ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΙΣΤΟΥ ΚΑΙ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

Διπλωματική Εργασία

της

Σαμαρά Γεωργίας

Θεσσαλονίκη, Οκτώβριος 2023

ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ BLOCKCHAIN ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΙΣΤΟΥ ΚΑΙ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

Γεωργία Σαμαρά

Πτυχίο Οικονομικών Επιστημών, Πανεπιστήμιο Μακεδονίας, 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Γεωργιάδης Χρήστος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 30/10/2023

Γεωργιάδης Χρήστος	Στειακάκης Εμμανουήλ	Δασίλας Απόστολος
.....	.....	.....

Σαμαρά Γεωργία

.....

Περίληψη

Η τεχνολογία Blockchain εμφανίστηκε το 2008, ως θεμέλιο του πρώτου αποκεντρωμένου κρυπτονομίσματος, Bitcoin. Το blockchain είναι ένα αποκεντρωμένο και κατανεμημένο δημόσιο καθολικό, όπου καταγράφονται και ομαδοποιούνται όλα τα κρυπτογραφικά υπογεγραμμένα δεδομένα σε μπλοκ. Κάθε μπλοκ συνδέεται με το προηγούμενο μέσω του κατακερματισμού του, σχηματίζοντας έτσι την αλυσίδα μπλοκ. Ουσιαστικά, η τεχνολογία Blockchain ενσωματώνει πολλές προϋπάρχουσες έννοιες, όπως η κρυπτογραφία δημόσιου κλειδιού, η ψηφιακή υπογραφή, οι αλγόριθμοι συναίνεσης και οι κρυπτογραφικές συναρτήσεις κατακερματισμού, σε μία ενιαία λύση. Παρότι η τεχνολογία αυτή είναι σχετικά νέα, τα κύρια χαρακτηριστικά της, όπως η αποκέντρωση, η διαφάνεια, η ανωνυμία, η ανθεκτικότητα στις παραβιάσεις και ο αμετάβλητος χαρακτήρας της, την έχουν καταστήσει ευρέως αποδεκτή σε πολλούς τομείς που απαιτούν κοινή χρήση δεδομένων μεταξύ πολλών μερών, χρηματοοικονομικούς και μη. Η παρούσα διπλωματική εργασία παρέχει μια συστηματική βιβλιογραφική επισκόπηση της τεχνολογίας Blockchain, καθώς και της κύριας επέκτασής της πέρα από τις επικυρώσιμες συναλλαγές, γνωστή ως έξυπνα συμβόλαια. Εξετάζει τις διαφορετικές αρχιτεκτονικές προσεγγίσεις, τα βασικά χαρακτηριστικά και συστατικά μέρη της τεχνολογίας, συζητά ορισμένα μοντέλα συναίνεσης που χρησιμοποιούνται σε δίκτυα blockchain, καθώς και ορισμένους από τους περιορισμούς και τα ζητήματα ασφάλειας και ιδιωτικότητας που την περιβάλλουν. Στόχος της εργασίας είναι να προσδιορίσει τις εφαρμογές και την επίδραση της τεχνολογίας Blockchain στις διάφορες πτυχές του ηλεκτρονικού εμπορίου, συμπεριλαμβανομένων των αποκεντρωμένων ηλεκτρονικών χώρων αγοράς, των συστημάτων ψηφιακών πληρωμών, των προγραμμάτων ανταμοιβής πιστών πελατών και της διαδικασίας έγκρισης και αξιολόγησης των κινητών εφαρμογών. Τέλος, παρουσιάζεται μια μελέτη περίπτωσης σχετικά με τη διαχείριση έξυπνων συμβολαίων, με επίκεντρο την υλοποίηση μιας αποκεντρωμένης εφαρμογής ηλεκτρονικού εμπορίου (Dapp) που βασίζεται στο blockchain Ethereum.

Λέξεις Κλειδιά: Τεχνολογία Blockchain, Αποκεντρωμένες Εφαρμογές, Ηλεκτρονικό Εμπόριο, Έξυπνα Συμβόλαια, Solidity

Abstract

Blockchain technology appeared in 2008, as the foundation of the first decentralized cryptocurrency, Bitcoin. Blockchain is a decentralized and distributed public ledger where all cryptographically signed data is recorded and grouped into blocks. Each block is connected to the previous one through its hash, thus forming the block chain. Essentially, Blockchain technology integrates many pre-existing concepts, such as public key cryptography, digital signature, consensus algorithms and cryptographic hash functions, into a unified solution. Although this technology is relatively new, its main features, such as decentralization, transparency, anonymity, tamper resistance and immutability, have made it widely accepted in many fields that require data sharing between many parties, financial and non-financial. This thesis provides a systematic literature review of Blockchain technology, as well as its main extension beyond verifiable transactions, known as smart contracts. It examines the different architectural approaches, key features and components of the technology, discusses some of the consensus models used in blockchain networks, and also touches on some of the limitations and security and privacy issues surrounding it. The objective of the thesis is to identify the applications and impact of Blockchain technology in the various aspects of e-commerce, including decentralized e-marketplaces, digital payment systems, customer loyalty programs, and mobile app approval and evaluation process. Finally, a case study on smart contract management is presented, focusing on the implementation of a decentralized e-commerce application (Dapp) based on the Ethereum blockchain.

Keywords: Blockchain Technology, Decentralized Applications, E-commerce, Smart Contracts, Solidity

Ευχαριστίες

Πρώτα απ’ όλα, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας, κ. Χρήστο Γεωργιάδη, για την διαρκή καθοδήγηση και τις συμβουλές που μου προσέφερε όλο αυτό το διάστημα εκπόνησής της. Παράλληλα, θα ήθελα να απευθύνω ιδιαίτερες ευχαριστίες στον υποψήφιο Διδάκτορα κ. Αντώνη Γιατζή, για την πολύτιμη βοήθειά του στην υλοποίηση της εφαρμογής. Επιπλέον, θα ήθελα να ευχαριστήσω τους καθηγητές, κ. Εμμανουήλ Στειακάκη και κ. Απόστολο Δασίλα, για την συμμετοχή τους στην εξεταστική επιτροπή. Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στους γονείς μου, Μίλτο και Τασούλα, και στην αδερφή μου Ευγενία, για την υποστήριξή τους και την κατανόηση που έδειξαν καθ’ όλη την διάρκεια των μεταπτυχιακών μου σπουδών.

Αφιερώνω την παρούσα διπλωματική εργασία στην κόρη μου, Νεφέλη.

Περιεχόμενα

Κατάλογος Εικόνων

Συμβολισμοί

P2P Peer-to-Peer

PoW Proof-of-Work

PoS Proof-of-Stake

PoA Proof-of-Activity

ABI Application Binary Interface

API Application Programming Interface

EVM Ethereum Virtual Machine

JSON JavaScript Object Notation

MSP Membership Service Provider

IPFS InterPlanetary File System

NFT Non Fungible Token

SPMC Secure Multi-Party Computation

1.Εισαγωγή

Η τεχνολογία Blockchain είναι μια επαναστατική εφεύρεση που έχει τη δυνατότητα να μεταμορφώσει πολλούς κλάδους, από τη χρηματοδότηση και τη διαχείριση της εφοδιαστικής αλυσίδας μέχρι την υγειονομική περίθαλψη και την ψηφοφορία. Στον πυρήνα του, το blockchain είναι ένα αποκεντρωμένο και κατανεμημένο καθολικό που επιτρέπει ασφαλείς και διαφανείς συναλλαγές χωρίς την ανάγκη για μεσάζοντες ή κεντρικές αρχές. Οι συναλλαγές ομαδοποιούνται σε μπλοκ, τα οποία συνδέονται μεταξύ τους χρονολογικά, δημιουργώντας έτσι μια δομή δεδομένων σε σχήμα αλυσίδας, που ονομάζεται επίσης αλυσίδα μπλοκ. Το blockchain αποτελείται από τέσσερα θεμελιώδη στοιχεία. Πρώτον, υπάρχει ο κατακερματισμός, ένας κρυπτογραφικός αλγόριθμος που χρησιμοποιείται για την σύνδεση όλων των μπλοκ μεταξύ τους. Δεύτερον, η ψηφιακή υπογραφή, μια κρυπτογραφική τεχνική που παρέχει έλεγχο ταυτότητας και ακεραιότητα των συναλλαγών στο δίκτυο. Το τρίτο στοιχείο είναι το P2P δίκτυο, ένα αποκεντρωμένο δίκτυο κόμβων (υπολογιστών) που διευκολύνει την επικοινωνία, την κοινή χρήση και τη διανομή δεδομένων σε ολόκληρο το δίκτυο. Τέλος, ο μηχανισμός συναίνεσης, ο οποίος περιλαμβάνει ένα σύνολο ψηφιακών διαδικασιών, χρησιμοποιείται για την επικύρωση των συναλλαγών και την διατήρηση της ακεραιότητας και της ασφάλειας του blockchain. Η επιτυχία της τεχνολογίας Blockchain εξαρτάται σε μεγάλο βαθμό από τα χαρακτηριστικά της, όπως η αποκέντρωση, η διαφάνεια, η ψευδωνυμία, η αυτονομία, η ανθεκτικότητα στις παραβιάσεις, ο αμετάβλητος χαρακτήρας της, η δυνατότητα ελέγχου, η ανοχή σε σφάλματα και η ασφάλεια, τα οποία προσφέρουν πολλά πλεονεκτήματα σε σχέση με τα παραδοσιακά συστήματα.

Η τεχνολογία αυτή έγινε ευρέως γνωστή το 2009 με την κυκλοφορία του δικτύου Bitcoin (Nakamoto, 2008), του πρώτου από τα πολλά σύγχρονα κρυπτονομίσματα, τα οποία αποτελούν την αρχική έκδοση της τεχνολογίας Blockchain, γνωστή και ως η πρώτη γενιά, Blockchain 1.0. Το Bitcoin χρησιμοποιείται κυρίως για τη μεταφορά ψηφιακού νομίσματος από έναν χρήστη σε έναν άλλο χωρίς να χρειάζονται μεσάζοντες, όπως τράπεζες ή χρηματοπιστωτικά ιδρύματα. Βασίζεται σε έναν αλγόριθμο συναίνεσης απόδειξης εργασίας (PoW) για την επικύρωση των συναλλαγών και την ασφάλεια του δικτύου. Τα blockchain δεύτερης γενιάς, Blockchain 2.0, εισήχθησαν το 2014 με την δημιουργία του Ethereum (Buterin, 2014). Η κύρια λειτουργικότητα που προστέθηκε

ήταν η δυνατότητα εκτέλεσης έξυπνων συμβολαίων. Τα έξυπνα συμβόλαια είναι συμβόλαια που εκτελούνται αυτόματα όταν πληρούνται ορισμένες προϋποθέσεις, με τους όρους της συμφωνίας απευθείας γραμμένους σε κώδικα. Αυτή η προστιθέμενη λειτουργικότητα αύξησε τις πιθανές περιπτώσεις χρήσης για την τεχνολογία Blockchain πέρα από απλές συναλλαγές κρυπτονομισμάτων. Ακολουθεί η τρίτη γενιά, Blockchain 3.0, η οποία έχει λιγότερο σαφή ορισμό από τις προηγούμενες. Η τρίτη γενιά συμπεριλαμβάνει αποκεντρωμένες εφαρμογές σε επίπεδο επιχειρήσεων, που πρωταρχικό στόχο έχουν τη δημιουργία ενός πιο αποκεντρωμένου και δημοκρατικού οικοσυστήματος όπου τα άτομα και οι επιχειρήσεις μπορούν να αλληλεπιδρούν μεταξύ τους χωρίς να χρειάζονται μεσάζοντες, με εφαρμογές σε ένα ευρύτερο σύνολο βιομηχανιών εκτός του τομέα της χρηματοδότησης και της οικονομίας (Bhutta et al., 2021).

Αυτή η εξέλιξή της τεχνολογίας έχει οδηγήσει στην αυξανόμενη υιοθέτησή της σε όλους σχεδόν τους τομείς που απαιτούν κοινή χρήση δεδομένων μεταξύ πολλών μερών, όπως στην διαχείριση εφοδιαστικής αλυσίδας, στις διασυνοριακές πληρωμές, στην χρηματοδότηση εμπορίου, στις αγορές προβλέψεων, στα συστήματα αξιολόγησης προϊόντων, στα προγράμματα επιβράβευσης πιστών πελατών, στα συστήματα διαχείρισης ταυτότητας, στις εφαρμογές crowdsourcing, καθώς και στις έξυπνες συμβάσεις και δημοπρασίες. Προβλέπεται, μάλιστα, ότι τα ετήσια έσοδα των εταιρικών εφαρμογών που βασίζονται σε blockchain παγκοσμίως θα φτάσουν τα 19,9 δισεκατομμύρια δολάρια έως το 2025, με ετήσιο ρυθμό ανάπτυξης 26,2%, από περίπου 2,5 δισεκατομμύρια δολάρια που ήταν το 2016 (Zhang et al., 2019). Η ευρεία αυτή εξάπλωση της τεχνολογίας διαταράσσει τις παραδοσιακές επιχειρηματικές διαδικασίες και τις συναλλαγές, οι οποίες πλέον μπορούν να λειτουργούν με αποκεντρωμένο τρόπο, με το blockchain να παρέχει εμπιστοσύνη, προστασία της ιδιωτικής ζωής, χαμηλότερο κόστος συναλλαγής, ακεραιότητα συναλλαγών και βελτίωση της συνολικής αποδοτικότητας (Casino et al., 2019). Γι’ αυτούς τους λόγους η τεχνολογία Blockchain μπορεί να χαρακτηριστεί ως ένα από τα σημαντικότερα κυρίαρχα θέματα σήμερα, λαμβάνοντας σημαντική προσοχή τόσο από ερευνητές όσο και από επιχειρηματικούς οργανισμούς, προσελκύοντας μεγάλες επενδύσεις σε δυτικές χώρες. Συγκεκριμένα, οι Ηνωμένες Πολιτείες πρωτοστατούν στις επενδύσεις blockchain, αρκετές χώρες όπως η Αυστραλία, ο Καναδάς και η Νότια Κορέα σχεδιάζουν να αναβαθμίσουν τα υπάρχοντα

συστήματα τους χρησιμοποιώντας τεχνολογία Blockchain, ενώ το Ισραήλ έχει ήδη δημιουργήσει ένα κέντρο καινοτομίας blockchain (Zhang et al., 2020).

1.1. Αντικείμενο και στόχοι της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία παρέχει μια συστηματική βιβλιογραφική επισκόπηση της τεχνολογίας Blockchain, καθώς και της κύριας επέκτασής της πέρα από τις επικυρώσιμες συναλλαγές, γνωστή ως έξυπνα συμβόλαια. Εξετάζει διαφορετικές κατηγορίες προσεγγίσεων υλοποίησης, συζητά τα βασικά χαρακτηριστικά και στοιχεία της τεχνολογίας, εξετάζει ορισμένα μοντέλα συναίνεσης που χρησιμοποιούνται σε δίκτυα blockchain, καθώς επίσης αγγίζει ορισμένους από τους περιορισμούς, τα ζητήματα ασφάλειας και ιδιωτικότητας που περιβάλλουν την τεχνολογία. Ο στόχος αυτής της εργασίας είναι να προσδιορίσει τις εφαρμογές και την επίδραση της τεχνολογίας Blockchain στις διάφορες πτυχές του ηλεκτρονικού εμπορίου, συμπεριλαμβανομένων των αποκεντρωμένων ηλεκτρονικών χώρων αγοράς, των συστημάτων ψηφιακών πληρωμών, των προγραμμάτων ανταμοιβής πιστών πελατών, και της διαδικασίας έγκρισης και αξιολόγησης των κινητών εφαρμογών. Τέλος, η παρούσα διπλωματική εργασία παρουσιάζει μια μελέτη περίπτωσης σχετικά με τη διαχείριση έξυπνων συμβολαίων, με επίκεντρο την υλοποίηση μιας αποκεντρωμένης εφαρμογής ηλεκτρονικού εμπορίου (Dapp) που βασίζεται στο blockchain Ethereum. Ο σκοπός της μελέτης περίπτωσης είναι να παράσχει μια ολοκληρωμένη προσέγγιση και να προσφέρει γνώσεις για τον πολύπλευρο τομέα της διαχείρισης έξυπνων συμβολαίων, αποκαλύπτοντας τις δυνατότητες μετασχηματισμού των έξυπνων συμβολαίων σε εφαρμογές ηλεκτρονικού εμπορίου και όχι μόνο.

1.2. Δομή της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία δομείται σε έξι κεφάλαια. Το πρώτο κεφάλαιο περιλαμβάνει τα εισαγωγικά στοιχεία, το αντικείμενο και τους στόχους της διπλωματικής εργασίας, τη δομή της και τη μεθοδολογία που χρησιμοποιήθηκε για την συγγραφή της.

Το δεύτερο κεφάλαιο αποτελεί μια λεπτομερή βιβλιογραφική επισκόπηση της τεχνολογίας Blockchain. Αρχικά παρουσιάζεται η κατηγοριοποίηση των δικτύων και γίνεται μια περιγραφή της αρχιτεκτονικής και της διαδικασίας εκτέλεσης των

συναλλαγών. Στην συνέχεια αναλύονται τα βασικά χαρακτηριστικά της τεχνολογίας, τα οποία είναι η αποκέντρωση, η διαφάνεια, η ανθεκτικότητα στις παραβιάσεις και η ανωνυμία, καθώς επίσης προσεγγίζονται οι βασικές έννοιες και τα συστατικά μέρη όπως το καθολικό, οι κρυπτογραφικές συναρτήσεις κατακερματισμού, οι συναλλαγές, η ασύμμετρη κρυπτογραφία και οι διευθύνσεις. Επιπλέον, γίνεται μια ανάλυση των αλγορίθμων συναίνεσης και των διάφορων ζητημάτων λειτουργικότητας, όπως η επεκτασιμότητα, η κατανάλωση ενέργειας και η καθυστέρηση των συναλλαγών. Τέλος, πραγματοποιείται ανάλυση των διάφορων ζητημάτων ασφάλειας, όπως οι επιθέσεις διπλής δαπάνης, οι επιθέσεις στο πρωτόκολλο επικοινωνίας και οι επιθέσεις εξόρυξης, καθώς επίσης περιγράφονται οι προκλήσεις απορρήτου σε σενάρια blockchain και οι προτεινόμενες λύσεις διατήρησής του.

Στο τρίτο κεφάλαιο πραγματοποιείται μια ανάλυση των έξυπνων συμβολαίων, τα οποία αποτελούν την κύρια επέκταση της τεχνολογίας Blockchain πέρα από τις επικυρώσιμες συναλλαγές. Αρχικά, παρουσιάζεται η δομή και η διαδικασία λειτουργίας ενός έξυπνου συμβολαίου. Στην συνέχεια γίνεται αναφορά στις πλατφόρμες blockchain που υποστηρίζουν την ανάπτυξη έξυπνων συμβολαίων, όπως επίσης πραγματοποιείται μια σύγκριση μεταξύ των δύο πιο διαδεδομένων πλατφορμών, Ethereum και Hyperledger Fabric. Τέλος, αναλύονται τα διάφορα ζητήματα ιδιωτικότητας και ασφάλειας, παρουσιάζονται κάποια αυτοματοποιημένα εργαλεία ανάλυσης ασφάλειας για έξυπνα συμβόλαια, και αναλύονται τα διάφορα νομικά ζητήματα.

Ακολουθεί στο τέταρτο κεφάλαιο μια συστηματική έρευνα, βάσει της σύγχρονης βιβλιογραφίας, για την επίδραση της τεχνολογίας Blockchain στις διάφορες πτυχές του ηλεκτρονικού εμπορίου όπως στους αποκεντρωμένους ηλεκτρονικούς χώρους αγοράς, στα συστήματα ψηφιακών πληρωμών, στα προγράμματα ανταμοιβής πιστών πελατών, και στην διαδικασία έγκρισης και αξιολόγησης των κινητών εφαρμογών. Αναφέρονται οι περιορισμοί των υφιστάμενων παραδοσιακών συστημάτων και τα πλεονεκτήματα που προσφέρει η τεχνολογία Blockchain στην κάθε περίπτωση, όπως επίσης παρουσιάζονται διάφορες εφαρμογές που αφορούν όλα τα παραπάνω και βασίζονται στην τεχνολογία Blockchain.

Στο πέμπτο κεφάλαιο παρουσιάζεται μια μελέτη περίπτωσης σχετικά με τη διαχείριση έξυπνων συμβολαίων, με επίκεντρο την υλοποίηση μιας αποκεντρωμένης εφαρμογής ηλεκτρονικού εμπορίου (Dapp) που βασίζεται στο blockchain Ethereum. Ως μελέτη περίπτωσης, η παρούσα εφαρμογή παρέχει γνώσεις σχετικά με το σχεδιασμό, την υλοποίηση και την ενσωμάτωση έξυπνων συμβολαίων σε εφαρμογές πραγματικού κόσμου. Δείχνει πώς τα έξυπνα συμβόλαια μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση των διαδικασιών και τη διαχείριση δεδομένων στο blockchain, ειδικά στο πλαίσιο ενός Dapp ηλεκτρονικού εμπορίου. Επιπλέον, υπογραμμίζει τη σημασία των ασφαλών αλληλεπιδράσεων με τους χρήστες, του χειρισμού σφαλμάτων και της συνεχούς ανάπτυξης στη διαχείριση έξυπνων συμβολαίων.

Τέλος, στο έκτο κεφάλαιο διατυπώνονται τα συμπεράσματα της διατριβής, τα όρια και οι περιορισμοί που εντοπίζονται καθώς και οι μελλοντικές επεκτάσεις της εφαρμογής που υλοποιήθηκε.

1.3. Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για τη συγγραφή της παρούσας διπλωματικής εργασίας βασίστηκε στη βιβλιογραφική ανασκόπηση δημοσιεύσεων από διάφορες επιστημονικές βάσεις δεδομένων. Αρχικά, καθορίστηκαν οι βασικές έννοιες και στη συνέχεια, επιλέχθηκαν συγκεκριμένες λέξεις-κλειδιά, όπως επίσης προσδιορίστηκε το χρονικό διάστημα από το έτος 2018 έως σήμερα, με σκοπό να περιοριστούν τα αποτελέσματα της αναζήτησης. Ακολούθησε μια συστηματική αναζήτηση βιβλιογραφίας σε ηλεκτρονικές βάσεις δεδομένων, με κύριες πηγές το Google Scholar και τη βιβλιοθήκη του Πανεπιστημίου Μακεδονίας. Στη συνέχεια, εξετάστηκαν τα άρθρα για να επιλεγούν αυτά που θα συμπεριληφθούν στην ανασκόπηση. Απορρίφθηκαν όσα δεν σχετίζονταν με την εργασία βάσει τίτλων ή περιλήψεων, καθώς και διαδικτυακά άρθρα με αμφίβολη αξιοπιστία. Τα επιλεγμένα άρθρα αξιολογήθηκαν ως προς την ποιότητα και την συνάφειά τους, και τέλος, εξήχθησαν τα δεδομένα βάσει των οποίων πραγματοποιήθηκε η λεπτομερής ανάλυση και σύνθεση της διπλωματικής εργασίας.

2.Τεχνολογία Blockchain

Το blockchain είναι ένα δημόσιο ψηφιακό καθολικό όπου καταγράφονται όλες οι κρυπτογραφικά υπογεγραμμένες συναλλαγές με χρονολογική σειρά και ομαδοποιούνται σε μπλοκ, με το καθένα να εξαρτάται από τον κατακερματισμό του προηγούμενου μπλοκ, σχηματίζοντας έτσι μια δομή δεδομένων σε σχήμα αλυσίδας. Αυτή η αλυσίδα των μπλοκ αποτελεί την βασική ιδέα της τεχνολογίας blockchain, από όπου προέρχεται και το όνομά της. Κάθε μπλοκ αποτελείται από μια κεφαλίδα, η οποία περιέχει μεταδεδομένα για το μπλοκ, και το σώμα, το οποίο περιέχει ένα σύνολο συναλλαγών. Κάθε συναλλαγή περιλαμβάνει έναν ή περισσότερους χρήστες του δικτύου blockchain και μια καταγραφή του τι συνέβη και υπογράφεται ψηφιακά από τον χρήστη που υπέβαλε τη συναλλαγή (Yaga et al., 2018). Το καθολικό αποθηκεύεται με κατανεμημένο τρόπο σε ένα P2P δίκτυο, είναι συγχρονισμένο παγκοσμίως και διαθέσιμο για λήψη από οποιονδήποτε μπορεί να συνδεθεί στο δίκτυο αυτό. Με άλλα λόγια, ένα blockchain μπορεί να θεωρηθεί ως ένα υπολογιστικό φύλλο που αντιγράφεται χιλιάδες φορές σε ένα παγκόσμιο δίκτυο υπολογιστών και ενημερώνεται τακτικά, έτσι ώστε οι νέες συναλλαγές να μπορούν να γίνουν μέρος του υπολογιστικού αυτού φύλλου (Van der Auwera et al., 2020). Ουσιαστικά, η τεχνολογία blockchain ενσωματώνει προϋπάρχουσες έννοιες, όπως η κρυπτογραφία δημόσιου κλειδιού, η ψηφιακή υπογραφή, η συναίνεση και οι κρυπτογραφικές συναρτήσεις κατακερματισμού, σε μία ενιαία λύση. Το 2008 έκανε την εμφάνισή της ως θεμέλιο του πρώτου αποκεντρωμένου κρυπτονομίσματος Bitcoin (Nakamoto, 2008).

Σύμφωνα με τον Waldo (2019) τρεις είναι οι βασικοί στόχοι της τεχνολογίας. Ο πρώτος είναι η εξασφάλιση της ανωνυμίας των συμμετεχόντων, η οποία επιτυγχάνεται με τη χρήση κρυπτογραφίας ασύμμετρου κλειδιού. Ο δεύτερος στόχος είναι η παροχή ενός δημόσιου καθολικού όπου καταγράφεται το σύνολο των συναλλαγών, που δεν μπορούν να τροποποιηθούν μόλις επαληθευτούν και συμφωνηθούν. Η χρήση αυτού του καθολικού για την επαλήθευση των συναλλαγών εκτός από την ανταλλαγή ηλεκτρονικών μετρητών υπήρξε η κύρια επέκταση της τεχνολογίας blockchain (Waldo, 2019). Ο τρίτος, και τελικός στόχος, είναι η αποκέντρωση, δηλαδή το σύστημα να είναι ανεξάρτητο από οποιοδήποτε αξιόπιστο τρίτο μέρος. Στην περίπτωση των κρυπτονομισμάτων αυτό αποτελεί και το κύριο πλεονέκτημά της, καθώς επιτρέπει τις

άμεσες συναλλαγές μεταξύ των χρηστών χωρίς την ανάγκη μιας αξιόπιστης αρχής. Με την πάροδο των χρόνων έχουν αναπτυχθεί διάφορες νέες τεχνολογίες που σχετίζονται με την τεχνολογία blockchain, όπως επίσης πολυάριθμες παραλλαγές των δικτύων της, με την πλειονότητα όμως αυτών να μοιράζονται κοινές βασικές έννοιες.

Σε αυτό το κεφάλαιο παρουσιάζεται μια επισκόπηση της τεχνολογίας Blockchain. Αρχικά παρουσιάζεται η κατηγοριοποίηση των δικτύων και γίνεται μια περιγραφή της αρχιτεκτονικής και της διαδικασίας εκτέλεσης των συναλλαγών. Στην συνέχεια, αναλύονται τα βασικά χαρακτηριστικά της τεχνολογίας, καθώς επίσης προσεγγίζονται οι βασικές έννοιες και τα συστατικά μέρη της. Επιπλέον, γίνεται μια ανάλυση των αλγορίθμων συναίνεσης και των διάφορων ζητημάτων λειτουργικότητας. Τέλος, παρουσιάζονται τα διάφορα ζητήματα ασφάλειας και ιδιωτικότητας.

2.1. Κατηγοριοποίηση των δικτύων Blockchain

Η ταξινόμηση των δικτύων blockchain μπορεί να πραγματοποιηθεί σε δύο διαφορετικές κατηγορίες, βάσει της ιδιοκτησίας του δικτύου και βάσει των δικαιωμάτων πρόσβασης των χρηστών. Στην πρώτη κατηγορία τα δίκτυα διακρίνονται σε δημόσια, ιδιωτικά ή κοινοπραξία. Στην δεύτερη κατηγορία διακρίνονται σε permissionless και permissioned, όπου στην πρώτη περίπτωση οποιοσδήποτε χρήστης μπορεί να εγγραφεί στο δίκτυο και να συμμετάσχει στη διαδικασία δημιουργίας και επαλήθευσης νέου μπλοκ, ενώ στην δεύτερη, μόνο οι εξουσιοδοτημένοι ή προκαθορισμένοι κόμβοι μπορούν να το κάνουν. Πολλές φορές δημιουργείται σύγχυση μεταξύ των διακρίσεων με αποτέλεσμα ο όρος δημόσιο blockchain να θεωρείται ταυτόσημος με το permissionless blockchain και ο όρο ιδιωτικό blockchain να ταυτίζεται με το permissioned blockchain. Καθώς η μία κατηγοριοποίηση μπορεί να θεωρηθεί συμπληρωματική της άλλης, σε αυτή την ενότητα θα επικεντρωθούμε μονό στην διάκριση βάσει των δικαιωμάτων πρόσβασης των χρηστών.

Permissionless Blockchain. Είναι αποκεντρωμένες πλατφόρμες καθολικών προσβάσιμες με ίσες δυνατότητες από όλους, χωρίς να απαιτείται οποιαδήποτε διαδικασία ταυτοποίησης. Συνήθως δημιουργούνται με την χρήση λογισμικού ανοιχτού κώδικα. Οποιοσδήποτε χρήστης μπορεί να διαβάσει και να γράψει στο καθολικό, να ξεκινήσει και να ολοκληρώσει κάποια συναλλαγή εντός του δικτύου όπως επίσης να

συμμετάσχει στην διαδικασία επικύρωσης των συναλλαγών. Δεδομένου ότι τα permissionless δίκτυα είναι διαθέσιμα σε όλους για συμμετοχή, είναι επίσης εκτεθειμένα σε επιθέσεις και παραβιάσεις από κακόβουλους χρήστες. Ωστόσο, ο ισχυρός μηχανισμός συναίνεσης, όπως ο αλγόριθμος Proof of Work, σε συνδυασμό με την κρυπτογραφική επικύρωση ολόκληρου του blockchain κάθε φορά που προστίθεται ένα νέο μπλοκ (Puthal et al., 2018), προστατεύουν το δίκτυο από ενδεχόμενες παραποιήσεις του περιεχομένου των μπλοκ. Αυτή η κατηγορία είναι ελκυστική για εφαρμογές όπως τα blockchains καταγραφής συναλλαγών του κρυπτονομίσματος Bitcoin, οι οποίες επιδιώκουν να διασφαλίσουν ότι κανείς δεν μπορεί να ελέγξει ποιος μπορεί να συμμετάσχει και οι συμμετέχοντες δεν είναι πρόθυμοι να αποκαλύψουν τις ταυτότητές τους (Herlihy, 2019).

Permissioned Blockchain. Είναι ένας τύπος συστήματος blockchain όπου απαιτείται εξουσιοδότηση των συμμετεχόντων από κάποια αρχή, είτε κεντρική είτε αποκεντρωμένη, πριν από τη συμμετοχή τους στις λειτουργίες του δικτύου (Bhushan et al., 2021). Τα permissioned δίκτυα blockchain έχουν σχεδιαστεί για να διευκολύνουν την κοινή χρήση και την ανταλλαγή δεδομένων μεταξύ μιας ομάδας ατόμων, όπως σε έναν ιδιωτικό οργανισμό, ή μεταξύ πολλών οργανισμών, όπως σε μία κοινοπραξία. Η δημιουργία και η διατήρησή τους μπορεί να γίνει με την χρήση λογισμικού είτε ανοιχτού είτε κλειστού κώδικα. Σε ένα permissioned σύστημα blockchain, μόλις οι κόμβοι γίνουν μέρος του δικτύου, συμβάλλουν στη λειτουργία ενός αποκεντρωμένου δικτύου, με κάθε κόμβο να διατηρεί ένα αντίγραφο του καθολικού και να συνεργάζεται για να επιτευχθεί συναίνεση για ενημέρωση, αλλά σε αντίθεση με ένα permissionless blockchain, οι εγγραφές είναι περιορισμένες (Puthal et al., 2018). Δεδομένης της εμπιστοσύνης μεταξύ των κόμβων, αφού όλοι είναι εξουσιοδοτημένοι να δημοσιεύουν μπλοκ και καθώς η εξουσιοδότησή τους μπορεί να ανακληθεί σε περίπτωση κακής συμπεριφοράς, τα μοντέλα συναίνεσης που χρησιμοποιούνται είναι συνήθως ταχύτερα και λιγότερο υπολογιστικά ακριβά σε σχέση με τα μοντέλα συναίνεσης στα permissionless blockchains (Yaga et al., 2018). Εφαρμογές που βασίζονται σε permissioned δίκτυα blockchain είναι το Corda και το Quorum (Syed et al., 2019).

2.2. Αρχιτεκτονική της τεχνολογίας Blockchain

Με μια στενή έννοια, το blockchain είναι ένα ψηφιακό καθολικό κρυπτογραφικά υπογεγραμμένων συναλλαγών που ομαδοποιούνται σε μπλοκ, με το καθένα να εξαρτάται από το προηγούμενο μπλοκ, σχηματίζοντας έτσι μια δομή δεδομένων σε σχήμα αλυσίδας. Με μια ευρύτερη έννοια, ωστόσο, το blockchain μπορεί να θεωρηθεί ως το υποκείμενο πλαίσιο που περιλαμβάνει έναν αριθμό απαραίτητων στοιχείων, όπως το περιβάλλον αλληλεπίδρασης και οι εφαρμογές (Gao et al., 2018). Υπό αυτή την ευρύτερη έννοια, η αρχιτεκτονική της τεχνολογίας blockchain μπορεί να υποδιαιρεθεί σε τρία επίπεδα, σε επίπεδο δεδομένων, σε επίπεδο δικτύου και σε επίπεδο εφαρμογής, τα οποία αναλύονται παρακάτω.

Επίπεδο Δεδομένων (Data Layer). Το στρώμα αυτό περικλείει τη θεμελιώδη μονάδα ολόκληρης της τεχνολογίας blockchain, τη δομή της αλυσίδας μπλοκ δεδομένων, καθώς και τις σχετικές τεχνολογίες ψηφιακής υπογραφής και χρονικής σήμανσης (Zou et al., 2020). Κάθε μπλοκ περιέχει μια κεφαλίδα μπλοκ και δεδομένα μπλοκ. Η κεφαλίδα περιέχει μεταδεδομένα γι' αυτό το μπλοκ, όπως την χρονική σήμανση, που δείχνει την ώρα δημιουργίας του μπλοκ, την αξία nonce, έναν αυθαίρετο αριθμό που χρησιμοποιείται μόνο μία φορά, τον κατακερματισμό των δεδομένων (hash) και τον κατακερματισμό της κεφαλίδας του προηγούμενου μπλοκ. Το αρχικό μπλοκ, γνωστό και ως μπλοκ genesis, δεν περιέχει προηγούμενο κατακερματισμό παρά μόνο τον δικό του, και είναι το μπλοκ που καταγράφει την αρχική κατάσταση του συστήματος (Johar et al., 2021). Τα δεδομένα περιέχουν μια λίστα επικυρωμένων συναλλαγών που περιλαμβάνονται στο δίκτυο blockchain. Η ύπαρξη του προηγούμενου κατακερματισμού στην κεφαλίδα του μπλοκ είναι που συνδέει τα μπλοκ μεταξύ τους και έτσι σχηματίζεται η αλυσίδα μπλοκ. Αυτή η σύνδεση διασφαλίζει ότι οι πληροφορίες είναι αναλλοίωτες, διότι, εάν κάποιος σκοπεύει να τροποποιήσει ένα μπλοκ θα πρέπει επίσης να τροποποιήσει κι όλα τα προηγούμενα μπλοκ σε μια αλυσίδα (Gupta & Sadoghi, 2021), γεγονός που κάνει την επίθεση κρυπτογραφικά ακατόρθωτη.

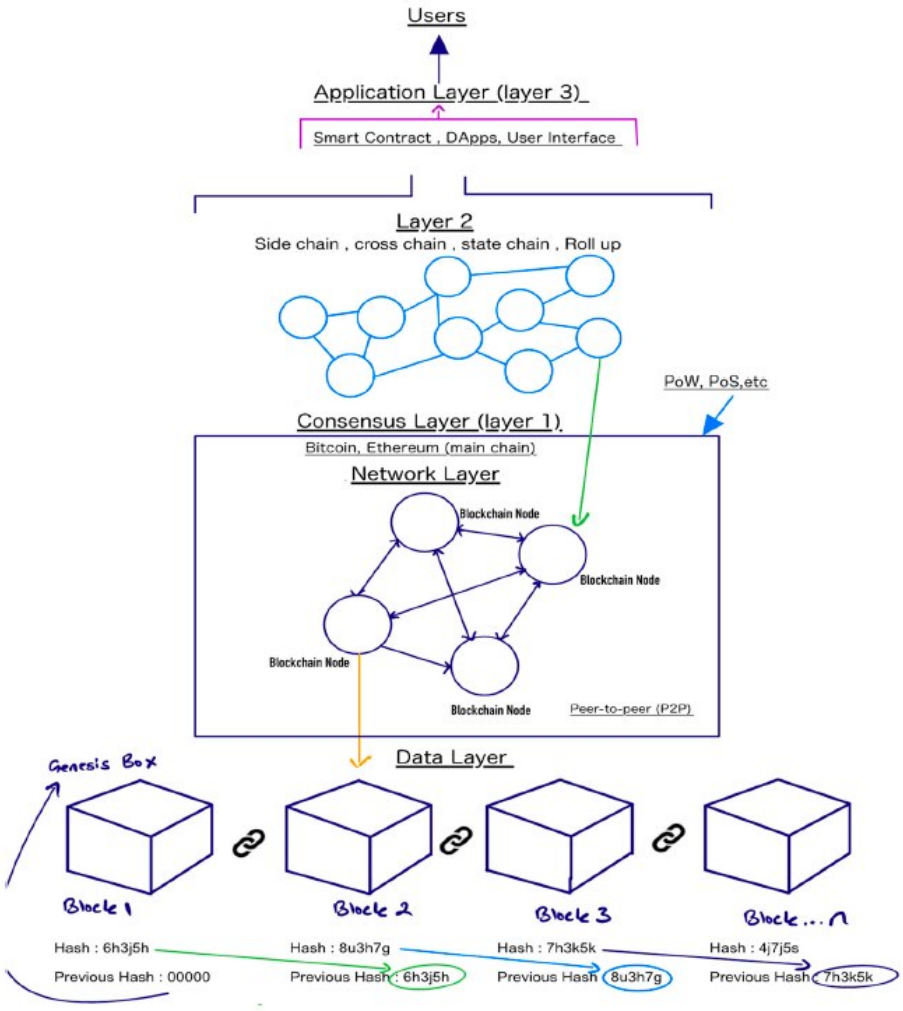
Επίπεδο Δικτύου (Network Layer). Σε αυτό το επίπεδο συμπεριλαμβάνονται το P2P δίκτυο και ο μηχανισμός συναίνεσης. Αρχικά, η τεχνολογία blockchain αποτελείται από ένα παγκόσμιο P2P δίκτυο, μια διαμόρφωση δικτύου όπου οι συμμετέχοντες διαμοιράζονται τους πόρους τους ισοδύναμα και μπορούν να επικοινωνήσουν μεταξύ

τους χωρίς να περάσουν από ένα κεντρικό σημείο. Συνεπώς, το δίκτυο λειτουργεί αποκεντρωμένα, χωρίς να υπάρχει κάποια ενιαία κεντρική αρχή. Οι πληροφορίες των συναλλαγών συνεχώς καταγράφονται στο ψηφιακό καθολικό και ανταλλάσσονται μεταξύ όλων των συμμετεχόντων, γνωστοί και ως κόμβοι, οι οποίοι είναι τα μεμονωμένα συστήματα μέσα στο κατανεμημένο δίκτυο. Ένα τυπικό δίκτυο blockchain έχει τρεις διαφορετικούς τύπους κόμβων, τους απλούς κόμβους (lightweight nodes), τους πλήρεις κόμβους (full nodes) και τους κόμβους εξόρυξης (mining ή publishing nodes). Ένας πλήρης κόμβος αποθηκεύει αντίγραφο του καθολικού και διασφαλίζει ότι οι συναλλαγές είναι έγκυρες, σε αντίθεση με έναν απλό κόμβο ο οποίος μπορεί απλώς να στέλνει και να λαμβάνει συναλλαγές, δεν αποθηκεύει ή διατηρεί αντίγραφο του blockchain και πρέπει να περάσει τις συναλλαγές του σε πλήρεις κόμβους (Yaga et al., 2018). Ένας κόμβος εξόρυξης είναι ένας πλήρης κόμβος με δυνατότητα εξόρυξης, δηλαδή τη διαδικασία δημιουργίας ενός νέου μπλοκ (Ismail & Materwala, 2019). Παρ' ότι κάποιοι κόμβοι έχουν διαφορετικά καθήκοντα όλοι θεωρούνται ίσοι και αποτελούν την ραχοκοκαλιά ολόκληρου του συστήματος (Van der Auwera et al., 2020).

Μια ακόμα βασική πτυχή της τεχνολογίας blockchain που συμπεριλαμβάνεται στο επίπεδο του δικτύου αφορά τον τρόπο με τον οποίο καθορίζεται ο χρήστης που δημοσιεύει το επόμενο μπλοκ, την στιγμή που υπάρχουν πολλοί χρήστες που ανταγωνίζονται για τη δημοσίευσή του. Δεδομένου ότι δεν υπάρχει κάποια κεντρική αρχή, και οι κόμβοι ή το ίδιο το δίκτυο μπορεί να είναι αναξιόπιστα, η συμφωνία μεταξύ των συμμετεχόντων διασφαλίζεται με την εφαρμογή ενός μηχανισμού συναίνεσης, ένα σύνολο δηλαδή καθιερωμένων κανόνων και κανονισμών σύμφωνα με τους οποίους προστίθενται μπλοκ στο σύστημα. Ουσιαστικά, το πρωτόκολλο συναίνεσης επιτρέπει στους συμμετέχοντες να συνεργάζονται, να συντονίζονται και να εξασφαλίζουν την επίτευξη μιας ορθολογικής απόφασης (Patel et al., 2020) σχετικά με την έγκριση ή απόρριψη μιας συναλλαγής. Έτσι, όλοι οι κόμβοι συμφωνούν για το ποια συναλλαγή πρέπει να επιλεχθεί, στην συνέχεια η επιλεγμένη συναλλαγή γίνεται γνωστή στο δίκτυο και θεωρείται πλέον έγκυρη. Περισσότερα για τον μηχανισμό συναίνεσης και τους διάφορους αλγόριθμους που έχουν αναπτυχθεί αναφέρονται σε επόμενη ενότητα.

Επίπεδο Εφαρμογής (Application Layer). Τέλος, το επίπεδο εφαρμογής παρουσιάζει τα διάφορα σενάρια και τις διάφορες εφαρμογές που μπορεί να ενσωματώσει το blockchain.

Εκτός του κόσμου των κρυπτονομισμάτων, η τεχνολογία blockchain έχει βρει εφαρμογή σε πολλούς κλάδους της οικονομίας, συμπεριλαμβανομένων των επιχειρηματικών υπηρεσιών, του διακανονισμού των ψηφιακών περιουσιακών στοιχείων, των αγορών προβλέψεων, των αυτοματοποιημένων συστημάτων συλλογισμού και των συστημάτων έξυπνων συμβολαίων. Μερικές εφαρμογές που αφορούν το ηλεκτρονικό εμπόριο θα αναλυθούν λεπτομερώς σε επόμενο κεφάλαιο.



Εικόνα 2.1. Αρχιτεκτονική της τεχνολογίας Blockchain (Bhujel & Rahulamathavan, 2022)

2.2.1. Διαδικασία εκτέλεσης συναλλαγής

Για να γίνει κατανοητή η λειτουργία ενός τυπικού δικτύου blockchain, σε αυτή την ενότητα εξετάζεται ένα σύνολο κόμβων που λειτουργούν σε ένα blockchain για να σχηματίσουν ένα P2P δίκτυο. Τα βήματα που ακολουθούνται στην διαδικασία εκτέλεσης μιας συναλλαγής είναι τα εξής.

Βήμα 1: Οι χρήστες χρησιμοποιούν ένα ζευγάρι δημόσιου/ιδιωτικού κλειδιού για να αλληλεπιδράσουν με το blockchain. Πρώτα κατακερματίζουν τα δεδομένα συναλλαγής χρησιμοποιώντας μια συνάρτηση κατακερματισμού (hash) και μετά κρυπτογραφούν τα κατακερματισμένα δεδομένα χρησιμοποιώντας το ιδιωτικό κλειδί τους, διαδικασία που είναι γνωστή ως ψηφιακή υπογραφή της συναλλαγής (Ismail & Materwala, 2019). Η ασύμμετρη κρυπτογραφία κλειδιού βοηθά στη διατήρηση της ακεραιότητας, του ελέγχου της ταυτότητας και της μη απόρριψης εντός του δικτύου (Bhushan et al., 2021). Στη συνέχεια οι υπογεγραμμένες συναλλαγές μεταδίδονται στους ομότιμους του δίκτυο.

Βήμα 2: Οι γειτονικοί κόμβοι επαληθεύουν την εγκυρότητα της συναλλαγής ελέγχοντας, πρώτον, την ταυτότητα του χρήστη, αποκρυπτογραφώντας την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του προτεινόμενου χρήστη, και δεύτερον, την ακεραιότητα των δεδομένων, κατακερματίζοντας τα δεδομένα συναλλαγής και συγκρίνοντάς τα με την αποκρυπτογραφημένη υπογραφή (Ismail & Materwala, 2019). Οι μη έγκυρες συναλλαγές απορρίπτονται και οι έγκυρες συναλλαγές αναμεταδίδονται περαιτέρω.

Βήμα 3: Οι έγκυρες συναλλαγές μεταδίδονται στους κόμβους εξόρυξης του δικτύου για εξόρυξη, δηλαδή συσκευάζονται με χρονική σήμανση στο υποψήφιο μπλοκ (Bhushan et al., 2021). Με βάση τον μηχανισμό συναίνεσης επιλέγεται ένας κόμβος εξόρυξης, ο οποίος εκπέμπει το μπλοκ σε ολόκληρο το δίκτυο.

Βήμα 4: Οι κόμβοι επικύρωσης επαληθεύουν την εγκυρότητα του μπλοκ ελέγχοντας, τον κατακερματισμό του μπλοκ, τη χρονική σήμανση του μπλοκ, που πρέπει να είναι μεγαλύτερη από τη χρονική σήμανση του προηγούμενου μπλοκ, το ύψος και το μέγεθος του μπλοκ, την τιμή κατακερματισμού του προηγούμενου μπλοκ και την εγκυρότητα όλων των συναλλαγών στο μπλοκ (Ismail & Materwala, 2019). Εάν όλα τα παραπάνω

είναι αληθή, κάθε κόμβος προσαρτά το μπλοκ στο δικό του αντίγραφο του καθολικού, αλλιώς το μπλοκ απορρίπτεται.

Τα τέσσερα αυτά βήματα επαναλαμβάνονται από κάθε κόμβο του δικτύου για κάθε μία συναλλαγή, προκειμένου να διασφαλιστεί η αυθεντικότητα και η ακεραιότητα της δραστηριότητας του blockchain.

2.3. Βασικά Χαρακτηριστικά του Blockchain

Η τεχνολογία Blockchain έχει πολλά χαρακτηριστικά που την καθιστούν δημοφιλή όπως η αποκέντρωση, αυτονομία, υψηλή ασφάλεια, ανοχή σε σφάλματα, διαφάνεια, ιχνηλασιμότητα, μη αναστρεψιμότητα, ακεραιότητα, αξιοπιστία, ανωνυμία και ταχύτερη επεξεργασία συναλλαγών από τους τραπεζικούς οργανισμούς. Σε αυτή την ενότητα θα επικεντρωθούμε στα τέσσερα πιο σημαντικά χαρακτηριστικά, την αποκέντρωση, την διαφάνεια, την ανθεκτικότητα στις παραβιάσεις και την ανωνυμία, από τα οποία προκύπτουν και όλα τα υπόλοιπα.

Αποκέντρωση. Το σημαντικότερο ίσως χαρακτηριστικό της τεχνολογίας Blockchain είναι η αποκέντρωση. Αποκέντρωση είναι ο τρόπος λειτουργίας ενός δικτύου κατά τον οποίο δεν υπάρχει κεντρική αρχή για να ελέγχει ή να λαμβάνει αποφάσεις σχετικά με την εκτέλεση των συναλλαγών (Rajasekaran et al., 2022). Στην τρέχουσα ψηφιακή οικονομία οι περισσότερες διαδικτυακές συναλλαγές βασίζονται στα παραδοσιακά συστήματα διαχείρισης συναλλαγών, τα οποία εξαρτώνται από μια κεντρική αξιόπιστη αρχή, όπως για παράδειγμα μία τράπεζα, η οποία είναι υπεύθυνη για την επικύρωση των συναλλαγών και την ασφάλειά τους. Το σύστημα που διευθύνεται από αυτήν την συγκεκριμένη αξιόπιστη αρχή μπορεί να παραβιαστεί και οι συναλλαγές να παραποιηθούν. Στην τεχνολογία Blockchain οι πληροφορίες καταγράφονται στο κατανεμημένο καθολικό και οι συναλλαγές επικυρώνονται από τους κόμβους του δικτύου με την χρήση ενός συνόλου κανόνων, μαθηματικών και αλγορίθμων συναίνεσης, διασφαλίζοντας έτσι την συνέπεια και την ακεραιότητα των πληροφοριών αυτών. Το χαρακτηριστικό της αποκέντρωσης επομένως εξαλείφει την ανάγκη εξάρτησης από μία ισχυρή κεντρική αρχή και αντ' αυτού μεταφέρει τον έλεγχο στους μεμονωμένους χρήστες του δικτύου, κάνοντας το σύστημα δίκαιο και πολύ πιο ασφαλές (Bhutta et al., 2021).

Διαφάνεια. Ένα ακόμα βασικό χαρακτηριστικό της τεχνολογίας Blockchain είναι ότι παρέχει υψηλό επίπεδο διαφάνειας, το οποίο επιτυγχάνεται μέσω της αντιγραφής των συναλλαγών. Όπως αναφέρθηκε παραπάνω, ένα δίκτυο blockchain έχει πολλούς κόμβους μεταξύ των οποίων επιτυγχάνεται η επικύρωση των συναλλαγών χωρίς να απαιτείται μια κεντρική αρχή. Κάθε συναλλαγή αντιγράφεται σε οποιονδήποτε υπολογιστή συμμετέχει στο δίκτυο blockchain κι έτσι ο κάθε χρήστης μπορεί να δει τις λεπτομέρειες και το ιστορικό οποιασδήποτε συναλλαγής (Golosova & Romanovs, 2018). Έτσι, κάθε κόμβος έχει τα ίδια δικαιώματα πρόσβασης και τις ίδιες υποχρεώσεις σε εξουσιοδοτημένες πληροφορίες (Lu, 2019), κάνοντάς τες διαφανείς, ανιχνεύσιμες και συνεπείς.

Ανθεκτικότητα. Η τεχνολογία Blockchain χαρακτηρίζεται επίσης από ανθεκτικότητα στις παραβιάσεις (tamper-resistance), ή όπως αλλιώς μπορεί να αναφέρεται στην βιβλιογραφία, αμετάβλητο χαρακτήρα (immutability) ή επιμονή (persistency), με όλες αυτές τις έννοιες να έχουν την ίδια σημασία, δηλαδή ότι, όταν ξεκινήσει μια συναλλαγή και εισαχθούν δεδομένα στο κατανεμημένο καθολικό του blockchain, δεν μπορούν να αλλοιωθούν ή να παραβιαστούν (Bhutta et al., 2021). Με τον μηχανισμό της συναίνεσης, κάθε καταχώρηση της συναλλαγής επικυρώνεται από την πλειοψηφία, έτσι προσπάθειες παραποίησης ή διαγραφής των προηγούμενων συναλλαγών θα απαιτήσουν τη συναίνεση της πλειοψηφίας του συστήματος, κάτι το οποίο είναι εξαιρετικά απίθανο (Gao et al., 2018).

Ανωνυμία. Τελευταίο βασικό χαρακτηριστικό της τεχνολογίας Blockchain είναι αυτό της ανωνυμίας. Τα δεδομένα ανταλλάσσονται μεταξύ των κόμβων του δικτύου χρησιμοποιώντας τεχνικές ασύμμετρης κρυπτογραφίας. Κάθε χρήστης αλληλεπιδρά με το δίκτυο blockchain μέσω μιας διεύθυνσης που δημιουργείται από το δημόσιο κλειδί, από την οποία και αναγνωρίζεται, και υπογράφει ψηφιακά τις συναλλαγές με την χρήση του ιδιωτικού κλειδιού. Μέσω της ψηφιακής υπογραφής πραγματοποιείται ο έλεγχος της ταυτότητας του. Αυτή η διαδικασία δημιουργεί εμπιστοσύνη χωρίς να είναι απαραίτητο να αποκαλυφθεί η πραγματική ταυτότητα των συμμετεχόντων. Επίσης, κάθε χρήστης μπορεί να δημιουργήσει όσα ζεύγη ασύμμετρων κλειδιών, και κατά συνέπεια όσων διευθύνσεων, επιθυμεί, αποφεύγοντας την έκθεση της ταυτότητάς του (Zheng et al., 2018).

2.4. Συστατικά μέρη του Blockchain

Η τεχνολογία Blockchain αρχικά φαίνεται σύνθετη και πολύπλοκη, ωστόσο, εξετάζοντας κάθε συστατικό της στοιχείο ξεχωριστά μπορεί να απλοποιηθεί και να γίνει εύκολα κατανοητή. Σε αυτή την ενότητα αναλύονται τα συστατικά μέρη της τεχνολογίας Blockchain, δηλαδή οι κρυπτογραφικές συναρτήσεις κατακερματισμού, οι συναλλαγές, η ασύμμετρη κρυπτογραφία, οι διευθύνσεις και το καθολικό.

