπάρχει κεντρική αρχή για την έκδοσή τους. Η σταθερή προσθήκη ενός ποσού νέων νομισμάτων είναι ανάλογη με τους ανθρακωρύχους που δαπανούν χρόνο και πόρους για να εξορύξουν χρυσό. Στην περίπτωσή μας, είναι ο χρόνος υπολογιστικής ισχύς της CPU και το ηλεκτρικό ρεύμα που δαπανώνται.

Το κίνητρο μπορεί επίσης να χρηματοδοτηθεί με τέλη συναλλαγής. Εάν η αξία εξόδου μιας συναλλαγής είναι μικρότερη από την αξία εισόδου της, η διαφορά είναι ένα τέλος συναλλαγής που προστίθεται στην αξία κινήτρου του μπλοκ που περιέχει τη συναλλαγή. Μόλις τεθεί σε κυκλοφορία ένας προκαθορισμένος αριθμός κερμάτων, το κίνητρο μπορεί να μεταβεί εξ ολοκλήρου σε τέλη συναλλαγής και να είναι εντελώς απαλλαγμένο από τον πληθωρισμό.



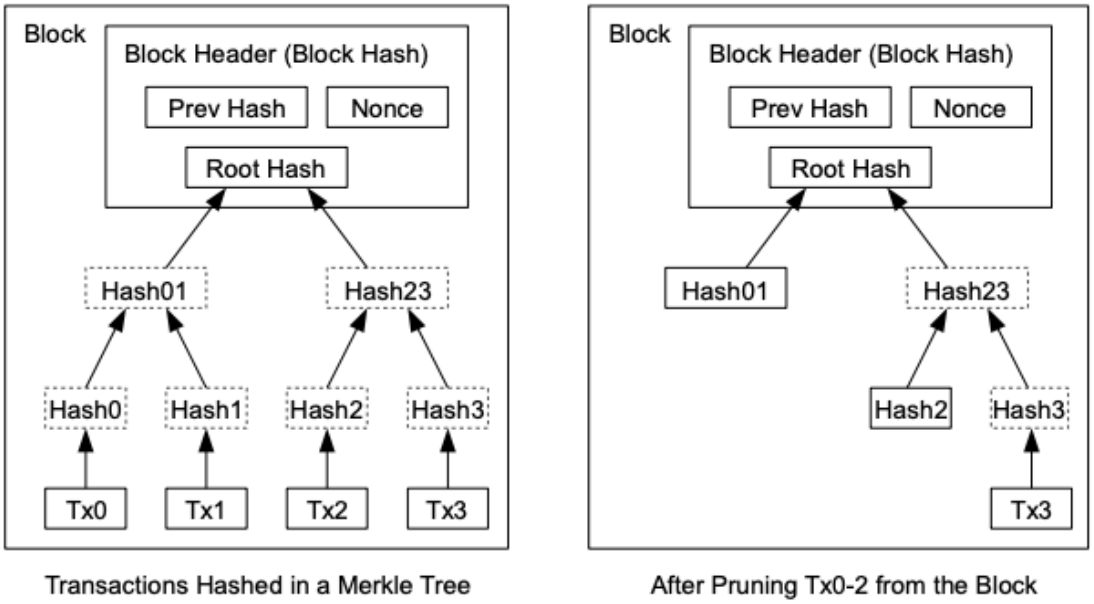
Εικόνα 4.6 Δομή block στο blockchain[67]

Οι κόμβοι που δωρίζουν τους υπολογιστικούς τους πόρους προς την επίλυση του nonce, και τη δημιουργία blocks ονομάζονται «miner nodes» και ανταμείβονται οικονομικά για τις προσπάθειές τους. Το κίνητρο μπορεί να βοηθήσει στην ενθάρρυνση των κόμβων να παραμείνουν έμπιστοι. Εάν ένας εισβολέας είναι σε θέση να συγκεντρώσει περισσότερη υπολογιστική ισχύ από όλους τους υπόλοιπους κόμβους, θα πρέπει να επιλέξει ανάμεσα στη χρήση των πόρων του, για να εξαπατήσει

τους χρήστες διπλοχρεώνοντας τους, είτε χρησιμοποιώντας τους για την δημιουργία νέων νομισμάτων. Συνεπώς η τήρηση των κανόνων θα πρέπει να είναι πιο επικερδές. Αυτό επιτυγχάνεται δημιουργώντας ένα σύστημα στο οποίο η δημιουργία νέων κρυπτονομισμάτων, είναι ευκολότερη από την υπονόμευση του συστήματος και τη δ ιατήρηση της εγκυρότητας του μεριδίου του. Όπως προαναφέρθηκε, το δίκτυο δέχεται μόνο το μεγαλύτερο blockchain ως το έγκυρο. Ως εκ τούτου, είναι σχεδόν αδύνατο για έναν εισβολέα να εισαγάγει μια ψευδής συναλλαγή, καθώς δε χρειάζεται μόνο να δημιουργήσει ένα μπλοκ με την επίλυση του nonce, αλλά πρέπει ταυτόχρονα να αγωνιστεί υπολογιστικά με τους υπόλοιπους κόμβους για να δημιουργήσει τα μεταγενέστερα μπλοκ, προκειμένου να κάνει τους υπόλοιπους κόμβους να αποδεχθούν τη συναλλαγή και το block του ως το έγκυρο. Αυτή η εργασία γίνεται ακόμη πιο δύσκολη, καθώς τα block στο blockchain συνδέονται κρυπτογραφικά μεταξύ τους.

4.8 Ανάκτηση χώρου στο δίσκο

Μόλις η τελευταία συναλλαγή σε ένα νόμισμα “θάφτει” κάτω από αρκετά μπλοκ, οι παλιότερες συναλλαγές πριν από αυτήν θα μπορέσουν να διαγράφουν για εξοικονόμηση χώρου στο δίσκο. Για να διευκολυνθεί αυτό χωρίς να σπάσει το κατακερματισμό του μπλοκ, οι συναλλαγές κατακερματίζονται σε ένα Merkle Tree, με μόνο τη ρίζα που περιλαμβάνεται στο κατακερματισμό του μπλοκ. Τα παλιά μπλοκ μπορούν στη συνέχεια να συμπιεστούν απομακρύνοντας τα κλαδιά του δέντρου. Οι



Εικόνα 4.7 Σύνδεση block στο blockchain[69]

εσωτερικοί κατακερματισμοί δεν χρειάζεται να αποθηκευτούν. Μια κεφαλίδα μπλοκ χωρίς συναλλαγές θα ήταν περίπου 80 byte. Αν υποθέσουμε ότι δημιουργούνται μπλοκ κάθε 10 λεπτά, 80 bytes * 6 * 24 * 365 = 4,2MB ανά έτος [68].

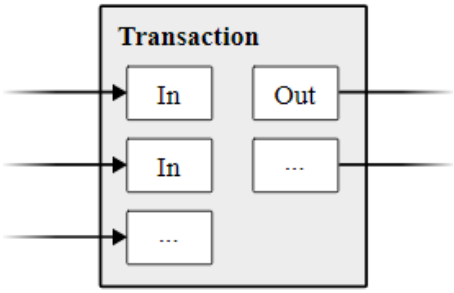
4.9 Απλοποιημένη επαλήθευση πληρωμής

Είναι δυνατή η επαλήθευση πληρωμών[70] χωρίς να εκτελείται ένας πλήρης κόμβος δικτύου. Ένας χρήστης πρέπει να κρατήσει μόνο ένα αντίγραφο των κεφαλίδων μπλοκ της μακρύτερης αλυσίδας PoW, το οποίο μπορεί να πάρει ζητώντας κόμβους δικτύου μέχρι να πειστεί ότι έχει τη μεγαλύτερη αλυσίδα και να αποκτήσει την διακλάδωση Merkle που συνδέει τη συναλλαγή με το μπλοκ στο οποίο έχει κάνει timestamp. Δεν μπορεί να ελέγξει τη συναλλαγή μόνος του, αλλά συνδέοντάς την με ένα μέρος στην αλυσίδα, μπορεί να δει ότι ένας κόμβος δικτύου το έχει αποδεχτεί και αν προστέθηκαν μπλοκ μετά από αυτό για να επιβεβαιώσει περαιτέρω ότι το δίκτυο το έχει αποδεχτεί.

Ως εκ τούτου, η επαλήθευση είναι αξιόπιστη εφ' όσον οι τίμιοι κόμβοι ελέγχουν το δίκτυο, αλλά είναι πιο ευάλωτο εάν το δίκτυο έχει κυριευτεί από έναν εισβολέα. Ενώ οι κόμβοι δικτύου μπορούν να επαληθεύσουν τις συναλλαγές τους, η απλοποιημένη μέθοδος μπορεί να ξεγελαστεί από τις κατασκευασμένες συναλλαγές ενός εισβολέα για όσο χρονικό διάστημα ο εισβολέας μπορεί να συνεχίσει να κυριεύει το δίκτυο. Μία στρατηγική για την προστασία από αυτό θα ήταν η αποδοχή ειδοποιήσεων από κόμβους δικτύου όταν εντοπίζουν ένα μη έγκυρο μπλοκ, ζητώντας από το λογισμικό του χρήστη να κατεβάσει ολόκληρο το μπλοκ και τις ενημερωμένες συναλλαγές για να επιβεβαιώσει την αντίφαση. Οι επιχειρήσεις που λαμβάνουν συχνές πληρωμές πιθανότατα θα εξακολουθούν να θέλουν να λειτουργούν τους δικούς τους κόμβους για πιο ανεξάρτητη ασφάλεια και ταχύτερη επαλήθευση.

4.10 Συνδυασμός και διαίρεση συναλλαγών σε block

Αν και θα ήταν δυνατόν να χειριστείτε νομίσματα μεμονωμένα, θα ήταν δύσκολο να κάνετε μια ξεχωριστή συναλλαγή για κάθε σεντ σε μια μεταφορά. Για να επιτρέπεται ο διαχωρισμός και ο συνδυασμός της αξίας, οι συναλλαγές περιέχουν πολλαπλές εισόδους και εξόδους[71]. Κανονικά θα υπάρχει είτε μία είσοδος από μια μεγαλύτερη προηγούμενη συναλλαγή είτε πολλαπλές εισόδους που συνδυάζουν μικρότερα ποσά, και το πολύ δύο εξόδους: μία για την πληρωμή και μία επιστρέφει την αλλαγή, εάν υπάρχει, πίσω στον αποστολέα.



Εικόνα 4.8 Δομή συναλλαγών block [72]

Πρέπει να σημειωθεί ότι το fan-out[71], όπου μια συναλλαγή εξαρτάται από πολλές συναλλαγές, και αυτές οι συναλλαγές εξαρτώνται από πολλές άλλες, δεν αποτελεί πρόβλημα εδώ. Δεν υπάρχει ποτέ η ανάγκη εξαγωγής ενός πλήρους αυτόνομου αντιγράφου του ιστορικού μιας συναλλαγής.

4.11 Απόρρητο

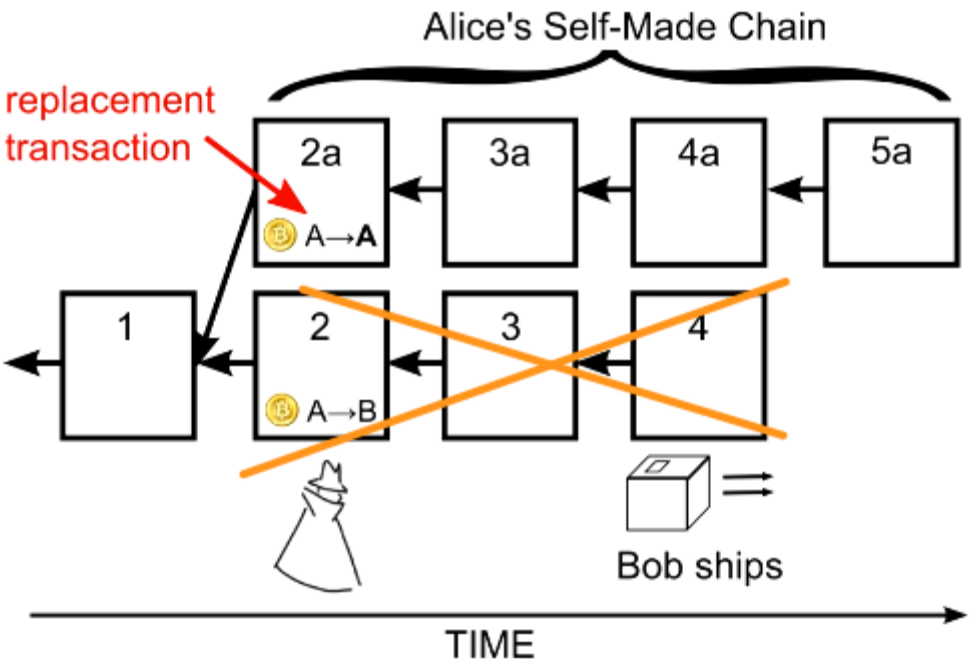
Το παραδοσιακό τραπεζικό μοντέλο επιτυγχάνει ένα επίπεδο απορρήτου περιορίζοντας την πρόσβαση σε πληροφορίες στα εμπλεκόμενα μέρη και στον αξιόπιστο τρίτο. Η ανάγκη δημοσίευσης όλων των συναλλαγών δημόσια αποκλείει αυτήν τη μέθοδο, αλλά το απόρρητο εξακολουθεί να διατηρείται διατηρώντας τα δημόσια κλειδιά ανώνυμα. Το κοινό μπορεί να δει ότι κάποιος στέλνει ένα ποσό σε κάποιον άλλο, αλλά χωρίς πληροφορίες που συνδέουν τη συναλλαγή με οποιονδήποτε. Αυτό είναι παρόμοιο με το επίπεδο πληροφοριών που κυκλοφόρησαν από τα χρηματιστήρια, όπου ο χρόνος και το μέγεθος των μεμονωμένων συναλλαγών, δημοσιοποιείται, αλλά χωρίς να πούμε ποια ήταν τα μέρη.

Ως πρόσθετο τείχος προστασίας, πρέπει να χρησιμοποιείται ένα νέο ζεύγος κλειδιών για κάθε συναλλαγή, ώστε να μην συνδέεται με έναν κοινό κάτοχο. Ορισμένες συνδέσεις εξακολουθούν να είναι αναπόφευκτες με συναλλαγές πολλαπλών εισόδων, οι οποίες αποκαλύπτουν απαραίτητα ότι οι καταχωρήσεις τους ανήκαν στον ίδιο κάτοχο. Ο κίνδυνος είναι ότι εάν αποκαλυφθεί ο κάτοχος ενός κλειδιού, η σύνδεση θα μπορούσε να αποκαλύψει άλλες συναλλαγές που ανήκαν στον κάτοχο.

4.12 Πιθανότητα επιτυχίας επιτιθέμενου

Θεωρούμε το σενάριο[73] ενός εισβολέα που προσπαθεί να δημιουργήσει μια εναλλακτική αλυσίδα γρηγορότερα από την ειλικρινή αλυσίδα. Ακόμα κι αν αυτό επιτευχθεί, δεν αφήνει το σύστημα ανοιχτό σε αυθαίρετες αλλαγές, όπως η δημιουργία αξίας από το πουθενά ή η λήψη χρημάτων που δεν ανήκαν ποτέ στον εισβολέα. Οι κόμβοι δεν πρόκειται να αποδεχτούν μια μη έγκυρη συναλλαγή ως πληρωμή και οι ειλικρινείς κόμβοι δεν θα αποδεχθούν ποτέ ένα μπλοκ που τις περιέχει. Ένας εισβολέας μπορεί να προσπαθήσει να αλλάξει μόνο μία από τις συναλλαγές του για

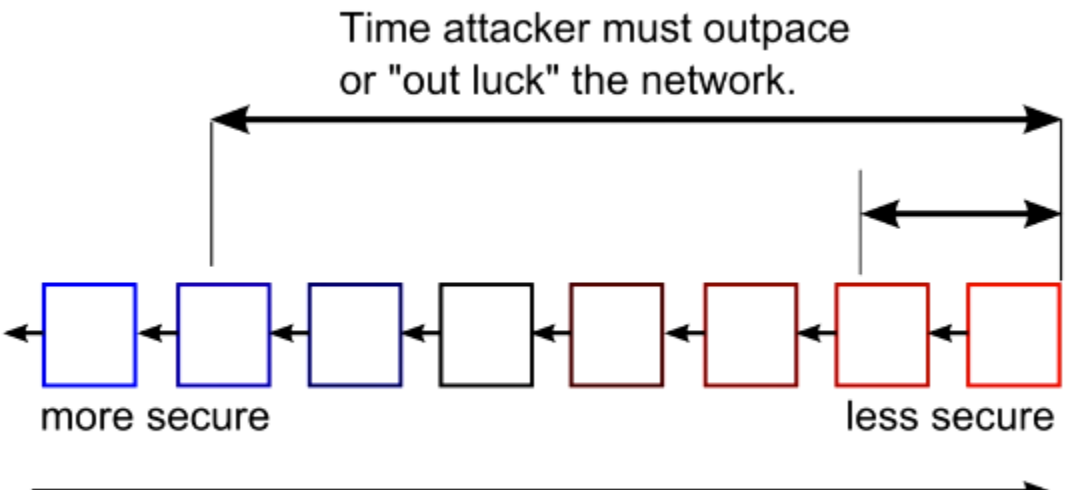
να πάρει πίσω χρήματα που ξόδεψε πρόσφατα. Ο αγώνας μεταξύ της έντιμης αλυσίδας και της αλυσίδας επιτιθέμενου μπορεί να χαρακτηριστεί ως Binomial Random Walk[74]. Το συμβάν επιτυχίας είναι η έντιμη αλυσίδα να επεκτείνεται κατά ένα μπλοκ, αυξάνοντας το προβάδισμά της κατά +1, και το γεγονός αποτυχίας είναι η αλυσίδα του επιτιθέμενου να επεκτείνεται κατά ένα μπλοκ, μειώνοντας τη διαφορά κατά -1.



Εικόνα 4.9 Προσπάθεια δημιουργίας εναλλακτική αλυσίδα[75]

Η πιθανότητα ενός επιτιθέμενου να ξεπεράσει ένα δεδομένο έλλειμμα, είναι ανάλογη με το πρόβλημα Gambler's Ruin [76]. Ας υποθέσουμε ότι ένας παίκτης με απεριόριστη πίστωση ξεκινά με έλλειμμα και παίζει δυνητικά έναν άπειρο αριθμό δοκιμών, για να προσπαθήσει να φτάσει στο σημείο εξισορρόπησης. Μπορούμε να υπολογίσουμε την πιθανότητα να φτάσει στο σημείο αυτό, ή την πιθανότητα, δηλαδή, ένας επιτιθέμενος να φτάσει το μήκος της ειλικρινής αλυσίδας, ως εξής:

Δεδομένης της υπόθεσής μας ότι p> q, η πιθανότητα q_z μειώνεται εκθετικά καθώς ο αριθμός τον μπλοκ που πρέπει να καλύψει ο επιτιθέμενος αυξάνεται. Οι πιθανότητές



Εικόνα 4.10 Επίπεδα ασφαλείας των μπλοκ[77]

του, ελαχιστοποιούνται σε περίπτωση που η ταχύτητα επίλυσης του επόμενου block είναι μικρότερη ή ίση από αυτή της έντιμης αλυσίδας.

