Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Τεχνολογία Blockchain στο αθλητικό στοίχημα: Ενίσχυση της διαφάνειας, της ασφάλειας και της αποτελεσματικότητας στις επιχειρηματικές διαδικασίες** **Blockchain Technology in Sports Betting: Enhancing Transparency, Security and Efficiency in Business Processes**
Ονοματεπώνυμο Φοιτητή	**Αντώνιος Ζολώτας**
Πατρώνυμο	**Γρηγόριος**
Αριθμός Μητρώου	**ΜΠΚΣΑ20015**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Καθηγητής**

Ημερομηνία Παράδοσης **11/2024**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Μιχαήλ Ψαράκης Αναπληρωτής Καθηγητής	Παναγιώτης Κοτζανικολάου Καθηγητής

ΕΥΧΑΡΙΣΤΊΕΣ

Θα ήθελα να ευχαριστήσω τον κ. Κοτζανικολάου, για το χρόνο, την υποστήριξη και την καθοδήγηση. Είχα την τιμή να έχω εκπληκτική εποπτεία και είμαι εξαιρετικά ευγνώμων για την ατελείωτη προσπάθεια σας και το χρόνο σας.

Επίσης θα ήθελα να ευχαριστήσω τον κ. Αποστόλου, που μου έδωσε την δυνατότητα να ασχοληθώ με μια άκρως ενδιαφέρουσα μελέτη και για όλες τις γνώσεις και τα εφόδια που κατάφερα να αποκτήσω ολοκληρώνοντας τον μεταπτυχιακό κύκλο σπουδών μου. Σας ευχαριστώ όλους για την γνώση, τον ενθουσιασμό και τις συμβουλές που μου παρείχατε καθόλη τη διάρκεια της μελέτης μου καθώς και τα πολύτιμα σχόλια κατά την ολοκλήρωσή της.

Τέλος θα ήθελα να ευχαριστήσω τη γυναίκα μου (Βάλια), τον αδερφό μου (Θάνο) και τους γονείς μου για τη βοήθεια και την ατελείωτη ενθάρρυνση και υποστήριξη καθ'όλη την διάρκεια της μελέτης μου.

Περίληψη

Η παρούσα διπλωματική εργασία εστιάζει στη σημασία των έξυπνων συμβολαίων και της τεχνολογίας blockchain στις σύγχρονες επιχειρηματικές διαδικασίες, με ιδιαίτερη έμφαση στις εφαρμογές τους στον τομέα του διαδικτυακού στοιχήματος. Η τεχνολογία blockchain προσφέρει μια καινοτόμο προσέγγιση στη διαχείριση και την ασφάλεια συναλλαγών, ενώ τα έξυπνα συμβόλαια επιτρέπουν την αυτοματοποίηση διαδικασιών που παραδοσιακά απαιτούσαν ανθρώπινη παρέμβαση.

Η εργασία αναλύει πώς τα έξυπνα συμβόλαια συμβάλλουν στην αποτελεσματικότητα και την ασφάλεια των διαδικτυακών στοιχημάτων, μειώνοντας την ανάγκη για μεσάζοντες και εξασφαλίζοντας τη διαφάνεια στις συναλλαγές. Επιπλέον, παρέχονται τεχνικά παραδείγματα που αναδεικνύουν την εφαρμογή αυτών των συμβολαίων σε πλατφόρμες διαδικτυακού στοιχήματος, περιγράφοντας τις διαδικασίες δημιουργίας, επιβεβαίωσης και εκτέλεσης συναλλαγών μέσω έξυπνων συμβολαίων.

Η μελέτη επίσης διερευνά τις προκλήσεις που σχετίζονται με την ασφάλεια και την κανονιστική συμμόρφωση, αναλύοντας περιπτώσεις που υπογραμμίζουν τις απαιτήσεις και τα πιθανά ρίσκα που συνδέονται με τη χρήση της τεχνολογίας blockchain. Μέσω αυτής της έρευνας, αναδεικνύεται η δυναμική του blockchain και των έξυπνων συμβολαίων να επαναστατήσουν τη βιομηχανία του στοιχήματος, παρέχοντας έναν πιο ασφαλή και αποτελεσματικό τρόπο διεξαγωγής συναλλαγών.

Η εργασία καταλήγει σε συμπεράσματα που επισημαίνουν τη σημασία της υιοθέτησης αυτών των τεχνολογιών για την ενίσχυση της ασφάλειας και της διαφάνειας στο διαδικτυακό στοίχημα, καθώς και τις προοπτικές ανάπτυξής τους στο μέλλον.

Abstract

This thesis focuses on the importance of smart contracts and blockchain technology in modern business processes, with a special emphasis on their applications in the field of online betting. Blockchain technology offers an innovative approach to transaction management and security, while smart contracts enable the automation of processes that traditionally required human intervention.

The paper analyzes how smart contracts contribute to the efficiency and security of online betting, reducing the need for intermediaries and ensuring transparency in transactions. In addition, technical examples are provided that highlight the application of these contracts in online betting platforms, describing the processes of creating, confirming and executing transactions through smart contracts.

The study also explores challenges related to security and regulatory compliance, analyzing cases that highlight the requirements and potential risks associated with the use of blockchain technology. Through this research, the potential of blockchain and smart contracts to revolutionize the betting industry is highlighted, providing a more secure and efficient way to conduct transactions.

The paper reaches conclusions that point to the importance of adopting these technologies to enhance security and transparency in online betting, as well as their future development prospects.

Πίνακας Περιεχομένων

Κεφάλαιο 1: Εισαγωγή

1.1 ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

1.1.1 Εισαγωγή στην τεχνολογία Blockchain

Η τεχνολογία Blockchain έχει τη μοναδική ικανότητα να προσφέρει διαφάνεια. Σε ένα blockchain, κάθε συναλλαγή καταγράφεται και γίνεται ορατή σε όλους τους συμμετέχοντες στο δίκτυο. Αφού καταγραφεί, καμία συναλλαγή δεν μπορεί να αλλάξει ή να διαγραφεί από το blockchain, διασφαλίζοντας ένα ακριβές ιστορικό αρχείο. Δημιουργεί εμπιστοσύνη, γιατί οι χρήστες μπορούν να ελέγχουν μόνοι τους τις πληροφορίες και να διασφαλίζουν την ακρίβειά τους.

Ασφάλεια
Ένα άλλο βασικό πλεονέκτημα της τεχνολογίας blockchain είναι η ασφάλεια. Η αποκεντρωμένη φύση των blockchains τα καθιστά εγγενώς ασφαλή έναντι των επιθέσεων hacking επειδή δεν έχουν ένα μόνο σημείο αποτυχίας. Επιπλέον, οι συναλλαγές σε blockchains είναι ασφαλείς μέσω προηγμένων κρυπτογραφικών αλγορίθμων που έχουν σχεδιαστεί για να είναι ασφαλείς από παραβιάσεις. Αυτό σημαίνει ότι από τη στιγμή που μια συναλλαγή καταγράφεται σε μια αλυσίδα μπλοκ, δεν μπορεί να αλλάξει χωρίς να ακυρωθεί ολόκληρη η αλυσίδα και να ειδοποιηθούν οι άλλοι συμμετέχοντες [1].

Αποδοτικότητα
Τα συστήματα blockchain έχουν τη δυνατότητα να βελτιώσουν σημαντικά την αποτελεσματικότητα σε πολλούς κλάδους. Εξαλείφοντας τους μεσάζοντες οι συναλλαγές μπορούν να διεκπεραιωθούν ταχύτερα και με χαμηλότερο κόστος σε blockchains. Για παράδειγμα, η αποστολή χρημάτων διεθνώς μέσω παραδοσιακών τραπεζικών καναλιών μπορεί να διαρκέσει μέρες και να επιφέρει σημαντικές χρεώσεις. Ωστόσο, η χρήση κρυπτονομισμάτων που βασίζονται στην τεχνολογία blockchain επιτρέπει σχεδόν στιγμιαίες μεταφορές με ελάχιστες χρεώσεις [2]. Επιπλέον, τα έξυπνα συμβόλαια μπορούν να αυτοματοποιήσουν τις μη αυτόματες διαδικασίες εκτελώντας προκαθορισμένες ενέργειες όταν πληρούνται ορισμένες προϋποθέσεις – εξοικονομώντας χρόνο και μειώνοντας τα σφάλματα.
Η τεχνολογία Blockchain έχει φέρει επανάσταση στον τρόπο με τον οποίο σκεφτόμαστε την αποθήκευση και την κοινή χρήση δεδομένων. Η αποκεντρωμένη φύση του παρέχει διαφάνεια, διασφαλίζοντας παράλληλα ότι οι συναλλαγές είναι ασφαλείς από οποιαδήποτε μορφή τροποποίησης ή διαγραφής αφού επιβεβαιωθούν με συναίνεση μεταξύ των συμμετεχόντων στο δίκτυο [3]. Οι κρυπτογραφικοί κατακερματισμοί διαδραματίζουν κρίσιμο ρόλο στη διατήρηση της ακεραιότητας των δεδομένων εντός των μπλοκ – καθιστώντας ουσιαστικά αδύνατο για οποιονδήποτε να τροποποιήσει πληροφορίες χωρίς ανίχνευση [4]. Τα έξυπνα συμβόλαια εξαλείφουν τους μεσάζοντες επιβάλλοντας αυτόματα τους όρους της συμφωνίας όταν πληρούνται συγκεκριμένα κριτήρια, βελτιστοποιώντας έτσι την αποτελεσματικότητα σε διάφορους τομείς όπως η χρηματοδότηση ή η διαχείριση της εφοδιαστικής αλυσίδας [5]. Οι αλυσίδες μπλοκ προσφέρουν επίσης βελτιώσεις στην απόδοση μειώνοντας τις καθυστερήσεις που προκαλούνται από επαληθεύσεις τρίτων και εκσυγχρονίζοντας τις μη αυτόματες διαδικασίες μέσω της αυτοματοποίησης [6]. Με λίγα λόγια, αυτά τα συστήματα προσφέρουν διαφάνεια, ασφάλεια και αποτελεσματικότητα ταυτόχρονα.

Οι κλάδοι που βασίζονται στην εμπιστοσύνη και την υπευθυνότητα επωφελούνται περισσότερο από τη διαφάνεια στα συστήματα blockchain. Σε μια αλυσίδα εφοδιασμού, για παράδειγμα, η προέλευση και η διαδρομή των προϊόντων μπορούν να παρακολουθούνται χρησιμοποιώντας μια αλυσίδα μπλοκ, διασφαλίζοντας έτσι ότι όλα τα εμπλεκόμενα μέρη μπορούν να πιστοποιήσουν τη γνησιότητα των αγαθών καθώς και τη συμμόρφωσή τους με τα πρότυπα.

Αυτό βοηθά στην πρόληψη των απατών, μεταξύ άλλων, καθιστώντας τους ανθρώπους υπεύθυνους για ό,τι κάνουν.

Ασφάλεια

Τα περισσότερα blockchain διαθέτουν χαρακτηριστικά ασφαλείας τα οποία είναι πολύ σημαντικά για τη λειτουργία τους. Η χρήση κρυπτογραφικών αλγορίθμων εγγυάται την ακεραιότητα των δεδομένων και τη μη απόρριψη αυτών των λογιστικών βιβλίων κατά την ηρεμία ή τη μεταφορά. Ένας κρυπτογραφικός κατακερματισμός συνδέει κάθε μπλοκ με το προηγούμενο, δημιουργώντας έτσι μια κατάσταση όπου η παραβίαση οποιουδήποτε μέρους του γίνεται σχεδόν αδύνατη χωρίς να γίνει αντιληπτή. Σαν να μην αρκεί αυτό, οι επιθέσεις είναι δύσκολες εναντίον αποκεντρωμένων δικτύων όπως αυτό, επειδή δεν υπάρχει κανένα σημείο από το οποίο μπορεί να προκληθεί αποτυχία [4].

Αλλά αυτά τα ίδια χαρακτηριστικά κάνουν επίσης την τεχνολογία blockchain ελκυστική για βιομηχανίες όπου οι πληροφορίες πρέπει να παραμένουν πλήρεις και ασφαλείς πάντα. Για παράδειγμα, στον χρηματοοικονομικό τομέα, τα αρχεία θα μπορούσαν να διατηρούνται με ασφάλεια έτσι ώστε κανείς να μην αμφισβητεί τη γνησιότητά τους, οδηγώντας σε μειωμένες περιπτώσεις δόλιας δραστηριότητας σε συνδυασμό με αυξημένη εμπιστοσύνη μεταξύ των συμμετεχόντων [5]. Ομοίως, τα δικαιώματα απορρήτου των ασθενών θα διατηρούνταν εάν οι πάροχοι υγειονομικής περίθαλψης χρησιμοποιούσαν blockchains, καθώς μη εξουσιοδοτημένα άτομα δεν θα είχαν πρόσβαση σε προσωπικά δεδομένα υγείας [6].

Αποδοτικότητα

Η αυτοματοποίηση που προκύπτει από τα έξυπνα συμβόλαια βελτιώνει σημαντικά τα επίπεδα απόδοσης εντός των ιδρυμάτων ιδιαίτερα για περιπτώσεις που περιλαμβάνουν δύσκολες διαδικασίες και αργούς ρυθμούς. Τα έξυπνα συμβόλαια εξαλείφουν την ανάγκη των διαμεσολαβητών, μειώνοντας έτσι τον χρόνο που απαιτείται συν το κόστος που προκύπτει κατά τα στάδια εκτέλεσης και επιβολής, όταν τα μέρη συμφωνούν για οτιδήποτε συμβατικό. Ο κλάδος των χρηματοοικονομικών υπηρεσιών καθώς και τα συστήματα διαχείρισης επιχειρήσεων ακινήτων βασίζονται σε μεγάλο βαθμό σε αυτά λόγω εγγενών προβλημάτων που σχετίζονται με μεγάλες περιόδους συναλλαγών ή δαπανηρές νομικές διαδικασίες [7].

Κάθε φορά που εκπληρώνονται προκαθορισμένες προϋποθέσεις, τα έξυπνα συμβόλαια εκτελούν όρους εξοικονομώντας χρόνο εκτός από την πρόληψη ανθρώπινων λαθών που ενδέχεται να προκαλέσουν διαφωνίες σχετικά με ζητήματα συμμόρφωσης που προκύπτουν από την ατελή εκπλήρωση των υποχρεώσεων. Ας υποθέσουμε ότι υπήρχε ένα ακίνητο που πωλούνταν σε ακίνητη περιουσία. Η μεταβίβαση ιδιοκτησίας μαζί με την επεξεργασία πληρωμών θα μπορούσε να γίνει αυτόματα με έξυπνα συμβόλαια, ελαχιστοποιώντας έτσι τη συμμετοχή μεσιτών ή δικηγόρων, καθιστώντας την έτσι ταχύτερη από πριν. Το ίδιο ισχύει και για τη διαχείριση της εφοδιαστικής αλυσίδας όπου η επαλήθευση μαζί με τις διαδικασίες πληρωμής μπορεί να πραγματοποιηθεί αυτόματα μέσω έξυπνων συμβάσεων, οδηγώντας έτσι σε βελτιώσεις αποτελεσματικότητας και μειωμένο διοικητικό κόστος.

1.1.2 Εφαρμογές τεχνολογίας blockchain

Η χρήση της τεχνολογίας blockchain δεν περιορίζεται σε κρυπτονομίσματα όπως το Bitcoin. Αυτό το σύστημα μπορεί να χρησιμοποιηθεί σε διάφορους κλάδους λόγω του υψηλού επιπέδου ασφαλείας και της διαφάνειάς του.

Πρώτον, παρέχει ορατότητα και ιχνηλασιμότητα σε όλες τις αλυσίδες εφοδιασμού. Οι εταιρείες μπορούν να καταγράφουν όλες τις συναλλαγές στο blockchain, διασφαλίζοντας έτσι τη συμμόρφωση και την αυθεντικότητα του προϊόντος. Αυτό βοηθά στην αποφυγή της απάτης, ενώ μειώνει το κόστος [8].

Δεύτερον, οι εγκαταστάσεις υγειονομικής περίθαλψης μπορούν να το αξιοποιήσουν για την καλύτερη διαχείριση των αρχείων των ασθενών. Μέσω αυτής της μεθόδου, μόνο εξουσιοδοτημένο προσωπικό θα έχει πρόσβαση σε ενημερωμένες και σωστές πληροφορίες σχετικά με το ιστορικό υγείας των ατόμων. Προωθεί επίσης την ανταλλαγή δεδομένων μεταξύ

διαφορετικών παρόχων, οδηγώντας σε συντονισμένη παροχή φροντίδας, επομένως βελτιωμένα αποτελέσματα [9].

Τρίτον, ο χρηματοοικονομικός τομέας επωφελείται πολύ από την αλυσίδα μπλοκ πέρα από τα ψηφιακά νομίσματα. Η τεχνολογία χρησιμοποιεί ένα ασφαλές σύστημα δημόσιου καθολικού που επαληθεύει τις συναλλαγές σε πραγματικό χρόνο μειώνοντας τους κινδύνους που σχετίζονται με απάτες ή την εμφάνιση λαθών κατά τη διάρκεια διακανονισμών διασυνοριακών πληρωμών κ.λπ. όπου εμπλέκονται μεσάζοντες. Τα έξυπνα συμβόλαια αυτοματοποιούν τις οικονομικές συμφωνίες μειώνοντας το κόστος συναλλαγής [10].

Ένας άλλος τομέας όπου θα μπορούσε να εφαρμοστεί είναι η βιομηχανία ακινήτων. Δημιουργώντας ένα μητρώο ανοιχτού κώδικα χωρίς παραποίηση που εμφανίζει αρχεία τίτλων ιδιοκτησίας μαζί με σχετικές λεπτομέρειες, τα έξυπνα συμβόλαια διευκολύνουν ταχύτερες διαδικασίες μεταβίβασης ακινήτων εξαλείφοντας την ανάγκη για δικηγόρους ή αντιπροσώπους [11].

Πέμπτον, αλλά όχι λιγότερο σημαντικό, η ασφάλεια των συστημάτων ψηφοφορίας θα μπορούσε να βελτιωθεί σημαντικά μέσω της χρήσης blockchains. Όταν οι ψήφοι καταγράφονται σε αυτόν τον τύπο βάσης δεδομένων, η ακεραιότητα των εκλογών είναι εγγυημένη καθώς καθίσταται αδύνατο για οποιονδήποτε να χειραγωγήσει τα αποτελέσματα, καθώς θα είχαν ήδη καταχωρηθεί σε ένα αμετάβλητο ψηφιακό βιβλίο [12].

Η αποκεντρωμένη φύση της τεχνολογίας Blockchain σε συνδυασμό με τα χαρακτηριστικά διαφάνειας την καθιστά ιδανική για εφαρμογές που απαιτούν εμπιστοσύνη και υπευθυνότητα μεταξύ των συμμετεχόντων. Εξασφαλίζει αντίσταση έναντι αστοχιών ή επιθέσεων παρέχοντας έτσι ασφαλείς πλατφόρμες όπου μπορούν να πραγματοποιηθούν μόνο έγκυρες συναλλαγές. Για άλλη μια φορά η αποτελεσματικότητά της εμφανίζεται εδώ με την αυτοματοποίηση των διαδικασιών που μειώνει το κόστος ενώ αυξάνει τη λειτουργική αποτελεσματικότητα [7].