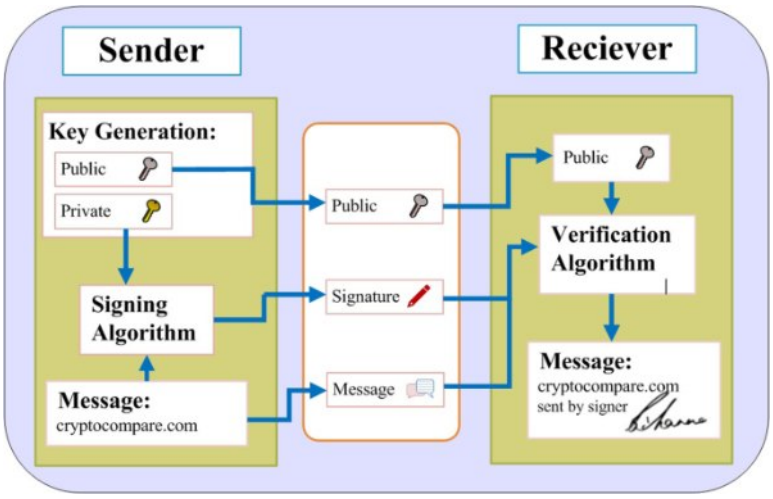
Κρυπτογραφικές συναρτήσεις κατακερματισμού. Ένα βασικό στοιχείο της τεχνολογίας Blockchain είναι η χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού για διάφορες λειτουργίες όπως η παραγωγή διευθύνσεων, η δημιουργία μοναδικών αναγνωριστικών και η διασφάλιση της κεφαλίδας και των δεδομένων του μπλοκ. Κατακερματισμός, ή μια συνάρτηση κατακερματισμού, είναι μια μαθηματική διαδικασία με την οποία οποιαδήποτε είσοδος (input), όπως για παράδειγμα ένα αρχείο, ένα κείμενο ή μια εικόνα, μετατρέπεται σε έξοδο (output) με σταθερό μήκος (Hill et al., 2018), που ονομάζεται σύνοψη (digest). Επιτρέπει στα άτομα να λαμβάνουν ανεξάρτητα δεδομένα εισόδου, να κατακερματίζουν αυτά τα δεδομένα και να εξάγουν το ίδιο αποτέλεσμα αποδεικνύοντας έτσι ότι δεν υπήρξε καμία αλλαγή στα δεδομένα, καθώς, ακόμη και η μικρότερη αλλαγή στην είσοδο, όπως για παράδειγμα αλλαγή ενός bit, θα έχει ως αποτέλεσμα μια εντελώς διαφορετική ανάλυση εξόδου (Yaga et al., 2018). Ο κατακερματισμός είναι μοναδικός για κάθε μπλοκ και καθορίζει την ταυτότητά του, σαν ένα δακτυλικό αποτύπωμα (Bamakan et al., 2020). Ουσιαστικά, η χρήση του επιτρέπει τον έλεγχο της ακεραιότητας των πληροφοριών. Υπάρχουν πολλές κρυπτογραφικές συναρτήσεις κατακερματισμού που χρησιμοποιούνται στην τεχνολογία Blockchain, όπως ο SHA-256 και ο MD5 (Johar et al., 2021; Hill et al., 2018).

Συναλλαγές. Μια συναλλαγή αντιπροσωπεύει μια αλληλεπίδραση μεταξύ δύο μερών. Στις παραδοσιακές εφαρμογές blockchain, όπως το κρυπτονόμισμα Bitcoin, μια συναλλαγή αντιπροσωπεύει μια ανταλλαγή χρημάτων μεταξύ δύο οντοτήτων ή χρηστών του δικτύου (Gupta & Sadoghi, 2021). Ανάλογα με την κάθε εφαρμογή blockchain, τα δεδομένα που περιλαμβάνει μια συναλλαγή μπορεί να διαφέρουν, ωστόσο η διαδικασία εκτέλεσης της συναλλαγής είναι σε μεγάλο βαθμό η ίδια, όπως έχει αναλυθεί λεπτομερώς στην υποενότητα 2.2.1. Η τρέχουσα κατάσταση του blockchain αντιπροσωπεύεται από αυτές τις συναλλαγές, οι οποίες δημιουργούνται συνεχώς από

τους κόμβους και στη συνέχεια συγκεντρώνονται σε μπλοκ (Puthal et al., 2018). Η συνεχής παροχή νέων μπλοκ, ακόμη και με μηδενικές συναλλαγές, είναι κρίσιμη για τη διατήρηση της ασφάλειας του δικτύου blockchain καθώς έτσι αποτρέπονται οι κακόβουλοι χρήστες από το να "καλύψουν τη διαφορά" και να κατασκευάσουν μια μακρύτερη, αλλαγμένη αλυσίδα μπλοκ (Yaga et al., 2018).

Ασύμμετρη Κρυπτογραφία. Στην κρυπτογραφία ασύμμετρου κλειδιού, ή όπως αλλιώς είναι γνωστή κρυπτογραφία δημόσιου κλειδιού, υπάρχουν δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό, τα οποία συνδέονται μαθηματικά μεταξύ τους. Η τεχνολογία Blockchain χρησιμοποιεί τις δυνατότητες της ασύμμετρης κρυπτογραφίας σε διάφορες λειτουργίες. Εν συντομία, τα ιδιωτικά κλειδιά χρησιμοποιούνται για την ψηφιακή υπογραφή των συναλλαγών, τα δημόσια κλειδιά χρησιμοποιούνται για την παραγωγή διευθύνσεων και την επαλήθευση των υπογραφών που δημιουργούνται με ιδιωτικά κλειδιά, όπως επίσης παρέχεται η δυνατότητα επαλήθευσης ότι ο χρήστης που μεταφέρει αξία σε έναν άλλο χρήστη έχει στην κατοχή του το ιδιωτικό κλειδί που μπορεί να υπογράψει τη συναλλαγή (Yaga et al., 2018).

Για να πραγματοποιήσουν οποιαδήποτε συναλλαγή, οι χρήστες πρέπει να διαθέτουν ένα ψηφιακό πορτοφόλι, που χρησιμοποιείται για την αποθήκευση δημόσιων και ιδιωτικών κλειδιών καθώς και των σχετικών διευθύνσεων (Hill et al., 2018). Κάθε συναλλαγή εκκινεί τον αλγόριθμο δημιουργίας κλειδιών που δημιουργεί ένα νέο δημόσιο και ιδιωτικό κλειδί για τον αποστολέα (Van der Auwera et al., 2020). Το δημόσιο κλειδί δημοσιοποιείται, χωρίς να μειώνεται η ασφάλεια της διαδικασίας, και χρησιμεύει ως η διεύθυνση που είναι γνωστή σε όλους, ενώ το ιδιωτικό κλειδί χρησιμοποιείται για την ψηφιακή υπογραφή συναλλαγών και διατηρείται μυστικό από τον χρήστη (Puthal et al., 2018). Η κρυπτογράφηση αυτή επιτρέπει μια σχέση εμπιστοσύνης μεταξύ χρηστών που δεν γνωρίζουν ή δεν εμπιστεύονται ο ένας τον άλλο, παρέχοντας έναν μηχανισμό για την επαλήθευση της ακεραιότητας και της αυθεντικότητας των συναλλαγών, επιτρέποντας ταυτόχρονα τις συναλλαγές να παραμένουν δημόσιες (Yaga et al., 2018).



Εικόνα 2.2. Διάγραμμα ψηφιακής υπογραφής Bitcoin (Fang et al., 2020)

Διευθύνσεις. Οι διευθύνσεις σε ένα δίκτυο blockchain είναι σύντομες, αλφαριθμητικές συμβολοσειρές χαρακτήρων που λειτουργούν ως μοναδικά αναγνωριστικά και χρησιμοποιούνται ως τερματικά σημεία "προς" και "από" σε μια συναλλαγή (Yaga et al., 2018). Για παράδειγμα, στην περίπτωση του κρυπτονομίσματος Bitcoin, οι διευθύνσεις είναι αναγνωριστικά που χρησιμοποιούνται για την αποστολή και την λήψη Bitcoin (Hill et al., 2018). Υπάρχουν διάφορες μέθοδοι για την εξαγωγή διευθύνσεων. Μια μέθοδος είναι η δημιουργία ενός δημόσιου κλειδιού, η εφαρμογή μιας κρυπτογραφικής συνάρτησης κατακερματισμού σε αυτό και η μετατροπή του κατακερματισμού σε κείμενο: δημόσιο κλειδί → κρυπτογραφική συνάρτηση κατακερματισμού → διεύθυνση (Yaga et al., 2018). Η χρήση των διευθύνσεων συμβάλει στην διατήρηση της ανωνυμίας των χρηστών του δικτύου blockchain καθώς μπορούν να δημιουργήσουν όσα ζεύγη ασύμμετρων κλειδιών, και κατά συνέπεια όσων διευθύνσεων, επιθυμούν, εξασφαλίζοντας έτσι ότι η ταυτότητά τους παραμένει κρυφή.

Καθολικό. Ένα καθολικό είναι μια συλλογή συναλλαγών. Καθ' όλη την διάρκεια της ιστορίας, χειρόγραφες βάσεις δεδομένων έχουν χρησιμοποιηθεί για την παρακολούθηση της ανταλλαγής αγαθών και υπηρεσιών, στην σύγχρονη όμως εποχή, ένα καθολικό αποθηκεύεται ψηφιακά, συχνά σε μεγάλες βάσεις δεδομένων οι οποίες ανήκουν και διαχειρίζονται από ένα κεντρικό αξιόπιστο τρίτο μέρος για λογαριασμό μιας κοινότητας χρηστών (Yaga et al., 2018). Στην τεχνολογία Blockchain η διαφορά έγκειται στο ότι η ιδιοκτησία και η φυσική αρχιτεκτονική του δικτύου είναι κατανεμημένες. Μια

κατανεμημένη βάση δεδομένων διανέμει τα δεδομένα σε πολλούς κόμβους αποθήκευσης που συνδέονται μέσω του δικτύου για μεγαλύτερη χωρητικότητα αποθήκευσης και υψηλότερη ταυτόχρονη πρόσβαση (Lu, 2019). Στην τεχνολογία Blockchain το καθολικό είναι μια ακολουθία από μπλοκ, όπου κάθε μπλοκ είναι μια οργανωμένη ακολουθία συναλλαγών ενός συμφωνηθέντος μεγέθους, το οποίο διαφέρει από σύστημα σε σύστημα (Waldo, 2019). Σε αντίθεση με τις παραδοσιακές βάσεις δεδομένων, που παρέχουν λειτουργίες για την προσθήκη, διαγραφή, αλλαγή και αναζήτηση δεδομένων, στο καθολικό του blockchain υπάρχουν μόνο δύο λειτουργίες, αυτή της προσθήκης και αυτή της αναζήτησης (Lu, 2019). Αυτό καθιστά το καθολικό απαραβίαστο, καθώς, κανένας χρήστης δεν μπορεί να προσθέσει, να διαγράψει ή να τροποποιήσει τις καταχωρίσεις στο καθολικό μόλις καταγραφούν (Herlihy, 2019).

2.5. Μοντέλα Συναίνεσης

Όπως έχει αναφερθεί παραπάνω, ένα από τα βασικότερα χαρακτηριστικά της τεχνολογίας Blockchain είναι η αποκέντρωση, δηλαδή η λειτουργία του δικτύου χωρίς να υπάρχει ένα αξιόπιστο τρίτο μέρος για τον έλεγχο και την επικύρωση των συναλλαγών. Όλοι οι κόμβοι θεωρούνται ίσοι και είναι υπεύθυνοι για να καταλήξουν σε συμφωνία σχετικά με το αν μια συναλλαγή είναι έγκυρη και πρέπει να προστεθεί στο καθολικό ή όχι. Αυτή η συμφωνία επιτυγχάνεται με την ύπαρξη του μηχανισμού συναίνεσης, που θεωρείται ο πυρήνας κάθε blockchain. Το πρωτόκολλο συναίνεσης είναι ένα σύνολο κανόνων και κανονισμών που ακολουθούνται κατά τις συναλλαγές στην τεχνολογία blockchain, δημιουργώντας ένα επίπεδο εμπιστοσύνης όσον αφορά την ενημέρωση ή τη μεταφορά των δεδομένων μεταξύ των τελικών χρηστών (Rajasekaran et. al., 2022). Μετά την ολοκλήρωση της διαδικασία συναίνεσης, αφού ένα μπλοκ έχει επαληθευτεί και προσαρτηθεί στο καθολικό, οποιαδήποτε τροποποίηση ή η διαγραφή είναι ανέφικτη.

Συμμετέχοντας στο δίκτυο blockchain οι χρήστες συμφωνούν με την αρχική κατάσταση του συστήματος, όπως έχει καταγραφεί στο genesis μπλοκ, και με το μοντέλο συναίνεσης που χρησιμοποιείται για την προσθήκη των μπλοκ στο σύστημα. Ανάλογα με το είδος του δικτύου blockchain υπάρχουν διαφορές στον τρόπο που επιτυγχάνεται η συναίνεση μεταξύ των συμμετεχόντων. Για παράδειγμα, στα permissionless δίκτυα blockchain όλοι οι κόμβοι εξόρυξης καθορίζουν τη συναίνεση, ενώ, στα permissioned

δίκτυα blockchain η συναίνεση καθορίζεται μόνο από ένα επιλεγμένο σύνολο κόμβων (Bamakan et al., 2020). Σε αυτή την ενότητα θα πραγματοποιηθεί μια ανάλυση των πιο σημαντικών αλγορίθμων συναίνεσης που χρησιμοποιούνται ευρέως στα δίκτυα blockchain καθώς επίσης θα αναφερθούν τα πλεονεκτήματα και τα μειονεκτήματα του καθενός.

Proof of Work (PoW). Ο αλγόριθμος αυτός εμφανίστηκε το 1999 με σκοπό την πρόληψη επιθέσεων άρνησης υπηρεσίας (DoS), επιθέσεις που αποτρέπουν τους νόμιμους χρήστες από τη χρήση μιας υπηρεσίας (Yadav & Singh, 2020). Αποτελεί την πιο γνωστή μέθοδο συναίνεσης που χρησιμοποιείται στο δίκτυο του κρυπτονομίσματος Bitcoin. Στο μοντέλο PoW ο χρήστης που θα δημοσιεύει το επόμενο μπλοκ είναι αυτός που θα λύσει πρώτος ένα περίπλοκο υπολογιστικό πρόβλημα. Το υπολογιστικό πρόβλημα είναι σχεδιασμένο με τέτοιο τρόπο ώστε η επίλυσή του να είναι δύσκολη, αλλά ο έλεγχος της έγκυρης λύσης να είναι εύκολος, επιτρέποντας σε όλους τους πλήρεις κόμβους του δικτύου να επικυρώνουν εύκολα τυχόν προτεινόμενα μπλοκ (Yaga et al., 2018). Συνήθως το υπολογιστικό πρόβλημα είναι ο υπολογισμός μιας τιμής κατακερματισμού της συνεχώς μεταβαλλόμενης κεφαλίδας μπλοκ, που πρέπει να είναι ίση ή μικρότερη από μια ορισμένη δεδομένη αξία (Zheng et al., 2018). Όλοι οι κόμβοι εξόρυξης πρέπει να υπολογίσουν την τιμή κατακερματισμού κάνοντας συνεχώς αλλαγές στην κεφαλίδα του μπλοκ, για παράδειγμα στο πεδίο nonce, μέχρι να επιτευχθεί ο στόχος. Μόλις ένας κόμβος βρει την τιμή nonce που ικανοποιεί την προκαθορισμένη απαίτηση την μεταδίδει στο δίκτυο, οι υπόλοιποι κόμβοι επαληθεύουν την ορθότητά της και προσθέτουν το αντίστοιχο μπλοκ στο αντίγραφο του blockchain. Ο κόμβος που δημοσίευσε την σωστή τιμή κατακερματισμού κερδίζει την ανταμοιβή. Σε κάποιες περιπτώσεις, περισσότεροι του ενός κόμβοι ενδέχεται να δημιουργήσουν ταυτόχρονα έγκυρα μπλοκ. Αυτή η κατάσταση δημιουργεί ένα fork, δηλαδή δύο διακλαδώσεις της αλυσίδας, και επιλύεται επιλέγοντας την μακρύτερη διακλάδωση ως έγκυρη, καθώς αυτή αντιπροσωπεύει την μέγιστη εργασία που έχει γίνει από έναν κόμβο (Syed et al., 2019).

Ο αλγόριθμος συναίνεσης PoW είναι κατάλληλος για permissionless δίκτυα, όπου το μέγεθος του δικτύου μπορεί να είναι πολύ μεγάλο, καθώς παρέχει υψηλά επίπεδα ασφάλειας από κυβερνο-επιθέσεις, ασφάλεια στην διαδικασία συναίνεσης και αποδεκτά επίπεδα επεκτασιμότητας (Bamakan et al., 2020). Ωστόσο, υπάρχουν αρκετά

μειονεκτήματα. Το κυριότερο είναι η μεγάλη ενεργειακή κατανάλωση κατά την διαδικασία εξόρυξης και επικύρωσης των μπλοκ. Άλλα μειονεκτήματα είναι η ευπάθεια σε επιθέσεις πλειοψηφίας (51% attack), σε περίπτωση που ένα υποσύνολο κόμβων εξόρυξης αναλάβει τον έλεγχο της συνολικής επεξεργαστικής ισχύος του δικτύου (Bhushan et al., 2021), και το χαμηλό ποσοστό συναλλαγών, διότι απαιτείται πολύς χρόνος για την δημιουργία ενός μπλοκ.

Proof of Stake (PoS). Ο αλγόριθμος PoS εφαρμόστηκε για πρώτη φορά το 2012 από το κρυπτονόμισμα PeerCoin και χρησιμοποιεί τον "πλούτο" των κόμβων εξόρυξης, δηλαδή το μερίδιο του κρυπτονομίσματος που κατέχουν, ως παράγοντα για την δημοσίευση νέων μπλοκ, αντί της υπολογιστικής ισχύος που απαιτεί ο αλγόριθμος PoW (Johar et al., 2021). Το μερίδιο που κατέχει ένας χρήστης δεν μπορεί να δαπανηθεί, έτσι ουσιαστικά το συγκεκριμένο μοντέλο συναίνεσης βασίζεται στην ιδέα ότι όσο περισσότερο έχει επενδύσει ο χρήστης στο σύστημα, τόσο πιο πιθανό είναι να θέλει το σύστημα να πετύχει και τόσο λιγότερο πιθανό να θέλει να το ανατρέψει (Yaga et al., 2018). Η διαδικασία επιλογής του κόμβου που θα επικυρώσει το επόμενο νέο μπλοκ είναι τυχαία και η πιθανότητα ενός κόμβου να επιλεχθεί είναι ανάλογη του μεριδίου που κατέχει σε σχέση με το συνολικό ποσό του κρυπτονομίσματος που υπάρχει στο δίκτυο, δηλαδή, όσο μεγαλύτερη είναι η "εγγύηση" (stake) του χρήστη τόσο μεγαλύτερες είναι οι πιθανότητες να δημιουργήσει το επόμενο μπλοκ. Οι κόμβοι εξόρυξης λαμβάνουν ως ανταμοιβή τα τέλη της συναλλαγής, ενώ στην περίπτωση που προσπαθήσουν να επικυρώσουν ένα μη έγκυρο μπλοκ χάνουν ένα μέρος της "εγγύησης", επομένως, το ποσό της "εγγύησης" θα πρέπει να είναι υψηλότερο από τη συνολική χρέωση συναλλαγής, για να αποφευχθεί η προσθήκη οποιουδήποτε δόλιου μπλοκ (Yadav & Singh, 2020).

Αυτός ο αλγόριθμος δημιουργήθηκε για να ξεπεράσει τα προβλήματα που προκύπτουν από τον αλγόριθμο συναίνεσης PoW, όπως η απαίτηση υψηλής υπολογιστικής ισχύος, υψηλή κατανάλωση ηλεκτρικής ενέργειας και ο πολύς χρόνος που χρειάζεται για την επικύρωση μιας συναλλαγής. Ωστόσο, υπάρχουν κάποια μειονεκτήματα, καθώς το δίκτυο υποφέρει από κάποιου είδους συγκέντρωση και χαμηλότερο κόστος κακής συμπεριφοράς (Bamakan et al., 2020).

Proof of Authority (PoA). Το πρωτόκολλο συναίνεσης αυτό, γνωστό και ως Proof of Identity, προτάθηκε το 2015 και βασίζεται στο ότι η εξουσία εκχωρείται σε ένα σύνολο προκαθορισμένων κόμβων, δίνοντάς τους τη δυνατότητα να δημοσιεύουν νέα μπλοκ (Gao et al., 2018). Οι κόμβοι δημοσίευσης, ή αλλιώς επικυρωτές, είναι επίσημα εγκεκριμένοι λογαριασμοί των οποίων η ταυτότητα επαληθεύεται συμβολαιογραφικά από ένα εξουσιοδοτημένο σύστημα και διατηρείται δημόσια στην αλυσίδα ώστε να μπορεί να πραγματοποιείται έλεγχος (Ismail & Materwala, 2019). Αντίστοιχα με τον αλγόριθμο PoS, όπου οι χρήστες διακυβεύουν το μερίδιο του κρυπτονομίσματος που κατέχουν, στον αλγόριθμο PoA οι συμμετέχοντες διακυβεύουν την φήμη τους, το οποίο τους αποτρέπει από το να ενεργούν με κακόβουλο τρόπο. Επιπλέον, βασίζεται σε ένα σχήμα Round-Robin, όπου οι κόμβοι εναλλάσσονται στη δημιουργία μπλοκ και ορίζεται ένα χρονικό παράθυρο μέσα στο οποίο κάθε κόμβος μπορεί να προτείνει ένα μόνο μπλοκ (Bhushan et al., 2021).

Ο συγκεκριμένος μηχανισμός συναίνεσης έχει δύο κύρια πλεονεκτήματα, την ενεργειακή αποδοτικότητα και τη γρήγορη επικύρωση των συναλλαγών (Syed et al., 2019). Ωστόσο, το γεγονός ότι η δημοσίευση των μπλοκ πραγματοποιείται από μία σταθερή ομάδα επαληθευμένων κόμβων οδηγεί το δίκτυο προς την συγκέντρωση, γι' αυτό και ο αλγόριθμος PoA θεωρείται πιο κατάλληλος για permissioned δίκτυα blockchain. Ένα ακόμα μειονέκτημα είναι ότι δεν έχει δοκιμαστεί ακόμη για την απόδοση και την προστασία του ενάντια σε απειλές που αφορούν την ασφάλεια του δικτύου (Ismail & Materwala, 2019).

Practical Byzantine Fault Tolerance (PBFT). Ο συγκεκριμένος αλγόριθμος προτάθηκε το 1999 από τους Castro και Liskov (1999) ως λύση στο πρόβλημα των Βυζαντινών Στρατηγών. Το πρόβλημα αυτό αφορά τη διεξαγωγή μιας επιτυχημένης επίθεσης σε αντίπαλη πόλη από τον βυζαντινό στρατό, κατά την οποία για να κερδίσει ο βυζαντινός στρατός πρέπει όλοι οι πιστοί στρατηγοί να εργαστούν στο ίδιο σχέδιο και να επιτεθούν ταυτόχρονα, επιμένοντας στο αποφασισμένο σχέδιο ακόμα κι αν ένας μικρός αριθμός προδοτών προσπαθεί να το ανατρέψει (Puthal et al., 2018). Με την ίδια λογική, ο αλγόριθμος PBFT χρησιμοποιείται σε ένα δίκτυο blockchain για να επιτευχθεί συναίνεση μεταξύ των συμμετεχόντων ακόμα και με την παρουσία κακόβουλων χρηστών. Μπορεί να αντικρούσει την συμπεριφορά των κακόβουλων κόμβων και να

συνεχίσει μια κανονική λειτουργία, με την υπόθεση ότι δεν ξεπερνούν το ένα τρίτο των συνολικών κόμβων του δικτύου. Για παράδειγμα, εάν υπάρχει στο σύστημα ένας κακόβουλος κόμβος, τουλάχιστον τέσσερις κόμβοι πρέπει να συμφωνούν για να επιτευχθεί συναίνεση. Επίσης, η φύση του μηχανισμού είναι ντετερμινιστική, δηλαδή μόλις συμπεριληφθεί ένα μπλοκ στην αλυσίδα μπλοκ η απόφαση είναι οριστική (Gao et al., 2018).

Στο πρωτόκολλο PBFT, μια ομάδα κόμβων επιλέγεται από μια κεντρική αρχή με έναν κόμβο ως αρχηγό και τους άλλους ως εφεδρικούς, όπου όλοι οι κόμβοι του συστήματος επικοινωνούν μεταξύ τους με στόχο να φτάσουν σε συμφωνία υποθέτοντας ότι όλοι οι ειλικρινείς κόμβοι έχουν το ίδιο ακριβώς αντίγραφο του καθολικού (Ismail & Materwala, 2019). Η συναίνεση επιτυγχάνεται σε γύρους, με ένα νέο μπλοκ να καθορίζεται σε κάθε έναν γύρο. Η διαδικασία χωρίζεται σε τρεις φάσεις. Στην πρώτη φάση ο κόμβος αρχηγός, ο οποίος είναι διαφορετικός σε κάθε γύρο και εκλέγεται με ψηφοφορία από τους άλλους κόμβους, στέλνει στους εφεδρικούς κόμβους την προβλεπόμενη τιμή που πρέπει να δεσμευτεί στο blockchain (Gao et al., 2018). Στην δεύτερη φάση, οι εφεδρικοί κόμβοι επαληθεύουν την τιμή και την εκπέμπουν στους υπόλοιπους κόμβους. Τέλος, στην τρίτη φάση, εάν περισσότερα από τα δύο τρίτα των κόμβων συμφωνούν για την τιμή που θα δεσμευτεί, το μπλοκ προστίθεται στο καθολικό. Εάν δεν μπορεί να επιτευχθεί συναίνεση οι συναλλαγές απορρίπτονται. Το πιο γνωστό δίκτυο blockchain που χρησιμοποιεί το μοντέλο PBFT είναι το Hyperledger.

Ο αλγόριθμος αυτός χαρακτηρίζεται από ενεργειακή απόδοση εξαλείφοντας διάφορα ζητήματα που προκύπτουν από άλλους αλγόριθμους, όπως αναφέρθηκαν παραπάνω. Ωστόσο, αντιμετωπίζει πρόβλημα στην επεκτασιμότητα, διότι απαιτεί αρκετούς γύρους επικοινωνίας μέχρι να επιτευχθεί συναίνεση. Επίσης, ένα ακόμα σημαντικό μειονέκτημα είναι ότι οι συμμετέχοντες πρέπει να είναι γνωστοί, δεν μπορεί οποιοσδήποτε να εγγραφεί στο δίκτυο (Hill et al., 2018), γεγονός που κάνει το σύστημα λιγότερο αποκεντρωμένο.

Με το το πέρασμα των χρόνων πολλοί αλγόριθμοι συναίνεσης έχουν κάνει την εμφάνισή τους και κυρίως αποτελούν παραλλαγές ή συνδυασμούς των αλγορίθμων που

αναλύθηκαν παραπάνω. Σε αυτό το σημείο θα γίνει μια πολύ σύντομη περιγραφή ορισμένων από αυτούς.

Delegated Proof of Stake (DPoS). Αποτελεί βελτίωση του αλγορίθμου PoS, όπου οι συμμετέχοντες εκλέγουν τους κόμβους εξόρυξης, που σε αυτή την περίπτωση ονομάζονται αντιπρόσωποι (delegates), οι οποίοι έχουν την δυνατότητα δημιουργίας και επικύρωσης των μπλοκ.

Proof of Elapsed Time (PoET). Είναι ένας αλγόριθμος blockchain που δημιουργήθηκε από την Intel χρησιμοποιώντας το Trusted Execution Environment (TEE) για να υπάρχει τυχαιότητα και ασφάλεια κατά τη διαδικασία ψηφοφορίας, χρησιμοποιώντας εγγυημένο χρόνο αναμονής (Hill et al., 2018).

Proof of Space (PoSpace) ή **Proof of Capacity** (PoC). Σε αυτό το μοντέλο συναίνεσης αντί να χρησιμοποιείται η υπολογιστική ισχύς του κόμβου εξόρυξης χρησιμοποιείται η χωρητικότητα αποθήκευσης των συσκευών για την αποθήκευση των πιθανών λύσεων στην διαδικασία εξόρυξης κρυπτονομισμάτων, με τον περισσότερο αποθηκευτικό χώρο να έχει μεγαλύτερες πιθανότητες να κερδίσει την ανταμοιβή εξόρυξης (Johar et al., 2021).

Proof of Activity. Αποτελεί ένα συνδυασμό των αλγορίθμων PoW και PoS, όπου η διαδικασία της εξόρυξης πραγματοποιείται ακριβώς όπως στα συστήματα PoW και στην συνέχεια η επικύρωση των μπλοκ πραγματοποιείται από μια τυχαία επιλεγμένη ομάδα κόμβων όπως στα συστήματα PoS.

Proof of Importance (PoI). Αυτός ο αλγόριθμος χρησιμοποιείται από το κρυπτονόμισμα New Economic Movement (NEM) και η βασική ιδέα είναι ότι δίνεται μια βαθμολογία σπουδαιότητας σε κάθε λογαριασμό του δικτύου blockchain, βάσει της οποίας επηρεάζεται το πώς μπορεί κάθε κόμβος να προσθέσει συναλλαγές στο blockchain (Hill et al., 2018).

Proof of Existence (PoE). Αποτελεί μοντέλο συναίνεσης για την επαλήθευση ψηφιακών εγγράφων που αποθηκεύονται με ψηφιακή υπογραφή και χρονική σήμανση σε ένα δίκτυο.

Proof of Stake Velocity. Χρησιμοποιείται προκειμένου να επικυρωθούν οι συναλλαγές και να ασφαλιστεί το P2P δίκτυο του κρυπτονομίσματος Reddcoin, όπου σύμφωνα με τον αλγόριθμο αυτό, οι ανταμοιβές διανέμονται με βάση το πόσα νομίσματα έχει στην κατοχή του ένας κόμβος και πόσο συχνά διεκπεραιώνονται συναλλαγές στον κόμβο αυτό (Johar et al., 2021).

Proof of Burn (PoB). Αλγόριθμος συναίνεσης όπου οι επικυρωτές δημιουργούν ένα μπλοκ και ανταμείβονται αφού "κάψουν" τα δικά τους ψηφιακά νομίσματα, δηλαδή αφού τα στείλουν σε μια διεύθυνση από την οποία δεν είναι δυνατή η ανάκτησή τους (Syed et al., 2019).

2.6. Ζητήματα λειτουργικότητας

Όπως όλες οι τεχνολογίες έτσι και η τεχνολογία Blockchain έχει ορισμένους περιορισμούς που αποτελούν πρόκληση όσον αφορά την υιοθέτηση της, με τα κυριότερα ζητήματα να αναφέρονται παρακάτω.

Επεκτασιμότητα. Η επεκτασιμότητα ορίζεται ως η ικανότητα ενός συστήματος, δικτύου, ή διαδικασίας να διαχειρίζεται τον αυξανόμενο φόρτο εργασίας ή να επεκτείνει τις δυνατότητές του για την αντιμετώπιση της ανάπτυξης αυτής (Zou et al., 2020). Τα δίκτυα blockchain, όπως είναι σήμερα, πάσχουν από προβλήματα επεκτασιμότητας, τα οποία δημιουργούν ανησυχία σχετικά με την δυνατότητα κλιμάκωσης των δικτύων στα απαιτούμενα επίπεδα για γενική χρήση. Αυτά τα ζητήματα προκύπτουν από περιορισμούς που οδηγούν σε χαμηλή απόδοση, από υψηλή καθυστέρηση συναλλαγών και από αυξανόμενες ανάγκες σε πόρους (Yang et al., 2019). Όλοι οι αλγόριθμοι συναίνεσης απαιτούν από τους πλήρεις κόμβους να διαθέτουν ένα αντίγραφο του καθολικού, δηλαδή όλων των συναλλαγών που πραγματοποιήθηκαν στο δίκτυο, απαιτώντας έτσι πολύ χώρο αποθήκευσης. Οι απαιτήσεις για αποθηκευτικό χώρο συνεχίζουν να αυξάνονται καθώς αυξάνεται ο αριθμός των συναλλαγών. Επιπρόσθετα, ο περιορισμός του μεγέθους του μπλοκ 1MB συμβάλλει σημαντικά στο ζήτημα της

επεκτασιμότητας, καθώς επιβεβαιώνονται μόνο 6-7 συναλλαγές σε ένα δευτερόλεπτο (Puthal et al., 2018) και δεν μπορούν να συγκριθούν με συστήματα όπως το δίκτυο επεξεργασίας πιστωτικών καρτών της VISA, που διαχειρίζεται συνεχώς χιλιάδες συναλλαγές ανά δευτερόλεπτο (Casino et al., 2019). Μια λύση στο ζήτημα της επεκτασιμότητας είναι να αυξηθεί το όριο του μεγέθους του μπλοκ, ωστόσο, κάτι τέτοιο θα αυξήσει ακόμα περισσότερο την κατανάλωσης ενέργειας και θα δημιουργήσει προβλήματα στην ασφάλεια του δικτύου.

Κατανάλωση ενέργειας. Η κυριότερη πρόκληση όσον αφορά την υιοθέτηση της τεχνολογίας Blockchain είναι η υψηλή κατανάλωση ενέργειας. Η υψηλή αυτή κατανάλωση οφείλεται στην εκτέλεση του μηχανισμού συναίνεσης που βασίζεται στην χρήση έντονης υπολογιστικής ισχύος, κυρίως στον αλγόριθμο PoW για τον υπολογισμό του κατάλληλου κατακερματισμού ενός μπλοκ. Οι διάφορες εκτιμήσεις για το πόση ηλεκτρική ενέργεια καταναλώνεται από ένα δίκτυο blockchain δηλώνουν ότι ισοδυναμεί με την ετήσια κατανάλωση ενέργειας ενός ολόκληρου έθνους, με αναφορά του αμερικανικού περιοδικού Grist να δηλώνει πως το δίκτυο του κρυπτονομίσματος Bitcoin μέχρι το 2020 θα φτάσει να καταναλώνει την ίδια ποσότητα ενέργειας που χρησιμοποιεί ολόκληρος ο κόσμος (Ismail & Materwala, 2019). Μερικοί μάλιστα έχουν ισχυριστεί ότι το Bitcoin και τα σχετικά κρυπτονομίσματα είναι μηχανισμοί για τη μετατροπή της ηλεκτρικής ενέργειας σε νόμισμα (Waldo, 2019). Ωστόσο, είναι σημαντικό να σημειωθεί ότι η υψηλή κατανάλωση ενέργειας δεν είναι αποτέλεσμα αναποτελεσματικών αλγορίθμων ή απαρχαιωμένου υλικού, αντίθετως, τα δίκτυα blockchain είναι ενεργοβόρα εκ του σχεδιασμού τους για να προστατεύονται από διάφορες επιθέσεις (Sedlmeir et al., 2020). Μια λύση στο πρόβλημα αυτό είναι η χρήση εναλλακτικών μηχανισμών συναίνεσης που είναι ενεργειακά πιο αποδοτικοί, όπως για παράδειγμα ο PoS και ο PoA, οι οποίοι δεν απαιτούν υπολογιστική πολυπλοκότητα, ωστόσο έχουν ο καθένας τα μειονεκτήματά τους, όπως έχουν αναφερθεί παραπάνω.

Καθυστέρηση. Η καθυστέρηση στις συναλλαγές είναι μια ακόμα σοβαρή πρόκληση που περιορίζει την υιοθέτηση της τεχνολογίας Blockchain και οφείλεται κυρίως στις διαδικασίες δημιουργίας και επικύρωσης των μπλοκ. Για παράδειγμα, στο δίκτυο του κρυπτονομίσματος Bitcoin ο μέσος χρόνος εξόρυξης ενός μπλοκ από τους κόμβους είναι 10 λεπτά και ο μέσος χρόνος επικύρωσης της συναλλαγή είναι περίπου μία ώρα (Cai et

al., 2018). Επιπλέον, συνιστάται η αναμονή για τουλάχιστον μια ακολουθία από έξι μπλοκ ώστε να είναι σίγουρο ότι οι συναλλαγές πράγματι έχουν τεθεί σε ισχύ, γεγονός που εισάγει ακόμα μεγαλύτερη καθυστέρηση στην επιβεβαίωση μιας συναλλαγής. Ουσιαστικά, αυτό είναι το κόστος δημιουργίας εμπιστοσύνης σε ένα μη αξιόπιστο δίκτυο.

2.7. Ζητήματα ασφάλειας

Όπως γίνεται αντιληπτό απ' όλα τα παραπάνω, η τεχνολογία Blockchain έχει προσελκύσει σημαντική προσοχή τόσο από ερευνητές όσο και από επιχειρηματικούς οργανισμούς, καθώς τα χαρακτηριστικά της προσφέρουν πολλά οφέλη και εγγυώνται πιο αξιόπιστες και πρόσφορες υπηρεσίες. Ωστόσο, προκειμένου να γίνει αποτελεσματική χρήση της τεχνολογίας, είναι σημαντικό να ληφθούν υπόψη οι προκλήσεις που σχετίζονται με την ασφάλεια και την ιδιωτικότητα.

Η ασφάλεια στο blockchain μπορεί να οριστεί ως η προστασία των πληροφοριών συναλλαγής και των δεδομένων σε ένα μπλοκ έναντι εσωτερικών και περιφερειακών, κακόβουλων και ακούσιων απειλών. Οι περισσότερες επιθέσεις στο blockchain προέρχονται από ανέντιμους κόμβους που στοχεύουν στον έλεγχο της δημιουργίας μπλοκ στην αλυσίδα, ωστόσο δεν αποκλείονται και οι απειλές που οφείλονται σε εξωτερικούς παράγοντες, οδηγώντας σε πολλά προβλήματα, συμπεριλαμβανομένης της απώλειας κεφαλαίων. Στην παρούσα ενότητα πραγματοποιείται μια καταγραφή των κυριότερων επιθέσεων και των επιπτώσεων αυτών στην ασφάλεια του δίκτυο blockchain, οι οποίες γενικά μπορούν να ταξινομηθούν σε τέσσερις κατηγορίες. Στην πρώτη κατηγορία ανήκουν οι επιθέσεις διπλής δαπάνης, στην δεύτερη κατηγορία ανήκουν οι επιθέσεις που αφορούν το πρωτόκολλο επικοινωνίας, στην τρίτη κατηγορία ανήκουν οι επιθέσεις εξόρυξης, και τέλος, στην τέταρτη κατηγορία ανήκουν οι επιθέσεις που απειλούν την ασφάλεια των πορτοφολιών των κρυπτονομισμάτων.

2.7.1. Επιθέσεις διπλής δαπάνης

Το πρόβλημα της διπλής δαπάνης αναφέρεται στο ότι ένας καταναλωτής μπορεί να δαπανήσει το ίδιο κρυπτονόμισμα περισσότερες από μία φορές για πολλαπλές συναλλαγές. Χάρη στη χρήση του κατακερματισμού στο blockchain, το κάθε νόμισμα στο καθολικό μπορεί να εντοπιστεί στην πρώτη εγγραφή όταν δημιουργήθηκε,

επομένως, η πλαστογραφία σε ανύπαρκτο νόμισμα είναι αδύνατη σε ένα δημόσιο αποκεντρωμένο καθολικό (Cai et al., 2018). Ωστόσο, αυτό δεν αποτρέπει την αναπαραγωγή ενός ψηφιακού νομίσματος και την χρήση του περισσότερες από μία φορές. Παρακάτω αναλύονται μερικοί τρόποι με τους οποίους επιτυγχάνονται οι επιθέσεις διπλής δαπάνης.

Επίθεση Race. Αποτελεί έναν τύπο επίθεσης που μπορεί να εφαρμοστεί εύκολα σε blockchains που βασίζονται στο μηχανισμό συναίνεσης PoW. Αναφέρεται σε μια επίθεση όπου ένας κακόβουλος χρήστης ή μια ομάδα χρηστών επιχειρεί να χειραγωγήσει το αποτέλεσμα μιας συναλλαγής, εκτελώντας ενέργειες σε γρήγορη διαδοχή για να παρεμποδίσει την κανονική διαδικασία συναίνεσης. Η επίθεση ξεκινά όταν ένας εισβολέας στέλνει γρήγορα δύο ή περισσότερες αντικρουόμενες συναλλαγές στο δίκτυο. Αρχικά, ο εισβολέας στέλνει μια συναλλαγή ως πληρωμή, για παράδειγμα σε έναν έμπορο, ο οποίος αποστέλλει το προϊόν χωρίς να περιμένει επιβεβαίωση της συναλλαγής, ενώ παράλληλα, ο εισβολέας στέλνει μια άλλη αντικρουόμενη συναλλαγή στο δίκτυο την οποία οι κόμβοι του δικτύου αποδέχονται ως έγκυρη και θεωρούν την πρώτη συναλλαγή, με την οποία αποστέλλονται τα κρυπτονομίσματα στον έμπορο, ως άκυρη (Bhushan et al., 2021). Ο επιτιθέμενος εκμεταλλεύεται τον ενδιάμεσο χρόνο μεταξύ της έναρξης και της επιβεβαίωσης δύο συναλλαγών επιτυγχάνοντας έτσι γρήγορη εκκίνηση μιας επίθεσης διπλής δαπάνης (Li et al., 2020). Μια πρόταση για την πρόληψη αυτής της επίθεσης είναι να γίνεται έλεγχος, από τους ομότιμους κόμβους του δικτύου κατά τη λήψη μιας νέας συναλλαγής, για προηγούμενη χρήση των νομισμάτων της συναλλαγής στο blockchain και στη μνήμη του. Οι ομότιμοι προσθέτουν αυτά τα νομίσματα στη δεξαμενή μνήμης τους και τα προωθούν σε ολόκληρο το δίκτυο μόνο εάν δεν έχουν βρεθεί σε προηγούμενες συναλλαγές (Bhushan et al., 2021). Ουσιαστικά αυτός ο τρόπος εστιάζει στον εντοπισμό της επίθεσης και όχι στην αποτροπή της.

Επίθεση πλειοψηφίας ή επίθεση 51% (Majority attack ή 51% attack). Η εμπιστοσύνη σε ένα δίκτυο blockchain επιτυγχάνεται μέσω του κατανεμημένου μηχανισμού συναίνεσης. Ωστόσο, ο μηχανισμός συναίνεσης είναι ευάλωτος σε επιθέσεις 51%. Στα blockchains που βασίζονται στο μηχανισμό συναίνεσης PoW, μια τέτοια επίθεση μπορεί να ξεκινήσει εάν ένας κόμβος εξόρυξης ή μια ομάδα κόμβων εξόρυξης, ή όπως ονομάζεται δεξαμενή εξόρυξης (mining pool), αποκτήσει ισχύ κατακερματισμού

περισσότερη από το 50% της συνολικής ισχύος κατακερματισμού ολόκληρου του blockchain (Bhushan et al., 2021). Στα blockchains που βασίζονται στο μηχανισμό συναίνεσης PoS, η επίθεση 51% μπορεί επίσης να συμβεί εάν ο αριθμός των νομισμάτων που ανήκουν σε ένα μόνο κόμβο εξόρυξης είναι περισσότερος από το 50% του συνολικού blockchain (Li et al., 2020). Σε αυτή την περίπτωση ένας εισβολέας μπορεί να εκμεταλλευτεί αυτή την ευπάθεια για να καταστρέψει το δίκτυο και να εξαπολύσει επιθέσεις όπως, αντιστροφή συναλλαγών και εκκίνηση επίθεσης διπλής δαπάνης, εξαίρεση και τροποποίηση της διάταξης των συναλλαγών, παρεμπόδιση των κανονικών εργασιών εξόρυξης άλλων κόμβων και παρακώλυση της λειτουργίας επιβεβαίωσης των κανονικών συναλλαγών (Li et al., 2020). Ένας τρόπος πρόληψης της επίθεσης είναι η αποτροπή μιας ομάδας εξόρυξης ή ακόμα κι ενός μεμονωμένου κόμβου εξόρυξης από το να επιτύχει το μισό του συνολικού ποσοστού κατακερματισμού εντός του δικτύου. Αυτό μπορεί να επιτευχθεί αυξάνοντας την ισχύ κατακερματισμού του δικτύου, μέσω της παροχής κινήτρων σε περισσότερους κόμβους εξόρυξης να ενταχθούν στο δίκτυο και να ανταγωνιστούν για ανταμοιβές μπλοκ. Μια ακόμα λύση αποτελεί η εφαρμογή αλγορίθμων συναίνεσης PoS ή PoA αντί του PoW. Στην περίπτωση του PoS οι χρήστες διακυβεύουν το μερίδιο του κρυπτονομίσματος που κατέχουν, ενώ στην περίπτωση του PoA οι χρήστες διακυβεύουν την φήμη τους, το οποίο τους αποτρέπει από το να ενεργούν με κακόβουλο τρόπο, μειώνοντας την πιθανότητα μιας επίθεσης 51%.

Επίθεση Finney. Είναι μια επίθεση διπλής δαπάνης που απαιτεί ο κακόβουλος χρήστης να εξορύξει εκ των προτέρων μια συναλλαγή σε μπλοκ (Dasgupta et al., 2019). Οι επιθέσεις Finney λειτουργούν εκμεταλλευόμενες το γεγονότος ότι σε ορισμένα δίκτυα blockchain υπάρχει μια χρονική καθυστέρηση μεταξύ της εξόρυξης ενός μπλοκ και της προσθήκης του στο δίκτυο. Ο εισβολέας ξεκινά με την κρυφή εξόρυξη ενός μπλοκ σε μια ξεχωριστή αλυσίδα και στη συνέχεια περιμένει να προστεθεί στο δίκτυο. Μόλις προστεθεί το μπλοκ, ο εισβολέας το απελευθερώνει στο δημόσιο δίκτυο και ξοδεύει γρήγορα το ίδιο κρυπτονόμισμα σε μια άλλη συναλλαγή προτού το υπόλοιπο δίκτυο αντιληφθεί τη διπλή δαπάνη (Bhushan et al., 2021). Με αυτόν τον τρόπο, ο εισβολέας είναι σε θέση να ξεγελάσει το δίκτυο ώστε να αποδεχτεί τη διπλή δαπάνη ως νόμιμη, κλέβοντας ουσιαστικά κρυπτονομίσματα από το δίκτυο. Οι επιθέσεις Finney βασίζονται στο ότι ο εισβολέας έχει επαρκή υπολογιστική ισχύ για την εξόρυξη μπλοκ γρηγορότερα από το υπόλοιπο δίκτυο, επιτρέποντάς του να χειριστεί το blockchain για δικό του

κέρδος. Αν και είναι δύσκολο να αποτραπεί μια τέτοια επίθεση, μια λύση που μειώνει τον κίνδυνο εκτέλεσής της είναι η αναμονή για περισσότερες επιβεβαιώσεις πριν την ολοκλήρωση μιας συναλλαγής (Iqbal & Matulevičius, 2021). Η απαίτηση περισσότερων επιβεβαιώσεων ώστε να θεωρείται έγκυρη μια συναλλαγή, κάνει πιο δύσκολο για έναν εισβολέα να εκτελέσει μια επίθεση Finney, καθώς θα πρέπει να ξοδέψει μεγαλύτερο αριθμό νομισμάτων.

2.7.2. Επιθέσεις στο πρωτόκολλο επικοινωνίας

Η P2P φύση του δικτύου blockchain απαιτεί από όλους τους κόμβους να χρησιμοποιούν τα πρωτόκολλα blockchain για την παροχή υπηρεσιών δικτύου (Bhushan et al., 2021). Αυτό οδηγεί σε διάφορους τύπους απειλών δικτύου, με τους κυριότερους να περιγράφονται λεπτομερώς παρακάτω.

Επίθεση Έκλειψης (Eclipse attack). Σε μια τέτοιου είδους επίθεση ένας εισβολέας είναι ικανός να ελέγχει έναν τεράστιο αριθμό διευθύνσεων IP και να μονοπωλεί όλες τις εισερχόμενες και εξερχόμενες συνδέσεις του κόμβου θύματος, γεγονός που απομονώνει το θύμα από τους άλλους ομότιμους του δικτύου (Bhushan et al., 2021). Αυτό επιτρέπει στον εισβολέα να ελέγχει τις πληροφορίες που λαμβάνει ο κόμβος θύμα, να χειρίζεται τη συμπεριφορά του ή ακόμα και να εκμεταλλευτεί την υπολογιστική ισχύ του για να πραγματοποιήσει τις δικές του κακόβουλες πράξεις. Πιο συγκεκριμένα, στο δίκτυο του Bitcoin υπάρχουν δύο τύποι επίθεσης έκλειψης, η επίθεση botnet και η επίθεση υποδομής. Η επίθεση botnet ξεκινά από bots με διαφορετικά εύρη διευθύνσεων IP, ενώ η επίθεση υποδομής μοντελοποιεί την απειλή από μια ISP, εταιρεία ή έθνος-κράτος, που έχει συνεχόμενες διευθύνσεις IP (Li et al., 2020). Στην περίπτωση που ο εισβολέας πραγματοποιήσει μια επιτυχημένη επίθεση έκλειψης είναι σε θέση να εξαπολύσει κι άλλες επιθέσεις, όπως επιθέσεις διπλής δαπάνης με Zero-confirmation και N-confirmation συναλλαγές, επιθέσεις εγωιστικής εξόρυξης ή ακόμη να δημιουργήσει κάποια διακλάδωση στην αλυσίδα (adversarial forks) (Bhushan et al., 2021). Οι Heilman et al. (2015), οι οποίοι ήταν αυτοί που παρουσίασαν την επίθεση Έκλειψης, πρότειναν στο άρθρο τους δέκα αντίμετρα, μερικά από τα οποία είναι η εφαρμογή συνδέσεων feeler, η εφαρμογή συνδέσεων anchor, η χρήση περισσότερων buckets, η απαγόρευση ανεπιθύμητων μηνυμάτων ADDR, η διαφοροποίηση των εισερχόμενων συνδέσεων και ο εντοπισμός ανωμαλιών.

Επίθεση Sybil. Αποτελεί ένα γενικό τύπο επίθεσης σε P2P δίκτυα όπου ένας εισβολέας δημιουργεί πολλαπλές ψευδείς ταυτότητες σε ένα αποκεντρωμένο δίκτυο, γνωστές και ως συβιλιανοί κόμβοι (sybil nodes), προκειμένου να το χειραγωγήσει (Dasgupta et al., 2019). Δημιουργώντας πολλαπλές ταυτότητες, ο εισβολέας μπορεί να αποκτήσει τον έλεγχο ενός σημαντικού τμήματος του δικτύου, διακόπτοντας την διάδοση των έντιμων κόμβων του ή απομονώνοντας έναν κόμβο στόχο από τους υπόλοιπους του δικτύου, θέτοντας σε κίνδυνο την ασφάλεια και την ακεραιότητά του δικτύου. Στην περίπτωση των blockchains, ο εισβολέας μπορεί να χρησιμοποιήσει εικονικές μηχανές, πολλές συσκευές ή διευθύνσεις IP ως ψεύτικους κόμβους για την επίθεση, οι οποίοι του δίνουν την ικανότητα να αποκηρύξει τα μεταδιδόμενα μπλοκ και να υπερψηφίσει τους αυθεντικούς κόμβους (Johar et al., 2021). Αυτός ο τύπος επίθεσης μπορεί χρησιμοποιηθεί με σκοπό την χειραγώγηση του μηχανισμούς συναίνεσης, την τροποποίηση έγκυρων συναλλαγών, ή ως μέσο για την εκτόξευση διαφορετικών επιθέσεων, όπως επιθέσεις άρνησης υπηρεσίας ή επιθέσεις διπλής δαπάνης. Μια επίθεση Sybil είναι δύσκολο να αποτραπεί, ωστόσο, υπάρχουν μερικές προτάσεις για να ξεπεραστεί. Αρχικά μια λύση είναι ο περιορισμός των κόμβων εξόρυξης ώστε να μην εξορύσσουν διαδοχικά μπλοκ. Εάν ένας κόμβος εξόρυξης έχει ήδη εξορύξει ένα μπλοκ, τότε δεν θα εκτελέσει τη διαδικασία εξόρυξης έως ότου λάβει τουλάχιστον ένα μπλοκ από άλλους κόμβους εξόρυξης (Iqbal & Matulevičius, 2021). Ακόμη μια πρόταση, όμοια με την περίπτωση της επίθεσης Finney, είναι η αναμονή για περισσότερες επιβεβαιώσεις πριν την ολοκλήρωση μιας συναλλαγής.

Επίθεση Transaction Malleability. Η "ευκαμψία" των συναλλαγών αποτελεί μια ευπάθεια του πρωτοκόλλου Bitcoin που επιτρέπει σε έναν επιτιθέμενο να τροποποιήσει μια συναλλαγή αφού δημιουργηθεί, αλλά πριν επιβεβαιωθεί στο δίκτυο και προστεθεί σε ένα μπλοκ. Λειτουργεί αξιοποιώντας τον τρόπο με τον οποίο οι συναλλαγές κατακερματίζονται και μεταδίδονται σε ένα δίκτυο blockchain. Οι διευθύνσεις προέλευσης και προορισμού, καθώς και το ποσό της συναλλαγής, δεν μπορούν να παραποιηθούν, ο επιτιθέμενος ωστόσο μπορεί να τροποποιήσει άλλα τμήματα της συναλλαγής πριν μεταδοθεί στο δίκτυο, όπως το πεδίο "υπογραφή", με αποτέλεσμα ένα αναγνωριστικό συναλλαγής (TXID) που διαφέρει από το πρωτότυπο (Dasgupta et al., 2019). Αυτό μπορεί να προκαλέσει σύγχυση, καθώς η αρχική συναλλαγή μπορεί να εμφανίζεται ως μη επιβεβαιωμένη, ενώ μια δεύτερη συναλλαγή με τα ίδια κεφάλαια

μπορεί να φαίνεται επιβεβαιωμένη. Μια τέτοια επίθεση θεωρείται ως εναλλακτική επίθεση διπλής δαπάνης, με την διαφορά ότι σε αυτή την περίπτωση ο επιτιθέμενος δεν είναι αυτός που δημιουργεί την συναλλαγή (Bhushan et al., 2021). Ένα αντίμετρο που προτείνεται για την αντιμετώπιση αυτής της επίθεσης είναι η Πρόταση Βελτίωσης του Bitcoin 62 (BIP 62), η οποία περιλαμβάνει πολλαπλές μετρήσεις επαλήθευσης συναλλαγών για την επικύρωση μιας νέας συναλλαγής (Bhushan et al., 2021). Μια ακόμα προτεινόμενη λύση είναι η εφαρμογή του πρωτοκόλλου Segregated Witness (SegWit). Το SegWit είναι μια αναβάθμιση μαλακής διακλάδωσης (soft fork) που διαχωρίζει τα δεδομένα υπογραφής από τα δεδομένα συναλλαγής. Αυτός ο διαχωρισμός βοηθά στην αποτροπή της επίθεσης, καθιστώντας πιο δύσκολη την τροποποίηση του αναγνωριστικού συναλλαγής για έναν κακόβουλο χρήστη.

2.7.3. Επιθέσεις εξόρυξης

Στα τρέχοντα συστήματα blockchain που βασίζονται στον μηχανισμό συναίνεσης PoW, οι κόμβοι εξόρυξης, ή αλλιώς ανθρακωρύχοι, συνήθως σχηματίζουν ομάδες, γνωστές ως δεξαμενές εξόρυξης (mining pools), για να συνδυάσουν την υπολογιστική τους ισχύ και να αυξήσουν τις πιθανότητές τους να κερδίσουν ανταμοιβές για την εύρεση νέων μπλοκ. Η διαμόρφωση των δεξαμενών μπορεί να προσφέρει στους κόμβους εξόρυξης σταθερά έσοδα, αλλά εισάγει κρίσιμα ζητήματα, τα οποία μπορεί ένας κακόβουλος χρήστης να εκμεταλλευτεί για να ξεκινήσει είτε εξωτερικές επιθέσεις είτε εσωτερικές επιθέσεις στην δεξαμενή εξόρυξης. Στην συνέχεια περιγράφονται μερικοί από αυτούς τους τύπους απειλών.