Εξετάζουμε τώρα πόσο καιρό πρέπει να περιμένει ο παραλήπτης μιας νέας συναλλαγής, προτού να είμαστε βέβαιοι, ότι ο αποστολέας δεν μπορεί να τροποποιήσει τη συναλλαγή. Υποθέτουμε ότι πραγματοποιείται μία συναλλαγή μεταξύ δύο ατόμων. Αρχικά ο αποστολέας πραγματοποιεί την συναλλαγή προσωρινά και στην συνέχεια ξεγελάει το σύστημα, τροποποιώντας την, με σκοπό την αντιστροφή της μετά από κάποιο χρονικό διάστημα. Ο παραλήπτης θα ειδοποιηθεί όταν συμβεί αυτό, αλλά ο αποστολέας ελπίζει ότι θα είναι πολύ αργά.

Ο παραλήπτης δημιουργεί ένα νέο ζεύγος κλειδιών και δίνει το δημόσιο κλειδί στον αποστολέα λίγο πριν την υπογραφή. Αυτό εμποδίζει τον αποστολέα να προετοιμάσει μια αλυσίδα μπλοκ εκ των προτέρων, δουλεύοντας συνεχώς, έως ότου είναι αρκετά τυχερός για να μπορέσει να προηγηθεί, εκτελώντας τη συναλλαγή εκείνη τη στιγμή. Μόλις αποσταλεί η συναλλαγή, ο ανέντιμος αποστολέας αρχίζει να εργάζεται κρυφά σε μια παράλληλη αλυσίδα που περιέχει μια εναλλακτική έκδοση της συναλλαγής του.

Ο παραλήπτης περιμένει έως ότου η συναλλαγή έχει προστεθεί σε ένα μπλοκ και z μπλοκ έχουν συνδεθεί μετά από αυτό. Δεν ξέρει την ακριβή πρόοδο που έχει σημειώσει ο επιτιθέμενος, αλλά αν υποθέσουμε ότι τα ειλικρινεί μπλοκ χρειάστηκαν τον μέσο αναμενόμενο χρόνο ανά μπλοκ, η πιθανή πρόοδος του εισβολέα θα είναι μια κατανομή Poisson με αναμενόμενη αξία:

$$\lambda = z\frac{q}{p}$$

Για να υπολογίσουμε την πιθανότητα ότι ο επιτιθέμενος θα μπορούσε ακόμα και τώρα να προφτάσει την ειλικρινή αλυσίδα, πολλαπλασιάζουμε την πυκνότητα του Poisson για κάθε πρόοδο που θα μπορούσε να έχει σημειώσει με την πιθανότητα να μπορούσε να προφτάσει αυτό από το σημείο:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Αναδιάταξη για να αποφευχθεί το άθροισμα της άπειρης ουράς της κατανομής:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

Μετατροπή σε κώδικα γλωσσάς C:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z){
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++){
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
```