Οι δυνατότητες του blockchain δεν είναι περιορισμένες καθώς συνεχίζει να εξελίσσεται με την πάροδο του χρόνου. Παρέχει μοναδικές δυνατότητες στις επιχειρήσεις να βελτιώσουν τις δραστηριότητές τους μέσω της διαφάνειας και της δόμησης εμπιστοσύνης με τα ενδιαφερόμενα μέρη. Επομένως, περισσότεροι τομείς είναι πιθανό να υιοθετήσουν αυτήν την τεχνολογία στο εγγύς μέλλον, οδηγώντας σε αυξημένη ασφάλεια παράλληλα με τη δημιουργία νέων συστημάτων που θα οδηγήσουν στην αποτελεσματικότητα εντός των οργανισμών [13] .

1.1.3 Τεχνολογία Blockchain στο αθλητικό στοίχημα

Ο κλάδος των στοιχημάτων κερδίζει δισεκατομμύρια δολάρια κάθε χρόνο. Ο τρόπος με τον οποίο οι διαδικτυακές στοιχηματικές εταιρείες κερδίζουν χρήματα από τα αθλητικά στοιχήματα είναι να ενεργούν ως ενδιάμεσοι λαμβάνοντας στοιχήματα από πελάτες. Το κάνουν αυτό θέτοντας τις πιθανότητες να επιτύχουν το περιθώριο κέρδους ενός ιστοτόπου στοιχημάτων (bookmaker). Προσαρμόζοντας τις αποδόσεις, οι ιστότοποι στοιχημάτων μπορούν να ελέγξουν πόσο μεγάλο κέρδος θα κερδίσουν σε κάθε αγώνα ή οποιοδήποτε είδος στοιχήματος προσφέρουν [40].

Η τεχνολογία Blockchain είναι ένα αποκεντρωμένο σύστημα για ασφαλή ψηφιακή επαλήθευση και αποθήκευση συναλλαγών και δεδομένων, χωρίς την ανάγκη κεντρικής αρχής ή διαμεσολαβητών. Το blockchain, που δημιουργήθηκε αρχικά για τον χρηματοοικονομικό τομέα και τη διαπραγμάτευση ψηφιακών νομισμάτων, αυξάνει το φάσμα των πιθανών εφαρμογών του σε διάφορους άλλους τομείς την τελευταία δεκαετία, όπως η υγειονομική περίθαλψη, η διοίκηση, η εφοδιαστική αλυσίδα και ο αθλητισμός.
Ένα άλλο προϊόν που χρησιμοποιεί την τεχνολογία blockchain είναι οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (DAO). Αυτοί επιτρέπουν σε περισσότερους θαυμαστές να συμμετέχουν στη διαχείριση αθλητικών ομάδων ή οργανισμών.

Ο χώρος του αθλητικού στοιχήματος περιβαλλόταν πάντα από ένα στρώμα διαμάχης και κινδύνου διαφθοράς. Η τεχνολογία Blockchain έχει τη δυνατότητα να φέρει επανάσταση στη βιομηχανία αθλητικών στοιχημάτων, προσφέροντας μεγαλύτερη διαφάνεια, ασφάλεια και

δικαιοσύνη στους παίκτες, καθώς και να επεκτείνει το πεδίο του στοιχήματος με τη χρήση κρυπτονομισμάτων.

Οι αποκεντρωμένες πλατφόρμες στοιχημάτων επιτρέπουν το peer-to-peer στοιχηματισμό και εξαλείφουν την ανάγκη για μεσάζοντες, με αυξημένη διαφάνεια και ασφάλεια.

Τα ανώνυμα στοιχήματα καθίστανται επίσης δυνατά από πλατφόρμες στοιχημάτων που βασίζονται σε blockchain, οι οποίες συμβάλλουν στην προστασία των προσωπικών πληροφοριών και του απορρήτου των συμμετεχόντων.

Η χρήση κρυπτονομισμάτων όπως το Bitcoin, το Ethereum και άλλα σε πλατφόρμες στοιχημάτων μπορεί να προσφέρει μεγαλύτερη ασφάλεια και ευκολία, με παραδοσιακά νομίσματα που ενέχουν μεγαλύτερο κίνδυνο ψηφιακής κακής χρήσης.

Όπως συμβαίνει με κάθε τάση, η υιοθέτηση του blockchain στον αθλητισμό έχει αντιμετωπίσει κριτική. Το ένα είναι η προσβασιμότητα, είτε από την άποψη του οικονομικού κόστους για την εφαρμογή ενός συστήματος blockchain είτε λόγω διαφορετικών επιπέδων ψηφιακής ωριμότητας. Ενώ αναφέραμε τη δυνατότητα του blockchain να εκδημοκρατίσει ορισμένες διαδικασίες στον αθλητισμό, (όπως η λήψη αποφάσεων, το στοίχημα, η διαχείριση δεδομένων και πολλά άλλα), ορισμένοι υποστηρίζουν ότι τα πλεονεκτήματά του είναι προσβάσιμα μόνο για μια ομάδα θαυμαστών που έχουν ψηφιακή παιδεία και αθλητικές ομάδες και οργανισμούς με επαρκή οικονομικά μέσα για να επενδύσουν σε αυτά τα τεχνολογικά προηγμένα συστήματα.

Η χρήση του blockchain υπόκειται επίσης σε κανονιστική συμμόρφωση, όπως είδαμε στην περίπτωση των Αποκεντρωμένων Αυτόνομων Οργανισμών, αλλά και στις συναλλαγές κρυπτονομισμάτων, τα στοιχήματα και τη διαχείριση δεδομένων. Ενώ ένα από τα βασικά πλεονεκτήματα της χρήσης του blockchain στον αθλητισμό είναι ότι μπορεί να προάγει τη διαφάνεια και να αποτρέπει τη διαφθορά και την απάτη λόγω της αμετάβλητης φύσης του, όπως σε κάθε άλλο κλάδο, είναι σημαντικό να τηρούνται οι νόμοι περί προστασίας προσωπικών δεδομένων και να αποτρέπεται η κατάχρηση οποιωνδήποτε στοιχείων των ενδιαφερομένων χωρίς τη συγκατάθεσή τους.

Το Blockchain είναι χωρίς αμφιβολία ένας αναπτυσσόμενος κλάδος που δεν έχει ακόμη αξιοποιήσει πλήρως τις δυνατότητές του. Θα συνεχίσουμε με ανυπομονησία να παρακολουθούμε την εξέλιξή του καθώς προσπαθούμε να παραμείνουμε στην πρώτη γραμμή των σημαντικών εξελίξεων στον κόσμο των ψηφιακών τεχνολογιών και της καινοτομίας στον αθλητισμό.

1.2 ΣΚΟΠΟΣ ΔΙΑΤΡΙΒΗΣ

Στόχοι διατριβής

Ο βασικός στόχος αυτής της μελέτης είναι να προσδιορίσει τον ριζοσπαστισμό που θα μπορούσε να επιφέρει η τεχνολογία blockchain και τα έξυπνα συμβόλαια όσον αφορά τη διαφάνεια, την ασφάλεια και την αποτελεσματικότητα στις επιχειρηματικές δραστηριότητες, ειδικά στον κλάδο των αθλητικών στοιχημάτων. Ως εκ τούτου, αυτή η έρευνα σκοπεύει να διερευνήσει πώς αυτές οι εφευρέσεις μπορούν να διορθώσουν τις επικρατούσες αδυναμίες σε αυτόν τον τομέα μέσω μιας εξέτασης των αρχών, των χρήσεων καθώς και των προκλήσεων γύρω από το blockchain. Κατά συνέπεια, η έρευνα θα:

1. Αναλύσει τις θεμελιώδεις αρχές της τεχνολογίας Blockchain: Μια λεπτομερής ματιά στο τι συνθέτει τα blockchain, όπως η δομή τους. αλγόριθμοι συναίνεσης που χρησιμοποιούνται μεταξύ άλλων όπως οι διαδικασίες συναλλαγών [3], [13].
2. Διερευνήσει τον ρόλο και τους λειτουργικούς μηχανισμούς των έξυπνων συμβάσεων: Θα εξετάσει πώς λειτουργούν μηχανικά, καθώς και όπου μπορούν να εφαρμοστούν πιο αποτελεσματικά σε διαφορετικούς τομείς, δίνοντας παράλληλα μεγάλη έμφαση στην αυτοματοποίηση της διαδικασίας μέσω της μείωσης των μεσαζόντων [5].
3. Αξιολογήσει τα οφέλη της ασφάλειας και της διαφάνειας: Αυτή η ενότητα θα αξιολογήσει τα χαρακτηριστικά ασφαλείας, συμπεριλαμβανομένης της αποκεντρωμένης φύσης που

προέρχονται από κρυπτογραφικά ιδρύματα που ενισχύουν την εμπιστοσύνη στις επιχειρηματικές συναλλαγές που εκτελούνται χρησιμοποιώντας τεχνολογία blockchain [4] [11].

4. Προσδιορισμός Εφαρμογών Ειδικών για Βιομηχανίες: Διαφορετικοί τομείς θα πρέπει να λαμβάνονται υπόψη όπως τα αθλητικά στοιχήματα, όπου δίνονται παραδείγματα που δείχνουν επιτυχυμένες ιστορίες μαζί με κινδύνους που ενέχονται κατά τη διαδικασία υλοποίησης [14].
5. Θα εξετάσει ρυθμιστικά ζητήματα και ζητήματα ασφάλειας που αντιμετωπίζουν τα συστήματα χρησιμοποιώντας την τεχνολογία: Πρέπει να εξεταστούν οι κανονισμοί εντός των οποίων λειτουργούν τα έξυπνα συμβόλαια παράλληλα με την εξασφάλιση ασφαλών μεθόδων χρήσης σύμφωνα με τις απαιτήσεις συμμόρφωσης.

Σχέση με τις τρέχουσες τεχνολογικές τάσεις

Το Blockchain είναι η ταχύτερα αναπτυσσόμενη τεχνολογική εφεύρεση από την ίδρυσή του και την υιοθέτησή του μόνο αυτόν τον αιώνα, ξεπερνώντας μέχρι στιγμής όλα τα άλλα επιτεύγματα που έχουν επιτευχθεί σε παρόμοια χρονική περίοδο πριν από αυτό. Η ικανότητά του να εξασφαλίζει ασφάλεια και διαφάνεια ταυτόχρονα, έχει προκαλέσει μεγάλες αλλαγές σε διάφορους κλάδους παγκοσμίως, καθώς προσφέρει επίσης μεγαλύτερη αποτελεσματικότητα στις διαδικασίες.

Η συνάφεια της διατριβής με τις τρέχουσες τεχνολογικές τάσεις μπορεί να περιγραφεί ως εξής:

1. Το blockchain κερδίζει ολοένα και περισσότερο έδαφος σε διάφορους τομείς, όπως η χρηματοδότηση, η αλυσίδα εφοδιασμού και η υγειονομική περίθαλψη. Οι βιομηχανίες χρειάζεται να εξερευνήσουν διαφορετικές περιπτώσεις χρήσης αυτής της καινοτομίας, ακόμα και πέρα από τον άμεσο τομέα τους. Η παρούσα έρευνα επικεντρώνεται στον κλάδο των αθλητικών στοιχημάτων, που εκτιμάται ότι είναι έτοιμος για σημαντικές αλλαγές μέσω της εφαρμογής της τεχνολογίας blockchain [16].
2. Σε μια εποχή όπου οι παραβιάσεις δεδομένων και οι απάτες είναι συχνό φαινόμενο, η ανάγκη για ασφαλή και ανοιχτά συστήματα είναι μεγαλύτερη από ποτέ. Με την αποκεντρωμένη φύση του και το αμετάβλητο χαρακτηριστικό του καθολικού του, το blockchain προσφέρει ισχυρές λύσεις σε αυτά τα προβλήματα, καθιστώντας το ιδιαίτερα σχετικό και απαραίτητο τώρα [17].
3. Καινοτομία στα Έξυπνα Συμβόλαια: Αντιπροσωπεύουν μια σημαντική καινοτομία για την αυτοματοποίηση των συναλλαγών με ασφάλεια χωρίς κανέναν μεσάζοντα. Αυτή η διατριβή διερευνά τον τρόπο με τον οποίο εξορθολογίζουν τις επιχειρηματικές διαδικασίες μειώνοντας έτσι το κόστος ενώ παράλληλα ενισχύουν την εμπιστοσύνη σε διάφορες εφαρμογές, ιδιαίτερα στο αθλητικό στοίχημα [18].
4. Ρυθμιστικές εξελίξεις: Οι κυβερνήσεις και οι ρυθμιστικοί φορείς παγκοσμίως παλεύουν με τη ρύθμιση του blockchain, αλλά οι επιχειρήσεις που επιθυμούν να υιοθετήσουν την τεχνολογία πρέπει πρώτα να κατανοήσουν τις κανονιστικές προκλήσεις που αντιμετωπίζουν σε διαφορετικές δικαιοδοσίες πριν προβούν σε οποιαδήποτε κίνηση. Αυτή η διατριβή καλύπτει τέτοιες πτυχές διαφωτίζοντας τους αναγνώστες σχετικά με το εξελισσόμενο νομικό τοπίο [19].

Κεφάλαιο 2: Blockchain & Smart Contracts

2.1 ΕΙΣΑΓΩΓΗ ΣΤΟ BLOCKCHAIN ΚΑΙ ΣΤΑ SMART CONTRACTS

2.1.1 Ιστορία και Εξέλιξη

Η τεχνολογία Blockchain έχει τις ρίζες της στη λευκή βίβλο του Bitcoin, που δημοσιεύτηκε το 2008 από μια ανώνυμη προσωπικότητα με το όνομα Satoshi Nakamoto. Εκεί, το blockchain περιγράφεται ως ένα σύστημα ηλεκτρονικών συναλλαγών τύπου peer-to-peer, που χρησιμοποιεί μηχανισμό απόδειξης εργασίας (proof of work) για να επιτρέψει τις συναλλαγές χωρίς την ανάγκη εμπιστοσύνης μεταξύ των μερών και χωρίς να απαιτείται κάποιος αξιόπιστος τρίτος. Η ιδέα πίσω από αυτό ήταν ότι ένα κατανεμημένο καθολικό που ονομάζεται «blockchain» θα μπορούσε να καταγράφει όλες αυτές τις συναλλαγές με διαφάνεια, διασφαλίζοντας ταυτόχρονα την ασφάλεια μέσω της κρυπτογραφίας [3].

Ωστόσο, η έννοια του blockchain βασίζεται σε προηγούμενες εργασίες στην κρυπτογραφία και την επιστήμη των υπολογιστών. Το 1991, ο W.Scott Stornetta και ο Stuart Haber ανέπτυξαν μια μέθοδο για τη χρονοσήμανση ψηφιακών εγγράφων που αποτρέπει την αναδρομή καθώς και την παραβίαση. Αυτό έθεσε τα θεμέλια για κρυπτογραφικές ιδέες που χρησιμοποιούνται στο blockchain [20]. Έγινε επίσης ένα άλλο βήμα προς την εξασφάλιση κατανεμημένων δικτύων επαληθεύοντας αποτελεσματικά την ακεραιότητα των δεδομένων χρησιμοποιώντας δέντρα Merkle που σχεδιάστηκαν από τον Ralph Merkle το 1980 [21].

Η τεχνολογία Blockchain έχει επιτύχει σημαντικά ορόσημα με την πάροδο του χρόνου. Η εισαγωγή του Bitcoin αντιπροσώπευε μια πραγματική εφαρμογή όπου οι άνθρωποι μπορούν να δουν πώς λειτουργεί πρακτικά όσον αφορά τα ψηφιακά νομίσματα που κυκλοφόρησαν το 2009. Το 2013 ο Vitalik Buterin πρότεινε το Ethereum. Μια πλατφόρμα βασισμένη στα θεμέλια του bitcoin που επιτρέπει στους προγραμματιστές να δημιουργούν αποκεντρωμένες εφαρμογές που τροφοδοτούνται από έξυπνες συμβάσεις - αυτοεκτελούμενες συμφωνίες των οποίων οι όροι είναι γραμμένοι απευθείας σε κώδικα που είναι αποθηκευμένος σε blockchains [5]. Η δυνατότητα προγραμματισμού κωδικών σε αυτά τα κατανεμημένα λογιστικά βιβλία σηματοδότησε ένα ακόμη σημείο καμπής προς περιπτώσεις ευρύτερης χρήσης αυτής της καινοτομίας πέρα από τις οικονομικές συναλλαγές.

Από τότε πολλές άλλες πλατφόρμες έχουν έρθει για να καλύψουν διαφορετικές ανάγκες και προκλήσεις που τίθενται από τις επιχειρήσεις κατά την εφαρμογή λύσεων blockchain. Για παράδειγμα, υπάρχει μηχανισμός συναίνεσης απόδειξης στοιχήματος γνωστός ως Peercoin, ο οποίος εισήχθη μαζί με την ιδέα των sidechains ή ακόμα και λύσεις διαλειτουργικότητας όπως το Polkadot που αναπτύχθηκε από τον Gavin Wood [22] [23].

2.1.2 Συνάφεια στη σύγχρονη τεχνολογία

Η τεχνολογία Blockchain αποτελεί βασικό στήριγμα της πρόσφατης τεχνολογικής επανάστασης που επιλύει ορισμένα πιο δύσκολα προβλήματα που αντιμετωπίζουν διαφορετικοί κλάδοι. Είναι πολύτιμο λόγω πολλών χαρακτηριστικών που σχετίζονται με την εμπιστοσύνη, την ασφάλεια και την αποτελεσματικότητα.

1. Αξιοπιστία και Διαφάνεια: Ο τρόπος με τον οποίο λειτουργεί το blockchain όταν είναι αποκεντρωμένο, αφαιρεί την ανάγκη για μια κεντρική αρχή, ελαχιστοποιώντας έτσι τις πιθανότητες αποτυχίας σε ένα σημείο ή διαφθοράς. Σε αυτό το είδος δικτύου, κάθε συναλλαγή που συμβαίνει καταγράφεται και είναι ορατή από όλα τα μέλη και έτσι γίνεται πιο ανοιχτή. Οι χρήστες είναι σε θέση να εμπιστεύονται ο ένας τον άλλον εύκολα, επειδή κάθε άτομο μπορεί να ελέγξει εάν τα δεδομένα έχουν παραβιαστεί ή όχι [1].