Επίθεση εγωιστικής εξόρυξης (Selfish mining attack). Οι Eyal και Sirer (2018) ήταν οι πρώτοι που εισήγαγαν την στρατηγική εγωιστικής εξόρυξης σύμφωνα με την οποία μια δεξαμενή εξόρυξης διατηρεί ιδιωτικό το μπλοκ που ανακαλύπτει δημιουργώντας σκόπιμα διακλάδωση της αλυσίδας. Οι "εγωιστές" ανθρακωρύχοι που ανήκουν στην δεξαμενή συνεχίζουν να εξορύσσουν μπλοκ πάνω στην ιδιωτική διακλάδωση της αλυσίδας, ενώ οι έντιμοι ανθρακωρύχοι συνεχίζουν την εξόρυξη στην δημόσια διακλάδωση της αλυσίδας. Όταν τελικά προστεθεί ένα νέο μπλοκ στη δημόσια αλυσίδα, οι "εγωιστές" κόμβοι εξόρυξης απελευθερώνουν τα ιδιωτικά τους μπλοκ στο κοινό, δίνοντάς τους ένα πλεονέκτημα έναντι των άλλων κόμβων αυξάνοντας την πιθανότητα τα μπλοκ τους να προστεθούν στη δημόσια αλυσίδα μπλοκ, καθώς η μεγαλύτερη

διακλάδωση καθίσταται έγκυρη. Έτσι οι ανέντιμοι κόμβοι εξόρυξης λαμβάνουν υψηλότερες ανταμοιβές εις βάρος των έντιμων κόμβων που σπαταλούν τον χρόνο τους και την υπολογιστική ισχύ τους σε μπλοκ που προορίζονται να μην αποτελούν μέρος του blockchain (Eyal & Sirer, 2018). Παρακινούμενοι από την απόκτηση μεγαλύτερων ανταμοιβών, οι ορθολογικοί ανθρακωρύχοι μπορεί να τείνουν να συμμετέχουν σε εγωιστικές δεξαμενές εξόρυξης, προκειμένου να αυξήσουν την υπολογιστική τους ισχύ και την ικανότητά τους να εξορύξουν μεγαλύτερη αλυσίδα (Gao et al., 2018). Ένα προτεινόμενο αντίμετρο γι' αυτή την επίθεση είναι το σχήμα Freshness Preferred (FP), το οποίο χρησιμοποιεί χρονικές σημάνσεις που δεν μπορούν να πλαστογραφηθούν εντός της κεφαλίδας του μπλοκ, ούτως ώστε να αναγνωρίζονται τα μπλοκ που εξορύχθηκαν πρόσφατα. Αυτή η προσέγγιση μειώνει τα ιδιοτελή κίνητρα εξόρυξης, καθώς τα τετράγωνα που συγκρατούνται χάνουν τον αγώνα ενάντια στα πρόσφατα εξορυσσόμενα μπλοκ (Bhushan et al., 2021).

Επίθεση Block Withholding. Σε αυτόν τον τύπο επίθεσης, ένας κακόβουλος ανθρακωρύχος που έχει βρει ένα μπλοκ δεν το υποβάλει, αλλά επιλέγει είτε να το εγκαταλείψει άμεσα, είτε να αναβάλει την υποβολή του για να αυξήσει την ανταμοιβή του, υπονομεύοντας και στις δύο περιπτώσεις την ανταμοιβή της δεξαμενής στην οποία συμμετέχει. Στην πρώτη περίπτωση ο επιτιθέμενος δεν κερδίζει καμία ανταμοιβή, αλλά η δεξαμενή χάνει την ευκαιρία να κερδίσει την ανταμοιβή του μπλοκ, ενώ στην δεύτερη περίπτωση, ο επιτιθέμενος πρέπει να εκτελέσει μια σύνθετη επίθεση απόκρυψης του μπλοκ, παρόμοια με αυτή στην επίθεση εγωιστική εξόρυξης, έτσι ώστε όταν το αποκαλύψει να κερδίσει μεγαλύτερη ανταμοιβή.

Μια παραλλαγή αυτής της επίθεσης αποτελεί η επίθεση pool block withholding, όπου μια δεξαμενή εξόρυξης διοχετεύει μέρος της ισχύος κατακερματισμού της σε άλλες δεξαμενές για να αποκτήσει πρόσθετα έσοδα, χωρίς να συμβάλει στη διαδικασία εξόρυξης των δεξαμενών αυτών. Συνήθως, μια ομάδα εξόρυξης αποτελείται από δύο τύπους χρηστών, τους κανονικούς κόμβους εξόρυξης, που παράγουν το PoW και το υποβάλουν στον δεύτερο τύπο χρήστη, τον διαχειριστή της δεξαμενής. Ο διαχειριστής μεταδίδει το μπλοκ που δημιουργήθηκε πρόσφατα σε ολόκληρο το δίκτυο και στην συνέχεια είναι υπεύθυνος για τη δίκαιη κατανομή των ανταμοιβών μεταξύ των κόμβων εξόρυξης στην δεξαμενή (Bhushan et al., 2021). Σε αυτό το είδος επίθεσης, ο

διαχειριστής της δεξαμενής χρησιμοποιεί μερικούς από τους ανθρακωρύχους για να διεισδύει σε μια άλλη δεξαμενή θύμα, στην οποία οι ανθρακωρύχοι αυτοί προσποιούνται ότι δουλεύουν πάνω στα υπολογιστικά παζλ αλλά στην πραγματικότητα δεν κάνουν τίποτα. Οι επιτιθέμενοι ανθρακωρύχοι λαμβάνουν ανταμοιβή από τον διαχειριστή της δεξαμενής θύμα, καθώς δεν μπορεί να αναγνωρίσει ότι είναι κακόβουλοι. Παρόλο που η υπολογιστική δύναμη της δεξαμενής που πραγματοποιεί την επίθεση μειώνεται σε αυτό το σενάριο, η επιπλέον ανταμοιβή που απολαμβάνει από τις δεξαμενές στις οποίες έχει διεισδύσει αυξάνει τη συνολική χρησιμότητά της (Bhushan et al., 2021).

Επίθεση Fork-After Withholding. Η επίθεση αυτή αποτελεί έναν συνδυασμό των επιθέσεων εγωιστικής εξόρυξης και block withholding, στην οποία η ανταμοιβή για τον επιτιθέμενο είναι πάντα ίση ή μεγαλύτερη από την αντίστοιχη μιας επίθεσης block withholding. Η βασική ιδέα είναι ότι ένας επιτιθέμενος μπορεί να χωρίσει την υπολογιστική του ισχύ μεταξύ μιας τίμιας εξόρυξης και μιας εξόρυξης διείσδυσης, με στόχο μια δεξαμενή θύμα, όπως συμβαίνει σε μια επίθεση block withholding (Kwon et al., 2017). Η διαφορά έγκειται στο γεγονός ότι όταν ο επιτιθέμενος βρει ένα νόμιμο μπλοκ δεν το εγκαταλείπει, όπως συμβαίνει στην επίθεση block withholding, ούτε όμως το υποβάλει αμέσως στον διαχειριστή της δεξαμενής, αλλά περιμένει έναν εξωτερικό ειλικρινή κόμβο εξόρυξης να δημοσιεύσει το δικό του μπλοκ, οπότε και διαδίδει το δικό του ελπίζοντας να προκαλέσει μια διακλάδωση στην αλυσίδα, όπως συμβαίνει στην επίθεση εγωιστικής εξόρυξης (Kwon et al., 2017). Μέχρι στιγμής δεν έχει αναφερθεί καμία πρακτική πρόληψης γι' αυτή την επίθεση.

2.7.4. Απειλές στην ασφάλεια των πορτοφολιών

Για να πραγματοποιήσουν συναλλαγές ή να αποκτήσουν πρόσβαση σε νομίσματα σε ένα blockchain, οι χρήστες πρέπει να διαθέτουν δημόσια και ιδιωτικά κλειδιά. Το ψηφιακό πορτοφόλι κρυπτονομισμάτων είναι ένα κομμάτι λογισμικού ή υλικού που χρησιμοποιείται για την δημιουργία, την αποθήκευση και την διαχείριση αυτών των κλειδιών των λογαριασμών κρυπτονομισμάτων. Ένα πορτοφόλι κρυπτονομισμάτων ουσιαστικά λειτουργεί σαν ένα παραδοσιακό πορτοφόλι, αλλά αντί να διατηρεί φυσικό νόμισμα, κατέχει ψηφιακά στοιχεία. Τα ιδιωτικά κλειδιά λειτουργούν όπως λειτουργεί ένας κωδικός πρόσβασης και επιτρέπουν στον κάτοχο του πορτοφολιού να έχει πρόσβαση και να στείλει τα κρυπτονόμισματά του, ενώ τα δημόσια κλειδιά

χρησιμοποιούνται ως διεύθυνση για τη λήψη κρυπτονομισμάτων. Όπως γίνεται αντιληπτό, το να κατέχει κάποιος το ιδιωτικό κλειδί ενός πορτοφολιού είναι ισοδύναμο με τον πλήρη έλεγχο του αντίστοιχου λογαριασμού κρυπτονομισμάτων, επομένως, η σωστή διαχείριση των κλειδιών είναι πολύ σημαντική για την διατήρηση της ασφάλειας. Τα πορτοφόλια κρυπτονομισμάτων φέρουν γενικά τις βασικές λειτουργίες για την διαχείριση του ιδιωτικού κλειδιού και την διαχείριση των συναλλαγών. Η διαχείριση κλειδιών περιλαμβάνει τη δημιουργία, την αποθήκευση, την εισαγωγή και την εξαγωγή ενός ιδιωτικού κλειδιού και η διαχείριση συναλλαγών περιλαμβάνει τη μεταφορά και τη συλλογή tokens, καθώς και την αναζήτηση στο ιστορικό συναλλαγών και υπολοίπων του λογαριασμού (He et al., 2020). Ωστόσο, η ακατάλληλη εφαρμογή αυτών των λειτουργιών μπορεί να εισάγει ευπάθειες που μπορούν να οδηγήσουν σε επιθέσεις. Επιπλέον, μια ακόμα απειλή για την ασφάλεια του ψηφιακού πορτοφολιού προκύπτει από το λειτουργικό σύστημα (OS) στο οποίο φιλοξενείται το πορτοφόλι, καθώς ένας εισβολέας ενδέχεται να αξιοποιήσει τις δυνατότητες που παρέχονται από το λειτουργικό σύστημα με σκοπό την πραγματοποίηση επιθέσεων. Ο στόχος ενός εισβολέα είναι να σπάσει την εμπιστευτικότητα, την ακεραιότητα ή τις ιδιότητες διαθεσιμότητας των δεδομένων στα πορτοφόλια κι αυτό περιλαμβάνει την απόκτηση του ιδιωτικού κλειδιού, την παραβίαση συναλλαγών που ξεκίνησαν πρόσφατα, την παραβίαση ιστορικών συναλλαγών, τον αποκλεισμό της δημιουργίας νέων συναλλαγών, την άρνηση ερωτήσεων πληροφοριών συναλλαγών και ούτω καθεξής (He et al., 2020). Στη συνέχεια αναλύονται μερικές ευπάθειες των πορτοφολιών που μπορούν να οδηγήσουν σε επιθέσεις.

Ευάλωτη υπογραφή. Αποτελεί μια ευπάθεια στον μηχανισμό ψηφιακής υπογραφής, ο οποίος χρησιμοποιείται για τον έλεγχο της ταυτότητας συναλλαγών στο blockchain. Οι ψηφιακές υπογραφές διασφαλίζουν ότι μόνο ο νόμιμος κάτοχος ενός πορτοφολιού κρυπτονομισμάτων μπορεί να ξεκινήσει μια συναλλαγή και ότι η συναλλαγή δεν μπορεί να τροποποιηθεί ή να παραποιηθεί αφού πραγματοποιηθεί, ωστόσο, σε ορισμένες περιπτώσεις, ο μηχανισμός αυτός μπορεί να είναι ευάλωτος σε επιθέσεις. Για παράδειγμα, ένας εισβολέας μπορεί να είναι σε θέση να εκμεταλλευτεί τις αδυναμίες στον αλγόριθμο υπογραφής ή στην υλοποίηση του αλγόριθμου στο λογισμικό του πορτοφολιού για να πλαστογραφήσει μια έγκυρη υπογραφή ή να ξεγελάσει το πορτοφόλι ώστε να αποδεχτεί μια μη έγκυρη υπογραφή, γεγονός που μπορεί να οδηγήσει σε κλοπή

κρυπτονομισμάτων από το πορτοφόλι του θύματος ή εκκίνηση δόλιων συναλλαγών χωρίς τη γνώση ή τη συναίνεση του θύματος.

Ελαττωματική δημιουργία κλειδιών. Είναι μια ευπάθεια που προκύπτει όταν τα ιδιωτικά κλειδιά που χρησιμοποιούνται για την πρόσβαση και την εξουσιοδότηση συναλλαγών στο πορτοφόλι δεν δημιουργούνται με ασφάλεια ή με αρκετά τυχαίο τρόπο. Τα ιδιωτικά κλειδιά είναι ουσιαστικά μεγάλες σειρές αριθμών και γραμμάτων που χρησιμοποιούνται για την υπογραφή και την εξουσιοδότηση συναλλαγών στο blockchain. Εάν ένα πορτοφόλι κρυπτονομισμάτων δημιουργεί ιδιωτικά κλειδιά χρησιμοποιώντας μια εσφαλμένη ή ανασφαλή μέθοδο, ένας εισβολέας μπορεί να είναι σε θέση να μαντέψει ή να εξαναγκάσει το ιδιωτικό κλειδί και να αποκτήσει πρόσβαση στο πορτοφόλι του χρήστη. Για παράδειγμα, η χρήση μιας προβλέψιμης γεννήτριας τυχαίων αριθμών (Random Number Generator) για την δημιουργία κλειδιών, όπως η Random.nextInt() στην Java, μπορεί να αποδειχθεί ανασφαλής λόγω της προβλέψιμης φύσης της (Sai et al., 2019).

Έλλειψη ελέγχου κατά την δημιουργία διεύθυνσης. Η απειλή αυτή αναφέρεται σε μια ευπάθεια που προκύπτει όταν ένα πορτοφόλι δεν παρέχει επαρκή έλεγχο στις διευθύνσεις που χρησιμοποιούνται για τη λήψη κρυπτονομισμάτων. Σε ορισμένα πορτοφόλια, οι διευθύνσεις ενδέχεται να δημιουργούνται αυτόματα ή εν αγνοία του χρήστη, κάτι που μπορεί να οδηγήσει σε κινδύνους για την ασφάλεια. Για παράδειγμα, εάν ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στο πορτοφόλι κρυπτονομισμάτων ενός χρήστη, είναι σε θέση να δημιουργήσει νέες διευθύνσεις και να κατευθύνει τις εισερχόμενες συναλλαγές σε αυτές τις διευθύνσεις.

2.8. Ζητήματα ιδιωτικότητας

Η τεχνολογία Blockchain χρησιμοποιεί πολύπλοκες κρυπτογραφικές μεθόδους ώστε να διασφαλιστεί ότι το αποκεντρωμένο καθολικό είναι ασφαλές. Ωστόσο, η διατήρηση της ιδιωτικής ζωής, ή αλλιώς του απορρήτου, είναι μία από τις μεγαλύτερες προκλήσεις στην τεχνολογία αυτή. Το απόρρητο είναι η ικανότητα ενός μεμονωμένου ατόμου ή μιας ομάδας να διατηρεί ορισμένες προσωπικές πληροφορίες ή δραστηριότητες κρυφές ή περιορισμένες από το κοινό ή από άλλους. Αναφέρεται στο δικαίωμα ενός ατόμου να ελέγχει τα προσωπικά του δεδομένα και να αποφασίζει ποιος έχει πρόσβαση σε αυτά.

Στην περίπτωση του blockchain, το απόρρητο αποτελεί τη δυνατότητα εκτέλεσης συναλλαγών χωρίς διαρροή πληροφοριών αναγνώρισης. Παράλληλα, το απόρρητο επιτρέπει σε έναν χρήστη να παραμείνει ανώνυμος, αποκαλύπτοντας διακριτικά τον εαυτό του χωρίς να εκθέτει τη δραστηριότητά του σε ολόκληρο το δίκτυο. Το blockchain είναι κυρίως ευάλωτο στη διαρροή του απορρήτου των συναλλαγών λόγω του γεγονότος ότι οι λεπτομέρειες και τα υπόλοιπα όλων των δημόσιων κλειδιών αποθηκεύονται δημόσια και είναι ορατά σε όλους στο δίκτυο. Στην ουσία, τα κατακερματισμένα προσωπικά δεδομένα παρέχουν ψευδωνυμία αλλά όχι ανωνυμία. Στην ενότητα αυτή θα πραγματοποιηθεί ανάλυση των προκλήσεων απορρήτου που συναντώνται σε σενάρια blockchain καθώς και των προτεινόμενων λύσεων για την διατήρηση αυτού.

2.8.1. Προκλήσεις απορρήτου σε σενάρια blockchain

Σε αυτό το σημείο θα γίνει αναφορά στις σημαντικότερες προκλήσεις που μπορούν να οδηγήσουν σε διαρροή απορρήτου. Αυτές περιλαμβάνουν τη δυνατότητα σύνδεσης συναλλαγών με συγκεκριμένους χρήστες, προβλήματα στη διαχείριση και ανάκτηση ιδιωτικών κλειδιών, καθώς και ζητήματα που αφορούν το απόρρητο των δεδομένων εντός της αλυσίδας.

Δυνατότητα σύνδεσης συναλλαγών με τον χρήστη. Οι χρήστες που συμμετέχουν σε permissionless δίκτυα blockchain μπορούν να δημιουργήσουν όσα ζεύγη κλειδιών θέλουν, δηλαδή μπορούν να δημιουργήσουν πολλαπλές διευθύνσεις, με παρόμοιο τρόπο όπως μπορεί ένα άτομο να δημιουργήσει πολλούς τραπεζικούς λογαριασμούς (Zhang et al., 2019). Ωστόσο, αυτό παρέχει ψευδωνυμία και όχι ανωνυμία στους χρήστες, καθώς το καθολικό καταγράφει το ιστορικό κάθε συναλλαγής μαζί με τις διευθύνσεις του αποστολέα και του παραλήπτη σε γραφήματα συναλλαγών blockchain, τα οποία μπορούν να συνδέσουν όλες τις ανεξάρτητες διευθύνσεις δημόσιου κλειδιού στον χρήστη. Μόλις συνδεθούν όλες οι συναλλαγές που σχετίζονται με έναν χρήστη, είναι εύκολο να συναχθούν άλλες πληροφορίες σχετικά με τον χρήστη αυτό, όπως το υπόλοιπο του λογαριασμού, το είδος και η συχνότητα των συναλλαγών του, και η χρήση τέτοιων στατιστικών δεδομένων για συναλλαγές και λογαριασμούς σε συνδυασμό με κάποιες βασικές γνώσεις σχετικά με έναν χρήστη, μπορούν να οδηγήσουν στην αποκάλυψη της πραγματικής του ταυτότητας (Zhang et al., 2019).

Πολλές διευθύνσεις του ίδιου χρήστη θα μπορούσαν να συσχετίζονται από συναλλαγές πολλαπλών εισόδων (multi-entry transactions), οι οποίες απαιτούν διαφορετικές διευθύνσεις που ανήκουν στον ίδιο χρήστη αποδεικνύοντας τη γνώση όλων των ιδιωτικών κλειδιών, καθιστώντας όλες τις διευθύνσεις εισόδου συνδεδεμένες με τον ίδιο χρήστη, ή από συναλλαγές με αλλαγή (transactions with change) οι οποίες επιτρέπουν τον εντοπισμό του χρήστη όταν χρησιμοποιεί την ίδια δημόσια διεύθυνση για να πάρει μερικά περιουσιακά στοιχεία που έχουν υποστεί αλλαγή (Bernabe et al., 2019). Ένας ακόμα τρόπος με τον οποίο μπορεί να αποκαλυφθεί η ταυτότητα ενός χρήστη είναι μέσω των διαδικτυακών πληρωμών. Πιο συγκεκριμένα, εάν ένας χρήστης κάνει αγορές μέσω διαδικτύου και τις πληρώσει με κρυπτονόμισμα, είναι πιθανό ένας αντίπαλος ή ένας πάροχος υπηρεσιών Διαδικτύου να προσδιορίσει μοναδικά τη συναλλαγή αυτή στο blockchain και να την συνδέσει με τον χρήστη μέσω των cookies του προγράμματος περιήγησης. Τέλος, μια πρόκληση για την διατήρηση της ανωνυμίας των χρηστών αποτελεί η P2P αρχιτεκτονική του δικτύου blockchain. Οι κόμβοι του blockchain επικοινωνούν μεταξύ τους σε μια επικάλυψη P2P δικτύου μέσω του Διαδικτύου, γεγονός που τους καθιστά εντοπίσιμους στο δίκτυο μέσω των IP διευθύνσεών τους, τις οποίες διαρρέουν όταν υποβάλλουν νέες συναλλαγές (Bernabe et al., 2019). Παρατηρώντας τις δημόσιες διευθύνσεις που χρησιμοποιούνται στο blockchain, ένας άλλος κόμβος του δικτύου θα μπορούσε να συνδέσει μια διεύθυνση με ένα πορτοφόλι και τον πραγματικό χρήστη, παρά την υποτιθέμενη ανωνυμία των νέων διευθύνσεων που δημιουργούνται τυχαία (Bernabe et al., 2019).

Διαχείριση και ανάκτηση ιδιωτικών κλειδιών. Κατά την αξιοποίηση του blockchain, τα ιδιωτικά κλειδιά του χρήστη χρησιμοποιούνται για την υπογραφή κάθε συναλλαγής και λαμβάνονται υπόψη ως διαπιστευτήρια αναγνώρισης, επομένως, είναι κρίσιμα για την ασφάλεια και το απόρρητο του χρήστη (Bhutta et al., 2021). Για τον λόγο αυτό είναι σημαντικό να επιβληθούν συστήματα διαχείρισης κλειδιών. Τα πορτοφόλια blockchain είναι αυτά που διατηρούν τα κλειδιά ενός χρήστη στις συσκευές του, είτε on-line είτε off-line. Η παραβίασή τους μπορεί να οδηγήσει όχι μόνο σε διαρροή απορρήτου αλλά και σε κλοπή ταυτότητας. Οι απειλές αυτές που αφορούν την ασφάλεια των πορτοφολιών αναλύθηκαν λεπτομερώς στην υποενότητα 2.7.4.

Απόρρητο των δεδομένων εντός αλυσίδας. Ενώ ο αμετάβλητος χαρακτήρας της τεχνολογίας Blockchain είναι ένα από τα μεγαλύτερα δυνατά της σημεία, αποτελεί μια σημαντική πρόκληση όσον αφορά την προστασία της ιδιωτικής ζωής. Όπως έχει ήδη αναφερθεί αρκετές φορές, μόλις προστεθούν οι συναλλαγές στο blockchain είναι αμετάβλητες και μόνιμες, δηλαδή δεν μπορούν να διαγραφούν ή να τροποποιηθούν, έτσι ολόκληρο το ιστορικό του blockchain είναι διαθέσιμο σε κάθε μέρος που επιθυμεί να το δει (Dasgupta et al., 2019). Αυτό μπορεί να δημιουργήσει κινδύνους για το απόρρητο μεμονωμένων ατόμων ή οργανισμών, καθώς οι προσωπικές ή εμπιστευτικές τους πληροφορίες μπορούν να εκτεθούν χωρίς τη συγκατάθεσή τους. Επιπλέον, η απουσία μηχανισμού διαγραφής ή αφαίρεσης δεδομένων από το blockchain μπορεί να δημιουργήσει ζητήματα κανονιστικής συμμόρφωσης, καθώς οι νόμοι περί προστασίας δεδομένων ενδέχεται να απαιτούν τη διαγραφή προσωπικών πληροφοριών υπό ορισμένες συνθήκες.

2.8.2 Λύσεις διατήρησης απορρήτου στο blockchain

Έχουν προταθεί πολλές μέθοδοι για την εξασφάλιση της ανωνυμίας και την διατήρηση του απορρήτου στο blockchain, οι οποίες, σύμφωνα με την βιβλιογραφία, μπορούν να ταξινομηθούν ευρέως σε δύο κατηγορίες, λύσεις mixing και λύσεις anonymous.

Mixing. Όπως υποδηλώνει το όνομα, οι τεχνικές mixing "αναμειγνύουν" πολλαπλές συναλλαγές με τρόπο που καθιστά δύσκολο τον εντοπισμό τους στην αρχική τους πηγή. Έχουν σχεδιαστεί για να αποτρέπουν την σύνδεση μεταξύ διευθύνσεων και ιστορικό συναλλαγών μέσω της μεταφοράς χρημάτων από πολλαπλές διευθύνσεις εισόδου σε πολλαπλές διευθύνσεις εξόδου. Για παράδειγμα, ένας χρήστης Α με διεύθυνση Α θέλει να στείλει κάποια χρήματα στον χρήστη Β με διεύθυνση Β, εάν όμως πραγματοποιήσει απευθείας μια συναλλαγή με τη διεύθυνση εισόδου Α και τη διεύθυνση εξόδου Β, η σχέση μεταξύ τους ενδέχεται να αποκαλυφθεί. Έτσι, ο χρήστης Α θα μπορούσε να στείλει χρήματα σε έναν έμπιστο μεσάζοντα C, ο οποίος στην συνέχεια μεταφέρει τα χρήματα στον χρήστη Β με πολλαπλές εισόδους c1, c2, c3, κ.λπ., και πολλαπλές εξόδους d1, d2, B, d3, κ.λπ., μέσα στις οποίες περιέχεται και η διεύθυνση του χρήστη Β. Με αυτόν τον τρόπο γίνεται πιο δύσκολο να αποκαλυφθεί η σχέση μεταξύ των χρηστών Α και Β. Ωστόσο, ο ενδιάμεσος θα μπορούσε να είναι ανέντιμος και να αποκαλύψει σκόπιμα τις προσωπικές πληροφορίες των χρηστών Α και Β ή θα μπορούσε επίσης να

μεταφέρει τα χρήματα του χρήστη Α στη δική του διεύθυνση αντί για τη διεύθυνση του χρήστη Β (Zheng et al., 2018). Παρ' όλα αυτά, τα πρωτόκολλα mixing επιλέγονται γιατί εφαρμόζονται σε ήδη υπάρχοντα blockchain, όπως το Bitcoin, ενώ οι άλλες κρυπτογραφικές λύσεις απαιτούν ένα νέο στιγμιότυπο του blockchain, με μεγαλύτερες συναλλαγές λόγω του μέγεθος των αποδείξεων ή των υπογραφών (Bernabe et al., 2019).

Τα πιο γνωστά πρωτόκολλα mixing είναι το Mixcoin, το Coinjoin και το CoinShuffle. Το Mixcoin (Bonneau et al., 2014) παρέχει ανώνυμες πληρωμές σε Bitcoin και παρόμοια κρυπτονομίσματα, όπως επίσης παρέχει μια απλή μέθοδο για την αποφυγή ανέντιμων συμπεριφορών. Ο μεσάζοντας κρυπτογραφεί τις απαιτήσεις των χρηστών, συμπεριλαμβανομένου του χρηματικού ποσού και της ημερομηνίας μεταφοράς με το ιδιωτικό του κλειδί, έτσι σε περίπτωση κλοπής των χρημάτων οποιοσδήποτε θα μπορούσε να εντοπίσει την απάτη, ωστόσο, δεν θα μπορούσε να την αποτρέψει. Το Coinjoin (Maxwell, 2013) ανωνυμοποιεί τις συναλλαγές Bitcoin "αναμειγνύοντας" πολλούς λογαριασμούς και αναδιανέμοντας τα νομίσματα με ψευδο-τυχαίο τρόπο. Για παράδειγμα, εάν ορισμένοι κόμβοι θέλουν να κρύψουν τα χρήματά τους, δημιουργούν από κοινού μια ενιαία συναλλαγή που συνδυάζει όλες τις συναλλαγές τους. Κάθε κόμβος παρέχει μια διεύθυνση εισόδου και εξόδου και στη συνέχεια σχηματίζουν μια συναλλαγή με αυτές τις διευθύνσεις. Η σειρά των διευθύνσεων εισόδου και εξόδου είναι τυχαία διατεταγμένη, επομένως οι υπόλοιποι κόμβοι δεν θα μπορούν να προσδιορίσουν την αντιστοίχιση μεταξύ των διευθύνσεων εισόδου και εξόδου. Τέλος, το CoinShuffle (Ruffing et al., 2014), επεκτείνει περαιτέρω την ιδέα του Coinjoin και εξασφαλίζει την διατήρηση του απορρήτου χωρίς την ανάγκη ενός αξιόπιστου τρίτου μέρους για την "ανάμειξη" των συναλλαγών. Το CoinShuffle θεωρείται ως ένα εντελώς αποκεντρωμένο πρωτόκολλο ανάμειξης νομισμάτων και έχει τη δυνατότητα να διασφαλίζει ασφάλεια έναντι κλοπής και ανωνυμία, χρησιμοποιώντας ένα νέο πρωτόκολλο ανώνυμης ομαδικής επικοινωνίας, που ονομάζεται Dissent (Zhang et al., 2019).

Anonymous. Το γενικό χαρακτηριστικό των ανώνυμων λύσεων είναι ότι το απόρρητο διατηρείται με βάση την κρυπτογραφία. Οι πιο γνωστές εφαρμογές ανώνυμων λύσεων είναι το Zerocoin, το Zerocash και το CryptoNote. Το Zerocoin (Miers et al., 2013) είναι ένα κατανεμημένο σύστημα ηλεκτρονικών μετρητών που χρησιμοποιεί αποδείξεις μηδενικής γνώσης για να σπάσει τη σύνδεση μεταξύ των συναλλαγών και να αποτρέψει

τις αναλύσεις γραφημάτων συναλλαγών. Σε αντίθεση με τις προαναφερθείσες προσεγγίσεις mixing, στο Zerocoin ο χρήστης δεν ζητάει την ανταλλαγή νομισμάτων σε ένα σύνολο ανάμειξης, αλλά μπορεί να δημιουργήσει ο ίδιος τα ZeroCoins αποδεικνύοντας ότι κατέχει την ίση αξία των Bitcoin μέσω του πρωτοκόλλου Zerocoin. Ωστόσο, εξακολουθεί να αποκαλύπτει τον προορισμό και τα ποσά των πληρωμών (Zheng et al., 2018). Με σκοπό να ξεπεράσει τα προβλήματα του Zerocoin, προτάθηκε το Zerocash (Sasson et al., 2014), γνωστό και ως Zcash, το οποίο χρησιμοποιεί μια βελτιωμένη έκδοση της απόδειξης μηδενικής γνώσης, το zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARK), το οποίο αποκρύπτει επιπλέον πληροφορίες σχετικά με τις συναλλαγές, όπως το ποσό και τις διευθύνσεις παραλήπτη, για την επίτευξη ισχυρών εγγυήσεων απορρήτου. Ωστόσο, κι αυτή η λύση αποτελεί μια πολύπλοκη κρυπτογραφική μέθοδο που επιβραδύνει τις συναλλαγές. Τέλος, μια ακόμα γνωστή ανώνυμη λύση είναι το CryptoNote, που αποτελεί μία από τις τυπικές εφαρμογές της μεθόδου υπογραφής δακτυλίου (ring signature). Η υπογραφή δακτυλίου είναι ένας τύπος ψηφιακής υπογραφής όπου, δεδομένης μιας ομάδας μελών με ιδιωτικά και δημόσια κλειδιά, η υπογραφή εκτελείται από ένα από τα μέλη της ομάδας, αλλά η ίδια η υπογραφή δεν αποκαλύπτει ποιος την υπέγραψε (Bernabe et al., 2019). Το όνομα προέρχεται από από τον αλγόριθμο υπογραφής που χρησιμοποιεί τη δομή τύπου δακτυλίου και όχι από την αλγεβρική της δομή. Το CryptoNote υιοθετεί υπογραφές δακτυλίου για να κρύψει τη σύνδεση μεταξύ των διευθύνσεων των συναλλαγών του αποστολέα. Πιο συγκεκριμένα, το CryptoNote κατασκευάζει το δημόσιο κλειδί του αποστολέα με πολλά άλλα κλειδιά, έτσι ώστε να είναι αδύνατο να προσδιοριστεί ποιος πραγματικά έστειλε, ή αλλιώς υπέγραψε, τη συναλλαγή (Zhang et al., 2019).

3.Έξυπνα Συμβόλαια

Ο όρος "έξυπνο συμβόλαιο" εμφανίστηκε την δεκαετία του 1990 και ορίστηκε από τον Αμερικανό ερευνητή Nick Szabo (1994), ως ένα πρωτόκολλο ηλεκτρονικών συναλλαγών που εκτελεί τους όρους μιας σύμβασης. Οι γενικοί στόχοι του σχεδιασμού έξυπνων συμβολαίων είναι η ικανοποίηση κοινών συμβατικών όρων (όπως οι όροι πληρωμής, τα προνόμια, η εμπιστευτικότητα, ακόμη και η επιβολή), η ελαχιστοποίηση εξαιρέσεων, τόσο κακόβουλων όσο και τυχαίων, και η ελαχιστοποίηση της ανάγκης για αξιόπιστους μεσάζοντες (Szabo, 1994). Η ιδέα αυτή δεν έλαβε αρκετή προσοχή εκείνη την εποχή, παρά μόνο αρκετά χρόνια αργότερα, με την εμφάνιση και την ανάπτυξη της τεχνολογίας Blockchain. Τα έξυπνα συμβόλαια και η τεχνολογία Blockchain είναι ανεξάρτητες ιδέες, ωστόσο, η τεχνολογία Blockchain είναι ιδιαίτερα κατάλληλη για την ανάπτυξη έξυπνων συμβολαίων, λόγω των χαρακτηριστικών της αποκέντρωσης, της αντοχής σε παραβιάσεις και της ιχνηλασιμότητας, που αποτρέπουν την κακόβουλη παραβίαση των όρων της σύμβασης. Η συσχέτιση μεταξύ έξυπνου συμβολαίου και blockchain έγινε δημοφιλής με την ανάπτυξη του blockchain Ethereum (Vigliotti, 2021). Ωστόσο, πρέπει να σημειωθεί ότι η εκτέλεση έξυπνων συμβολαίων δεν υποστηρίζεται από κάθε blockchain.

Το επίθετο "έξυπνο" σημαίνει ότι η λειτουργικότητα ενός αντικειμένου έχει βελτιωθεί σημαντικά μέσω εφαρμογών λογισμικού, δηλαδή, μέρος της λειτουργικότητας έχει αυτοματοποιηθεί (Vigliotti, 2021). Στην συγκεκριμένη περίπτωση, τα έξυπνα συμβόλαια παρέχουν αυτοματοποίηση της εκτέλεσης μιας συμφωνίας μεταξύ μη αξιόπιστων συμμετεχόντων, δίνοντας τη δυνατότητα μετατροπής των παραδοσιακών συμβολαίων σε ψηφιακά συμβόλαια. Αναλυτικότερα, ένα έξυπνο συμβόλαιο είναι εκτελέσιμος κώδικας που φιλοξενείται στο blockchain, αποθηκεύει πληροφορίες, επεξεργάζεται εισόδους και εγγράφει εξόδους χάρη στις προκαθορισμένες συναρτήσεις του (Khan et al., 2021). Εκτελείται αυτόματα όταν πληρούνται καθορισμένες προϋποθέσεις, χωρίς τη συμμετοχή ενός αξιόπιστου τρίτου μέρους. Ένα έξυπνο συμβόλαιο μπορεί να εκτελεί υπολογισμούς, να αποθηκεύει πληροφορίες, να εκθέτει ιδιότητες για να αντικατοπτρίζει μια κατάσταση που εκτίθεται δημόσια και, εάν χρειάζεται, να στέλνει αυτόματα κεφάλαια σε άλλους λογαριασμούς, δεν χρειάζεται καν να εκτελεί μια οικονομική συνάρτηση (Yaga et al., 2018). Επιπλέον, ένα έξυπνο συμβόλαιο μπορεί να επικαλεστεί και να δημιουργήσει ένα

άλλο έξυπνο συμβόλαιο δημοσιεύοντας ένα μήνυμα, το οποίο δεν καταγράφεται στο blockchain, αλλά χρησιμοποιείται είτε για δημιουργία ενός νέου έξυπνου συμβολαίου είτε για κλήση συναρτήσεων σε άλλα έξυπνα συμβόλαια (Alharby et al., 2018). Τα έξυπνα συμβόλαια χρησιμοποιούνται για τη βελτίωση της διαφάνειας στη διαχείριση δεδομένων, την αποκέντρωση της διαχείρισης συσκευών με περιορισμένους πόρους και την ενεργοποίηση των αλλαγών των όρων της συμφωνίας κατά το χρόνο εκτέλεσης, ενώ εκτελούνται πάνω από ένα αποκεντρωμένο και διαφανές δίκτυο (Khan et al., 2021).

Σε αυτό το κεφάλαιο, παρουσιάζεται μια λεπτομερής περιγραφή των έξυπνων συμβολαίων. Αρχικά, γίνεται ανάλυση της δομής και της διαδικασίας λειτουργίας τους. Στην συνέχεια, γίνεται αναφορά στις πλατφόρμες blockchain που υποστηρίζουν την ανάπτυξη έξυπνων συμβολαίων. Επιπλέον, πραγματοποιείται σύγκριση μεταξύ των δύο πιο διαδεδομένων πλατφορμών στον χώρο. Τέλος, αναλύονται τα ζητήματα ιδιωτικότητας και ασφάλειας, γίνεται αναφορά στα αυτοματοποιημένα εργαλεία ανάλυσης ασφάλειας, και αναλύονται τα νομικά ζητήματα που αφορούν τα έξυπνα συμβόλαια.

3.1. Δομή και λειτουργία ενός έξυπνου συμβολαίου

Τα έξυπνα συμβόλαια συνήθως ορίζονται ως μια συλλογή από εκτελέσιμους κώδικες (functions) που εκτελούνται σε ένα ομότιμο δίκτυο στο πλαίσιο του blockchain, βασίζονται σε συμβάντα (events) και προσδιορίζονται από δεδομένα (state) (Liu et al., 2020; Hu et al., 2021). Με άλλα λόγια, μπορούν να θεωρηθούν ως κρυπτογραφικά αυτόνομα κουτιά που ξεκλειδώνονται μόνο όταν πληρούνται προκαθορισμένες συνθήκες (Liu et al., 2020). Κάθε έξυπνο συμβόλαιο έχει μια τυπική δομή η οποία αποτελείται από τέσσερις φάσεις. Αρχικά υπάρχει η φάση της δημιουργίας, στην συνέχεια η φάση της ανάπτυξης, την οποία ακολουθεί η φάση της εκτέλεσης και τέλος, η τέταρτη φάση της ολοκλήρωσης.

Η πρώτη φάση κατασκευής ενός έξυπνου συμβολαίου είναι αυτή της δημιουργίας (creation), στην οποία εμπλέκονται πολλά μέρη, όπως οι ενδιαφερόμενοι, προγραμματιστές και ενδεχομένως δικηγόροι. Περιλαμβάνει την αρχικοποίηση του έξυπνου συμβολαίου, όπου τα εμπλεκόμενα μέρη καθορίζουν τους όρους και τις προϋποθέσεις της σύμβασης. Η επίτευξη της συμφωνίας πολλές φορές απαιτεί την

βοήθεια δικηγόρων ή νομικών συμβούλων. Στην συνέχεια, οι προγραμματιστές μετατρέπουν αυτήν τη συμφωνία σε κώδικα με την μορφή εντολών «if…then…else», χρησιμοποιώντας μια γλώσσα προγραμματισμού που υποστηρίζεται από την επιλεγμένη πλατφόρμα blockchain (Kemmoe et al., 2020). Παρόμοια με την διαδικασία ανάπτυξης λογισμικού, η διαδικασία της μετατροπής ενός έξυπνου συμβολαίου σε κώδικα αποτελείται από τον σχεδιασμό, την υλοποίηση και την επικύρωση, δηλαδή την δοκιμή (testing) (Zheng et al., 2020).

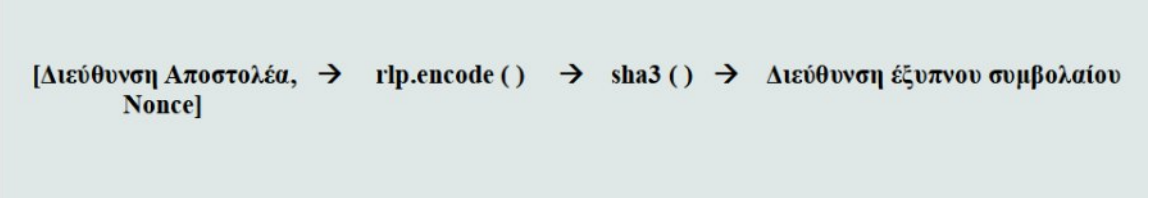
Σημαντικό είναι να σημειωθεί πως για να αναπτύξει ένας χρήστης ένα έξυπνο συμβόλαιο στο blockchain χρειάζεται έναν λογαριασμό, δηλαδή μια διεύθυνση πορτοφολιού. Όπως έχει αναφερθεί στο προηγούμενο κεφάλαιο, ένα ψηφιακό πορτοφόλι χρησιμοποιείται για τη δημιουργία και αποθήκευση των κρυπτογραφικών κλειδιών καθώς και των σχετικών διευθύνσεων, με το δημόσιο κλειδί να χρησιμοποιείται ως αναγνωριστικό ενός λογαριασμού, δηλαδή ως διεύθυνση, και το ιδιωτικό κλειδί να χρησιμοποιείται για την ψηφιακή υπογραφή των συναλλαγών. Η μαθηματική σύνδεση μεταξύ του δημόσιου και του ιδιωτικού κλειδιού επιτρέπει την πραγματοποίηση ελέγχου σχετικά με το ποιος υπέγραψε τα δεδομένα, καθώς και ότι τα δεδομένα που υπογράφηκαν δεν έχουν αλλοιωθεί (Hill et al., 2018).

Σχετικά με τα ψηφιακά πορτοφόλια, υπάρχουν πέντε διαφορετικοί τύποι, τα πορτοφόλια υπολογιστών (desktop wallets), τα πορτοφόλια ιστού (web wallets), τα πορτοφόλια υλικού (hardware wallets), τα πορτοφόλια κινητών συσκευών (mobile wallets) και τα πορτοφόλια χαρτιού (paper wallets). Στην πρώτη περίπτωση το πορτοφόλι είναι λογισμικό εγκατεστημένο στον υπολογιστή του χρήστη με τα ιδιωτικά κλειδιά να αποθηκεύονται σε αυτόν, συνεπώς πρόσβαση στα ιδιωτικά κλειδιά έχει ο ιδιοκτήτης του μηχανήματος στο οποίο είναι εγκατεστημένο το λογισμικό του πορτοφολιού (Hill et al., 2018). Στην δεύτερη περίπτωση, τα πορτοφόλια ιστού βασίζονται στο cloud και είναι προσβάσιμα από οποιαδήποτε συσκευή μέσω της χρήσης προγραμμάτων περιήγησης όπως για παράδειγμα Google Chrome και Firefox, με τα ιδιωτικά κλειδιά να αποθηκεύονται στον διακομιστή των αντίστοιχων παρόχων υπηρεσιών (Moniruzzaman et al., 2020). Όσον αφορά τα πορτοφόλια υλικού, πρόκειται για φυσικά πορτοφόλια που είναι μικρά και φορητά στη φύση, όπως μονάδες USB, τα οποία έχουν κατασκευαστεί ειδικά για την αποθήκευση και τον χειρισμό των ιδιωτικών κλειδιών (Hill et al., 2018).

Επόμενη περίπτωση, τα πορτοφόλια για κινητά τηλέφωνα, τα οποία είναι εφαρμογές σχεδιασμένες για κινητές συσκευές, τόσο για λειτουργικά συστήματα Android όσο και iOS, στις οποίες αποθηκεύονται τα ιδιωτικά κλειδιά και οι σχετικές διευθύνσεις. Η δημοτικότητάς τους αυξάνεται μέρα με τη μέρα καθώς αυξάνεται η χρήση των έξυπνων κινητών συσκευών (smartphones) (Moniruzzaman et al., 2020). Τέλος, τα πορτοφόλια χαρτιού αναφέρονται στα ιδιωτικά κλειδιά που έχουν εκτυπωθεί σε ένα χαρτί και χρησιμοποιούνται κυρίως ως αντίγραφα ασφαλείας.

Εικόνα 3.1. Πορτοφόλι χαρτιού Ethereum (Moniruzzaman et al., 2020)

Η δεύτερη φάση αφορά την ανάπτυξη (deployment) των επικυρωμένων έξυπνων συμβολαίων σε πλατφόρμες blockchain, δηλαδή την δημοσίευση και αποθήκευση του κώδικα στο blockchain. Μόλις αναπτυχθεί, κάθε έξυπνο συμβόλαιο εκχωρείται σε μια διεύθυνση 160-bit και εκτελείται κάθε φορά που δημιουργείται μια συναλλαγή χρησιμοποιώντας τη διεύθυνση αυτή (Alharby et al., 2018). Η διεύθυνση του έξυπνου συμβολαίου καθορίζεται από τη διεύθυνση πορτοφολιού του αποστολέα και από το nonce, έναν ακέραιο αριθμό που αυξάνεται κάθε φορά που η διεύθυνση στέλνει οποιαδήποτε συναλλαγή, δηλαδή, την στιγμή που έχει αναπτυχθεί το έξυπνο συμβόλαιο το nonce ισούται με 0, αφού το έξυπνο συμβόλαιο στείλει την πρώτη συναλλαγή το nonce θα αυξηθεί στο 1 κ.ο.κ. (Das, 2021). Πιο συγκεκριμένα, το nonce και η διεύθυνση του αποστολέα τοποθετούνται στον πίνακα και στη συνέχεια κωδικοποιούνται με την συνάρτηση rlp.encode(), μετά το αποτέλεσμα της συνάρτησης αυτής κατακερματίζεται με την συνάρτηση κατακερματισμού sha3() παράγοντας δεδομένα 32 Byte, και η διεύθυνση του έξυπνου συμβολαίου χρησιμοποιεί τα τελευταία 20 Byte αυτών των δεδομένων κατακερματισμού (Das, 2021).



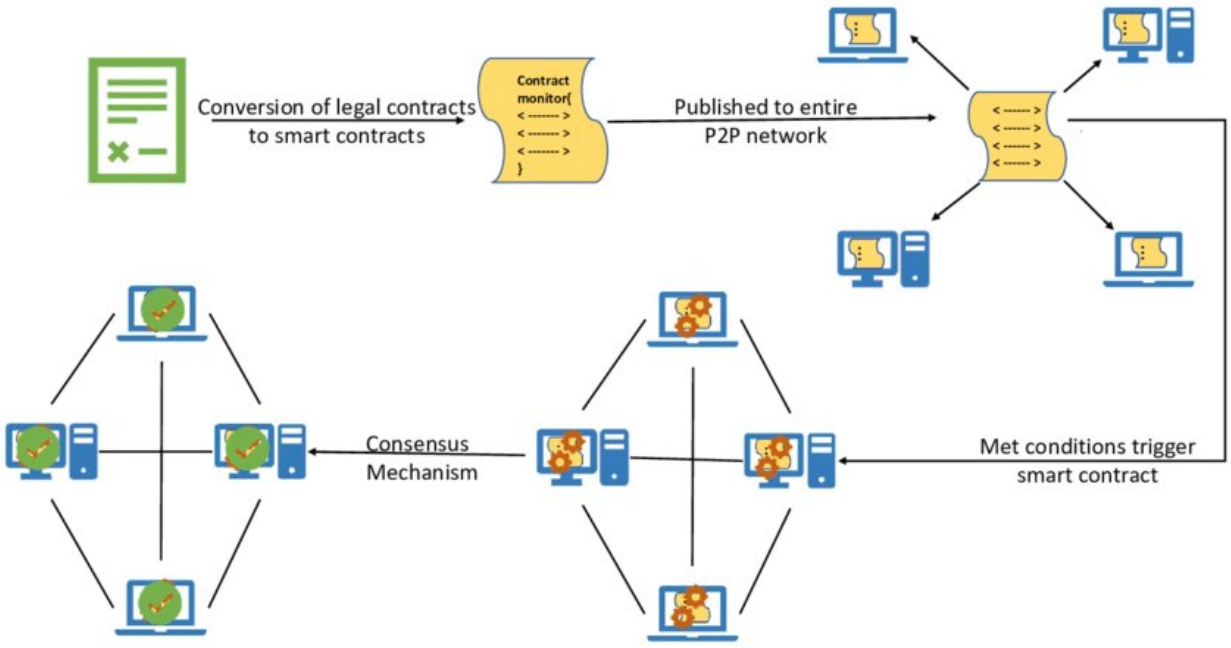
Εικόνα 3.2. Μηχανισμός δημιουργίας της διεύθυνσης ενός έξυπνου συμβολαίου

Μετά την αποθήκευση του έξυπνου συμβολαίου στο blockchain καμία τροποποίηση δεν είναι εφικτή, έτσι οποιαδήποτε ενημέρωση απαιτεί από τους προγραμματιστές να δημιουργήσουν και να δημοσιεύσουν μια νέα έκδοση του έξυπνου συμβολαίου. Μόλις μεταφορτωθεί στην πλατφόρμα blockchain το έξυπνο συμβόλαιο βρίσκεται στην αρχική του κατάσταση, η οποία αντιπροσωπεύει τις αρχικές τιμές των εσωτερικών μεταβλητών του συγκεκριμένου έξυπνου συμβολαίου (Kemmoe et al., 2020).

Σειρά έχει η τρίτη φάση, η οποία αφορά την εκτέλεση (execution) του έξυπνου συμβολαίου. Κάθε συναλλαγή θα πρέπει να περιέχει τη συνάρτηση του έξυπνου συμβολαίου που επιθυμεί ο χρήστης να χρησιμοποιήσει, καθώς και τα ορίσματα της συνάρτησης αυτής (Kemmoe et al., 2020). Μόλις το δίκτυο blockchain λάβει τη συναλλαγή επαληθεύονται διάφορες συνθήκες, όπως η ψηφιακή υπογραφή, η συναλλαγή χαρακτηρίζεται νόμιμη, το έξυπνο συμβόλαιο εκτελείται και η συναλλαγή προστίθεται σε μπλοκ από έναν κόμβο εξόρυξης (Hewa et al., 2021). Στην συνέχεια το επιβεβαιωμένο μπλοκ διαδίδεται εντός του δικτύου και επικυρώνεται από κάθε κόμβο με βάση το πρωτόκολλο συναίνεσης. Μόλις ολοκληρωθεί η διαδικασία συναίνεσης το μπλοκ προσαρτάται στο δίκτυο. Για πολλές υλοποιήσεις blockchain, οι κόμβοι δημοσίευσης εκτελούν τον κώδικα του έξυπνου συμβολαίου ταυτόχρονα με τη δημοσίευση νέων μπλοκ, ενώ υπάρχουν ορισμένες υλοποιήσεις blockchain στις οποίες υπάρχουν κόμβοι δημοσίευσης που δεν εκτελούν κώδικα έξυπνου συμβολαίου, αλλά επικυρώνουν τα αποτελέσματα των κόμβων που εκτελούν (Yaga et al., 2018).

Τέλος, η τέταρτη φάση αφορά την ολοκλήρωση (completion) του έξυπνου συμβολαίου και περιλαμβάνει την προσάρτηση του μπλοκ στο blockchain, μόλις ολοκληρωθεί η διαδικασία συναίνεσης. Μετά την εκτέλεση ενός έξυπνου συμβολαίου οι καταστάσεις όλων των εμπλεκομένων ενημερώνονται. Οι συναλλαγές κατά την εκτέλεση των έξυπνων συμβολαίων καθώς και των ενημερωμένων καταστάσεων αποθηκεύονται σε

blockchains, ενώ τα ψηφιακά στοιχεία έχουν μεταφερθεί από τον ένα λογαριασμό στον άλλο, ολοκληρώνοντας τον κύκλο ζωής του έξυπνου συμβολαίου (Zheng et al., 2020).



Εικόνα 3.3. Κύκλος ζωής ενός έξυπνου συμβολαίου (Mohanty, 2022)

Προκειμένου να γίνει κατανοητή η παραπάνω διαδικασία θα εξετάσουμε ως παράδειγμα την περίπτωση μεταβίβασης της ιδιοκτησίας ενός διαμερίσματος. Έστω ότι ο Αγοραστής θέλει να αγοράσει ένα διαμέρισμα από τον Πωλητή. Παραδοσιακά, μια τέτοια συμφωνία θα απαιτούσε την συμμετοχή πολλών μεσαζόντων για να ολοκληρωθεί, όπως έναν μεσίτη, έναν συμβολαιογράφο, ένα δικηγόρο κλπ., αυξάνοντας το απαιτούμενο κόστος και τον απαιτούμενο χρόνο. Ας υποθέσουμε ότι όλα τα εμπλεκόμενα μέρη αποφασίσουν να προχωρήσουν την διαδικασία επιλέγοντας την χρήση ενός έξυπνου συμβολαίου. Ο καθένας έχει μια διεύθυνση, δηλαδή ένα δημόσιο κλειδί, από το οποίο αναγνωρίζεται. Αρχικά συμφωνούν με τους όρους αγοραπωλησίας οι οποίοι υποβάλλονται στο έξυπνο συμβόλαιο, το οποίο υπογράφεται ψηφιακά με το ιδιωτικό κλειδί του Πωλητή. Ο Αγοραστής μεταφέρει το απαιτούμενο χρηματικό ποσό από την διεύθυνση του στην διεύθυνση του Πωλητή υπογράφοντας την σύμβαση με το ιδιωτικό του κλειδί. Η συναλλαγή επαληθεύεται από κάθε κόμβο του δικτύου προκειμένου για να επικυρωθούν η εγκυρότητα της ιδιοκτησίας και η μεταφορά του χρηματικού ποσού. Εφόσον η συναλλαγή επαληθευτεί, το χρηματικό ποσό αποδεσμεύεται αυτόματα στο πορτοφόλι

του Πωλητή και ο Αγοραστής λαμβάνει τον τίτλο ιδιοκτησίας του ακινήτου. Με την ολοκλήρωση του έξυπνου συμβολαίου η μεταβίβαση του ακινήτου και η ενημερωμένη ιδιοκτησία καταγράφονται στο blockchain.

3.2. Πλατφόρμες ανάπτυξης έξυπνων συμβολαίων

Τα έξυπνα συμβόλαια μπορούν να αναπτυχθούν σε διάφορες πλατφόρμες blockchain όπως για παράδειγμα το Bitcoin, Ethereum, NXT, Hyperledger Fabric, Rootstock, NEM, Waves, Stellar και Corda, με την κάθε μία να προσφέρει διαφορετικές δυνατότητες. Σε αυτή την ενότητα γίνεται μια αναφορά σε μερικές από αυτές τις πλατφόρμες, όπως επίσης παρουσιάζεται μια σύγκριση μεταξύ των Ethereum και Hyperledger Fabric, των πιο διαδεδομένων πλατφορμών ανάπτυξης έξυπνων συμβολαίων.

Bitcoin. Όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, είναι ένα permissionless δίκτυο blockchain με κύριο στόχο την μεταφορά κρυπτονομισμάτων και την καταγραφή συναλλαγών. Ο ανοιχτός και αμετάβλητος χαρακτήρας του έχει εμπνεύσει την ανάπτυξη πρωτοκόλλων που εφαρμόζουν έξυπνα συμβόλαια. Η γλώσσα προγραμματισμού που χρησιμοποιείται στο Bitcoin, η C++ (Bitcoin-core), είναι αυστηρά περιορισμένη, έτσι μόνο απλά έξυπνα συμβόλαια, όπως για παράδειγμα το κλείδωμα μιας πληρωμής μέχρι μια συγκεκριμένη ημερομηνία, μπορούν να εφαρμόζονται απευθείας στο Bitcoin (Ante, 2021).