```
    }
    return sum;
}
```

Θέτοντας σαν q=0.1 τα αποτελέσματα ως προς P είναι:

Τιμή z	Αποτελέσματα P
0	1.0000000
1	0.2045873
2	0.0509779
3	0.0131722
4	0.0034552
5	0.0009137
6	0.0002428
7	0.0000647
8	0.0000173
9	0.0000046
10	0.0000012

Πίνακας 1: πιθανότητα επιτυχίας επίθεσης

5 Κατηγορίες Blockchains

5.1 Δημοσία Blockchain

Αν κάποιος επιθυμεί να δημιουργήσει ένα εντελώς ανοιχτό blockchain, παρόμοιο με το Bitcoin, το οποίο επιτρέπει σε όλους να ενταχθούν και να συνεισφέρουν στο δίκτυο, μπορεί να επιλέξει ένα δημόσιο blockchain [78]. Σε ένα δημόσιο blockchain, όλοι είναι ελεύθεροι να συμμετέχουν στις βασικές δραστηριότητες του δικτύου blockchain. Οποιοσδήποτε μπορεί να διαβάσει, να γράψει και να ελέγξει τις συνεχιζόμενες δραστηριότητες στο δημόσιο δίκτυο blockchain, το οποίο βοηθά ένα δημόσιο blockchain να διατηρήσει την αυτοδιοικούμενη φύση του.

Το δημόσιο δίκτυο λειτουργεί βάσει ενός συστήματος παροχής κινήτρων που ενθαρρύνει την συμμετοχή και την διατήρηση του δικτύου ευέλικτο. Οι δημόσιες αλυσίδες προσφέρουν μια ιδιαίτερα σημαντική λύση από την άποψη μιας πραγματικά αποκεντρωτικής, εκδημοκρατισμένης και χωρίς εξουσία λειτουργίας.

Υπάρχουν όμως και αρκετά μειονεκτήματα σε ένα δημόσιο blockchain. Το κύριο είναι η μεγάλη κατανάλωση ενέργειας που είναι απαραίτητη για τη διατήρηση του κατανεμημένου δημόσιου καθολικού. Άλλα ζητήματα περιλαμβάνουν την έλλειψη πλήρους ιδιωτικότητας και ανωνυμίας. Αυτό μπορεί να οδηγήσει σε ασθενέστερη ασφάλεια του δικτύου και της ταυτότητας του συμμετέχοντος. Κατά καιρούς οι συμμετέχοντες μπορεί επίσης να περιλαμβάνουν δόλια μέλη που μπορεί να εμπλέκονται σε κακόβουλες δραστηριότητες όπως πειρατεία, κλοπή token και συμφόρηση δικτύου.

5.2 Ιδιωτικά Blockchain

Τα ιδιωτικά blockchains [79] είναι υλοποιήσεις που απευθύνονται σε μια επιχείρηση ή σε μια ομάδα επιχειρήσεων με την ταυτότητα όλων των χρηστών του συστήματος να είναι γνωστή. Σε ένα ιδιωτικό blockchain δίνεται η δυνατότητα περιορισμού στο ποιος μπορεί να συνδεθεί σε αυτό. Πρόκειται στην ουσία για κατανεμημένες βάσεις δεδομένων που επιτρέπουν στα μέλη τους να αποφασίσουν για το ποιος μπορεί να συμμετάσχει στο μηχανισμό συναίνεσης και ποιοι μπορούν να επαληθεύουν τις συναλλαγές. Οι δε κόμβοι ενός ιδιωτικού blockchain αποκτούν τη δυνατότητα να εγγράφουν πληροφορίες στο blockchain μέσω των εγγεγραμμένων και επαληθευμένων μελών.

Σημαντικές περιπτώσεις ιδιωτικών blockchains είναι:

- Corda
- Hyperledger
- Multichain
- Quorum
- Sequence

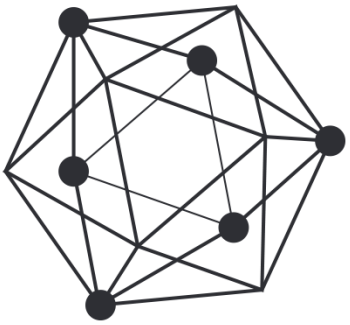
Εάν κάποιος χρειάζεται να λειτουργήσει ένα ιδιωτικό blockchains που επιτρέπει μόνο επιλεγμένη είσοδο επαληθευμένων συμμετεχόντων, όπως αυτές για μια ιδιωτική επιχείρηση, μπορεί να επιλέξει μια ιδιωτική εφαρμογή Blockchain. Ένας συμμετέχων μπορεί να εγγραφεί σε ένα τέτοιο ιδιωτικό δίκτυο μόνο μέσω μιας γνήσια και επαληθευμένης πρόσκλησης. Απαιτείται επίσης επικύρωση είτε από τον/τους χειριστή του δικτύου είτε από ένα σαφώς καθορισμένο πρωτόκολλο που εφαρμόζεται από το δίκτυο.

Η κύρια διάκριση μεταξύ του δημόσιου και του ιδιωτικού blockchains είναι ότι οι ιδιωτικές αλυσίδες μπλοκ ελέγχουν ποιος επιτρέπεται να συμμετέχει στο δίκτυο, εκτελεί το πρωτόκολλο συναίνεσης που αποφασίζει τα δικαιώματα και τις ανταμοιβές εξόρυξης και διατηρεί το κοινό καθολικό. Ο ιδιοκτήτης ή ο χειριστής έχει το δικαίωμα

να παρακάμψει, να επεξεργαστεί ή να διαγράψει τις απαραίτητες καταχωρήσεις στο blockchain, οπού θεωρείται αναγκαίο.

Στην πραγματικότητα, ένα ιδιωτικό blockchain δεν είναι αποκεντρωμένο, αλλά είναι ένα κατανεμημένο καθολικό που λειτουργεί ως μια κλειστή και ασφαλής βάση δεδομένων που βασίζεται σε έννοιες κρυπτογραφίας. Από τεχνική άποψη, δεν μπορούν όλοι να εκτελέσουν έναν πλήρη κόμβο στο ιδιωτικό blockchain, να πραγματοποιήσουν συναλλαγές ή να επικυρώσουν και να επαληθεύσουν τις αλλαγές του blockchain.

5.3 Hyperledger



Εικόνα 5.1 Hyperledger logo[81]

Το Hyperledger [80] είναι ένα παγκόσμιο έργο blockchain για επιχειρήσεις που προσφέρει το απαραίτητο πλαίσιο, πρότυπα, κατευθυντήριες γραμμές και εργαλεία για τη δημιουργία blockchain ανοιχτού κώδικα και σχετικές εφαρμογές για χρήση σε διάφορους κλάδους. Τα project της Hyperledger περιλαμβάνουν μια ποικιλία από πλατφόρμες blockchain που διαθέτουν άδεια για επιχειρήσεις, όπου οι συμμετέχοντες στο δίκτυο είναι γνωστοί μεταξύ τους και επομένως έχουν εγγενές ενδιαφέρον να συμμετάσχουν στη διαδικασία συναίνεσης.

Χρησιμοποιώντας τα διαθέσιμα στοιχεία κάτω από το ger umbrella, μια επιχείρηση μπορεί να εφαρμόσει διάφορες αρθρωτές λύσεις και υπηρεσίες blockchain για να βελτιώσει σημαντικά την απόδοση των λειτουργιών της και την αποτελεσματικότητα των επιχειρηματικών διαδικασιών της.

Το Hyperledger δημιουργήθηκε με στόχο την επιτάχυνση της συνεργασίας σε ολόκληρη τη βιομηχανία για την ανάπτυξη υψηλής απόδοσης και αξιόπιστης τεχνολογίας blockchain και κατανεμημένης τεχνολογίας καθολικό που θα μπορούσε να χρησιμοποιηθεί σε διάφορους κλάδους για τη βελτίωση της αποτελεσματικότητας, των επιδόσεων και των συναλλαγών των διαφόρων επιχειρησιακών διαδικασιών.

5.3.1 Hyperledger Fabric

Το Hyperledger Fabric [82] είναι ένα blockchain framework που ως βάση λειτουργίας του έχει την ανάπτυξη προϊόντων, λύσεων και εφαρμογών που βασίζονται σε blockchain χρησιμοποιώντας στοιχεία plug-and-play που προορίζονται για χρήση σε ιδιωτικές επιχειρήσεις.

Κύρια χαρακτηριστικά:

- Το Hyperledger είναι ένα εταιρικό πλαίσιο, ανοιχτού κώδικα κατανεμημένο λογιστικό που κυκλοφόρησε από το Linux Foundation τον Δεκέμβριο του 2015.
- Το Fabric είναι μια highly-modular πλατφόρμα, αποκεντρωμένης τεχνολογίας καθολικού (decentralized ledger technology, DLT) που σχεδιάστηκε από την IBM για βιομηχανική επιχειρηματική χρήση.
- Επειδή το Hyperledger Fabric είναι ιδιωτικό και απαιτεί άδεια πρόσβασης, οι επιχειρήσεις μπορούν να διαχωρίσουν πληροφορίες (όπως τιμές), καθώς και οι συναλλαγές μπορούν να επιταχυνθούν επειδή ο αριθμός των κόμβων στο δίκτυο είναι μειωμένος.
- Το Fabric 2.0 κυκλοφόρησε τον Ιανουάριο του 2020. Τα κύρια χαρακτηριστικά αυτής της έκδοσης είναι οι ταχύτερες συναλλαγές, η ενημερωμένη τεχνολογία έξυπνων συμβολαίων και η βελτιωμένη κοινή χρήση δεδομένων.

Τα παραδοσιακά δίκτυα blockchain δεν μπορούν να υποστηρίξουν ιδιωτικές συναλλαγές και εμπιστευτικές συμβάσεις που είναι υψίστης σημασίας για τις

επιχειρήσεις. Το Hyperledger Fabric σχεδιάστηκε ως απάντηση σε αυτό ως ένα modular, επεκτάσιμο και ασφαλές θεμέλιο για την προσφορά βιομηχανικών λύσεων blockchain.

Το Hyperledger Fabric είναι η μηχανή ανοιχτού κώδικα για το blockchain και φροντίζει για τα πιο σημαντικά χαρακτηριστικά για την αξιολόγηση και τη χρήση του blockchain για περιπτώσεις επιχειρηματικής χρήσης.

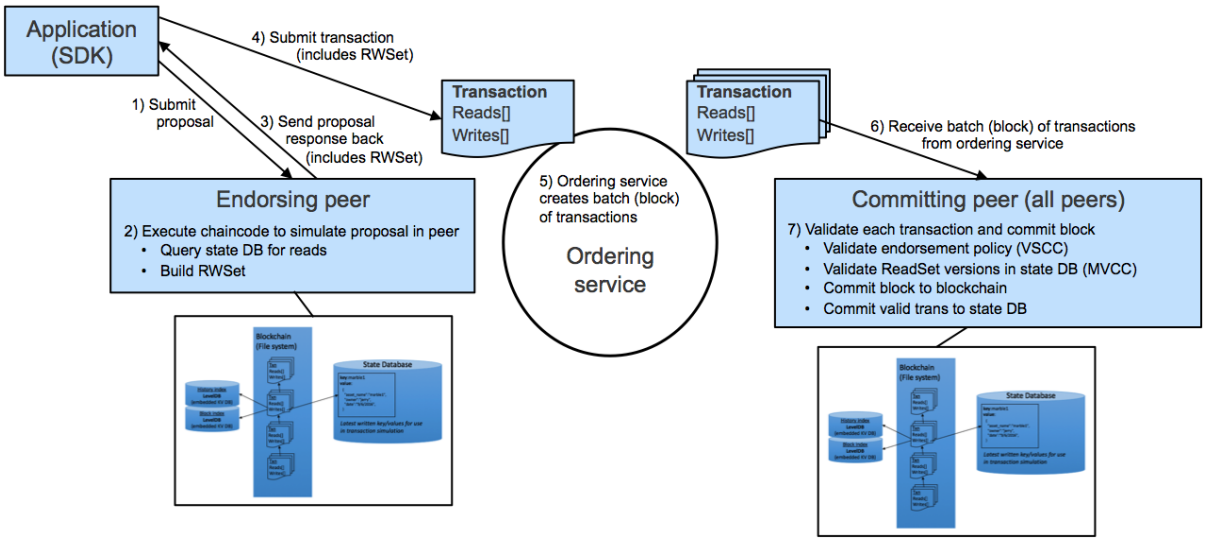
Στα ιδιωτικά βιομηχανικά δίκτυα, η επαληθεύσιμη ταυτότητα ενός συμμετέχοντος είναι πρωταρχική απαίτηση. Το Hyperledger Fabric υποστηρίζει συνδρομές βάσει άδειας. Όλοι οι συμμετέχοντες στο δίκτυο πρέπει να έχουν γνωστές ταυτότητες. Πολλοί επιχειρηματικοί τομείς, όπως η υγειονομική περίθαλψη και τα οικονομικά, δεσμεύονται από κανονισμούς προστασίας δεδομένων που επιβάλλουν τη διατήρηση δεδομένων σχετικά με τους διάφορους συμμετέχοντες και την αντίστοιχη πρόσβασή τους σε διάφορα σημεία δεδομένων. Το Fabric υποστηρίζει τέτοια συνδρομή βάσει άδειας.

Η modular αρχιτεκτονική του Hyperledger Fabric διαχωρίζει τη ροή εργασίας της επεξεργασίας συναλλαγών σε τρία διαφορετικά στάδια:

- έξυπνα συμβόλαια που ονομάζονται chaincode που περιλαμβάνουν την κατανεμημένη λογική επεξεργασία και συμφωνία του συστήματος
- παραγγελία συναλλαγών
- επικύρωση και δέσμευση συναλλαγής

Αυτός ο διαχωρισμός προσφέρει πολλαπλά οφέλη:

- Μειωμένος αριθμός επιπέδων εμπιστοσύνης και επαλήθευσης που διατηρεί το δίκτυο και την επεξεργασία χωρίς ακαταστασία
- Βελτιωμένη επεκτασιμότητα δικτύου
- Καλύτερη συνολική απόδοση



Εικόνα 5.2 Transaction lifecycle in v1.0 of Hyperledger Fabric[83]

Επιπλέον, η υποστήριξη του Hyperledger Fabric για plug-and-play διαφόρων εξαρτημάτων επιτρέπει την εύκολη επαναχρησιμοποίηση των υπαρχόντων χαρακτηριστικών και την έτοιμη ενσωμάτωση διαφόρων μονάδων. Για παράδειγμα, εάν υπάρχει ήδη μια συνάρτηση που επαληθεύει την ταυτότητα του συμμετέχοντος, ένα δίκτυο σε εταιρικό επίπεδο πρέπει απλώς να συνδέσει και να επαναχρησιμοποιήσει αυτήν την υπάρχουσα μονάδα αντί να δημιουργήσει την ίδια λειτουργία από την αρχή.

Οι συμμετέχοντες στο δίκτυο έχουν τρεις διακριτούς ρόλους:

- Εγκριτής (Endorser)
- Εκτελεστής (Committer)

- Συναίνων (Consenter)

Με λίγα λόγια, η πρόταση συναλλαγής υποβάλλεται στον έγκριτή σύμφωνα με την προκαθορισμένη πολιτική έγκρισης σχετικά με τον αριθμό των απαιτούμενων εγγραφών. Μετά από επαρκείς εγκρίσεις από τους έγκριτες, μια παρτίδα ή μπλοκ συναλλαγών παραδίδεται στους εκτελεστές. Οι εκτελεστές επικυρώνουν ότι ακολουθήθηκε η πολιτική έγκρισης και ότι δεν υπάρχουν αντικρουόμενες συναλλαγές. Μόλις γίνουν και οι δύο έλεγχοι, οι συναλλαγές καταχωρούνται στο καθολικό.

Εφόσον μόνο οδηγίες επιβεβαίωσης, όπως υπογραφές και σετ ανάγνωσης/εγγραφής, αποστέλλονται μέσω του δικτύου, η επεκτασιμότητα και η απόδοση του δικτύου βελτιώνονται. Μόνο οι έγκριτές και οι εκτελεστές έχουν πρόσβαση στη συναλλαγή που οδηγεί στην βελτίωση της ασφάλειας λόγο του περιορισμένου αριθμού συμμετεχόντων που έχουν πρόσβαση σε σημαντικά δεδομένα.

5.3.2 Hyperledger Burrow

Το Hyperledger Burrow [84] είναι ένα λογισμικό που μπορεί να χρησιμοποιηθεί για την εκτέλεση κόμβων σε ένα εξουσιοδοτημένο δίκτυο blockchain. Επειδή οι συμμετέχοντες σε επιτρεπόμενες blockchain είναι γνωστοί και αξιόπιστοι από το υπόλοιπο δίκτυο, είναι δυνατό να επιτευχθούν υψηλότερες ταχύτητες και απόδοση από τα δημοσία blockchain.

Σε αντίθεση με τα blockchain απόδειξης εργασίας όπως το Ethereum, το Hyperledger Burrow χρησιμοποιεί έναν αλγόριθμο συναίνεσης Βυζαντινής ανοχής σε σφάλματα για να καθορίσει την οριστικότητα της συναλλαγής. Δεν υπάρχει κόστος εξόρυξης ή συναλλαγής και μπορεί να εκτελέσει έξυπνα συμβόλαια σε πολύ μεγαλύτερη κλίμακα από τα δημοσία blockchain.

Αν και είναι παρόμοιο με πολλά άλλα εργαλεία Hyperledger blockchain, η εστίαση του Hyperledger Burrow είναι να παρέχει μια "καθαρή και απλή" εμπειρία προγραμματιστή, σύμφωνα με το Hyperledger Wiki[85]. Το βασικό στοιχείο του Hyperledger Burrow είναι μια εξουσιοδοτημένη εφαρμογή της Εικονικής Μηχανής Ethereum[86], η οποία της επιτρέπει να αλληλεπιδρά με έξυπνα συμβόλαια σε άλλα δίκτυα που βασίζονται στο Ethereum.

5.3.3 Hyperledger Explorer

Η αρχιτεκτονική του περιλαμβάνει έναν διακομιστή ιστού που εκτελείται στο backend και είναι υπεύθυνος για την αλληλεπίδραση με όλα τα άλλα στοιχεία και τη διατήρηση της απαραίτητης ερωτήματος και απόκρισης διακομιστή. Τα web sockets χρησιμοποιούνται για την επικοινωνία μεταξύ του διακομιστή και των διαφόρων στοιχείων Hyperledger Explorer [87] του πελάτη. Μια βάση δεδομένων RethinkDB χρησιμοποιείται για την αποθήκευση των απαραίτητων λεπτομερειών σχετικά με τα στοιχεία blockchain, όπως πληροφορίες σχετικά με μπλοκ, συναλλαγές και έξυπνα συμβόλαια, και αυτό μπορεί να ζητηθεί για οποιεσδήποτε απαραίτητες πληροφορίες. Ένα repository ασφαλείας φροντίζει να διασφαλίζει ότι διατηρείται μόνο ασφαλής και εξουσιοδοτημένη πρόσβαση για την είσοδο στον Hyperledger Explorer.

Το Hyperledger Explorer επιτρέπει μια ενοποιημένη οπτικοποίηση σε επίπεδο επιχείρησης, η οποία μπορεί να χρειαστεί σε πραγματικό χρόνο από έναν προγραμματιστή blockchain που αναπτύσσει μια συγκεκριμένη λειτουργία ή στοιχείο στο blockchain ή από έναν ερευνητή που επιδιώκει να μελετήσει ιστορικές εξελίξεις ή από υπεύθυνους χειριστές blockchain για τη διαχείριση του blockchain ή από την ανώτατη διοίκηση.

5.3.4 Hyperledger Composer

Το Hyperledger Composer [88] έχει υλοποιηθεί σε Javascript, μια γλώσσα προγραμματισμού platform-independent που υποστηρίζει επίσης τη χρήση ενσωματωμένων βιβλιοθηκών και χρησιμοποιεί διαθέσιμες λειτουργίες και scripts για να κάνει τις λειτουργίες επεκτάσιμες και επαναχρησιμοποιήσιμες. Το Composer είναι ένα framework ανάπτυξης εφαρμογών που απλοποιεί και επιταχύνει τη δημιουργία εφαρμογών blockchain Hyperledger fabric.

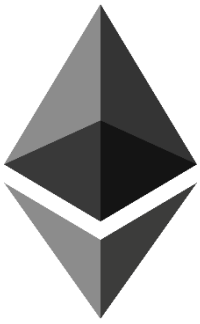
Χρησιμοποιώντας το Hyperledger Composer, ένας επιχειρηματίας χωρίς τεχνικές γνώσεις μπορεί εύκολα να συνεργαστεί με έναν προγραμματιστή για τη δημιουργία συγκεκριμένων λειτουργιών. Περιλαμβάνουν τον καθορισμό των επιχειρηματικών κανόνων βάσει των οποίων θα διεκπεραιώνονται οι συναλλαγές blockchain, τον ορισμό των περιουσιακών στοιχείων που ανταλλάσσονται σε περιπτώσεις χρήσης που βασίζονται σε blockchain και ορίζουν ελέγχους για τους συμμετέχοντες, την ταυτότητά τους, τους ρόλους και τα επίπεδα πρόσβασης για την εκτέλεση των διαφόρων ειδών συναλλαγών.

Ομοίως, ένας προγραμματιστής που χρησιμοποιεί το Hyperledger Composer μπορεί εύκολα να δημιουργήσει και να διαμορφώσει βασικά στοιχεία του blockchain που περιλαμβάνουν τα ψηφιακά στοιχεία του δικτύου, τη λογική των συναλλαγών, τους συμμετέχοντες και τα στοιχεία ελέγχου πρόσβασης. Το Composer υποστηρίζει την κοινή χρήση, την επαναχρησιμοποίηση και την επεκτασιμότητα των στοιχείων σε διάφορους οργανισμούς. Κάποιος μπορεί εύκολα να δημιουργήσει τα απαιτούμενα σενάρια και τα API που είναι απαραίτητα για την επιχειρηματική υλοποίηση χρησιμοποιώντας το Hyperledger Composer. Υποστηρίζει επίσης περιπτώσεις χρήσης και δοκιμές σε πραγματικό χρόνο, οι οποίες μπορούν να πραγματοποιηθούν ακόμη και μέσω του διαδικτυακού περιβάλλοντος του Composer χωρίς την ανάγκη τοπικών εγκαταστάσεων.

Χρησιμοποιώντας το Hyperledger Composer, είναι δυνατό για κάποιον να δημιουργήσει και να εκτελέσει ένα δείγμα blockchain και να χορηγήσει περιορισμένη άδεια σε διάφορους συμμετέχοντες. Για παράδειγμα, μπορεί κανείς εύκολα να δημιουργήσει ένα «Δίκτυο ευπαθών αγαθών» που διευκολύνει το εμπόριο ειδών όπως φρούτα και λαχανικά, περιλαμβάνει συμμετέχοντες όπως αγρότες, φορτωτές και εισαγωγείς, ορίζει μεμονωμένους ρόλους για κάθε συμμετέχοντα, παρακολουθεί αποστολές, αναγνώριση, παρακολούθηση και αναφορά της κατάστασης των αγαθών σε διάφορα στάδια της αλυσίδας εφοδιασμού και διαχείριση πληρωμών.

6 Ethereum

6.1 Ορισμός



Εικόνα 6.1 Ethereum logo[94]

Το Ethereum είναι ένα αποκεντρωμένο blockchain ανοιχτού κώδικα με λειτουργικότητα έξυπνων συμβολαίων. Το Ether [89] (ETH ή Ξ) είναι το εγγενές κρυπτονόμισμα της πλατφόρμας. Η πλατφόρμα επιτρέπει σε οποιονδήποτε να αναπτύξει μόνιμες και αμετάβλητες αποκεντρωμένες εφαρμογές σε αυτήν, με τις οποίες οι χρήστες μπορούν να αλληλοεπιδρούν. Οι εφαρμογές αποκεντρωμένης χρηματοδότησης (Decentralized finance, DeFi [90]) παρέχουν μια ευρεία γκάμα χρηματοοικονομικών υπηρεσιών χωρίς την ανάγκη τυπικών χρηματοοικονομικών ενδιάμεσων, όπως χρηματιστηριακές εταιρείες, ανταλλακτήρια ή τράπεζες, όπως να επιτρέπουν στους χρήστες κρυπτονομισμάτων να δανείζονται έναντι της περιουσία τους ή να τα δανείζουν για τόκους. Το Ethereum επιτρέπει επίσης τη δημιουργία και την ανταλλαγή NFT [91], τα οποία είναι μη εναλλάξιμες λεκτικές μονάδες που συνδέονται με ψηφιακά έργα τέχνης ή άλλα αντικείμενα του πραγματικού κόσμου και πωλούνται ως μοναδική ψηφιακή ιδιοκτησία. Επιπλέον, πολλά άλλα κρυπτονομίσματα λειτουργούν ως λεκτικές μονάδες ERC-20 [92] βασισμένες στο Ethereum blockchain και έχουν χρησιμοποιήσει την πλατφόρμα για προσφορές αρχικών νομισμάτων.

Το Ethereum έχει αρχίσει να εφαρμόζει μια σειρά αναβαθμίσεων που ονομάζονται Ethereum 2.0 [93], η οποία περιλαμβάνει μια μετάβαση στο PoS και στοχεύει στην αύξηση της απόδοσης των συναλλαγών με χρήση διαμοιρασμού.

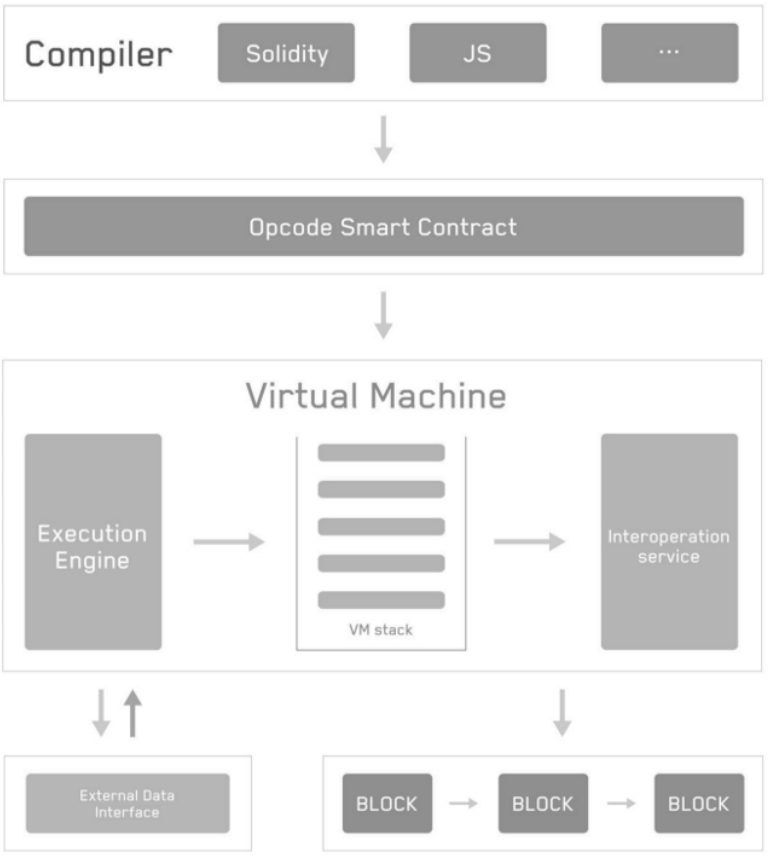
6.2 Ether

Το Ether (ETH) είναι το κρυπτονόμισμα που δημιουργείται από το πρωτόκολλο Ethereum ως ανταμοιβή στους miners [95] σε ένα σύστημα PoW για την προσθήκη μπλοκ στο blockchain. Είναι το μόνο νόμισμα που είναι αποδεκτό για την πληρωμή των τελών συναλλαγών, τα οποία επίσης πηγαίνουν στους miners. Η ανταμοιβή μπλοκ μαζί με τα τέλη συναλλαγής παρέχουν το κίνητρο στους miners να διατηρήσουν το blockchain να αναπτύσσεται (δηλαδή να συνεχίσουν να επεξεργάζονται νέες συναλλαγές). Επομένως, το ETH είναι θεμελιώδες για τη λειτουργία του δικτύου. Κάθε λογαριασμός Ethereum έχει ETH υπόλοιπο και μπορεί να στείλει ETH σε οποιονδήποτε άλλο λογαριασμό. Η μικρότερη υπομονάδα του ETH είναι γνωστή ως Wei [96] και είναι ίση με 10^{-18} ETH. Το Ether συχνά αναφέρεται λανθασμένα ως "Ethereum".