2. Ασφάλεια: Οι μέθοδοι που χρησιμοποιούνται από την τεχνολογία blockchain για την προστασία δεδομένων βασίζονται σε πολύπλοκες κρυπτογραφικές τεχνικές. Ένα μπλοκ έχει ένα μοναδικό αναγνωριστικό που ονομάζεται κατακερματισμός, το οποίο προέρχεται από το προηγούμενο που οδηγεί σε μια αλυσίδα που δεν μπορεί να αλλάξει χωρίς να επηρεαστούν οι άλλοι, επομένως είναι δύσκολο για οποιονδήποτε να αλλάξει οτιδήποτε έχει καταγραφεί σε μπλοκ. Η επαλήθευση που γίνεται μέσω μηχανισμών συναίνεσης ενισχύει την ασφάλεια ακόμη περισσότερο, καθώς οι συναλλαγές πρέπει πρώτα να λάβουν συμφωνία έγκρισης μεταξύ των συμμετεχόντων στο δίκτυο προτού γίνουν μέρος του blockchain [4].
3. Αποτελεσματικότητα: Στις περισσότερες περιπτώσεις τα παραδοσιακά συστήματα χρησιμοποιούν μεσάζοντες κατά τη διάρκεια των συναλλαγών αυξάνοντας έτσι τα έξοδα που προκύπτουν καθώς και τον χρόνο που απαιτείται για την ολοκλήρωση λόγω των διαδικασιών επαλήθευσης που εμπλέκονται με αυτά καθώς και η εκτέλεση που είναι χειροκίνητη, προκαλώντας μερικές φορές και καθυστερήσεις. Αυτό που κάνει το blockchain είναι να συντομεύει αυτές τις διαδικασίες μέσω έξυπνων συμβάσεων που αυτοματοποιούν την επαλήθευση παράλληλα με τις πτυχές εκτέλεσης που εμπλέκονται σε αυτές. Ο χρηματοοικονομικός τομέας θα επωφεληθεί σε μεγάλο βαθμό από τις μειωμένες περιόδους συναλλαγών και το κόστος, ενώ η διαχείριση της εφοδιαστικής αλυσίδας μαζί με την ακίνητη περιουσία θα πραγματοποιήσει επίσης σημαντικές βελτιώσεις [14].
4. Αποκεντρωμένες Εφαρμογές (DApps): Με πλατφόρμες όπως το Ethereum ήρθαν νέες δυνατότητες καινοτομίας, εν μέρει χάρη στο γεγονός ότι οι προγραμματιστές έχουν πλέον πρόσβαση στα εργαλεία που χρειάζονται κατά τη δημιουργία DApps που μπορούν να λειτουργήσουν χωρίς να βασίζονται σε οποιονδήποτε μεμονωμένο οργανισμό που ενεργεί ως μεσάζων ή αρχή σε τέτοιες εφαρμογές. Ορισμένοι τομείς στους οποίους μπορεί να γίνουν μάρτυρες αυτών των εφευρέσεων περιλαμβάνουν τη χρηματοδότηση (αποκεντρωμένη χρηματοδότηση ή DeFi), τη διακυβέρνηση καθώς και την ψηφιακή ταυτότητα μεταξύ άλλων [5].

Συμπερασματικά, αυτό που έχει επιφέρει η τεχνολογία blockchain δεν είναι τίποτα λιγότερο από μια επανάσταση στη σύγχρονη τεχνολογία. Παρέχει ασφαλείς, διαφανείς και αποτελεσματικές λύσεις, καθιστώντας το εφαρμόσιμο σε διάφορους κλάδους για την επίλυση διαφορετικών προκλήσεων.

2.2 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΟΥ BLOCKCHAIN

Αποκέντρωση (Decentralization)

Η τεχνολογία Blockchain βασίζεται στην αποκέντρωση, η οποία είναι το βασικό χαρακτηριστικό της που την ξεχωρίζει από τα κεντρικά συστήματα. Σε ένα αποκεντρωμένο δίκτυο blockchain, κανένας μόνος συμμετέχων δεν έχει τον έλεγχο ολόκληρου του δικτύου. Αντίθετα, όλοι οι συμμετέχοντες ή οι κόμβοι μοιράζονται τον έλεγχο μέσα τους όπου κάθε κόμβος αποθηκεύει ένα αντίγραφο της πλήρους αλυσίδας μπλοκ και συμμετέχει στην επαλήθευση και την καταγραφή συναλλαγών [12].

Υπάρχουν πολλά οφέλη που πρέπει να αποκομιστούν από την αποκέντρωση του blockchain:
Ισχυρότητα: Τα αποκεντρωμένα δίκτυα είναι λιγότερο επιρρεπή σε επιθέσεις ή αποτυχίες, καθώς δεν διαθέτουν ένα μόνο σημείο αστοχίας. Εάν ένας κόμβος παραβιαστεί ή τεθεί εκτός σύνδεσης, οι υπόλοιποι θα εξακολουθούν να λειτουργούν κανονικά [16].

Ασφαλείς συναλλαγές: Εδώ οι συναλλαγές δεν χρειάζονται αξιόπιστους μεσάζοντες επειδή ολόκληρο το δίκτυο τις επικυρώνει. Κατά συνέπεια, αυτό μειώνει τις ευκαιρίες για απάτη και διαφθορά δημιουργώντας ένα περιβάλλον όπου δεν μπορεί να δοθεί εμπιστοσύνη σε άλλους συμμετέχοντες ή κεντρική αρχή [3].

Αντίσταση στη λογοκρισία: Τα δεδομένα που είναι αποθηκευμένα σε blockchains δεν μπορούν εύκολα να ελεγχθούν ή να αλλάξουν από οποιαδήποτε οντότητα, καθιστώντας έτσι δύσκολη τη λογοκρισία τους. Αυτό έχει ιδιαίτερη σημασία όταν η ελευθερία της πληροφόρησης και της έκφρασης διακυβεύεται [24].

Αμεταβλητότητα (Immutability)

Μόλις καταγραφούν σε μια αλυσίδα μπλοκ τα δεδομένα γίνονται αμετάβλητα που σημαίνει ότι δεν μπορούν να τροποποιηθούν ξανά αργότερα. Ο κρυπτογραφικός κατακερματισμός μαζί με τον τρόπο δομής των μπλοκ διευκολύνει αυτήν την ιδέα μέσα στις αλυσίδες μπλοκ. Κάθε μπλοκ περιέχει κατακερματισμό των προηγούμενων, δημιουργώντας έτσι αλυσίδες μπλοκ κρυπτογραφικά συνδεδεμένων μεταξύ τους, έτσι ώστε αν κάποιο από αυτά παραβιαστεί, όχι μόνο τα δικά του αλλά και τα επόμενα hashes θα έπρεπε να αλλάξουν επίσης – κάτι υπολογιστικά ανέφικτο [4].

Παρακάτω είναι μερικά ακόμη οφέλη που προκύπτουν από την αμετάβλητη σε σχέση με τις αλυσίδες μπλοκ:

1. Ακεραιότητα δεδομένων: Δεδομένου ότι τίποτα δεν μπορεί να αλλάξει μόλις γραφτεί σε αυτό, η ακεραιότητα είναι εγγυημένη για πάντα, επειδή κανείς δεν θα διαγράψει ποτέ οτιδήποτε, είτε τυχαία είτε εσκεμμένα. Αυτό καθιστά μια τέτοια τεχνολογία καταλληλότερη για εφαρμογές όπου η ορθότητα και η συνέπεια των πληροφοριών είναι πρωταρχικής σημασίας [17].
2. Δυνατότητα ελέγχου: Η ύπαρξη ενός αμετάβλητου συστήματος επιτρέπει τη δημιουργία διαφανών επαληθεύσιμων αρχείων συναλλαγών που πραγματοποιήθηκαν με την πάροδο του χρόνου, τα οποία μπορούν πάντα να χρησιμοποιηθούν κατά τη διάρκεια των ελέγχων. Αυτή η δυνατότητα είναι πιο χρήσιμη στον χρηματοοικονομικό τομέα, καθώς και στη διαχείριση της εφοδιαστικής αλυσίδας, όπου η δυνατότητα παρακολούθησης των αλλαγών που γίνονται σε κάθε βήμα στην πορεία γίνεται κρίσιμη [1].
3. Ασφάλεια: Οι επιτιθέμενοι από το σχεδιασμό τους δυσκολεύονται να παραβιάσουν τέτοια συστήματα λόγω της αμετάβλητης φύσης τους, επομένως ενισχύουν την ασφάλεια γύρω τους. Αυτό βοηθά στην προστασία από απάτες ή κυβερνοεπιθέσεις [25].

Διαφάνεια (Transparency)

Μια άλλη αρχή που βασίζεται στην τεχνολογία blockchain είναι η διαφάνεια. Αυτό αναφέρεται στο πόσο ελεύθερα προσβάσιμα δεδομένα συναλλαγών θα πρέπει να είναι μέσα σε ένα δεδομένο δίκτυο, έτσι ώστε οποιοσδήποτε εμπλεκόμενος να μπορεί να δει τι συμβαίνει όλη την περίοδο. Με άλλα λόγια, στα παραδοσιακά κεντρικά συστήματα κανείς δεν μπορεί εύκολα να δει ολόκληρη την εγγραφή γεγονότων, ενώ σε μια αλυσίδα μπλοκ κάθε καταγεγραμμένη συναλλαγή είναι ορατή σε οποιονδήποτε κόμβο [14].

Στη συνέχεια θα περιγράψουμε ορισμένα πλεονεκτήματα που προκύπτουν από τη διαφάνεια των blockchain:

1. Εμπιστοσύνη: Οι άνθρωποι τείνουν να εμπιστεύονται περισσότερο όταν έχουν τρόπους να επαληθεύουν την ειλικρίνεια ανεξάρτητα, καθιστώντας έτσι την ακεραιότητα πρωταρχικής σημασίας μεταξύ των κοινών λογιστικών βιβλίων. Αυτό συμβαίνει κυρίως σε περιβάλλοντα που δεν υπάρχει εμπιστοσύνη μεταξύ διαφορετικών μερών [11].
2. Υπευθυνότητα: Όταν όλα γίνονται ανοιχτά, τότε οι άνθρωποι αισθάνονται υπεύθυνοι για τις ενέργειές τους γνωρίζοντας πολύ καλά ότι και οι άλλοι θα το γνωρίζουν καθώς κάθε κίνημα παρακολουθείται μόνιμα κάπου δημοσίως διαθέσιμο. Σε αυτήν την περίπτωση, οι δόλιες δραστηριότητες θα μειωθούν ενώ ενισχύονται οι ηθικές συμπεριφορές [17].
3. Κανονιστική συμμόρφωση: Για τη συμμόρφωση με τους κανονισμούς, μπορεί να είναι χρήσιμο για το blockchain να φωτίσει τα πράγματα δημιουργώντας ένα αποδεδειγμένο αμετάβλητο αρχείο όλων των συναλλαγών που έχουν πραγματοποιηθεί. Αυτό ισχύει

πολύ σε κλάδους όπου οι χρηματοοικονομικές υπηρεσίες και οι υπηρεσίες υγείας ελέγχονται σε μεγάλο βαθμό [19].

4. Δυνατότητα ελέγχου: Η ύπαρξη ενός αμετάβλητου συστήματος επιτρέπει τη δημιουργία διαφανών επαληθεύσιμων αρχείων συναλλαγών που πραγματοποιήθηκαν με την πάροδο του χρόνου, τα οποία μπορούν πάντα να χρησιμοποιηθούν κατά τη διάρκεια των ελέγχων. Αυτή η δυνατότητα είναι πιο χρήσιμη στον χρηματοοικονομικό τομέα, καθώς και στη διαχείριση της εφοδιαστικής αλυσίδας, όπου η δυνατότητα παρακολούθησης των αλλαγών που γίνονται σε κάθε βήμα στην πορεία είναι κρίσιμη [1].

2.3 ΔΟΜΗ ΤΟΥ BLOCKCHAIN

Η πιο βασική δομή του blockchain βρίσκεται μέσα στα μπλοκ του που σχηματίζουν αλυσίδες όταν συνδυάζονται. Κάθε μπλοκ περιέχει μια λίστα συναλλαγών. Ένας κρυπτογραφικός κατακερματισμός συνδέει κάθε επόμενο μπλοκ πίσω στο προηγούμενο δημιουργώντας έτσι μια αμετάβλητη αλυσίδα γνωστή ως blockchain. Αυτή η ρύθμιση προστατεύει την ακεραιότητα και την ασφάλεια των δεδομένων κατά την καταχώρισή τους στο καθολικό [3].

Τα στοιχεία που συνήθως περιλαμβάνονται σε ένα μπλοκ είναι:

1. Κεφαλίδα – Περιέχει μεταδεδομένα όπως αριθμό μπλοκ ή χρονική σήμανση και κρυπτογραφικούς κατακερματισμούς από προηγούμενα μπλοκ.
2. Συναλλαγές – Ένα τμήμα που διατηρεί αρχεία σχετικά με τις μεταφορές που πραγματοποιήθηκαν μεταξύ των συμμετεχόντων κατά τη συγκεκριμένη περίοδο.
3. Nonce – Τυχαίοι αριθμοί που χρησιμοποιούνται σε κρυπτογραφικούς υπολογισμούς κατά την εξόρυξη [4].

Μέσω της αλυσίδας των μπλοκ μαζί κάθε προσπάθεια αλλαγής θα χρειαζόταν αλλαγή όχι μόνο στοχευμένων αλλά και επακόλουθων κατακερματισμών μπλοκ. Αυτό είναι υπολογιστικά μη πρακτικό, επομένως διατηρείται η αμετάβλητη ικανότητα εντός του blockchain[16].

Λειτουργίες κατακερματισμού

Οι πτυχές ασφάλειας και ακεραιότητας του blockchain βασίζονται σε μεγάλο βαθμό σε συναρτήσεις κατακερματισμού που λαμβάνουν εισόδους και, στη συνέχεια, επιστρέφουν συμβολοσειρές byte σταθερού μεγέθους ως έξοδο ή πέψη. Φαίνονται τυχαία αλλά μοναδικά για διαφορετικές εισόδους, ακόμη και με την παραμικρή αλλαγή στην είσοδο, θα πρέπει να υπάρχει σημαντική διαφορά μεταξύ των κατακερματισμών [21].

Μερικοί βασικοί ρόλοι που διαδραματίζουν τα hashes στα blockchain περιλαμβάνουν:

1. Σύνδεση μπλοκ – Οι ασφαλείς αλυσίδες επιτυγχάνονται όταν κάθε μπλοκ διατηρεί τον κατακερματισμό του προηγούμενου.
2. Επαλήθευση συναλλαγών – Η ακεραιότητα της συναλλαγής διασφαλίζεται μέσω κατακερματισμού πριν συμπεριληφθεί σε ένα συγκεκριμένο χρονικό πλαίσιο.
3. Το Proof of Work - Mining χρησιμοποιεί αυτές τις λειτουργίες για να λύσει κρυπτογραφικούς γρίφους [3].
4. Το SHA-256 (χρησιμοποιείται από το Bitcoin) και το Keccak-256 (χρησιμοποιείται από το Ethereum) είναι μεταξύ των συναρτήσεων κατακερματισμού που χρησιμοποιούνται συνήθως σε αυτό το σύστημα.

Κόμβοι & Δίκτυα

Ένας κόμβος αναφέρεται σε κάθε μεμονωμένο υπολογιστή που συμμετέχει στο πρωτόκολλο blockchain σχηματίζοντας αυτό που ονομάζεται δίκτυο. Μπορούν να διακριθούν διαφορετικοί τύποι:

1. Πλήρεις κόμβοι – Αποθήκευση από πλήρη αντίγραφα όλων των μπλοκ και επαλήθευση των συναλλαγών καθώς και εγκυρότητα ολόκληρης της αλυσίδας μπλοκ.

2. Ελαφροί κόμβοι ή απλοποιημένοι κόμβοι επαλήθευσης πληρωμών (SPV) – Αυτοί αποθηκεύουν μόνο ορισμένα μέρη ολόκληρης της αλυσίδας μπλοκ που βασίζονται σε πλήρεις κόμβους για σκοπούς επικύρωσης όταν πρόκειται για συναλλαγές που τους αφορούν [26].
3. Κόμβοι εξόρυξης – Εκτέλεση υπολογιστικής εργασίας που απαιτείται κατά τη διάρκεια της διαδικασίας εξόρυξης, η οποία τελικά οδηγεί σε προσθήκη νέων μπλοκ σε αυτό το κατανεμημένο σύστημα καθολικού, γνωστό ως blockchain.

Μέσω της peer-to-peer επικοινωνίας μεταξύ τους οι κόμβοι σχηματίζουν αποκεντρωμένα δίκτυα όπου δεν υπάρχει αστοχία μεμονωμένου σημείου, διασφαλίζοντας έτσι την ευρωστία σε τέτοια συστήματα [12].

2.4 ΑΛΓΟΡΙΘΜΟΙ ΣΥΜΦΩΝΙΑΣ

Απόδειξη Εργασίας (PoW)

Ο αλγόριθμος συναίνεσης που χρησιμοποιήθηκε από το Bitcoin όταν δημιουργήθηκε ονομάζεται Απόδειξη Εργασίας (PoW). Για να κερδίσουν, οι εξορύκτες πρέπει να συναγωνιστούν μεταξύ τους λύνοντας δύσκολους κρυπτογραφικούς γρίφους. Μόλις ένας εξορύκτης λύσει πρώτα το πρόβλημα, τότε ανταμείβεται με τη δυνατότητα να προσθέσει ένα άλλο μπλοκ στο blockchain. Το επίπεδο δυσκολίας για αυτά τα παζλ προσαρμόζεται κάθε τόσο, προκειμένου να μην γίνονται πολύ εύκολα ή δύσκολα, γεγονός που διασφαλίζει ότι τα μπλοκ προστίθενται συνεχώς [3].
Το PoW παρέχει μια σειρά από οφέλη:

1. Άμυνα: Για την αλλαγή του blockchain, απαιτείται δαπανηρή και χρονοβόρα ποσότητα υπολογιστικής εργασίας.
2. Αποκέντρωση: Η ευρεία διανομή των εξορυκτών ενθαρρύνεται από το PoW, το οποίο βελτιώνει την ασφάλεια του δικτύου.

Ωστόσο, υπάρχουν επίσης ορισμένα σημαντικά μειονεκτήματα στο PoW:

1. Κατανάλωση ενέργειας: Μπορεί να προκύψουν περιβαλλοντικές ανησυχίες καθώς η διαδικασία εξόρυξης χρησιμοποιεί μεγάλες ποσότητες ενέργειας.
2. Κίνδυνοι συγκεντροποίησης: Με την πάροδο του χρόνου η ισχύς της εξόρυξης μπορεί να συγκεντρωθεί σε λίγα χέρια οδηγώντας σε συγκέντρωση [27].

Αποδεικτικά στοιχεία για Ποντάρισμα (PoS)

Τα αποδεικτικά στοιχεία που βασίζονται στο ποντάρισμα ή το Proof of Stake (PoS) είναι ένας άλλος αλγόριθμος συναίνεσης που σχεδιάστηκε για την αντιμετώπιση ορισμένων αναποτελεσματικών στο PoW. Οι επικυρωτές επιλέχθηκαν με βάση τον αριθμό των νομισμάτων που κατέχουν και είναι πρόθυμοι να ποντάρουν ως εγγύηση για τη δημιουργία νέων μπλοκ καθώς και για την επικύρωση συναλλαγών με αυτήν τη μέθοδο. Αν και συνήθως χρησιμοποιούνταν τυχαιοποιημένες διαδικασίες επιλογής, ο πλούτος και το ποντάρισμα αυξάνουν τις πιθανότητες επιλογής [28].