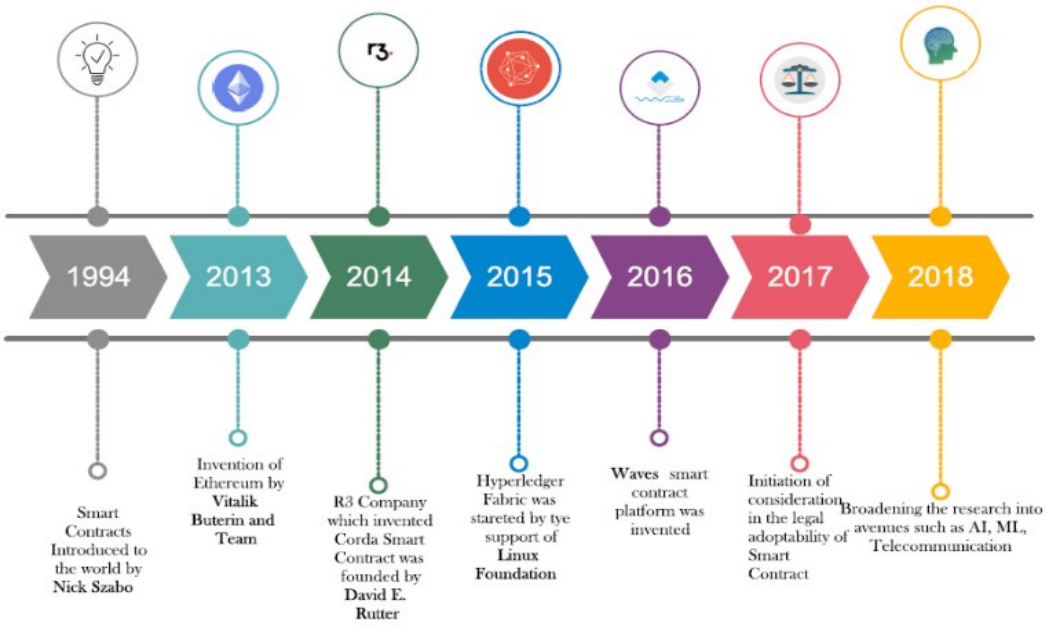
NXT. Είναι μια πλατφόρμα blockchain ανοιχτού κώδικα που βασίζεται εξ ολοκλήρου στο πρωτόκολλο συναίνεσης Proof-of-Stake (Popov, 2016). Μέχρι σήμερα πολλά έξυπνα συμβόλαια έχουν αναπτυχθεί και περιλαμβάνονται στην συγκεκριμένη πλατφόρμα. Η πλατφόρμα NXT χρησιμοποιεί κυρίως τη δική της προσαρμοσμένη γλώσσα προγραμματισμού για τη σύνταξη έξυπνων συμβολαίων, γνωστή ως NXTScript ή Nxt-Asset-Exchange. Η NXTScript έχει σχεδιαστεί ειδικά για απλότητα, ασφάλεια και προβλεψιμότητα, και είναι σκόπιμα λιγότερο περίπλοκη από ορισμένες άλλες γλώσσες προγραμματισμού που χρησιμοποιούν άλλες πλατφόρμες blockchain και χαρακτηρίζονται ως Turing-complete. Ωστόσο, το γεγονός ότι η γλώσσα προγραμματισμού αυτή δεν είναι Turing-complete, σημαίνει ότι μπορούν να αξιοποιηθούν μόνο τα υπάρχοντα πρότυπα και δεν μπορεί να αναπτυχθεί εξατομικευμένο έξυπνο συμβόλαιο (Khan et al., 2021).

Ethereum. Αποτελεί την μεγαλύτερη και πιο δημοφιλή πλατφόρμα ανάπτυξης έξυπνων συμβολαίων. Είναι ένα permissionless δίκτυο blockhain που διαθέτει το δικό του κρυπτονόμισμα, το Ether. Το Ether χρησιμοποιείται για χρεώσεις συναλλαγών ώστε να προστατεύεται το δίκτυο από κακόβουλες εκτελέσεις έξυπνων συμβολαίων, όπως επίσης λειτουργεί ως κίνητρο για τους κόμβους εξόρυξης ώστε να δημιουργήσουν νέα μπλοκ, καθώς υπάρχει σαν ανταμοιβή σε όσους επικυρώνουν συναλλαγές (Cai et al., 2018).

Εκτός από την ικανότητα μεταφοράς κρυπτονομίσματος, το Ethereum εστιάζει στην παροχή μιας υποδομής blockchain ως πλατφόρμα ή ως θεμέλιο για το σχεδιασμό διαφόρων ειδών αποκεντρωμένων εφαρμογών καθολικού που καλούνται "Dapps" (Hamilton, 2020). Αυτό επιτυγχάνεται με τη βοήθεια της εικονικής μηχανής, EVM (Ethereum Virtual Machine), που είναι το περιβάλλον εκτέλεσης για έξυπνα συμβόλαια, με κάθε κόμβο του δικτύου να εκτελεί μια υλοποίησή της και να ακολουθεί τις ίδιες οδηγίες, ώστε να διατηρηθεί η συναίνεση στο blockchain (Khan et al., 2021). Ethereum έξυπνα συμβόλαια μπορούν να αναπτυχθούν σε πολλές γλώσσες προγραμματισμού που χαρακτηρίζονται ως Turing-complete, όπως η Solidity. Κατά την μεταγλώττιση, ο πηγαίος κώδικας του έξυπνου συμβολαίου μετατρέπεται σε μορφή bytecode, ώστε να μπορεί να ερμηνευθεί από την EVM, και δημιουργείται η δυαδική διεπαφή (ABI) του συμβολαίου (Alharby et al., 2018). Το ABI είναι μια συμβολοσειρά JSON που περιγράφει τη σύνθεση της σύμβασης, δηλαδή τις συναρτήσεις καθώς και τους τύπους παραμέτρων κάθε συνάρτησης (Lee, 2019), και είναι ο τυπικός τρόπος αλληλεπίδρασης με συμβόλαια στο οικοσύστημα Ethereum, τόσο εκτός του blockchain όσο και για αλληλεπίδραση μεταξύ συμβολαίων.

Hyperledger Fabric. Είναι μια πλατφόρμα τεχνολογίας κατανεμημένου καθολικού, ανοιχτού κώδικα, που υποστηρίζει έξυπνα συμβόλαια, με μεγάλο μέρος της αρχικής ανάπτυξής του να έχει γίνει από την IBM, για χρήση σε επίπεδο επιχείρησης (Hamilton, 2020). Σε αντίθεση με τις πλατφόρμες που αναφέρθηκαν παραπάνω που είναι permissionless και μπορεί οποιοσδήποτε να συμμετάσχει στο δίκτυο, η πλατφόρμα Hyperledger Fabric είναι permissioned, δηλαδή, μόνο ορισμένοι πιστοποιημένοι οργανισμοί μπορούν να συμμετάσχουν μέσω συνδρομής, και το δίκτυο αποτελείται από τους ομότιμους οι οποίοι ανήκουν στους οργανισμούς αυτούς. Το καθολικό αναπτύχθηκε στην κορυφή της βάσης δεδομένων CouchDB no-sql, και το έξυπνο συμβόλαιο, που

ονομάζεται Chain-Code στην ορολογία Hyperledger, μπορεί να αναπτυχθεί χρησιμοποιώντας γλώσσες προγραμματισμού Java, NodeJs και GoLang (Hewa et al., 2021). Η πλατφόρμα αυτή προσφέρει ευελιξία για ένα ευρύ σύνολο περιπτώσεων βιομηχανικής χρήσης και έχει στόχο να διασυνδέει τα μέλη του δικτύου της σε όλους τους επιχειρηματικούς τομείς.



Εικόνα 3.4. Χρονοδιάγραμμα εξέλιξης των έξυπνων συμβολαίων (Hewa et al., 2021)

3.2.1 Σύγκριση μεταξύ πλατφορμών Ethereum και Hyperledger Fabric

Η ανάλυσή του Ante (2021) αποκάλυψε 41 διαφορετικές πλατφόρμες έξυπνων συμβολαίων, και αυτό μόνο στις υποκείμενες συζητήσεις της έρευνας, με τις πλατφόρμες Ethereum και Hyperledger Fabric να επιλέγονται συχνότερα από τις υπόλοιπες, η μεν για την ανάπτυξη δημοσίων έργων blockchain και η δε για την ανάπτυξη ιδιωτικών έργων blockchain. Για τον λόγο αυτό, στην συγκεκριμένη υποενότητα παρουσιάζεται μια σύγκριση μεταξύ αυτών των πλατφορμών.

Οι πλατφόρμες Ethereum και Hyperledger Fabric διαφέρουν σε πολλές πτυχές. Αρχικά, η βασική τους διαφορά εντοπίζεται στον τύπο του δικτύου blockchain που χρησιμοποιούν. Το Ethereum είναι ένα permissionless δίκτυο, στο οποίο οποιοσδήποτε μπορεί να συμμετάσχει χωρίς την ανάγκη για επικύρωση ταυτότητας, ενώ το

Hyperledger Fabric είναι ένα permissioned δίκτυο, όπου οι χρήστες πρέπει να έχουν επικυρωμένες ταυτότητες για να συμμετάσχουν.

Στην περίπτωση του Ethereum, για την συμμετοχή στο δίκτυο πρωταρχικό ρόλο διαδραματίζουν οι λογαριασμοί Ethereum, που είναι δύο ειδών. Το πρώτο είδος είναι οι Εξωτερικοί Ιδιόκτητοι Λογαριασμοί (Externally Owned Accounts ή EOA), οι οποίοι ελέγχονται από το αντίστοιχο ιδιωτικό κλειδί του ιδιοκτήτη και διατηρούν ένα υπόλοιπο (balance). Μπορούν να χρησιμοποιηθούν για συναλλαγές, για μεταφορά χρημάτων ή για επίκληση σε άλλα έξυπνα συμβόλαια (Alharby et al., 2018). Το δεύτερο είδος είναι οι Λογαριασμοί Συμβολαίου (Contract Accounts), οι οποίοι ελέγχονται από την λογική του κώδικα του έξυπνου συμβολαίου και έχουν υπόλοιπο (balance), χώρο αποθήκευσης (storage) και κατάσταση (state) (Alharby et al., 2018). Κάθε φορά που ένας λογαριασμός συμβολαίου λαμβάνει ένα μήνυμα ο κώδικάς του ενεργοποιείται, επιτρέποντάς του να διαβάζει και να γράφει στον εσωτερικό χώρο αποθήκευσης και να στέλνει άλλα μηνύματα σε άλλο λογαριασμό συμβολαίου (Buterin, 2014). Στην περίπτωση του Hyperledger Fabric, για να συμμετάσχουν οι χρήστες στο σύστημα, πρέπει να εγγραφούν στο blockchain χρησιμοποιώντας μια υπηρεσία συνδρομής που παρέχεται από έναν Πάροχο Υπηρεσιών Μέλους (Membership Service Provider - MSP). Αυτοί οι MSP είναι ρυθμισμένοι στο πλαίσιο του συστήματος, και μπορεί να υπάρχει περισσότερο από ένας MSP για κάθε χρήστη, ωστόσο, όλα τα μέλη πρέπει να έχουν επιτυχώς αποκτήσει πρόσβαση μέσω ενός ή περισσότερων MSP (Hill et al., 2018).

Μια ακόμα διαφορά αφορά την γλώσσα προγραμματισμού που χρησιμοποιείται για την σύνταξη έξυπνων συμβολαίων, με το Ethereum να χρησιμοποιεί κυρίως την Solidity ενώ το Hyperledger Fabric να υποστηρίζει έξυπνα συμβόλαια πολλών γλωσσών, όπως Java, NodeJs και GoLang. Σχετικά με την εκτέλεση του κώδικα του συμβολαίου, ο πηγαίος κώδικας στο Ethereum περιλαμβάνεται σε μια συναλλαγή, η οποία διαδίδεται στο ομότιμο δίκτυο και οποιοσδήποτε κόμβος εξόρυξης λαμβάνει αυτήν τη συναλλαγή μπορεί να την εκτελέσει στην τοπική εικονική μηχανή του (Buterin, 2014). Κάθε συναλλαγή απαιτείται να καλύψει το υπολογιστικό κόστος του οποίου η θεμελιώδης μονάδα είναι το gas, το οποίο καταναλώνεται κατά τη διάρκεια της διαδικασίας ανάπτυξης και εκτέλεσης των έξυπνων συμβολαίων (Liu et al., 2020). Κάθε μία από τις συναρτήσεις που εκτελούνται σε μια συναλλαγή σχετίζεται με μια ποσότητα gas που

αντιπροσωπεύει την πολυπλοκότητα της διαδικασίας του έξυπνου συμβολαίου, δηλαδή, όσο πιο περίπλοκη είναι η διαδικασία του έξυπνου συμβολαίου, τόσο μεγαλύτερη είναι η αξία της κατανάλωσης gas (Li et al., 2020). Η ελάχιστη τιμή του gas είναι 1 Wei, η μικρότερη μονάδα Ether, όπου 1 Ether ισούται με 10^{18} Wei. Στο Hyperledger Fabric, όταν δημιουργείται μια συναλλαγή από την εφαρμογή, η συναλλαγή εκτελείται και υπογράφεται μόνο από καθορισμένους ομότιμους, οι οποίοι αφού λάβουν την πρόταση συναλλαγής από τη εφαρμογή την εκτελούν ο καθένας ανεξάρτητα, επικαλούμενοι το Chain-Code στο οποίο αναφέρεται η συναλλαγή (Androulaki et al, 2018). Για ασφάλεια, το Chain-Code εκτελείται σε περιβάλλον κοντέινερ, για παράδειγμα Docker, για απομόνωση.

Τέλος, μια διαφορά που αξίζει να σημειωθεί είναι πως η πλατφόρμα Ethereum, όπως έχει αναφερθεί παραπάνω, έχει δικό της εσωτερικό κρυπτονόμισμα, το Ether, ενώ το Hyperledger δεν έχει εκδώσει ποτέ δικό του κρυπτονόμισμα, κι αυτό οφείλεται στο γεγονός ότι το Hyperledger δεν είναι το ίδιο ένα blockchain, αλλά μια συλλογή τεχνολογιών που χρησιμοποιούνται για τη δημιουργία νέων blockchain, οι οποίες σχεδιάστηκαν και κατασκευάστηκαν ρητά για περιπτώσεις εταιρικής χρήσης και όχι για τις δημόσιες αγορές (Hill et al., 2018).

3.3. Ζητήματα ασφάλειας

Παρόλο που οι αρχιτεκτονικές των δικτύων blockchain και των έξυπνων συμβολαίων προστατεύονται από την χρήση κρυπτογραφίας και πρωτοκόλλων, ο κώδικας των έξυπνων συμβολαίων περιέχει σφάλματα (bugs) και τρωτά σημεία (vulnerabilities) τα οποία μπορεί να οδηγήσουν σε σημαντικά προβλήματα, όπως απώλεια πολλών χρημάτων ή διαρροή ιδιωτικών δεδομένων (Rouhani & Deters, 2019). Ένα από τα πιο γνωστά παραδείγματα είναι η επίθεση DAO τον Ιούνιο του 2016 που προκλήθηκε από ένα σφάλμα στον κώδικα του έξυπνου συμβολαίου και είχε ως αποτέλεσμα την απώλεια του ενός τρίτου των περιουσιακών στοιχείων του οργανισμού (Kemmoe et al., 2020). Μια άλλη επίθεση έγινε στο SmartBillions, που παρουσίασε ένα πλήρως αποκεντρωμένο και διαφανές σύστημα λαχειοφόρου αγοράς, όταν ένας εισβολέας χειρίστηκε επιτυχώς τον κατακερματισμό μπλοκ της συνάρτησης λοταρίας του έξυπνου συμβολαίου και εξανάγκασε το αποτέλεσμα υπέρ του, λαμβάνοντας 400 Ether (Khan et al., 2021). Άλλοι λόγοι που μπορούν να επιτρέψουν την πραγματοποίηση επιθέσεων είναι σφάλματα

προγραμματισμού, περιορισμοί στις γλώσσες προγραμματισμού και κενά ασφαλείας (Hewa et al., 2021). Όπως γίνεται αντιληπτό, η εστίαση στα ζητήματα ασφαλείας καθίσταται υψίστης σημασίας, καθώς επηρεάζουν την λειτουργικότητα ολόκληρου του blockchain και μπορούν να οδηγήσουν σε πολλά προβλήματα που αφορούν την ακρίβεια του δικτύου, την απώλεια εγγενούς κρυπτονομίσματος, ακόμα και τον τερματισμό της διαθεσιμότητας του συστήματος (Hewa et al., 2021).

Σε αυτή την ενότητα παρουσιάζονται οι κυριότερες ευπάθειες και τα σφάλματα που μπορούν να οδηγήσουν σε επιθέσεις, καθώς και τα αυτοματοποιημένα εργαλεία ανάλυσης ασφάλειας που υπάρχουν για έξυπνα συμβόλαια. Οι περισσότερες περιπτώσεις χρήσης και επιθέσεις που συναντώνται στην βιβλιογραφία αναφέρονται στα έξυπνα συμβόλαια της πλατφόρμας Ethereum, για τον λόγο αυτό θα επικεντρωθούμε στην συγκεκριμένη πλατφόρμα.

Ευπάθεια επανεισόδου (Reentrancy vulnerability). Όταν ένα συμβόλαιο καλεί ένα άλλο συμβόλαιο η τρέχουσα εκτέλεση του συμβολαίου περιμένει μέχρι την ολοκλήρωση του συμβολαίου που έχει κληθεί, ουσιαστικά, μεταβιβάζει τον έλεγχο σε αυτό το άλλο συμβόλαιο (Wohrer & Zdun, 2018). Η ατομικότητα και η διαδοχικότητα των συναλλαγών μπορεί να οδηγήσει τους προγραμματιστές να πιστέψουν ότι, όταν καλείται μια μη αναδρομική συνάρτηση, δεν μπορεί να επανεισαχθεί πριν από τη λήξη της, ωστόσο, αυτό δεν συμβαίνει πάντα, γιατί ο εναλλακτικός μηχανισμός μπορεί να επιτρέψει στον χρήστη να επανεισάγει μια συνάρτηση κλήσης (Atzei et al., 2017). Αυτό δίνει την ευκαιρία σε έναν εισβολέα να προσπαθήσει να χειραγωγήσει την κατάστασή του συμβολαίου ή να παραβιάσει τη ροή ελέγχου μέσω κακόβουλου κώδικα (Wohrer & Zdun, 2018). Τέτοια περίπτωση αποτελεί η επίθεση DAO, που αναφέρθηκε στην εισαγωγή αυτής της ενότητας.

Λανθασμένος χειρισμός εξαιρέσεων (Mishandled exceptions). Ορισμένες συναρτήσεις χαμηλού επιπέδου στην γλώσσα προγραμματισμού Solidity, όπως η send που χρησιμοποιείται για την αποστολή Ether, δεν δημιουργούν εξαίρεση σε περίπτωση αποτυχίας, αλλά αναφέρουν την κατάσταση επιστρέφοντας μια τιμή boolean (Perez & Livshits, 2021). Υπάρχουν αρκετές περιπτώσεις όπου μπορεί να τεθεί μια εξαίρεση, όπως εάν η εκτέλεση ξεμείνει από gas, εάν η στοίβα κλήσεων φτάνει στο όριό της, ή

όταν εκτελείται η εντολή throw (Atzei et al., 2017). Ωστόσο, δεν υπάρχει ομοιομορφία στον τρόπο με τον οποίο η Solidity χειρίζεται τις εξαιρέσεις. Στην περίπτωση που η τιμή της κατάστασης είναι ψευδής, αλλά ο χρήστης συνεχίζει την εκτέλεση της συναλλαγής ακόμη και αν η πληρωμή αποτύχει, οδηγείται σε σοβαρή επίθεση ψευδούς ανανέωσης (False Top-Up Attack) (Duan et al., 2022). Σε μια τέτοια περίπτωση, η ανταλλαγή δεν λαμβάνει τα πραγματικά tokens, η εκτέλεση της συναλλαγής δεν έφερε εξαίρεση και ο χρήστης έλαβε το πραγματικό αρχείο επαναφόρτισης, με αποτέλεσμα οι χρήστες να μπορούν να κλέψουν πραγματικά περιουσιακά στοιχεία (Duan et al., 2022).

Δεσμευμένο νόμισμα Ether (Locked Ether). Όπως κάθε λογαριασμός στο Ethereum, έτσι και τα έξυπνα συμβόλαια που βασίζονται σε αυτό μπορούν να λαμβάνουν Ether. Ωστόσο, υπάρχουν αρκετοί λόγοι για τους οποίους τα ληφθέντα κεφάλαια ενδέχεται να δεσμευτούν μόνιμα στο συμβόλαιο. Ο πιο συνηθισμένος λόγος είναι όταν το συμβόλαιο εξαρτάται από ένα εξωτερικό συμβόλαιο που δεν υπάρχει πλέον. Μια τέτοια περίπτωση μπορεί να συμβεί όταν μια σύμβαση χρησιμοποιεί μια άλλη σύμβαση ως βιβλιοθήκη για να εκτελέσει ορισμένες ενέργειες για λογαριασμό της (Perez & Livshits, 2021). Εάν το εξωτερικό συμβόλαιο έχει καταστραφεί χρησιμοποιώντας την εντολή SELFDESTRUCT της EVM, δηλαδή ο κώδικάς του έχει αφαιρεθεί και τα χρήματά του έχουν μεταφερθεί, και αυτός ήταν ο μόνος τρόπος για το συμβόλαιο να στείλει Ether, αυτό θα έχει ως αποτέλεσμα το μόνιμο "κλείδωμα" των κεφαλαίων (Perez & Livshits, 2021). Αυτό συνέβη το 2017, όταν ένα συμβόλαιο που χρησιμοποιήθηκε ως βιβλιοθήκη από το Parity Wallet δεν είχε αρχικοποιηθεί σωστά και μπορούσε να καταστραφεί από οποιονδήποτε. Χάκερς εκμεταλλεύτηκαν αυτό το κενό ασφαλείας και η καταστροφή της βιβλιοθήκης είχε ως αποτέλεσμα το πάγωμα πάνω από 500.000 Ether σε 587 πορτοφόλια (Duan et al., 2022).

Εξάρτηση από την σειρά εκτέλεσης συναλλαγών (Transaction Order Dependency). Στην πλατφόρμα Ethereum οι χρήστες στέλνουν συναλλαγές μέσω των οποίων επικαλούνται συναρτήσεις σε ένα έξυπνο συμβόλαιο, ενώ οι κόμβοι εξόρυξης του δικτύου συσκευάζουν τις συναλλαγές σε μπλοκ (Zheng et al., 2020). Οι κόμβοι εξόρυξης επιλέγουν τις συναλλαγές που θα συσκευάσουν σύμφωνα με την μεγαλύτερη ανταμοιβή που θα λάβουν, δηλαδή τα τέλη εκτέλεσης που καταβάλλονται από τους χρήστες που επικαλούνται τις συναρτήσεις (Atzei et al., 2017). Επομένως, η ακολουθία μιας σειράς

συναλλαγών που συσκευάζονται στο μπλοκ δεν είναι η ίδια με τη σειρά δημιουργίας συναλλαγών. Κατά συνέπεια, ο κώδικας της σύμβασης δεν μπορεί να γνωρίζει τη σειρά των συναλλαγών (Duan et al., 2022). Αυτό δημιουργεί πρόβλημα, καθώς η σειρά δύο ή περισσότερων συναλλαγών που επικαλούνται το ίδιο έξυπνο συμβόλαιο επηρεάζει το τελικό αποτέλεσμα, δηλαδή τη νέα κατάσταση του blockchain (Rouhani & Deters, 2019), δίνοντας σε έναν εισβολέα την ευκαιρία να εκμεταλλευτεί αυτήν την ιδιότητα και να πραγματοποιήσει μια επίθεση.

Σφάλματα ακέραιων αριθμών (Integer bugs). Είναι ένας κοινός τύπος σφάλματος σε πολλές γλώσσες προγραμματισμού που αναφέρεται στα σφάλματα που σχετίζονται με την αριθμητική ακέραιων αριθμών, στην συγκεκριμένη περίπτωση, στα έξυπνα συμβόλαια. Τα σφάλματα αυτά ταξινομούνται σε 3 κατηγορίες, (α) αριθμητικά σφάλματα που περιλαμβάνουν υπερχείλιση ακέραιου αριθμού (integer overflow), υπορροή ακέραιου αριθμού (integer underflow) και διαίρεση με το μηδέν, (β) σφάλματα περικοπής που εμφανίζονται κατά τη μετατροπή μεγαλύτερων ακεραίων σε μικρότερους και (γ) σφάλματα που εμφανίζονται κατά τη μετατροπή μεταξύ ενυπόγραφων και ανυπόγραφων ακεραίων (Hu et al., 2021). Στο πλαίσιο των έξυπνων συμβολαίων Ethereum τα συγκεκριμένα σφάλματα μπορεί να έχουν καταστροφικές συνέπειες. Για παράδειγμα, εάν ένας μετρητής βρόχου υπερχειλίσει δημιουργώντας έναν άπειρο βρόχο, τα κεφάλαια μιας σύμβασης θα μπορούσαν να παγώσουν εντελώς (Perez & Livshits, 2021). Τέτοιες περιπτώσεις μπορούν να τις εκμεταλλευτούν εισβολείς και να πραγματοποιήσουν μια επίθεση, όπως έγινε τον Απρίλιο του 2018, όταν σχεδόν 6 δισεκατομμύρια Κινεζικά Γουάν κλάπηκαν από χάκερ λόγω υπερχείλισης ακεραίων στον κώδικα σύμβασης του έργου της αμερικανικής αλυσίδας BEC, γεγονός που μείωσε την αγοραία αξία των tokens σχεδόν σε μηδέν (Duan et al., 2022).

3.3.1. Αυτοματοποιημένα εργαλεία ανάλυσης ασφάλειας για έξυπνα συμβόλαια

Το γεγονός ότι τα έξυπνα συμβόλαια είναι γενικά σχεδιασμένα για να διατηρούν κεφάλαια που εκφράζονται σε Ether τα κάνει πολύ δελεαστικούς στόχους, καθώς μια επιτυχημένη επίθεση μπορεί να επιτρέψει στον εισβολέα να κλέψει άμεσα κεφάλαια από τη σύμβαση (Perez & Livshits, 2021). Αυτό, σε συνδυασμό με τον αμετάβλητο χαρακτήρα των δεδομένων στο blockchain, καθιστά ιδιαίτερα σημαντικό τον διεξοδικό

έλεγχο των έξυπνων συμβολαίων πριν την ανάπτυξη του bytecode τους στο blockchain. Για τον σκοπό αυτό έχουν δημιουργηθεί πολλά αυτοματοποιημένα εργαλεία ανάλυσης που χρησιμοποιούνται για την εκτέλεση ανάλυσης ασφάλειας όταν τα έξυπνα συμβόλαια έχουν σχεδόν ολοκληρωθεί, ανιχνεύοντας πιθανά τρωτά σημεία και σφάλματα, όπως αυτά που συζητήθηκαν παραπάνω.

Τα εργαλεία αυτά χρησιμοποιούν διάφορες τεχνικές για τον εντοπισμό τρωτών σημείων και την ενίσχυση της ασφάλειας των έξυπνων συμβολαίων Ethereum, με τις πιο συχνά χρησιμοποιούμενες τεχνικές να είναι η στατική και η δυναμική ανάλυση. Η στατική ανάλυση περιλαμβάνει την εξέταση του πηγαίου κώδικα της σύμβασης χωρίς την εκτέλεσή του, την ανάλυση της δομής του κώδικα, της ροής ελέγχου, των εκχωρήσεων μεταβλητών και των αλληλεπιδράσεων συναρτήσεων για τον εντοπισμό πιθανών τρωτών σημείων και σφαλμάτων κωδικοποίησης. Από την άλλη, η δυναμική ανάλυση περιλαμβάνει την εκτέλεση του κώδικα του έξυπνου συμβολαίου και την παρακολούθηση της συμπεριφοράς του σε ένα ελεγχόμενο περιβάλλον, όπως ένα δοκιμαστικό δίκτυο ή μια προσομοίωση blockchain. Επιτρέπει την εξερεύνηση διαφορετικών διαδρομών εκτέλεσης, τον εντοπισμό σφαλμάτων χρόνου εκτέλεσης και τον εντοπισμό πιθανών τρωτών σημείων ασφαλείας που μπορεί να προκύψουν κατά την εκτέλεση της σύμβασης. Η δυναμική ανάλυση μπορεί να περιλαμβάνει τεχνικές όπως η συμβολική εκτέλεση, όπου ο κώδικας του συμβολαίου εκτελείται με συμβολικές εισόδους για την παρακολούθηση πιθανών καταστάσεων δεδομένων και την αποκάλυψη πιθανών τρωτών σημείων ή παρακολούθηση του χρόνου εκτέλεσης για την παρατήρηση της συμπεριφοράς του συμβολαίου, των μεταβλητών τιμών και των αλληλεπιδράσεων με άλλα συμβόλαια ή εξωτερικές εξαρτήσεις. Μια ακόμα συχνά χρησιμοποιούμενη τεχνική είναι το Fuzzing, μια τεχνική που περιλαμβάνει τη δημιουργία ενός ευρέος φάσματος τυχαίων ή τροποποιημένων εισόδων για τον έλεγχο των λειτουργιών της σύμβασης και την εξερεύνηση διαφορετικών διαδρομών εκτέλεσης. Η τεχνική Fuzzing βοηθά στον εντοπισμό τρωτών σημείων και απροσδόκητων συμπεριφορών που ενδέχεται να μην ανιχνευθούν μέσω των παραδοσιακών μεθόδων δοκιμών.

Στην βιβλιογραφία συναντώνται πάνω από 40 αυτοματοποιημένα εργαλεία ανάλυσης ασφαλείας για έξυπνα συμβόλαια, που κυρίως στηρίζονται στις παραπάνω τεχνικές ανάλυσης. Σε αυτό το σημείο θα πραγματοποιηθεί μια σύντομη ανάλυση των πιο διαδεδομένων εργαλείων ανοιχτού κώδικα.

OYENTE. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που δημιουργήθηκε το 2016 και εφαρμόστηκε σε Python. Αποτελεί ένα από τα πρώτα αυτοματοποιημένα εργαλεία ανάλυσης ασφάλειας ειδικά προσαρμοσμένα για έξυπνα συμβόλαια Ethereum, και έχει χρησιμεύσει ως σημαντική πηγή έμπνευσης για πολλά άλλα έργα. Το OYENTE χρησιμοποιεί συμβολική εκτέλεση και μια τεχνική γνωστή ως επίλυση περιορισμών, για να εξερευνήσει όλες τις πιθανές διαδρομές εκτέλεσης ενός έξυπνου συμβολαίου και να ελέγξει για τρωτά σημεία (Luu et al., 2016). Εκτελώντας συμβολικά το bytecode του συμβολαίου, προσδιορίζει περιπτώσεις όπου τα αποτελέσματα υπολογισμού εξαρτώνται από χρονικές σημάνσεις μπλοκ, μη χειριζόμενες εξαιρέσεις από κλήσεις ή την πιθανότητα επανεισόδου.

Mythril. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που επινοήθηκε το 2017 και αναπτύχθηκε σε Python. Πραγματοποιεί στατική ανάλυση στον bytecode EVM του συμβολαίου και εντοπίζει ευπάθειες ασφαλείας σε έξυπνα συμβόλαια που έχουν δημιουργηθεί για Ethereum, Hedera, Quorum, Vechain, Roostock, Tron και άλλα blockchains που είναι συμβατά με EVM (ConsenSys, 2018). Το Mythril χρησιμοποιεί τρεις προσεγγίσεις για την ανάλυση των έξυπνων συμβολαίων, συμβολική εκτέλεση, επίλυση SMT και ανάλυση κηλίδων, με τα ελεγμένα τρωτά σημεία να αναφέρονται λεπτομερώς στην ηλεκτρονική τεκμηρίωση. Μπορεί επίσης να χρησιμοποιηθεί, σε συνδυασμό με άλλα εργαλεία και τεχνικές, στην πλατφόρμα ανάλυσης ασφάλειας MythX (ConsenSys, 2018).

Smartcheck. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που εφευρέθηκε το 2017 και έχει υλοποιηθεί σε Java. Αποτελεί ένα επεκτάσιμο εργαλείο στατικής ανάλυσης που επισημαίνει πιθανές ευπάθειες στα έξυπνα συμβόλαια, αναζητώντας συγκεκριμένα συντακτικά μοτίβα στον πηγαίο κώδικα. Το SmartCheck μετατρέπει τον πηγαίο κώδικα Solidity σε δέντρο σύνταξης XML. Τα τρωτά σημεία καθορίζονται ως εκφράσεις διαδρομής Xquery, που χρησιμοποιούνται για την

αναζήτηση των μοτίβων στο δέντρο XML (Tikhomirov et al., 2018). Το SmartCheck έχει σχεδιαστεί για να εντοπίζει πολλές κατηγορίες τρωτών σημείων όπως ευπάθειες επανεισόδου, αριθμητικά λάθη, μη χειρισμό εξαιρέσεων και εξάρτηση από την σειρά εκτέλεσης συναλλαγών. Σύμφωνα με προειδοποίηση που εμφανίζεται στο GitHub, το έργο έχει καταργηθεί από το 2020, καθώς επίσης η Web έκδοση του SmartCheck, που ήταν διαθέσιμη μέσω της ιστοσελίδας της εταιρείας, τερματίστηκε. Η ανάλυση ενδέχεται να λειτουργεί εσφαλμένα για εκδόσεις Solidity που ξεκινούν με 0.6.0.

MAIN. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που δημιουργήθηκε το 2018 και αναπτύχθηκε σε Python. Χρησιμοποιεί διαδικαστική συμβολική ανάλυση και συγκεκριμένο επικυρωτή για την εμφάνιση πραγματικών εκμεταλλεύσεων, εστιάζοντας στην περίπτωση του δεσμευμένου Ether (Nikolić et al., 2018). Το MAIN εκτελεί συμβολικά τον bytecode EVM και ελέγχει για ίχνη εκτέλεσης που υποδεικνύουν ότι το συμβόλαιο μπορεί να αυτοκαταστραφεί ή να αποστραγγιστεί από Ether από αυθαίρετες διευθύνσεις ή ότι δέχεται Ether χωρίς τη λειτουργικότητα μιας πληρωμής. Για να απορριφθούν τα ψευδώς θετικά, τα συμβόλαια αναλύονται δυναμικά με την ανάπτυξή τους σε μια ιδιωτική αλυσίδα μπλοκ και την επίθεση τους με τις υπολογισμένες συναλλαγές (Nikolić et al., 2018).

MadMax. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφαλείας που εφευρέθηκε το 2018 και έχει υλοποιηθεί σε Python. Αποτελεί ένα εργαλείο στατικής ανάλυσης που επικεντρώνεται στον εντοπισμό τρωτών σημείων και αναποτελεσματικοτήτων που σχετίζονται με το αέριο (gas) εντός του κώδικα των συμβολαίων. Το MadMax αναλύει τον bytecode των έξυπνων συμβολαίων Ethereum για να εντοπίσει πιθανά ζητήματα που θα μπορούσαν να οδηγήσουν σε υψηλή κατανάλωση αερίου, επιθέσεις άρνησης υπηρεσίας ή αναποτελεσματική εκτέλεση συμβολαίων. Χρησιμοποιεί έναν συνδυασμό δύο προσεγγίσεων, με την πρώτη να είναι ένας απομεταγλωττιστής που βασίζεται στην ανάλυση ροής και την δεύτερη να είναι δηλωτικά ερωτήματα δομής προγράμματος. Αυτή η συνδυασμένη ανάλυση συλλαμβάνει έννοιες υψηλού επιπέδου για συγκεκριμένο τομέα, όπως αποθήκευση δυναμικής δομής δεδομένων και βρόχοι με ασφαλή επαναφορά, και επιτυγχάνει υψηλή ακρίβεια και επεκτασιμότητα (Grech et al., 2018).

Securify. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που επινοήθηκε το 2018 και εφαρμόστηκε σε Java. Αποτελεί ένα επεκτάσιμο και πλήρως αυτοματοποιημένο εργαλείο στατικής ανάλυσης, που ελέγχει τις ιδιότητες ασφαλείας του bytecode EVM των έξυπνων συμβολαίων και υποδεικνύει τις συμπεριφορές του συμβολαίου ως ασφαλείς ή μη ασφαλείς σε σχέση με μια δεδομένη ιδιότητα (Tsankov et al., 2018). Η ανάλυση του Securify αποτελείται από δύο βήματα. Πρώτον, εκτελεί συμβολικά το γράφημα εξάρτησης του συμβολαίου για να εξαγάγει ακριβείς σημασιολογικές πληροφορίες από τον κώδικα, και στη συνέχεια, ελέγχει τη συμμόρφωση και τα μοτίβα παραβίασης που καταγράφουν επαρκείς προϋποθέσεις για να αποδειχθεί εάν μια ιδιότητα ισχύει ή όχι (Tsankov et al., 2018).

ContractFuzzer. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφαλείας που εφευρέθηκε το 2018 και εφαρμόστηκε σε GO. Αποτελεί ένα εργαλείο ειδικά σχεδιασμένο για την αυτοματοποιημένη δοκιμή fuzzing των έξυπνων συμβολαίων Ethereum. Το ContractFuzzer αξιοποιεί τις δυνατότητες της συμβολικής εκτέλεσης και των τεχνικών fuzzing γενεών για να εξερευνήσει διαφορετικές διαδρομές εκτέλεσης και καταστάσεις δεδομένων εντός της σύμβασης. Το ContractFuzzer δημιουργεί ασαφείς εισόδους με βάση τις προδιαγραφές ABI των έξυπνων συμβολαίων, καθορίζει τα δοκιμαστικά oracles για την ανίχνευση τρωτών σημείων ασφαλείας, εργαλειοποιεί το EVM για την καταγραφή της συμπεριφοράς του χρόνου εκτέλεσης των έξυπνων συμβολαίων και αναλύει αυτά τα αρχεία καταγραφής για να αναφέρει ευπάθειες ασφάλειας (Jiang et al., 2018).

Slither. Είναι ένα δημόσια διαθέσιμο πλαίσιο (framework) που δημιουργήθηκε το 2018 και έχει υλοποιηθεί σε Python. Το Slither λειτουργεί ως εργαλείο στατικής ανάλυσης, μετατρέποντας τον πηγαίο κώδικα Solidity σε μια ενδιάμεση αναπαράσταση που ονομάζεται SlithIR, και εκτελεί ένα ευρύ φάσμα ελέγχων για τον εντοπισμό ζητημάτων ασφαλείας. Χρησιμοποιεί έναν συνδυασμό κοινώς χρησιμοποιούμενων τεχνικών ανάλυσης όπως η ροή δεδομένων (dataflow) και η παρακολούθηση κηλίδων (taint tracking) για τη σάρωση των συμβάσεων, εντοπίζοντας περίπου 20 κοινά τρωτά σημεία, όπως η ευπάθεια επανεισόδου, οι μη αρχικοποιημένες μεταβλητές, οι τιμές επιστροφής αχρησιμοποίητων συναρτήσεων, η αυθαίρετη αποστολή ether και άλλα (Feist et al., 2019). Το Slither δημιουργεί εκτενείς αναφορές που παρέχουν λεπτομερείς πληροφορίες

σχετικά με τα εντοπισμένα τρωτά σημεία, συμπεριλαμβανομένων των επηρεαζόμενων θέσεων κώδικα και προτάσεων για βελτιστοποίηση, καθώς μπορεί επίσης να χρησιμοποιηθεί για κατανόηση του κώδικα και υποβοηθούμενη αναθεώρησή του.

SolidityCheck. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης ασφάλειας που επινοήθηκε το 2019 και αναπτύχθηκε σε C++. Αποτελεί ένα εργαλείο στατικής ανάλυσης που χρησιμοποιεί κανονικές εκφράσεις (regular expressions) για να ορίσει τα χαρακτηριστικά των προβληματικών δηλώσεων, ενώ χρησιμοποιεί κανονική αντιστοίχιση (regular matching) και τεχνικές παρέμβασης στο πρόγραμμα (program instrumentation) για την πρόληψη ή τον εντοπισμό προβλημάτων (Zhang et al., 2019). Η κύρια διαδικασία του SolidityCheck χωρίζεται σε τέσσερα βήματα, το πρώτο είναι η μορφοποίηση κωδικών, το δεύτερο είναι το φιλτράρισμα των λέξεων-κλειδιών, το τρίτο είναι ο εντοπισμός και η πρόληψη των προβλημάτων, και τέλος, το τέταρτό βήμα είναι η αναφορά ανίχνευσης και το προληπτικό συμβόλαιο. Εδώ εμφανίζεται μια αναφορά ανίχνευσης 18 τύπων προβλημάτων ασφαλείας, εκτός από το πρόβλημα επανεισόδου και υπερχείλισης ακέραιων αριθμών, για τα οποία συνδυάζονται κανονικές εκφράσεις και τεχνικές παρέμβασης στο πρόγραμμα ώστε να επιτευχθεί η πρόληψή τους, και δημιουργείται ένα συμβόλαιο που αποτρέπει τα δύο αυτά προβλήματα (Zhang et al., 2019).

Echidna. Είναι ένα δημόσια διαθέσιμο εργαλείο ανάλυσης που εφευρέθηκε το 2020 και αναπτύχθηκε σε Haskell. Αποτελεί ένα εργαλείο δοκιμών βασισμένο σε ιδιότητες (property-based testing tool), που λαμβάνει ως είσοδο κώδικα Solidity ή Vyper συν ιδιότητες ενσωματωμένες στο έξυπνο συμβόλαιο, και χρησιμοποιεί τεχνικές fuzzing για την ανακάλυψη πιθανών τρωτών σημείων σε έξυπνα συμβόλαια Ethereum. Το Echidna λειτουργεί σε δύο βήματα. Στο πρώτο βήμα, αξιοποιεί το εργαλείο Slither για να μεταγλωττίσει τα έξυπνα συμβόλαια και να τα αναλύσει, ώστε να εντοπίσει χρήσιμες σταθερές και συναρτήσεις που χειρίζονται απευθείας Ether (Grieco et al., 2020). Στο δεύτερο βήμα, ξεκινά η καμπάνια fuzzing, κατά την οποία δημιουργούνται τυχαίες συναλλαγές χρησιμοποιώντας το ABI που παρέχεται από τη σύμβαση και σημαντικές σταθερές που ορίζονται στο συμβόλαιο, για τον εντοπισμό παραβίασης των ιδιοτήτων (Grieco et al., 2020). Το Echidna είναι πολύ εύκολο στη χρήση και υποστηρίζει τα

περισσότερα πλαίσια ανάπτυξης συμβολαίων, συμπεριλαμβανομένων των Truffle και Embark.

Τέλος, ορισμένα ακόμα γνωστά εργαλεία ανάλυσης ασφαλείας ανοιχτού κώδικα για έξυπνα συμβόλαια είναι το EtherTrust (Grishchenko et al., 2018), το Osiris (Torres et al., 2018), το SmartInspect (Bragagnolo et al., 2018), το Vandal (Brent et al., 2018), το teEther (Krupp & Rossow, 2018), το EthIR (Albert et al., 2018), το ILF (He et al., 2019), το SAFEVM (Albert et al., 2019), το Manticore (Mossberg et al., 2019), το EasyFlow (Gao et al., 2019), το VERISMART (So et al., 2020), το NeuCheck (Lu et al., 2021) και το SmartTest (So et al., 2021).

3.4. Ζητήματα ιδιωτικότητας

Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, η αποκέντρωση είναι ένα βασικό χαρακτηριστικό της τεχνολογίας Blockchain και κατά συνέπεια και των έξυπνων συμβολαίων που βασίζονται σε αυτή. Τα δεδομένα των συναλλαγών αποθηκεύονται στο δημόσιο καθολικό έτσι ώστε όλοι οι κόμβοι στο ομότιμο δίκτυο να μπορούν να δουν και να επικυρώσουν το περιεχόμενό τους. Ο μηχανισμός αυτός προσφέρει διαφάνεια στο σύστημα, ωστόσο, μπορεί να προκαλέσει προβλήματα στο απόρρητο καθώς είναι πιθανό να αποκαλυφθούν ορισμένες ευαίσθητες πληροφορίες, όπως εμπορικά μυστικά ή πληροφορίες τιμολόγησης (Hewa et al., 2021). Αυτή η έλλειψη απορρήτου προκαλεί ανησυχία στις εταιρείες και τους οργανισμούς, περιορίζοντας την υιοθέτηση των έξυπνων συμβολαίων σε ορισμένες επιχειρηματικές περιπτώσεις.

Για την προστασία της ιδιωτικότητας και την διατήρηση του απορρήτου του χρήστη όσον αφορά τα έξυπνα συμβόλαια οι πιο συχνές λύσεις που προτείνονται στην βιβλιογραφία είναι δύο, η χρήση ασφαλούς υπολογισμού πολλαπλών μερών (Secure Multi-Party Computation ή SPMC) και η χρήση αποδείξεων μηδενικής γνώσης (Zero Knowledge Proofs). Το SMPC είναι ένα κρυπτογραφικό σχήμα που επιτρέπει σε πολλές οντότητες να εκτελούν πρωτόκολλα για να υπολογίζουν από κοινού μια συνάρτηση με εισροές τα προσωπικά τους δεδομένα χωρίς αυτά να αποκαλύπτονται. Η λογική είναι η εξής, δίνονται n συμμετέχοντες P1, P2, P3,. . . ,Pn με τον καθένα από αυτούς να έχει ιδιωτικά δεδομένα, δηλαδή εισροές, d1, d2,. . . ,dn αντίστοιχα. Οι συμμετέχοντες θα διατηρήσουν τις δικές τους εισροές ιδιωτικές και θα υπολογίσουν τη δημόσια συνάρτηση

F(d1,d2,. . . ,dn) χρησιμοποιώντας τις εισροές των υπολοίπων (Feng et al., 2019). Κάθε συμμετέχοντας λαμβάνει μόνο μέρος της εισόδου και διατηρεί ένα σημείο σε διαφορετικό πολυώνυμο για να προσδιορίσει μια μεταβλητή που δημιουργεί ένα μέρος των δεδομένων (Bernabe et al., 2019). Στην περίπτωση του blockchain, το SMPC μπορεί να χρησιμοποιηθεί για τον διαχωρισμό της εκτέλεσης έξυπνων συμβολαίων καθώς και για τη διαχείριση του λογαριασμού και των κλειδιών χωρίς να απαιτείται συμμετοχή τρίτων (Bernabe et al., 2019). Ένα εργαλείο που χρησιμοποιεί την τεχνολογία SMPC και παρέχει λύση στο πρόβλημα διασφάλισης του απορρήτου κατά την εκτέλεση των έξυπνων συμβολαίων είναι το Enigma (Zyskind et al., 2015), όπου τα δεδομένα διανέμονται σε διαφορετικούς κόμβους με τον καθένα να υπολογίζει ορισμένες συναρτήσεις με κατανεμημένο τρόπο ώστε να μην υπάρχει διαρροή πληροφοριών.

Η δεύτερη λύση για την διασφάλιση του απορρήτου κατά την εκτέλεση των έξυπνων συμβολαίων είναι η χρήση αποδείξεων μηδενικής γνώσης. Αποτελεί ένα κρυπτογραφικό πρωτόκολλο που επιτρέπει σε ένα μέρος, τον prover, να αποδείξει σε ένα άλλο μέρος, τον verifier, ότι μια δεδομένη δήλωση είναι αληθής, χωρίς να αποκαλύπτει οποιαδήποτε πληροφορία εκτός από το ότι η ίδια η απόδειξη είναι σωστή (Bernabe et al., 2019). Οι μαθηματικές αρχές των αποδείξεων μηδενικής γνώσης δεν θα αναλυθούν σε αυτό το σημείο, καθώς υπάρχουν πολλά σχετικά άρθρα και βιβλία μέσα από τα οποία μπορούν να γίνουν κατανοητές, όπως το "*Fundamentals of computer security"* (Pieprzyk et al., 2013). Ένα αποκεντρωμένο σύστημα έξυπνων συμβολαίων που χρησιμοποιεί αποδείξεις μηδενικής γνώσης είναι το Hawk (Kosba et al., 2016). Το Hawk είναι ένα εργαλείο που επιτρέπει στους προγραμματιστές να δημιουργούν έξυπνες συμβάσεις χωρίς την ανάγκη εφαρμογής οποιασδήποτε κρυπτογραφίας (Khan et al., 2021). Πιο συγκεκριμένα, ο μεταγλωττιστής Hawk μεταγλωττίζει αυτόματα ένα συμβόλαιο σε ένα κρυπτογραφικό πρωτόκολλο, δηλαδή κρυπτογραφεί τις πληροφορίες συναλλαγής, όπως για παράδειγμα το υπόλοιπο της συναλλαγής, και επαληθεύει την ορθότητα των συναλλαγών χρησιμοποιώντας αποδείξεις μηδενικής γνώσης, χωρίς να προβάλει το περιεχόμενο των συναλλαγών (Zheng et al., 2020). Με τον τρόπο αυτό διασφαλίζεται η διατήρηση της ιδιωτικότητας των συμβαλλόμενων μερών.

3.5. Νομικά ζητήματα

Στην παρούσα ενότητα θα παρουσιαστεί μια ακόμα κρίσιμη πτυχή των έξυπνων συμβολαίων, η νομική. Προς το παρόν είναι αμφίβολο αν οι σχέσεις που υπογράφηκαν μέσω ενός έξυπνου συμβολαίου και όχι μέσω μιας νομικής σύμβασης έχουν οποιαδήποτε νομική ισχύ και παράγουν οποιοδήποτε νομικό αποτέλεσμα (Cappiello & Carullo, 2021). Το κύριο ερώτημα που δημιουργείται είναι σε ποιο βαθμό τα έξυπνα συμβόλαια μπορούν να αντιπροσωπεύουν, να αντικαταστήσουν ή να συμπληρώσουν τα παραδοσιακά συμβόλαια και σε ποιο βαθμό τα νομικά ιδρύματα θα πρέπει να συνεργάζονται με προγραμματιστές και χρήστες των τεχνολογιών Blockchain (Ante, 2021). Οι έρευνες γενικά συμφωνούν ότι τα έξυπνα συμβόλαια δεν θα αντικαταστήσουν τη νομοθεσία αυτή καθαυτή, καθώς, ο νόμος δεν περιορίζεται σε ένα σύνολο γραπτών κανόνων που μπορεί να εφαρμόζεται μηχανικά ακόμη και στην απλούστερη περίπτωση (Cappiello & Carullo, 2021). Ωστόσο, τα έξυπνα συμβόλαια μπορούν να αντιπροσωπεύουν συγκεκριμένες νομικά δεσμευτικές συμβάσεις, και ως εκ τούτου, είναι απαραίτητη η ανάλυση και κατανόηση της συμβατότητας του υπάρχοντος δικαίου και των έξυπνων συμβάσεων (Ante, 2021).

Ένα ακόμα ερώτημα που τίθεται είναι το κατά πόσο είναι απαραίτητη η άμεση ρύθμιση των έξυπνων συμβολαίων. Μερικοί υποστηρικτές της τεχνολογίας υποστηρίζουν ότι το να κρίνουμε έξυπνες συμβάσεις εντός των ορίων του τρέχοντος νομικού συστήματος είναι προβληματικό, διότι δεν υπάρχει σύνδεση μεταξύ των δύο τομέων (Drummer & Neumann, 2020). Αυτή είναι η περίπτωση όπου ο κώδικας είναι ο ίδιος ο νόμος, όπως έχει διατυπωθεί από τον Lawrence Lessig (2006). Ωστόσο, παρά την άποψη αυτή, έρευνες δείχνουν ότι τα έξυπνα συμβόλαια εξακολουθούν να εμπίπτουν στα όρια της καθιερωμένης νομικής κατανόησής μας και επομένως πρέπει να συμμορφώνονται με τους κανόνες και τις αρχές του (Drummer & Neumann, 2020). Αναλυτικότερα, τα αποτελέσματα της έρευνας του Jaccard (2018) επισημαίνουν την νομική συνάφεια των έξυπνων συμβολαίων και τα διαφοροποιούν τοποθετώντας τα σύμφωνα με νομικές κατηγορίες. Πιο συγκεκριμένα, θεωρεί πως τα έξυπνα συμβόλαια υπόκεινται στην εφαρμογή του δικαίου των συμβάσεων και του εταιρικού δικαίου, ενώ η χρήση τους για τη δημιουργία ενός δικαιώματος που μοιάζει με ιδιοκτησία, δηλαδή έξυπνη ιδιοκτησία, δεν μπορεί να αναγνωριστεί νομικά προς το παρόν.

Επιπροσθέτως, μερικά ακόμη ζητήματα που πρέπει να ληφθούν υπόψη είναι, αρχικά, η διαφοροποίηση των νόμων και των κανονισμών της κάθε χώρας, κάτι που καθιστά πολύπλοκη την διασφάλιση της τήρησής τους, οδηγώντας στο ερώτημα αν η νέα αυτή τεχνολογία απαιτεί αλλαγές στο διεθνές δίκαιο. Ένα ακόμα ζήτημα αποτελεί το γεγονός ότι οι ρήτρες ή οι όροι του νόμου δεν είναι ποσοτικοποιήσιμοι, επομένως είναι ακόμα πολύπλοκο να μοντελοποιηθούν αυτές οι συνθήκες σε έξυπνα συμβόλαια, ώστε να είναι κατάλληλες για να τις εκτελέσει μια μηχανή (Khan et al., 2021). Προκειμένου, λοιπόν, να υπάρξει μια ευρεία εφαρμογή των έξυπνων συμβολαίων πρέπει να πραγματοποιηθούν πιο συγκεκριμένες αναλύσεις που θα εμβαθύνουν στα προαναφερθέντα ζητήματα.

4.Εφαρμογές της τεχνολογίας Blockchain σε Περιβάλλοντα Ιστού και Κινητών Συσκευών

Το Διαδίκτυο αρχικά χρησιμοποιήθηκε ως ένα δίκτυο που εξυπηρετούσε κυρίως σκοπούς επικοινωνίας στον στρατό και τα εκπαιδευτικά ιδρύματα, χρειάστηκαν αρκετές δεκαετίες για να μεταμορφωθεί σε μια τεχνολογική πλατφόρμα που μπόρεσε να φιλοξενεί και να υλοποιεί εμπορικές εφαρμογές (Treiblmaier & Sillaber, 2021). Ωστόσο, η εισαγωγή του Παγκόσμιου Ιστού είναι που άλλαξε ριζικά την ανταλλαγή των φυσικών αγαθών και τις επιχειρηματικές διαδικασίες, μεταφέροντάς τες από την αναλογική εποχή στην ψηφιακή. Αυτό οδήγησε στην δημιουργία του ηλεκτρονικού εμπορίου, δίνοντας τη δυνατότητα στις εταιρείες και τους οργανισμούς να προσεγγίσουν ένα παγκόσμιο κοινό, αυξάνοντας σημαντικά την εμβέλεια και την αποτελεσματικότητα των προσπαθειών μάρκετινγκ και πωλήσεων.