Η μετάβαση στο Ethereum 2.0 μπορεί να μειώσει το ποσοστό έκδοσης του Ether. Δεν υπάρχει επί του παρόντος εφαρμοσμένο σκληρό ανώτατο όριο για τη συνολική παροχή Ether.

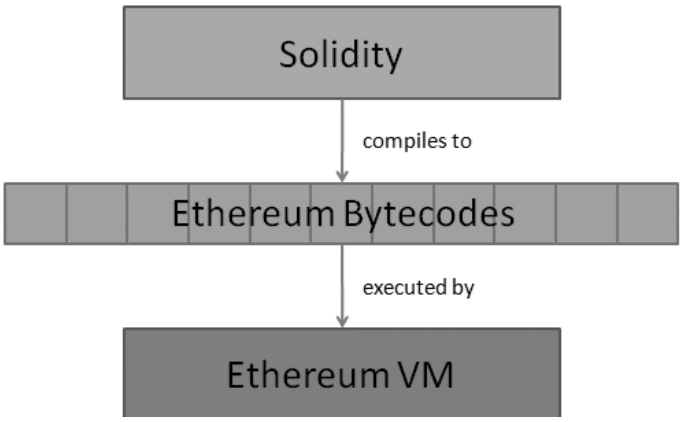
6.3 Ethereum Virtual Machine

Ethereum Virtual Machine [97] (EVM) είναι μια υπολογιστική μηχανή που λειτουργεί σαν ένας αποκεντρωμένο υπολογιστή που έχει εκατομμύρια εκτελέσιμα έργα. Λειτουργεί ως η εικονική μηχανή που είναι το θεμέλιο της συνολικής λειτουργικής δομής του Ethereum. Θεωρείται ότι είναι το μέρος του Ethereum που τρέχει την εκτέλεση και την ανάπτυξη έξυπνων συμβολαίων. Ο ρόλος του EVM είναι να αναπτύξει μια σειρά από επιπλέον λειτουργίες στο Blockchain για να διασφαλίσει ότι οι χρήστες αντιμετωπίζουν περιορισμένα προβλήματα στο κατανεμημένο καθολικό. Κάθε κόμβος Ethereum τρέχει στο EVM για να διατηρήσει τη συναίνεση σε όλο το blockchain. Το Ethereum περιλαμβάνει κάτι που ονομάζεται έξυπνα συμβόλαια, ένα κομμάτι κώδικα που εκτελείται στο Ethereum. Το EVM είναι εντελώς απομονωμένο που σημαίνει ότι ο κώδικας μέσα στο EVM δεν έχει πρόσβαση σε δίκτυο, σύστημα αρχείων ή άλλες διεργασίες.



Εικόνα 6.3 Ethereum Virtual Machine[98]

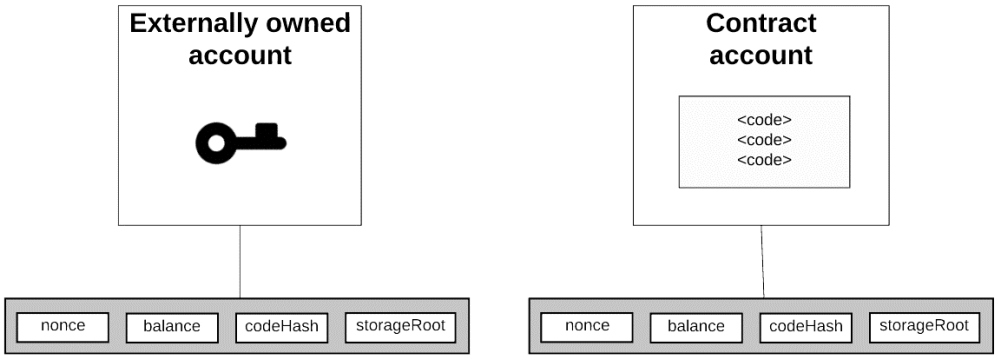
Το Ethereum έχει δύο τύπους λογαριασμών: Λογαριασμούς Εξωτερικής ιδιοκτησίας [99] (EOA, externally-owned accounts) και Λογαριασμούς Συμβολαίου, οι οποίοι αντιμετωπίζονται ισότιμα στο πλαίσιο του EVM. Η αφαίρεση λογαριασμών προσπαθεί να το μειώσει σε έναν μόνο λογαριασμό που σημαίνει ότι τόσο οι EOA όσο και οι λογαριασμοί συμβολαίου λειτουργούν παρόμοια. Τα EOA ελέγχονται από ιδιωτικά κλειδιά, ενώ οι λογαριασμοί συμβολαίων αποθηκεύονται στα έξυπνα συμβόλαια, γνωστά και ως έξυπνα πορτοφόλια. Ένα συμβόλαιο που είναι γραμμένο στην κωδικοποίηση smart-contract [100] μετατρέπεται σε κάτι που ονομάζεται bytecode. Το μεγαλύτερο μέρος του πηγαίου κώδικα για τη χρήση έξυπνων συμβολαίων γίνεται με τη χρήση γλώσσας προγραμματισμού από το Solidity [101]. Στη συνέχεια μετατρέπεται σε κωδικούς λειτουργίας για να ερμηνευτεί από το EVM. Στη συνέχεια, το EVM χρησιμοποιεί τους κωδικούς λειτουργίας για να ολοκληρώσει ορισμένες εργασίες. Έτσι, το EVM λειτουργεί σαν ένας μεγάλος αποκεντρωμένος ή master υπολογιστής για την ολοκλήρωση όλων των τύπων εργασιών στο blockchain.



Εικόνα 6.2 Εκτέλεση έξυπνου συμβολαίου[102]

6.4 Accounts

Οι δύο τύποι έχουν λογαριασμό ETH, μπορούν να στείλουν ETH σε οποιονδήποτε λογαριασμό, μπορούν να καλέσουν οποιαδήποτε public function ενός συμβολαίου ή να δημιουργήσουν ένα νέο συμβόλαιο και προσδιορίζονται στο blockchain από τη διεύθυνσή τους.



Εικόνα 6.5 Είδη λογαριασμών[103]

Οι λογαριασμοί χρηστών είναι ο μόνος τύπος που μπορεί να δημιουργήσει συναλλαγές. Για να είναι έγκυρη μια συναλλαγή, πρέπει να υπογραφεί χρησιμοποιώντας το ιδιωτικό κλειδί του λογαριασμού αποστολής και τη δεκαεξαδική συμβολοσειρά 64 χαρακτήρων από την οποία προέρχεται η διεύθυνση του λογαριασμού. Ο αλγόριθμος που χρησιμοποιείται για την παραγωγή της υπογραφής είναι ο ECDSA [104]. Σημαντική παρατήρηση είναι ότι αυτός ο αλγόριθμος επιτρέπει σε κάποιον να αντλήσει τη διεύθυνση του υπογράφοντος από την υπογραφή χωρίς να γνωρίζει το ιδιωτικό κλειδί.

Τα συμβόλαια είναι ο μόνος τύπος λογαριασμού που έχει συσχετισμένο κώδικα (ένα σύνολο συναρτήσεων και δηλώσεις μεταβλητών) και μέγεθος συμβολαίων (τις τιμές των μεταβλητών ανά πάσα στιγμή). Μια συνάρτηση σύμβασης μπορεί να λάβει ορίσματα και μπορεί να έχει τιμές επιστροφής. Μέσα στο σώμα μιας συνάρτησης, εκτός από τις δηλώσεις ροής ελέγχου, ο κώδικας μιας σύμβασης μπορεί να περιλαμβάνει οδηγίες για αποστολή ETH, ανάγνωση και εγγραφή στην μνήμης της, δημιουργία προσωρινής μνήμης που διαγράφεται στο τέλος της συνάρτησης, εκτέλεση αριθμητικής και λειτουργίες κατακερματισμού, καλεί τις δικές του λειτουργίες, καλεί δημόσιες λειτουργίες άλλων συμβάσεων, δημιουργεί νέα συμβόλαια και ζητά πληροφορίες σχετικά με την τρέχουσα συναλλαγή ή το blockchain.

6.5 Διευθύνσεις Ethereum

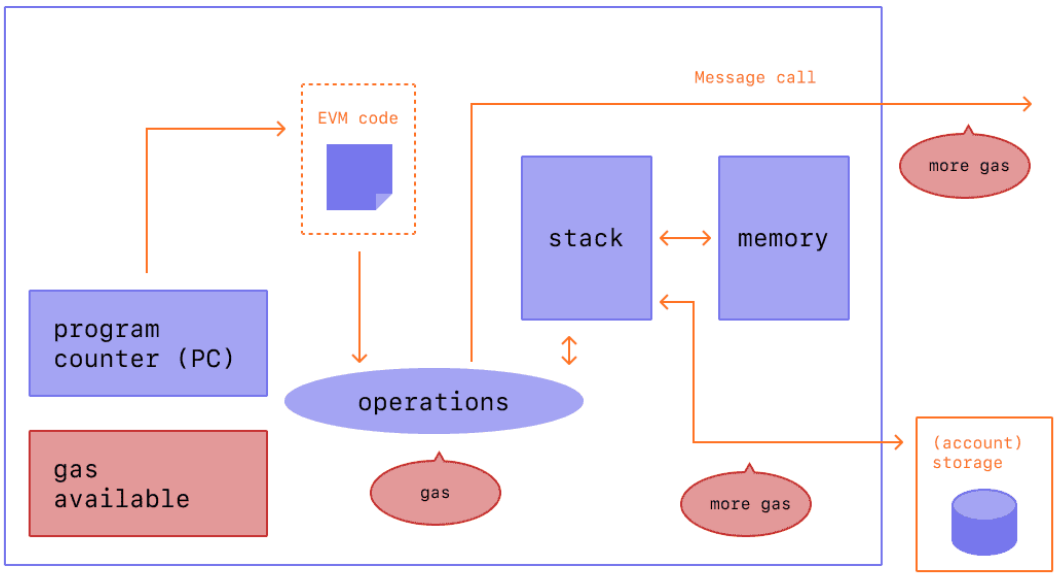
Οι διευθύνσεις Ethereum[105] αποτελούνται από το πρόθεμα "0x", ένα κοινό αναγνωριστικό για το δεκαεξαδικό. Συνδέεται με τα δεξιά 20 byte του κατακερματισμού Keccak-256[106] του δημόσιου κλειδιού ECDSA (η καμπύλη που χρησιμοποιείται είναι η λεγόμενη secp256k1). Στο δεκαεξαδικό, δύο ψηφία αντιπροσωπεύουν ένα byte, που σημαίνει ότι οι διευθύνσεις περιέχουν 40 δεκαεξαδικά ψηφία. Οι διευθύνσεις συμβολαίου είναι στην ίδια μορφή, ωστόσο, καθορίζονται από τον αποστολέα και το nonce της δημιουργίας της συναλλαγής.

6.6 Gas

Gas [107] είναι μια λογιστική μονάδα εντός του EVM που χρησιμοποιείται για τον υπολογισμό μιας προμήθειας συναλλαγής, η οποία είναι το ποσό του ETH που πρέπει να καταβάλει ο αποστολέας μιας συναλλαγής στον κόμβο που θα καταχώρισει τη συναλλαγή στο blockchain.

Κάθε τύπος λειτουργίας που εκτελείται από το EVM είναι ενσωματωμένος (hardcoded) με ένα συγκεκριμένο κόστος Gas, το οποίο προορίζεται να είναι χονδρικά ανάλογο με το ποσό των πόρων (υπολογισμός και αποθήκευση) που πρέπει να δαπανήσει ένας κόμβος για να εκτελέσει αυτήν τη λειτουργία.

Κατά τη δημιουργία μιας συναλλαγής, ο αποστολέας πρέπει να καθορίσει την τιμή του Gas καθώς και να του προσδιορίσει ένα όριο. Το όριο αυτού είναι η μέγιστη ποσότητα Gas που είναι διατεθειμένος να χρησιμοποιήσει ο αποστολέας στη συναλλαγή και η τιμή του είναι το ποσό του ETH που επιθυμεί να πληρώσει ο αποστολέας στον κόμβο ανά μονάδα Gas που θα χρησιμοποιηθεί. Όσο υψηλότερη είναι η τιμή του, τόσο μεγαλύτερο κίνητρο έχει ένας κόμβος να συμπεριλάβει τη συναλλαγή στο μπλοκ του, και επομένως, τόσο πιο γρήγορα θα συμπεριληφθεί η συναλλαγή στο blockchain.



Εικόνα 6.6 χρεώσεις Gas κατά την εκτέλεση[108]

Ο αποστολέας δηλώνει την πλήρη ποσότητα Gas (δηλαδή το όριο του) εκ των προτέρων, κατά την έναρξη της εκτέλεσης της συναλλαγής, και στο τέλος επιστρέφεται η ποσότητα που δεν χρησιμοποιήθηκε. Εάν σε οποιοδήποτε σημείο η συναλλαγή δεν έχει αρκετό Gas για να εκτελεστεί η επόμενη λειτουργία, η συναλλαγή ακυρώνεται αλλά το Gas που χρησιμοποιήθηκε δεν επιστρέφεται. Οι τιμές του Gas συνήθως εκφράζονται σε Gwei, δηλαδή giga wei, μια υπομονάδα του ETH ίση με 10^{-9} ETH.

Αυτός ο μηχανισμός χρέωσης έχει σχεδιαστεί για να μετριάζει τα ανεπιθύμητα μηνύματα συναλλαγών, να αποτρέπει ατέρμονους βρόγχους κατά την εκτέλεση του συμβολαίου και να παρέχει κατανομή πόρων δικτύου βάσει της αγοράς.

6.7 ERC-20 Tokens

Το ERC-20 (Ethereum Request for Comments 20) Token Standard επιτρέπει ανταλλάξιμα νομισμάτων (token) στο Ethereum blockchain. Το πρότυπο, που προτάθηκε από τον Fabian Vogelsteller [109] τον Νοέμβριο του 2015, εφαρμόζει ένα API για νομίσματα σε έξυπνα συμβόλαια. Το πρότυπο παρέχει λειτουργίες συμπεριλαμβανομένης της μεταφοράς νομισμάτων από έναν λογαριασμό σε έναν άλλο, λήψη του τρέχοντος υπολοίπου νομίσματος ενός λογαριασμού και λήψη της συνολικής προσφοράς νομισμάτων διαθέσιμο στο δίκτυο. Τα έξυπνα συμβόλαια που εφαρμόζουν σωστά τις διαδικασίες ERC-20 ονομάζονται ERC-20 Token Contracts, και βοηθούν στην παρακολούθηση των νομισμάτων που δημιουργούνται στο Ethereum. Πολλά κρυπτονομίσματα έχουν κυκλοφορήσει σαν ERC-20 tokens. Τα τέλη για την αποστολή ERC-20 tokens πρέπει να καταβάλλονται με Ether.

6.8 ERC-721 NON-FUNGIBLE TOKEN

Το ERC-721 [110] (Ethereum Request for Comments 721) εισάγει ένα πρότυπο για το NFT, με άλλα λόγια, αυτός ο τύπος Token είναι μοναδικός και μπορεί να έχει διαφορετική αξία από ένα άλλο token που προέρχεται από το ίδιο Έξυπνο Συμβόλαιο, ίσως λόγω της ηλικίας, της σπανιότητάς του ή ακόμα και κάτι άλλο σαν την οπτική του.

Όλα τα NFT έχουν μια μεταβλητή uint256 που ονομάζεται tokenId, επομένως για οποιοδήποτε συμβόλαιο ERC-721, η διεύθυνση συμβολαίου ζεύγους, uint256 tokenId πρέπει να είναι μοναδική.

Παρέχει λειτουργίες όπως η μεταφορά token από έναν λογαριασμό σε άλλον, η λήψη του τρέχοντος υπολοίπου ενός λογαριασμού, η απόκτηση του κατόχου ενός συγκεκριμένου token και επίσης η συνολική προσφορά του διακριτικού που είναι διαθέσιμο στο δίκτυο. Εκτός από αυτές, έχει επίσης ορισμένες άλλες λειτουργίες, όπως να εγκρίνει ότι το πλήθος tokens από έναν λογαριασμό μπορεί να μετακινηθεί από λογαριασμό τρίτου μέρους.

Εάν ένα Έξυπνο Συμβόλαιο εφαρμόζει τις ακόλουθες μεθόδους και συμβάντα, μπορεί να ονομαστεί Non-Fungible Token Contract ERC-721 και, μόλις αναπτυχθεί, θα είναι υπεύθυνο να παρακολουθεί τα tokens που δημιουργούνται στο Ethereum.

6.9 Non-fungible Tokens

Το Ethereum επιτρέπει επίσης τη δημιουργία μοναδικών και αδιαίρετων νομισμάτων, που ονομάζονται non-fungible tokens (NFT). Δεδομένου ότι τα νομίσματα αυτού του τύπου είναι μοναδικά, έχουν χρησιμοποιηθεί για να αναπαραστήσουν πράγματα όπως συλλεκτικά αντικείμενα, ψηφιακή τέχνη, αθλητικά αναμνηστικά, εικονικά ακίνητα και αντικείμενα μέσα σε παιχνίδια.

Το πρώτο project NFT, το Etheria [111], ένας τρισδιάστατος χάρτης εμπορεύσιμων και προσαρμόσιμων εξαγωνικών πλακιδίων, παρατάχθηκε στο δίκτυο τον Οκτώβριο του 2015 και παρουσιάστηκε ζωντανά στο DEVCON1 τον Νοέμβριο του ίδιου έτους. Το 2021, ο Christie πούλησε μια ψηφιακή εικόνα με ένα NFT από την Beeple [112] για 69,3 εκατομμύρια δολάρια, καθιστώντας τον τρίτο πολυτιμότερο εν ζωή καλλιτέχνη από άποψη τιμών δημοπρασίας εκείνη την εποχή. Γη, κτίρια και είδωλα σε εικονικούς κόσμους που βασίζονται σε blockchain μπορούν επίσης να αγοραστούν και να πωληθούν ως NFT, μερικές φορές για εκατοντάδες χιλιάδες δολάρια.

6.10 Web3

Το πρώτο web [113] ήταν απλώς ο παγκόσμιος ιστός, που κυκλοφόρησε από τον Tim Berners-Lee [114] το 1989, ο οποίος επέτρεπε σε άτομα με τεχνική τεχνογνωσία να τοποθετούν πληροφορίες στο διαδίκτυο με αποκεντρωμένο τρόπο. Το Web 2.0[115], που ονομάστηκε για πρώτη φορά σε ένα άρθρο περιοδικού το 1999, είδε την ανάπτυξη εύχρηστων εργαλείων που επιτρέπουν σε οποιονδήποτε να δημιουργεί περιεχόμενο στο διαδίκτυο, όχι μόνο σε ειδικούς, αλλά με κόστος συγκέντρωσης στους τεχνολογικούς γίγαντες που έχουμε σήμερα, όπως το Facebook και Google. Η ιδέα πίσω από το Web3 είναι να πάρουμε τον παγκόσμιο ιστό όπως τον ξέρουμε και να προσθέσουμε την τεχνολογία blockchain παντού.

Στον πυρήνα του Web3 βρίσκονται κατανεμημένες εφαρμογές [116] (ή dapps) που έχουν δημιουργηθεί χρησιμοποιώντας το Ethereum blockchain, το οποίο ανταμείβει τους χρήστες που βοηθούν στη διατήρηση του δικτύου του στο διαδίκτυο.

Πολλοί προγραμματιστές Web3 έχουν επιλέξει να δημιουργήσουν dapps λόγω της εγγενούς αποκέντρωσης του Ethereum:

- Οποιοσδήποτε είναι στο δίκτυο έχει άδεια χρήσης της υπηρεσίας ή με άλλα λόγια, δεν απαιτείται άδεια.
- Κανείς δεν μπορεί να σας αποκλείσει ή να σας αρνηθεί την πρόσβαση στην υπηρεσία.

- Οι πληρωμές ενσωματώνονται μέσω του εγγενούς διακριτικού, ether (ETH).
- Το Ethereum είναι turing-complete[117], που σημαίνει ότι μπορείτε να προγραμματίσετε σχεδόν οτιδήποτε.
- Οι servers Web3 δεν μπορούν να “πέσουν” διότι χρησιμοποιούν το δίκτυο του Ethereum

Περιορισμοί Web3:

- Επεκτασιμότητα: Οι συναλλαγές είναι πιο αργές στο web3 επειδή είναι αποκεντρωμένες. Οι αλλαγές στην κατάσταση, όπως μια πληρωμή, πρέπει να υποβληθούν σε επεξεργασία από έναν miner και να διαδοθούν σε όλο το δίκτυο.
- UX: Η αλληλεπίδραση με εφαρμογές web3 μπορεί να απαιτεί επιπλέον βήματα, λογισμικό και εκπαίδευση. Αυτό μπορεί να είναι ένα εμπόδιο στην υιοθέτηση.
- Προσβασιμότητα: Η έλλειψη ενσωμάτωσης στα σύγχρονα προγράμματα περιήγησης ιστού καθιστά το web3 λιγότερο προσβάσιμο στους περισσότερους χρήστες.
- Κόστος: Τα περισσότερα επιτυχημένα dapp τοποθετούν πολύ μικρά τμήματα του κώδικά τους στο blockchain καθώς είναι ακριβό.

6.11 MetaMask

Το MetaMask[118] είναι μια επέκταση προγράμματος περιήγησης που έχει σχεδιαστεί για να διευκολύνει την πρόσβαση στο οικοσύστημα των Dapp του Ethereum. Χρησιμεύει επίσης ως πορτοφόλι για τη διατήρηση ERC-20 tokens που επιτρέπει στους χρήστες να έχουν πρόσβαση σε υπηρεσίες που έχουν δημιουργηθεί στο δίκτυο, μέσω του πορτοφολιού.

Εικόνα 6.7 Λογότυπο του MetaMask[119]

6.12 Decentralized finance

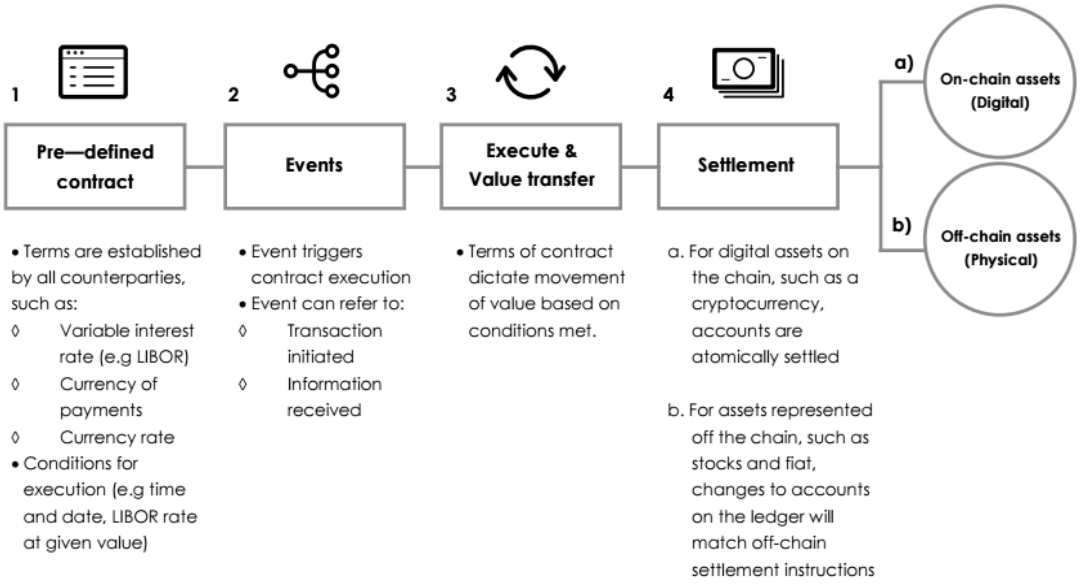
Η αποκεντρωμένη χρηματοδότηση (DeFi) είναι ένα use case του Ethereum. Προσφέρει παραδοσιακά χρηματοοικονομικά μέσα σε μια αποκεντρωμένη αρχιτεκτονική, μακριά από τον έλεγχο των εταιρειών και των κυβερνήσεων, όπως κεφάλαια χρηματαγοράς που επιτρέπουν στους χρήστες να κερδίζουν τόκους. Η πρόσβαση στις αποκεντρωμένες χρηματοοικονομικές εφαρμογές γίνεται συνήθως μέσω μιας εφαρμογής ή Web3-enabled επέκτασης προγράμματος περιήγησης, όπως το MetaMask, το οποίο επιτρέπει στους χρήστες να αλληλεπιδρούν απευθείας με το blockchain Ethereum μέσω ενός ιστότοπου. Πολλά από αυτά τα DApps μπορούν να συνδεθούν και να συνεργαστούν για να δημιουργήσουν πολύπλοκες χρηματοοικονομικές υπηρεσίες.

7 Smart Contracts

Ένα έξυπνο συμβόλαιο, όπως κάθε συμβόλαιο, καθορίζει τους όρους μιας συμφωνίας. Αλλά σε αντίθεση με ένα παραδοσιακό συμβόλαιο, οι όροι ενός έξυπνου συμβολαίου φέρονται ως κώδικας που εκτελείται σε μια αλυσίδα μπλοκ όπως το Ethereum. Τα έξυπνα συμβόλαια επιτρέπουν στους προγραμματιστές να δημιουργούν εφαρμογές που επωφελούνται από την ασφάλεια, την αξιοπιστία και την προσβασιμότητα του blockchain, ενώ προσφέρουν εξελιγμένη λειτουργικότητα P2P.

Χρησιμοποιούνται σε πολλούς τομείς, από νέα χρηματοοικονομικά εργαλεία μέχρι logistics και ηλεκτρονικά παιχνίδια, και αποθηκεύονται σε blockchain όπως κάθε άλλη συναλλαγή κρυπτογράφησης. Μόλις προστεθεί μια εφαρμογή έξυπνου συμβολαίου στο blockchain, γενικά δεν μπορεί να αντιστραφεί ή να αλλάξει.

Οι εφαρμογές που υποστηρίζονται από έξυπνα συμβόλαια αναφέρονται συχνά ως «αποκεντρωμένες εφαρμογές» ή «dapps» και περιλαμβάνουν τεχνολογία αποκεντρωμένης χρηματοδότησης (ή DeFi) που στοχεύει να μεταμορφώσει τον τραπεζικό κλάδο. Οι εφαρμογές DeFi επιτρέπουν στους κατόχους κρυπτονομισμάτων να συμμετέχουν σε περίπλοκες χρηματοοικονομικές συναλλαγές όπως αποταμίευση, δάνεια και ασφάλιση, από οπουδήποτε στον κόσμο, χωρίς μια τράπεζα ή άλλο χρηματοπιστωτικό ίδρυμα να κάνει περικοπές.



Εικόνα 7.1 Τρόποι εκτέλεσης συμβολαίων[128]

Επί του παρόντος, το Ethereum είναι η πιο δημοφιλής πλατφόρμα έξυπνων συμβολαίων, αλλά πολλά άλλα blockchain κρυπτονομισμάτων (συμπεριλαμβανομένων των EOS[120], Neo[121], Tezos[122], Tron[123], Polkadot [124] και Algorand [125]) μπορούν να τα εκτελέσουν. Ένα έξυπνο συμβόλαιο μπορεί να δημιουργηθεί και να αναπτυχθεί σε ένα blockchain από οποιονδήποτε. Αποτελούν λογισμικό ανοιχτό κώδικα, πράγμα που σημαίνει ότι κάθε ενδιαφερόμενος μπορεί να δει ακριβώς ποια λογική ακολουθεί ένα έξυπνο συμβόλαιο όταν λαμβάνει ψηφιακά στοιχεία.

Τα Κύρια χαρακτηριστικά των έξυπνων συμβολαίων είναι:

- Τα έξυπνα συμβόλαια είναι γραμμένα σε διάφορες γλώσσες προγραμματισμού (συμπεριλαμβανομένων των Solidity, Web Assembly[126] και Michelson[127]).
- Κάθε κόμβος στο δίκτυο αποθηκεύει ένα αντίγραφο όλων των υπαρχόντων έξυπνων συμβολαίων και της τρέχουσας κατάστασής τους μαζί με το blockchain και τα δεδομένα συναλλαγών.

- Όταν ένα έξυπνο συμβόλαιο λαμβάνει κεφάλαιο από έναν χρήστη, ο κώδικάς του εκτελείται από όλους τους κόμβους του δικτύου προκειμένου να επιτευχθεί συναίνεση σχετικά με το αποτέλεσμα και τη ροή αξίας που προκύπτει. Αυτό είναι που επιτρέπει στα έξυπνα συμβόλαια να εκτελούνται με ασφάλεια χωρίς καμία κεντρική αρχή, ακόμη και όταν οι χρήστες πραγματοποιούν περίπλοκες οικονομικές συναλλαγές με άγνωστες οντότητες.
- Για να την εκτέλεση ένας έξυπνου συμβόλαιού στο δίκτυο Ethereum, ο χρήστης θα πρέπει να πληρώσει Gas.
- Μόλις αναπτυχθούν σε μια αλυσίδα μπλοκ, τα έξυπνα συμβόλαια γενικά δεν μπορούν να τροποποιηθούν, ακόμη και από τον δημιουργό τους. Αυτό διασφαλίζει ότι δεν μπορούν να λογοκριθούν ή να τερματιστούν.

7.1.1 Ταχύτητα, αποτελεσματικότητα και ακρίβεια:

Μόλις εκπληρωθεί ένας όρος, η σύμβαση εκτελείται αμέσως. Επειδή τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα, δεν υπάρχει καμία γραφειοκρατία για επεξεργασία και δεν δαπανάται χρόνος για τη συμφωνία σφαλμάτων που συχνά προκύπτουν από τη μη αυτόματη συμπλήρωση εγγράφων.

7.1.2 Εμπιστοσύνη και διαφάνεια:

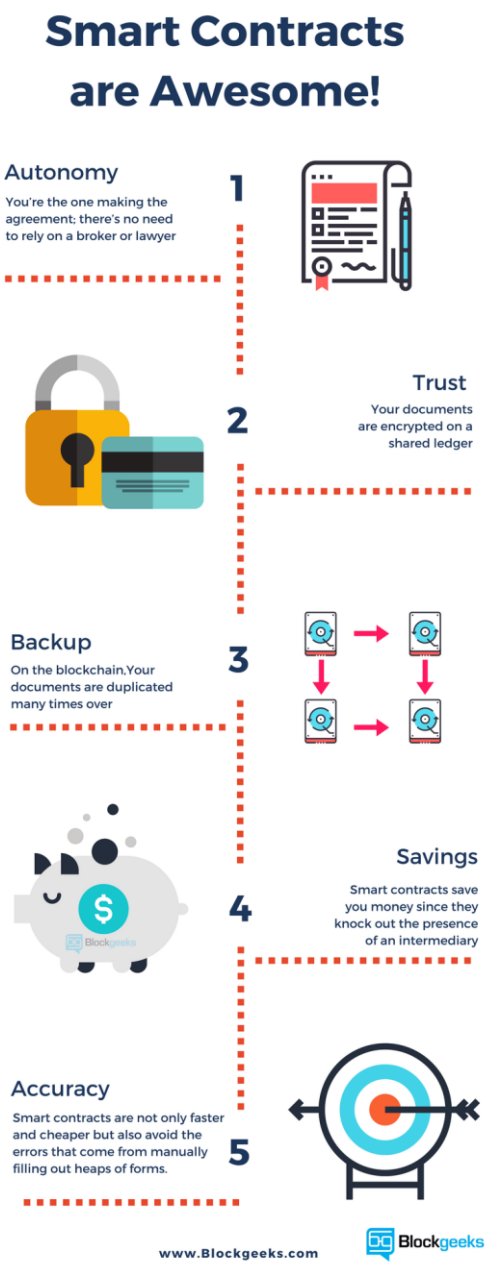
Επειδή δεν εμπλέκεται τρίτο μέρος και επειδή τα κρυπτογραφημένα αρχεία συναλλαγών μοιράζονται μεταξύ των συμμετεχόντων, δεν υπάρχει λόγος να αμφισβητηθεί εάν οι πληροφορίες έχουν τροποποιηθεί για προσωπικό όφελος.

7.1.3 Ασφάλεια:

Τα αρχεία συναλλαγών Blockchain είναι κρυπτογραφημένα, γεγονός που τα καθιστά πολύ δύσκολο σε κάποιον να αποκτήσει παράνομα πρόσβαση σε αυτά. Επιπλέον, επειδή κάθε εγγραφή συνδέεται με τις προηγούμενες και τις επόμενες εγγραφές σε ένα κατανεμημένο καθολικό, οι κακόβουλοι χρήστες θα πρέπει να αλλάξουν ολόκληρη την αλυσίδα για να αλλάξουν μία μόνο εγγραφή.

7.1.4 Εξοικονόμηση πόρων:

Τα έξυπνα συμβόλαια εξαλείφουν την ανάγκη για μεσάζοντες να χειρίζονται τις συναλλαγές και, κατ' επέκταση, τις σχετικές χρονικές καθυστερήσεις και χρεώσεις.



Εικόνα 7.2 Χαρακτηριστικά έξυπνων συμβολαίων[129]

8 Περιπτώσεις χρήσης του blockchain

Τα έξυπνα συμβόλαια παράχουν την υποδομή για μη χρηματοοικονομικές εφαρμογές που βασίζονται σε blockchain σε διάφορους τομείς. Τα βασικά χαρακτηριστικά του blockchain, όπως η αποκεντρωμένη λειτουργία, η αμετάβλητη διαδρομή ελέγχου, η προέλευση των δεδομένων, η ασφάλεια και το απόρρητο, το έχουν καταστήσει κατάλληλη εναλλακτική λύση για παραδοσιακές κεντρικές εφαρμογές και η εξέλιξη του έξυπνου συμβολαίου το έχει κάνει πραγματικότητα. Σε αυτήν την ενότητα, εξετάζουμε τους κύριους τομείς εφαρμογών που χρησιμοποιούν blockchain και έξυπνα συμβολαια.

8.1 Εφαρμογές στην υγεία

Τα συστήματα υγειονομικής περίθαλψης σε κάθε χώρα και περιοχή παλεύουν με το πρόβλημα των σιλό δεδομένων, πράγμα που σημαίνει ότι οι ασθενείς και οι πάροχοι υγειονομικής περίθαλψής τους δεν έχουν πλήρη εικόνα του ιατρικού ιστορικού. Το 2016, το Πανεπιστήμιο Johns Hopkins δημοσίευσε έρευνα[130] που δείχνει ότι η τρίτη κύρια αιτία θανάτου στις ΗΠΑ ήταν ιατρικά λάθη που προέρχονται από κακή συντονισμένη φροντίδα, όπως προγραμματισμένες ενέργειες που δεν ολοκληρώθηκαν όπως επιδιώκονταν ή σφάλματα παράλειψης στα αρχεία ασθενών.

Μια πιθανή λύση [131] σε αυτό το πρόβλημα είναι η δημιουργία ενός συστήματος βασισμένου στο blockchain για ιατρικά αρχεία που μπορεί να συνδεθεί με το υπάρχον λογισμικό ηλεκτρονικών ιατρικών αρχείων και να λειτουργήσει ως γενική, ενιαία προβολή του αρχείου ενός ασθενούς. Είναι σημαντικό να τονίσουμε ότι τα πραγματικά δεδομένα ασθενών δεν πηγαίνουν στο blockchain, αλλά ότι κάθε νέο αρχείο που προσαρτάται στο blockchain, είτε σημείωμα ιατρού, συνταγή ή αποτέλεσμα εργαστηρίου, μεταφράζεται σε μια μοναδική συνάρτηση κατακερματισμού, μια μικρή σειρά από γράμματα και αριθμούς. Κάθε συνάρτηση κατακερματισμού είναι μοναδική και μπορεί να αποκωδικοποιηθεί μόνο εάν το άτομο που κατέχει τα δεδομένα, σε αυτήν την περίπτωση, ο ασθενής δώσει τη συγκατάθεσή του.

Σε αυτό το σενάριο, κάθε φορά που υπάρχει μια τροποποίηση σε ένα αρχείο ασθενούς και κάθε φορά που ο ασθενής συναινεί να κοινοποιήσει μέρος του ιατρικού του αρχείου, αυτό καταγράφεται στο blockchain ως συναλλαγή. Η Medicalchain[132] είναι ένα κορυφαίο παράδειγμα εταιρείας που συνεργάζεται με παρόχους υγειονομικής περίθαλψης για την εφαρμογή EMR με δυνατότητα blockchain.

Τα βασικά οφέλη των EMR με δυνατότητα blockchain είναι:

Μια ολοκληρωμένη ενιαία πηγή αλήθειας των ιατρικών αρχείων ενός ασθενούς, που δημιουργεί μια καλύτερη εμπειρία για τους ασθενείς και τους παρόχους υγειονομικής περίθαλψης.

Επιτρέπουν στους ασθενείς να βλέπουν κάθε φορά που ενημερώνονται τα ιατρικά τους αρχεία και να δίνουν τη ρητή συγκατάθεσή τους κάθε φορά που κοινοποιούνται σε παρόχους υγειονομικής περίθαλψης ή άλλους. Οι ασθενείς μπορούν επίσης να επιλέξουν να μοιραστούν τα ιατρικά τους αρχεία (ή μέρος των ιατρικών τους αρχείων) με ερευνητές και να θέσουν χρονικά όρια για το χρονικό διάστημα που οποιοσδήποτε τρίτος μπορεί να έχει πρόσβαση στις ιατρικές τους πληροφορίες.

Οι ασφαλιστές μπορούν να λάβουν άμεση, επικυρωμένη επιβεβαίωση των υπηρεσιών υγειονομικής περίθαλψης απευθείας από τους ασθενείς, χωρίς το χρόνο και το κόστος ενός διαμεσολαβητή

Πέρα από τη δημιουργία ιατρικών αρχείων που βασίζονται σε blockchain, η Medicalchain αναπτύσσει επίσης μια πλατφόρμα πάνω στην οποία άλλοι μπορούν να δημιουργήσουν υπηρεσίες ψηφιακής υγείας. Όπως μια εικονική συμβουλευτική υπηρεσία καθώς και μιας υπηρεσίας ανταλλαγής ιατρικών δεδομένων, όπου οι ασθενείς μπορούν να επιλέξουν να πουλήσουν τα ανώνυμα ιατρικά τους δεδομένα, σε

αντάλλαγμα για Medtokens [133], για την υποστήριξη της ανάπτυξης ψηφιακών εφαρμογών υγείας.

Η εμφάνιση πολύ πιο ολοκληρωμένων, ψηφιοποιημένων και κοινοποιήσιμων αρχείων υγείας ασθενών θα έχει βαθύ αντίκτυπο στην αγορά υγειονομικής περίθαλψης τροφοδοτώντας πιο προηγμένες αναλύσεις. Για παράδειγμα, η εξατομικευμένη ιατρική είναι ένας πολλά υποσχόμενος τομέας, αλλά η ανάπτυξή της παρεμποδίζεται σοβαρά από την έλλειψη επαρκών δεδομένων υψηλής ποιότητας. Η πρόσβαση σε πιο αξιόπιστα και διαδεδομένα δεδομένα σε επίπεδο πληθυσμού θα επέτρεπε πολύ πιο ισχυρή κατάτμηση και ανάλυση των στοχευμένων ιατρικών αποτελεσμάτων.

8.2 Διαχείριση Εφοδιαστικής Αλυσίδας

Το επιχείρησιακο μοντέλο blockchain [134] μπορεί να μεταμορφώσει την αλυσίδα εφοδιασμού με αυτές τις τρεις περιπτώσεις χρήσης:

- Ανιχνευσιμότητα
- Διαφάνεια
- Εμπορευσιμότητα

Η ανιχνευσιμότητα βελτιώνει τη λειτουργική αποτελεσματικότητα χαρτογραφώντας και οπτικοποιώντας τις αλυσίδες εφοδιασμού επιχειρήσεων. Ο αυξανόμενος αριθμός καταναλωτών ζητά πληροφορίες προέλευσης για τα προϊόντα που αγοράζουν. Το Blockchain βοηθά τους οργανισμούς να κατανοήσουν την αλυσίδα εφοδιασμού τους και να προσελκύσουν τους καταναλωτές με πραγματικά, επαληθεύσιμα και αμετάβλητα δεδομένα.

Η διαφάνεια δημιουργεί εμπιστοσύνη συλλέγοντας βασικά σημεία δεδομένων, όπως πιστοποιήσεις και αξιώσεις, και στη συνέχεια παρέχει πρόσβαση σε αυτά τα δεδομένα. Μόλις εγγραφεί στο blockchain Ethereum, η αυθεντικότητά του μπορεί να επαληθευτεί από τρίτους πιστοποιητές. Οι πληροφορίες μπορούν να ενημερωθούν και να επικυρωθούν σε πραγματικό χρόνο.

Η εμπορευσιμότητα είναι μια μοναδική blockchain προσφορά που επαναπροσδιορίζει την έννοια της συμβατικής αγοράς. Χρησιμοποιώντας το blockchain, μπορεί κάποιος να αγοράσει ή να πουλήσει τμηματικά ιδιοκτησία, ψηφιακά, ενός αντικείμενου. Παρόμοια με το πώς ένα χρηματιστήριο επιτρέπει τη διαπραγμάτευση των μετοχών μιας εταιρείας, αυτή η κλασματική ιδιοκτησία επιτρέπει σε αυτές τις μονάδες να αντιπροσωπεύουν την αξία του μεριδίου ενός μετόχου σε ένα δεδομένο αντικείμενο. Αυτές οι μονάδες είναι εμπορεύσιμες και οι χρήστες μπορούν να μεταβιβάσουν την ιδιοκτησία χωρίς να αλλάξει χέρια το φυσικό περιουσιακό στοιχείο.

8.3 Ηλεκτρονική ψηφοφορία

Όπως αναφέρεται στα προηγούμενα κεφάλαια το blockchain είναι ένα ψηφιακό καθολικό, έχοντας ως βάση τους κόμβους του δικτύου της για να επαληθεύει, να επεξεργάζεται και να καταγράφει όλες τις συναλλαγές σε όλο το σύστημα. Χάρη στην κρυπτογράφηση και την αποκέντρωση, δεδομένα συναλλαγών του blockchain είναι άφθαρτη και κάθε εγγραφή είναι εύκολα επαληθεύσιμη.

Αυτό το είδος υποδομής συστήματος είναι εξαιρετικά χρήσιμο για ψηφοφορία[137], επειδή μια ψήφος είναι ένα μικρό κομμάτι δεδομένων υψηλής αξίας. Όσοι θέλουν να ψηφίσουν πρέπει να εγκαταλείψουν τα σπίτια τους και να υποβάλουν χάρτινα ψηφοδέλτια σε μια τοπική αρχή. Παρόλο των παλιότερων προσπαθειών που έχουν γίνει, έχει αποδειχθεί δύσκολη η εμπιστοσύνη στα αποτελέσματα λόγω των μεγάλων κενών ασφάλεια των πληροφορικών συστημάτων του δημοσίου.

Η ασφαλής ψηφιακή κάλπη της Horizon [137] αντιπροσωπεύει μια οικονομικά αποδοτική και έξυπνη λύση στα προβλήματα που αντιμετωπίζουμε στις σημερινές διαδικασίες ψηφοφορίας. Οι συμμετέχοντες θα χρησιμοποιήσουν Decision tokens [138] (HST) για να μπορέσουν να ψηφίσουν από κινητό τηλέφωνο ή υπολογιστή, τα οποία στη συνέχεια συνδέονται σε ένα αμετάβλητο blockchain και χρησιμοποιούνται

για την αξιόπιστη επαλήθευση του αποτελέσματος των εκλογών. Δεν μπορεί να υπάρξει χειραγώγηση, σφάλματα εγγραφής ή παραβίαση. Περισσότερο από την ψηφοφορία, ωστόσο, αυτό το σύστημα θα είναι χρήσιμο απλώς για τη λήψη αποφάσεων σε ένα περιβάλλον όπου πόροι και εξουσία διαμοιρασμένα.

8.4 Υπηρεσίες ταυτοποίησης

Η αποκεντρωμένη και ψηφιακή ταυτοποίηση [139] μπορεί να χρησιμοποιηθεί με πολλούς τρόπους. Μερικοί από τους οποίους είναι:

- Αυτοκυρίαρχη ταυτότητα
- Νομισματοποίηση δεδομένων
- Φορητότητα δεδομένων

Η αυτοκυριαρχία ταυτότητας [140] (Self-sovereign identity-SSI) είναι η έννοια ότι οι άνθρωποι και οι επιχειρήσεις μπορούν να αποθηκεύουν τα δικά τους δεδομένα ταυτότητας στις δικές τους συσκευές, επιλέγοντας ποιες πληροφορίες θα κοινοποιούνται στους επικυρωτές χωρίς να βασίζονται σε ένα κεντρικό αποθετήριο δεδομένων ταυτότητας. Αυτές οι ταυτότητες θα μπορούσαν να δημιουργηθούν ανεξάρτητα από έθνη-κράτη, εταιρείες ή παγκόσμιους οργανισμούς.

Η νομισματοποίηση δεδομένων αναφέρεται στη χρήση προσωπικών δεδομένων για μετρήσιμο οικονομικό όφελος. Τα δεδομένα από μόνα τους έχουν αξία, αλλά οι πληροφορίες που προέρχονται από προσωπικά αναγνωρίσιμα δεδομένα αυξάνουν σημαντικά την αξία των υποκείμενων δεδομένων. Υπάρχουν εκατομμύριο byte δεδομένων που δημιουργούνται κάθε μέρα, από 4,39 δισεκατομμύρια χρήστες του Διαδικτύου. Πάνω από το 60% του παγκόσμιου ΑΕΠ αναμένεται να ψηφιοποιηθεί έως το 2022, πράγμα που σημαίνει ότι τα προσωπικά δεδομένα θα συνεχίσουν να αυξάνονται σε αξία. Επί του παρόντος, τα διαδικτυακά δεδομένα που παράγουμε είναι ασαφής, αόρατα και πολύπλοκα. Η απόδοση είναι κρίσιμης σημασίας στις διαδικασίες ιδιοκτησίας και η SSI καθιστά δυνατή την απόδοση των διαδικτυακών σας δεδομένων στο DID [141] (decentralized identifier) σας. Από εκεί, τα άτομα θα μπορούσαν να δημιουργήσουν έσοδα από τα προσωπικά τους δεδομένα, για παράδειγμα, νοικιάζοντάς τα σε αλγόριθμους εκπαίδευσης τεχνητής νοημοσύνης ή επιλέγοντας να πουλήσουν τα δεδομένα τους σε διαφημιστές. Οι χρήστες θα έχουν επίσης την επιλογή να διατηρούν τα δεδομένα τους κρυμμένα και προστατευμένα από εταιρείες ή κυβερνήσεις.

Το άρθρο 20 του Γενικού Κανονισμού Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης [142] (EU GDPR) παρέχει στους χρήστες το δικαίωμα στη φορητότητα των δεδομένων, το οποίο αφορά το δικαίωμα του υποκειμένου των δεδομένων να διαβιβάζονται τα προσωπικά του δεδομένα απευθείας από τον έναν ελεγκτή στον άλλο, όταν αυτό είναι τεχνικά εφικτό. Αυτό το δικαίωμα έχει τη δυνατότητα να βελτιώσει την εμπειρία των χρηστών, περιορίζοντας την ανάγκη να επαληθεύσουν εκ νέου την ταυτότητά τους σε διάφορες υπηρεσίες και πλατφόρμες. Με DIDs και επαληθεύσιμα διαπιστευτήρια, είναι δυνατή η εύκολη μετεγκατάσταση ταυτοτήτων που ήταν αποθηκεμένες σε κάποιο σύστημα. Η φορητότητα δεδομένων μειώνει την τριβή για τον χρήστη, ενώ απλοποιεί τη διαδικασία εγγραφής που αυξάνει την υιοθέτηση των χρηστών. Η φορητότητα δεδομένων DID επιτρέπει επίσης επαναχρησιμοποιήσιμα διαπιστευτήρια, όπου ο χρήστης μπορεί γρήγορα να επαληθεύσει ξανά τον εαυτό του ενώ πληροί τις ρυθμιστικές απαιτήσεις Know Your Customer (KYC). Αυτό είναι ιδιαίτερα χρήσιμο για τη μείωση του χρόνου επιβίβασης πελατών που αποφεύγει τα ποσοστά εγκατάλειψης και μειώνει το κόστος στον χρηματοπιστωτικό τομέα, παρακάμπτοντας τη δυσκίνητη διαδικασία επαλήθευσης ταυτότητας, όπου συνήθως πρέπει να παρέχονται και να ελέγχονται πολλά έγγραφα.

8.5 Internet of Things

Η τεχνολογία πίσω από τους αισθητήρες και τα έξυπνα chips εξελίσσεται με ταχείς ρυθμούς, καθιστώντας τα όλο και πιο φορητά και εφαρμόσιμα για αλληλεπιδράσεις σε

πραγματικό χρόνο με blockchain καθολικά. Ο συνδυασμός blockchain και Internet of Things (IoT) [143][144] έχει ευρείες δυνατότητες για τη δημιουργία μιας αγοράς υπηρεσιών μεταξύ συσκευών και δίνει στις εταιρείες την ευκαιρία να δημιουργήσουν αξία από τα δεδομένα που συλλέγονται. Ο αυξανόμενος αριθμός αναδυόμενων πρωτοκόλλων blockchain, συνεργασιών και παρόχων συσκευών IoT δείχνει ήδη ότι υπάρχει καλή εφαρμογή για το blockchain στον τομέα του IoT.

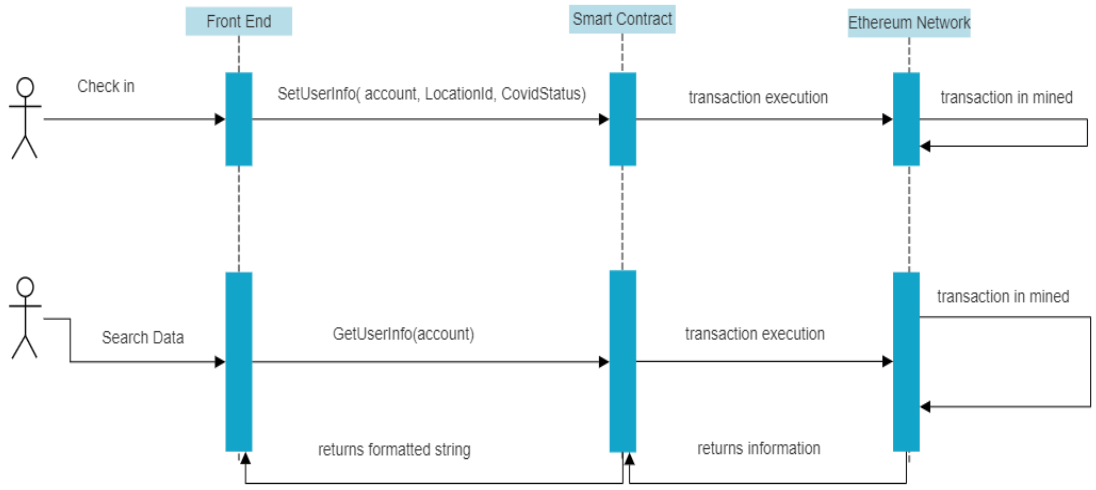
Η Chain of Things [145] (CoT) είναι μια κοινοπραξία τεχνολόγων και κορυφαίων εταιρειών blockchain. Διερευνά τις καλύτερες δυνατές περιπτώσεις χρήσης όπου ένας συνδυασμός blockchain και IoT μπορεί να προσφέρει σημαντικά οφέλη σε βιομηχανικές, περιβαλλοντικές και ανθρωπιστικές εφαρμογές. Μέχρι στιγμής, η CoT έχει δημιουργήσει το Maru, μια ολοκληρωμένη λύση υλικού blockchain και IoT για την επίλυση προβλημάτων ταυτότητας, ασφάλειας και διαλειτουργικότητας. Υπάρχουν τρεις ανεπτυγμένες περιπτώσεις χρήσης που ονομάζονται Chain of Security [146], Chain of Solar [147] και Chain of Shipping [148].

Το IOTA[149] είναι ένα πρωτόκολλο για γρήγορο διακανονισμό συναλλαγών και ακεραιότητα δεδομένων, με το καθολικό Tangle [150] που εξαλείφει την ανάγκη για δαπανηρή εξόρυξη (επικύρωση συναλλαγών). Το IOTA είναι μια πολλά υποσχόμενη υποδομή για συσκευές IoT που πρέπει να επεξεργάζονται μεγάλες ποσότητες μικροδεδομένων. Τα χαρακτηριστικά του καθολικού Tangle, το οποίο είναι το κατανεμημένο καθολικό που υποστηρίζει το IOTA, είναι η επικοινωνία από μηχανή με μηχανή, μικροπληρωμές χωρίς χρέωση και δεδομένα ανθεκτικά απέναντι σε επιθέσεις από κβαντικούς υπολογιστές. Η IOTA έχει δημιουργήσει μια αγορά δεδομένων αισθητήρων και εισέρχεται στην αγορά για πληροφορίες που βασίζονται σε ανάλυση δεδομένων, που υποστηρίζονται από περισσότερες από 20 παγκόσμιες εταιρείες.

Το Modum.io [151] συνδυάζει αισθητήρες IoT με την τεχνολογία blockchain, παρέχοντας ακεραιότητα δεδομένων για συναλλαγές που αφορούν φυσικά προϊόντα. Οι αισθητήρες modum καταγράφουν περιβαλλοντικές συνθήκες, όπως η θερμοκρασία, στις οποίες υπόκεινται τα εμπορεύματα κατά τη μεταφορά τους. Όταν τα αγαθά φτάνουν στο επόμενο σημείο διέλευσης ή στον τελικό πελάτη, τα δεδομένα του αισθητήρα επαληθεύονται σε σχέση με προκαθορισμένες συνθήκες σε ένα έξυπνο συμβόλαιο στο blockchain. Το συμβόλαιο επικυρώνει ότι οι όροι πληρούν όλες τις απαιτήσεις που ορίζονται από τον αποστολέα, τους πελάτες τους ή μια ρυθμιστική αρχή και ενεργοποιεί διάφορες ενέργειες, όπως ειδοποιήσεις προς τον αποστολέα και τον παραλήπτη, πληρωμή ή αποδέσμευση αγαθών.

9 Προτεινομένη εφαρμογή

Στο κεφάλαιο αυτό θα παρουσιαστούν λεπτομέρειες που αφορούν τον σχεδιασμό και την υλοποίηση της αποκεντρωμένης εφαρμογής που αναπτύχθηκε στα πλαίσια της παρούσας διπλωματικής εργασίας. Η παρακάτω εφαρμογή δημιουργήθηκε με σκοπό την αξιολόγηση του επιπέδου δυσκολίας σχεδίασης και ανάπτυξης μιας εφαρμογής έξυπνου συμβολαίου στο blockchain του Ethereum και στην συνέχεια ενσωμάτωσης της στο δίκτυο του Ethereum. Η διεπαφή του χρήστη χωρίζεται και δυο τμήματα. Σε πρώτο μέρος ο χρήστης καταχωρεί την παρούσα τοποθεσία του και αποτελέσματα του τελευταίου covid test που έκανε. Σε δεύτερο μέρος παρέχεται η δυνατότητα αναζήτησης των καταχωρημένων δεδομένων οποιουδήποτε χρήστη μέσω της διεύθυνσης πορτοφολιού του.



Εικόνα 9.1 UML διάγραμμα ακολουθίας έξυπνων συμβολαίων

9.1 Περιγραφή υλοποίησης εφαρμογής

9.1.1 Επεξήγηση backend

Ο παρακάτω κώδικα αναπτύχθηκε στην γλώσσα προγραμματισμού solidity με compiler έκδοσης 0.7.0 . Το smart contract χρησιμοποιείται για την αποθήκευση τον δεδομένων ενός χρήστη στο blockchain μέσο της συνάρτησης SetUserInfo() και την συνέχεια προσφέρει την δυνατότητα μέσο της GetUserInfo() να επιστέψει στην web3 σελίδα τα αποτελέσματα με βάση του ιδιωτικού κλειδιού του wallet (address UserId) του χρήστη σε μια συμβολοσειράς. Λειτουργεί σας το backend του project επιτρέποντας στο frond end να προβάλει τα αποτελέσματα του αναζητά ο χρήστης. Στην συγκεκριμένη περίπτωση να ελέγξει αν κάποιος που επισκέφτηκε μια τοποθεσία νόσησε μια από τις επέμενες ημέρες. Αυτό γίνεται από την ημερομηνία που καταχωρήθηκε η συναλλαγή στο block.

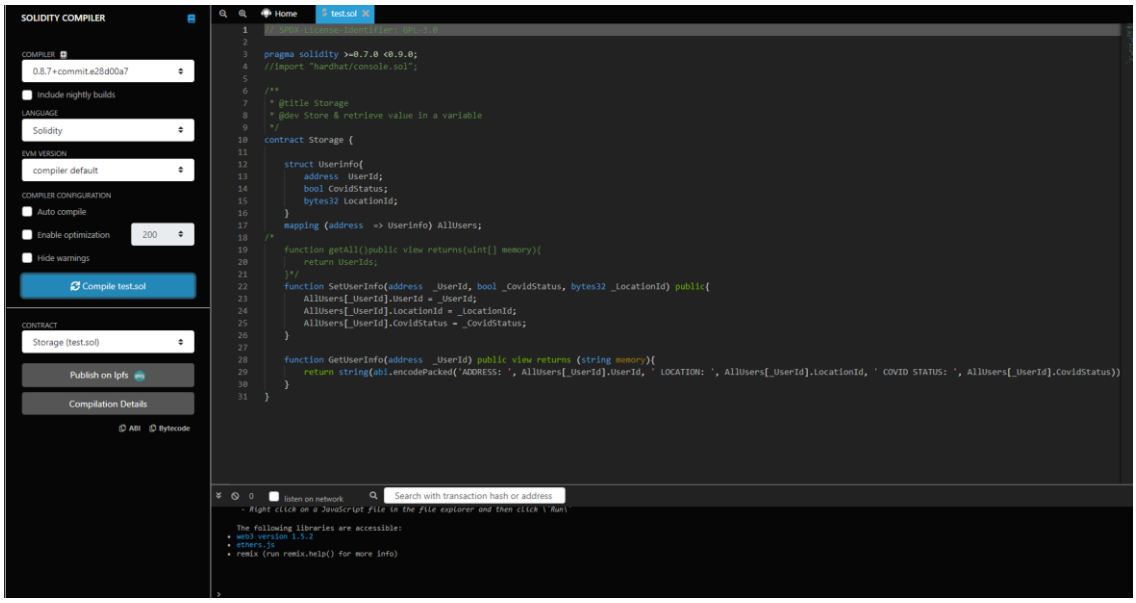
Storage.sol:

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;

/**
 * @title Storage
 * @dev Store & retrieve value in a variable
 */
contract Storage {
```

```
    struct Userinfo{
        address  UserId;
        bool CovidStatus;
        bytes32 LocationId;
    }
    mapping (address  => Userinfo) AllUsers;
/*
    function getAll()public view returns(uint[] memory){
        return UserIds;
    }*/
    function SetUserInfo(address  _UserId, bool _CovidStatus, bytes32
_LocationId) public{
        AllUsers[_UserId].UserId = _UserId;
        AllUsers[_UserId].LocationId = _LocationId;
        AllUsers[_UserId].CovidStatus = _CovidStatus;
    }

    function GetUserInfo(address  _UserId) public view returns (string
memory){
        return string(abi.encodePacked('ADDRESS: ',
AllUsers[_UserId].UserId, ' LOCATION: ', AllUsers[_UserId].LocationId,
' COVID STATUS: ', AllUsers[_UserId].CovidStatus));
    }
}
```