Τα πλεονεκτήματα περιλαμβάνουν:

1. Ενεργειακή απόδοση: Η επικύρωση μπλοκ μειώνει σημαντικά την κατανάλωση ενέργειας με POS.
2. Ασφάλεια: Οι επικυρωτές έχουν οικονομικά συμφέροντα για να διατηρούν τα δίκτυα ασφαλή από επιθέσεις.

Ωστόσο, εξακολουθούν να υπάρχουν προκλήσεις που αντιμετωπίζει το POS:

1. Αρχική διανομή: Ο έλεγχος στα δίκτυα θα μπορούσε να επηρεαστεί από τον τρόπο κατανομής των στοιχημάτων αρχικά.
2. Πολυπλοκότητα: Μερικές φορές μπορεί να απαιτούνται πιο περίπλοκοι από τους μηχανισμούς POW για την εφαρμογή [5]

Άλλοι τρόποι συμφωνίας:

Αρκετοί άλλοι μηχανισμοί έχουν προταθεί προκειμένου να ξεπεραστούν τα μειονεκτήματα που σχετίζονται με POW και POS. όπως:

Εξουσιοδοτημένη απόδειξη συμμετοχής (DPOS): Ένας μικρός αριθμός αντιπροσώπων εκλέγεται από ενδιαφερόμενα μέρη που επικυρώνουν τις συναλλαγές ενώ δημιουργούν νέα μπλοκ, έτσι ώστε να ενισχυθεί η αποτελεσματικότητα και να ελαχιστοποιηθούν οι κίνδυνοι συγκέντρωσης [29].

Πρακτική βυζαντινή ανοχή σφαλμάτων (PBFT): Αυτό το σύστημα εφαρμόζεται όταν αντιμετωπίζουμε επιτρεπόμενες αλυσίδες μπλοκ όπου οι επικυρωτές συμφωνούν για την κατάσταση της αλυσίδας μπλοκ μέσω της πλειοψηφίας, επιτρέποντας έτσι υψηλή απόδοση συναλλαγών και χαμηλή καθυστέρηση [30].
Απόδειξη Εξουσιοδότησης (PoA): Απαιτείται βεβαίωση σε ορισμένους επικυρωτές που πρέπει να ακολουθούν καθορισμένους κανόνες προτού μπορέσουν να συμμετάσχουν σε αυτόν τον μηχανισμό που συνήθως λειτουργεί καλύτερα για ιδιωτικές ή κοινοπραξίες blockchains με ημι-κεντρική εμπιστοσύνη [31].

Κάθε μέθοδος συναίνεσης ποικίλλει ως προς τα μέτρα ασφαλείας που λαμβάνονται, τα επίπεδα αποτελεσματικότητας που επιτυγχάνονται και τον βαθμό αποκέντρωσης που εφαρμόζεται, επομένως τις καθιστά κατάλληλες για διαφορετικούς τύπους εφαρμογών blockchain.

2.5 ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΠΙΒΕΒΑΙΩΣΗ ΣΥΝΑΛΛΑΓΩΝ

Κύκλος Ζωής Συναλλαγών Blockchain

Αυτά είναι τα στάδια που εμπλέκονται σε έναν κύκλο ζωής συναλλαγών σε οποιοδήποτε δεδομένο blockchain:

1. Έναρξη: Ένας χρήστης ξεκινά μια συναλλαγή δημιουργώντας ένα μήνυμα που περιέχει πληροφορίες σχετικά με τον αποστολέα, τον παραλήπτη, το ποσό που αποστέλλεται και την ψηφιακή υπογραφή.
2. Μετάδοση: Η συναλλαγή μεταδίδεται μέσω του δικτύου όπου λαμβάνεται από πολλούς κόμβους.
3. Επικύρωση: Οι κόμβοι επικυρώνουν τις συναλλαγές επαληθεύοντας την αυθεντικότητά τους. έλεγχος εάν υπήρχαν αρκετά κεφάλαια διαθέσιμα για αποστολή καθώς και διασφάλιση ότι όλοι οι κανόνες πρωτοκόλλου έχουν τηρηθεί κατά τη δημιουργία [32].

Εξόρυξη και επικύρωση

Η συμπερίληψη μιας συναλλαγής στο blockchain περιλαμβάνει εξόρυξη και επικύρωση ειδικά σε blockchain που βασίζονται σε PoW, όπως το Bitcoin:

1. Δεξαμενή συναλλαγών: Οι έγκυρες συναλλαγές συγκεντρώνονται σε ένα μέρος που αναφέρεται ως mempool ή επίσης γνωστό ως ομάδα μνήμης.
2. Δημιουργία μπλοκ: Οι εξορύκτες επιλέγουν ορισμένες συναλλαγές από το mempool και στη συνέχεια τις συναρμολογούν σχηματίζοντας νέα μπλοκ.
3. Απόδειξη εργασίας: Οι εξορύκτες λύνουν κρυπτογραφικούς γρίφους μέσω της εκτέλεσης υπολογιστικής εργασίας όπου ανταγωνίζονται μεταξύ τους μέχρι να λύσει κάποιος πρώτος. Δεύτερον, όταν λυθεί το παζλ, μεταδίδεται μέσα στο δίκτυο, ολοκληρώνοντας έτσι τη διαδικασία που ονομάζεται απόδειξη εργασίας.
4. Επαλήθευση : Άλλοι κόμβοι ελέγχουν εάν οι προτεινόμενες λύσεις (που δημοσιεύτηκαν από τον εξορύκτη) είναι σωστές ή όχι, εκτός από την επικύρωση ολόκληρης της δομής μπλοκ συμπεριλαμβανομένου του περιεχομένου του. Εάν κριθεί έγκυρο, προστίθεται στην αλυσίδα διαφορετικά απορρίπτεται [3].

Τα blockchains που βασίζονται σε PoS έχουν ελαφρώς διαφορετικές διαδικασίες:

1. Επιλογή επικυρωτή: Οι επικυρωτές επιλέγονται ανάλογα με το ποσό του κρυπτονομίσματος που διακυβεύονται.
2. Δημιουργία μπλοκ: Ο επικυρωτής που επιλέχθηκε δημιουργεί ένα νέο μπλοκ και το προσθέτει στην αλυσίδα.
3. Βεβαίωση: Άλλοι επικυρωτές επιβεβαιώνουν την εγκυρότητα αυτού του μπλοκ, εάν είναι έγκυρο, προσθέτουν αυτό το μπλοκ στο δικό τους αντίγραφο του blockchain, όπου μετά την προσθήκη κάθε επικυρωτής μπλοκ λαμβάνει ανταμοιβή [28].
4. Η δημιουργία και ο έλεγχος ταυτότητας των συναλλαγών είναι σημαντικές για τη διατήρηση της ασφάλειας του blockchain. Η τεχνολογία Blockchain διασφαλίζει ένα αξιόπιστο και ασφαλές σύστημα καταγραφής για όλες τις συναλλαγές, επαληθεύοντας την εγκυρότητά τους και την κατάλληλη καταγραφή τους.

2.6 ΈΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ - ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

Ορισμός και Χαρακτηριστικά: Ένα έξυπνο συμβόλαιο είναι μια συμφωνία στην οποία οι όροι γράφονται απευθείας σε κώδικα, ώστε να μπορεί να εκτελείται μόνος του και αποθηκεύεται σε blockchain διασφαλίζοντας την επαλήθευση της αμετάβλητης διαφάνειας κατά τη διάρκεια του χρόνου εκτέλεσης. Αυτή η ιδέα εισήχθη για πρώτη φορά από τον Nick Szabo τη δεκαετία του 1990 ως μέρος της ευρύτερης αντίληψής του για τη χρήση πρωτοκόλλων υπολογιστών για τη διευκόλυνση, την επαλήθευση ή την επιβολή διαπραγματευτικών συμβάσεων [33].

Κύρια χαρακτηριστικά των έξυπνων συμβολαίων:

1. Αυτο-εκτέλεση: Οι συμβάσεις μπορούν να εκτελεστούν αυτόματα με έξυπνα συμβόλαια εάν πληρούνται ορισμένες προϋποθέσεις, χωρίς μεσάζοντες.
2. Αμετάβλητο: Οι κωδικοί έξυπνων συμβολαίων δεν μπορούν να τροποποιηθούν μετά την ανάπτυξή τους, διασφαλίζοντας ότι οι συμφωνίες παραμένουν συνεπείς και αξιόπιστες.
3. Διαφάνεια: Οι όροι και η εκτέλεση μιας σύμβασης είναι ορατά σε όλους τους εμπλεκόμενους συμμετέχοντες, ενισχύοντας την εμπιστοσύνη και την υπευθυνότητα.
4. Ασφάλεια: Οι κρυπτογραφικοί μηχανισμοί του blockchain προστατεύουν τα έξυπνα συμβόλαια από παραποίηση ή απάτη [5].
5. Αποτελεσματικότητα: Οι έξυπνες συμβάσεις εξοικονομούν χρόνο και χρήμα στις παραδοσιακές διαδικασίες σύναψης συμβάσεων αυτοματοποιώντας τις [18].

Εφαρμογές σε διαφορετικούς κλάδους

Η ευελιξία και η αποτελεσματικότητα των έξυπνων συμβολαίων τα καθιστούν εφαρμόσιμα σε πολλούς τομείς όπως τα παρακάτω παραδείγματα:

1. Τα έξυπνα συμβόλαια αυτοματοποιούν πολύπλοκες χρηματοοικονομικές συναλλαγές και μειώνουν την ανάγκη για μεσάζοντες σε αυτόν τον τομέα. Για παράδειγμα, μπορούν να διεκπεραιώνουν αυτόματα πληρωμές, να διευκολύνουν εμπορικούς διακανονισμούς και να επεξεργάζονται αιτήσεις ασφαλιστικών αποζημιώσεων. Επιπλέον, οι πλατφόρμες Αποκεντρωμένης Χρηματοδότησης (DeFi) χρησιμοποιούν έξυπνα συμβόλαια για υπηρεσίες όπως ο δανεισμός ή η λήψη δανείων, χωρίς να απαιτείται η μεσολάβηση των παραδοσιακών τραπεζών [22] [30].
2. Η διαφάνεια και η αποτελεσματικότητα στις αλυσίδες εφοδιασμού μπορούν να βελτιωθούν μέσω έξυπνων συμβολαίων που καταγράφουν αμετάβλητα την κίνηση και την προέλευση των αγαθών. Επιπλέον, τα έξυπνα συμβόλαια μπορούν να εκτελούν αυτόματα πληρωμές όταν τα προϊόντα φτάνουν σε συγκεκριμένα σημεία και πληρούν τους συμφωνημένους όρους. Η IBM, για παράδειγμα, έχει συνεργαστεί με τη Maersk και άλλες εταιρείες για την ανάπτυξη λύσεων blockchain που παρακολουθούν και διαχειρίζονται την εφοδιαστική αλυσίδα [8].

3. Ακίνητα: Οι συναλλαγές ακινήτων γίνονται εύκολες με έξυπνες επαφές καθώς αυτοματοποιούν τη διαδικασία μεταβίβασης ιδιοκτησίας καθώς και τις διαδικασίες πληρωμής, επομένως μπορούν επίσης να διαχειριστούν συμφωνίες ενοικίασης παράλληλα με τα αρχεία ακινήτων, αλλά αυτό θα εξαλείψει τους μεσίτες ή τους δικηγόρους, εξορθολογίζοντας έτσι τις συναλλακτικές δραστηριότητες μειώνοντας έτσι το κόστος [11] .
4. Υγειονομική περίθαλψη: Η αποτελεσματικότητα και η ασφάλεια της διαχείρισης δεδομένων υγειονομικής περίθαλψης μπορούν να επιτευχθούν μέσω έξυπνων επαφών που διασφαλίζουν ότι τα αρχεία των ασθενών είναι ακριβή και ενημερωμένα, προσβάσιμα μόνο από εξουσιοδοτημένα άτομα. Βοηθά επίσης στην αυτοματοποίηση της επεξεργασίας ασφαλιστικών απαιτήσεων, ενώ καταγράφει με ασφάλεια και διαφάνεια τα δεδομένα κλινικών δοκιμών [13].
5. Νομική βιομηχανία: Συμφωνίες δικαιωμάτων πνευματικής ιδιοκτησίας διαθήκες, καταπιστεύματα, μεταξύ άλλων, θα μπορούσαν να αυτοματοποιηθούν με τη βοήθεια έξυπνων συμβάσεων, επιταχύνοντας έτσι τον χρόνο εκτέλεσης για νομικά έγγραφα, καθώς παρακάμπτουν τους νομικούς μεσάζοντες [8].
6. Συστήματα ψηφοφορίας: Τα συστήματα ψηφοφορίας μπορούν να επωφεληθούν από έξυπνα συμβόλαια που εγγυώνται την ακριβή καταγραφή της καταμέτρησης των ψήφων, μειώνοντας έτσι τις πιθανότητες για απάτη ή παραποίηση, παρέχοντας έτσι ασφαλή επαληθεύσιμη εκλογική διαδικασία [11].

2.7 Γλώσσες Προγραμματισμού για Έξυπνα Συμβόλαια

Τα έξυπνα συμβόλαια είναι συμβάσεις αυτοεκτελούμενες όπου οι όροι της συμφωνίας εγγράφονται απευθείας σε κώδικα. Λειτουργούν σε πλατφόρμες blockchain και διευκολύνουν ασφαλείς συναλλαγές χωρίς μεσάζοντες, έχουν αναπτυχθεί διάφορες γλώσσες προγραμματισμού για τη δημιουργία έξυπνων συμβολαίων με καθεμία να έχει τα μοναδικά χαρακτηριστικά της, πλεονεκτήματα.

Solidity

Η γλώσσα προγραμματισμού Solidity είναι η πιο διαδεδομένη για τη δημιουργία έξυπνων συμβολαίων στο blockchain του Ethereum. Δημιουργήθηκε ειδικά για να υποστηρίζει την ανάπτυξη έξυπνων συμβολαίων και είναι μια στατικά πληκτρολογημένη γλώσσα, πράγμα που σημαίνει ότι ο τύπος κάθε μεταβλητής καθορίζεται κατά τη διάρκεια της μεταγλώττισης. Παρέχει υποστήριξη για πολύπλοκες δομές δεδομένων, όπως η κληρονομικότητα και οι βιβλιοθήκες, κάνοντάς την ιδιαίτερα ευέλικτη και προσαρμόσιμη σε διάφορες χρήσεις [23].

Βασικά χαρακτηριστικά της γλώσσας Solidity:

1. Προσανατολισμός συμβάσεων: Οι συναρτήσεις είναι ενσωματωμένες στη γλώσσα, επιτρέποντας εύκολη χρήση τους σε συνδυασμό με μεταβλητές κατάστασης ή συμβάντα.
2. Στατική πληκτρολόγηση: Η στατική πληκτρολόγηση βοηθά στον εντοπισμό σφαλμάτων κατά τη μεταγλώττιση, γεγονός που οδηγεί σε καλύτερη αξιοπιστία κώδικα.
3. Κληρονομικότητα: Η υποστήριξη πολλαπλής κληρονομικότητας επιτρέπει στους προγραμματιστές να δημιουργούν πιο σύνθετα συμβόλαια, βασισμένα σε υπάρχοντα.
4. Διαλειτουργικότητα: Οι αποκεντρωμένες εφαρμογές (DApps) συχνά χρειάζεται να αλληλεπιδρούν με άλλες συμβάσεις και εξωτερικές εφαρμογές, και η Solidity το επιτρέπει αυτό μέσω της στιβαρότητας της [34].

Το μεγάλο ποσοστό υιοθέτησης σε συνδυασμό με την εκτενή τεκμηρίωση έχει καταστήσει τη γλώσσα Solidity πρότυπο του κλάδου μεταξύ των προγραμματιστών blockchain παγκοσμίως. Η προσανατολισμένη στη σύμβαση φύση της γλώσσας εξασφαλίζει σαφή οργάνωση του κώδικα, γεγονός που επιτρέπει τη δημιουργία αξιόπιστων και ευκολοσυντήρητων έξυπνων συμβολαίων.

Επιπλέον, η Solidity προσφέρει μια ποικιλία προηγμένων λειτουργιών, όπως τροποποιητές συναρτήσεων, δυνατότητες χειρισμού συμβάντων και χαμηλού επιπέδου λειτουργίες κλήσεων, οι οποίες παρέχουν πλούσιες δυνατότητες για την ανάπτυξη συμβολαίων.

Ωστόσο, οι πρακτικές κωδικοποίησης πρέπει να είναι προσεκτικές λόγω της πολυπλοκότητας της Solidity και των πιθανών ευπαθειών που μπορεί να προκύψουν αν ο κώδικας δεν έχει δοκιμαστεί σωστά. Η λάθος διαχείριση του κώδικα μπορεί να οδηγήσει σε σοβαρά ζητήματα ασφαλείας, καθώς η ευελιξία της γλώσσας είναι ένας από τους λόγους που οδήγησαν στο περίφημο hack του DAO στο παρελθόν. Ωστόσο, είναι σημαντικό να αναφερθεί ότι εργαλεία όπως το Mythril και το Oyente χρησιμοποιούνται συνήθως για την ανίχνευση ευπαθειών στους κώδικες Solidity [35].

Vyper

Η γλώσσα Vyper είναι μια γλώσσα προγραμματισμού που έχει δημιουργηθεί για την ανάπτυξη έξυπνων συμβάσεων στο blockchain Ethereum. Ο κύριος στόχος της είναι να προσφέρει μεγαλύτερη ασφάλεια σε σχέση με τη Solidity, ενώ παραμένει εύκολη στην επιθεώρηση και τον έλεγχο του κώδικα. Είναι μια στατικά δακτυλογραφημένη γλώσσα με έμφαση στην απλότητα και την αναγνωσιμότητα, μειώνοντας έτσι τους πιθανούς κινδύνους ασφαλείας [5].

Κύρια χαρακτηριστικά της γλώσσας Vyper:

1. Ευκολία: Σύμφωνα με τους Luu et al (2016), η γλώσσα έχει απλή σύνταξη και minimal σχεδιασμό που δεν έχει πολλές πιθανότητες για λάθη.
2. Ασφάλεια: Η Vyper έχει κατασκευαστεί με ασφάλεια με διάφορα χαρακτηριστικά που μειώνουν τους φορείς επίθεσης ενώ αποτρέπουν κοινές ευπάθειες.
3. Κατανοησιμότητα: Αυτή η γλώσσα προγραμματισμού που εστιάζει στην αναγνωσιμότητα καθιστά τον κώδικα πιο ευανάγνωστο και κατανοητό και για άτομα που εμπλέκονται στον έλεγχό του.