Το ηλεκτρονικό εμπόριο είναι η αγορά και πώληση αγαθών και υπηρεσιών μέσω του Διαδικτύου. Αυτό μπορεί να περιλαμβάνει οτιδήποτε, από την αγορά ενός προϊόντος από ένα ηλεκτρονικό κατάστημα μέχρι την πληρωμή για μια υπηρεσία. Ο όρος ηλεκτρονικό εμπόριο χρησιμοποιείται συχνά ως γενικός όρος για κάθε τύπο ψηφιακής συναλλαγής, αλλά ουσιαστικά είναι μια συναλλαγή μεταξύ δύο μερών. Από τη μία πλευρά, ο αγοραστής πραγματοποιεί μια αγορά, ενώ από την άλλη πλευρά, ο πωλητής παρέχει τα αγαθά ή τις υπηρεσίες. Η συναλλαγή διευκολύνεται από ένα διαδικτυακό σύστημα πληρωμών, όπως το PayPal ή μια τραπεζική μεταφορά. Το ηλεκτρονικό εμπόριο αποτελεί πλέον ένα παγκόσμιο επιχειρηματικό μοντέλο, όπου οι λιανικές πωλήσεις ηλεκτρονικού εμπορίου ανήλθαν σε 4,89 τρις αμερικάνικα δολάρια (USD) το 2021 με αναμενόμενη ανάπτυξη σε 6,39 τρις αμερικάνικα δολάρια (USD) έως το 2024 (Treiblmaier & Sillaber, 2021). Τα τελευταία χρόνια το ηλεκτρονικό εμπόριο έχει ενισχυθεί ακόμα περισσότερο από την έξαρση της πανδημίας του COVID-19, που είχε παγκόσμιο αντίκτυπο επηρεάζοντας όλες τις αγορές και τις εταιρείες, κάνοντας επιτακτική την ανάγκη για ψηφιακό μετασχηματισμό.

Οι περισσότερες εταιρείες ηλεκτρονικού εμπορίου σήμερα στοχεύουν να μεγιστοποιήσουν το κέρδος για τους μετόχους αυξάνοντας το αντίστοιχο δίκτυο συμμετεχόντων που χρησιμοποιούν την πλατφόρμα, συμπεριλαμβανομένων πωλητών, αγοραστών, προγραμματιστών, μεταπωλητών, ενδιάμεσων παρόχων υπηρεσιών (όπως πάροχοι logistics), υπηρεσιών πύλης πληρωμών και θεσμικών μεσαζόντων, συμπεριλαμβανομένων νομικών συμβούλων (Subramanian, 2018). Οι στρατηγικές που αναπτύσσονται από ηλεκτρονικές αγορές (e-marketplaces) για την αύξηση των αποτελεσμάτων του δικτύου περιλαμβάνουν την εξατομίκευση των υπηρεσιών που προσφέρονται στην πλατφόρμα, συστήματα συστάσεων για αγαθά και υπηρεσίες, μηχανισμοί εμπιστοσύνης και απλοποίηση των συναλλαγών (Subramanian, 2018).

Επιπλέον, η εφεύρεση και η δημοτικότητα των έξυπνων κινητών συσκευών είχε σημαντικό αντίκτυπο στο ηλεκτρονικό εμπόριο. Η συμπεριφορά των καταναλωτών έχει αλλάξει δραματικά, καθώς έχουν πλέον πρόσβαση σε σημαντικές πληροφορίες και εφαρμογές από τις κινητές τους συσκευές ανά πάσα στιγμή, και μπορούν να αγοράζουν αγαθά και υπηρεσίες εν κινήσει. Για παράδειγμα, στην περίπτωση ενός αθλητικού αγώνα, όλες οι διαδικασίες από τη διαφήμιση του αθλητικού παιχνιδιού μέχρι την αγορά και παράδοση των εισιτηρίων και την είσοδο στο γήπεδο, μπορούν πλέον να γίνουν με την χρήση μιας έξυπνης κινητής συσκευής (Chang et al., 2019). Αυτό έχει οδηγήσει στην ανάπτυξη νέων επιχειρηματικών μοντέλων, όπως ηλεκτρονικοί χώροι αγοράς μόνο για κινητές συσκευές.

Λαμβάνοντας όλα τα παραπάνω υπόψη, γίνεται αντιληπτό ότι η τεχνολογία Blockchain είναι ιδανική για εφαρμογές ηλεκτρονικού εμπορίου αφού έχει σχεδιαστεί να αποθηκεύει πληροφορίες συναλλαγών, ωστόσο, αυτά τα δεδομένα δεν χρειάζεται απαραίτητα να είναι οικονομικά. Μπορεί να είναι οποιαδήποτε διακριτή ενέργεια που απαιτεί ένα αμετάβλητο αρχείο, όπως εναλλακτικοί τρόποι πληρωμής, ταχύτερες συναλλαγές και βελτιωμένη διεκπεραίωση παραγγελιών (Mohammed et al., 2021). Το blockchain έχει τη δυνατότητα να γίνει μια σημαντική πηγή καινοτομιών στις επιχειρήσεις συνεισφέροντας στην βελτίωση της απόδοσης, την βελτιστοποίηση και αυτοματοποίηση των επιχειρηματικών διαδικασιών, επιτρέποντας στις εταιρείες να εξοικονομήσουν χρόνο και κόστος (Casino et al., 2019). Σε αυτό το κεφάλαιο θα πραγματοποιηθεί μελέτη της επίδρασης της τεχνολογίας Blockchain στις διάφορες πτυχές του ηλεκτρονικού εμπορίου

όπως στα συστήματα ψηφιακών πληρωμών, στους αποκεντρωμένους ηλεκτρονικούς χώρους αγοράς, στα προγράμματα ανταμοιβής πιστών πελατών, όπως επίσης στην διαδικασία έγκρισης και αξιολόγησης των κινητών εφαρμογών. Επιπλέον, θα παρουσιαστούν διάφορες εφαρμογές που αφορούν όλα τα παραπάνω και βασίζονται στην τεχνολογία Blockchain.

4.1. Τεχνολογία Blockchain και αποκεντρωμένοι ηλεκτρονικοί χώροι αγοράς (e-marketplaces)

Προκειμένου να ανταλλάσσουν φυσικά αγαθά στο Διαδίκτυο, οι χρήστες χρησιμοποιούν ηλεκτρονικούς χώρους αγοράς. Οι ηλεκτρονικοί χώροι αγοράς είναι ηλεκτρονικές πλατφόρμες όπου προμηθευτές και αγοραστές συνευρίσκονται και διενεργούν αγοραπωλησίες προϊόντων ή υπηρεσιών. Η Amazon και το eBay ήταν από τις πρώτες ηλεκτρονικές αγορές που γεννήθηκαν στα μέσα της δεκαετίας του 1990, όταν το Διαδίκτυο κέρδιζε την επικρατούσα τάση (Taylor, 2020). Τέτοιες ηλεκτρονικές αγορές προσφέρουν σημαντικές λύσεις ασφαλείας, μειώνοντας τον κίνδυνο απάτης, λειτουργώντας ως μεσάζοντες με φήμη (reputational intermediaries) (Earle et al., 2022) Ένας αγοραστής και ένας πωλητής δεν μπορούν έχουν προηγούμενη συμβασιακή σχέση μεταξύ τους, αλλά οι μεσάζοντες έχουν συμβασιακή σχέση με όλους τους εμπλεκόμενους, και μπορούν να παρέχουν διαβεβαιώσεις ότι και οι δύο θα λάβουν αυτό που τους οφείλουν (Earle et al., 2022). Ουσιαστικά, οι μεσάζοντες λειτουργούν ως αξιόπιστοι διαμεσολαβητές που παρέχουν την υπηρεσία σύνδεσης και προστασίας των πωλητών και των αγοραστών που επιθυμούν να ανταλλάξουν αγαθά, προκειμένου να μετριαστούν ορισμένοι από τους σχετικούς κινδύνους συναλλαγών στο Διαδίκτυο, όπως επίσης και για να διευκολυνθεί η διεκπεραίωση της χρηματοοικονομικής συναλλαγής, με αντάλλαγμα μια αμοιβή που είναι πιθανώς ένα ποσοστό περικοπής της συναλλαγής (Kabi & Franqueira, 2018).

Με βάση τα παραπάνω, γίνεται αντιληπτό πως ένα από τα κύρια καθήκοντα αυτών των διαμεσολαβητών, όπως είναι οι πάροχοι πλατφορμών, είναι να συλλέγουν προσφορές και αιτήματα από διάφορες πηγές, π.χ. μέσω των API τους, και να αντιστοιχίζουν αυτά τα δεδομένα ακολουθώντας ορισμένους κανόνες (Alt, 2020). Τα βήματα που εμπλέκονται σε αυτόν τον μετασχηματισμό δεδομένων, όπως η ομογενοποίηση και η ταξινόμηση, συχνά δεν είναι διαφανή και οι πάροχοι ενδέχεται να χρησιμοποιήσουν

αυτές τις εργασίες για να ενισχύσουν την ανταγωνιστική τους θέση στην αγορά (Alt, 2020). Με τον τρόπο αυτό οι μεγάλες πλατφόρμες ηλεκτρονικού εμπορίου μπορούν να προκαλέσουν μονοπώλιο, έχοντας ως αποτέλεσμα έλεγχο των τιμών και υψηλές προμήθειες (Chang et al., 2019). Επιπλέον, η συλλογή όλων αυτών των πληροφοριών για την αγοραστική συμπεριφορά των χρηστών προκαλούν ανησυχίες σχετικά με το απόρρητο. Για παράδειγμα, πρόσφατα οι υπάλληλοι της Amazon διέρρευσαν δεδομένα για δωροδοκίες στην Κίνα (Chang et al., 2019). Επίσης, ο έλεγχος της πλατφόρμας από μια κεντρική αρχή μπορεί να οδηγήσει σε λογοκρισία, επειδή υπάρχει η πιθανότητα υιοθέτησης πολιτικών που εισάγουν διακρίσεις.

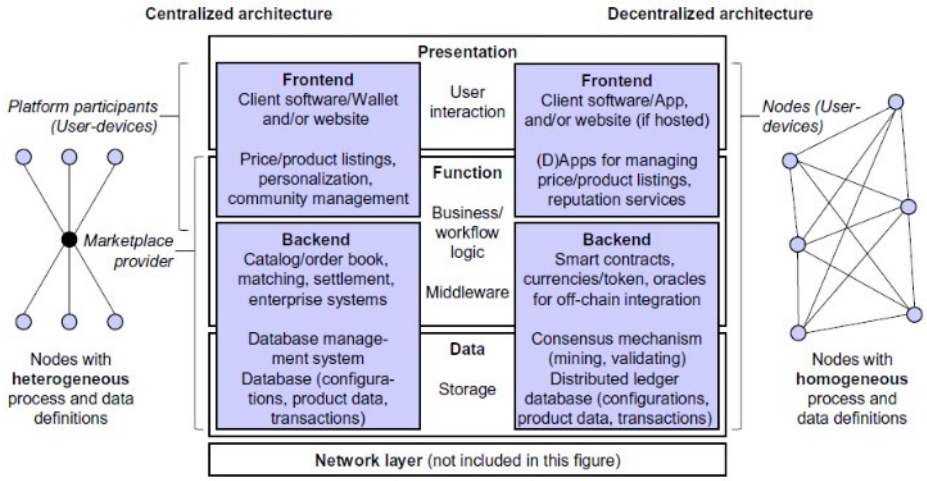
Οι πλατφόρμες ηλεκτρονικού εμπορίου και η τεχνολογία Blockchain έχουν τη δυνατότητα να γίνουν ένας ισχυρός συνδυασμός, καθώς η τεχνολογία αυτή παρέχει ασφάλεια και διαφάνεια σε όλα τα παραπάνω κρίσιμα σημεία. Το blockchain προσφέρει τη ραχοκοκαλιά για έναν νέο τρόπο επιχειρηματικής δραστηριότητας και τη δημιουργία πραγματικά αποκεντρωμένων εφαρμογών χωρίς κεντρικό σημείο αστοχίας και ιεραρχική ιδιοκτησία των δεδομένων του χρήστη, προσφέροντας πλεονεκτήματα για την ασφάλεια των δεδομένων, το απόρρητο και την ιδιοκτησία, καθώς και τη δυνατότητα μείωσης του κόστους καταβολής προμηθειών στους μεσάζοντες. Στην συνέχεια εξετάζονται αναλυτικά όλα αυτά τα πλεονεκτήματα.

4.1.1. Πλεονεκτήματα ηλεκτρονικών αγορών που βασίζονται στην τεχνολογία Blockchain

Η εξασφάλιση υψηλού επιπέδου ασφάλειας στις συναλλαγές είναι ένας κρίσιμος παράγοντας για τις επιχειρήσεις, ειδικότερα στον ψηφιακό κόσμο. Η τεχνολογία Blockchain είναι εγγενώς ασφαλής, χάρη στην αποκεντρωμένη φύση της και τη χρήση κρυπτογραφίας, γεγονός που κάνει το σύστημα να είναι ανθεκτικό σε παραβίαση δεδομένων, τόσο κακόβουλης όσο και ακούσιας (Merlina & Setty, 2022). Επιπλέον, δεδομένου ότι όλες οι συναλλαγές καταγράφονται σε δημόσιο καθολικό, γίνεται πολύ πιο δύσκολο να διαπράξει κανείς απάτη ή να συμμετάσχει σε άλλες σκιώδεις πρακτικές. Αυτό εξασφαλίζει ότι οι πληροφορίες δεν έχουν παραβιαστεί, κι έτσι διασφαλίζεται η προστασία των οικοσυστημάτων ηλεκτρονικού εμπορίου για τους πελάτες, τους προμηθευτές, τους πωλητές και τις μεταφορικές εταιρείες (Lim et al., 2019).

Ένα ακόμα πλεονέκτημα μιας αγοράς που βασίζεται σε blockchain είναι πως οι συναλλαγές είναι συνήθως λιγότερο δαπανηρές από αυτές στις παραδοσιακές πλατφόρμες ηλεκτρονικού εμπορίου. Στις παραδοσιακές πλατφόρμες υπάρχουν διαμεσολαβητές όπως τράπεζες, πιστωτικά ιδρύματα ή πύλες πληρωμών, δηλαδή νομικές οντότητες που διασφαλίζουν την επικύρωση των συναλλαγών με την επιβολή νομικής σύμβασης (Subramanian, 2018). Αυτό προσθέτει σημαντικό κόστος στις συναλλαγές. Με την εισαγωγή τεχνολογιών Blockchain, ωστόσο, εξαλείφεται η ανάγκη για μεσάζοντες, οι πληρωμές γίνονται απευθείας μεταξύ του λιανοπωλητή και του πελάτη μειώνοντας το κόστος και αυξάνοντας τα κέρδη (Lim et al., 2019). Επιπροσθέτως, η τεχνολογία Blockchain επιτρέπει μια διαδρομή ελέγχου κάθε φορά που γίνεται μια ενέργεια κατά τη διάρκεια της συναλλαγής (Lim et al., 2019). Αυτή η βελτιωμένη ιχνηλασιμότητα των προϊόντων και των υπηρεσιών επιτρέπει στους πελάτες να γνωρίζουν από πού προέρχονται τα προϊόντα και πώς παράγονται, μειώνοντας έτσι τον κίνδυνο απάτης.

Τέλος, οι ιδιότητες της εγγενούς διαφάνειας και αποκέντρωσης της εξουσίας μειώνουν τον κίνδυνο αυθαίρετων αποφάσεων (Merlina & Setty, 2022). Στις παραδοσιακές ηλεκτρονικές αγορές, ο έλεγχος από από μια ενιαία, κεντρική αρχή μπορεί να οδηγήσει σε λογοκρισία, καθώς η αρχή αυτή έχει τη δυνατότητα να αποκλείσει χρήστες από την υποβολή αντικειμένων ή προσφορών στην πλατφόρμα, όπως επίσης πολλές φορές επιλέγει να συνδέει ανθρώπους μόνο σε ορισμένες χώρες και να ασκεί επιχειρηματικές δραστηριότητες για ορισμένα αγαθά (Earle et al., 2022). Αντίθετα, οι αποκεντρωμένες αγορές μπορούν να προσφέρουν διαφανή και μη τροποποιημένη πρόσβαση σε πληροφορίες, όπως το επιθυμεί ο πωλητής, δεδομένου ότι κάθε κόμβος είναι σε θέση να αναγράφει τιμές, εμπορεύματα και κριτικές που αφορούν αγαθά (Subramanian, 2018).



Εικόνα 4.1. Αρχιτεκτονική μιας κεντρικής και μιας αποκεντρωμένης ηλεκτρονικής αγοράς (Alt, 2020)

4.1.2. Εφαρμογές ηλεκτρονικών αγορών που βασίζονται στην τεχνολογία Blockchain

Σε αυτό το σημείο θα πραγματοποιηθεί μια ανάλυση ορισμένων αποκεντρωμένων ηλεκτρονικών αγορών που βασίζονται στην τεχνολογία Blockchain.

La'zooz. Οι υπηρεσίες ταξί που παρέχονται από διάσημες startups όπως η Uber, η Taxify και η Lyft υλοποιούνται χρησιμοποιώντας μια κεντρική προσέγγιση και η διαδικασία κράτησης ταξί γίνεται μέσω μεσάζοντα, επομένως δεν παρέχει διαφάνεια (Shaikh & Mohammad, 2020). Η δημιουργία της πλατφόρμας La'zooz, με στόχο να δημιουργήσει ένα πιο αποτελεσματικό και οικονομικό δίκτυο μεταφορών, που να είναι πιο δίκαιο για όλους τους εμπλεκόμενους, μεταφέρει την κοινή χρήση διαδρομής στο επόμενο επίπεδο. Αποτελεί μια αποκεντρωμένη πλατφόρμα κοινής χρήσης διαδρομής (ridesharing) σε πραγματικό χρόνο, που χρησιμοποιεί τεχνολογία Blockchain για να αντιστοιχίζει τους οδηγούς με τους επιβάτες, καθώς επιτρέπει στους ιδιοκτήτες ιδιωτικών αυτοκινήτων να μοιράζονται τις κενές θέσεις τους με άλλους επιβάτες που ταξιδεύουν στην ίδια διαδρομή.

Το υποκείμενο σκεπτικό της πλατφόρμας είναι το εξής. Οποιαδήποτε συσκευή εκτελεί το Dapp της La'zooz, όπως έξυπνες κινητές συσκευές, wearables και υπολογιστές της κοινότητας των χρηστών της, μπορεί να εγγραφεί ως ένας από τους υπολογιστικούς

κόμβους του δικτύου, που ονομάζεται "road miner" (Yuan & Wang, 2018). Τα δεδομένα που δημιουργούνται σε πραγματικό χρόνο επαληθεύονται και αποθηκεύονται σε ένα κρυπτογραφικό καθολικό που διατηρείται από την κοινότητα, μέσω του οποίου συντονίζονται και εκτελούνται όλες οι συμπεριφορές κοινής χρήσης διαδρομής, τα προγράμματα και οι πληρωμές (Yuan & Wang, 2018). Σε αντίθεση με τις παραδοσιακές πλατφόρμες κοινής χρήσης, η La'zooz δεν λαμβάνει προμήθεια από οδηγούς ή επιβάτες, αλλά χρησιμοποιεί ένα κρυπτονόμισμα που ονομάζεται ZOO για την επεξεργασία πληρωμών, την παροχή κινήτρων στους οδηγούς και την επιβράβευση των επιβατών για κοινή χρήση διαδρομών. Επιπλέον, η πλατφόρμα σχεδίασε έναν νέο αλγόριθμο συναίνεσης που ονομάζεται "proof-of-movement", ο οποίος ενθαρρύνει τους υπολογιστικούς κόμβους να οδηγούν με το Dapp της La'zooz που εκτελείται στις συσκευές τους, συνεισφέροντας έτσι στην κοινότητα, μοιράζοντας τα δεδομένα μεταφοράς τους στην πορεία και βοηθώντας τη La'zooz να δημιουργήσει τον τοπικό ιστό κοινωνικής μεταφοράς (Yuan & Wang, 2018).

Η πλατφόρμα La'zooz παρέχει επίσης μια σειρά από άλλες υπηρεσίες στους επιβάτες, συμπεριλαμβανομένης μιας εφαρμογής για κινητά που επιτρέπει στους χρήστες να βρίσκουν τις καλύτερες διαδρομές και οδηγούς, μιας διαδικτυακής πλατφόρμας που παρέχει πληροφορίες σχετικά με τους οδηγούς και τις διαδρομές και ένα ασφαλές σύστημα πληρωμών που επιτρέπει στους χρήστες να πληρώνουν χρησιμοποιώντας το κρυπτονόμισμα ZOO.

OpenBazaar. Αποτελεί μια πλήρως αποκεντρωμένη πλατφόρμα ηλεκτρονικού εμπορίου. Το OpenBazaar είναι λογισμικό ανοιχτού κώδικα που επιτρέπει στους χρήστες να δημιουργούν συνδέσεις P2P με τις οποίες μπορούν να αγοράσουν ή να πουλήσουν οποιοδήποτε αγαθό ή υπηρεσία και να πραγματοποιήσουν συναλλαγές σε Bitcoin, χωρίς να απαιτείται καταβολή τελών σε μεσάζοντα ή χρήση τράπεζας ή πιστωτικής κάρτας (Earle et al., 2022). Σε αντίθεση με τα συμβατικά δίκτυα ηλεκτρονικού εμπορίου, δεν έχει κεντρικό σημείο αστοχίας και δεν μπορεί να ελεγχθεί από μία μόνο οντότητα. Αυτή η αποκέντρωση επιτυγχάνεται με την χρήση της τεχνολογίας Blockchain, έξυπνων συμβολαίων ρικαρδιανού τύπου και μεσεγγύηση πολλαπλών υπογραφών (multisignature-escrow). Ο πυρήνας της αρχιτεκτονικής της πλατφόρμας είναι το πρωτόκολλο ανοιχτού κώδικα InterPlanetary File System (IPFS), το οποίο

χρησιμοποιείται για την αποθήκευση και τη διανομή όλων των δεδομένων της ηλεκτρονικής αγοράς. Οι καταχωρίσεις αποθηκεύονται μέσω IPFS χρησιμοποιώντας μια υλοποίηση του κατανεμημένου πίνακα κατακερματισμού (DHT), όπου οι κόμβοι αποθηκεύουν τον κατακερματισμό ενός συγκεκριμένου χρήστη, στοιχείου ή ανατροφοδότησης μαζί με την τοποθεσία τους στο δίκτυο (Arps & Christin, 2020). Εάν ένας κόμβος επισκεφτεί μια σελίδα προμηθευτή ή δει μία από τις καταχωρίσεις του, το ίδιο αποθηκεύει τις πληροφορίες που λαμβάνει τοπικά για ορισμένο χρονικό διάστημα, επιτρέποντας ένα πρόσθετο επίπεδο πλεονασμού σε όλο το δίκτυο (Arps & Christin, 2020).

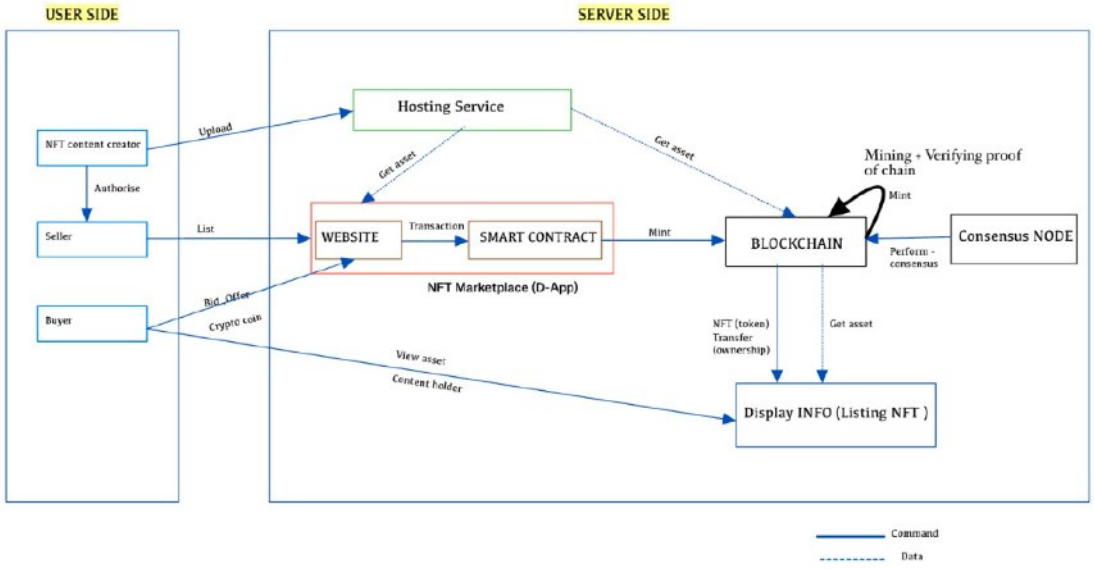
Το χαρακτηριστικό που ξεχώρισε το OpenBazaar ήταν η εισαγωγή συντονιστών, δηλαδή πιθανών διαμεσολαβητών για την επίλυση διαφορών. Οι συντονιστές είναι χρήστες που προσφέρονται εθελοντικά να μεσολαβήσουν σε διαφορές μεταξύ άλλων χρηστών και να αποφασίσουν την ενδεχόμενη διανομή των κεφαλαίων χρησιμοποιώντας συναλλαγές πολλαπλών υπογραφών, και το κάνουν με αντάλλαγμα ένα μικρό σταθερό ποσοστό αμοιβής (Arps & Christin, 2020). Οι συντονιστές επιλέγονται από τον πωλητή κατά την δημιουργία της καταχώρισης. Τα κεφάλαια ενός αγοραστή σε ένα blockchain κρατούνται σε μεσεγγύηση, με την χρήση έξυπνων συμβολαίων, και ο αγοραστής και ο πωλητής, σε περίπτωση διαφοράς, δεσμεύονται εκ των προτέρων να τηρήσουν την απόφαση του διαμεσολαβητή, ο οποίος μεταφέρει αμετάκλητα τα κεφάλαια στον πωλητή ή πίσω στον αγοραστή (Earle et al., 2022). Δηλαδή, όσον αφορά την πληρωμή, οι χρήστες έχουν την επιλογή να στείλουν απευθείας κρυπτονόμισμα στον πωλητή για την εξόφληση τους αντικειμένου ή να χρησιμοποιήσουν το σύστημα μεσολάβησης ώστε να κρατηθούν σε αναμονή τα κεφάλαια μέχρι να παραληφθεί το αντικείμενο. Στην δεύτερη περίπτωση, ο υποψήφιος αγοραστής καταθέτει τα κεφάλαια σε ένα καθορισμένο πορτοφόλι Bitcoin το οποίο απαιτεί δύο από τις τρεις υπογραφές ώστε τα κεφάλαια να αποδεσμευτούν (Earle et al., 2022).

Μερικοί ακόμα ηλεκτρονικοί χώροι αγορών είναι το BitBay, μια αποκεντρωμένη αγορά που βασίζεται στην τεχνολογία Blockchain και επιτρέπει στα άτομα να αγοράζουν και να πωλούν αγαθά και υπηρεσίες απευθείας μεταξύ τους, και η Particl, μια πλατφόρμα ανοιχτού κώδικα που βασίζεται σε blockchain που στοχεύει να παρέχει έναν πιο ιδιωτικό και ασφαλή τρόπο αγοράς και πώλησης αγαθών και υπηρεσιών στο διαδίκτυο,

χρησιμοποιώντας μια σειρά από τεχνολογίες αιχμής, συμπεριλαμβανομένης της χρήσης ενός συστήματος dual-token και ενός ενσωματωμένου νομίσματος απορρήτου, για να δημιουργήσει ένα οικοσύστημα που δίνει προτεραιότητα στο απόρρητο και την ασφάλεια των χρηστών.

OpenSea. Είναι μια αποκεντρωμένη πλατφόρμα που βασίζεται στην τεχνολογία Blockchain και επιτρέπει στους χρήστες να "κόβουν" (mint), να πωλούν και να αγοράζουν NFTs (Non Fungible Tokens). Τα NFTs είναι tokens αποθηκευμένα σε ένα blockchain που μπορούν να χρησιμοποιηθούν για να αντιπροσωπεύσουν την ιδιοκτησία ενός συγκεκριμένου ψηφιακού στοιχείου, όπως ένα έργο τέχνης, μουσική, συλλεκτικά αντικείμενα ή περιουσιακά στοιχεία παιχνιδιών (Pinto-Gutiérrez et al., 2022). Η κύρια διαφορά μεταξύ των NFTs και των κρυπτονομισμάτων, όπως το Bitcoin ή το Ethereum, είναι ότι τα κρυπτονομίσματα είναι ανταλλάξιμα, δηλαδή αξίζουν όλα το ίδιο ποσό, ενώ τα NFTs είναι μη ανταλλάξιμα, που σημαίνει ότι το ένα δεν μπορεί να αντικατασταθεί με το άλλο, καθώς το καθένα είναι μοναδικό (Pinto-Gutiérrez et al., 2022). Το OpenSea θεωρείται ως η μεγαλύτερη αγορά για NFTs, με περισσότερους από ένα εκατομμύριο χρήστες που κατέχουν και εμπορεύονται μοναδικά ψηφιακά στοιχεία στο blockchain Ethereum.

Ένα από τα βασικά χαρακτηριστικά της αγοράς OpenSea, και οποιασδήποτε άλλης πλατφόρμας αγορών NFTs, είναι το blockchain, ένα διαφανές, αμετάβλητο καθολικό για την αποθήκευση, οπτικοποίηση και διαχείριση τόσο νομισμάτων όσο και NFTs, που καταγράφει σε ποιον ανήκει τι και πού βρίσκονται τα αρχεία, προστατεύοντας αυτά και τις συναλλαγές κρυπτογραφικά (Bhujel & Rahulamathavan, 2022). Αυτό επιτρέπει ένα αποκεντρωμένο σύστημα εμπιστοσύνης και φήμης που δίνει την δυνατότητα στους χρήστες να βλέπουν το ιστορικό συναλλαγών, τις αξιολογήσεις και τις κριτικές άλλων χρηστών, κάτι που βοηθά στη διασφάλιση της ασφάλειας και της αξιοπιστίας των συναλλαγών. Επιπλέον, η πλατφόρμα επιτρέπει στους χρήστες να βλέπουν την προέλευση κάθε NFT, η οποία περιλαμβάνει πληροφορίες σχετικά με τη δημιουργία, την ιδιοκτησία και το ιστορικό συναλλαγών του NFT. Η Εικόνα 4.2 απεικονίζει το συνολικό οικοσύστημα που έχει αναπτυχθεί γύρω από τα NFTs, και πιο συγκεκριμένα τους συμμετέχοντες και τα στοιχεία με τα οποία αλληλεπιδρούν.



Εικόνα 4.2. Οικοσύστημα NFT (Bhujel & Rahulamathavan, 2022)

Όπως φαίνεται και στην παραπάνω εικόνα, μια αποκεντρωμένη εφαρμογή web (Dapp) είναι βασικό συστατικό ενός οικοσυστήματος NFT, μέσω του οποίου διαπραγματεύονται περιουσιακά στοιχεία NFT. Οι χρήστες μπορούν να στέλνουν συναλλαγές μέσω της εφαρμογής web σε ένα έξυπνο συμβόλαιο που υλοποιεί το πρωτόκολλο της αγοράς (NFTM), καθώς και ένα token συμβόλαιο για λογαριασμό τους, το οποίο τους επιτρέπει να εκτελούν ποικίλες εργασίες, όπως εξόρυξη και εμπορία, με καθεμία από αυτές τις εργασίες αναφέρεται ως Συμβάν (Bhujel & Rahulamathavan, 2022). Στα πρωτόκολλα NFTM, υπάρχουν τρεις τρόποι αποθήκευσης αυτών των συμβάντων, εκτός αλυσίδας, εντός αλυσίδας ή σε υβριδική αλυσίδα. Το OpenSea χρησιμοποιεί το υβριδικό μοντέλο αποθήκευσης όπου συνδυάζει συμβάντα On-chain και Off-chain, διασφαλίζοντας τη διαφάνεια και την ακεραιότητα των δεδομένων ενώ συνδέει On-chain και Off-chain με κρυπτογραφικούς ελέγχους, παρέχοντας το επίπεδο αποκέντρωσης και ασφάλειας που προσδοκούν οι χρήστες (Bhujel & Rahulamathavan, 2022).

Το OpenSea παρέχει επίσης ένα ευρύ φάσμα εργαλείων και δυνατοτήτων για τους δημιουργούς, καθώς κι ένα ισχυρό API, που επιτρέπει στους προγραμματιστές να ενσωματώνουν τα έργα τους με την πλατφόρμα, δίνοντας τη δυνατότητα στους προγραμματιστές να δημιουργήσουν τις δικές τους αγορές, παιχνίδια και εφαρμογές που χρησιμοποιούν NFTs και το οικοσύστημα OpenSea (White et al., 2022). Τέλος, ένα ακόμα σημαντικό χαρακτηριστικό του OpenSea είναι ότι υποστηρίζει πολλαπλά δίκτυα

blockchain. Η πλατφόρμα επιτρέπει στους χρήστες να δημιουργούν και να ανταλλάσσουν NFT σε πολλά δίκτυα blockchain, συμπεριλαμβανομένων των Ethereum, Polygon, Solana και Klatyn (Bhujel & Rahulamathavan, 2022). Μερικοί ακόμα ηλεκτρονικοί χώροι αγορών για την δημιουργία, διαπραγμάτευση και αγοραπωλησία NFTs είναι το Rarible, το SuperRare και το KnownOrigin.

4.2. Επίδραση της τεχνολογίας Blockchain στα συστήματα ψηφιακών πληρωμών

Όπως αναφέρθηκε παραπάνω, η εξέλιξη των ασύρματων δικτύων τηλεπικοινωνιών και η επικράτηση των έξυπνων κινητών συσκευών αποτελούν παράγοντες που ωθούν τη συνεχή ανάπτυξη και επέκταση της αγοράς ηλεκτρονικού εμπορίου. Το ηλεκτρονικό εμπόριο είναι ένα σύστημα που περιλαμβάνει προμηθευτές, προϊόντα, web domains, ιστοσελίδες, διακομιστές, συστήματα πληρωμής, συστήματα παράδοσης προϊόντων και καταναλωτές (Kim & Kim, 2020). Το σύστημα πληρωμών σε μια πλατφόρμα ηλεκτρονικού εμπορίου είναι ένας κρίσιμος και ουσιαστικός παράγοντας που καθορίζει σε μεγάλο βαθμό την πραγματοποίηση μιας αγοράς από τους καταναλωτές, γι' αυτό εξετάζεται ξεχωριστά στην παρούσα ενότητα.

Με την εξέλιξη της τεχνολογίας διαδικτύου, σχεδόν κάθε τομέας έχει μετασχηματιστεί μεταβαίνοντας από την συμβατική στην ψηφιακή εποχή. Αυτό φυσικά συμπεριλαμβάνει και τις μεθόδους πληρωμής, οι οποίες έχουν υποστεί δραστικές αλλαγές από την ανταλλαγή οντοτήτων στο internet banking (Ahmed et al., 2021). Με την άφιξη της ηλεκτρονικής πληρωμής και τα συστήματα ψηφιακών πορτοφολιών, η πραγματοποίηση πληρωμών έχει γίνει πιο εύκολη από ποτέ και με την αυξανόμενη ζήτηση για τέτοιες υπηρεσίες, ο αριθμός των χρηστών που χρησιμοποιούν συστήματα άμεσης μεταφοράς χρημάτων αυξάνονται ραγδαία (Ahmed et al., 2021). Συνεπώς, η ύπαρξη ενός αξιόπιστου συστήματος ηλεκτρονικών πληρωμών σε μια πλατφόρμα ηλεκτρονικού εμπορίου είναι υψίστης σημασίας προκειμένου οι καταναλωτές να νιώθουν εμπιστοσύνη και να πραγματοποιούν συναλλαγές μέσω αυτής. Ένα αξιόπιστο σύστημα ηλεκτρονικών πληρωμών απαιτεί αμοιβαίο έλεγχο ταυτότητας, μέσω του οποίου τα μέρη που συναλλάσσονται μπορούν να επιβεβαιώσουν το ένα την ταυτότητα του άλλου, εμπιστευτικότητα, η οποία διασφαλίζει ότι τα στοιχεία της συναλλαγής δεν αποκαλύπτονται σε τρίτους, ακεραιότητα, η οποία υποδεικνύει ότι τα μηνύματα δεν

έχουν παραβιαστεί κατά τη μετάδοση, και μη αποκήρυξη, η οποία αποτρέπει την αβάσιμη απόρριψη ολοκληρωμένων συναλλαγών (Kim & Kim, 2020).

Ωστόσο, τα τρέχοντα συστήματα διαδικτυακών πληρωμών αντιμετωπίζουν αρκετά προβλήματα που μπορούν να κλονίσουν την εμπιστοσύνη των καταναλωτών. Αρχικά, υπάρχει ένα ενιαίο σημείο αποτυχίας. Εάν ο κεντρικός διακομιστής στον οποίο λειτουργεί το σύστημα πέσει εκτός λειτουργίας για συντήρηση, οι χρήστες θα αντιμετωπίσουν καθυστερήσεις στη συναλλαγή τους, κάτι που συμβαίνει πολύ συχνά (Ahmed et al., 2021). Επίσης, σε περίπτωση που ο κεντρικός διακομιστής διακοπεί, όλες οι τρέχουσες συναλλαγές αποτυγχάνουν και οι χρήστες πρέπει να τις επαναλάβουν. Επιπρόσθετα, υπάρχουν ζητήματα διαφάνειας και εμπιστευτικότητας, καθώς οποιοσδήποτε στον οργανισμό έχει πρόσβαση στην κεντρική βάση δεδομένων μπορεί να χειριστεί τα δεδομένα, που μπορεί να είναι στοιχεία λογαριασμού χρήστη, υπόλοιπο λογαριασμού, δεδομένα συναλλαγών ή τα ίδια τα δεδομένα του συστήματος (Ahmed et al., 2021). Ακόμα, η ασφάλεια σε τέτοιες διαδικτυακές πληρωμές αποτελεί ένα ζήτημα ζωτικής σημασίας ούτως ώστε να μετριαστούν οι διάφοροι κίνδυνοι και οι οικονομικές ανεπάρκειες. Τέλος, όσον αφορά την περίπτωση των διασυνοριακών συναλλαγών ηλεκτρονικού εμπορίου μέσω πλατφόρμας, τα συνήθη προβλήματα που προκύπτουν είναι η παραποίηση πληροφοριών συναλλαγών, κατάχρηση κεφαλαίων, διαρροή πληροφοριών καταναλωτή, πιστωτικός κίνδυνος συναλλαγής κ.λπ. (Liao & Shao, 2021).

Μια λύση στα παραπάνω προβλήματα παρέχει η χρήση της τεχνολογίας Blockchain, και πιο συγκεκριμένα η πληρωμή μέσω κρυπτονομισμάτων, που αποτελούν την πιο ώριμη εφαρμογή blockchain με ευρεία υιοθέτηση. Τα κρυπτονομίσματα αναφέρονται επίσης ως αποκεντρωμένα συστήματα πληρωμών. Τέτοια αποκεντρωμένα συστήματα πληρωμών δεν βασίζονται σε αξιόπιστα μέρη, όπως για παράδειγμα μια κεντρική τράπεζα, αλλά χρησιμοποιούν ένα δημόσιο κατανεμημένο καθολικό, δηλαδή το blockchain, για την καταγραφή των συναλλαγών. Οι συναλλαγές πραγματοποιούνται απευθείας μεταξύ χρηστών μέσω του P2P δικτύου και επαληθεύονται από κόμβους του δικτύου μέσω της χρήσης κρυπτογραφίας (Zhang et al., 2020), ενώ το blockchain συνδέεται χρονολογικά από έναν κατακερματισμό και σε μεγάλο βαθμό αναπαράγεται από αμοιβαία δύσπιστους κόμβους. Το πρώτο αποκεντρωμένο κρυπτονόμισμα είναι το Bitcoin (Nakamoto, 2008) και αποτελεί ένα παγκόσμιο σύστημα πληρωμών χωρίς κεντρική τράπεζα. Από την

ανάπτυξη του Bitcoin, το 2009, ένας αριθμός κρυπτονομισμάτων έχουν δημιουργηθεί για την κάλυψη διαφορετικών αναγκών και διαφορετικών σκοπών. Τέτοια κρυπτονομίσματα είναι το Ethereum, το οποίο μπορεί να χρησιμοποιηθεί από προγραμματιστές για να πληρωθεί το κόστος συναλλαγών και οι υπηρεσίες στο δίκτυο Ethereum, το Bitcoin Cash, το οποίο δημιουργείται μετά από την σκληρή διακλάδωση (hard fork) του Bitcoin, το Ripple, ένα παγκόσμιο κέντρο διακαθαρισμού για άλλα νομίσματα ή άλλες οντότητες αξίας όπως το δολάριο, το ευρώ, η λίρα και το Bitcoin, το Litecoin, που αποτελεί μια πρώιμη αντικατάσταση του Bitcoin κι έχει σχεδιαστεί για να επιτρέπει στους απλούς ανθρώπους να εξορύσσουν, και το Dash, το οποίο μπορεί να πληρωθεί άμεσα μέσω ενός μοναδικού δικτύου δύο επιπέδων (Zhang et al., 2020).

Εκτός από την χρήση κρυπτονομισμάτων, που αποτελούν μια ήδη υπάρχουσα εφαρμογή, η τεχνολογία Blockchain μπορεί να εφαρμοστεί ως υποδομή για την δημιουργία πλατφόρμας πληρωμών τρίτων. Μια τέτοια εφαρμογή θα μπορούσε να μετριάσει τα προβλήματα που είναι κοινά στα τρέχοντα συστήματα ψηφιακών πληρωμών και να προσφέρει πολλά οφέλη όπως ενίσχυση της εμπιστοσύνης μεταξύ πελατών και εμπόρων, χαμηλότερο κόστος συναλλαγής, μείωση πιστωτικών κινδύνων, εξάλειψη ψευδών πληρωμών καθώς και διαρροής πληροφοριών των καταναλωτών, και τέλος να διασφαλίζει την ασφάλεια των συναλλαγών κατά την πληρωμή (Liao & Shao, 2021).

4.2.1. Περιορισμοί των υφιστάμενων ψηφιακών συστημάτων πληρωμών και πλεονεκτήματα που προσφέρει η χρήση της τεχνολογίας Blockchain

Τα παραδοσιακά συστήματα πληρωμών, όπως οι πιστωτικές κάρτες, οι τραπεζικές μεταφορές και το PayPal, βασίζονται σε μεσάζοντες, όπως τράπεζες, για την επαλήθευση και την επεξεργασία των συναλλαγών. Αυτοί οι μεσάζοντες ενεργούν ως έμπιστα τρίτα μέρη και διαδραματίζουν κρίσιμο ρόλο στη διατήρηση της ασφάλειας και της σταθερότητας του χρηματοπιστωτικού συστήματος. Ωστόσο, αυτή η κεντρική δομή καθιστά επίσης τα παραδοσιακά συστήματα πληρωμών ευάλωτα σε απειλές ασφαλείας, όπως το hacking, η απάτη και η κλοπή ταυτότητας. Επιπρόσθετα, αυτή η κεντρική δομή υποφέρει από ζητήματα διαφάνειας και εμπιστευτικότητας, καθώς ευαίσθητα δεδομένα χρηστών και συναλλαγών είναι εκτεθειμένα σε οποιονδήποτε έχει πρόσβαση στην

κεντρική βάση δεδομένων. Ένα ακόμα κύριο πρόβλημα στα τρέχοντα διαδικτυακά συστήματα πληρωμών είναι πως υπάρχει ένα ενιαίο σημείο αποτυχίας. Έτσι σε περίπτωση που ο κεντρικός διακομιστής στον οποίο λειτουργεί το σύστημα πέσει εκτός λειτουργίας για συντήρηση, οι χρήστες θα αντιμετωπίσουν καθυστερήσεις στη συναλλαγή τους, κάτι που συμβαίνει πολύ συχνά (Ahmed et al., 2021). Επιπλέον, αυτά τα συστήματα μπορεί να είναι αργά και δαπανηρά, ειδικά όσον αφορά τις διασυνοριακές συναλλαγές. Η διαδικασία πληρωμής σε τρέχουσες πύλες πληρωμών περιλαμβάνει πολλά βήματα και συνήθως χρειάζονται 3 ημέρες για να διευθετηθεί μια συναλλαγή, καθώς υπάρχουν πολλά διαφορετικά μέρη που εμπλέκονται στη μεταφορά των χρημάτων, χρονικό διάστημα το οποίο μπορεί να διαρκέσει έως και μία εβδομάδα ή ακόμα περισσότερο στην περίπτωση των διεθνών πληρωμών. Επίσης, οι τράπεζες χρεώνουν υψηλές προμήθειες και τέλη για τέτοιες συναλλαγές, καθώς οι διακομιστές της τράπεζας πρέπει να χειριστούν αυτές τις πρόσθετες συναλλαγές, γεγονός που αυξάνει την υπερφόρτωσή τους (Ahmed et al., 2021).

Από την άλλη πλευρά, τα συστήματα πληρωμών που βασίζονται σε blockchain προσφέρουν λύσεις σε όλα τα παραπάνω προβλήματα. Αρχικά τα συστήματα αυτά είναι αποκεντρωμένα. Οι αποκεντρωμένοι κατανεμημένοι λογαριασμοί του blockchain υποστηρίζουν τη μετάδοση από σημείο σε σημείο με μεγαλύτερη ασφάλεια και αξιοπιστία, αποτρέποντας έτσι την παραποίηση και την υπεξαίρεση πληροφοριών συναλλαγών (Liao & Shao, 2021), εξαλείφοντας επίσης τον κίνδυνο hacking και απάτης. Επιπλέον, η έλλειψη αυτή των διαμεσολαβητών μειώνει τις προμήθειες που καταβάλλονται στα παραδοσιακά συστήματα πληρωμών. Επιπρόσθετα, η χρήση ασύμμετρης κρυπτογραφίας υποστηρίζει ανώνυμες συναλλαγές και προστατεύει τις πληροφορίες αυτών, καθιστώντας τες πιο ασφαλείς, ενώ η χρήση έξυπνων συμβολαίων εγγυάται την αποτελεσματικότητα των συναλλαγών και μειώνει τον πιστωτικό κίνδυνο της συναλλαγής (Liao & Shao, 2021). Τέλος, οι συναλλαγές blockchain υποβάλλονται σε επεξεργασία σε πραγματικό χρόνο, μειώνοντας τον χρόνο αναμονής για την ολοκλήρωση της συναλλαγής και παρέχοντας μια ταχύτερη εναλλακτική λύση σε σχέση με τις παραδοσιακές μεθόδους πληρωμής.

4.2.2. Ψηφιακά συστήματα πληρωμών που βασίζονται στην τεχνολογία Blockchain

Σε αυτό το σημείο θα πραγματοποιηθεί ανάλυση της Monetha, μιας πλατφόρμας ψηφιακών πληρωμών που βασίζεται στην τεχνολογία Blockchain.

Monetha. Είναι μια πλατφόρμα επεξεργασίας πληρωμών ηλεκτρονικού εμπορίου που βασίζεται σε blockchain και στοχεύει στο να διευκολύνει τις αποκεντρωμένες συναλλαγές μεταξύ εμπόρων και πελατών σε όλο τον κόσμο. Τροφοδοτείται από το blockchain Ethereum και χρησιμοποιεί έξυπνα συμβόλαια για την αυτοματοποίηση και τον εξορθολογισμό της διαδικασίας πληρωμής και για την εξασφάλιση ασφαλών και γρήγορων συναλλαγών. Η πλατφόρμα της Monetha προσφέρει μια ποικιλία λειτουργιών, όπως μια πύλη πληρωμής, εργαλεία για τους εμπόρους και ένα πρόγραμμα ανταμοιβής πιστών πελατών. Το πλαίσιο (framework) είναι ασφαλές, απρόσβλητο σε ένα μόνο σημείο ελέγχου ή αστοχίας, και διαφανές, καθώς όλες οι αλληλεπιδράσεις είναι δημόσιες και μπορούν να επαληθευτούν από οποιονδήποτε.

Στον πυρήνα της πλατφόρμας Monetha βρίσκεται η επαναστατική πύλη πληρωμών της, η οποία επιτρέπει ασφαλείς, γρήγορες και χαμηλού κόστους συναλλαγές. Με τα υπάρχοντα συστήματα πληρωμών η διαδικασία πληρωμής είναι ακριβή και αργή, καθώς υπάρχουν έως και 16 διαφορετικά βήματα διευθέτησης μιας συναλλαγής και έως και 15 διαφορετικές χρεώσεις στις πύλες πληρωμών. Η Monetha προσφέρει μια λύση πληρωμών μέσω κινητού, όπου με τη βοήθεια του blockchain Ethereum, μπορούν να πραγματοποιούνται πληρωμές μόνο σε ένα βήμα και με μία μόνο χρέωση, που έχει ως αποτέλεσμα αποδοχή πληρωμών γενικά έως και 5 φορές φθηνότερα και έως και 10000 φορές γρηγορότερα για τους εμπόρους σε σχέση με τα παραδοσιακά συστήματα πληρωμών (Monetha, 2017). Εκτός από την πύλη πληρωμών της, η Monetha προσφέρει επίσης ένα αποκεντρωμένο σύστημα εμπιστοσύνης και φήμης, το οποίο παρακολουθεί την αξιοπιστία των εμπόρων και των πελατών και βοηθά στη διασφάλιση της ευθύνης όλων των χρηστών και της ασφάλειας της πλατφόρμας. Αυτό το σύστημα χρησιμοποιεί έξυπνα συμβόλαια για την αποθήκευση των αξιολογήσεων των εμπόρων και των χρηστών και περιλαμβάνει επίσης λειτουργίες όπως η πρόληψη της απάτης και οι έλεγχοι κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Κάθε φορά που πραγματοποιείται μια συναλλαγή, ανεξάρτητα από το αν πρόκειται για λιανικό ή

ηλεκτρονικό εμπόριο, το blockchain αποθηκεύει όλες τις πληροφορίες που απαιτούνται για τη διασφάλιση της εμπιστοσύνης, όπως τον χρόνο της συναλλαγής, τις διευθύνσεις λήψης και αποστολής, τους όρους εγγύησης, τον χρόνο παράδοσης κτλ, οι οποίες ευαίσθητες πληροφορίες κατακερματίζονται και διατίθενται μόνο σε εξουσιοδοτημένους χρήστες (Monetha, 2017). Με βάση αυτές τις πληροφορίες, οι πελάτες και οι έμποροι θα μπορούν να υποβάλουν/λύσουν μια διαφωνία και να αξιολογήσουν ο ένας τον άλλο, με αποτέλεσμα να παρέχετε στους εμπόρους η ηρεμία ότι οι πληρωμές των πελατών τους θα είναι ασφαλείς και ότι θα μπορούν να εμπιστεύονται τις κριτικές και τις αξιολογήσεις άλλων χρηστών. Επίσης ένα σημαντικό χαρακτηριστικό είναι πως η φήμη που δημιουργείται στην πλατφόρμα είναι μεταβιβάσιμη, δηλαδή, μόλις καθιερωθούν τα δεδομένα φήμης μπορούν να μετακινηθούν αβίαστα σε διάφορες πλατφόρμες ή παρόχους υπηρεσιών.

Τέλος, μία ακόμα λειτουργία που προσφέρει η Monetha είναι ένα παγκόσμιο πρόγραμμα επιβράβευσης, το οποίο παρέχει στους πελάτες εκπτώσεις, ανταμοιβές και άλλα κίνητρα για τη χρήση της πλατφόρμας. Ουσιαστικά, οι χρήστες κερδίζουν πόντους σε αντάλλαγμα για τη διατήρηση του διαδικτυακού τους προφίλ και την κοινή χρήση των δεδομένων τους με εταιρείες. Με άλλα λόγια, οι χρήστες μπορούν να χρησιμοποιούν το ψηφιακό τους προφίλ σαν μια παγκόσμια εκπτωτική κάρτα που ξεκλειδώνει πολλά μεγάλα πλεονεκτήματα (Monetha, 2017). Μπορούν να εξαργυρώνουν αυτούς τους πόντους για προϊόντα, κουπόνια ή να αποκτήσουν πρόσβαση σε αποκλειστικές προσφορές, μέσα από μια παγκόσμια λίστα διαδικτυακών και εκτός σύνδεσης συνεργατών που αποτελούν μέρος του δικτύου Monetha, συμπεριλαμβανομένων ηλεκτρονικών καταστημάτων, καταστημάτων λιανικής, μπαρ και εστιατορίων (Monetha, 2017).

4.3. Τεχνολογία Blockchain και προγράμματα ανταμοιβής πιστών πελατών

Οι στρατηγικές μάρκετινγκ από τις εταιρείες έχουν υποστεί σημαντικούς μετασχηματισμούς με την εφαρμογή του Διαδικτύου, όπως για παράδειγμα οικοδόμηση σχέσεων με τους πελάτες, επιτρέποντας τη διαδραστικότητα και την παροχή πιο εξατομικευμένων προσφορών (Lemos et al., 2022). Οι εταιρείες σχεδόν σε κάθε χώρα, από τα τέλη του 19ου αιώνα, έχουν αναπτύξει και εφαρμόζουν προγράμματα

επιβράβευσης πιστών πελατών, γνωστά και ως προγράμματα αφοσίωσης, για να διατηρήσουν τους πελάτες τους και να τους ενθαρρύνουν να αγοράσουν τα προϊόντα τους, συνήθως, προσφέροντας πόντους και εκπτώσεις (Sönmeztürk & Erten, 2020). Τα προγράμματα αυτά παρέχουν μέσα για τον εντοπισμό ενός συγκεκριμένου πελάτη και τη συστηματική συλλογή και διατήρηση δεδομένων, τα οποία περιλαμβάνουν προσωπικές πληροφορίες, μοτίβα αγορών, ιστορικό συναλλαγών και αγαπημένα κανάλια πωλήσεων, επιτρέποντας έτσι πιο εξατομικευμένες τακτικές μάρκετινγκ (Lemos et al., 2022). Η χρήση τέτοιων προγραμμάτων αναγνωρίζεται ως ένας από τους πιο αποτελεσματικούς τρόπους διασφάλισης της αφοσίωσης των πελατών στην μάρκα και στα προϊόντα ή τις υπηρεσίες που προσφέρει, δημιουργώντας έτσι συνεχώς αυξανόμενες πωλήσεις. Ωστόσο, η αποτελεσματικότητα αυτή έχει πρόσφατα αμφισβητηθεί.

Παραδοσιακά, τα προγράμματα αφοσίωσης υποφέρουν από ζητήματα όπως υψηλό κόστος δημιουργίας και συντήρησης, χαμηλά ποσοστά εξαργύρωσης ανταμοιβών, λίγα κίνητρα συμμετοχής για τους πελάτες και ανησυχίες όσον αφορά την ασφάλεια των δεδομένων. Αρχικά, η δημιουργία και η διατήρηση ενός προγράμματος επιβράβευσης αποτελεί μια σημαντική επένδυση, και ο έλεγχος του λειτουργικού κόστους αποτελεί πρόκληση (Tu et al., 2022). Είτε κάνουν προσαρμογές σε μια υπάρχουσα εφαρμογή, είτε κατασκευάζουν τη δική τους από την αρχή, οι εταιρείες συχνά πληρώνουν υψηλές τιμές για τον προγραμματισμό και την συντήρηση του προγράμματος ανταμοιβής (Srivastava et al., 2019). Επιπρόσθετα, τα έξοδα λειτουργίας ενός τέτοιου προγράμματος περιλαμβάνουν επιπλέον εργασίες μάρκετινγκ, εκπαίδευση των συνεργατών, και τέλος τις ίδιες τις ανταμοιβές που προσφέρονται στους πελάτες (Perez et al., 2020). Όλα αυτά είναι λογικό να δημιουργούν προβληματισμούς στις εταιρείες σχετικά με το αν αξίζει μια τέτοια επένδυση, ειδικότερα όταν υπάρχει αβεβαιότητα ως προς την επιτυχία της.