9.2 Compile and deploy

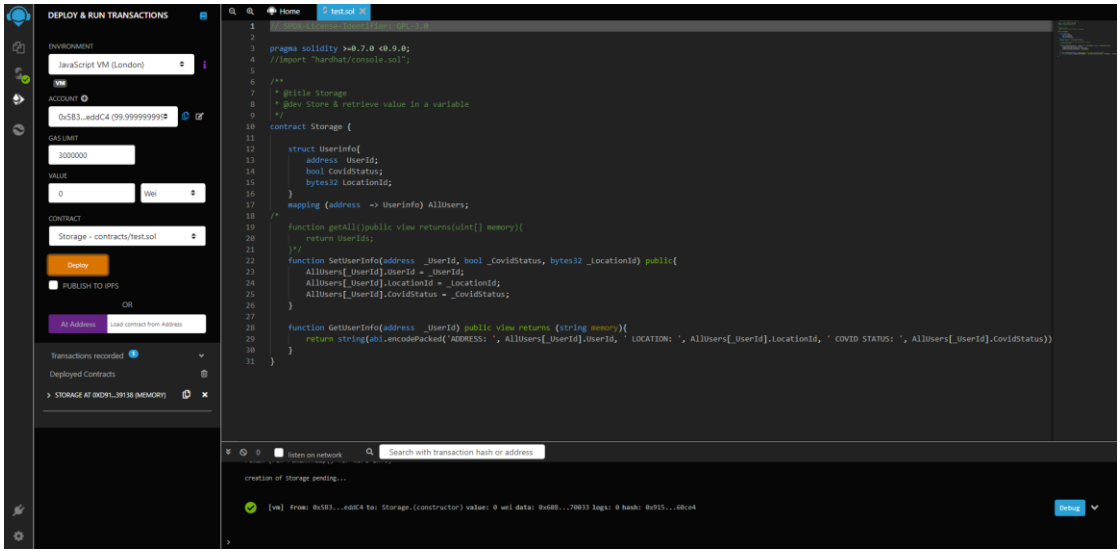
Μετά την εκτέλεση του compiler αν είναι επιτυχής παίρνουμε την κωδικοποίηση ABI η οποία θα πρέπει να την εισάγουμε στο Frondend της εφαρμογής μας. Η κωδικοποίηση ABI είναι σε μορφή JSON και χρειάζεται για να κάνουμε κλήσεις στο συμβόλαιο.



Εικόνα 9.2 compile of smart contract

Στην συνέχεια πρέπει να γίνει το deployment του συμβολαίου. Έτσι ώστε να πάρουμε την διεύθυνση του συμβολαίου και να το δημοσιεύσουμε για να είναι διαθεσίμο στους χρηστές του Ethereum δικτύου.

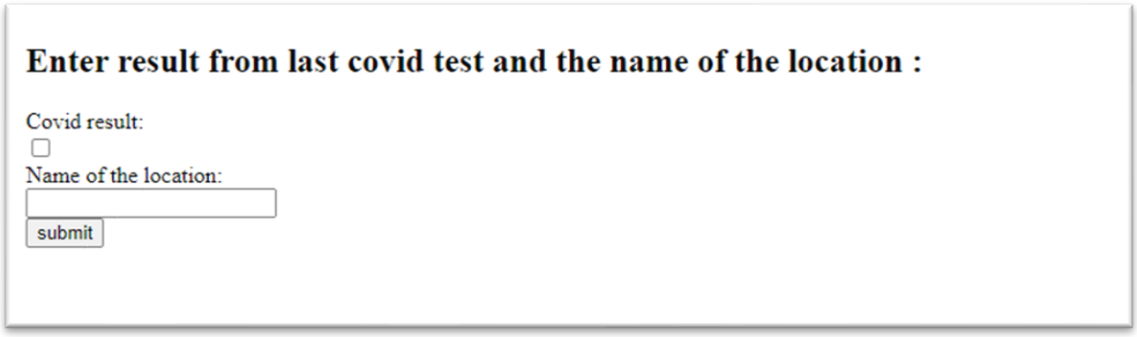
Εφόσον τα παραπάνω βήματα ήταν επιτύχεις μπορούμε να προχωρήσουμε στην γραφή του Frond end για την εισαγωγή και την παρουσίαση των δεδομένων στον χρήστη.