Για όσους ενδιαφέρονται για την ασφάλεια και την απλότητα στα συστήματά τους, αυτό είναι πολύ σημαντικό. Ο κίνδυνος σφαλμάτων μπορεί να μειωθεί με την υιοθέτηση μιας μινιμαλιστικής προσέγγισης όσον αφορά την ασφάλεια στα έξυπνα συμβόλαια, επειδή τα βοηθά να γίνονται ευκολότερα στον έλεγχο καθώς και στη διατήρησή τους με την πάροδο του χρόνου. Τα τρωτά σημεία συχνά προκύπτουν όταν χρησιμοποιούνται συγκεκριμένες συναρτήσεις, όπως τροποποιητές ή δηλώσεις συναρμολόγησης ενσωματωμένων. Γι' αυτό, η Solidity δεν τις περιλαμβάνει, κάνοντάς την λιγότερο ασφαλή από τη Vyper, η οποία είναι πιο περιορισμένη αλλά ασφαλέστερη.

Ωστόσο, η τεκμηρίωση για σύνθετες εφαρμογές είναι περιορισμένη λόγω της παρουσίας λιγότερων χαρακτηριστικών σε σύγκριση με τη σταθερότητα, γεγονός που μπορεί να περιορίσει τη χρήση πέρα από τις απλές συμβάσεις όπου η ασφάλεια είναι βασική θεωρείται αρκετά καλή από τους προγραμματιστές που κατασκευάζουν πολύ περίπλοκες ή πλούσιες σε χαρακτηριστικά DApps.

Άλλες γλώσσες για έξυπνα συμβόλαια

Υπάρχουν πολλές γλώσσες που μπορούν να χρησιμοποιηθούν για τη σύνταξη προγραμμάτων έξυπνων συμβολαίων εκτός από τη Vyper, όπως οι παρακάτω:

1. Chaincode: Γράφεται είτε σε Go είτε σε JavaScript. Το Chaincode επιτρέπει την ευέλικτη και αποτελεσματική ανάπτυξη προσαρμοσμένων εφαρμογών για τις ανάγκες των επιχειρήσεων στην πλατφόρμα Hyperledger Fabric.
2. Michelson: Σχεδιάστηκε ειδικά για να επιτρέπει την επίσημη επαλήθευση των έξυπνων συμβολαίων στο blockchain της Tezos, διασφαλίζοντας ότι εκτελούνται σύμφωνα με τις επιδιωκόμενες συμπεριφορές. Η απλότητά του το καθιστά ιδανικό για εφαρμογές που απαιτούν υψηλή ασφάλεια (Goodman, 2014).
3. Η γλώσσα προγραμματισμού Plutus: Βασίζεται στη γλώσσα Haskell και χρησιμοποιείται για τη σύνταξη έξυπνων συμβολαίων με επίκεντρο την ασφαλή ορθότητα. Το έργο

blockchain Cardano αξιοποιεί επίσης τους ισχυρούς τύπους εγγυήσεων ασφάλειας της Haskell, όταν είναι απαραίτητο (IOHK, 2017).

4. Scilla: Είναι μια γλώσσα προγραμματισμού μεσαίου επιπέδου για έξυπνα συμβόλαια που σχεδιάστηκε για το blockchain Zilliqa. Δίνει έμφαση στην ασφάλεια μέσω επίσημων μεθόδων επαλήθευσης. Η φύση του ενδιάμεσου επιπέδου της Scilla διασφαλίζει τόσο υψηλότερους τύπους προγραμματισμού όσο και καλύτερη προστασία των συμβολαίων από κοινές ευπάθειες (Sergey et al., 2018).

Κάθε γλώσσα έχει σχεδιαστεί λαμβάνοντας υπόψη διαφορετικές απαιτήσεις αναγκών σε διάφορες πλατφόρμες όπου εκτελούνται, παρέχοντας έτσι επιλογές για προγραμματιστές ανάλογα με τις δυνατότητες της πλατφόρμας.

Σύγκριση μεταξύ γλωσσών

Η επιλογή μιας γλώσσας προγραμματισμού που θα χρησιμοποιηθεί για την ανάπτυξη έξυπνων συμβολαίων εξαρτάται από διάφορους παράγοντες, όπως οι ιδιαιτερότητες του έργου, τα επίπεδα ασφάλειας που απαιτούνται για την πολυπλοκότητα.

• Solidity: Πρόκειται για μια ευέλικτη και ευρέως υποστηριζόμενη γλώσσα προγραμματισμού με πλούσια τεκμηρίωση και ενεργή υποστήριξη από την κοινότητα. Είναι ιδανική για τη δημιουργία πολύπλοκων ή πλούσιων σε χαρακτηριστικά DApps που εκτελούνται στο Ethereum.

• Vyper: Ενδείκνυται για περιπτώσεις όπου η απλότητα είναι προτεραιότητα, προκειμένου να διασφαλιστεί η ασφάλεια κατά την εκτέλεση του κώδικα. Μειώνει τις πιθανές αδυναμίες και ενισχύει την ασφάλεια του συστήματος συνολικά.

• Chaincode: Υποστηρίζει πολλαπλές γλώσσες προγραμματισμού, καθιστώντας το κατάλληλο για επιχειρήσεις που χρησιμοποιούν Hyperledger Fabric και απαιτούν ευελιξία με mainstream γλώσσες όπως η Java και η Go.

• Michelson: Είναι η καταλληλότερη γλώσσα για εφαρμογές που απαιτούν επίσημη επαλήθευση, προκειμένου να διασφαλιστεί η ορθότητα. Η αποτυχία στην επαλήθευση μπορεί να οδηγήσει σε σοβαρές συνέπειες. Οι εφαρμογές που απαιτούν υψηλή αξιοπιστία μπορούν να αναπτυχθούν εύκολα με αυτήν τη γλώσσα, καθώς επιτρέπει τη συγγραφή κώδικα που μπορεί να ελεγχθεί προκειμένου να διασφαλιστεί η σωστή λειτουργία του.

• Scilla: Αναπτύχθηκε για το blockchain Zilliqa και δίνει προτεραιότητα στην ασφάλεια μέσω επίσημων μεθόδων επαλήθευσης, καθιστώντας την ανθεκτική σε κοινές ευπάθειες.

Συνοψίζοντας τα έξυπνα συμβόλαια αποτελούν σημαντική ανακάλυψη στην εκτέλεση και επιβολή των συμφωνιών. Έχουν υιοθετηθεί σε διάφορους κλάδους λόγω της ικανότητάς τους να αυτοματοποιούν τις διαδικασίες, να διασφαλίζουν τη διαφάνεια και να παρέχουν ασφάλεια. Η Solidity και η Vyper είναι γλώσσες προγραμματισμού που χρησιμοποιούνται για την ανάπτυξη αυτών των έξυπνων συμβάσεων το καθένα με τα δικά του μοναδικά χαρακτηριστικά και πλεονεκτήματα.

Η Solidity εξακολουθεί να είναι η πιο δημοφιλής επιλογή λόγω της ευελιξίας του και της ευρείας βάσης υποστήριξης, αλλά θα πρέπει να κωδικοποιηθεί προσεκτικά λόγω της πολυπλοκότητάς της που απαιτεί ελέγχους ασφαλείας. Για έργα όπου η απλότητα και η ασφάλεια είναι βασικές ανησυχίες, η Vyper προσφέρει μια πιο ασφαλή επιλογή που μπορεί επίσης να διαβαστεί εύκολα. Τα Chaincode, Michelson, Plutus, μεταξύ άλλων, εξυπηρετούν συγκεκριμένες πλατφόρμες blockchain φέρνοντας μαζί τους διαφορετικά πλεονεκτήματα.

Καθώς η τεχνολογία blockchain συνεχίζει να εξελίσσεται παράλληλα με τα έξυπνα συμβόλαια, θα πρέπει να περιμένουμε περισσότερες εξελίξεις καθώς και νέες περιπτώσεις χρήσης. Οι προγραμματιστές πρέπει να καταλάβουν τι μπορούν να κάνουν καλύτερα αυτές οι γλώσσες προγραμματισμού, ενώ παράλληλα γνωρίζουν τους περιορισμούς τους, ώστε να μπορούν να

επιλέξουν το κατάλληλο εργαλείο για τη δουλειά, ενισχύοντας έτσι την καινοτομία σε όλους τους τομείς μέσω της υιοθέτησής τους.

2.8 Ασφάλεια και προκλήσεις σε Blockchain και έξυπνα συμβόλαια

Κοινά τρωτά σημεία

Τα δίκτυα blockchain προσφέρουν εξαιρετικά χαρακτηριστικά ασφαλείας καθώς και διαφάνεια, αν και αυτό δεν σημαίνει ότι δεν έχουν και αδυναμίες. Η γνώση τέτοιων κοινών τρωτών σημείων είναι σημαντική κατά τον σχεδιασμό μέτρων εναντίον τους.

- Επίθεση 51%: Η επίθεση 51% είναι ένα από τα πιο διάσημα τρωτά σημεία στα δίκτυα blockchain όπου ένα άτομο ή ομάδα αναλαμβάνει τον έλεγχο πάνω από το ήμισυ της ισχύος εξόρυξης, με αποτέλεσμα να μπορεί να χειριστεί ολόκληρη την αλυσίδα. Μπορούν να αντιστρέψουν τις συναλλαγές, να διπλασιάσουν τα νομίσματα ή ακόμα και να σταματήσουν την επιβεβαίωση νέων, γεγονός που υπονομεύει σε μεγάλο βαθμό την ακεραιότητα καθώς και την εμπιστοσύνη εντός του συστήματος (Nakamoto, 2008).
- Σφάλματα και ευπάθειες έξυπνων συμβολαίων: Τα έξυπνα συμβόλαια είναι ασφαλή μόνο υπό την προϋπόθεση ότι έχουν συνταχθεί με χρήση ασφαλών κωδικών. Σφάλματα ή άλλα είδη αδυναμιών που εντοπίζονται σε αυτούς τους κωδικούς μπορεί να οδηγήσουν σε σημαντικές παραβιάσεις ασφάλειας. Για παράδειγμα, το έξυπνο συμβόλαιο Ethereum που χρησιμοποιήθηκε στο DAO αξιοποιήθηκε κατά τη διάρκεια 201$ προκαλώντας ζημιές σε αιθέρες αξίας περίπου εξήντα εκατομμυρίων δολαρίων [35].
- Επιθέσεις επανάληψης: Μια επίθεση επανάληψης συμβαίνει όταν μια συναλλαγή αναμεταδίδεται δόλια ή κακόβουλα. Αυτό γίνεται πιο δύσκολο σε συστήματα όπου η ίδια συναλλαγή θα μπορούσε να ισχύει σε διαφορετικές αλυσίδες μπλοκ [36].
- Επιθέσεις Sybil: Σε αυτόν τον τύπο επίθεσης, ένας αντίπαλος δημιουργεί πολυάριθμες πλαστές ταυτότητες έτσι ώστε να αποκτήσει τον έλεγχο του δικτύου ή να παρεμβαίνει στην κανονική λειτουργία του [37].
- Phishing and Social Engineering: Οι χρήστες blockchain και έξυπνων συμβολαίων μπορεί να πέσουν θύματα διαφόρων επιθέσεων phishing καθώς και κοινωνικής μηχανικής όπως κάθε άλλο ψηφιακό σύστημα. Τέτοιες επιθέσεις ξεγελούν τα άτομα ώστε να δώσουν ιδιωτικά κλειδιά, θέτοντας σε κίνδυνο την ασφάλειά τους.
- Τρωτά σημεία του μηχανισμού συναίνεσης: Διαφορετικοί μηχανισμοί συναίνεσης έχουν τα μοναδικά τρωτά σημεία τους. Για παράδειγμα, η Απόδειξη Εργασίας (PoW) καταναλώνει πολλή ενέργεια που δεν είναι φιλική προς το περιβάλλον και μπορεί να οδηγήσει σε συγκεντρωτισμό, ενώ τίποτα δεν διακυβεύεται προβλήματα κατά την αρχική κατανομή πλούτου που σχετίζεται με την Απόδειξη Πονταρίσματος (PoS) [33].

Στρατηγικές Μετριασμού

Για την αντιμετώπιση της ευαισθησίας του blockchain και των έξυπνων συμβολαίων, απαιτείται μια πολύπλευρη προσέγγιση. Αυτό συνεπάγεται τεχνικές λύσεις καθώς και βέλτιστες πρακτικές.

1. Ενισχυμένα πρωτόκολλα ασφαλείας: Προκειμένου να αποφευχθούν επιθέσεις κατά 51%, θα μπορούσαν να εφαρμοστούν βελτιωμένα πρωτόκολλα ασφαλείας, όπως διαφοροποιημένα πισίνες εξόρυξης που θα κατανείμουν την ισχύ κατακερματισμού πιο ομοιόμορφα στο δίκτυο, καθιστώντας δύσκολο για οποιοδήποτε μέρος να αποκτήσει τον έλεγχο [38].
2. Έξυπνοι έλεγχοι συμβάσεων και επίσημη επαλήθευση: Θα πρέπει να διενεργούνται τακτικοί έλεγχοι στα έξυπνα συμβόλαια και να εφαρμόζεται επίσημη επαλήθευση όποτε

είναι δυνατόν, καθώς αυτά τα δύο μέτρα μειώνουν σημαντικά τα σφάλματα ή τις ευπάθειες. Το Oyente και το Mythril είναι μερικά εργαλεία που θα μπορούσαν να ελέγξουν για πιθανά ζητήματα σε έναν κώδικα έξυπνης σύμβασης πριν από την ανάπτυξη. Η επίσημη επαλήθευση χρησιμοποιεί μαθηματικές αποδείξεις για να διασφαλίσει ότι τα έξυπνα συμβόλαια συμπεριφέρονται όπως προβλέπεται, εξαλείφοντας έτσι πολλά πιθανά σημεία αδυναμίας [39].

3. Προστασία επανάληψης: Αυτό περιλαμβάνει τη δημιουργία μηχανισμών έτσι ώστε οι συναλλαγές που πραγματοποιούνται σε ένα blockchain να μην μπορούν να ισχύουν σε άλλο. Ένας τρόπος για να επιτευχθεί αυτό είναι να συμπεριλάβετε μοναδικά αναγνωριστικά αλυσίδας στις συναλλαγές που θα βοηθήσουν στην αποφυγή επιθέσεων επανάληψης [40].
4. Μετριασμός επίθεσης Sybil: Τα δίκτυα blockchain μπορούν να καταστήσουν πιο δύσκολο για τους εισβολείς που θέλουν να δημιουργήσουν πολλαπλές πλαστές ταυτότητες μέσω της εφαρμογής επαλήθευσης ταυτότητας μαζί με συστήματα φήμης, αντιμετωπίζοντας έτσι τις επιθέσεις sybil. Η απόδειξη ταυτότητας και η χρήση αποκεντρωμένων λύσεων ταυτότητας είναι μερικές τεχνικές που μπορεί να λειτουργήσουν αποτελεσματικά [41].
5. Εκπαίδευση και ευαισθητοποίηση χρηστών: Είναι σημαντικό να εκπαιδεύονται οι χρήστες σχετικά με επιθέσεις κοινωνικής μηχανικής, όπως απάτες ηλεκτρονικού ψαρέματος, οι οποίες χρησιμοποιούνται συχνά εναντίον τους και σε αυτόν τον τομέα. Πρέπει να γνωρίζουν πώς μπορούν να προστατευθούν καλύτερα από τέτοιες απειλές, συμπεριλαμβανομένης της διδασκαλίας σχετικά με τρόπους διαφοροποίησης των γνήσιων ιστοσελίδων από κακόβουλους, καθώς και τον ασφαλή χειρισμό των ιδιωτικών κλειδιών μεταξύ άλλων [40].
6. Βελτιώσεις του μηχανισμού συναίνεσης: Θα πρέπει να υπάρχει συνεχής έρευνα για την ανάπτυξη μηχανισμών συναίνεσης, καθώς μπορούν να βοηθήσουν στην αντιμετώπιση εγγενών τρωτών σημείων. Για παράδειγμα, τα υβριδικά μοντέλα συναίνεσης που συνδυάζουν πτυχές του PoW και του PoS είναι ικανά να εξισορροπούν την ασφάλεια έναντι της αποτελεσματικότητας. Το Delegated Proof of Stake (DPoS) και το Practical Byzantine Fault Tolerance (PBFT) είναι πρωτόκολλα που προσφέρουν εναλλακτικές λύσεις στους παραδοσιακούς μηχανισμούς συναίνεσης και στη διαδικασία μετριάζουν ορισμένα από τα μειονεκτήματά τους [14] [19].
7. Τακτικές ενημερώσεις και διαχείριση ενημερώσεων κώδικα: Η συνεχής ενημέρωση πλατφορμών blockchain καθώς και έξυπνων συμβολαίων με τρέχουσες ενημερώσεις κώδικα ασφαλείας είναι ένας τρόπος με τον οποίο μπορούν να αντιμετωπιστούν γνωστές αδυναμίες. Αυτό συνεπάγεται την υιοθέτηση μιας ενεργούς στάσης απέναντι στη διαχείριση ευπάθειας σε συνδυασμό με ταχεία απόκριση κάθε φορά που εντοπίζεται οποιοδήποτε τέτοιο ελάττωμα [42].
8. Πορτοφόλια πολλαπλών υπογραφών: Η ενίσχυση της ασφάλειας μπορεί να επιτευχθεί απαιτώντας την έγκριση πολλών μερών πριν από την εκτέλεση μιας συναλλαγής μέσω πορτοφολιών πολλαπλών υπογραφών, εξαλείφοντας έτσι μεμονωμένα σημεία αποτυχίας ενώ ταυτόχρονα παρέχουν πρόσθετα επίπεδα για την προστασία των μεταφορών [43].
9. Πρότυπα ασφαλείας και βέλτιστες πρακτικές: Για τον μετριασμό των κινδύνων που σχετίζονται με την ανάπτυξη blockchain, θα βοηθούσε στη θέσπιση προτύπων ασφαλείας εκτός από την τήρησή τους σε διάφορες διαδικασίες που εμπλέκονται. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) μεταξύ άλλων οργανισμών έχει δημοσιεύσει οδηγίες σχετικά με τον τρόπο με τον οποίο οι προγραμματιστές ή οι επιχειρήσεις μπορούν να ασφαλίσουν τις εφαρμογές τους σε αυτόν τον τομέα [44].
10. Decentralized Oracles: Σε περίπτωση που ένα έξυπνο συμβόλαιο βασίζεται σε εξωτερικές πηγές δεδομένων, τότε θα πρέπει να χρησιμοποιούνται αποκεντρωμένοι

χρησμοί, ώστε να αποφευχθεί η ύπαρξη μεμονωμένων σημείων αστοχίας, καθώς επαληθεύουν την αξιοπιστία και διασφαλίζουν την ακεραιότητα κατά την ασφαλή εισαγωγή τέτοιου είδους πληροφοριών σε αυτά τα συμβόλαια Το Chainlink είναι ένα παράδειγμα όπου τα έργα παρέχουν αποκεντρωμένα δίκτυα μαντείου για την τροφοδοσία εξωτερικών δεδομένων σε έξυπνες συμβάσεις [45].

Συνοψίζοντας, αν και υπάρχουν πολλά πλεονεκτήματα της τεχνολογίας blockchain και των έξυπνων συμβάσεων, έχουν επίσης ορισμένα ζητήματα ασφάλειας. Η διόρθωση αυτών των αδυναμιών χρειάζεται μια ολιστική στρατηγική που περιλαμβάνει τεχνολογικές λύσεις, εκπαίδευση των χρηστών και τήρηση προτύπων. Η διασφάλιση ότι τα συστήματα blockchain παραμένουν αξιόπιστα και ασφαλή μπορεί να επιτευχθεί μέσω ισχυρών ελέγχων ασφαλείας που ενημερώνονται για την αντιμετώπιση νέων κινδύνων καθώς έρχονται.