Επιπλέον, η συμμετοχή των πελατών είναι θεμελιώδης για οποιοδήποτε πρόγραμμα επιβράβευσης, καθώς η ύπαρξη μεγάλου αριθμού μελών δεν αποτελεί εγγύηση για την επιτυχία του προγράμματος (Perez et al., 2020). Σύμφωνα με έρευνες, κατά μέσο όρο, οι καταναλωτές είναι εγγεγραμμένοι σε 14,8 προγράμματα επιβράβευσης, αλλά συμμετέχουν ενεργά μόνο 6,7 από αυτά. Με άλλα λόγια, αν και ο αριθμός των μελών συνεχίζει να αυξάνεται, μόνο τα μισά από αυτά τα μέλη είναι ενεργά (Tu et al., 2022). Αυτό οφείλεται σε πολλούς παράγοντες, όπως για παράδειγμα στην ευκολία χρήσης του

προγράμματος. Πολλές φορές η ύπαρξη καρτών μέλους ή οι περίπλοκες διαδικασίες εγγραφής αντί να ενισχύουν την εμπειρία του πελάτη μπορούν στην πραγματικότητα να έχουν το αντίθετο αποτέλεσμα (Srivastava et al., 2019). Σύμφωνα με έρευνα, το 33% των millennial καταναλωτών αντιπαθούν τα προγράμματα επιβράβευσης απλώς και μόνο επειδή υπάρχουν πάρα πολλές κάρτες για να κουβαλούν μαζί τους (Srivastava et al., 2019). Επίσης, σύμφωνα με μια άλλη έρευνα, το 57% των μελών αυτών των προγραμμάτων επιβράβευσης πιστεύει ότι χρειάζεται πολύς χρόνος για να κερδίσει μια ανταμοιβή και το 53% πιστεύει ότι οι ανταμοιβές που δίνουν αυτά τα συστήματα δεν είναι πολύ ενδιαφέρουσες (Sönmeztürk & Erten, 2020). Αυτή η έλλειψη κινήτρων οδηγεί σε χαμηλή ικανοποίηση των πελατών, η οποία με την σειρά της οδηγεί σε ένα ακόμα ζήτημα, στα χαμηλά ποσοστά εξαργύρωσης πόντων. Τέλος, ορισμένοι καταναλωτές είναι επιφυλακτικοί σχετικά και την ασφάλεια των προσωπικών τους δεδομένων και ανησυχούν για ενδεχόμενη παραβίαση αυτών. Μια δημοσκόπηση της Harris Poll διαπίστωσε ότι το 71% των καταναλωτών ήταν λιγότερο πιθανό να συμμετάσχουν σε ένα πρόγραμμα επιβράβευσης πιστών πελατών που συνέλεγε προσωπικές πληροφορίες πέρα από το όνομα και τον αριθμό τηλεφώνου (Srivastava et al., 2019).

Για όλους αυτούς τους λόγους πολλοί μελετητές στο μάρκετινγκ έχουν αρχίσει να αμφισβητούν τη συνολική αποτελεσματικότητα των προγραμμάτων αφοσίωσης στη διατήρηση των καταναλωτών, και τονίζουν την ανάγκη βελτίωσης των υφιστάμενων προγραμμάτων (Rahman, 2021). Η τεχνολογία Blockchain επιλύει τα παραπάνω ζητήματα, προσφέροντας νέες μεθόδους στον τρόπο με τον οποίο αναπτύσσονται, παρακολουθούνται και διαδίδονται στους πελάτες τα συστήματα ανταμοιβής πιστών πελατών, όπως επίσης θεωρείται ότι είναι καλός υποψήφιος για να ανταποκριθεί στις νέες προσδοκίες των χρηστών απέναντι στα συστήματα αφοσίωσης και να τα κάνει πιο αξιόπιστα (Sönmeztürk & Erten, 2020). Στην συνέχεια εξετάζονται λεπτομερώς τα πλεονεκτήματα που προσφέρει η τεχνολογία Blockchain στα προγράμματα επιβράβευσης πιστών πελατών.

4.3.1. Πλεονεκτήματα προγραμμάτων ανταμοιβής πιστών πελατών που βασίζονται στην τεχνολογία Blockchain

Όπως αναφέρθηκε παραπάνω, παραδοσιακά, τα προγράμματα αφοσίωσης υποφέρουν από ζητήματα όπως υψηλό κόστος, χαμηλά ποσοστά εξαργύρωσης, λίγα κίνητρα συμμετοχής για τους πελάτες και ανησυχίες όσον αφορά την ασφάλεια. Η τεχνολογία Blockchain είναι σε θέση να επιλύσει τα παραπάνω ζητήματα, οδηγώντας στην δημιουργία βελτιωμένων και πιο αποτελεσματικών προγραμμάτων. Θεωρείται κατάλληλη για τη διαχείριση άυλων περιουσιακών στοιχείων, όπως οι πόντοι ανταμοιβής σε ένα τέτοιο πρόγραμμα, καθώς το blockchain είναι ένα κατανεμημένο καθολικό που διέπεται από ένα δίκτυο ομοτίμων και τα δεδομένα που είναι αποθηκευμένα σε αυτό είναι αμετάβλητα και ανιχνεύσιμα (Tu et al., 2022).

Αρχικά, ένα πρόγραμμα επιβράβευσης πελατών που βασίζεται σε blockchain μπορεί μειώσει το κόστος της διαχείρισης του συστήματος με την χρήση έξυπνων συμβολαίων που αναφέρουν ασφαλείς, ανιχνεύσιμες και διαφανείς συναλλαγές, μειώνοντας το κόστος που σχετίζεται με σφάλματα και απάτες (Srivastava et al., 2019). Εκτός από τη μείωση του λειτουργικού κόστους, τα προγράμματα που είναι βασισμένα σε blockchain μπορούν επίσης να επηρεάσουν τις συμπεριφορές συμμετοχής των πελατών μέσω τριών χαρακτηριστικών. Οι συναλλαγές γίνονται σχεδόν σε πραγματικό χρόνο, υπάρχει δυνατότητα δημιουργίας προγράμματος συνασπισμού μεταξύ πολλών επωνυμιών, και καθίσταται δυνατή η ανταλλαγή πόντων μεταξύ των ομοτίμων (Tu et al., 2022). Αυτά τα χαρακτηριστικά μπορούν να καλλιεργήσουν κίνητρα στους πελάτες να συμμετάσχουν πιο ενεργά στο πρόγραμμα.

Πιο συγκεκριμένα, η αποκεντρωμένη φύση της τεχνολογίας Blockchain επιτρέπει στα μέλη του προγράμματος να παρακολουθούν τους πόντους και τις ανταμοιβές τους σχεδόν σε πραγματικό χρόνο, απελευθερώνοντας τις εταιρείες και τα ίδια τα μέλη από τη φυσική κατοχή καρτών και κουπονιών, δίνοντάς τους μεγαλύτερη ιδιοκτησία και ευελιξία στις ανταμοιβές τους και μια εμπειρία πιο ευχάριστη, χωρίς τριβές (Madhani, 2022). Επιπλέον, τα προγράμματα ανταμοιβής πιστών πελατών που βασίζονται σε blockchain μπορούν να κοινοποιηθούν πιο εύκολα μεταξύ διαφορετικών επιχειρήσεων. Ένα πρόβλημα με τα παραδοσιακά προγράμματα επιβράβευσης είναι ότι συχνά περιορίζονται σε μία συγκεκριμένη επιχείρηση και οι χρήστες συνήθως πρέπει να

μείνουν εντός του συστήματος για μεγάλο χρονικό διάστημα προκειμένου να συγκεντρώνουν πόντους για να κερδίσουν ανταμοιβές, που μπορεί να μην είναι πολύ ενδιαφέρουσες τις περισσότερες φορές (Sönmeztürk & Erten, 2020). Με τα προγράμματα αφοσίωσης που βασίζονται σε blockchain, οι πελάτες μπορούν να κερδίσουν πόντους από πολλές επιχειρήσεις και να τους εξαργυρώσουν σε ένα μόνο μέρος. Επίσης ένα τέτοιο πρόγραμμα θα μπορούσε να δώσει την δυνατότητα στους χρήστες να ανταλλάσσουν μεταξύ τους απευθείας πόντους που εκδίδονται από διαφορετικές εταιρείες (Tu et al., 2022). Όλα αυτά δίνουν κίνητρα στα μέλη του προγράμματος να έχουν πιο ενεργή συμμετοχή, γεγονός που επίσης συμβάλει στην μείωση των χαμηλών ποσοστών εξαργύρωσης.

Ένα ακόμα πλεονέκτημα των προγραμμάτων ανταμοιβής πιστών πελατών που βασίζονται στην τεχνολογία Blockchain είναι πως μπορούν να ενσωματωθούν πιο εύκολα με άλλα συστήματα. Δεδομένου ότι ένα blockchain είναι ένα αποκεντρωμένο και κατανεμημένο καθολικό, μπορεί εύκολα να έχει πρόσβαση και να ενημερώνεται από πολλά μέρη. Έτσι, με την χρήση της τεχνολογίας Blockchain σε ένα οικοσύστημα μάρκετινγκ, όλα τα μέρη που συμμετέχουν σε προγράμματα αφοσίωσης πελατών, όπως έμποροι, καταναλωτές, διαχειριστές συστημάτων πληροφοριών, υποστήριξη πελατών, σημεία πώλησης και άλλοι οργανισμοί, θα μπορούν να είναι αποτελεσματικά διασυνδεδεμένα και ενσωματωμένα (Madhani, 2022). Αντί για ένα κατακερματισμένο σύστημα, όλα τα μέρη που ασχολούνται με τα προγράμματα επιβράβευσης μπορούν να εργαστούν συνεργικά για να βελτιώσουν την εμπειρία των πελατών, οδηγώντας έτσι σε αυξημένη αρμονία καναλιών και ρευστή εμπειρία πελατών (Rahman, 2021).

Τέλος, η τεχνολογία Blockchain μπορεί να δημιουργήσει ένα πιο ασφαλές και διαλειτουργικό περιβάλλον που δεν είναι εφικτό με κεντρικές βάσεις δεδομένων (Madhani, 2022). Ο αμετάβλητος και ανιχνεύσιμος χαρακτήρας της τεχνολογίας παρέχει βεβαιότητα στο σύστημα ότι οι πληροφορίες είναι έγκυρες, παρά το γεγονός ότι προέρχεται από διαφορετικές πηγές, όπως επίσης κανείς δεν μπορεί να επιχειρήσει να κάνει κατάχρηση του συστήματος χωρίς αυτή η προσπάθεια να γίνει ορατή από τους άλλους συμμετέχοντες (Perez et al., 2020).

4.3.2. Εφαρμογές προγραμμάτων ανταμοιβής πιστών πελατών που βασίζονται στην τεχνολογία Blockchain

Στο σημείο αυτό θα πραγματοποιηθεί ανάλυση δύο προγραμμάτων επιβράβευσης πιστών πελατών που βασίζονται στην τεχνολογία Blockchain.

Asia Miles. Η ασιατική αεροπορική εταιρεία Cathay Pacific μεταμόρφωσε το πρόγραμμα επιβράβευσής της, Asia Miles, σε συνεργασία με την Accenture, αναπτύσσοντας τεχνολογία Blockchain και επιτρέποντας έτσι στους πελάτες, τους συνεργάτες αεροπορικών εταιρειών και την ίδια την αεροπορική εταιρεία να διαχειρίζονται αεροπορικά μίλια και ανταμοιβές μελών σε πραγματικό χρόνο με ένα νέο κρυπτονόμισμα που ονομάζεται "BigCoin" (Madhani, 2022). Το πρόγραμμα αφοσίωσης Asia Miles λειτουργεί επιβραβεύοντας τα μέλη με μίλια για τη συμμετοχή τους σε διάφορες δραστηριότητες όπως αγορές, ταξίδια, φαγητό σε εστιατόρια και πολλά άλλα. Τα μέλη κερδίζουν μίλια για αυτές τις δραστηριότητες, τα οποία στη συνέχεια μπορούν να εξαργυρωθούν για μια ποικιλία ανταμοιβών, όπως πτήσεις, διαμονή σε ξενοδοχεία και εμπορεύματα. Τα μίλια που κερδίζονται καταγράφονται σε ένα καθολικό blockchain, το οποίο παρέχει μια ασφαλή και διαφανή καταγραφή της δραστηριότητας και των ανταμοιβών ενός μέλους.

Η αποτελεσματικότητα του προγράμματος έχει βελτιωθεί με τη χρήση της τεχνολογίας Blockchain, καθώς οι συναλλαγές διεκπεραιώνονται γρήγορα και με ασφάλεια, μειώνοντας τον χρόνο που χρειάζονται τα μίλια για να πιστωθούν στον λογαριασμό ενός μέλους. Αυτό επιτρέπει στα μέλη να λαμβάνουν τις ανταμοιβές τους έγκαιρα και να απολαμβάνουν τα οφέλη του προγράμματος πιο γρήγορα. Επίσης, η διαδικασία εξαργύρωσης γίνεται εύκολη και βολική, με τα μέλη να έχουν πρόσβαση στις πληροφορίες του λογαριασμού τους και να παρακολουθούν τις ανταμοιβές τους από οπουδήποτε στον κόσμο. Επιπρόσθετα, με την εφαρμογή για κινητά, το Asia Miles αναλύει τη συμπεριφορά των πελατών και προσφέρει στους χρήστες εξατομικευμένες προτάσεις ακολουθώντας τεχνικές ενεργής εξατομίκευσης (Polat, 2022). Επιπλέον, η εφαρμογή έχει τη δυνατότητα αλληλεπίδρασης με βάση τα συμφραζόμενα, προσφέροντας στους χρήστες πληροφορίες σχετικά με την περιοχή στην οποία ταξιδεύουν, όπως για παράδειγμα διαθέσιμα εστιατόρια, δίνοντάς τους έτσι την δυνατότητα να διαχειρίζονται πλήρως τα ταξίδια τους (Polat, 2022).

Loyyal. Είναι μια start-up που ιδρύθηκε το 2014 με έδρα το Σαν Φρανσίσκο. Αποτελεί μια πλατφόρμα αφοσίωσης και ανταμοιβών που βασίζεται στην τεχνολογία Blockchain και την χρήση έξυπνων συμβολαίων, με στόχο να βοηθά τις επιχειρήσεις να δημιουργούν και να διαχειρίζονται προγράμματα επιβράβευσης. Επιτρέπει στους πελάτες να κερδίζουν και να εξαργυρώνουν ανταμοιβές σε πολλές επωνυμίες και κανάλια ενώ παράλληλα δίνει τη δυνατότητα στις επιχειρήσεις να παρακολουθούν και να διαχειρίζονται εύκολα την αφοσίωση των πελατών. Η Loyyal χρησιμοποιεί την πλατφόρμα Hyperledger Fabric με σκοπό να ενοποιήσει τον κατακερματισμένο κλάδο προγραμμάτων αφοσίωσης πελατών εισάγοντας διαλειτουργικότητα δεδομένων μεταξύ των προγραμμάτων αυτών, επιτρέποντας συμμαχίες πολλών προμηθευτών, δυναμικές επιλογές έκδοσης και εξαργύρωσης πόντων σε κάθε πελάτη, διαφάνεια σχεδόν σε πραγματικό χρόνο, εξοικονόμηση κόστους, πρόληψη απάτης και κατάχρησης και γενικά ενισχυμένη διατήρηση και ικανοποίηση πελατών, μέσω ενός μόνο ψηφιακού πορτοφολιού (Ahmad et al., 2021).

Χρησιμοποιώντας την εφαρμογή για smartphone της Loyyal, ο χρήστης κερδίζει πόντους κάθε φορά που εκτελεί συγκεκριμένες δραστηριότητες όπως ταξίδια, επίσκεψη σε μουσεία ή διαμονή σε ξενοδοχεία, και μπορεί να χρησιμοποιήσει αυτούς τους κερδισμένους πόντους για να αντισταθμίσει το κόστος των υπόλοιπων τουριστικών του δραστηριοτήτων (Morabito, 2017). Για παράδειγμα, όταν ένας χρήστης αγοράζει αεροπορικά εισιτήρια από μία πόλη για μια άλλη, η πιστωτική του κάρτα μεταφέρει τους πόντους που απονέμονται στο ψηφιακό του πορτοφόλι σε πραγματικό χρόνο. Με αυτόν τον τρόπο, ο χρήστης μπορεί να χρησιμοποιήσει αμέσως τους πόντους που μόλις κέρδισε για να αναβαθμίσει το δωμάτιό του σε ένα τοπικό ξενοδοχείο της πόλης που επισκέπτεται. Έτσι, σε αυτό το παράδειγμα, ο πελάτης μπορεί να απολαύσει μια βελτιωμένη εμπειρία, ενώ ταυτόχρονα οι αεροπορικές εταιρείες και οι ξενοδοχειακές εταιρείες έχουν αποκτήσει έναν πιο χαρούμενο και ικανοποιημένο πελάτη που είναι πολύ πιθανό να επιστρέψει (Morabito, 2017).

4.4. Επίδραση της τεχνολογίας Blockchain στην έγκριση και αξιολόγηση των κινητών εφαρμογών

Όπως έχει ήδη αναφερθεί αρκετές φορές σε αυτό το κεφάλαιο, η ταχεία και ανεξέλεγκτη ανάπτυξη του Διαδικτύου και η δημιουργία του ηλεκτρονικού εμπορίου έχουν αλλάξει ριζικά την συμπεριφορά των καταναλωτών, μεταφέροντάς την από την αναλογική εποχή στην ψηφιακή. Με την τεράστια ροή πληροφοριών που υπάρχει στο Διαδίκτυο, οι χρήστες διαφορετικών πλατφορμών ηλεκτρονικού εμπορίου που αναζητούν ορισμένα προϊόντα ή υπηρεσίες έρχονται αντιμέτωποι με έναν μεγάλο αριθμό επιλογών, καθιστώντας τη διαδικασία λήψης αποφάσεων σύνθετη και χρονοβόρα. Το φιλτράρισμα πληροφοριών είναι μια σημαντική διαδικασία που ανακουφίζει αυτό το πρόβλημα και βοηθά τους χρήστες να λαμβάνουν ικανοποιητικές αποφάσεις με ευκολία (Mekouar et al., 2022). Αυτή η διαδικασία φιλτραρίσματος επιτυγχάνεται μέσα από τα συστήματα συστάσεων (Recommender Systems), τα οποία παρέχουν μια λύση στο κρίσιμο ζήτημα της υπερφόρτωσης πληροφοριών, διευκολύνοντας έτσι τη διαδικασία αγορών.

Το σύστημα συστάσεων είναι ένα εργαλείο λογισμικού που παρέχει εξατομικευμένες προτάσεις στους χρήστες για στοιχεία όπως προϊόντα, υπηρεσίες ή περιεχόμενο, σύμφωνα με τις προτιμήσεις και τα ενδιαφέροντά τους. Χρησιμοποιεί τεχνικές ανάλυσης δεδομένων για να προβλέψει τις προτιμήσεις και τα ενδιαφέροντα ενός χρήστη με βάση τη συμπεριφορά, τις ενέργειες και τα σχόλιά του. Στην σημερινή εποχή, τα συστήματα συστάσεων βρίσκονται παντού στην καθημερινή ζωή των ανθρώπων και τους υποστηρίζουν στη λήψη αποφάσεων. Δεν χρησιμοποιούνται μόνο από ιστότοπους ηλεκτρονικού εμπορίου και διαδικτυακές αγορές, αλλά και από τα μέσα κοινωνικής δικτύωσης, όπως το Facebook, το LinkedIn και το YouTube, από διαδικτυακές συνδρομητικές υπηρεσίες, όπως το Netflix, από υπηρεσίες ροής, πλατφόρμες που βασίζονται σε cloud και εφαρμογές για κινητές συσκευές. Οι επιχειρήσεις χρησιμοποιούν συστήματα συστάσεων για να επιταχύνουν τις αναζητήσεις και να διευκολύνουν τους χρήστες να έχουν πρόσβαση σε περιεχόμενο σχετικό με αυτούς, εστιάζοντας στη δημιουργία ενός εξατομικευμένου ταξιδιού για τον χρήστη και μια συνολικά βελτιωμένη εμπειρία, η οποία έχει ως αποτέλεσμα αυξημένη διατήρηση πελατών και πωλήσεις (Mekouar et al., 2022).

Για τη δημιουργία των προτάσεων, τα συστήματα συστάσεων βασίζονται στη συλλογή δεδομένων από τους χρήστες, από τα οποία μπορούν να συναχθούν πληροφορίες για τις προτιμήσεις τους. Τα δεδομένα μπορούν να συλλεχθούν με δύο τρόπους, είτε ρητά, συλλέγοντας τις αξιολογήσεις που υποβλήθηκαν από τους χρήστες, είτε σιωπηρά, παρακολουθώντας τη συμπεριφορά των χρηστών, όπως για παράδειγμα το ιστορικό περιήγησης, τις εφαρμογές που έχουν ληφθεί, τα τραγούδια που ακούστηκαν κ.λπ., καθώς επίσης συλλέγονται δημογραφικά χαρακτηριστικά, συμπεριλαμβανομένης της ηλικίας, του φύλου και της εθνικότητας (Abduljabbar et al., 2021). Οι μεγάλες αυτές ποσότητες δεδομένων που συλλέγονται μεταφορτώνονται σε έναν διακομιστή όπου εκτελείται η προ-επεξεργασία και η αναπαράσταση δεδομένων, η οποία στην συνέχεια χρησιμοποιείται ως είσοδος σε έναν αλγόριθμο σύστασης (Mekouar et al., 2022). Ο αλγόριθμος πραγματοποιεί τους υπολογισμούς από τους οποίους προκύπτουν οι συστάσεις που αποστέλλονται πίσω στους χρήστες. Επομένως, το γενικό πλαίσιο ενός συστήματος συστάσεων αποτελείται από τη συλλογή δεδομένων και την κεντρική αποθήκευση, την προ-επεξεργασία και αναπαράσταση δεδομένων, τον υπολογισμό με συγκεκριμένο αλγόριθμο και τέλος τη σύσταση (Mekouar et al., 2022).

Ανάλογα με τον τρόπο με τον οποίο οι αλγόριθμοι των συστημάτων συστάσεων δημιουργούν συστάσεις, μπορούν να κατηγοριοποιηθούν σε διάφορους τύπους, με τις κυριότερες τεχνικές φιλτραρίσματος να είναι τρεις. Αρχικά, υπάρχει το συνεργατικό φιλτράρισμα (Collaborative Filtering), ένας τύπος αλγορίθμου συστάσεων που αναλύει τη συμπεριφορά και τις προτιμήσεις μιας ομάδας χρηστών για να κάνει συστάσεις για μεμονωμένους χρήστες. Αυτή η προσέγγιση βασίζεται στη συμπεριφορά των προηγούμενων χρηστών και στοχεύει στον εντοπισμό νέων συσχετίσεων χρήστη-αντικειμένων, αναλύοντας τις σχέσεις μεταξύ ενός χρήστη και τις αλληλεξαρτήσεις μεταξύ των προϊόντων (Abduljabbar et al., 2021). Η δεύτερη κατηγορία είναι το φιλτράρισμα βάσει περιεχομένου (Content-Based Filtering). Αυτά τα συστήματα προσπαθούν να προτείνουν αντικείμενα στους χρήστες που είναι παρόμοια με αυτά που τους άρεσαν στο παρελθόν. Η κύρια εστίασή τους είναι η χρήση αλγορίθμων για την εκμάθηση των προτιμήσεων των χρηστών και το φιλτράρισμα ενός συνόλου νέων στοιχείων που πιθανότατα ταιριάζουν με τις προτιμήσεις του χρήστη (Abduljabbar et al., 2021). Τέλος, υπάρχει το υβριδικό φιλτράρισμα (Hybrid Filtering), που αποτελεί έναν

συνδυασμό των δύο προηγούμενων τεχνικών, δηλαδή, του συνεργατικού φιλτραρίσματος και του φιλτραρίσματος βάσει περιεχομένου.

Όπως γίνεται αντιληπτό, τα συστήματα συστάσεων απαιτούν την ανάλυση και εξόρυξη τεράστιων ποσοτήτων διαφόρων τύπων δεδομένων χρηστών, προκειμένου να δημιουργηθούν ακριβείς συστάσεις. Τέτοια σύνολα δεδομένων συχνά περιλαμβάνουν ευαίσθητες πληροφορίες, ωστόσο τα περισσότερα συστήματα συστάσεων εστιάζουν στην ακρίβεια των μοντέλων και αγνοούν ζητήματα που σχετίζονται με την ασφάλεια και το απόρρητο των χρηστών (Himeur et al., 2022). Για την αντιμετώπιση αυτών των ζητημάτων ασφάλειας και διατήρησης της ιδιωτικής ζωής η τεχνολογία Blockchain παρουσιάζεται ως μια πολλά υποσχόμενη λύση. Η ενσωμάτωση της τεχνολογίας αυτής σε συστήματα συστάσεων παρέχει έναν πιο ασφαλή και διαφανή τρόπο διαχείρισης των δεδομένων του χρήστη και βελτιώνει τις προτάσεις των εφαρμογών, οδηγώντας τελικά σε καλύτερη εμπειρία χρήστη (Umekwudo & Shim, 2020)

Στην συνέχεια πραγματοποιείται ανάλυση των συστημάτων συστάσεων για κινητές εφαρμογές και των πλεονεκτημάτων που προσφέρει η ενσωμάτωση της τεχνολογίας Blockchain σε αυτά.

4.4.1. Συστήματα συστάσεων για κινητές εφαρμογές και πλεονεκτήματα που προσφέρει η τεχνολογία Blockchain

Εκτός από την ταχεία ανάπτυξη του Διαδικτύου, ραγδαία είναι και η εξέλιξη των έξυπνων κινητών συσκευών, όπως τα έξυπνα τηλέφωνα, τα tablets και τα έξυπνα ρολόγια, με διαφορετικούς τύπους να εισάγονται καθημερινά στην αγορά. Το επίθετο "κινητός" αναφέρεται στη φορητότητα της συσκευής και συνεπάγεται την οικουμενική πρόσβαση του χρήστη σε πληροφορίες, δηλαδή από οποιοδήποτε μέρος σε οποιαδήποτε χρονική στιγμή. Αυτή η δυνατότητα πρόσβασης σε πληροφορίες και εφαρμογές ανά πάσα στιγμή, ανεξάρτητα από τη γεωγραφική θέση του χρήστη, έχει ως αποτέλεσμα στην εποχή μας η χρήση των κινητών συσκευών να ξεπερνά την χρήση των επιτραπέζιων και φορητών υπολογιστών. Το γεγονός αυτό έχει οδηγήσει πολλούς προγραμματιστές στο να υιοθετήσουν την προσέγγιση "mobile first", δηλαδή "πρώτα το κινητό", οδηγώντας έτσι στην ανάπτυξη εκατομμύρια εφαρμογών για κινητές συσκευές,

οι οποίες εμφανίζονται για να αναλάβουν κάθε πτυχή των δραστηριοτήτων των χρηστών (Umekwudo & Shim, 2020).

Οι εφαρμογές για κινητά τηλέφωνα, γνωστές ως mobile apps, είναι προγράμματα λογισμικού που έχουν αναπτυχθεί για κινητές συσκευές και διατίθενται στις αγορές εφαρμογών, γνωστές ως app stores, όπου οι χρήστες μπορούν να περιηγηθούν, να κατεβάσουν και να εγκαταστήσουν κινητές εφαρμογές στις συσκευές τους. Δύο δημοφιλείς αγορές εφαρμογών είναι το Google Play Store, για συσκευές Android, και το Apple App Store, για συσκευές iOS όπως το iPad και το iPhone. Υπάρχουν επίσης άλλες αγορές όπως το Amazon Appstore για συσκευές Android, το Huawei AppGallery για συσκευές της Huawei, και το Galaxy Store για συσκευές Samsung. Αυτές οι αγορές ακολουθούν ένα κεντρικό μοντέλο, στο οποίο μία οντότητα είναι υπεύθυνη για την διασφάλιση των βασικών χαρακτηριστικών της διανομής λογισμικού, δηλαδή την παράδοση, την ανακάλυψη εφαρμογών, τις οικονομικές συναλλαγές και την έγκριση εφαρμογών (Trezentos & Pires, 2017). Αυτός ο συγκεντρωτισμός συνοδεύεται από εγγενή μειονεκτήματα, με το κυριότερο να είναι η λίγη έως καθόλου διαφάνεια, και κάποια άλλα, όπως η έλλειψη εμπιστοσύνης και η οικονομική αναποτελεσματικότητα.

Η ύπαρξη όλων αυτών των αγορών και ο τεράστιος αριθμός των εφαρμογών που είναι διαθέσιμες σε αυτές, δυσκολεύει τους χρήστες να βρουν την κατάλληλη εφαρμογή για τις ανάγκες τους. Τα συστήματα συστάσεων έρχονται να βοηθήσουν, αξιοποιώντας πληροφορίες όπως ο αριθμός των λήψεων, οι ενεργοί χρήστες και η συχνότητα χρήσης, για να προτείνουν εφαρμογές που ταιριάζουν στα ενδιαφέροντα και τη συμπεριφορά του κάθε χρήστη (Umekwudo & Shim, 2020). Υπάρχουν πολλά τέτοια συστήματα, όπως το AppJoy, το AppsFire, το AppAware και το Appazzar. Ωστόσο, όλα αυτά τα συστήματα εστιάζουν στην ακρίβεια των μοντέλων και αγνοούν ζητήματα που σχετίζονται με την ασφάλεια και το απόρρητο των χρηστών (Himeur et al., 2022). Πάνω στα ζητήματα της διαφάνειας, της έλλειψης εμπιστοσύνης, ασφάλειας και απορρήτου, η τεχνολογία Blockchain παρουσιάζεται ως μια πολλά υποσχόμενη λύση, που εγγυάται κρυπτογραφικά το απόρρητο του χρήστη και μπορεί να βοηθήσει σημαντικά στη βελτίωση των πλαισίων συστάσεων, διασφαλίζοντας την ασφάλεια, την ακεραιότητα των δεδομένων, την εμπιστευτικότητα και την προσβασιμότητα (Umekwudo & Shim, 2020).

Αρχικά, η τεχνολογία Blockchain παρέχει έναν αποκεντρωμένο τρόπο διαχείρισης των δεδομένων των χρηστών στα συστήματα συστάσεων εφαρμογών. Αυτό σημαίνει ότι δεν υπάρχει κεντρική αρχή που έχει πρόσβαση και έλεγχο στα δεδομένα, καθώς οι ευαίσθητες πληροφορίες των χρηστών αποθηκεύονται σε ένα κατανεμημένο καθολικό και είναι πλήρως κρυπτογραφημένες, προσφέροντας ένα υψηλό επίπεδο ασφάλειας (Abduljabbar et al., 2021). Αυτή η αποκέντρωση δημιουργεί επίσης αξιοπιστία στο σύστημα, καθώς δεν απαιτείται εμπιστοσύνη σε μια κεντρική αρχή αλλά στον μηχανισμό συναίνεσης, ο οποίος διασφαλίζει ότι η κατάσταση του καθολικού ενημερώνεται με τη συμφωνία ή τη συναίνεση όλων των συμμετεχόντων (Mekouar et al., 2022). Αυτό συμβάλει στη δημιουργία ενός πιο αξιόπιστου συστήματος συστάσεων, στο οποίο μπορούν να βασίζονται οι χρήστες για ακριβείς και αμερόληπτες συστάσεις.

Επιπλέον, η τεχνολογία Blockchain επιτρέπει τη δημιουργία διαφανών αλγορίθμων στα συστήματα συστάσεων. Συχνά, οι χρήστες δεν γνωρίζουν πώς διαμορφώνονται οι προτάσεις εφαρμογών λόγω της έλλειψης διαφάνειας στους αλγορίθμους. Μέσω της τεχνολογίας Blockchain, οι αλγόριθμοι αυτοί μπορούν να γίνουν πιο διαφανείς, διατηρώντας παράλληλα το απόρρητο των χρηστών, καθώς η δύναμη του συστήματος blockchain είναι να κάνει υπολογισμούς χωρίς να αποκαλύπτει τις πληροφορίες των χρηστών (Abduljabbar et al., 2021). Για παράδειγμα, τα συστήματα προτάσεων εφαρμογών μπορούν να χρησιμοποιούν έξυπνα συμβόλαια, για να παρέχουν έναν σαφή και διαφανή τρόπο παρακολούθησης του τρόπου με τον οποίο γίνονται οι προτάσεις και να επιτρέπουν στους χρήστες να επαληθεύουν ότι τα δεδομένα τους χρησιμοποιούνται με δίκαιο και διαφανή τρόπο. Έτσι οι χρήστες δεν αγνοούν πλέον πώς προβλέπονται οι βαθμολογίες των εφαρμογών, καθώς τα στοιχεία, οι χρήστες και οι λειτουργίες υπολογισμού βαθμολογίας είναι ορατά σε όλους τους χρήστες του συστήματος (Mekouar et al., 2022).

4.4.2. Συστήματα συστάσεων που βασίζονται στη τεχνολογία Blockchain

Σε αυτό το σημείο θα πραγματοποιηθεί ανάλυση του πρωτοκόλλου AppCoins, που αποτελεί ένα παράδειγμα εφαρμογής της τεχνολογίας Blockchain στην διαδικασία έγκρισης και αξιολόγησης των κινητών εφαρμογών

AppCoins. Είναι ένα και κατανεμημένο πρωτόκολλο ανοιχτού κώδικα, το οποίο χρησιμοποιεί τεχνολογία Blockchain για να δημιουργήσει μια πιο διαφανή και αποτελεσματική οικονομία κινητών εφαρμογών. Το πρωτόκολλο AppCoins είναι χτισμένο πάνω από το blockchain Ethereum και έχει σχεδιαστεί για να αντιμετωπίζει πολλές από τις προκλήσεις που αντιμετωπίζει ο κλάδος των εφαρμογών για κινητές συσκευές σήμερα, όπως η απόκτηση χρηστών, η δημιουργία εσόδων και η εμπιστοσύνη. Παρέχει μια πλατφόρμα για τους προγραμματιστές ώστε να δημιουργούν και να διανέμουν εφαρμογές για κινητές συσκευές, λαμβάνοντας ένα δίκαιο μερίδιο των εσόδων που δημιουργούνται από τις εφαρμογές τους, ενώ παράλληλα επιτρέπει στους χρήστες να ανακαλύψουν, να εγκαταστήσουν και να χρησιμοποιήσουν αυτές τις εφαρμογές με πιο αποτελεσματικό και ασφαλή τρόπο.

Αρχικά, το πρωτόκολλο AppCoins εισάγει το λεγόμενο σύστημα Απόδειξης Προσοχής (Proof-of-Attention). Ο μηχανισμός απόδειξης προσοχής περιλαμβάνει την παρακολούθηση και την επαλήθευση των αλληλεπιδράσεων των χρηστών εντός εφαρμογών, με την χρήση της τεχνολογίας Blockchain. Αξιοποιώντας έξυπνα συμβόλαια, το πρωτόκολλο μπορεί να επικυρώσει και να καταγράψει την προσοχή και τις δραστηριότητες των χρηστών, όπως η ολοκλήρωση ορισμένων εργασιών, η παρακολούθηση διαφημίσεων, η παροχή σχολίων ή η συμμετοχή σε αγορές εντός εφαρμογής. Αυτό επιτρέπει στους προγραμματιστές να επαληθεύσουν ότι οι χρήστες όντως έδωσαν προσοχή στην εφαρμογή τους για τον απαιτούμενο χρόνο (Trezentos & Pires, 2017). Πιο συγκεκριμένα, οι προγραμματιστές χρησιμοποιούν το "AppCoin" token για να διαφημίσουν τις εφαρμογές τους στους χρήστες, οι οποίοι κερδίζουν tokens ως ανταμοιβή για την ενεργή συμμετοχή και την προσοχή τους. Τα tokens αυτά μπορούν να χρησιμοποιηθούν για αγορές εντός εφαρμογής, για ξεκλείδωμα premium λειτουργιών ή ακόμη και για ανταλλαγή με άλλα κρυπτονομίσματα (AppCoins, 2017).

Παράλληλα, οι διαφημίσεις και οι συναλλαγές εντός των εφαρμογών χρησιμοποιούνται για τη δημιουργία της φήμης του προγραμματιστή, παρέχοντας ένα αυτοματοποιημένο σύστημα διακυβέρνησης στην έγκριση εφαρμογών με βάση την κατάταξη του προγραμματιστή (AppCoins, 2017). Η φήμη ενός προγραμματιστή έχει δύο στοιχεία: την κατάταξη και το επίπεδο κατάταξης. Η κατάταξη μπορεί να έχει τις τιμές "Άγνωστο", "Αξιόπιστο" ή "Κρίσιμο" και δηλώνει εάν ένας προγραμματιστής είναι νέος στην

κοινότητα, εάν είναι ήδη γνωστός και θεωρείται έντιμος ή εάν θεωρείται ανέντιμος, αντίστοιχα (Trezentos & Pires, 2017). Η κατάταξη μπορεί να αλλάξει είτε αυτόματα, ανάλογα με το ποσό των αγορών εντός εφαρμογής και των διαφημιστικών συναλλαγών που είναι αποθηκευμένες στο blockchain, είτε μέσω του μηχανισμού της διαμάχης. Στην πρώτη περίπτωση το επίπεδο κατάταξης ορίζεται από την αλληλεπίδραση ή τον όγκο των συναλλαγών των εφαρμογών και όχι από τις λήψεις. Η δημοτικότητα των εφαρμογών θα επηρεάσει το επίπεδο κατάταξης ενός προγραμματιστή, καθώς τα κορυφαία παιχνίδια και οι εφαρμογές θα έχουν από προεπιλογή περισσότερες συναλλαγές, και, ως εκ τούτου, θα απολαμβάνουν υψηλότερη αξιόπιστη κατάταξη (AppCoins, 2017).

Στην δεύτερη περίπτωση, η διαμάχη είναι ένας μηχανισμός τιμωρίας των προγραμματιστών που παραδίδουν κακές εφαρμογές, είτε επειδή περιέχουν κακόβουλο λογισμικό είτε επειδή είναι ψεύτικες, δηλαδή δεν κάνουν τίποτα και μπορεί να περιέχουν μόνο διαφημίσεις (Trezentos & Pires, 2017). Μέσω του πρωτοκόλλου οποιοσδήποτε χρήστης μπορεί να ανοίξει μια διαμάχη εναντίον ενός προγραμματιστή, δηλαδή να ισχυριστεί ότι ένας προγραμματιστής είναι ανέντιμος, και οποιοσδήποτε χρήστης μπορεί να συμμετάσχει σε οποιαδήποτε πλευρά της διαφωνίας, είτε υπέρ είτε κατά του προγραμματιστή. Η κατάταξη του προγραμματιστή αλλάζει ανάλογα με το αποτέλεσμα της διαμάχης. Με αυτό τον τρόπο η κοινότητα αποφασίζει εάν ένας προγραμματιστής και οι αντίστοιχες εφαρμογές του είναι αξιόπιστες ή όχι, και οι λόγοι που οδήγησαν στην απόφαση αυτή είναι δημόσιοι σε όλους (Trezentos & Pires, 2017). Σε αυτή τη φήμη βασίζεται το σύστημα συστάσεων για να προτείνει σχετικές εφαρμογές στους χρήστες, λαμβάνοντας υπόψη παράγοντες όπως οι αξιολογήσεις χρηστών και οι κριτικές.

Συνολικά, το πρωτόκολλο AppCoins δίνει την δυνατότητα να ενσωματωθούν οι αγορές εφαρμογών, οι χρήστες και οι προγραμματιστές σε ένα ενιαίο οικοσύστημα. Στο AppCoins, τα διαφορετικά app stores λειτουργούν ως oracles των έξυπνων συμβολαίων, με τα οποία σχετίζονται καθεμία από τις βασικές συναλλαγές της πλατφόρμας, δημιουργώντας διαφάνεια και ένα επίπεδο εμπιστοσύνης για την οικονομία, καθιστώντας πολλούς μεσάζοντες ξεπερασμένους (AppCoins, 2017).

5.Μελέτη περίπτωσης διαχείρισης έξυπνου συμβολαίου

Σε αυτό το κεφάλαιο παρουσιάζεται μια μελέτη περίπτωσης σχετικά με τη διαχείριση έξυπνων συμβολαίων, με επίκεντρο την υλοποίηση μιας απλής, αλλά πλήρως λειτουργικής, αποκεντρωμένης εφαρμογής ηλεκτρονικού εμπορίου (Dapp) που βασίζεται στο blockchain Ethereum. Η μελέτη περίπτωσης περιλαμβάνει την ανάπτυξη ενός έξυπνου συμβολαίου γραμμένο σε Solidity, τη γλώσσα προγραμματισμού που χρησιμοποιείται για τη δημιουργία έξυπνων συμβολαίων στο blockchain Ethereum. Το έξυπνο συμβόλαιο χρησιμεύει ως η ραχοκοκαλιά της εφαρμογής ηλεκτρονικού εμπορίου, επιτρέποντας την διαχείριση των προϊόντων. Παρουσιάζει διάφορες λειτουργίες προσαρμοσμένες σε ένα σενάριο ηλεκτρονικού εμπορίου, δίνοντας τη δυνατότητα στους χρήστες να δημιουργούν νέα προϊόντα παρέχοντας ονόματα και τιμές, να επαληθεύουν τη διαθεσιμότητα των προϊόντων και να πραγματοποιούν ασφαλείς συναλλαγές αγοράς με χρήματα που μεταφέρονται στον πωλητή μετά την επιτυχή ολοκλήρωση. Ακόμα, το έξυπνο συμβόλαιο εκπέμπει βασικά συμβάντα, ειδοποιώντας τις εξωτερικές εφαρμογές για κρίσιμες ενέργειες εντός του συμβολαίου και επιτρέποντας δυναμικές απαντήσεις σε αλλαγές κατάστασης στο blockchain. Επιπλέον, το έξυπνο συμβόλαιο ελέγχεται διεξοδικά χρησιμοποιώντας το Slither, ένα εργαλείο στατικής ανάλυσης για έξυπνες συμβάσεις, ώστε να διασφαλιστεί η ευρωστία του και να εντοπιστούν πιθανές ευπάθειες ασφαλείας. Αυτή η ολοκληρωμένη διαδικασία δοκιμών συμβάλλει στην αξιοπιστία της σύμβασης και διασφαλίζει τη συμμόρφωση με τις βέλτιστες πρακτικές στην ανάπτυξη έξυπνων συμβολαίων.

Επιπρόσθετα, η μελέτη περίπτωσης διερευνά την ενσωμάτωση του έξυπνου συμβολαίου με το Front-end της εφαρμογής μέσω της βιβλιοθήκης web3.js, επιτρέποντας στο Dapp να αλληλεπιδρά με το συμβόλαιο, να καλεί τις λειτουργίες του και να ανακτά δεδομένα από το blockchain, όπως τη λίστα των προϊόντων και τις λεπτομέρειες τους. Αυτό δείχνει πώς χρησιμοποιούνται τα έξυπνα συμβόλαια σε εφαρμογές πραγματικού κόσμου και πώς μπορούν να ενσωματωθούν απρόσκοπτα με διεπαφές χρήστη. Επιπλέον, η φιλική προς τον χρήστη διεπαφή ενθαρρύνει την ενεργό αφοσίωση των χρηστών, επιτρέποντας στους χρήστες να αλληλεπιδρούν με το έξυπνο συμβόλαιο απευθείας από τα προγράμματα περιήγησής τους μέσω του MetaMask. Οι χρήστες μπορούν να δημιουργήσουν προϊόντα, να αγοράσουν αντικείμενα και να προβάλλουν τη λίστα των προϊόντων, δείχνοντας πως

μπορούν να χρησιμοποιηθούν τα έξυπνα συμβόλαια για τη συμμετοχή των χρηστών σε αποκεντρωμένες εφαρμογές. Τέλος, η μελέτη περίπτωσης πραγματεύεται τις πρακτικές πτυχές της ανάπτυξης και διαμόρφωσης έξυπνων συμβολαίων στο δίκτυο Ethereum, παρέχοντας πληροφορίες για τα θεμελιώδη στοιχεία της αποτελεσματικής διαχείρισης έξυπνων συμβολαίων. Αυτό περιλαμβάνει τη χρήση διευθύνσεων συμβολαίων και δυαδικών διεπαφών εφαρμογών (ABI) ως απαραίτητα στοιχεία για την ανάπτυξη και την ενημέρωση των συμβάσεων. Ο σκοπός της παρούσας μελέτης περίπτωσης είναι να παρέχει μια ολοκληρωμένη προσέγγιση και να προσφέρει γνώσεις για τον πολύπλευρο τομέα της διαχείρισης έξυπνων συμβολαίων, αποκαλύπτοντας τις δυνατότητες μετασχηματισμού των έξυπνων συμβολαίων σε εφαρμογές ηλεκτρονικού εμπορίου και όχι μόνο.

Η δομή του κεφαλαίου έχει ως εξής. Αρχικά, παρουσιάζονται οι τεχνολογίες και τα εργαλεία που εμπλέκονται στην υλοποίηση της εφαρμογής. Στην συνέχεια, παρέχεται ο κώδικας του έξυπνου συμβολαίου και αναλύονται τα διάφορα στοιχεία του. Έπειτα, πραγματοποιείται ο έλεγχος ασφαλείας του έξυπνου συμβολαίου, με τη χρήση του εργαλείου Slither. Στη συνέχεια, περιγράφεται η διαδικασία ανάπτυξης του συμβολαίου στο δίκτυο blockchain. Τέλος, εξετάζεται το Front-end της εφαρμογής και παρουσιάζονται παραδείγματα που επιδεικνύουν τη λειτουργία του.

5.1. Τεχνολογίες και εργαλεία που εμπλέκονται στην υλοποίηση της εφαρμογής

Σε αυτή την ενότητα παρουσιάζονται οι τεχνολογίες και τα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση της αποκεντρωμένης εφαρμογής. Πολλά από τα παρακάτω εργαλεία αποτελούν κορυφαίες και πρωτοπόρες λύσεις στον τομέα των αποκεντρωμένων εφαρμογών, ενώ διαδραματίζουν κρίσιμο ρόλο στις τρέχουσες εξελίξεις.

Solidity. Είναι μια γλώσσα προγραμματισμού υψηλού επιπέδου ειδικά σχεδιασμένη για τη σύνταξη έξυπνων συμβολαίων σε πλατφόρμες blockchain, με το Ethereum να αποτελεί την πιο σημαντική εφαρμογή της. Αντλώντας έμπνευση από την Python, την JavaScript και τη C++, η Solidity καθιστά τον κώδικα οικείο σε προγραμματιστές από διάφορα υπόβαθρα προγραμματισμού. Η γλώσσα πληκτρολογείται στατικά,

υποστηρίζοντας την κληρονομικότητα και τον πολυμορφισμό, καθώς και βιβλιοθήκες και πολύπλοκους τύπους που καθορίζονται από το χρήστη (Ethereum Foundation, 2023). Τα έξυπνα συμβόλαια που γράφονται σε Solidity είναι δομημένα παρόμοια με τις κλάσεις στον αντικειμενοστραφή προγραμματισμό. Ο κώδικας των συμβολαίων αποτελείται από μεταβλητές και συναρτήσεις που διαβάζουν και τροποποιούν αυτές, όπως στον παραδοσιακό εντολοδοτικό προγραμματισμό (Wohrer & Zdun, 2018). Η δομή του αρχείου προέλευσης, η δομή της σύμβασης καθώς και όλες οι δυνατότητες της Solidity, όπως οι global variables, οι modifiers, και τα events, δεν θα αναλυθούν εδώ, καθώς η λεπτομερής ανάλυση τους βρίσκεται στο *"Solidity Documentation Release 0.8.21."* (Ethereum Foundation, 2023). Όσες δυνατότητες της γλώσσας χρησιμοποιήθηκαν για την δημιουργία του έξυπνου συμβολαίου της εφαρμογής θα αναφερθούν στην αντίστοιχη ενότητα.

Η Solidity εξελίσσεται συνεχώς με την πάροδο του χρόνου, και οι νεότερες εκδόσεις pragma συνήθως ενσωματώνουν βέλτιστες πρακτικές και βιομηχανικά πρότυπα. Κατά την περίοδο συγγραφής της εργασίας, η Solidity είχε φτάσει στην έκδοση 0.8.21. Ωστόσο, για την υλοποίηση του έξυπνου συμβολαίου της εφαρμογής επιλέχθηκε η έκδοση 0.8.0, ώστε να διασφαλιστεί η συμβατότητα με τις απαραίτητες εξαρτήσεις, τις βιβλιοθήκες και την υπάρχουσα βάση κώδικα.

Truffle. Είναι ένα ευρέως χρησιμοποιούμενο πλαίσιο ανάπτυξης που έχει σχεδιαστεί με σκοπό να βελτιστοποιήσει τη δημιουργία, τη δοκιμή και την ανάπτυξη έξυπνων συμβολαίων Ethereum (ConsenSys Software Inc., n.d.) Στον πυρήνα του, το Truffle περιλαμβάνει έναν μεταγλωττιστή Solidity, ο οποίος μεταγλωττίζει αυτόματα τα έξυπνα συμβόλαια, δημιουργώντας τη δυαδική διεπαφή εφαρμογής (ABI) και τον bytecode της σύμβασης, απαραίτητα για τις αλληλεπιδράσεις με το δίκτυο Ethereum. Το Truffle ακολουθεί μια τυποποιημένη δομή έργου, η οποία οργανώνει τον κώδικα της έξυπνης σύμβασης, τις δοκιμές και τις διαμορφώσεις με βολικό τρόπο. Αυτή η δομή διευκολύνει τη συνεργασία μεταξύ προγραμματιστών που εργάζονται στο ίδιο έργο. Επιπλέον, παρέχει ένα ολοκληρωμένο πλαίσιο δοκιμών, που επιτρέπει στους προγραμματιστές να γράφουν και να εκτελούν δοκιμαστικές περιπτώσεις, προσομοιώνοντας συναλλαγές και αλληλεπιδράσεις με το blockchain, προκειμένου να εντοπίζουν τρωτά σημεία πριν από την ανάπτυξη στο δίκτυο Ethereum.

Το Truffle εισάγει την έννοια των migration scripts, τα οποία είναι αρχεία JavaScript που χειρίζονται την ανάπτυξη έξυπνων συμβολαίων στο δίκτυο Ethereum. Τα migration scripts βοηθούν στη διαχείριση της διαδικασίας ανάπτυξης συμβολαίου, επιτρέποντας τον έλεγχο της έκδοσης και την ομαλή αναβάθμιση καθώς εξελίσσεται το Dapp. Επιπλέον, το Truffle διευκολύνει τη διαχείριση δικτύου, επιτρέποντας στους προγραμματιστές να διαμορφώνουν πολλαπλά δίκτυα για το Dapp τους, συμπεριλαμβανομένων του mainnet, των δοκιμαστικών δικτύων ή ιδιωτικών δικτύων Ethereum. Επίσης, ενσωματώνεται απρόσκοπτα με το Ganache, ένα προσωπικό blockchain Ethereum για σκοπούς ανάπτυξης και δοκιμής. Αυτή η ευελιξία επιτρέπει την εύκολη ανάπτυξη και δοκιμή σε διαφορετικά περιβάλλοντα. Επιπλέον, παρέχει εργαλεία για την επαλήθευση και την επικύρωση του κώδικα έξυπνων συμβολαίων στο Etherscan ή σε άλλους εξερευνητές μπλοκ.

Ganache. Είναι μέρος του οικοσυστήματος Truffle Suite. Αποτελεί μια προσωπική πλατφόρμα blockchain προσαρμοσμένη για σκοπούς ανάπτυξης και δοκιμών κατανεμημένων εφαρμογών Ethereum και Filecoin (ConsenSys Software Inc., n.d.). Το Ganache δημιουργεί ένα τοπικό και ιδιωτικό περιβάλλον blockchain Ethereum απευθείας στο μηχάνημα του προγραμματιστή. Αυτό επιτρέπει την ανάπτυξη και δοκιμή των έξυπνων συμβολαίων σε ένα ασφαλές και ντετερμινιστικό περιβάλλον, εξαλείφοντας την ανάγκη αλληλεπίδρασης με το ζωντανό κεντρικό δίκτυο ή τα δοκιμαστικά δίκτυα Ethereum κατά τη φάση της ανάπτυξης (development).

Η πλατφόρμα είναι προ-διαμορφωμένη με δοκιμαστικούς λογαριασμούς, ο καθένας από τους οποίους περιέχει δοκιμαστικό Ether (ETH), διευκολύνοντας την προσομοίωση πραγματικών αλληλεπιδράσεων στο blockchain. Με την άμεση εξόρυξη ενεργοποιημένη, οι συναλλαγές εξορύσσονται γρήγορα, παρέχοντας γρήγορη ανατροφοδότηση στους προγραμματιστές κατά τη διάρκεια της δοκιμής και του εντοπισμού σφαλμάτων. Το Ganache UI προσφέρει μια φιλική προς το χρήστη διεπαφή ιστού, επιτρέποντας στους προγραμματιστές να εξερευνήσουν και να επιθεωρήσουν τα μπλοκ, τις συναλλαγές και τα συμβάντα του blockchain. Αυτή η εικόνα δίνει τη δυνατότητα στους προγραμματιστές να αναλύουν τις αλληλεπιδράσεις τους με το blockchain και να αντιμετωπίζουν αποτελεσματικά προβλήματα.

Επιπλέον, το Ganache ενσωματώνεται απρόσκοπτα με δημοφιλή εργαλεία ανάπτυξης Ethereum όπως το Truffle και το Remix, απλοποιώντας την ανάπτυξη έξυπνων συμβολαίων απευθείας στο περιβάλλον Ganache από αυτά τα εργαλεία. Οι προγραμματιστές έχουν επίσης την ευελιξία να προσαρμόζουν τις συνθήκες δικτύου για να προσομοιώνουν διάφορα σενάρια, ενισχύοντας περαιτέρω τις ολοκληρωμένες δυνατότητες δοκιμών του Ganache.

Web3.js. Είναι μια βιβλιοθήκη JavaScript που χρησιμεύει ως γέφυρα μεταξύ των εφαρμογών ιστού (Front-ends) και του blockchain Ethereum. Επιτρέπει στους προγραμματιστές να αλληλεπιδρούν με το δίκτυο Ethereum, να έχουν πρόσβαση σε έξυπνες συμβάσεις και να εκτελούν διάφορες λειτουργίες που σχετίζονται με το blockchain απευθείας από το πρόγραμμα περιήγησης. Το Web3.js επιτρέπει στις αποκεντρωμένες εφαρμογές (Dapps) να συνδέονται με τους λογαριασμούς Ethereum των χρηστών, να υπογράφουν συναλλαγές με ασφάλεια και να ανακτούν δεδομένα από το blockchain, καθιστώντας το ένα θεμελιώδες εργαλείο για τη δημιουργία εφαρμογών που βασίζονται στο Ethereum.

Στην παρούσα μελέτη περίπτωσης, η βιβλιοθήκη web3.js χρησιμοποιείται για να διευκολύνει την αλληλεπίδραση της διεπαφής (HTML, CSS και JavaScript) με το blockchain του Ethereum και το αναπτυγμένο έξυπνο συμβόλαιο. Συγκεκριμένα, η εφαρμογή χρησιμοποιεί το web3.js για να συνδεθεί στο δίκτυο Ethereum και να αλληλεπιδράσει με τον λογαριασμό MetaMask του χρήστη, επιτρέποντας την κλήση των συναρτήσεων του έξυπνου συμβολαίου και την ακρόαση συγκεκριμένων συμβάντων που εκπέμπονται από το έξυπνο συμβόλαιο. Συνολικά, το web3.js διαδραματίζει κρίσιμο ρόλο σε αυτή την εφαρμογή, επιτρέποντας την απρόσκοπτη επικοινωνία μεταξύ της διεπαφής και του blockchain Ethereum.