Εικόνα 9.2 deployment of smart contract

9.3 Frond end

9.3.1 DataEntry.html



Εικόνα 9.3 DataEntry.html

9.3.2 Html κώδικας για DataEntry:

```html
<!DOCTYPE html>
<html lang="en">

<head>
  <script type="text/javascript" src="node_modules/web3/dist/web3.min.js"></script>
  <title>check in form</title>

</head>

<body>

  <h2>Enter result from last covid test and the name of the location :</h2>

    <form id="InfoToStore">
    <label for="fname">Covid result:</label><br>
    <input type="checkbox" id="CovidResults" name="CovidResults"><br>
    <label for="lname">Name of the location:</label><br>
    <input type="text" id="location" name="location"><br>
    <input id="submitBtn" type="submit" value="submit"/>
  </form>

  <script>

    // Check for a Web3 provider
    if (typeof web3 !== 'undefined') {
      web3 = new Web3(ethereum);
      console.log(web3.eth.accounts);
    } else {
      web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"));
    }

    var address = "0xd9145CCE52D386f254917e481eB44e9943F39138"; // Contract address
    var contract = new web3.eth.Contract([
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            }
        ],
        "name": "GetUserInfo",
        "outputs": [
            {
                "internalType": "string",
                "name": "",
                "type": "string"
            }
        ],
        "stateMutability": "view",
        "type": "function"
    },
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            },
            {
                "internalType": "bool",
                "name": "_CovidStatus",
                "type": "bool"
            },
            {
                "internalType": "bytes32",
                "name": "_LocationId",
                "type": "bytes32"
            }
        ],
        "name": "SetUserInfo",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function"
    }
], address);
  console.log(contract);

  async function ImportData(LocationId,CovidStatus) {
    const accounts = await window.ethereum.request({method: 'eth_requestAccounts'});
    const account = accounts[0];
    const StorageApply = await contract.methods.SetUserInfo( account, LocationId, CovidStatus);
  }

  const form = document.getElementById("InfoToStore");
  form.addEventListener('submit', (event) => {
    event.preventDefault();
    console.log(form.location.value,form.CovidResults.value);
    ImportData(form.location.value,form.CovidResults.value);
  })

  </script>

</body>
```

Εικόνα 9.4 DataEntry.html code

Οι πρώτες γραμμές του κώδικα είναι Html και JavaScript για την μορφοποίηση της σελίδας και την εισαγωγή των πεδίων που ο χρήστης θα καταχωρήσει τις μεταβλητές.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <script type="text/javascript"
src="node_modules/web3/dist/web3.min.js"></script>
  <title>check in form</title>
</head>
<body>
  <h2>Enter result from last covid test and the name of the location :</h2>
    <form id="InfoToStore">
    <label for="fname">Covid result:</label><br>
    <input type="checkbox" id="CovidResults" name="CovidResults"><br>
    <label for="lname">Name of the location:</label><br>
    <input type="text" id="location" name="location"><br>
    <input id="submitBtn" type="submit" value="submit"/>
  </form>
  <script>
```

Αυτό το κομμάτια κώδικα ελέγχει αν καταχωρήθηκε Provider στον client καθώς πρέπει να δοθεί στον client σας έναν τρόπο να συνδεθεί με το blockchain. Συγκεκριμένα, η βιβλιοθήκη web3js απαιτεί αντικείμενο Provider που περιλαμβάνει το πρωτόκολλο σύνδεσης και τη διεύθυνση/θύρα του κόμβου στον οποίο πρόκειται να συνδεθεί.

```
    // Check for a Web3 provider
    if (typeof web3 !== 'undefined') {
      web3 = new Web3(ethereum);
      console.log(web3.eth.accounts);
    } else {
      web3 = new Web3(new
Web3.providers.HttpProvider("http://localhost:8545"));
    }
```

Η μεταβλητή address περιέχει την διεύθυνση του συμβολαίου και η μεταβλητή contract περιέχει το ABI που πήραμε μετά το compile του smart contract. Πιο συγκεκριμένα η εντολή (new web3.eth.Contract(jsonInterface[, address][, options])), δημιουργεί ένα νέο instance συμβολαίου με όλες τις μεθόδους και τα συμβάντα που ορίζονται στο αντικείμενο διασύνδεσης json.

```
var address = "0xd9145CCE52D386f254917e481eB44e9943F39138"; // Contract
address
    var contract = new web3.eth.Contract([
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            }
        ],
        "name": "GetUserInfo",
        "outputs": [
            {
                "internalType": "string",
                "name": "",
                "type": "string"
            }
        ],
        "stateMutability": "view",
        "type": "function"
    },
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            },
            {
                "internalType": "bool",
                "name": "_CovidStatus",
                "type": "bool"
            },
            {
                "internalType": "bytes32",
                "name": "_LocationId",
                "type": "bytes32"
            }
        ],
        "name": "SetUserInfo",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function"
    }
], address);
  console.log(contract);
```

Η async [152] συνάρτηση, μέσο του metamask, ο χρήστης συνδέεται τον λογαριασμό του και φορτώνεται στην μνήμη η διεύθυνση του Ethereum λογαριασμού. Στην συνέχεια καλεί την συνάρτηση SetUserInfo() του συμβολαίου και καταχωρεί τα

δεδομένα στο block το οποίο μετά περιμένει έγκριση και τελικά την εισαγωγή του στο blockchain.

```
async function ImportData(LocationId,CovidStatus) {
  const accounts = await window.ethereum.request({method:
'eth_requestAccounts'});
  const account = accounts[0];
  const StorageApply = await contract.methods.SetUserInfo( account,
LocationId, CovidStatus);
}
```

Τέλος είναι η λειτουργία του κουμπιού submit που επιστρέφει τα δεόμενα, που καταχώρισε ο χρήστης, στην συνάρτηση ImportData(LocationId,CovidStatus).

```
const form = document.getElementById("InfoToStore");
form.addEventListener('submit', (event) => {
  event.preventDefault();
  console.log(form.location.value,form.CovidResults.value);
  ImportData(form.location.value,form.CovidResults.value);
})
```

9.3.3 DataSearch.html

Οι διάφορες μεταξύ των αρχείων DataSearch.html και DataEntry.html δεν είναι πολλές καθώς ο η ενσωμάτωση του συμβολαίου είναι ιδια όπως επίσης και το σώμα του html αρχείου.

Εικόνα 9.5 DataSearch.html

Οι κυριότερες διάφορες τους είναι ότι η SearchData() καλείται με όρισμα την διεύθυνση του Ethereum λογαριασμού του και στην συνέχεια καλεί την συνάρτηση, του συμβούλου, GetUserInfo που θα επιστρέψει μια συμβολοσειρά με τα στοιχεία του χρήστη που έχει τη συγκεκριμένη διεύθυνση wallet που καταχωρήθηκε προηγούμενος.

```
async function SearchData(address) {
    const accounts = await window.ethereum.request({method:
'eth_requestAccounts'});
    const account = accounts[0];
    const StoredData = await contract.methods.GetUserInfo(account);
    const statusEl = document.getElementById('InfoData');
    statusEl.innerHTML = StoredData;
  }
  const form = document.getElementById("SearchData");
  form.addEventListener('submit', (event) => {
    event.preventDefault();
    console.log(form.address.value);
    SearchData(form.address.value);
})
```

Εικόνα 9.6 Αποτελέσματα DataSearch.html

9.3.4 Html κώδικας για DataEntry:

indexSearch.html

```
<!DOCTYPE html>
<html lang="en">

<head>
  <script type="text/javascript" src="node_modules/web3/dist/web3.min.js"></script>
  <title>Search form</title>

</head>

<body>

  <h2>Enter wallet address for history :</h2>

    <form id="SearchData">

    <label for="lname">wallet address:</label><br>
    <input type="text" id="address" name="address"><br>
    <input id="submitBtn" type="submit" value="submit"/>
  </form>
  Info: <span id="InfoData">Loading...</span>
  <script>

    // Check for a Web3 provider
    if (typeof web3 !== 'undefined') {
      web3 = new Web3(ethereum);
      console.log(web3.eth.accounts);
    } else {
      web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:8545"));
    }

    var address = "0xd9145CCE52D386f254917e481eB44e9943F39138"; // Contract address
    var contract = new web3.eth.Contract([
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            }
        ],
        "name": "GetUserInfo",
        "outputs": [
            {
                "internalType": "string",
                "name": "",
                "type": "string"
            }
        ],
        "stateMutability": "view",
        "type": "function"
    },
    {
        "inputs": [
            {
                "internalType": "address",
                "name": "_UserId",
                "type": "address"
            },
            {
                "internalType": "bool",
                "name": "_CovidStatus",
                "type": "bool"
            },
            {
                "internalType": "bytes32",
                "name": "_LocationId",
                "type": "bytes32"
            }
        ],
        "name": "SetUserInfo",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function"
    }
], address);
  console.log(contract);

  async function SearchData(address) {
    const accounts = await window.ethereum.request({method: 'eth_requestAccounts'});
    const account = accounts[0];
    const StoredData = await contract.methods.GetUserInfo(account);
    const statusEl = document.getElementById('InfoData');
    statusEl.innerHTML = StoredData;
  }

  const form = document.getElementById("SearchData");
  form.addEventListener('submit', (event) => {
    event.preventDefault();
    console.log(form.address.value);
    SearchData(form.address.value);
  })