Κεφάλαιο 3: Επισκόπηση Έρευνας

3.1 ΕΦΑΡΜΟΓΗ BLOCKCHAIN & SMART CONTRACTS ΣΕ ΕΠΙΧΕΙΡΗΣΕΙΣ

Πιθανά οφέλη για τις επιχειρήσεις

Η τεχνολογία blockchain και τα έξυπνα συμβόλαια παρέχουν πολλά πλεονεκτήματα για τις επιχειρήσεις σε διάφορους κλάδους. Αυτές οι τεχνολογίες βελτιώνουν την αποτελεσματικότητα, τη διαφάνεια, την ασφάλεια, καθώς και μειώνουν το κόστος που είναι εγγενές στις παραδοσιακές επιχειρηματικές διαδικασίες.

1. Αποδοτικότητα και μείωση κόστους: Το Blockchain επιτρέπει άμεσες συναλλαγές peer-to-peer, εξαλείφοντας έτσι τους μεσάζοντες που καταναλώνουν χρόνο και χρήμα κατά την επεξεργασία των συναλλαγών. Για παράδειγμα, οι Tapscott & Tapscott (2016) υποστηρίζουν ότι οι διασυνοριακές πληρωμές μπορούν να εξορθολογιστούν στο πλαίσιο των χρηματοοικονομικών υπηρεσιών μέσω blockchain που μειώνει τον χρόνο διακανονισμού από ημέρες σε λεπτά. Η εκτέλεση της σύμβασης μπορεί να αυτοματοποιηθεί με έξυπνα συμβόλαια, μειώνοντας έτσι τις ανάγκες χειροκίνητης παρέμβασης μαζί με τα σχετικά έξοδα.
2. Διαφάνεια και Εμπιστοσύνη: Όλοι οι συμμετέχοντες μοιράζονται τα ίδια αμετάβλητα δεδομένα σε ένα αποκεντρωμένο σύστημα καθολικού, όπως η αλυσίδα των μπλοκ. Αυτό ενθαρρύνει την εμπιστοσύνη μεταξύ τους, επειδή κανείς δεν μπορεί να αλλάξει τα αρχεία χωρίς να το προσέξουν οι άλλοι [8]. Στη διαχείριση της εφοδιαστικής αλυσίδας για παράδειγμα, οι ενδιαφερόμενοι μπορούν να εντοπίσουν από πού προέρχονται τα αγαθά μέχρι την τρέχουσα θέση τους, διασφαλίζοντας έτσι τη γνησιότητα, ελαχιστοποιώντας παράλληλα τους κινδύνους απάτης.
3. Βελτίωση Ασφάλειας: Η ασφάλεια των δεδομένων ενισχύεται με τη χρήση κρυπτογραφικού αλγορίθμου σε blockchains όπου κάθε συναλλαγή καταγράφεται σε μπλοκ που προστίθενται σε αλυσίδες που αποτελούνται από προηγούμενες συναλλαγές. οποιαδήποτε αλλαγή θα απαιτούσε συναίνεση σε όλο το δίκτυο καθιστώντας σχεδόν αδύνατη την παραβίαση των πληροφοριών που αποθηκεύονται με αυτόν τον τρόπο [4].
4. Αξιοπιστία αυτοματισμού: Τα έξυπνα συμβόλαια εκτελούνται αυτόματα όταν πληρούνται οι καθορισμένες προϋποθέσεις, μειώνοντας παράλληλα την πιθανότητα ανθρώπινου λάθους, αυξάνοντας παράλληλα τον παράγοντα αξιοπιστίας, καθώς δεν μπορούν να αποτύχουν μόλις ενεργοποιηθούν, ακόμη κι αν ορισμένα γεγονότα αποτύχουν να συμβούν εντός δεδομένου χρονικού πλαισίου [18].
5. Κανονιστική συμμόρφωση: Η συμμόρφωση μπορεί να απλοποιηθεί μέσω μιας σαφούς διαδρομής ελέγχου που παρέχεται από το διαφανές αμετάβλητο καθολικό του blockchain, το οποίο καθιστά εύκολο για οποιονδήποτε να δει τι συνέβη ανά πάσα στιγμή, συμβάλλοντας έτσι στην τήρηση των αυστηρών κανονισμών που τους επιβάλλονται από τις αρχές σε περιπτώσεις όπως τα οικονομικά ή η υγειονομική περίθαλψη [46].

ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΕΡΙΠΤΩΣΕΩΝ

1. Οικονομικά - Διασυνοριακές πληρωμές: Το Ripple είναι ένα πρωτόκολλο πληρωμών με τεχνολογία blockchain που επιτρέπει γρήγορες φθηνές διεθνείς μεταφορές χρημάτων. Οι παραδοσιακές διασυνοριακές πληρωμές χρειάζονται πολύ χρόνο και περιλαμβάνουν πολλούς μεσάζοντες, αυξάνοντας έτσι το κόστος. Ωστόσο, με την τεχνολογία κυματισμών, οι ταχύτητες συναλλαγών μειώνονται σε

λίγα δευτερόλεπτα, ενώ παράλληλα μειώνονται τα έξοδα μέσω της εξάλειψης των διαμεσολαβητών [47].

2. Supply Chain Management – Προέλευση: Η IBM και η Maersk ανέπτυξαν το TradeLens. μια πλατφόρμα εφοδιαστικής αλυσίδας που βασίζεται στην τεχνολογία blockchain. Το σύστημα παρέχει προβολή σε πραγματικό χρόνο στις αποστολές για όλα τα μέρη που εμπλέκονται στην αλυσίδα εφοδιασμού, ενισχύοντας έτσι την αποτελεσματικότητα καθώς και την εμπιστοσύνη μεταξύ των συμμετεχόντων μειώνοντας τις καθυστερήσεις που σχετίζονται με τη γραφειοκρατία [44].
3. Υγειονομική περίθαλψη – Διαχείριση δεδομένων ασθενών: Το MedRec είναι ένα σύστημα διαχείρισης EMR που έχει δημιουργηθεί με χρήση blockchains. Εξασφαλίζει τον έλεγχο των ασθενών στα αρχεία υγείας τους, ενώ επιτρέπει στους εξουσιοδοτημένους παρόχους υγειονομικής περίθαλψης να έχουν ασφαλή πρόσβαση σε αυτά. Αυτό προάγει την καλύτερη ανταλλαγή πληροφοριών που οδηγεί σε βελτιωμένο συντονισμό φροντίδας [42].
4. Ασφάλιση – Αυτοματοποιημένη Επεξεργασία Απαιτήσεων: Η AXA κυκλοφόρησε το Fizzy, το οποίο είναι προϊόν ασφάλισης καθυστέρησης πτήσης που λειτουργεί χρησιμοποιώντας έξυπνα συμβόλαια πάνω από την υποδομή δικτύου blockchain. Σε περίπτωση που μια πτήση καθυστερήσει πέραν των δύο ωρών, το αερόθερμο ενεργοποιεί αυτόματα την πληρωμή αποζημίωσης στον αντισυμβαλλόμενο, εξαλείφοντας έτσι την ανάγκη συμπλήρωσης εντύπων αξιώσεων από τους πελάτες μαζί με μείωση του χρόνου διεκπεραίωσης.
5. Real Estate – Συναλλαγές ακινήτων: Το Propy χρησιμεύει ως παγκόσμια πλατφόρμα ακίνητης περιουσίας που υποστηρίζεται από blockchain που εξορθολογίζει τις συμφωνίες ακινήτων μέσω της αυτοματοποίησης, παρέχοντας παράλληλα σαφή αρχεία ιστορικού ιδιοκτησίας. Οι αγοραστές πωλητές μπορούν να ολοκληρώσουν τις συναλλαγές τους πιο γρήγορα με ασφάλεια χωρίς να εμπλέκονται άσκοπα μεσίτες ή δικηγόροι [48].

3.2 ΕΠΙΣΚΟΠΗΣΗ ΕΡΕΥΝΑΣ

Πεδίο εφαρμογής και Μεθοδολογία

Αυτή η μελέτη επιδιώκει να εξετάσει πώς η τεχνολογία blockchain καθώς και τα έξυπνα συμβόλαια μπορούν να μεταμορφώσουν διάφορες επιχειρηματικές διαδικασίες. Από αυτή την άποψη, θα εξετάσουμε τα βασικά του blockchain, τις εφαρμογές του σε διάφορους τομείς και τα πλεονεκτήματα ή τα μειονεκτήματα που συνεπάγεται η υιοθέτησή του.

Στόχοι της έρευνας:

1. Να κατανοήσουμε τα βασικά συστατικά μιας αλυσίδας μπλοκ και των έξυπνων συμβολαίων.
2. Να εξετάσουμε τα πιθανά οφέλη από τη χρήση blockchain για τις επιχειρήσεις.
3. Να παραθέσουμε παραδείγματα εφαρμογής των αλυσίδων μπλοκ σε διάφορους τομείς.
4. Να αναδείξουμε τις δυσκολίες που μπορεί να αντιμετωπίσουν οι εταιρείες κατά την εφαρμογή αυτής της τεχνολογίας στις δραστηριότητές τους.

Μεθοδολογία:

1. Ανασκόπηση Βιβλιογραφίας: Στην ανασκόπηση θα εξεταστούν διάφορες βιβλιογραφικές πηγές, όπως ερευνητικά και ακαδημαϊκά άρθρα από ειδικούς στους τομείς της κατανεμημένης λογιστικής και των αποκεντρωμένων συστημάτων, όπως το Bitcoin και άλλα κρυπτονομίσματα. Θα συμπεριληφθούν επίσης λευκές βίβλοι από οργανισμούς που ασχολούνται με την αποκέντρωση, εκθέσεις από συμβουλευτικές εταιρείες που ειδικεύονται σε συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS), βιβλία που αναλύουν συστήματα διαχείρισης ψηφιακής ταυτότητας (DIMS), όπως το Sovrin, καθώς

και μελέτες περιπτώσεων που καταγράφουν επιτυχημένες εφαρμογές αυτής της τεχνολογίας. Αυτές οι πηγές θα αξιολογηθούν προσεκτικά για να καλυφθούν όλες οι σημαντικές πτυχές, με στόχο να εξεταστούν οι δυνατότητες εφαρμογής της τεχνολογίας blockchain στην ενίσχυση της διαφάνειας στις εφοδιαστικές αλυσίδες, συμβάλλοντας παράλληλα στην επίτευξη των Στόχων Βιώσιμης Ανάπτυξης της Ατζέντας 2030 του ΟΗΕ, όπως η εξάλειψη της φτώχειας και η προώθηση της οικονομικής ανάπτυξης.

2. Ανάλυση Μελέτης Περίπτωσης: Σε αυτή τη φάση, θα αναλυθούν συγκεκριμένα παραδείγματα όπου οι αλυσίδες μπλοκ έχουν εφαρμοστεί με επιτυχία. Θα εξεταστούν τα βήματα που ακολουθήθηκαν κατά την εφαρμογή τους, τα οφέλη που προέκυψαν, καθώς και οι προκλήσεις που αντιμετωπίστηκαν κατά την υιοθέτησή τους.
3. Συνεντεύξεις και Έρευνες: Θα πραγματοποιηθούν συνεντεύξεις με ειδικούς του κλάδου, προγραμματιστές blockchain και ηγέτες επιχειρήσεων για να συγκεντρωθούν πληροφορίες σχετικά με τον τρόπο υιοθέτησης των αλυσίδων μπλοκ, τα πλεονεκτήματα και τα μειονεκτήματα που συνδέονται με αυτές, καθώς και τις πρακτικές που ακολουθούνται.
4. Ανάλυση Δεδομένων: Θα χρησιμοποιηθούν δεδομένα από διάφορες πηγές για την ανάλυση τάσεων και σχέσεων που θα βοηθήσουν στην κατανόηση των επιπτώσεων της εισαγωγής της τεχνολογίας blockchain στις διαδικασίες των οργανισμών παγκοσμίως. Η ανάλυση αυτή θα εξετάσει επίσης πώς συνδέεται με την επίτευξη των Στόχων Βιώσιμης Ανάπτυξης (ΣΒΑ) στην Ατζέντα 2030 του ΟΗΕ.

Κύρια ευρήματα

1. Βελτιωμένη λειτουργική αποτελεσματικότητα: Η μελέτη ανακάλυψε ότι η τεχνολογία blockchain βελτιώνει σημαντικά τη λειτουργική αποτελεσματικότητα μέσω της απλοποίησης των διαδικασιών και της αποκοπής των ενδιάμεσων. Για παράδειγμα, στα χρηματοοικονομικά, μειώνει τους χρόνους διακανονισμού και το κόστος συναλλαγής, επιτρέποντας έτσι ταχύτερες και φθηνότερες διασυνοριακές πληρωμές [16]
2. Αύξηση διαφάνειας καθώς και δημιουργία εμπιστοσύνης: Η εμπιστοσύνη μεταξύ των συμμετεχόντων ενισχύεται από ένα διαφανές αμετάβλητο λογιστικό σύστημα που παρέχεται από blockchains, το οποίο παρέχει ένα αρχείο συναλλαγών που μπορούν να επαληθευτούν. Βοηθά επίσης στη διαχείριση της εφοδιαστικής αλυσίδας όπου η διαφάνεια βοηθά στην παρακολούθηση της προέλευσης και της διαδρομής των προϊόντων, μειώνοντας έτσι τις απάτες και διασφαλίζοντας την αυθεντικότητα [13].
3. Καλύτερη ασφάλεια και ακεραιότητα δεδομένων: Σύμφωνα με αυτό το ερευνητικό έγγραφο, ένα από τα κύρια οφέλη που προκύπτουν από τα δίκτυα blockchain είναι η ικανότητά τους να προστατεύουν από παραβιάσεις ή μη εξουσιοδοτημένη πρόσβαση μέσω κρυπτογραφικών μηχανισμών ασφάλειας. Αυτό είναι ιδιαίτερα σημαντικό για τομείς όπως η υγειονομική περίθαλψη ή η χρηματοδότηση όπου η ακεραιότητα των πληροφοριών είναι κρίσιμης σημασίας [17].
4. Αυτοματοποίηση μέσω έξυπνων συμβολαίων: Πρόκειται για αυτοεκτελούμενες συμφωνίες με όρους γραμμένους σε γραμμές κώδικα που ενεργοποιούνται μόλις πληρούνται ορισμένες προκαθορισμένες προϋποθέσεις, αυτοματοποιώντας έτσι τις διαδικασίες χωρίς να απαιτείται ανθρώπινη παρέμβαση τις περισσότερες φορές. Αυτό το είδος διευθέτησης ενισχύει την αξιοπιστία, ενώ ταυτόχρονα μειώνει τις πιθανότητες για σφάλματα που προκύπτουν λόγω της άμεσης εμπλοκής των ανθρώπων. Για παράδειγμα στον ασφαλιστικό κλάδο. Η επεξεργασία των αξιώσεων μπορεί να αυτοματοποιηθεί χρησιμοποιώντας έξυπνα συμβόλαια εξοικονομώντας έτσι χρόνο και κόπους που δαπανώνται άσκοπα [18].
5. Κανονιστική συμμόρφωση μαζί με δυνατότητα ελέγχου: Το Blockchain λειτουργεί ως ένα ανοιχτό κατανεμημένο λογιστικό βιβλίο που παρέχει μια σαφή διαδρομή ελέγχου διευκολύνοντας τις επιχειρήσεις να συμμορφωθούν με τους κανονισμούς καθώς και να πληρούν τις νομικές απαιτήσεις, επομένως απλοποιεί σημαντικά τη συμμόρφωση με

τους κανονισμούς σε διάφορους κλάδους που έχουν αυστηρή εποπτεία, όπως η χρηματοδότηση ή η υγειονομική περίθαλψη.

6. Προκλήσεις & περιορισμοί: Ωστόσο, υπάρχουν αρκετές προκλήσεις μαζί με περιορισμούς που προσδιορίζονται από αυτό το ερευνητικό έγγραφο σε σχέση με την υιοθέτηση του blockchain, το οποίο περιλαμβάνει μεταξύ άλλων τεχνικές πτυχές όπως η επεκτασιμότητα και η διαλειτουργικότητα. ρυθμιστικές αβεβαιότητες· ανάγκες τυποποίησης· Το κόστος έγκαιρης υλοποίησης καθώς και η απαίτηση για εξειδικευμένο προσωπικό είναι υψηλή [10].
7. Πληροφορίες από περιπτωσιολογικές μελέτες: Οι περιπτωσιολογικές μελέτες που εξετάστηκαν κατά τη διάρκεια αυτής της έρευνας προσφέρουν πολύτιμες γνώσεις για πρακτικές χρήσεις και πλεονεκτήματα που σχετίζονται με την ανάπτυξη τεχνολογίας blockchain. Για παράδειγμα, η IBM μαζί με την πλατφόρμα TradeLens της Maersk καταδεικνύει πώς μπορεί να βελτιωθεί η διαφάνεια της εφοδιαστικής αλυσίδας μέσω της χρήσης blockchains αυξάνοντας παράλληλα την αποτελεσματικότητα (IBM, 2018). Ομοίως, το σύστημα MedRec δείχνει ότι μπορεί να επιτευχθεί καλύτερη διαχείριση δεδομένων ασθενών μέσω της χρήσης κατανεμημένων λογιστικών βιβλίων σε συνδυασμό με τον συντονισμό της φροντίδας στο πλαίσιο της υγειονομικής περίθαλψης [12].

Συνοπτικά, είναι σαφές από αυτά τα ευρήματα ότι τα έξυπνα συμβόλαια σε συνδυασμό με το blockchain έχουν τη δυνατότητα να φέρουν επανάσταση στις επιχειρηματικές δραστηριότητες σε διαφορετικούς κλάδους. Τα κέρδη αποτελεσματικότητας, οι βελτιώσεις ασφάλειας και τα οφέλη συμμόρφωσης που προσδιορίζονται εδώ χρησιμεύουν μόνο για να υπογραμμίσουν τη μετασχηματιστική τους ισχύ, αν και εξακολουθούν να υπάρχουν προκλήσεις που πρέπει να αντιμετωπιστούν πριν λάβει χώρα ευρύτερη υιοθέτηση, όπως φαίνεται από διάφορα παραδείγματα περιπτώσεων που επισημαίνονται σε αυτήν την έκθεση.

3.3 ΑΠΑΙΤΗΣΕΙΣ

Τεχνολογικές Απαιτήσεις

Για την επιτυχή εφαρμογή blockchains στις διαδικασίες των οργανισμών παράλληλα με τα έξυπνα συμβόλαια, υπάρχουν ορισμένες τεχνολογικές ανάγκες που πρέπει να ικανοποιηθούν χωρίς αποτυχία. Αυτά διασφαλίζουν ότι η υποδομή που υποστηρίζει τέτοια δίκτυα είναι αρκετά ισχυρή για να χειριστεί τις σύγχρονες επιχειρήσεις που απαιτούν στιβαρότητα καθώς και επεκτασιμότητα.