MetaMask. Είναι μια δημοφιλής επέκταση προγράμματος περιήγησης που λειτουργεί ως πορτοφόλι κρυπτονομισμάτων και διεπαφή για το blockchain Ethereum. Ως πορτοφόλι κρυπτονομισμάτων, επιτρέπει την δημιουργία λογαριασμών για χρήση στα διάφορα δίκτυα Ethereum και διατηρεί τα ιδιωτικά κλειδιά για τους λογαριασμούς, προκειμένου να είναι εφικτή η εξαγωγή τους ή η εισαγωγή νέων λογαριασμών. Επιπλέον, επιτρέπει την εναλλαγή μεταξύ των διαφόρων δικτύων Ethereum, ώστε οι

λογαριασμοί να αντικατοπτρίζουν το σωστό υπόλοιπο για κάθε δίκτυο, και δίνει τη δυνατότητα εκτέλεσης συναλλαγών μεταξύ λογαριασμών και την μεταφορά Ethers από έναν λογαριασμό σε άλλο (Lee, 2019). Εκτός από πορτοφόλι Ethereum, το MetaMask λειτουργεί και ως πάροχος Web3, εισάγοντας τη βιβλιοθήκη Javascript web3.js στο περιβάλλον του προγράμματος περιήγησης, διευκολύνοντας έτσι την αλληλεπίδραση μεταξύ ιστοσελίδων (Dapps) και του δικτύου Ethereum. Δρα ως γέφυρα μεταξύ του Dapp και των λογαριασμών Ethereum του χρήστη, επιτρέποντας την ασφαλή και απρόσκοπτη αλληλεπίδραση με αποκεντρωμένες εφαρμογές στο blockchain.

Το MetaMask έχει σχεδιαστεί κυρίως για να λειτουργεί με το blockchain Ethereum, αν και μπορεί να υποστηρίζει και άλλα δίκτυα. Επιτρέπει στους χρήστες να κάνουν εναλλαγή μεταξύ διαφορετικών δικτύων Ethereum, όπως το mainnet, τα δοκιμαστικά δίκτυα (Ropsten, Rinkeby, Kovan κ.λπ.) αλλά και προσαρμοσμένα δίκτυα. Αυτή η δυνατότητα επιτρέπει στους προγραμματιστές και τους χρήστες να δοκιμάζουν και να αλληλεπιδρούν με εφαρμογές σε διάφορα δίκτυα χωρίς να χρησιμοποιούν πραγματικό Ether στο κύριο δίκτυο. Η εφαρμογή που παρουσιάζεται σε αυτό το κεφάλαιο ζητά από το MetaMask να συνδεθεί σε ένα τοπικό δίκτυο blockchain που εκτίθεται από το Ganache.

5.2. Δημιουργία του έξυπνου συμβολαίου

Αρχικά, η μελέτη περίπτωσης περιλαμβάνει την ανάπτυξη ενός έξυπνου συμβολαίου, γραμμένο σε Solidity, χρησιμοποιώντας το πλαίσιο Truffle. Το έξυπνο συμβόλαιο, που ονομάζεται "Ecommerce", χρησιμεύει ως η ραχοκοκαλιά της εφαρμογής ηλεκτρονικού εμπορίου, χειρίζεται τη δημιουργία και την αγορά προϊόντων, τη διαχείριση των λεπτομερειών του προϊόντος και την παρακολούθηση της ιδιοκτησίας και της διαθεσιμότητας. Παρακάτω παρέχετε μια εικόνα του κώδικα της σύμβασης και αναλύονται τα διάφορα στοιχεία της.

```solidity
// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.0;

contract Ecommerce {
    struct Product {
        uint id;
        string name;
        uint price;
        address payable seller;
        address buyer;
        bool isAvailable;
    }

    uint productCount;
    Product[] public products;

    event ProductCreated(uint _id, string _name, address seller);
    event ProductPurchased(uint _id, address buyer);

    function createProduct(string memory _name, uint _price) public {
        require(_price > 0, "Price should be greater than zero");
        productCount++;
        Product memory newProduct = Product(productCount, _name, _price, payable(msg.sender), address(0), true);
        products.push(newProduct);
        emit ProductCreated(newProduct.id, _name, msg.sender);
    }

    function purchaseProduct(uint _id) public payable {
        require(_id > 0 && _id <= productCount, "Invalid product id");
        Product storage product = products[_id - 1];
        require(product.isAvailable == true, "Product not available");
        require(product.seller != msg.sender, "Seller can not be the buyer");
        product.buyer = msg.sender;
        product.isAvailable = false;
        emit ProductPurchased(_id, msg.sender);
        // Transfer funds to the seller
        product.seller.transfer(msg.value);
    }
}
```

Εικόνα 5.1. Κώδικας Solidity του έξυπνου συμβολαίου "Ecommerce"

Όπως φαίνεται στην εικόνα, το έξυπνο συμβόλαιο συμπεριλαμβάνει τα εξής:

Struct. Το έξυπνο συμβόλαιο ορίζει μια δομή με το όνομα "Product" για να αντιπροσωπεύει ένα προϊόν με το μοναδικό αναγνωριστικό, το όνομα, την τιμή, τη διεύθυνση του πωλητή, τη διεύθυνση του αγοραστή και την κατάσταση διαθεσιμότητας.

State Variables. Το έξυπνο συμβόλαιο περιλαμβάνει δύο μεταβλητές κατάστασης, την "productCount" η οποία παρακολουθεί τον συνολικό αριθμό προϊόντων στην αγορά, και την "products", ως πίνακα για την αποθήκευση όλων των προϊόντων που δημιουργήθηκαν.

Events. Το έξυπνο συμβόλαιο ορίζει δύο συμβάντα, το "ProductCreated" και το "ProductPurchased", που εκπέμπονται κατά τη δημιουργία ή την αγορά ενός προϊόντος, αντίστοιχα. Αυτά τα συμβάντα αποτελούν μια κρίσιμη πτυχή της διαχείρισης έξυπνων συμβολαίων, καθώς επιτρέπουν στις εξωτερικές εφαρμογές να ανταποκρίνονται στις αλλαγές κατάστασης του blockchain.

Functions. Το έξυπνο συμβόλαιο επιδεικνύει διάφορες λειτουργίες που σχετίζονται με τη διαχείριση προϊόντων σε ένα σενάριο ηλεκτρονικού εμπορίου. Συγκεκριμένα, περιλαμβάνει τις εξής συναρτήσεις:

- **"createProduct"**: Αυτή η συνάρτηση επιτρέπει στον χρήστη να δημιουργήσει ένα νέο προϊόν παρέχοντας το όνομα και την τιμή ως παραμέτρους. Επαληθεύει ότι η δοθείσα τιμή είναι μεγαλύτερη του μηδενός και προσθέτει το προϊόν στον πίνακα "products". Επιπλέον, εκπέμπει το συμβάν "ProductCreated".

- **"purchaseProduct"**: Αυτή η συνάρτηση επιτρέπει σε έναν χρήστη να αγοράσει ένα προϊόν καθορίζοντας το αναγνωριστικό του προϊόντος. Εκτελεί ορισμένες επικυρώσεις για το αναγνωριστικό του προϊόντος και τη διαθεσιμότητά του, διασφαλίζει ότι ο αγοραστής δεν είναι ο πωλητής και τέλος μεταφέρει τα χρήματα στον πωλητή. Ενημερώνει τις πληροφορίες αγοραστή και διαθεσιμότητας του προϊόντος και εκπέμπει το συμβάν "ProductPurchased".

Σε αυτό το σημείο πρέπει να αναφερθεί πως ο στόχος της παρούσας διπλωματικής εργασίας είναι να παρέχει ένα proof of concept. Το παραπάνω έξυπνο συμβόλαιο είναι ένα βασικό παράδειγμα, που παρουσιάζει τις πολύ βασικές λειτουργίες του ηλεκτρονικού εμπορίου, όπως η δημιουργία και η αγορά προϊόντων. Δεν αποσκοπεί στο να εξετάσει λεπτομερώς ή να παρουσιάσει περαιτέρω πλούσιες δυνατότητες που μπορεί να περιλαμβάνει μια πλατφόρμα ηλεκτρονικού εμπορίου.

5.3. Έλεγχος του έξυπνου συμβολαίου με το εργαλείο Slither

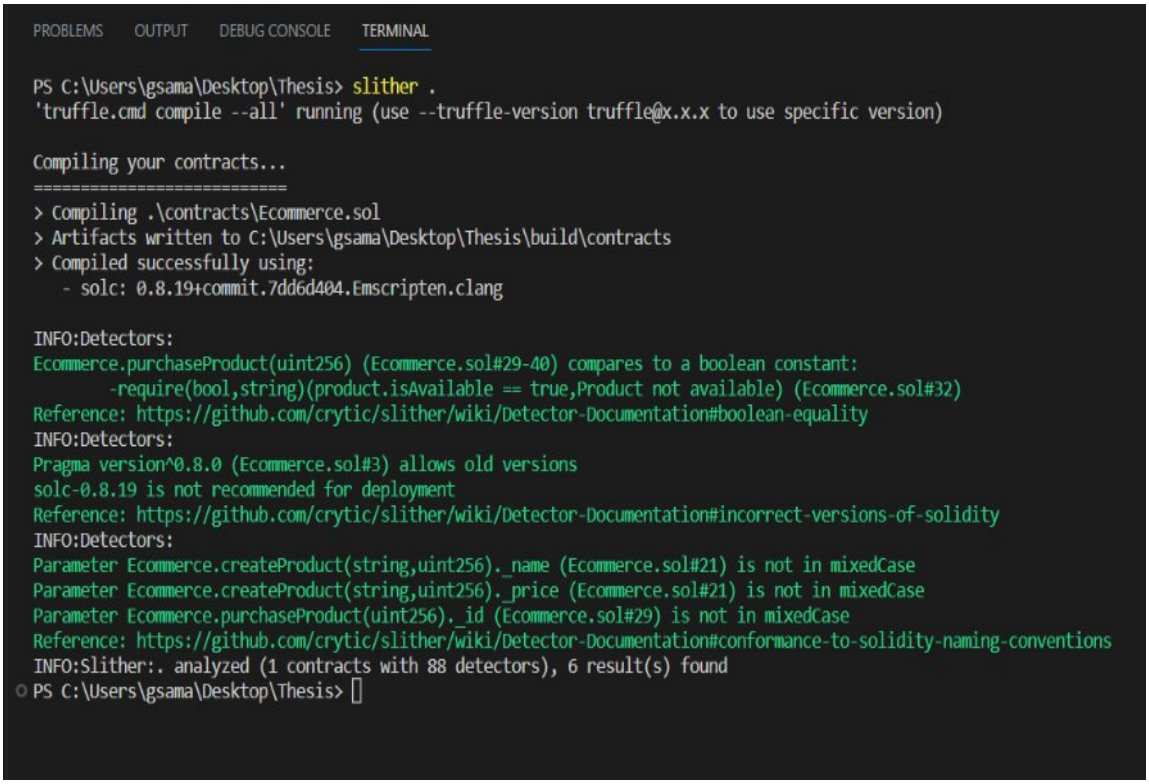
Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, ο αμετάβλητος χαρακτήρας των δεδομένων στο blockchain καθιστά ιδιαίτερα σημαντικό τον διεξοδικό έλεγχο των έξυπνων συμβολαίων πριν την ανάπτυξη του bytecode τους στο blockchain. Για την εκτέλεση ανάλυσης ασφάλειας έχουν δημιουργηθεί πολλά αυτοματοποιημένα εργαλεία, τα οποία έχουν αναλυθεί λεπτομερώς στο Κεφάλαιο 3, στην υποενότητα 3.3.1. Στην ενότητα αυτή, θα πραγματοποιηθεί ο έλεγχος ασφαλείας του έξυπνου συμβολαίου "Ecommerce". Η επιλογή του κατάλληλου εργαλείου εξαρτάται από τις απαιτήσεις του προγραμματιστή και τον τύπο των τρωτών σημείων που επιθυμεί να εντοπίσει. Συνιστάται πάντα ο έλεγχος της τεκμηρίωσης και της υποστήριξης της κοινότητας για κάθε εργαλείο, προκειμένου να βεβαιωθεί ότι ευθυγραμμίζεται με τις ανάγκες του προγραμματιστή.

Σε αυτή την μελέτη περίπτωσης το εργαλείο ανάλυσης ασφαλείας που επιλέχθηκε για τη δοκιμή του έξυπνου συμβολαίου είναι το Slither. Η επιλογή αυτή έγινε, αφενός, λόγω της απλότητας και ευκολίας του εργαλείου στην εγκατάσταση και στην χρήση, και αφετέρου, λόγω των πολλών χαρακτηριστικών που προσφέρει. Αρχικά, το Slither προσφέρει ένα ευρύ φάσμα ελέγχων ανάλυσης για τον εντοπισμό πιθανών τρωτών σημείων και αδυναμιών στα έξυπνα συμβόλαια Ethereum, με χαμηλά ψευδώς θετικά αποτελέσματα. Επίσης, επιτρέπει στους χρήστες να ορίζουν και να προσαρμόζουν τους δικούς τους κανόνες, παρέχοντας ευελιξία. Ένα ακόμα σημαντικό χαρακτηριστικό του Slither είναι ότι μπορεί να ενσωματωθεί σε ροές εργασιών ανάπτυξης, συστήματα συνεχούς ενοποίησης (CI) ή άλλα εργαλεία μέσω της διεπαφής γραμμής εντολών (CLI) ή του API. Αυτή η ενοποίηση διευκολύνει την αυτοματοποίηση της ανάλυσης ασφαλείας, επιτρέποντας αποτελεσματικούς και τακτικούς ελέγχους των έξυπνων συμβολαίων κατά τη διαδικασία ανάπτυξης. Τέλος, το Slither δημιουργεί εκτενείς

αναφορές που παρέχουν λεπτομερείς πληροφορίες σχετικά με τα εντοπισμένα τρωτά σημεία, ακριβείς πληροφορίες τοποθεσίας του σφάλματος στον πηγαίο κώδικα, αξιολογήσεις σοβαρότητας και συστάσεις για αποκατάσταση.

5.3.1. Αποτελέσματα

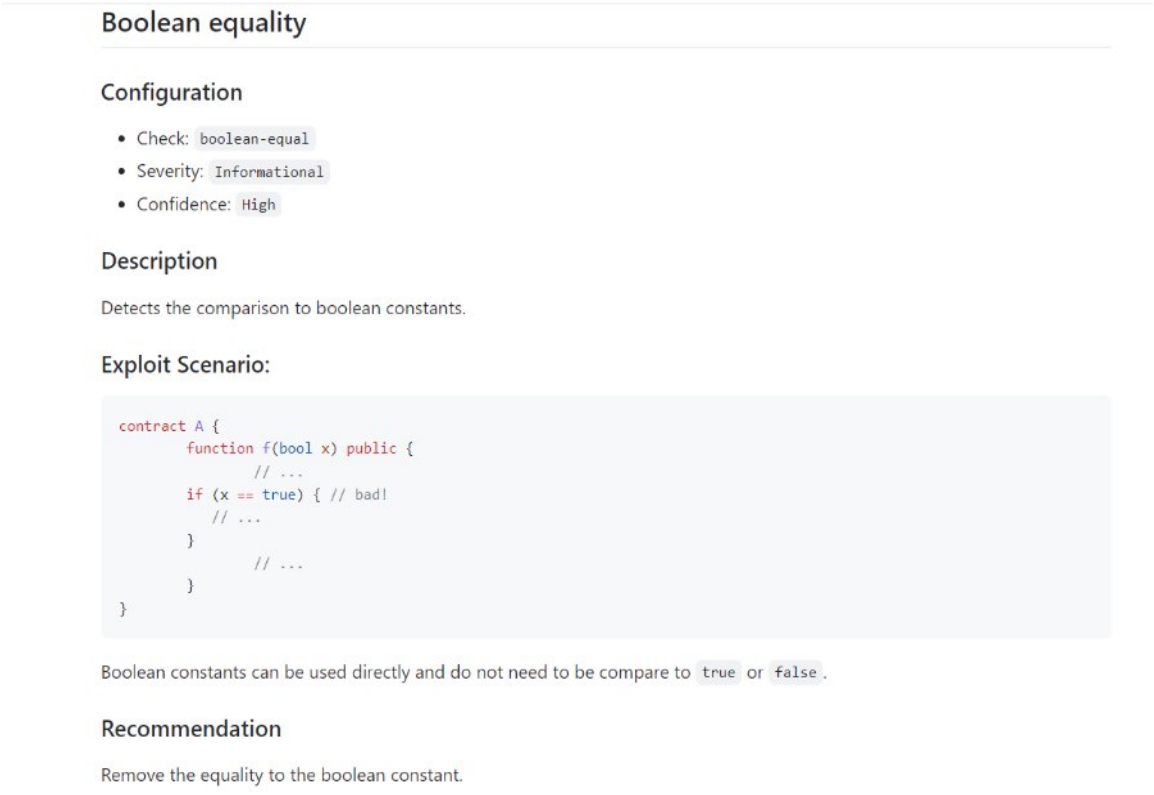
Το Slither χρησιμοποιεί 88 detectors για τον εντοπισμό πιθανών τρωτών σημείων και αδυναμιών στα έξυπνα συμβόλαια, με τον καθένα να έχει ένα επίπεδο impact και ένα επίπεδο confidence. Το πρώτο υποδεικνύει κατά πόσο το πρόβλημα που εντοπίστηκε είναι κρίσιμο ή όχι, και το δεύτερο υποδεικνύει την πιθανότητα το πρόβλημα που εντοπίστηκε να είναι ψευδώς θετικό. Επίσης παρέχεται μια λεπτομερής τεκμηρίωση όλως των detectors, όπου υπάρχουν ακριβείς πληροφορίες για τις διαμορφώσεις που ενεργοποιούν αυτό το σφάλμα στον πηγαίο κώδικα, καθώς και σύσταση για την διόρθωσή του. Παρακάτω παρουσιάζονται και αναλύονται τα αποτελέσματα που παρείχε το Slither για το έξυπνο συμβόλαιο "Ecommerce".



Εικόνα 5.2. Αποτελέσματα εργαλείου Slither για το συμβόλαιο "Ecommerce"

Όπως φαίνεται παραπάνω, στην αναφορά εμφανίζονται πέντε αποτελέσματα, με τα τρία να προέρχονται από τον ίδιο detector. Παρακάτω αναλύονται όλα τα αποτελέσματα με βάση την τεκμηρίωσή τους από το Slither wiki.

Το πρώτο αποτέλεσμα που εντοπίστηκε αφορά τον detector "boolean-equal", που ανιχνεύει την σύγκριση με μία σταθερά boolean, όπου το impact είναι ενημερωτικό (Informational), δηλαδή δεν είναι κρίσιμο για την ασφάλεια του έξυπνου συμβολαίου, και το confidence είναι υψηλό (High), δηλαδή δεν υπάρχει μεγάλη πιθανότητα ψευδώς θετικού αποτελέσματος. Σύμφωνα με την τεκμηρίωση, οι σταθερές Boolean μπορούν να χρησιμοποιηθούν απευθείας και δεν χρειάζεται να συγκρίνονται με αληθείς ή ψευδείς, και η σύσταση για διόρθωση προτείνει την αφαίρεση της ισότητας με τη σταθερά boolean (Crytic, 2018). Όλα τα παραπάνω συνοψίζονται στην Εικόνα 5.3.



Boolean equality

Configuration

- Check: `boolean-equal`
- Severity: `Informational`
- Confidence: `High`

Description

Detects the comparison to boolean constants.

Exploit Scenario:

```
contract A {
        function f(bool x) public {
                // ...
        if (x == true) { // bad!
           // ...
        }
                // ...
        }
}
```

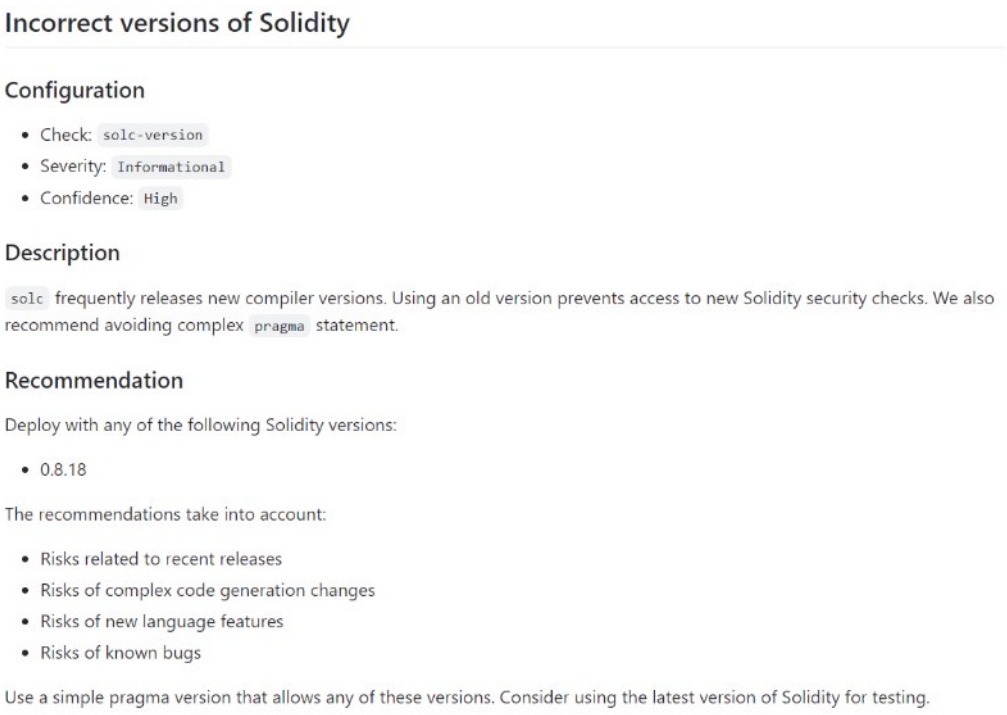
Boolean constants can be used directly and do not need to be compare to `true` or `false`.

Recommendation

Remove the equality to the boolean constant.

Εικόνα 5.3. Τεκμηρίωση σύγκρισης με μία σταθερά boolean (Crytic, 2018)

Το δεύτερο αποτέλεσμα που εντοπίστηκε αφορά τον detector "solc-version", ο οποίος ανιχνεύει λανθασμένη έκδοση Solidity, όπου, ομοίως με το πρώτο αποτέλεσμα, το impact είναι ενημερωτικό (Informational), δηλαδή δεν είναι κρίσιμο για την ασφάλεια του έξυπνου συμβολαίου, και το confidence είναι υψηλό (High), δηλαδή δεν υπάρχει μεγάλη πιθανότητα ψευδώς θετικού αποτελέσματος. Σύμφωνα με την τεκμηρίωση, η solc κυκλοφορεί συχνά νέες εκδόσεις μεταγλωττιστή και η χρήση μιας παλιάς έκδοσης αποτρέπει την πρόσβαση σε νέους ελέγχους ασφαλείας Solidity, ενώ η σύσταση για διόρθωση προτείνει την ανάπτυξη του συμβολαίου με την έκδοση Solidity 0.8.18 (Crytic, 2018). Η σύσταση λαμβάνει υπόψη κινδύνους που σχετίζονται με πρόσφατες εκδόσεις, κινδύνους σύνθετων αλλαγών δημιουργίας κώδικα, κινδύνους νέων γλωσσικών χαρακτηριστικών καθώς και κινδύνους γνωστών σφαλμάτων (Crytic, 2018). Όλα τα παραπάνω συνοψίζονται στην Εικόνα 5.4.



Incorrect versions of Solidity

Configuration

- Check: `solc-version`
- Severity: `Informational`
- Confidence: `High`

Description

`solc` frequently releases new compiler versions. Using an old version prevents access to new Solidity security checks. We also recommend avoiding complex `pragma` statement.

Recommendation

Deploy with any of the following Solidity versions:

- 0.8.18

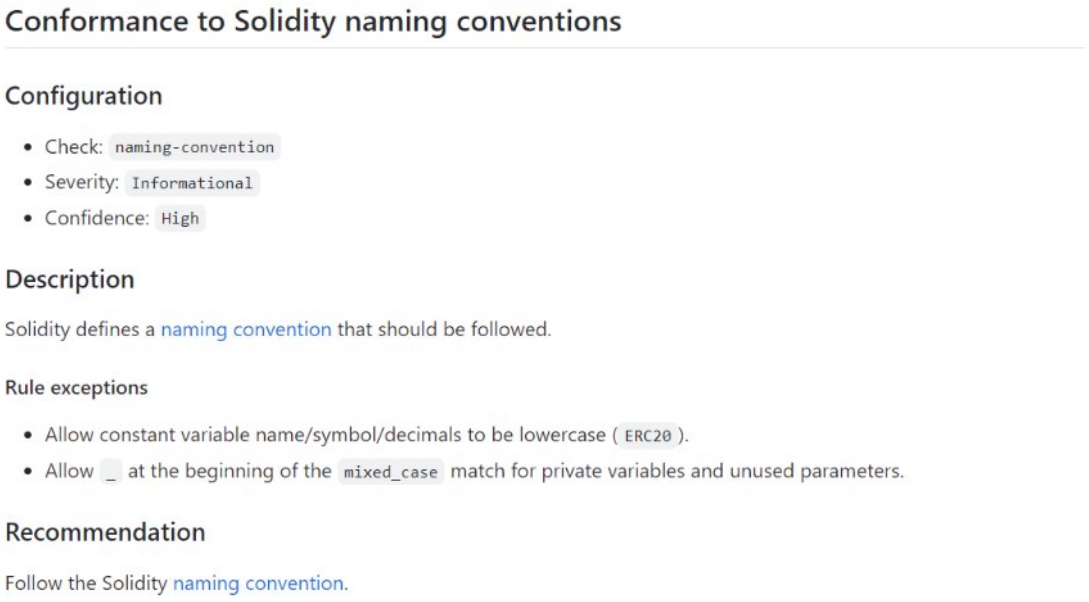
The recommendations take into account:

- Risks related to recent releases
- Risks of complex code generation changes
- Risks of new language features
- Risks of known bugs

Use a simple pragma version that allows any of these versions. Consider using the latest version of Solidity for testing.

Εικόνα 5.4. Τεκμηρίωση λανθασμένης έκδοσης Solidity (Crytic, 2018)

Τέλος, τα τελευταία τρία αποτελέσματα που εντοπίστηκαν αφορούν τον detector "naming-convention", που ανιχνεύει την μη συμμόρφωση με τις συμβάσεις ονομασίας Solidity, όπου, ομοίως με τα προηγούμενα αποτελέσματα, το impact είναι ενημερωτικό (Informational), δηλαδή δεν είναι κρίσιμο για την ασφάλεια του έξυπνου συμβολαίου, και το confidence είναι υψηλό (High), δηλαδή δεν υπάρχει μεγάλη πιθανότητα ψευδώς θετικού αποτελέσματος. Σύμφωνα με την τεκμηρίωση, η Solidity ορίζει μια σύμβαση ονομασίας που πρέπει να ακολουθείται, με εξαιρέσεις στους κανόνες να επιτρέπουν το όνομα/σύμβολο/δεκαδικά της σταθερής μεταβλητής να είναι πεζά (ERC20), και να επιτρέπεται _ στην αρχή της αντιστοίχισης mixed_case για ιδιωτικές μεταβλητές και αχρησιμοποίητες παραμέτρους (Crytic, 2018). Η σύσταση για διόρθωση προτείνει την συμμόρφωση με την σύμβαση ονομασίας της Solidity. Όλα τα παραπάνω συνοψίζονται στην Εικόνα 5.5.



Conformance to Solidity naming conventions

Configuration

- Check: `naming-convention`
- Severity: `Informational`
- Confidence: `High`

Description

Solidity defines a naming convention that should be followed.

Rule exceptions

- Allow constant variable name/symbol/decimals to be lowercase (`ERC20`).
- Allow `_` at the beginning of the `mixed_case` match for private variables and unused parameters.

Recommendation

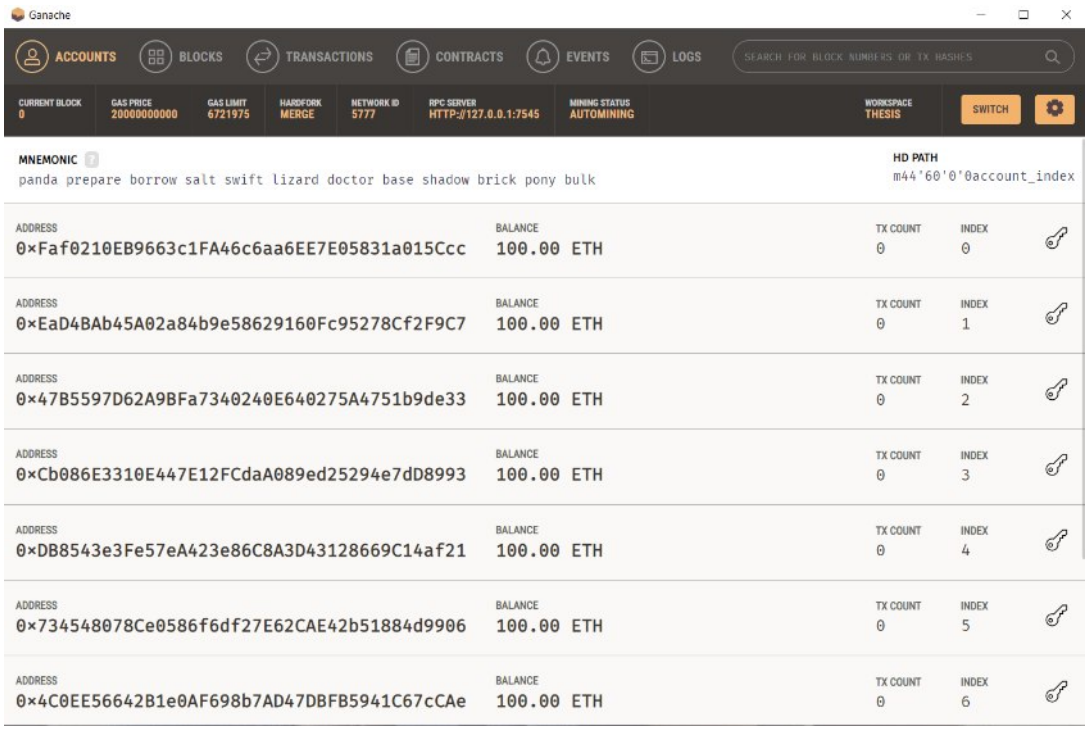
Follow the Solidity naming convention.

Εικόνα 5.5. Τεκμηρίωση συμμόρφωσης με τις συμβάσεις ονομασίας Solidity (Crytic, 2018)

Συμπερασματικά, στο έξυπνο συμβόλαιο "Ecommerce" δεν εντοπίστηκαν κρίσιμα τρωτά σημεία ασφαλείας. Τα ζητήματα που εντοπίστηκαν έχουν ενημερωτικό χαρακτήρα και δεν επηρεάζουν την λειτουργικότητα ή την ασφάλεια του συμβολαίου. Για τον λόγο αυτό αποφασίστηκε να μην πραγματοποιηθούν αλλαγές στον κώδικα της σύμβασης.

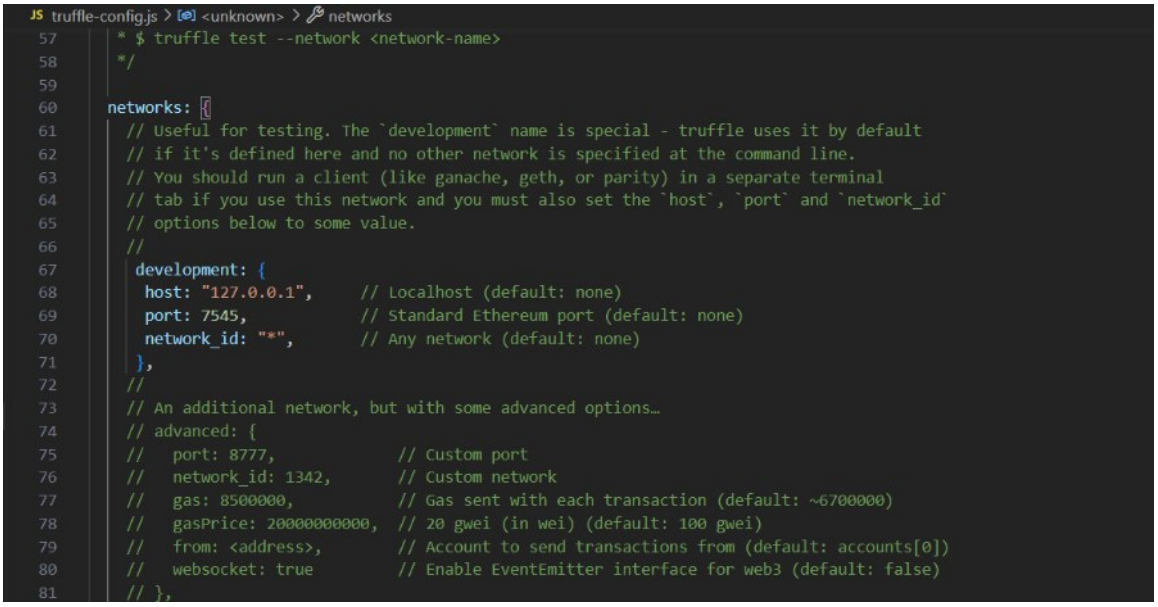
5.4. Ανάπτυξη του έξυπνου συμβολαίου στο δίκτυο blockchain

Μετά την δημιουργία του έξυπνου συμβολαίου και τον έλεγχό του με τα εργαλεία ανάλυσης ασφαλείας σειρά έχει η ανάπτυξή του στο δίκτυο blockchain. Όπως αναφέρθηκε σε προηγούμενη ενότητα, η ανάπτυξη του έξυπνου συμβολαίου θα γίνει σε ένα τοπικό και ιδιωτικό Ethereum blockchain, με την χρήση της πλατφόρμας Ganache. Συνεπώς, απαραίτητη είναι η εκτέλεση της πλατφόρμας Ganache, η οποία θα πρέπει να παραμείνει ανοιχτή καθ' όλη την διάρκεια ανάπτυξης, αλλά και στην συνέχεια, κατά την χρήση της εφαρμογής. Μετά την εκκίνηση της πλατφόρμας, αφού έχει επιλεχθεί το workspace στο οποίο θα εργαστούμε, εμφανίζεται η ενότητα Accounts, που περιέχει μια λίστα προ-δημιουργημένων δοκιμαστικών λογαριασμών μαζί με τις αντίστοιχες διευθύνσεις και τα υπόλοιπά τους. Δίπλα από την ενότητα Accounts υπάρχουν οι υπόλοιπες ενότητες που παρουσιάζουν πληροφορίες σχετικά με τα μπλοκ, τις συναλλαγές, τα συμβάντα, τα έξυπνα συμβόλαια και τα αρχεία καταγραφής. Ακριβώς κάτω από τις ενότητες εμφανίζονται ορισμένες παράμετροι δικτύου, όπως η τιμή του gas, το όριο του gas, το αναγνωριστικό του δικτύου, και άλλες διαμορφώσεις που σχετίζονται με το Ethereum. Όλα αυτά απεικονίζονται παρακάτω στην Εικόνα 5.6.



Εικόνα 5.6. Ganache workspace

Αρχικά, το έξυπνο συμβόλαιο πρέπει να μεταγλωττιστεί. Η μεταγλώττιση του συμβολαίου στο πλαίσιο Truffle γίνεται με την εντολή truffle compile. Μόλις ολοκληρωθεί η διαδικασία της μεταγλώττισης παρατηρούμε ότι μέσα στον φάκελο "build" έχει δημιουργηθεί ένα αρχείο JSON με το ABI και τον bytecode του συμβολαίου, ή όπως αλλιώς ονομάζονται, τα artifacts. Στην συνέχεια, πρέπει να γίνουν οι απαραίτητες αλλαγές στο αρχείο "truffle-config.js" ώστε να αναπτυχθεί το έξυπνο συμβόλαιο στο δίκτυο που δημιουργείται από το Ganache. Συγκεκριμένα, πραγματοποιείται αλλαγή του port με 7545 το οποίο αντιστοιχεί στον RPC SERVER του Ganache. Οι αλλαγές αυτές απεικονίζονται στην Εικόνα 5.7.



Εικόνα 5.7. Διαμόρφωση δικτύου

Τέλος, στον φάκελο migrations θα πρέπει να δημιουργηθεί το αρχείο με το migration script, όπως φαίνεται παρακάτω στην Εικόνα 5.8. Το migration script αρχικά εισάγει τα artifacts του έξυπνου συμβολαίου "Ecommerce.sol" χρησιμοποιώντας τη λειτουργία "artifacts.require" που παρέχεται από το Truffle. Αυτό του επιτρέπει να έχει πρόσβαση στο μεταγλωττισμένο συμβόλαιο και να αλληλεπιδρά μαζί του. Στην συνέχεια βρίσκεται η κύρια λειτουργία του script, η οποία εξάγει μια συνάρτηση που λαμβάνει ως αντικείμενο το "deployer". Το αντικείμενο "deployer" παρέχεται από το Truffle και χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων στο blockchain. Τέλος, η συνάρτηση " deployer.deploy" παίρνει τη σύμβαση "Ecommerce" και την αναπτύσσει με τα καθορισμένα ορίσματα του κατασκευαστή, εάν υπάρχουν. Σε περίπτωση που

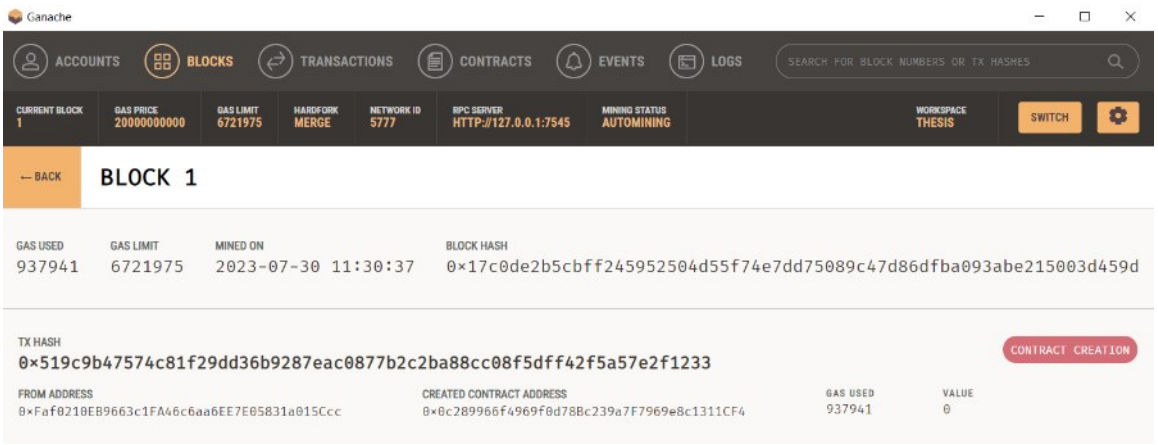
υπάρχουν πολλά έξυπνα συμβόλαια, ο αριθμός στην ονομασία του κάθε αρχείου υποδεικνύει την σειρά με την οποία θα γίνει η ανάπτυξη των συμβολαίων στο δίκτυο blockchain.

migrations > JS 1_ecommerce.js > ...

```
1  var Ecommerce = artifacts.require("./Ecommerce.sol");
2
3  module.exports = function (deployer) {
4    deployer.deploy(Ecommerce);
5  };
```

Εικόνα 5.8. Migration script

Σε αυτό το σημείο το συμβόλαιο είναι έτοιμο να αναπτυχθεί στο δίκτυο blockchain, διαδικασία η οποία, στο πλαίσιο Truffle, γίνεται με την εντολή truffle migrate. Μόλις ολοκληρωθεί η διαδικασία ανάπτυξης, στην ενότητα Blocks της πλατφόρμας Ganache παρατηρούμε ότι έχει δημιουργηθεί το block 1, στο οποίο περιλαμβάνονται όλες οι πληροφορίες εξόρυξης, καθώς και η διεύθυνση του αναπτυγμένου συμβολαίου. Επίσης, παρατηρούμε πως η Ganache χρησιμοποιεί από προεπιλογή τον πρώτο λογαριασμό από την λίστα των δοκιμαστικών λογαριασμών, για την δημιουργία της συναλλαγής. Παρακάτω στην Εικόνα 5.9 απεικονίζεται το block στο οποίο αποθηκεύτηκε το έξυπνο συμβόλαιο, με όλες τις λεπτομέρειες της συναλλαγής.



Εικόνα 5.9. Block στο οποίο αποθηκεύτηκε το έξυπνο συμβόλαιο

5.5. Front-end της Αποκεντρωμένης Εφαρμογής

Τελευταίο βήμα στην υλοποίηση της εφαρμογής, στα πλαίσια της μελέτης περίπτωσης διαχείρισης ενός έξυπνου συμβολαίου, είναι η δημιουργία της διεπαφής, ώστε να μπορούν οι χρήστες να αλληλεπιδρούν με το έξυπνο συμβόλαιο. Το front-end της εφαρμογής "Ecommerce Dapp" αποτελείται από ένα αρχείο HTML, ένα αρχείο CSS και ένα αρχείο JavaScript. Ο πλήρης κώδικας αυτών των αρχείων υπάρχει στο Παράρτημα Α. Παρακάτω αναλύονται τα διάφορα συστατικά μέρη.

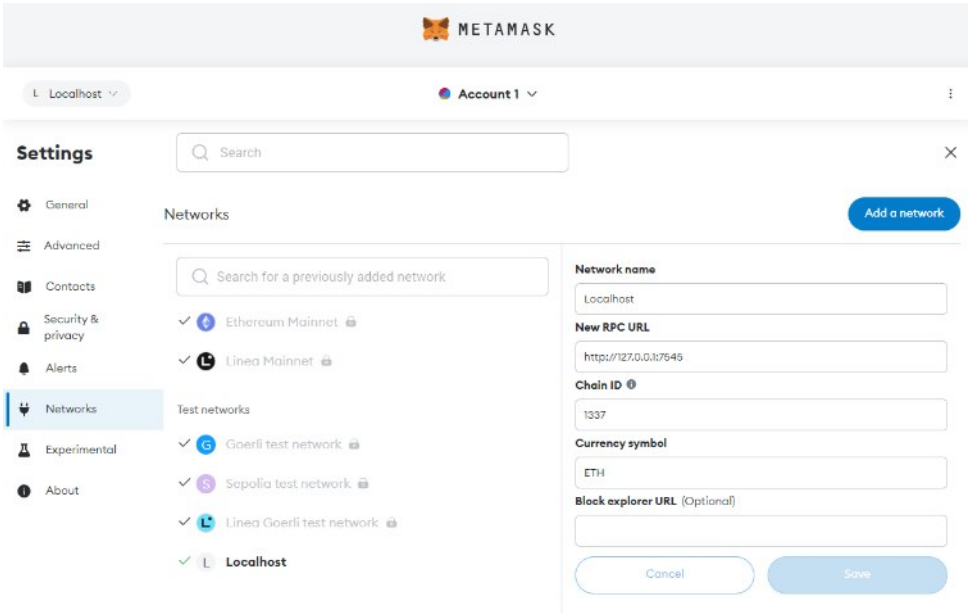
Αρχικά, το αρχείο HTML ορίζει τη δομή του Dapp, περιλαμβάνοντας φόρμες για τη δημιουργία και αγορά προϊόντων, ενότητα για την εμφάνιση της λίστας προϊόντων και απαραίτητα στοιχεία όπως επικεφαλίδες και div. Επιπλέον, συμπεριλαμβάνονται ετικέτες script που φορτώνουν τα αρχεία JavaScript "Web3.js" και "app.js". Το "Web3.js" φορτώνει τη βιβλιοθήκη Web3.js και καθιστά τις λειτουργίες της διαθέσιμες στο "app.js". Το "app.js" αλληλεπιδρά με το blockchain Ethereum. Το αρχείο CSS παρέχει το στυλ για τα στοιχεία HTML, ορίζοντας γραμματοσειρές, στοίχιση, περιγράμματα και άλλες οπτικές πτυχές που δημιουργούν μια φιλική προς το χρήστη διεπαφή.

Το αρχείο JavaScript αποτελεί ουσιαστικό στοιχείο της μελέτης περίπτωσης, καθώς καταδεικνύει την πρακτική ενσωμάτωση του front-end με το blockchain Ethereum, δείχνοντας πώς δημιουργούνται και αλληλεπιδρούν οι αποκεντρωμένες εφαρμογές του πραγματικού κόσμου με τα έξυπνα συμβόλαια. Συγκεκριμένα, εκτελεί μια σειρά κρίσιμων εργασιών, οι οποίες αναλύονται διεξοδικά παρακάτω.

Αρχικά, το αρχείο JavaScript αξιοποιεί τη βιβλιοθήκη web3.js για τη δημιουργία σύνδεσης με το δίκτυο Ethereum. Μέσω αυτής της σύνδεσης, οι χρήστες μπορούν να αλληλεπιδρούν με τους λογαριασμούς τους στο MetaMask, δίνοντας άδεια στην εφαρμογή να πραγματοποιεί συναλλαγές για λογαριασμό τους. Επίσης, δημιουργεί ένα στιγμιότυπο της σύμβασης, καθορίζοντας το ABI και την διεύθυνση του συμβολαίου, για αλληλεπίδραση με το αναπτυγμένο συμβόλαιο. Επιπλέον, σημαντική είναι η χρήση τεχνικών ασύγχρονου προγραμματισμού, οι οποίες αναλαμβάνουν τον χειρισμό των αλληλεπιδράσεων με το blockchain, εξασφαλίζοντας παράλληλα μια ανταποκρινόμενη και φιλική προς τον χρήστη εμπειρία.

Η λειτουργικότητα του front-end του Dapp είναι ενσωματωμένη σε χειριστές συμβάντων και συναρτήσεις, οι οποίες εκτελούνται με βάση τις αλληλεπιδράσεις των χρηστών με τα στοιχεία HTML. Πιο συγκεκριμένα, το αρχείο JavaScript ρυθμίζει χειριστές συμβάντων για τις υποβολές φορμών, όπως η δημιουργία και η αγορά ενός προϊόντος, ανακτά τις εισόδους των χρηστών, αλληλεπιδρά με τις συναρτήσεις του έξυπνου συμβολαίου και ενημερώνει ανάλογα το περιβάλλον χρήστη. Επιπλέον, υλοποιεί μια συνάρτηση για την εμφάνιση της λίστας των προϊόντων. Αντλώντας από το έξυπνο συμβόλαιο πληροφορίες σχετικά με τα προϊόντα μέσω queries, το αρχείο JavaScript διασφαλίζει την συστηματική επανάληψη των προϊόντων και τη δημιουργία δυναμικών στοιχείων HTML προκειμένου να παρουσιάσει τις απαραίτητες πληροφορίες στην ενότητα της λίστας προϊόντων. Ακόμα, ρυθμίζει τους ακροατές των συμβάντων "ProductCreated" και "ProductPurchased", για να ενημερώνεται και να ανανεώνεται αυτόματα η λίστα με κάθε νέα δημιουργία ή αγορά προϊόντος.

Τέλος, επισημαίνεται ότι για την ομαλή λειτουργία της εφαρμογής, απαιτείται η προσθήκη του δικτύου του Ganache στο Metamask, προκειμένου να διασφαλιστεί η σύνδεση στο συγκεκριμένο δίκτυο. Η διαδικασία προσθήκης του δικτύου παρουσιάζεται στην Εικόνα 5.10 και αποτελεί κρίσιμο βήμα για την ασφαλή και απρόσκοπτη επικοινωνία της εφαρμογής με το δίκτυο του Ganache.

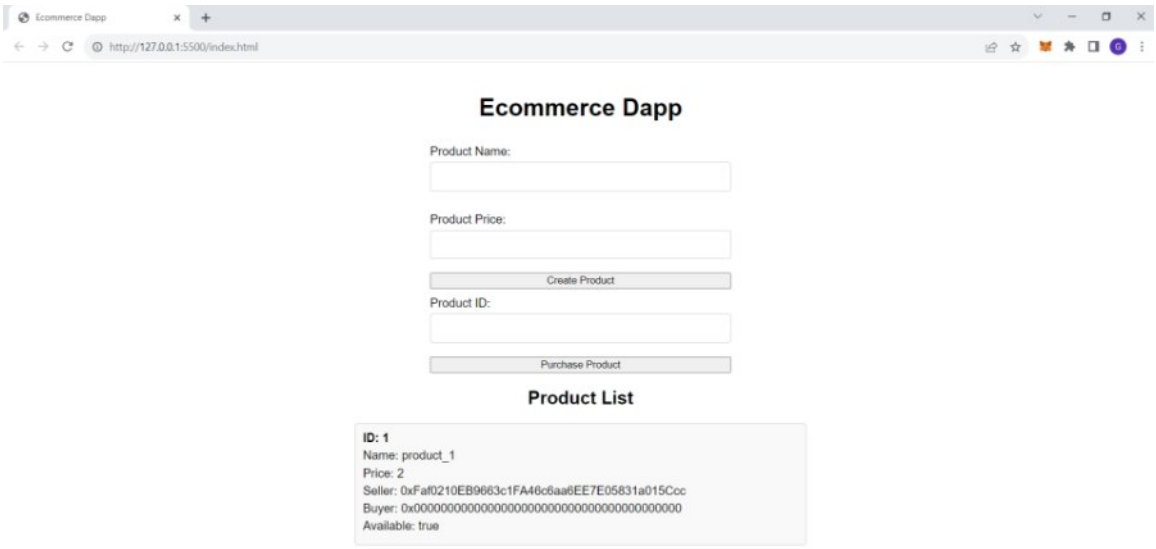


Εικόνα 5.10 Προσθήκη του δικτύου Ganache στο Metamask

5.5.1. Παράδειγμα χρήσης της Εφαρμογής

Η μελέτη περίπτωσης επικεντρώνεται στην υλοποίηση της εφαρμογής και δεν αποσκοπεί στην ανάπτυξη της εμπειρίας του χρήστη. Για τον λόγο αυτό, θεωρούμε ως δεδομένες κάποιες προϋποθέσεις που απαιτούνται για τη χρήση μιας αποκεντρωμένης εφαρμογής, όπως το γεγονός ότι ο χρήστης χρησιμοποιεί ένα πρόγραμμα περιήγησης συμβατό με Web3, με εγκατεστημένο έναν πάροχο Web3, που συνδέεται με το σωστό δίκτυο blockchain. Διάφορα σφάλματα που αφορούν τη σύνδεση με το MetaMask ή την αποτυχία μιας συναλλαγής, καταγράφονται και εμφανίζονται στο console.

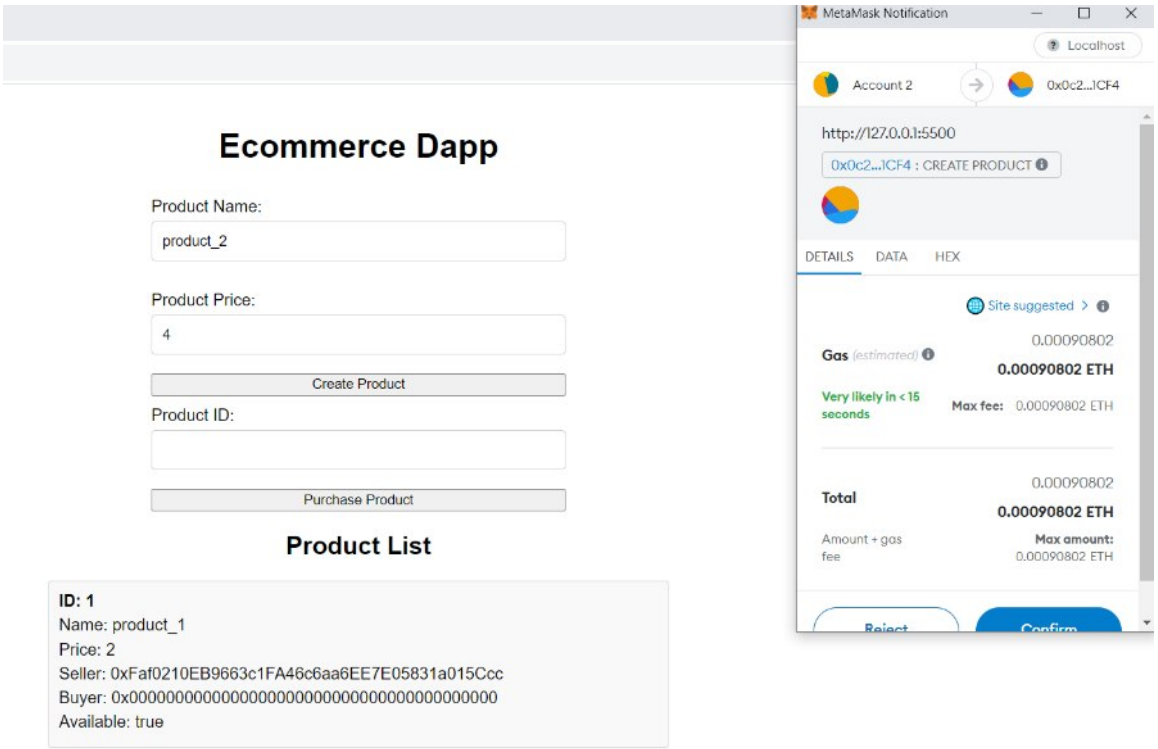
Όσον αφορά τη χρήση της εφαρμογής, κατά τη φόρτωση της ιστοσελίδας, παρατηρούμε τα πλαίσια για τη δημιουργία και την αγορά προϊόντων, ενώ επίσης εμφανίζεται η λίστα με τα προϊόντα που έχουν ήδη δημιουργηθεί. Μέχρι αυτό το σημείο, οποιοσδήποτε επιθυμεί μπορεί να περιηγηθεί στην ιστοσελίδα και να προβάλει τα διαθέσιμα προϊόντα, χωρίς να απαιτείται σύνδεση στο Metamask. Στην Εικόνα 5.11 φαίνεται η αρχική, και μοναδική, σελίδα της εφαρμογής.