  </script>

</body>
```

Εικόνα 9.7 DataSearch.html code

9.4 Εργαλεία Υλοποίησης

9.4.1 RemixIDE

Το Remix IDE [153] είναι ένα ισχυρό εργαλείο ανοιχτού κώδικα που βοηθά στην ανάπτυξή συμβολαίων Solidity απευθείας από το πρόγραμμα περιήγησης. Είναι γραμμένο σε JavaScript[154] και υποστηρίζει και τη χρήση στο πρόγραμμα περιήγησης, αλλά μπορεί να εκτελεστεί και σαν εφαρμογή τοπικά. Το Remix IDE διαθέτει Εργαλεία για δοκιμή, debugging και ανάπτυξη έξυπνων συμβολαίων και πολλά άλλα.

9.4.2 Javascript

Η JavaScript είναι μια γλώσσα προγραμματισμού που μπορεί να προσθέσει διαδραστικότητα σε έναν ιστότοπο. Η JavaScript είναι ευέλικτη και φιλική προς τους αρχάριους. Επιτρέπει την δημιουργία παιχνιδιών, 2D και 3D και ολοκληρωμένες εφαρμογές που βασίζονται σε βάσεις δεδομένων.
Η ίδια η JavaScript είναι σχετικά συμπαγής, αλλά πολύ ευέλικτη. Οι προγραμματιστές έχουν γράψει μια ποικιλία εργαλείων πάνω από τη βασική γλώσσα JavaScript, ξεκλειδώνοντας μια τεράστια ποσότητα λειτουργιών με ελάχιστη προσπάθεια. Αυτά περιλαμβάνουν:

- Διεπαφές προγραμματισμού εφαρμογών προγράμματος περιήγησης (Application Programming Interfaces-API) ενσωματωμένες σε προγράμματα περιήγησης ιστού, παρέχοντας λειτουργίες όπως δυναμική δημιουργία HTML και ρύθμιση στυλ CSS. συλλογή και χειρισμός ροής βίντεο από την κάμερα web ενός χρήστη ή δημιουργία τρισδιάστατων γραφικών και δειγμάτων ήχου.
- API τρίτων που επιτρέπουν στους προγραμματιστές να ενσωματώνουν λειτουργικότητα σε ιστότοπους από άλλους, όπως το Twitter ή το Facebook.
- Πλαίσια και βιβλιοθήκες τρίτων που εφαρμόζεται σε HTML για την επιτάχυνση της κατασκευής τοποθεσιών και εφαρμογών.

9.4.3 Node.js

Το Node.js[155] είναι μια πλατφόρμα που αναπτύχθηκε για εύκολη δημιουργία γρήγορων και επεκτάσιμων εφαρμογών δικτύου. Το Node.js χρησιμοποιεί ένα μοντέλο εισόδου/εξόδου που βασίζεται σε συμβάντα, το οποίο το καθιστά ελαφρύ και αποτελεσματικό, ιδανικό για εφαρμογές σε πραγματικό χρόνο με μεγάλος όγκο δεδομένων που εκτελούνται σε κατανεμημένες συστήματα. Το Node.js παρέχει επίσης μια πλούσια βιβλιοθήκη με διάφορες ενότητες JavaScript που απλοποιεί σε μεγάλο βαθμό την ανάπτυξη εφαρμογών Ιστού χρησιμοποιώντας το Node.js.

9.4.4 Node package manager

Το Node Package Manager [156] (NPM) χωρίζεται σε δύο ενότητες: πρώτα και κύρια, είναι ένα διαδικτυακό αποθετήριο για τη δημοσίευση έργων ανοιχτού κώδικα Node.js. Δεύτερον, είναι ένα βοηθητικό πρόγραμμα γραμμής εντολών για την αλληλεπίδραση με το εν λόγω αποθετήριο που βοηθά στην εγκατάσταση πακέτων, τη διαχείριση έκδοσης και τη διαχείριση εξαρτήσεων. Μια πληθώρα βιβλιοθηκών και εφαρμογών Node.js δημοσιεύονται στο npm και πολλές άλλες προστίθενται καθημερινά.

9.4.5 Web3.js

Το web3.js είναι μια συλλογή βιβλιοθηκών που επιτρέπουν την αλληλεπίδραση με έναν τοπικό ή απομακρυσμένο κόμβο ethereum, χρησιμοποιώντας μια σύνδεση HTTP [157] ή IPC[158]. Η βιβλιοθήκη web3 JavaScript αλληλεπιδρά με το blockchain

Ethereum. Μπορεί να ανακτήσει λογαριασμούς χρηστών, να στείλει συναλλαγές, να αλληλεπιδράσει με έξυπνα συμβόλαια.

Συμπεράσματα

Το blockchain αρχικά δημιουργήθηκε σαν ένα προϊόν για να μπορέσει να βασιστεί και να αναπτυχθεί το Bitcoin. Ενώ στα πρώτα της στάδια η τεχνολογία χρησιμοποιήθηκε σαν μια αποκεντρωμένη βάση δεδομένων για την αποθήκευση των συναλλαγών του Bitcoin, που πρόσφερε ανωνυμία και ταυτόχρονα ασφάλεια, σύντομα με την ανάπτυξη άλλων τεχνολογιών, όπως για παράδειγμα το Ethereum, εξελίχθηκε σε μια πλατφόρμα που μπορεί να χρησιμοποιηθεί για την υλοποίηση ενός τεράστιου εύρους εφαρμογών. Μια από τις πιο σημαντικές τεχνολογίες που δημιουργήθηκαν από το blockchain είναι τα έξυπνα συμβόλαια.

Τα έξυπνα συμβόλαια είναι αρκετά ευκολά στην ανάπτυξη και στην υλοποίηση τους. Απόδειξη αυτού είναι οι εφαρμογές που αναφερθήκαν, καθώς και η εφαρμογή που δημιουργήθηκε με αφορμή αυτή την εργασία. Λαμβάνοντας υπόψη τον αυτοματισμό που προσφέρουν, την δυνατότητα εκτέλεσης κατ' εντολή, υπό καθορισμένες συνθήκες, την ευκολία χρήσης τους από εφαρμογές και την μεγάλη άνοδο τιμών και δημοτικότητας των κρυπτονομισμάτων είναι εύκολο να δούμε τον λόγο που ένα αρκετά μεγάλο κομμάτι της αγοράς ξεκίνησε να ασχολείται με αυτά. Προβλήματα που υπήρχαν για χρόνια, όπως μια κοινή βάση δεδομένων για ασθενείς, αλλά και νεότερα προβλήματα, όπως αγοροπωλησίες και ιδιοκτησία ηλεκτρονικής τέχνης βρήκαν λύση βάση του blockchain.

Πολλές φορές, η χρήση τους δεν προσφέρει τη καλύτερη δυνατή λύση. Πρέπει να αναλογιστούμε πριν δημιουργήσουμε μια εφαρμογή αν τα εργαλεία που θα χρησιμοποιήσουμε είναι τα βέλτιστα και όχι απλά τα δημοφιλέστερα την δεδομένη χρονική στιγμή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] *Blockchain Explained*. (2022a, March 5). Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

[2] M. E. Peck, "Blockchains: How They Work and Why They'll Change the World, " 2017

[3] *bitcoin*. (n.d.). Bitcoin. https://bitcoin.org/el/how-it-works

[4] *Hyperledger – Open Source Blockchain Technologies*. (2022, February 22). Hyperledger Foundation. https://www.hyperledger.org

[5] Computer Hope. (2019, June 7). *What is a Decentralized System?* Computerhope.Com. https://www.computerhope.com/jargon/d/decentral.htm

[6] GeeksforGeeks. (2021, September 14). *Comparison - Centralized, Decentralized and Distributed Systems*. https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/#:%7E:text=Centralized%20systems%20are%20systems%20that,server%20and%20receives%20the%20response.

[7] *StackPath*. (n.d.). Stackpath.Com. https://blog.stackpath.com/distributed-system/#:%7E:text=A%20distributed%20system%2C%20also%20known,system%20to%20the%20end%2Duser

[8] Eagar, M. (2018, June 21). *What is the difference between decentralized and distributed systems?* Medium. Retrieved March 9, 2022, from https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462

[9] *Advantages and Disadvantages of Decentralized Blockchains*. (n.d.). World Crypto Index. Retrieved March 9, 2022, from https://www.worldcryptoindex.com/advantages-disadvantages-decentralized-blockchains/

[10] Moskov, A. (2022, March 4). *Are Crypto Domains Worth It?* CoinCentral. Retrieved March 9, 2022, from https://coincentral.com/distributed-system-architecture/#:%7E:text=Peer%2DTo%2DPeer%20Model&text=A%20P2P%20network%20is%20a,a%20client%20or%20a%20server.

[11] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." In *OsDI*, vol. 99, no. 1999, pp. 173-186. 1999.

[12] *From Distributed Consensus Algorithms to the Blockchain Consensus Mechanism*. (n.d.). Alibabacloud.Com. Retrieved March 9, 2022, from https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315

[13] *Proof of Work (PoW)*. (2021, July 22). Investopedia. https://www.investopedia.com/terms/p/proof-work.asp

[14] Daly, L. (2022, January 21). *What Is Proof of Stake (PoS) in Crypto?* The Motley Fool. https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-stake/#:%7E:text=Proof%20of%20stake%20is%20a,add%20them%20to%20the%20blockchain.

[15] Academy, B. (2022, February 21). *What Is a 51% Attack?* Binance Academy. https://academy.binance.com/en/articles/what-is-a-51-percent-attack

[16] *bitcoin*. (n.d.-b). Bitcoin. https://bitcoin.org/bitcoin.pdf

[17] *What Is Cryptography and How Does It Work? | Synopsys*. (n.d.). Synopsys. https://www.synopsys.com/glossary/what-is-cryptography.html

[18] Forouzan, Behrouz A., and Debdeep Mukhopadhyay. *Cryptography and network security*. Vol. 12. New York, NY, USA:: Mc Graw Hill Education (India) Private Limited, 2015.
[19] Wikipedia contributors. (2022p, February 28). *Block cipher*. Wikipedia. https://en.wikipedia.org/wiki/Block_cipher
[20] Wikipedia contributors. (2021f, October 26). *Stream cipher*. Wikipedia. https://en.wikipedia.org/wiki/Stream_cipher
[21] Wikipedia contributors. (2022g, February 10). *Substitution cipher*. Wikipedia. https://en.wikipedia.org/wiki/Substitution_cipher
[22] Chand, A. S. (2021, December 23). *AES Symmetric Encryption with Client-Server Model (Typescript — C#)*. Medium. https://chandabdulsalam.medium.com/aes-symmetric-encryption-with-client-server-model-typescript-c-ee9b773babb9
[23] Wikipedia contributors. (2022l, February 23). *Data Encryption Standard*. Wikipedia. https://en.wikipedia.org/wiki/Data_Encryption_Standard
[24] Wikipedia contributors. (2021a, April 7). *3-Way*. Wikipedia. https://en.wikipedia.org/wiki/3-Way
[25] Wikipedia contributors. (2021g, November 2). *Blowfish (cipher)*. Wikipedia. https://en.wikipedia.org/wiki/Blowfish_(cipher)
[26] Wikipedia contributors. (2022i, February 18). *Advanced Encryption Standard*. Wikipedia. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[27] Wikipedia contributors. (2022k, February 21). *Triple DES*. Wikipedia. https://en.wikipedia.org/wiki/Triple_DES
[28] Wikipedia contributors. (2022o, February 27). *Serpent (cipher)*. Wikipedia. https://en.wikipedia.org/wiki/Serpent_(cipher)
[29] Wikipedia contributors. (2021c, August 17). *Twofish*. Wikipedia. https://en.wikipedia.org/wiki/Twofish
[30] Wikipedia contributors. (2022r, March 3). *RC4*. Wikipedia. https://en.wikipedia.org/wiki/RC4
[31] Wikipedia contributors. (2021b, April 29). *E0 (cipher)*. Wikipedia. https://en.wikipedia.org/wiki/E0_(cipher)
[32] Wikipedia contributors. (2022n, February 25). *Salsa20*. Wikipedia. https://en.wikipedia.org/wiki/Salsa20#ChaCha_variant
[33] Wikipedia contributors. (2022e, February 7). *A5/1*. Wikipedia. https://en.wikipedia.org/wiki/A5/1
[34] Wikipedia contributors. (2021d, October 18). *Affine cipher*. Wikipedia. https://en.wikipedia.org/wiki/Affine_cipher
[35] Wikipedia contributors. (2022f, February 9). *Atbash*. Wikipedia. https://en.wikipedia.org/wiki/Atbash
[36] Wikipedia contributors. (2021e, October 18). *Autokey cipher*. Wikipedia. https://en.wikipedia.org/wiki/Autokey_cipher
[37] Wikipedia contributors. (2022h, February 17). *Beaufort cipher*. Wikipedia. https://en.wikipedia.org/wiki/Beaufort_cipher
[38] Wikipedia contributors. (2022t, March 8). *Caesar cipher*. Wikipedia. https://en.wikipedia.org/wiki/Caesar_cipher
[39] Al-Shabi, M. A. "A survey on symmetric and asymmetric cryptography algorithms in information security." *International Journal of Scientific and Research Publications (IJSRP)* 9, no. 3 (2019): 576-589.
[40] Wikipedia contributors. (2022s, March 6). *RSA (cryptosystem)*. Wikipedia. https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[41] Wikipedia contributors. (2022q, March 3). *Diffie–Hellman key exchange*. Wikipedia. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
[42] Wikipedia contributors. (2022b, January 29). *Digital Signature Algorithm*. Wikipedia. https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
[43] Wikipedia contributors. (2022u, March 9). *Paillier cryptosystem*. Wikipedia. https://en.wikipedia.org/wiki/Paillier_cryptosystem
[44] Wikipedia contributors. (2021h, December 5). *ElGamal encryption*. Wikipedia. https://en.wikipedia.org/wiki/ElGamal_encryption
[45] Wikipedia contributors. (2022m, February 23). *Elliptic-curve cryptography*. Wikipedia. https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[46] *Types of Encryption: Symmetric or Asymmetric? RSA or AES?* (2021, September 9). The Missing Report. https://preyproject.com/blog/en/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes/
[47] *Explaining the Crypto in Cryptocurrency*. (2021, August 24). Investopedia. https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/#:%7E:text=Cryptography%20is%20the%20mathematical%20and,the%20purpose%20of%20%22mining.%22
[48] Merkle, Ralph C. "A certified digital signature." In *Conference on the Theory and Application of Cryptology*, pp. 218-238. Springer, New York, NY, 1989.
[49] *Message digests and digital signatures*. (n.d.). Ibm. https://www.ibm.com/docs/en/ibm-mq/7.5?topic=concepts-message-digests
[50] Nadeem, S. M. (2020, November 24). *OpenPGP digital signature best practices*. Mailfence Blog. https://blog.mailfence.com/openpgp-digital-signature-best-practices/
[51] Goldreich, Oded, and Yair Oren. "Definitions and properties of zero-knowledge proof systems." *Journal of Cryptology* 7, no. 1 (1994): 1-32.
[52] Schor, L. (2019, June 7). *On Zero-Knowledge Proofs in Blockchains - Lukas Schor*. Medium. https://schor.medium.com/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1
[53] *Cryptography Hash functions*. (n.d.). Tutorialspoint. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
[54] *Hash Functions - Practical Cryptography for Developers*. (n.d.). Cryptobook. https://cryptobook.nakov.com/cryptographic-hash-functions
[55] *Merkle Tree*. (2021, July 26). Investopedia. https://www.investopedia.com/terms/m/merkle-tree.asp
[56] Wikipedia contributors. (2022j, February 21). *Merkle tree*. Wikipedia. https://en.wikipedia.org/wiki/Merkle_tree
[57] Wikipedia contributors. (2022a, January 20). *Ralph Merkle*. Wikipedia. https://en.wikipedia.org/wiki/Ralph_Merkle
[58] *Digital Currency*. (2022, January 14). Investopedia. https://www.investopedia.com/terms/d/digital-currency.asp
[59] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in bitcoin." In *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 906-917. 2012.
[60] R. (2021c, June 19). *How bitcoin works?* DEV Community. https://dev.to/codebyru/how-bitcoin-works-bitcoin-101-part-2-4e0i
[61] *Sectigo*. (n.d.). Sectigo. https://sectigo.com/resource-library/time-stamping-server

[62] *TSA(Time-Stamp Server)*. (n.d.). Changingtec. https://www.changingtec.com/EN/tsa.html
[63] Bogna, J. (2022, January 8). *What Is the Environmental Impact of Cryptocurrency?* PCMag UK. https://uk.pcmag.com/old-cryptocurrency/138047/what-is-the-environmental-impact-of-cryptocurrency
[64] *BlockChain Technology*. (n.d.). Berkeley. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
[65] *Blockchain Explained*. (2022, March 5). Investopedia. https://www.investopedia.com/terms/b/blockchain.asp
[66] *Genesis Block Definition*. (2021, July 2). Investopedia. https://www.investopedia.com/terms/g/genesis-block.asp#:%7E:text=A%20Genesis%20Block%20is%20the,occur%20on%20a%20blockchain%20network.
[67] *Security, the Blockchain, and Hashed Headersâ€¦*. (n.d.). Craigwright. https://craigwright.net/blog/bitcoin-blockchain-tech/security-the-blockchain-and-hashed-headers/
[68] Louw, L. (2021, September 23). *Bitcoin, the evolution of ledger systems and its influence on society*. Bitcoin Developer Conference. https://bsvdevcon.net/blog/bitcoin-the-evolution-of-ledger-systems-and-its-influence-on-society
[69] B. (2019, July 14). *Bitcoin White Paper: 7. Reclaiming Disk Space*. HackerNoon. https://hackernoon.com/bitcoin-white-paper-7-reclaiming-disk-space-d03rm2bi7
[70] *Simplified Payment Verification - Bitcoin Wiki*. (n.d.). Wiki.Bitcoinsv. https://wiki.bitcoinsv.io/index.php/Simplified_Payment_Verification#:%7E:text=Simplified%20Payment%20Verification%20(SPV)%20is,the%20properties%20of%20Merkle%20proofs.
[71] Fontana, B. L. (2021, June 1). *Theory of Bitcoin: The Bitcoin Whitepaper 'Combining and Splitting Value & Privacy' key takeaways*. CoinGeek. https://coingeek.com/theory-of-bitcoin-the-bitcoin-whitepaper-combining-and-splitting-value-privacy-key-takeaways/
[72] Wikipedia contributors. (2022d, February 1). *Fan-out*. Wikipedia. https://en.wikipedia.org/wiki/Fan-out
[73] *Bitcoin: A Peer-to-Peer Electronic Cash System*. (n.d.). Ussc. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
[74] *Binomial Dist & Random Walks*. (2021, June 27). Real Statistics Using Excel. https://www.real-statistics.com/binomial-and-related-distributions/binomial-distribution-and-random-walks/
[75] U. (2022, March 9). *How Bitcoin Works Under the Hood*. Stevekorex. http://stevekorex.blogspot.com/2014/12/how-bitcoin-works-under-hood.html
[76] *Gambler's Ruin Problem*. (n.d.). Columbia. Retrieved March 9, 2022, from http://www.columbia.edu/~ks20/FE-Notes/4700-07-Notes-GR.pdf
[77] *The Future is Statistical*. (n.d.). Profitwell. https://www.profitwell.com/recur/all/statistics-are-the-future-of-saas
[78] *Public, Private, Permissioned Blockchains Compared*. (2021, June 29). Investopedia. https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/
[79] Yang, Rebecca, Ron Wakefield, Sainan Lyu, Sajani Jayasuriya, Fengling Han, Xun Yi, Xuechao Yang, Gayashan Amarasinghe, and Shiping Chen. "Public and

private blockchain in construction business process and information integration." *Automation in construction* 118 (2020): 103276.

[80] Aggarwal, Shubhani, and Neeraj Kumar. "Hyperledger." In *Advances in Computers*, vol. 121, pp. 323-343. Elsevier, 2021.

[81] *Hyperledger png images | PNGEgg*. (n.d.). Pngegg. https://www.pngegg.com/en/search?q=hyperledger

[82] *Top 6 technical advantages of Hyperledger Fabric for blockchain networks*. (n.d.-a). IBM Developer. https://developer.ibm.com/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/

[83] IBM Developer. https://developer.ibm.com/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/

[84] *Hyperledger Burrow*. (2021, October 22). Investopedia. https://www.investopedia.com/terms/h/hyperledger-burrow.asp

[85] *Hyperledger Burrow - Hyperledger Burrow - Hyperledger Foundation*. (n.d.). Wiki.Hyperledger. https://wiki.hyperledger.org/display/burrow

[86] Ethereum. (n.d.-g). *Home*. Ethereum.Org. https://ethereum.org/en/

[87] *Hyperledger Explorer Definition*. (2021, October 29). Investopedia. https://www.investopedia.com/terms/h/hyperledger-explorer.asp

[88] *Introduction | Hyperledger Composer*. (n.d.). Hyperledger. https://hyperledger.github.io/composer/v0.19/introduction/introduction.html

[89] Ethereum. (n.d.-i). *What is ether (ETH)?* Ethereum.Org. https://ethereum.org/en/eth/

[90] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized finance." *Journal of Financial Regulation* 6, no. 2 (2020): 172-203.

[91] Conti, R. (2021, May 24). *What Is An NFT? Non-Fungible Tokens Explained*. Forbes Advisor UK. https://www.forbes.com/uk/advisor/investing/nft-non-fungible-token/#:%7E:text=NFT%20stands%20for%20non%2Dfungible,or%20exchanged%20for%20one%20another.

[92] Ethereum. (n.d.-b). *ERC-20 Token Standard*. Ethereum.Org. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

[93] Ethereum. (n.d.-e). *Ethereum upgrades (formerly 'Eth2')*. Ethereum.Org. https://ethereum.org/en/upgrades/

[94] *ethereum*. (n.d.-d). GitHub. https://github.com/ethereum

[95] *How Does Bitcoin Mining Work?* (2022, March 7). Investopedia. https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

[96] *What Is a Wei?* (2021, May 27). Investopedia. https://www.investopedia.com/terms/w/wei.asp

[97] C. (2021a, November 22). *Ethereum Virtual Machine (EVM)*. CoinMarketCap Alexandria. https://coinmarketcap.com/alexandria/glossary/ethereum-virtual-machine-evm

[98] Hancock, J. (2021, December 13). *What is Ethereum Virtual Machine? - Jeffrey Hancock*. Medium. https://ethex-smm.medium.com/what-is-ethereum-virtual-machine-892319e4cac7

[99] *Account Types, Gas, and Transactions — Ethereum Homestead 0.1 documentation*. (n.d.). Ethdocs. https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#:%7E:text=Externally%20owned%20account%20(EOAs)%3A,and%20is%20controlled%20by%20code.

[100] Ethereum. (n.d.-h). *Introduction to smart contracts*. Ethereum.Org. https://ethereum.org/en/developers/docs/smart-contracts/

[101] *Solidity — Solidity 0.8.12 documentation*. (n.d.). Soliditylang. https://docs.soliditylang.org/en/v0.8.12/
[102] *Execution process of Ethereum virtual machine*. (n.d.). Researchgate. https://www.researchgate.net/figure/Execution-process-of-Ethereum-virtual-machine_fig5_349918758
[103] *How does Ethereum work, anyway?* (n.d.). Preethikasireddy. https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway
[104] Sullivan, N. (2018, August 27). *ECDSA: The digital signature algorithm of a better internet*. The Cloudflare Blog. https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet/
[105] Choi, K. (2021, November 3). *What is an Ethereum Address*. Etherscan Information Center. https://info.etherscan.com/what-is-an-ethereum-address/#:%7E:text=An%20Ethereum%20address%20is%20a,receive%20funds%20from%20another%20party.
[106] *Keccak Team*. (n.d.). Keccak. https://keccak.team/keccak_specs_summary.html
[107] Ethereum. (n.d.-f). *Gas and fees*. Ethereum.Org. https://ethereum.org/en/developers/docs/gas/
[108] J. (2021b, August 11). *What is Gas Fee? Differentiate between Gas Price and Gas Limit*. Coin98 Insights - DeFi Content Hub. https://coin98insights.com/what-is-gas-fee
[109] Fabian Vogelsteller , Vitalik Buterin . (2015, November 19). *EIP-20: Token Standard*. Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-20
[110] Ethereum. (n.d.-c). *ERC-721 Non-Fungible Token Standard*. Ethereum.Org. https://ethereum.org/en/developers/docs/standards/tokens/erc-721/
[111] *Ξtheria - What is Ξtheria?* (n.d.). Etheria. https://etheria.world/whatis.html
[112] *beeple (@beeple)* | *Twitter*. (n.d.). twitter. https://twitter.com/beeple?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor
[113] *The World Wide Web project*. (n.d.). Cern. http://info.cern.ch/hypertext/WWW/TheProject.html
[114] Wikipedia contributors. (2022c, January 29). *Tim Berners-Lee*. Wikipedia. https://en.wikipedia.org/wiki/Tim_Berners-Lee
[115] O'Reilly, T. (2022, March 9). *What Is Web 2.0*. O'Reilly Media. https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html
[116] Ethereum. (n.d.-a). *Decentralized applications (dapps)*. Ethereum.Org. https://ethereum.org/en/dapps/
[117] Academy, B. (2019, May 21). *Turing Complete*. Binance Academy. https://academy.binance.com/en/glossary/turing-complete
[118] *A crypto wallet & gateway to blockchain apps* | *MetaMask*. (n.d.). Metamask. https://metamask.io/
[119] *MetaMask Fox*. (n.d.). MetaMask Fox. https://commons.wikimedia.org/wiki/File:MetaMask_Fox.svg
[120] *Home – EOSIO Blockchain Software & Services*. (2022, January 10). EOSIO. https://eos.io/
[121] N. (n.d.). *Neo Smart Economy*. Neo.Org. https://neo.org/
[122] *Tezos: A blockchain designed to evolve*. (n.d.). Tezos. https://tezos.com/
[123] *TRON Network* | *Decentralize The Web*. (n.d.). Tron. https://tron.network/
[124] *polkadot*. (n.d.). Polkadot. https://polkadot.network/

[125] *Algorand | The Blockchain for FutureFi*. (n.d.). Algorand. https://www.algorand.com/
[126] *WebAssembly*. (n.d.). Webassembly. https://webassembly.org/
[127] *Michelson: the language of Smart Contracts in Tezos — Tezos (master branch, 2022/03/09 17:06) documentation*. (n.d.). Tezos. https://tezos.gitlab.io/active/michelson.html
[128] Kumar, A. (2018, August 31). *Smart Contracts On The Blockchain: A deep dive in to Smart Contracts*. Medium. https://abhibvp003.medium.com/smart-contracts-on-the-blockchain-a-deep-dive-in-to-smart-contracts-9616ad26428c
[129] Rosic, A., Mitra, R., Mitra, R., Rosic, A., Molecke, R., & Rosic, A. (2020, November 25). *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*. Blockgeeks. https://blockgeeks.com/guides/smart-contracts/
[130] McMains, V. (2016, May 3). *Johns Hopkins study suggests medical errors are third-leading cause of death in U.S.* The Hub. https://hub.jhu.edu/2016/05/03/medical-errors-third-leading-cause-of-death/
[131] Armstrong, Stephen. "Bitcoin technology could take a bite out of NHS data problem." *Bmj* 361 (2018).
[132] *Home*. (n.d.-a). Medicalchain. https://medicalchain.com/en/
[133] *MedTokens*. (n.d.). MedTokens. https://www.blockdata.tech/tokens/medtokens
[134] Saberi, Sara, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen. "Blockchain technology and its relationships to sustainable supply chain management." *International Journal of Production Research* 57, no. 7 (2019): 2117-2135.
[135] *Supply Chain Management*. (2022, February 21). ConsenSys. https://consensys.net/blockchain-use-cases/supply-chain-management/
[136] *How Blockchain Technology Can Prevent Voter Fraud*. (2020, December 10). Investopedia. https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud/
[137] *horizonstate*. (n.d.). Horizonstate. https://horizonstate.com/
[138] *Decision Token (HST) Price to USD - Live Value Today*. (n.d.). Coinranking. https://coinranking.com/coin/1hWKWrL4Jb9Up+decisiontoken-hst
[139] Bakre, Akshay, Nikita Patil, and Sakshum Gupta. "Implementing decentralized digital identity using blockchain." *International Journal of Engineering Technology Science and Research* 4, no. 10 (2017): 379-385.
[140] Baars, D. S. "Towards self-sovereign identity using blockchain technology." Master's thesis, University of Twente, 2016.
[141] *Decentralized Identifiers (DIDs) v1.0*. (2021, August 3). W3.Org. https://www.w3.org/TR/2021/PR-did-core-20210803/
[142] *Art. 20 GDPR – Right to data portability*. (2018, March 28). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-20-gdpr/
[143] Gillis, A. S. (2022, March 4). *What is the internet of things (IoT)?* IoT Agenda. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[144] Dai, Hong-Ning, Zibin Zheng, and Yan Zhang. "Blockchain for Internet of Things: A survey." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8076-8094.
[145] *chainofthings*. (n.d.). Chainofthings. https://www.chainofthings.com/
[146] de Goede, Marieke. “The Chain of Security.” Review of International Studies 44, no. 1 (2018): 24–42.

[147] *CS2: Chain of Solar*. (n.d.). Chain of Things. https://www.chainofthings.com/cs2chainofsolar#:%7E:text=A%20public%20tool%20to%20monitor,and%2For%20other%20blockchain%20technologies.
[148] Pope, S. (2019, October 16). *Blockchain To Be A Gamechanger For Global Shipping*. Forbes. https://www.forbes.com/sites/stephenpope/2019/10/16/blockchain-to-be-a-gamechanger-for-global-shipping/?sh=3676c1ac512a
[149] *Home*. (n.d.-b). IOTA. https://www.iota.org/
[150] *Tangle ledger – Crypviz*. (n.d.). Crypviz. https://crypviz.io/en/knowledge-database/tangle-ledger/
[151] *Seamless and Trusted Block Data Exchange*. (n.d.). Modum. https://www.modum.io/
[152] *async function - JavaScript | MDN*. (2022, February 18). Developer.Mozilla. https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/async_function
[153] *Remix - Ethereum IDE*. (n.d.). Ethereum. https://remix.ethereum.org/
[154] *JavaScript.com*. (n.d.). Javascript. https://www.javascript.com/
[155] *nodejs*. (n.d.). Nodejs. https://nodejs.org/en/
[156] *npm*. (n.d.). Npmjs. https://www.npmjs.com/
[157] *HTTP | MDN*. (2021, December 27). Developer.Mozilla. https://developer.mozilla.org/en-US/docs/Web/HTTP
[158] *International Plumbing Code (IPC)*. (n.d.). Iccsafe. https://www.iccsafe.org/content/international-plumbing-code-ipc-home-page/