1. Επεκτασιμότητα: Η επεκτασιμότητα συμβαίνει να αποτελεί ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζει σήμερα το blockchain. Όταν έρχονται περισσότερες συναλλαγές, το σύστημα θα πρέπει να τις επεξεργαστεί, αλλά καθίσταται δύσκολο να γίνει κάτι τέτοιο, επειδή πρέπει πρώτα να επαληθευτούν όλες πριν πραγματοποιηθούν. Διαφορετικές προσεγγίσεις, συμπεριλαμβανομένης της διαμοιρασμού, των συναλλαγών εκτός αλυσίδας ή του δικτύου αστραπής που βασίζονται σε πρωτόκολλα επιπέδου δύο έχουν προταθεί ως λύσεις για την κλιμάκωση των blockchain [26].
2. Αμοιβαία λειτουργικότητα: Για το λόγο αυτό, τα blockchain πρέπει να έχουν την ικανότητα να συνεργάζονται με άλλα blockchain και συμβατικά συστήματα πληροφορικής χωρίς τριβές. Ως εκ τούτου, επιτρέπει σε διάφορες πλατφόρμες blockchain να επικοινωνούν μεταξύ τους, κάτι που τελικά οδηγεί στην ανταλλαγή πληροφοριών, καθιστώντας έτσι πιο λειτουργικές και δίνοντας χώρο για ολιστικές λύσεις σε αντάλλαγμα. Δίκτυα διαλειτουργικών blockchains δημιουργούνται από έργα όπως το Polkadot και το Cosmos [29][33].
3. Ασφάλεια: Μία από τις πιο κρίσιμες πτυχές είναι η διασφάλιση ότι υπάρχει ασφάλεια σε οποιοδήποτε σύστημα που βασίζεται στην τεχνολογία blockchain. Κοινά τρωτά σημεία, όπως επιθέσεις 51%, επιθέσεις Sybil και σφάλματα έξυπνων συμβολαίων θα πρέπει να

προστατεύονται κατά τη διάρκεια της ίδιας της φάσης σχεδιασμού. Η ασφαλής αρχιτεκτονική πρέπει να περιλαμβάνει προηγμένες κρυπτογραφικές τεχνικές μαζί με αλγόριθμους ισχυρής συναίνεσης εκτός από τη διενέργεια τακτικών ελέγχων σχετικά με τα μέτρα ασφαλείας που λαμβάνονται [37].

4. Αποδοτικότητα στη χρήση ενέργειας: Ο υψηλός ρυθμός με τον οποίο καταναλώνεται ενέργεια από ορισμένα δίκτυα είναι ένα σημείο ανησυχίας, ειδικά όταν μιλάμε για συναινετικές μεθόδους απόδειξης εργασίας (PoW). Η βιωσιμότητα στην υιοθέτηση του blockchain μπορεί να επιτευχθεί εάν καταλήξουμε σε πρωτόκολλα εξοικονόμησης ενέργειας όπως PoS ή DPoS σύμφωνα με τους King & Nadal (2012).
5. Φιλικές προς τον χρήστη διεπαφές: Η τεχνολογία Blockchain πρέπει να έχει μια εύχρηστη διεπαφή, ώστε να μπορεί να προσελκύει και άτομα που δεν γνωρίζουν την τεχνολογία. Αυτό σημαίνει ανάπτυξη εφαρμογών που παρέχουν διαισθητικά επίπεδα εμπειρίας χρήστη που αφαιρούν την πολυπλοκότητα από την άμεση αλληλεπίδραση μεταξύ των χρηστών και των υποκείμενων στοιχείων σε διαφορετικά συστήματα. Επίσης, η δημιουργία καλύτερης τεκμηρίωσης θα βοηθούσε σε αυτόν τον τομέα, καθώς πολλοί άνθρωποι δεν καταλαβαίνουν πώς λειτουργούν αυτά τα πράγματα [2].
6. Κανονιστική συμμόρφωση: Όλες οι τεχνολογικές λύσεις θα πρέπει να σχεδιάζονται λαμβάνοντας υπόψη τους υφιστάμενους νόμους, ενώ παράλληλα εξετάζονται και οι μελλοντικές αλλαγές. Η αποτυχία μπορεί να οδηγήσει σε νομικές συνέπειες, οδηγώντας έτσι κάποιον πίσω από τα κάγκελα ή ακόμη και να χάσει τα περιουσιακά του στοιχεία για πάντα! Ως εκ τούτου, οποιαδήποτε λύση τεθεί σε εφαρμογή θα πρέπει να διασφαλίζει έλεγχο, προστασία των δικαιωμάτων απορρήτου και υποχρεώσεις αναφοράς [23].

Ρυθμιστικές απαιτήσεις

Το ρυθμιστικό περιβάλλον της τεχνολογίας blockchain και των έξυπνων συμβάσεων εξακολουθούν να αλλάζουν και διαφορετικές δικαιοδοσίες υιοθετούν διαφορετικές προσεγγίσεις στη ρύθμισή τους. Προκειμένου οι επιχειρήσεις να εφαρμόσουν με επιτυχία την τεχνολογία blockchain, πρέπει να πλοηγηθούν σε αυτό το περίπλοκο ρυθμιστικό περιβάλλον.

1. Νομική αναγνώριση: Για να είναι εκτελεστές οι έξυπνες συμβάσεις, είναι απαραίτητο να αναγνωρίζονται ως νομικά δεσμευτικές συμφωνίες. Αυτό απαιτεί διευκρίνιση σχετικά με το νομικό καθεστώς των έξυπνων συμβολαίων και των συναλλαγών blockchain σε διάφορες δικαιοδοσίες όπου ισχύουν διαφορετικοί νόμοι. Ορισμένες χώρες έχουν ήδη εγκρίνει νόμους που αναγνωρίζουν τα έξυπνα συμβόλαια, ενώ άλλες βρίσκονται στη διαδικασία να το κάνουν [25].
2. Απόρρητο και προστασία δεδομένων: Η συμμόρφωση με τους κανονισμούς περί απορρήτου δεδομένων, όπως ο GDPR στην ΕΕ, είναι εξαιρετικά σημαντική. Οι λύσεις blockchain πρέπει να διασφαλίζουν ότι τα προσωπικά δεδομένα αντιμετωπίζονται σύμφωνα με αυτούς τους κανονισμούς, οι οποίοι ενδέχεται να περιλαμβάνουν τη χρήση τεχνικών για την ανωνυμοποίηση δεδομένων καθώς και τη δυνατότητα στους χρήστες να ελέγχουν τα προσωπικά τους στοιχεία [29][33].
3. Καταπολέμηση του ξεπλύματος χρήματος (AML) και Γνωρίστε τον Πελάτη σας (KYC): Οι απαιτήσεις AML και KYC πρέπει να πληρούνται από πλατφόρμες blockchain, ειδικά εκείνες που εμπλέκονται σε χρηματοοικονομικές συναλλαγές . Αυτό συνεπάγεται τον έλεγχο ταυτότητας του χρήστη και την παρακολούθηση ύποπτων συναλλαγών που αποσκοπούν στον τερματισμό της νομιμοποίησης εσόδων από παράνομες δραστηριότητες μεταξύ άλλων παράνομων δραστηριοτήτων .
4. Φορολογία και αναφορά: Θα πρέπει να υπάρχουν σαφείς κατευθυντήριες γραμμές σχετικά με τη φορολόγηση των περιουσιακών στοιχείων που αποκτώνται μέσω blockchains, επομένως θα πρέπει να υπάρχουν και κατάλληλοι μηχανισμοί για την αναφορά φόρων μετά την πραγματοποίηση τέτοιων συναλλαγών. Αυτό περιλαμβάνει την ενσωμάτωση αρχείων συναλλαγών κρυπτονομισμάτων σε φορολογικά συστήματα,

έτσι ώστε να μπορούν να δημιουργηθούν ακριβείς αναφορές σχετικά με τα κέρδη κεφαλαίου που προέρχονται από αυτά [44].

5. Προστασία καταναλωτή: Τα ρυθμιστικά πλαίσια θα πρέπει να έχουν διατάξεις που να προστατεύουν τους καταναλωτές από απάτη όταν χρησιμοποιούν υπηρεσίες που παρέχονται μέσω συστημάτων blockchain. Αυτό μπορεί να συνεπάγεται τη θέσπιση προτύπων για τη διαφάνεια μεταξύ των παρόχων υπηρεσιών, τη διασφάλιση των κεφαλαίων των πελατών και την ύπαρξη μηχανισμών επανόρθωσης σε περίπτωση διαφορών [43].
6. Πνευματική Ιδιοκτησία (IP): Η χρήση του blockchain για τη διαχείριση δικαιωμάτων πνευματικής ιδιοκτησίας απαιτεί καλά καθορισμένους κανόνες σχετικά με τον τρόπο με τον οποίο αυτά τα δικαιώματα καταγράφονται, μεταβιβάζονται και επιβάλλονται σε πλατφόρμες blockchain. Αυτό είναι απαραίτητο για τη διασφάλιση των συμφερόντων των δημιουργών και των καινοτόμων που χρησιμοποιούν αυτήν την τεχνολογία [29].

3.4 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Ανάλυση Απειλών

Η τεχνολογία Blockchain είναι ασφαλής, αλλά δεν είναι εντελώς απρόσβλητη σε απειλές ασφαλείας. Θα πρέπει να γίνει ανάλυση απειλών προκειμένου να διαπιστωθεί ποιοι κίνδυνοι μπορεί να προκύψουν από τη χρήση blockchain ή έξυπνων συμβολαίων και πώς μπορούν να μετριαστούν καλύτερα.

1. Επίθεση 51%: Όπως αναφέρθηκε προηγουμένως, μια επίθεση 51% συμβαίνει όταν ένα άτομο ή ομάδα αποκτά τον έλεγχο πάνω από το ήμισυ της συνολικής υπολογιστικής ισχύος σε ένα δίκτυο. Αυτό τους επιτρέπει να ελέγχουν το blockchain, να ξοδεύουν νομίσματα δύο φορές και να εμποδίζουν την επιβεβαίωση νέων συναλλαγών. Η αποφυγή τέτοιων επιθέσεων απαιτεί δεξαμενές εξόρυξης που είναι αποκεντρωμένες και ευρέως διανεμημένες [3].
2. Ευπάθειες έξυπνων συμβολαίων: Λάθη στον κώδικα για έξυπνα συμβόλαια θα μπορούσαν να οδηγήσουν σε τεράστιες οικονομικές απώλειες. Το πιο διαβόητο παράδειγμα είναι η επίθεση DAO στο Ethereum όπου ένας εισβολέας εκμεταλλεύτηκε ένα ελάττωμα στον κώδικα της σύμβασης για να εξαντλήσει χρήματα. Αυστηρός έλεγχος κωδικών καθώς και χρήση επίσημων οι τεχνικές επαλήθευσης θα βοηθούσαν στη διασφάλιση της φύλαξης των έξυπνων συμβολαίων [14][28].
3. Sybil Attacks: Κατά τη διάρκεια μιας επίθεσης Sybil, ένας αντίπαλος δημιουργεί πολλές πλαστές ταυτότητες κερδίζοντας έτσι επιρροή σε ένα δίκτυο. Το αποτέλεσμα θα μπορούσε να είναι διακοπή των μηχανισμών συναίνεσης ή ακόμη και χειραγώγηση των λειτουργιών του δικτύου. Συστήματα επαλήθευσης ταυτότητας που είναι ισχυρά μαζί με συστήματα φήμης μπορούν να βοηθήσουν στην αποτροπή του Sybil επιθέσεις [23].
4. Επιθέσεις απάντησης: Αυτές περιλαμβάνουν την επανάληψη μιας επικυρωμένης μεταφοράς δεδομένων με κακόβουλη πρόθεση. Αυτό μπορεί να αποφευχθεί με την εισαγωγή διασφαλίσεων έναντι τέτοιων επιθέσεων, για παράδειγμα μοναδικό αναγνωριστικό συναλλαγής [33].
5. Phishing και Κοινωνική Μηχανική: Οι χρήστες συστημάτων Blockchain είναι επιρρεπείς σε επιθέσεις phishing και κοινωνική μηχανική. Οι επιτιθέμενοι εξαπατούν άτομα ώστε να αποκαλύψουν τα ιδιωτικά τους κλειδιά ή άλλες πολύτιμες πληροφορίες. Η δημιουργία ευαισθητοποίησης σχετικά με αυτούς τους τύπους απειλών μεταξύ των χρηστών σε συνδυασμό με τον έλεγχο ταυτότητας πολλαπλών παραγόντων θα βοηθήσει στην ενίσχυση της ασφάλειας στο σύστημα [44].
6. Εκμεταλλεύσεις στον μηχανισμό συναίνεσης: Διαφορετικοί μηχανισμοί συναίνεσης έχουν διαφορετικά τρωτά σημεία. Για παράδειγμα, το PoW απαιτεί υψηλή κατανάλωση ενέργειας και μπορεί να οδηγήσει σε συγκέντρωση, ενώ το PoS θα μπορούσε να

αντιμετωπίσει πρόβλημα «δεν διακυβεύεται» μεταξύ άλλων. Επομένως, θα πρέπει να γίνεται συνεχής έρευνα για την εύρεση πιο ασφαλών και αποτελεσματικών αλγορίθμων συναίνεσης [35].

Διαχείριση κινδύνου

Είναι απαραίτητη μια καλή προσέγγιση διαχείρισης κινδύνου, ώστε οι προκλήσεις που σχετίζονται με την ασφάλεια στην τεχνολογία blockchain καθώς και τα έξυπνα συμβόλαια να μπορούν να αντιμετωπιστούν αποτελεσματικά. Τέτοιες στρατηγικές χρησιμοποιούν μείγματα τεχνικών λύσεων, βέλτιστων πρακτικών και προληπτικών μέτρων.

1. Έλεγχοι ασφαλείας και αναθεωρήσεις κώδικα: Οι τακτικοί έλεγχοι ασφάλειας είναι σημαντικοί επειδή βοηθούν στον εντοπισμό αδυναμιών σε συστήματα blockchain ή έξυπνες συμβάσεις που χρειάζονται επιδιόρθωση μέσω της διαδικασίας ελέγχου κώδικα που πολύ συχνά παραμελείται από τους ίδιους τους προγραμματιστές που μπορεί να μην γνωρίζουν πάντα πώς να το κάνουν. Αυτή η πρακτική θα πρέπει επομένως να γίνει ρουτίνα για όλους τους [40]
2. Επίσημη επαλήθευση: Οι κωδικοί έξυπνων συμβολαίων μπορούν να ελεγχθούν χρησιμοποιώντας μαθηματικές αποδείξεις, κάτι που κάνει η επίσημη επαλήθευση. Εδώ επαληθεύεται η ορθότητα, εξαλείφοντας έτσι πολλά πιθανά σημεία ευπάθειας σε τέτοιους κωδικούς, καθώς και διασφαλίζοντας ότι συμπεριφέρονται σύμφωνα με το σχέδιο. Μερικά εργαλεία που μπορούν να το κάνουν αυτό περιλαμβάνουν το Coq μαζί με την Isabelle μεταξύ άλλων [42].
3. Αποκεντρωμένοι μηχανισμοί ασφάλειας: Τα πορτοφόλια πολλαπλών υπογραφών και η αποκεντρωμένη επαλήθευση ταυτότητας είναι μεταξύ των διαφόρων επιλογών για βελτιωμένη ασφάλεια μέσω της αποκέντρωσης. Αυτό σημαίνει ότι οι ταυτότητες πρέπει να επαληθεύονται χωρίς να βασίζονται σε καμία κεντρική αρχή, ενώ οι συναλλαγές χρειάζονται πολλαπλές εγκρίσεις πριν εξουσιοδοτηθούν, μειώνοντας έτσι τις πιθανότητες μη εξουσιοδοτημένης πρόσβασης σε κεφάλαια [34][38][39].
4. Συνεχής παρακολούθηση και απόκριση συμβάντων: Οι χρόνοι γρήγορης απόκρισης απαιτούν συνεχή επιτήρηση, επομένως είναι σημαντικό να υπάρχει ένα σύστημα παρακολούθησης που θα εντοπίζει άμεσα τις απειλές. Επιπλέον, θα πρέπει να υπάρχουν επίσης λεπτομερή σχέδια απόκρισης συμβάντων σχεδιασμένα ειδικά για περιβάλλοντα blockchain, καθώς απαιτούν μοναδικές μεθόδους χειρισμού λόγω της κατανεμημένης φύσης τους [25].
5. Εκπαίδευση και κατάρτιση: Είναι σημαντικό να εκπαιδεύονται οι άνθρωποι σχετικά με τους καλύτερους τρόπους ασφάλειας των συστημάτων τους όταν χρησιμοποιούν τεχνολογία blockchain. Τακτικές εκπαιδευτικές συνεδρίες σε συνδυασμό με προγράμματα δημιουργίας ευαισθητοποίησης μπορούν να βοηθήσουν στον εντοπισμό επιθέσεων phishing, απόπειρες κοινωνικής μηχανικής μεταξύ άλλων κινδύνων που σχετίζονται με αυτούς τους τύπους συστημάτων [8][23].
6. Κανονιστική Συμμόρφωση: Η συμμόρφωση με τους ισχύοντες κανονισμούς και πρότυπα μπορεί να μειώσει τους νομικούς κινδύνους που σχετίζονται με έξυπνες συμβάσεις ή blockchains, ιδίως όταν δεν υπάρχουν κατάλληλοι έλεγχοι. Παραδείγματα περιλαμβάνουν νόμους για την προστασία προσωπικών δεδομένων, απαιτήσεις για την καταπολέμηση της χρηματοδότησης της τρομοκρατίας και του ξεπλύματος χρημάτων (AML), καθώς και ειδικές οδηγίες του κλάδου. Η εφαρμογή αυτών των κανονισμών όχι μόνο ενισχύει την ασφάλεια, αλλά και δημιουργεί εμπιστοσύνη στους ενδιαφερόμενους, διασφαλίζοντας ότι όλες οι διαδικασίες είναι νόμιμες και συμμορφώνονται με τις κανονιστικές απαιτήσεις [34].
7. Πλεονασμός και δημιουργία αντιγράφων ασφαλείας: Σε περίπτωση που συμβεί αποτυχία κάπου μέσα στο σύστημα blockchain κάποιου, τότε ο πλεονασμός μαζί με τις εφεδρικές λύσεις τους έχει καλύψει διασφαλίζοντας ότι δεν θα συμβεί απώλεια σε κανένα σημείο, επομένως η ανάκτηση γίνεται εύκολη ακόμα και μετά την απώλεια

δεδομένων εντελώς εκτός αλυσίδας, τα αντίγραφα ασφαλείας πρέπει επίσης να γίνονται τακτικά [12].