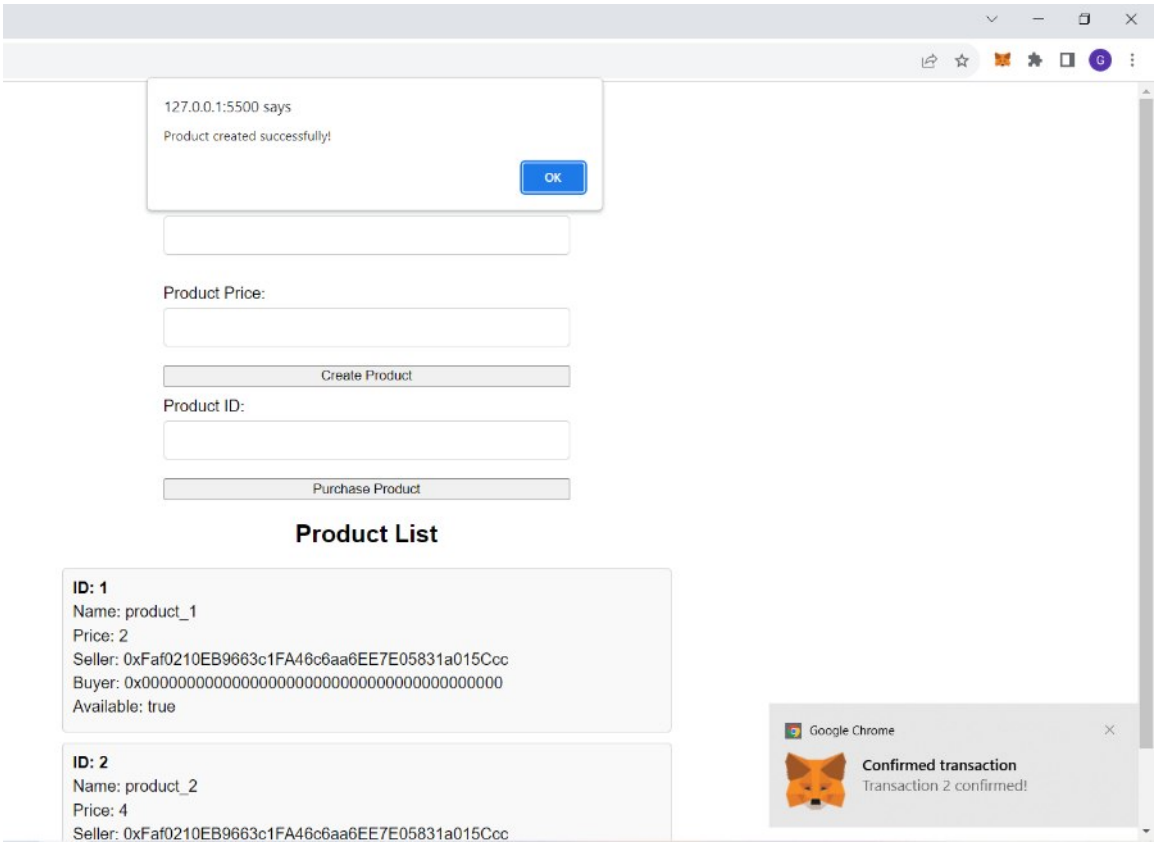
Εικόνα 5.11. Ιστοσελίδα της Εφαρμογής

5.5.1.1. Δημιουργία ενός προϊόντος

Για τη δημιουργία ενός προϊόντος, ο χρήστης καλείται να καταχωρίσει ένα όνομα και μια τιμή. Μετά το πάτημα του κουμπιού "Create Product", η εφαρμογή ζητά πρόσβαση στους λογαριασμούς Ethereum του χρήστη. Παρατηρούμε ότι εμφανίζεται ένα αναδυόμενο παράθυρο από το MetaMask, το οποίο περιέχει τις λεπτομέρειες της συναλλαγής, όπου ο χρήστης μπορεί να επιβεβαιώσει ή να απορρίψει τη συναλλαγή. Ουσιαστικά, ζητεί από τον χρήστη να υπογράψει κρυπτογραφικά τη συναλλαγή με το ιδιωτικό του κλειδί. Εάν ο χρήστης επιβεβαιώσει τη συναλλαγή, εμφανίζεται ένα μήνυμα που υποδεικνύει την επιτυχία ή την αποτυχία της συναλλαγής και αναλόγως ενημερώνεται η λίστα με τα προϊόντα. Η παραπάνω περιγραφή παρουσιάζεται στις επόμενες εικόνες, με την Εικόνα 5.12 να εμφανίζει τη δημιουργία ενός προϊόντος και την Εικόνα 5.13 να εμφανίζει την επιτυχή ολοκλήρωση της συναλλαγής και την ενημέρωση της λίστας προϊόντων.

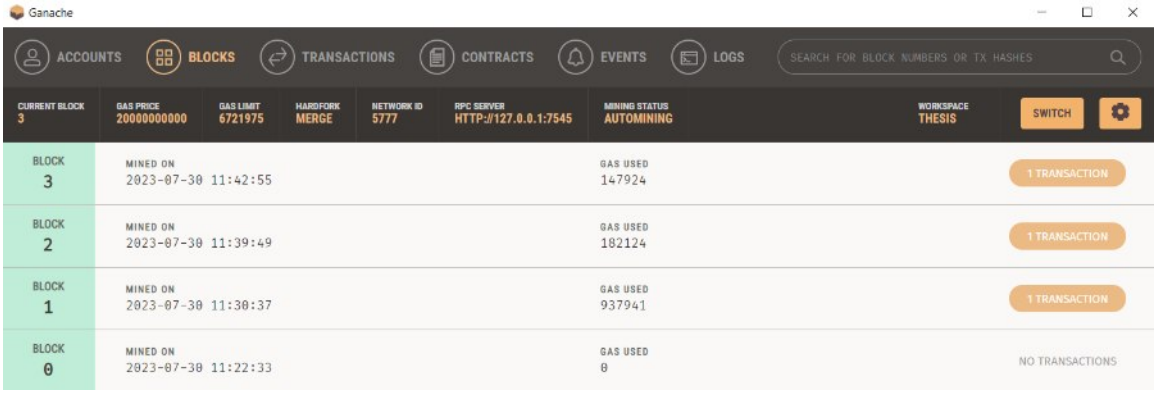


Εικόνα 5.12. Δημιουργία προϊόντος

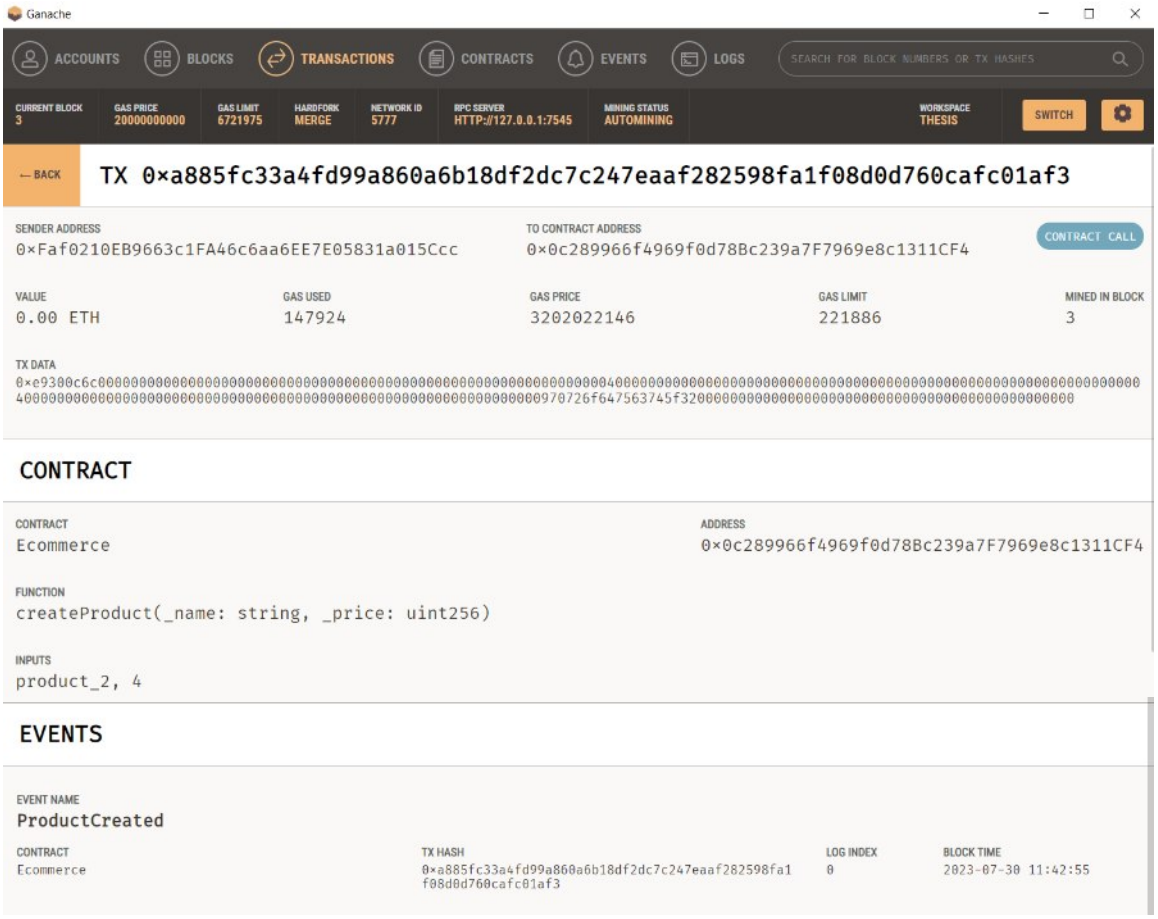


Εικόνα 5.13. Επιτυχής δημιουργία προϊόντος

Στο παραπάνω παράδειγμα, ο χρήστης δημιουργεί ένα προϊόν με όνομα "product_2" και τιμή 4. Όπως φαίνεται στο αναδυόμενο παράθυρο του Metamask, ο χρήστης χρησιμοποιεί το Account 2 για να στείλει μια συναλλαγή στην διεύθυνση του έξυπνου συμβολαίου, καλώντας την συνάρτηση του συμβολαίου "Create Product". Η δημιουργία προϊόντων επηρεάζει την κατάσταση του blockchain, καθώς κάθε νέο προϊόν που δημιουργείται καταγράφεται σε μια συναλλαγή η οποία αποθηκεύεται σε ένα καινούργιο block. Μέσω της πλατφόρμας Ganache, μπορούμε να παρατηρούμε τις αλλαγές στην κατάσταση του blockchain από την ενότητα Blocks. Επιπλέον, μας παρέχεται η δυνατότητα να εξετάζουμε τις συναλλαγές και όλες τις λεπτομέρειές τους στην ενότητα Transactions. Στις παρακάτω εικόνες 5.14 και 5.15 παρουσιάζεται η κατάσταση του blockchain και η συναλλαγή, αντίστοιχα, μετά τη δημιουργία του προϊόντος από το προηγούμενο παράδειγμα.



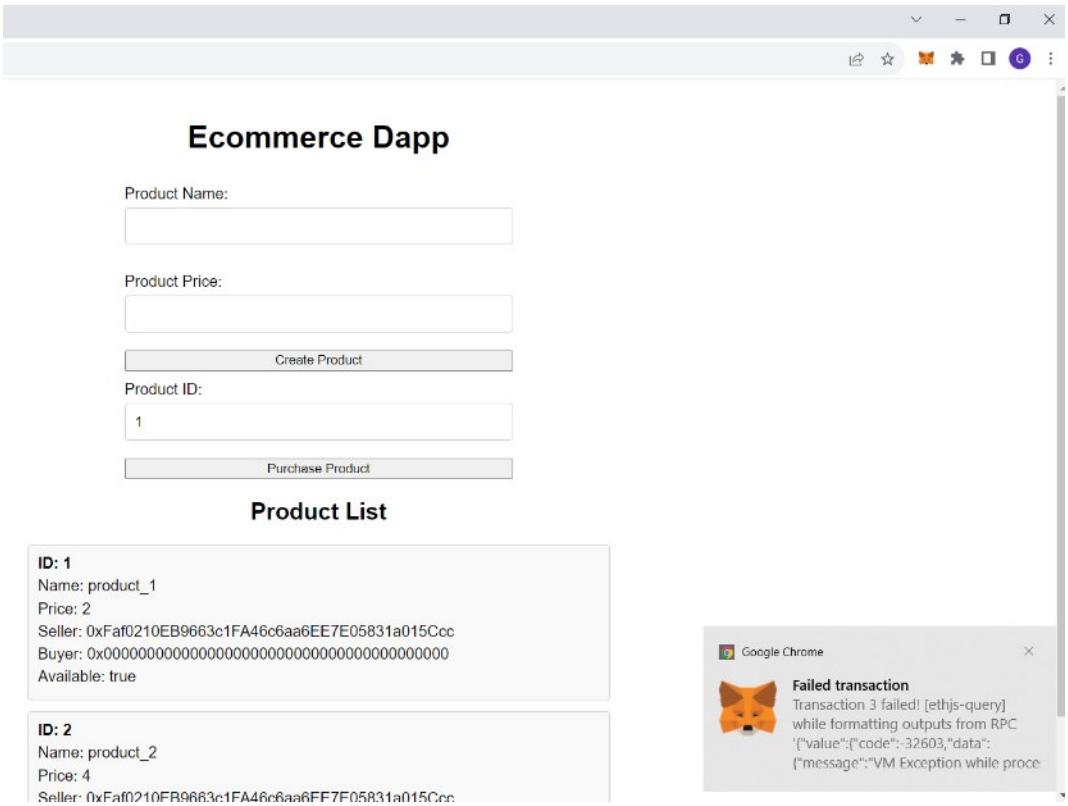
Εικόνα 5.14. Κατάσταση του Blockchain



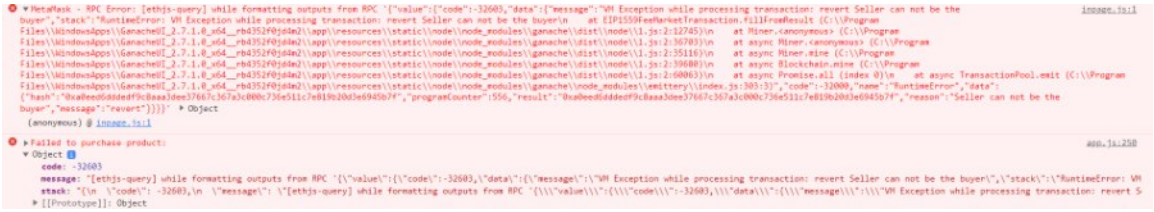
Εικόνα 5.15. Λεπτομέρειες συναλλαγής δημιουργίας προϊόντος

5.5.1.2. Αγορά ενός προϊόντος

Η διαδικασία για την αγορά ενός προϊόντος είναι παρόμοια με αυτή της δημιουργίας. Αρχικά ο χρήστης καλείται να καταχωρίσει το αναγνωριστικό του προϊόντος που επιθυμεί να αγοράσει. Έπειτα, με το πάτημα του κουμπιού "Purchase Product," η εφαρμογή απαιτεί πρόσβαση στους λογαριασμούς Ethereum του χρήστη. Εμφανίζεται ένα αναδυόμενο παράθυρο από το MetaMask, το οποίο περιέχει τις λεπτομέρειες της συναλλαγής, όπου ο χρήστης μπορεί να επιβεβαιώσει ή να απορρίψει τη συναλλαγή. Σημείο προσοχής αποτελεί το γεγονός ότι, όπως αναφέρθηκε και σε προηγούμενη ενότητα, το έξυπνο συμβόλαιο εκτελεί ορισμένες επικυρώσεις σχετικά με το αναγνωριστικό του προϊόντος και τη διαθεσιμότητά του, καθώς επίσης διασφαλίζει ότι ο αγοραστής δεν είναι ίδιος με τον πωλητή. Σε περίπτωση που δεν εκπληρούνται όλες οι επικυρώσεις, η συναλλαγή θα απορριφθεί, και ο σχετικός κωδικός σφάλματος θα εμφανιστεί στο console της εφαρμογής. Η παραπάνω διαδικασία παρουσιάζεται στις επόμενες εικόνες, όπου προβάλλεται αρχικά ένα παράδειγμα μιας αποτυχημένης συναλλαγής, ακολουθούμενο από ένα παράδειγμα μιας επιτυχημένης αγοράς ενός προϊόντος.

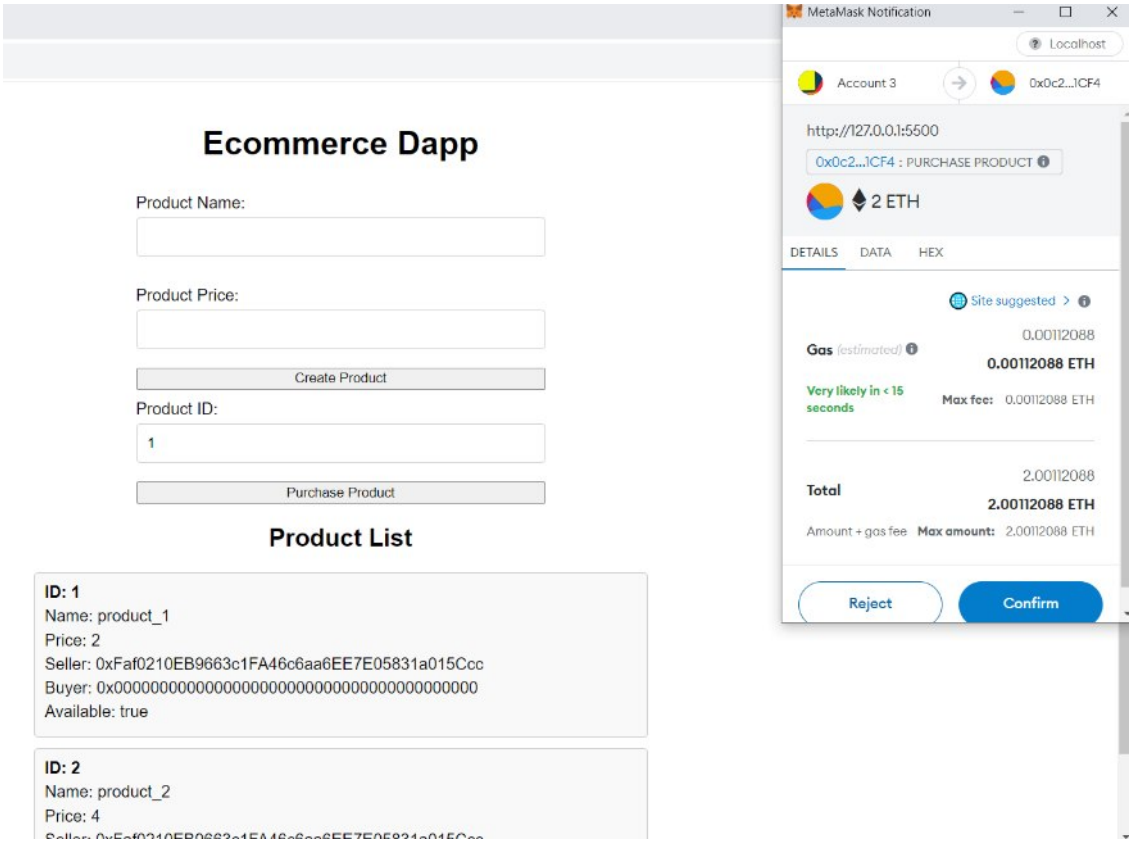


Εικόνα 5.16. Αποτυχία αγοράς ενός προϊόντος

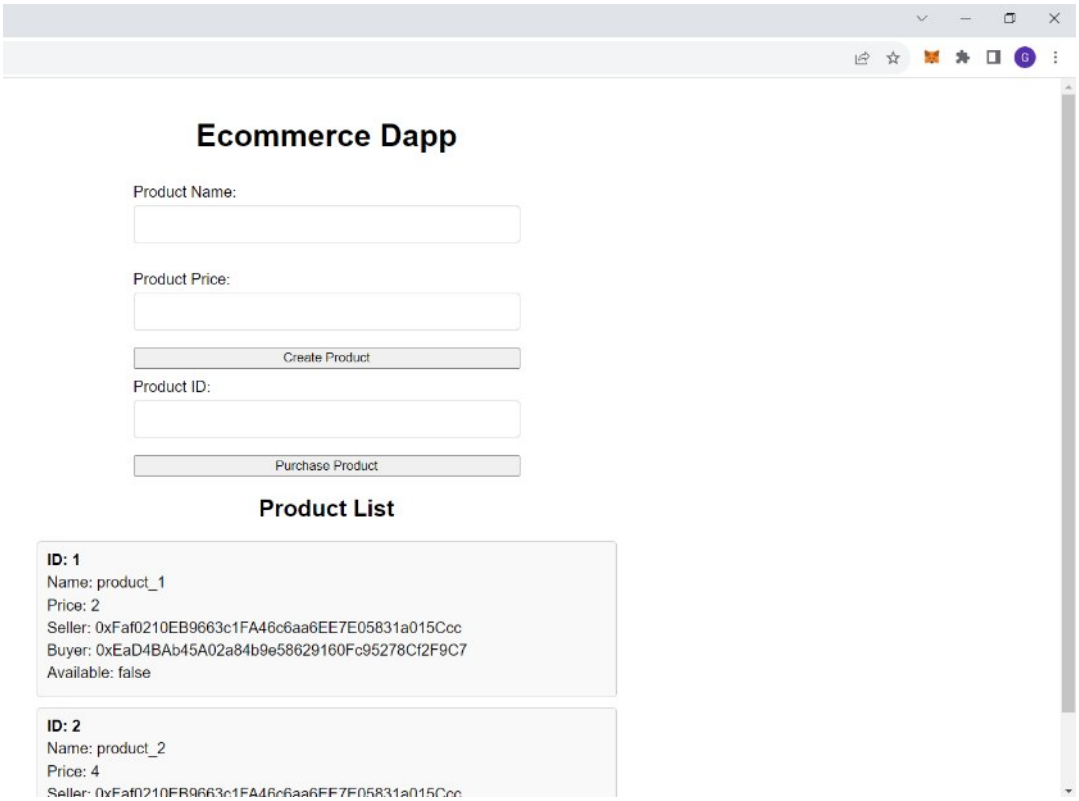


Εικόνα 5.17. Σφάλματα αποτυχίας της συναλλαγής

Στο παραπάνω παράδειγμα, ο ίδιος χρήστης που δημιούργησε το προϊόν με όνομα "product_1" προσπαθεί να το αγοράσει. Ωστόσο, παρατηρούμε ότι η συναλλαγή αποτυγχάνει και εμφανίζεται ένα μήνυμα απόρριψης της συναλλαγής στο Metamask, όπως φαίνεται στην Εικόνα 5.16. Επιπλέον, αν ελέγξουμε το console, βλέπουμε τα σφάλματα που εμφανίζονται στην Εικόνα 5.17 από το Metamask και στο αρχείο Javascript, με το μήνυμα που προβάλλεται να είναι το εξής: "VM Exception while processing transaction: revert Seller cannot be the buyer". Αντίστοιχα μηνύματα σφαλμάτων εμφανίζονται και σε άλλες περιπτώσεις που δεν εκπληρούνται οι επικυρώσεις της σύμβασης. Στην συνέχεια εξετάζεται ένα παράδειγμα μιας επιτυχημένης αγοράς ενός προϊόντος.

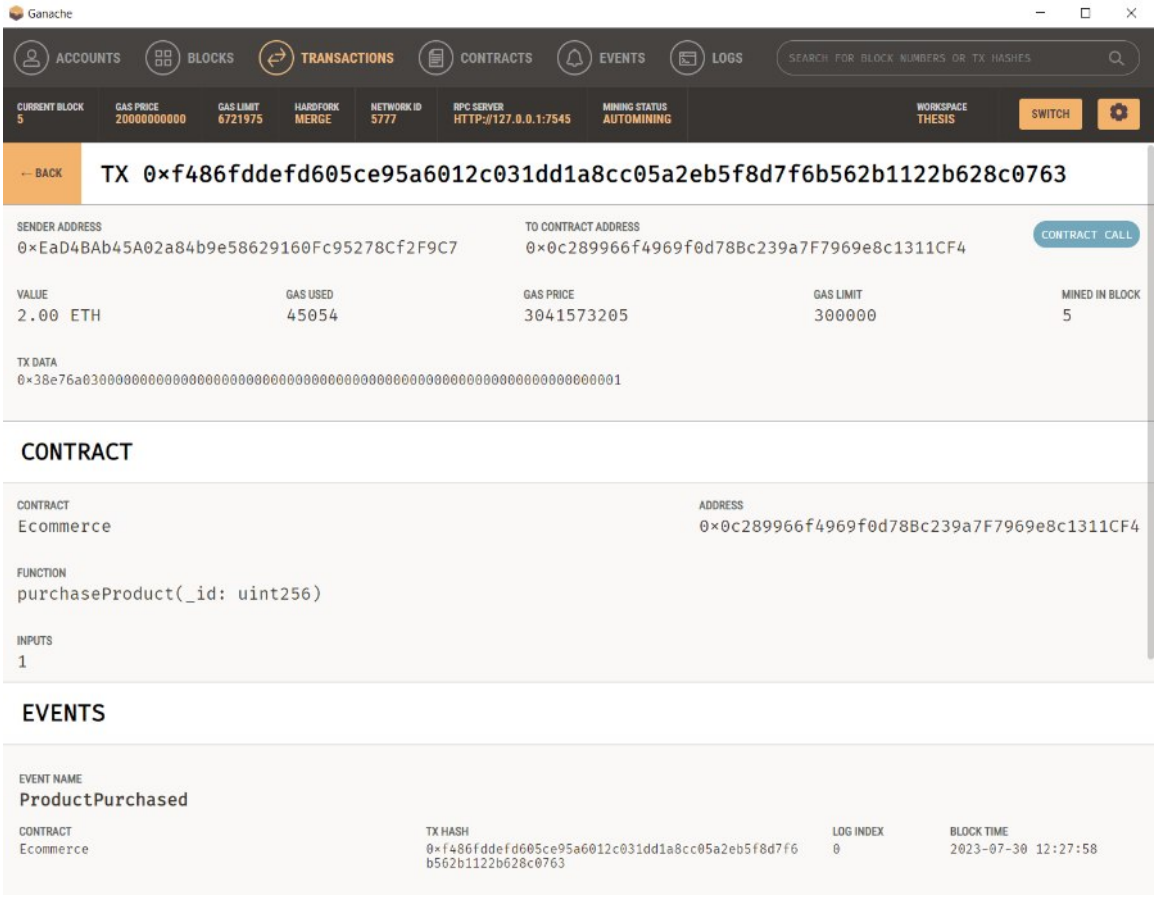


Εικόνα 5.18. Αγορά προϊόντος



Εικόνα 5.19. Ενημέρωση στοιχείων προϊόντος μετά την αγορά

Στο παραπάνω παράδειγμα, ο χρήστης προσπαθεί να αγοράσει το προϊόν με αναγνωριστικό 1. Όπως φαίνεται στο αναδυόμενο παράθυρο του Metamask, ο χρήστης χρησιμοποιεί το Account 3 για να στείλει μια συναλλαγή στην διεύθυνση του έξυπνου συμβολαίου, καλώντας την συνάρτηση του συμβολαίου "Purchase Product". Μόλις ολοκληρωθεί η αγορά, παρατηρούμε πως τα στοιχεία του αγοραστή και της διαθεσιμότητας του προϊόντος έχουν ενημερωθεί. Η αγορά προϊόντων, όπως και η δημιουργία προϊόντων, αλλάζει την κατάσταση του blockchain, καθώς η κάθε αγορά που πραγματοποιείται καταγράφεται σε μια συναλλαγή η οποία αποθηκεύεται σε ένα καινούργιο block. Στην παρακάτω εικόνα 5.20 παρουσιάζονται οι λεπτομέρειες της συναλλαγής μετά την αγορά του προϊόντος από το προηγούμενο παράδειγμα.



Εικόνα 5.20. Λεπτομέρειες συναλλαγής αγοράς προϊόντος

6.Επίλογος

Το blockchain αποτελεί μια μετασχηματιστική τεχνολογία που παρέχει τη βάση για την ανάπτυξη ασφαλών, κατανεμημένων εφαρμογών σε ποικίλους τομείς, υπερβαίνοντας τον αρχικό τομέα των νομισματικών αγορών. Η παρούσα διπλωματική εργασία αναλύει εκτενώς την τεχνολογία Blockchain, εξετάζοντας την εξέλιξή της, τις αρχιτεκτονικές προσεγγίσεις, τα μοντέλα συναίνεσης, καθώς και τα χαρακτηριστικά ασφάλειας και απορρήτου που αποτελούν ουσιαστικό μέρος της. Επιπλέον, διερευνά την επίδραση της τεχνολογίας Blockchain σε διάφορους τομείς του ηλεκτρονικού εμπορίου, όπως στα συστήματα ψηφιακών πληρωμών, στους αποκεντρωμένους ηλεκτρονικούς χώρους αγοράς, στα προγράμματα ανταμοιβής πιστών πελατών, καθώς και στη διαδικασία έγκρισης και αξιολόγησης κινητών εφαρμογών. Ακόμα, προσδιορίζει διάφορες εφαρμογές που σχετίζονται με αυτούς τους τομείς. Τέλος, παρουσιάζει μια μελέτη περίπτωσης που επικεντρώνεται στη διαχείριση έξυπνων συμβολαίων, εστιάζοντας στην υλοποίηση μιας αποκεντρωμένης εφαρμογής ηλεκτρονικού εμπορίου (Dapp) βασισμένης στο blockchain Ethereum.

6.1. Συμπεράσματα

Τα τελευταία χρόνια, παρατηρείται ένας αυξανόμενος αριθμός λύσεων που βασίζονται στην τεχνολογία Blockchain, πέρα από τις αρχικές εφαρμογές που αποτελούνταν από συστήματα ηλεκτρονικών νομισμάτων με τη διανομή ενός παγκόσμιου καθολικού που περιέχει όλες τις συναλλαγές. Παρά την ευρεία ανάπτυξη των εφαρμογών blockchain και την ευρεία διάδοση της τεχνολογίας σε διάφορους κλάδους, η χρήση της στις υπηρεσίες κινητής τηλεφωνίας και το ασύρματο περιβάλλον παραμένει περιορισμένη, με τις προοπτικές της να βρίσκονται ακόμα σε αρχικά στάδια. Καθώς η τεχνολογία αυτή γίνεται πιο ώριμη, τα blockchain αναμένεται να γίνουν όχι μόνο πιο επεκτάσιμα και αποτελεσματικά, αλλά και πιο ανθεκτικά, με τις εφαρμογές τους να διεισδύουν σε περισσότερους κλάδους από αυτούς που καλύπτονται στην παρούσα εργασία. Ωστόσο, πρέπει να τονιστεί ότι η τεχνολογία Blockchain εξακολουθεί να είναι σχετικά νέα, και οι οργανισμοί πρέπει να την αξιολογούν και να τη χρησιμοποιούν με προσοχή, όπως θα έκαναν με οποιαδήποτε άλλη τεχνολογική λύση που διαθέτουν, χρησιμοποιώντας την μόνο σε κατάλληλες καταστάσεις.

6.2. Όρια και περιορισμοί της διπλωματικής εργασίας

Στην παρούσα διατριβή, εντοπίζονται δύο κύριοι περιορισμοί που αφορούν στο κομμάτι της βιβλιογραφικής ανασκόπησης. Καταρχάς, ο περιορισμός στη χρήση της αγγλικής γλώσσας αποτελεί ένα σημαντικό ζήτημα, καθώς επιλέχθηκαν αποκλειστικά άρθρα που έχουν δημοσιευθεί στα αγγλικά. Αυτή η απόφαση αποκλείει πιθανότατα πολύτιμη έρευνα που διεξήχθη σε άλλες γλώσσες, με αποτέλεσμα τον περιορισμό του εύρους και του βάθους της μελέτης. Επιπλέον, ένας άλλος περιορισμός αφορά τη δυσκολία ή αδυναμία πρόσβασης στο πλήρες κείμενο ορισμένων δημοσιεύσεων, περιορίζοντας ενδεχομένως τη συνολική κατανόηση και το περιεχόμενο που προσφέρει η διατριβή.

Όσον αφορά την μελέτη περίπτωσης διαχείρισης ενός έξυπνου συμβολαίου, ο κύριος περιορισμός εντοπίζεται στην αδυναμία χρήσης περισσότερων του ενός αυτοματοποιημένων εργαλείων ανάλυσης ασφάλειας. Η αδυναμία αυτή οφείλεται είτε στην δυσκολία εγκατάστασης είτε σε προβλήματα που αντιμετωπίστηκαν κατά την εκτέλεση των διάφορων εργαλείων. Αυτό το γεγονός ενδεχομένως οδηγεί στη μη ανίχνευση τρωτών σημείων και σφαλμάτων στο έξυπνο συμβόλαιο.

6.3. Μελλοντικές Επεκτάσεις

Σχετικά με την εφαρμογή ηλεκτρονικού εμπορίου που αναπτύχθηκε ως μέρος της μελέτης περίπτωσης για τη διαχείριση ενός έξυπνου συμβολαίου, είναι σημαντικό να σημειωθεί πως πρόκειται για ένα βασικό παράδειγμα που μπορεί μελλοντικά να εξελιχθεί με πολλές προσθήκες και βελτιώσεις. Υπάρχουν αρκετές πιθανές ιδέες που πρέπει να εξεταστούν, όπως ο χειρισμός πολλαπλών πωλητών και η αποτελεσματική διαχείριση των αποθεμάτων προϊόντων. Επιπλέον, μπορεί να εξεταστεί η ενσωμάτωση πρόσθετων λειτουργιών που αφορούν την παράδοση ή την ακύρωση των παραγγελιών προκειμένου να βελτιωθεί η εμπειρία των χρηστών και να ενισχυθεί η λειτουργικότητα της πλατφόρμας.

Βιβλιογραφία

Abduljabbar, T. A., Tao, X., Zhang, J., Zhou, X., Li, L., & Cai, Y. (2021). A survey of privacy solutions using blockchain for recommender systems: Current status, classification and open issues. *The Computer Journal*, *64*(7), 1104-1129.

Ahmad, R. W., Salah, K., Jayaraman, R., Hasan, H. R., Yaqoob, I., & Omar, M. (2021). The role of blockchain technology in aviation industry. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), 4-15.

Ahmed, M. R., Meenakshi, K., Obaidat, M. S., Amin, R., & Vijayakumar, P. (2021). Blockchain based architecture and solution for secure digital payment system. In *ICC 2021-IEEE International Conference on Communications* (pp. 1- 6). IEEE.

Albert, E., Correas, J., Gordillo, P., Román-Díez, G., & Rubio, A. (2019). SAFEVM: a safety verifier for Ethereum smart contracts. In *Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis* (pp. 386-389).

Albert, E., Gordillo, P., Livshits, B., Rubio, A., & Sergey, I. (2018). Ethir: A framework for high-level analysis of ethereum bytecode. In *Automated Technology for Verification and Analysis: 16th International Symposium, ATVA 2018, Los Angeles, CA, USA, October 7-10, 2018, Proceedings* (pp. 513-520). Cham: Springer International Publishing.

Alharby, M., Aldweesh, A., & Van Moorsel, A. (2018). Blockchain-based smart contracts: A systematic mapping study of academic research (2018). In *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)* (pp. 1-6). IEEE.

Alt, R. (2020). Electronic Markets on blockchain markets. *Electronic Markets*, *30*(2), 181-188.

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

Ante, L. (2021). Smart contracts on the blockchain–A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519.

AppCoins. (2017). AppCoins White paper.

Arps, J. E., & Christin, N. (2020). Open market or ghost town? the curious case of OpenBazaar. In *International Conference on Financial Cryptography and Data Security* (pp. 561-577). Springer, Cham.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust* (pp. 164-186). Springer, Berlin, Heidelberg.

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

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, *7*, 164908-164940.

Bhujel, S., & Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors*, *22*(22), 8833.

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering, 90*, 106897.

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE Access, 9*, 61048-61073.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18* (pp. 486-504). Springer Berlin Heidelberg.

Bragagnolo, S., Rocha, H., Denker, M., & Ducasse, S. (2018). SmartInspect: solidity smart contract inspector. In *2018 International workshop on blockchain oriented software engineering (IWBOSE)* (pp. 9-18). IEEE.

Brent, L., Jurisevic, A., Kong, M., Liu, E., Gauthier, F., Gramoli, V., ... & Scholz, B. (2018). Vandal: A scalable security analysis framework for smart contracts. *arXiv preprint arXiv:1809.03981*.

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

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE Access*, *6*, 53019-53033.

Cappiello, B., & Carullo, G. (Eds.). (2021). *Blockchain, Law and Governance* (pp. 159 177). Springer.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain- based applications: Current status, classification and open issues. Te*lematics and Informatics, 36*, 55-81.

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

Chang, Y. W., Lin, K. P., & Shen, C. Y. (2019). Blockchain technology for e-marketplace. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 429-430). IEEE.

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. *Journal of Banking and Financial Technology*, *3*, 1-17.

Drummer, D., & Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of information technology*, *35*(4), 337-360.

Duan, L., Sun, Y., Zhang, K., & Ding, Y. (2022). Multiple-Layer Security Threats on the Ethereum Blockchain and Their Countermeasures. *Security and Communication Networks*, *2022*.

Earle, P. C., Gulker, M., & Stringham, E. P. (2022). Decentralized Marketplaces with Privately Enforced Contracts: A Case Study of OpenBazaar. *Journal of Private Enterprise*, *37*(4).

Ethereum Foundation (2023), Solidity Documentation Release 0.8.21. *Ethereum Foundation.*

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95-102.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art

review. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 1-15.

Feist, J., Grieco, G., & Groce, A. (2019). Slither: a static analysis framework for smart contracts. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)* (pp. 8-15). IEEE.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45-58.

Gao, J., Liu, H., Liu, C., Li, Q., Guan, Z., & Chen, Z. (2019). Easyflow: Keep ethereum away from overflow. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)* (pp. 23-26). IEEE.

Gao, W., Hatcher, W. G., & Yu, W. (2018). A survey of blockchain: Techniques, applications, and challenges. In *2018 27th international conference on computer communication and networks (ICCCN)* (pp. 1-11). IEEE.

Golosova, J., & Romanovs, A. (2018). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

Grech, N., Kong, M., Jurisevic, A., Brent, L., Scholz, B., & Smaragdakis, Y. (2018). Madmax: Surviving out-of-gas conditions in ethereum smart contracts. *Proceedings of the ACM on Programming Languages*, *2*(OOPSLA), 1-27.

Grieco, G., Song, W., Cygan, A., Feist, J., & Groce, A. (2020). Echidna: effective, usable, and fast fuzzing for smart contracts. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis* (pp. 557-560).

Grishchenko, I., Maffei, M., & Schneidewind, C. (2018). Ethertrust: Sound static analysis of ethereum bytecode. *Technische Universität Wien, Tech. Rep*, 1-41.

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

Hamilton, M. (2020). Blockchain distributed ledger technology: An introduction and focus on smart contracts. *Journal of Corporate Accounting & Finance*, *31*(2), 7-12.

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. *IEEE Network*, *34*(6), 114-119.

He, J., Balunović, M., Ambroladze, N., Tsankov, P., & Vechev, M. (2019). Learning to fuzz from symbolic execution with application to smart contracts. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 531-548).

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on bitcoin's peer-to-peer network. In *24th {USENIX} Security Symposium ({USENIX} Security 15)* (pp. 129-144).

Herlihy, M. (2019). Blockchains from a Distributed Computing Perspective. *Communications of the ACM, 62(2)*, 78-85.

Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., & Ylianttila, M. (2021). Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE Access*, *9*, 87643-87662.

Hill, B., Chopra, S., Valencourt, P., & Prusty, N. (2018). Blockchain Developer's Guide: Develop smart applications with Blockchain technologies-Ethereum, JavaScript, Hyperledger Fabric, and Corda. *Packt Publishing Ltd.*

Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., Amira, A., Varlamis, I., ... & Dimitrakopoulos, G. (2022). Blockchain-based recommender systems: Applications, challenges and future opportunities. *Computer Science Review*, *43*, 100439.

Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., & Lin, X. (2021). A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. Patterns, 2(2), 100179.

Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, *9*, 76153-76177.

Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry, 11(10),* 1198.

Jaccard, G. (2018). Smart contracts and the role of law. *Available at SSRN 3099885*.

Jiang, B., Liu, Y., & Chan, W. K. (2018). Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering* (pp. 259-269).

Johar, S., Ahmad, N., Asher, W., Cruickshank, H., & Durrani, A. (2021). Research and applied perspective to blockchain technology: A comprehensive survey. *Applied Sciences, 11(14)*, 6252.

Kabi, O. R., & Franqueira, V. N. (2018). Blockchain-based distributed marketplace. In *International Conference on Business Information Systems* (pp. 197-210). Springer, Cham.

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

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*(5), 2901-2925.

Kim, S. I., & Kim, S. H. (2020). E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, 1-13.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.

Krupp, J., & Rossow, C. (2018). {teEther}: Gnawing at Ethereum to Automatically Exploit Smart Contracts. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 1317-1333).

Kwon, Y., Kim, D., Son, Y., Vasserman, E., & Kim, Y. (2017, October). Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 195-209).

Lee, W. M. (2019). Beginning ethereum smart contracts programming. *With Examples in Python, Solidity and JavaScript.*

Lemos, C., Ramos, R. F., Moro, S., & Oliveira, P. M. (2022). Stick or Twist—The Rise of Blockchain Applications in Marketing Management. *Sustainability*, *14*(7), 4172.

Lessig L (2006) *Code: Version 2.0*. New York: Basic Books

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

Liao, Q., & Shao, M. (2021). Discussion on payment application in cross-border e-commerce platform from the perspective of blockchain. In *E3S Web of Conferences* (Vol. 235, p. 03020). EDP Sciences.

Lim, Y. H., Hashim, H., Poo, N., Poo, D. C. C., & Nguyen, H. D. (2019). Blockchain technologies in E-commerce: social shopping and loyalty program applications. In *International Conference on Human-Computer Interaction* (pp. 403-416). Springer, Cham.

Liu, T., Wu, J., Chen, L., Wu, Y., & Li, Y. (2020). Smart contract-based long-term auction for mobile blockchain computation offloading. *IEEE Access*, *8*, 36029-36042.

Lu, N., Wang, B., Zhang, Y., Shi, W., & Esposito, C. (2021). NeuCheck: A more practical Ethereum smart contract security analysis tool. *Software: Practice and Experience*, *51*(10), 2065-2084.

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

Luu, L., Chu, D., Olickel, H., Saxena, P., and Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24–28, 2016, pp. 254–269.

Madhani, P. M. (2022). Blockchain Deployment in Marketing: Developing Conceptual Frameworks and Research Propositions. *IUP Journal of Business Strategy*, *19*(3).

Maxwell, G. (2013). CoinJoin: Bitcoin privacy for the real world. In *Post on Bitcoin forum* (Vol. 3, p. 110).

Mekouar, L., Iraqi, Y., Damaj, I., & Naous, T. (2022). A survey on blockchain-based Recommender Systems: Integration architecture and taxonomy. *Computer Communications*, *187*, 1-19.

Merlina, A., Vitenberg, R., & Setty, V. (2022). A general and configurable framework for blockchain-based marketplaces. In *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing* (pp. 216-225).

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy* (pp. 397-411). IEEE.

Mohammed, S., Fiaidhi, J., Ramos, C., Kim, T. H., Fang, W. C., & Abdelzaher, T. (2021). Blockchain in eCommerce: A special issue of the ACM transactions on

internet of thingsBlockchain in eCommerce: A special issue of the ACM transactions on internet of things. *ACM Transactions on Internet Technology (TOIT)*, *21*(1), 11-55.

Monetha. (2017). Monetha White paper.

Moniruzzaman, M., Chowdhury, F., & Ferdous, M. S. (2020). Examining usability issues in blockchain-based cryptocurrency wallets. In *International Conference on Cyber Security and Computer Science* (pp. 631-643). Springer, Cham.

Morabito, V. (2017). Business innovation through blockchain. *Cham: Springer International Publishing*.

Mossberg, M., Manzano, F., Hennenfent, E., Groce, A., Grieco, G., Feist, J., ... & Dinaburg, A. (2019). Manticore: A user-friendly symbolic execution framework for binaries and smart contracts. In *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)* (pp. 1186-1189). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A. (2018). Finding the greedy, prodigal, and suicidal contracts at scale. In *Proceedings of the 34th annual computer security applications conference* (pp. 653-663).

Patel, V., Khatiwala, F., Shah, K., & Choksi, Y. (2020). A review on blockchain technology: Components, issues and challenges. In *ICDSMLA 2019* (pp. 1257-1262). Springer, Singapore.

Perez, D., & Livshits, B. (2021). Smart contract vulnerabilities: Vulnerable does not imply exploited. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 1325-1341).

Perez, L. J. D., Ibarra, L., Alejandro, G. F., Rumayor, A., & Lara-Alvarez, C. (2020). A loyalty program based on Waves blockchain and mobile phone interactions. *The Knowledge Engineering Review*, *35*.

Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of computer security*. Springer Science & Business Media.

Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D., & Velasquez, S. (2022). The NFT Hype: What Draws Attention to Non-Fungible Tokens?. *Mathematics*, *10*(3), 335.

Polat, E. (2022). Creating Loyal Customers with Digital Marketing Applications: The 5A Model. In *Handbook of Technology Application in Tourism in Asia* (pp. 257-273). Singapore: Springer Nature Singapore.

Popov, S. (2016). A probabilistic analysis of the nxt forging algorithm. *Ledger*, *1*, 69-83.

Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E. & Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. *IEEE Consumer Electronics Magazine, 7(4)*, 6-14.

Rahman, K. T. (2021). Applications of blockchain technology for digital marketing: A systematic review. *Blockchain Technology and Applications for Digital Marketing*, 16-31.

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments, 52*, 102039.

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

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). Coinshuffle: Practical decentralized coin mixing for bitcoin. In *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19* (pp. 345-364). Springer International Publishing.

Sai, A. R., Buckley, J., & Le Gear, A. (2019). Privacy and security analysis of cryptocurrency mobile applications. In *2019 fifth conference on mobile and secure services (MobiSecServ)* (pp. 1-6). IEEE.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy* (pp. 459-474). IEEE.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, *62*(6), 599-608.

Shaikh, E., & Mohammad, N. (2020). Applications of blockchain technology for smart cities. In *2020 fourth international conference on inventive systems and control (ICISC)* (pp. 186-191). IEEE.

So, S., Hong, S., & Oh, H. (2021). {SmarTest}: Effectively Hunting Vulnerable Transaction Sequences in Smart Contracts through Language {Model-Guided} Symbolic Execution. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 1361-1378).

So, S., Lee, M., Park, J., Lee, H., & Oh, H. (2020,). VeriSmart: A highly precise safety verifier for Ethereum smart contracts. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1678-1694). IEEE.

Sönmeztürk, O., Ayav, T., & Erten, Y. M. (2020). Loyalty program using blockchain. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 509-516). IEEE.

Srivastava, J. D., Kumar, N., & Bisht, H. (2019). Blockchain for loyalty rewards program management. *Amity University*, *21*(7), 94.

Subramanian, H. (2018). Decentralized blockchain-based electronic marketplaces. *Communications of t he A CM*, 6 1(1), 78–84.

Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE access, 7*, 176838-176869.

Szabo, N. (1994). Smart Contracts.

Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., & Alexandrov, Y. (2018). Smartcheck: Static analysis of ethereum smart contracts. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 9-16).

Torres, C. F., Schütte, J., & State, R. (2018). Osiris: Hunting for integer bugs in ethereum smart contracts. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 664-676).

Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: a framework for salient research topics. *Electronic Commerce Research and Applications*, *48*, 101054.

Trezentos P. & Pires D. (2017). AppCoins Distributed and Trusted App-based Transactions Protocol.

Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., & Vechev, M. (2018). Securify: Practical security analysis of smart contracts. In *Proceedings*

of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 67-82).

Tu, S. F., Hsu, C. S., & Wu, Y. T. (2022). A Loyalty System Incorporated with Blockchain and Call Auction. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(3), 1107-1123.

Umekwudo, J. O., & Shim, J. (2020). Blockchain technology for mobile applications recommendation systems. *Journal of Society for e-Business Studies*, *24*(3).

Van der Auwera, E., Schoutens, W., Giudici, M. P., & Alessi, L. (2020). Financial Risk Management for Cryptocurrencies. *Springer International Publishing*.

Vigliotti, M. G. (2021). What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts. *Frontiers in Blockchain*, *3*, 553671.

Waldo, J. (2019). A Hitchhiker's Guide to the Blockchain Universe. *Communications of the ACM*, *62(3)*, 38-42.

White, B., Mahanti, A., & Passi, K. (2022). Characterizing the OpenSea NFT marketplace. In *Companion Proceedings of the Web Conference 2022* (pp. 488-496).

Wohrer, M., & Zdun, U. (2018). Smart contracts: security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 2-8). IEEE.

Yadav, A. K., & Singh, K. (2020). Comparative analysis of consensus algorithms of blockchain technology. In *Ambient communications and computer systems* (pp. 205-218). Springer, Singapore.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *NISTIR 8202*. https://doi.org/10.6028/NIST.IR.8202

Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1508-1532.

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

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science*, *37*(4), 691-698.

Zhang, P., Xiao, F., & Luo, X. (2019). SolidityCheck: Quickly detecting smart contract problems through regular expressions. *arXiv preprint arXiv:1911.09425*.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.

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

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14(4),* 352-375.

Zou, Y., Meng, T., Zhang, P., Zhang, W., & Li, H. (2020). Focus on blockchain: A comprehensive survey on academic and application. *IEEE Access, 8,* 187182-187201.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*.

Ιστοσελίδες

ConsenSys. (2018). Mythril. *Github*, Διαθέσιμο: https://github.com/Consensys/mythril (2 Ιουλίου 2023)

ConsenSys Software Inc. (n.d.). Ganache – Documentation. Διαθέσιμο: https://trufflesuite.com/docs/ganache/ (19 Ιουλίου 2023).

ConsenSys Software Inc. (n.d.). Truffle - Documentation. Διαθέσιμο: https://trufflesuite.com/docs/truffle/ (19 Ιουλίου 2023)

Crytic. (2018). Slither - Detector Documentation. *Github*, Διαθέσιμο: https://github.com/crytic/slither/wiki/Detector-Documentation (20 Ιουλίου 2023)

Das, A. (2021). Smart contract address creation method & difference between smart contract address and wallet address (EOA). *Coinmonks*, Διαθέσιμο: https://medium.com/coinmonks/smart-contract-address-creation-method-difference-between-smart-contract-address-and-wallet-97b421506455 (14 Νοεμβρίου 2022)

Mohanty, S.P. (February 2022). Smart Contract Execution Steps. *ResearchGate*, Διαθέσιμο: https://www.researchgate.net/figure/Smart-Contract-Execution-Steps_fig2_358423428 (12 Σεπτεμβρίου 2022)

Taylor, N. (August 2020). What Is an E-Marketplace?. *Feedvisor*, Διαθέσιμο: https://feedvisor.com/resources/e-commerce-strategies/what-is-an-e-marketplace/ (7 Δεκεμβρίου 2022)

Παράρτημα Α

1. Αρχείο HTML (index.html):

```
<!DOCTYPE html>
<html>
  <head>
    <title>Ecommerce Dapp</title>
    <link rel="stylesheet" type="text/css" href="style.css">
  </head>
  <body>
    <h1>Ecommerce Dapp</h1>
    <form id="createProductForm">
      <label for="productName">Product Name:</label>
      <input type="text" id="productName" required>
      <br>
      <label for="productPrice">Product Price:</label>
      <input type="number" id="productPrice" required>
      <br>
      <button type="submit">Create Product</button>
    </form>

    <form id="purchaseProductForm">
      <label for="productId">Product ID:</label>
      <input type="number" id="productId" required>
      <br>
      <button type="submit">Purchase Product</button>
    </form>

    <h2>Product List</h2>
    <div id="productList"></div>

    <script src="https://cdn.jsdelivr.net/npm/web3@1.5.3/dist/web3.min.js"></script>
    <script src="app.js"></script>
  </body>
</html>
```

2. Αρχείο CSS (styles.css):

```
body {
  font-family: Arial, sans-serif;
  margin: 0;
  padding: 20px;
}

h1 {
  text-align: center;
}

h2 {
  margin-top: 20px;
  text-align: center;
}

form {
  display: flex;
  flex-direction: column;
  max-width: 400px;
  margin: 0 auto;
}

label {
  margin-top: 10px;
}

input[type="text"],
input[type="number"],
input[type="submit"] {
  padding: 10px;
  margin-top: 5px;
  border-radius: 4px;
  border: 1px solid #ccc;
  font-size: 14px;
}

input[type="submit"] {
```

```
    color: white;
    cursor: pointer;
  }

  #productList {
    max-width: 600px;
    margin: 0 auto;
  }

  .product {
    margin-top: 10px;
    padding: 10px;
    background-color: #f9f9f9;
    border: 1px solid #ccc;
    border-radius: 4px;
  }

  .product span {
    display: block;
    margin-bottom: 5px;
  }

  .product span:first-child {
    font-weight: bold;
  }
```

3. Αρχείο JavaScript (app.js):

```
// Connect to the Ethereum network using web3.js
const web3 = new Web3(Web3.givenProvider);

// Define the contract ABI and contract address
const contractABI = […
  ];
const contractAddress = '0x0c289966f4969f0d78Bc239a7F7969e8c1311CF4';

// Create an instance of the contract
const ecommerceContract = new web3.eth.Contract(contractABI, contractAddress);

```

```
12. // Handle form submission for creating a product
13. const createProductForm = document.getElementById('createProductForm');
14. createProductForm.addEventListener('submit', async (event) => {
15.   event.preventDefault();
16.
17.   const name = document.getElementById('productName').value;
18.   const price = document.getElementById('productPrice').value;
19.
20.   try {
21.     const accounts = await ethereum.request({ method: 'eth_requestAccounts' });
22.     const account = accounts[0];
23.
24.     await ecommerceContract.methods.createProduct(name, price)
25.       .send({ from: account });
26.
27.     // Product creation successful, update the UI
28.     alert('Product created successfully!');
29.
30.     // Clear the form
31.     createProductForm.reset();
32.     // Refresh the product list
33.     await displayProducts();
34.   } catch (error) {
35.     console.error('Failed to create product:', error);
36.   }
37. });
38.
39. // Function to display products
40. async function displayProducts() {
41.   try {
42.     const productListElement = document.getElementById('productList');
43.     productListElement.innerHTML = '';
44.
45.     let id = 0;
46.     let productExists = true;
47.     const products = [];
48.
49.     while (productExists) {
50.       try {
51.         const product = await ecommerceContract.methods.products(id).call();
```

```
      products.push(product);
      id++;
    } catch (error) {
      productExists = false;
    }
  }

  if (productListElement.children.length === 0) {
    for (const product of products) {
      const productElement = document.createElement('div');
      productElement.innerHTML = `
        <div class="product">
          <span>ID: ${product.id}</span>
          <span>Name: ${product.name}</span>
          <span>Price: ${product.price}</span>
          <span>Seller: ${product.seller}</span>
          <span>Buyer: ${product.buyer}</span>
          <span>Available: ${product.isAvailable}</span>
        </div>
      `;
      productListElement.appendChild(productElement);
    }
  }
 } catch (error) {
  console.error('Failed to retrieve products:', error);
 }
}

// Load the product list when the page loads
window.addEventListener('DOMContentLoaded', async () => {
 try {
  // Display the initial product list
  await displayProducts();

  // Listen for the 'ProductCreated' event to update the product list
  ecommerceContract.events.ProductCreated({}, async (error) => {
    if (!error) {
      await displayProducts();
    }
  });
```

```
92.
93.     // Listen for the 'ProductPurchased' event to update the product list
94.     ecommerceContract.events.ProductPurchased({}, async (error) => {
95.       if (!error) {
96.         await displayProducts();
97.       }
98.     });
99.   } catch (error) {
100.    console.error('Failed to connect to MetaMask:', error);
101.  }
102.});
103.
104.// Handle form submission for purchasing a product
105.const purchaseProductForm = document.getElementById('purchaseProductForm');
106.purchaseProductForm.addEventListener('submit', async (event) => {
107.  event.preventDefault();
108.
109.  const productId = document.getElementById('productId').value;
110.  const productIndex = productId - 1; // Correct index in the array
111.
112.  try {
113.    const accounts = await ethereum.request({ method: 'eth_requestAccounts' });
114.    const account = accounts[0];
115.
116.    // Fetch the product details based on the provided product ID
117.    const product = await ecommerceContract.methods.products(productIndex).call();
118.    const productPriceInWei = web3.utils.toWei(product.price.toString(), 'ether');
119.
120.    await ecommerceContract.methods.purchaseProduct(productId)
121.      .send({ from: account, value: productPriceInWei, gas: 300000 });
122.
123.    // Product purchase successful, update the UI
124.    alert('Product purchased successfully!');
125.
126.    // Clear the form
127.    purchaseProductForm.reset();
128.  } catch (error) {
129.    console.error('Failed to purchase product:', error);
130.  }
131.});
```