Συνοψίζοντας, είναι απαραίτητο να επιλυθούν προβλήματα ασφάλειας που σχετίζονται με την τεχνολογία blockchain και τις απαιτήσεις συμμόρφωσης των έξυπνων συμβάσεων τόσο από τεχνική όσο και από κανονιστική άποψη, ώστε να διασφαλιστεί η επιτυχής υιοθέτησή τους στις επιχειρηματικές δραστηριότητες. μέσω της εφαρμογής ισχυρών μέτρων, συμβαδίζοντας με τις αναδυόμενες απειλές καθώς και ακολουθώντας καθορισμένα πρότυπα.

3.5 ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ

Παραδείγματα Λεπτομερούς Εφαρμογής Blockchain

1. Walmart και IBM - Τροφική Αλυσίδα. Η εταιρεία σχημάτισε συνεργασία με την IBM για τη δημιουργία ενός συστήματος βασισμένου σε blockchain για την παρακολούθηση των τροφίμων στην αλυσίδα εφοδιασμού της. Με αυτόν τον τρόπο, μπόρεσε να εντοπίσει και να διορθώσει γρήγορα προβλήματα μόλυνσης στην αλυσίδα εφοδιασμού [46]

Συνοπτική περιγραφή: Η Walmart χρησιμοποίησε την αλυσίδα μπλοκ Food Trust της IBM για να ψηφιοποιήσει την αλυσίδα εφοδιασμού τροφίμων της, καταγράφοντας δεδομένα σε κάθε στάδιο από φάρμα σε κατάστημα, όπως από πού προέρχονταν τα προϊόντα ή πώς χειρίζονταν.

Αυτό μείωσε τον χρόνο που αφιερώθηκε στην ανίχνευση της πηγής των μολυσμένων τροφίμων από ημέρες σε δευτερόλεπτα, γεγονός που όχι μόνο εξοικονόμησε χρήματα αλλά και απέτρεψε την καταστροφή της φήμης, καθώς οι άνθρωποι μπορούσαν να καταναλώσουν ξανά ασφαλή προϊόντα.

Συμπεράσματα: Η υπόθεση έδειξε ότι όλοι οι εταίροι πρέπει να συνεργάζονται σε ολόκληρο το κανάλι διανομής. Εκτός από αυτό, απεικόνισε επίσης τη διαφάνεια που δημιουργεί αξία μέσω της υπευθυνότητας που φέρνουν τα blockchain τα οποία είναι πολύ σημαντικά για την εμπιστοσύνη και την ασφάλεια των πελατών.

2. De Beers - Diamond Tracking. Ο μεγαλύτερος παραγωγός διαμαντιών που εφάρμοσε παγκοσμίως το Tracr – μια εφαρμογή που τρέχει πάνω από ένα blockchain για να παρακολουθεί την κίνηση των διαμαντιών από τα ορυχεία μέχρι να φτάσουν σε καταστήματα λιανικής, ώστε να διασφαλίζεται η γνησιότητά τους και η ηθική προμήθεια τους [44] [46].

Συνοπτική περιγραφή: Κάθε βήμα που γίνεται από κάθε κομμάτι καταγράφεται στο Tracr ξεκινώντας με την εξαγωγή τους από την επιφάνεια της γης, κόβοντάς τα σε σχήματα κατάλληλα για την κατασκευή κοσμημάτων πριν τελικά πουληθούν τελικά προϊόντα σε διάφορα καταστήματα σε όλο τον κόσμο.

Αποτελέσματα που επιτεύχθηκαν: Άνοιξε την ορατότητα σε διάφορα τμήματα που εμπλέκονται στις αλυσίδες εφοδιασμού διαμαντιών, αυξάνοντας έτσι τη διαφάνεια σε ολόκληρη την αγορά, επιτρέποντας έτσι στους πελάτες να επαληθεύσουν εάν οι πολύτιμοι λίθοι τους όντως αποκτήθηκαν με δίκαια μέσα ή όχι. ως εκ τούτου, η αντιμετώπιση των ανησυχιών σχετικά με τα ορυκτά σύγκρουσης.

Συμπεράσματα: Αυτού του είδους οι περιπτώσεις δίνουν έμφαση στη διαφάνεια κατά μήκος των αλυσίδων εφοδιασμού, ιδίως όταν υπάρχει ανάγκη για υπεύθυνη προμήθεια εντός των βιομηχανιών. Επιπλέον, δείχνει επίσης πόσο χρήσιμα μπορούν να είναι τα blockchain για την ενίσχυση της εμπιστοσύνης των καταναλωτών σε αυτούς τους τομείς, υποστηρίζοντας παράλληλα πρωτοβουλίες εταιρικής κοινωνικής ευθύνης.

3. MediLedger - Ασφάλεια Φαρμακευτικής Αλυσίδας. Το MediLedger δημιουργήθηκε ως ένα ασφαλές και αποτελεσματικό δίκτυο για την παρακολούθηση φαρμακευτικών προϊόντων μέσω της εφοδιαστικής αλυσίδας χρησιμοποιώντας τεχνολογία blockchain

που μπορεί να βοηθήσει στην καταπολέμηση πλαστών φαρμάκων επαληθεύοντας την αυθεντικότητά τους [39].

Συνοπτική περιγραφή: Το σύστημα παρακολουθεί τις συναλλαγές και τις κινήσεις των φαρμάκων σε μια δημόσια λογιστική γνωστή ως DLT (τεχνολογία κατανεμημένης λογιστικής) ή απλώς τοποθετεί μια αλυσίδα μπλοκ.

Κάθε συσκευασία φαρμάκου λαμβάνει μοναδικούς κωδικούς αναγνώρισης κατά την παραγωγή και, στη συνέχεια, αυτοί καταγράφονται σε αυτήν την ψηφιακή κατανεμημένη βάση δεδομένων μαζί με άλλα σχετικά δεδομένα, όπως λεπτομέρειες κατασκευής. επιτρέποντας έτσι την εύκολη επαλήθευση όποτε είναι απαραίτητο.

Αποτελέσματα που επιτεύχθηκαν: Αύξησε την ορατότητα σε όλα τα στάδια που εμπλέκονται στη διαδικασία διανομής, μειώνοντας έτσι τις πιθανότητες να κυκλοφορήσουν πλαστά φάρμακα. επίσης απλοποίηση των διαδικασιών συμμόρφωσης που οδηγεί σε χαμηλότερο κόστος και καλύτερη αποτελεσματικότητα.

Συμπεράσματα: Αυτή η περίπτωση καταδεικνύει πώς μπορούν να χρησιμοποιηθούν τα blockchain για να διασφαλιστεί η ακεραιότητα των πληροφοριών προϊόντων, ενώ συμμορφώνονται με αυστηρούς κανόνες που διέπουν τέτοιους τομείς όπου η ασφάλεια πρέπει να προηγείται πριν από οτιδήποτε άλλο. επιδεικνύοντας επιπλέον πιθανούς τομείς όπου θα μπορούσαν να γίνουν επενδύσεις για τη μείωση των λειτουργικών δαπανών σε περιβάλλοντα με αυστηρή ρύθμιση [39].

Ιστορίες επιτυχίας – Τι λειτούργησε και γιατί

1. Ο αντίκτυπος του Ethereum στην αποκεντρωμένη χρηματοδότηση (DeFi): Η εισαγωγή των έξυπνων συμβολαίων μέσω της πλατφόρμας Ethereum οδήγησε σε μια ραγδαία ανάπτυξη εφαρμογών αποκεντρωμένης χρηματοδότησης (DeFi). Αυτές οι εφαρμογές επιτρέπουν στους ανθρώπους να δανείζουν, να δανείζονται ή να συναλλάσσονται άμεσα μεταξύ τους, χωρίς την ανάγκη μεσολαβητών, όπως οι τράπεζες [32][23].

Επιτεύγματα: Μέχρι στιγμής έχουν καταγραφεί δισεκατομμύρια που έχουν κλειδωθεί σε πολλά πρωτόκολλα χάρη στη φιλικότητα τους όσον αφορά την προσβασιμότητα σε σύγκριση με τις παραδοσιακές χρηματοοικονομικές υπηρεσίες, επειδή προσφέρουν περισσότερο έλεγχο παράλληλα με τη διαφάνεια για τους χρήστες.

Συμπεράσματα: Η ολοκλήρωση του DeFi υπογραμμίζει την ικανότητα ανατροπής της τεχνολογίας blockchain στα οικονομικά. Αναδεικνύει την ανάγκη για έλεγχο ασφάλειας και έξυπνου συμβολαίου, επειδή τα τρωτά σημεία μπορεί να οδηγήσουν σε σημαντικές οικονομικές απώλειες. Επιπλέον, το κίνημα DeFi δείχνει ότι η ρυθμιστική σαφήνεια είναι απαραίτητη για την προστασία των ατόμων και τη διασφάλιση της βιώσιμης ανάπτυξης [42].

2. Propy - Συναλλαγές Ακίνητης Περιουσίας: Το Propy είναι μια πλατφόρμα που βασίζεται σε blockchain η οποία απλοποιεί τις συναλλαγές ακινήτων αυτοματοποιώντας τις και παρέχοντας διαφανή αρχεία ιδιοκτησίας. Αυτό το σύστημα έχει διευκολύνει πολλές υψηλού προφίλ πωλήσεις ακινήτων, αποδεικνύοντας έτσι πόσο αποτελεσματική και ασφαλή μπορεί να γίνει η ακίνητη περιουσία όταν διεξάγεται μέσω της τεχνολογίας blockchain [48].

Επιτεύγματα: Το Propy πέτυχε να ολοκληρώσει διαφορετικές συμφωνίες ακινήτων σε όλες τις χώρες μειώνοντας τον χρόνο που απαιτείται καθώς και το κόστος που προκύπτει κατά τις παραδοσιακές διαδικασίες αγοράς ή πώλησης κατοικιών. Επιπλέον, ενισχύει τη σαφήνεια, ενώ μειώνει τις πιθανότητες για απάτη. Η υπόθεση Propy δείχνει πώς αυτός ο τύπος συστήματος μπορεί να βοηθήσει στην απλούστευση των περίπλοκων δραστηριοτήτων, διασφαλίζοντας παράλληλα ασφάλεια κατά τη διάρκεια εργασιών που σχετίζονται με την αγορά ή πώληση ακινήτων χρησιμοποιώντας τεχνολογία κατανεμημένης λογιστικής όπως τα blockchains για την εξασφάλιση συναλλαγών, μεταξύ άλλων.

3.6 ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

Ισχύοντες Κανονισμοί

Οι κανόνες σχετικά με το blockchain και τα έξυπνα συμβόλαια αλλάζουν γρήγορα σε όλο τον κόσμο. Πολλές χώρες έχουν υιοθετήσει διαφορετικές προσεγγίσεις όσον αφορά τη ρύθμιση. Είναι σημαντικό για τις επιχειρήσεις να γνωρίζουν τους ισχύοντες κανονισμούς τους εάν σκέφτονται να εφαρμόσουν τεχνολογία blockchain.

1. Ηνωμένες Πολιτείες: Η Επιτροπή Κεφαλαιαγοράς (SEC), Commodity Futures Trading Commission (CFTC) και Financial Crimes Enforcement Network (FinCEN) ρυθμίζουν όλα τα κρυπτονομίσματα στις αρχικές προσφορές νομισμάτων των ΗΠΑ (ICO) υπό τη δικαιοδοσία της SEC και ορισμένα ψηφιακά περιουσιακά στοιχεία ταξινομούνται ως τίτλους από αυτούς. Τα παράγωγα κρυπτονομισμάτων εποπτεύονται από την CFTC. Οι απαιτήσεις για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML) και η διαδικασία γνώσης του πελάτη (KYC) εμπίπτουν στην αρμοδιότητα του FinCEN [47].
2. Ευρωπαϊκή Ένωση: Η Ευρωπαϊκή Ένωση είναι ενεργή στις προσπάθειές της να ρυθμίσει την τεχνολογία blockchain. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) ορίζει αυστηρές οδηγίες για το απόρρητο των δεδομένων για blockchains που χειρίζονται προσωπικές πληροφορίες. Η πέμπτη οδηγία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες επεκτείνει τους κανόνες AML (Anti Money Laundering) για να καλύψει τις ανταλλαγές κρυπτονομισμάτων και τους παρόχους πορτοφολιών, ενώ ο προτεινόμενος κανονισμός για τις αγορές κρυπτονομισμάτων θα θεσπίσει ένα ολοκληρωμένο κανονιστικό πλαίσιο για τα κρυπτογραφικά περιουσιακά στοιχεία σε ολόκληρη την ΕΕ [41].
3. Κίνα: Η Κίνα έχει υιοθετήσει σκληρή γραμμή κατά των κρυπτονομισμάτων, απαγορεύοντας ICO και ανταλλαγές που διευκολύνουν τις συναλλαγές μεταξύ νομισμάτων fiat και ψηφιακών περιουσιακών στοιχείων. Ωστόσο, εξετάζει άλλες περιπτώσεις χρήσης blockchain, όπως συστήματα διαχείρισης εφοδιαστικής αλυσίδας ή ακόμη και ψηφιακά νομίσματα κεντρικής τράπεζας. Η People's Bank of China ανακοίνωσε πρόσφατα σχέδια για τη δημιουργία του δικού της εθνικού ψηφιακού νομίσματος χρησιμοποιώντας τεχνολογία κατανεμημένης λογιστικής που ονομάζεται DCEP – Digital Currency Electronic Payment System [38].
4. Ιαπωνία: Η Ιαπωνία έχει αγκαλιάσει την τεχνολογία blockchain, αλλά με σαφείς κανονισμούς και γύρω της: Το KYC/AML πρέπει να τηρείται από κάθε ανταλλακτήριο που θέλει να λειτουργεί νόμιμα εντός των ορίων της χώρας. Ο Οργανισμός Χρηματοοικονομικών Υπηρεσιών, ο οποίος εποπτεύει επίσης τον παραδοσιακό τραπεζικό τομέα, το κάνει εξίσου εδώ, ενθαρρύνοντας έτσι ασφαλείς πρακτικές σχετικά με την προστασία των καταναλωτών από απατεώνες, ενώ παράλληλα ενθαρρύνει την καινοτομία μεταξύ των παικτών

Τάσεις και μελλοντικές κατευθύνσεις

Το μέλλον των ρυθμιστικών προσεγγίσεων για την τεχνολογία blockchain και τα έξυπνα συμβόλαια μπορεί να περιλαμβάνει την επίτευξη ισορροπίας μεταξύ της προώθησης της καινοτομίας και της διασφάλισης της προστασίας των καταναλωτών. Μερικές πιθανές τάσεις ή κατευθύνσεις θα μπορούσαν να περιλαμβάνουν:

1. Ο Παγκόσμιος Ρυθμιστικός Συντονισμός Το Blockchain είναι ένα παγκόσμιο φαινόμενο που ξεπερνά τα σύνορα, επομένως πρέπει να υπάρχει κάποιο επίπεδο διεθνούς συντονισμού μεταξύ των ρυθμιστικών αρχών. Με αυτόν τον τρόπο οι νεοφυείς επιχειρήσεις δεν θα χρειαστεί να αντιμετωπίσουν διαφορετικούς κανόνες όταν κλιμακώνουν τις δραστηριότητές τους σε διάφορες δικαιοδοσίες [25].
2. Περισσότερη εστίαση στην προστασία των καταναλωτών Αναμένεται ότι οι μελλοντικοί κανονισμοί θα τονίσουν την ανάγκη προστασίας των καταναλωτών σε σχέση με τα

ψηφιακά περιουσιακά στοιχεία. Αυτό μπορεί να επιτευχθεί μέσω μέτρων διαφάνειας, όπως η απαίτηση από όλους τους εκδότες ICO να αποκαλύπτουν την ταυτότητά τους, ώστε οι επενδυτές να γνωρίζουν με ποιον έχουν να κάνουν ή να δημιουργήσουν μηχανισμούς για την επίλυση διαφορών που προκύπτουν από επενδυτικές συμβάσεις [11].

3. Ρύθμιση αποκεντρωμένης χρηματοδότησης (DeFi) Οι αποκεντρωμένες πλατφόρμες χρηματοδότησης όπως το Uniswap έχουν εκραγεί σε δημοτικότητα το περασμένο περίπου έτος, αλλά επί του παρόντος δεν εμπίπτουν στα υπάρχοντα ρυθμιστικά πλαίσια, καθώς λειτουργούν χωρίς μεσάζοντες. Ως εκ τούτου, οι ρυθμιστικές αρχές ενδέχεται να χρειαστούν νέα εργαλεία στο οπλοστάσιό τους ειδικά σχεδιασμένα για την επίβλεψη του τομέα DeFi που λαμβάνει υπόψη τις ανησυχίες σχετικά με τη συμμόρφωση με το AML/KYC καθώς και την προστασία των χρηστών από κινδύνους που σχετίζονται με δραστηριότητες πειρατείας που λαμβάνουν χώρα σε αυτές τις πλατφόρμες [23].
4. Απόρρητο Δεδομένων και Προστασία Πληροφοριών Δεδομένου ότι οι αλυσίδες μπλοκ είναι βάσεις δεδομένων απαραβίαστες που αποθηκεύουν τις συναλλαγές για πάντα στην αλυσίδα, συνεπάγεται ότι οποιοσδήποτε νόμος που επιδιώκει να προστατεύσει το απόρρητο των ανθρώπων πρέπει να βρει τρόπους να προσαρμόσει την αμετάβλητη φύση των εγγραφών του καθολικού. Ως εκ τούτου, η μελλοντική νομοθεσία για την προστασία των δεδομένων μπορεί να έχει σχεδιαστεί για την αντιμετώπιση των προκλήσεων που θέτει αυτή η πτυχή της τεχνολογίας κατανεμημένης λογιστικής [39].
5. Οι ρυθμιστικές αρχές της προώθησης της καινοτομίας θα μπορούσαν να συμβάλουν στην υιοθέτηση με την εισαγωγή πολιτικών που στοχεύουν στην τόνωση της δημιουργικότητας στη βιομηχανία blockchain, για παράδειγμα, δημιουργώντας ρυθμιστικά sandboxes που επιτρέπουν στις νεοφυείς επιχειρήσεις να πειραματίζονται με διαφορετικές περιπτώσεις χρήσης σε ελεγχόμενο περιβάλλον ή προσφέροντας φορολογικά κίνητρα που συνδέονται ειδικά με την ανάπτυξη εφαρμογών που σχετίζονται με το blockchain [41].
6. Συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα Για τη δημιουργία αποτελεσματικών ρυθμιστικών πλαισίων, είναι σημαντικό να υπάρχει συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα. Οι κυβερνήσεις και οι ρυθμιστικοί φορείς μπορούν να συνεργαστούν με τους ενδιαφερόμενους σε βιομηχανίες για να εκτιμήσουν τις δυνατότητες αυτής της τεχνολογίας καθώς και τις προκλήσεις της, δημιουργώντας έτσι κανόνες που θα λειτουργούν ενώ θα ενθαρρύνουν τη δημιουργικότητα [46].

Συνοπτικά, οι παραπάνω μελέτες περίπτωσης σχετικά με τις τεχνολογίες blockchain και τα έξυπνα συμβόλαια δείχνουν τις δυνατότητές τους να μεταμορφώσουν τα επιχειρηματικά δεδομένα. Επομένως, οι επιχειρήσεις χρειάζεται μόνο να εφαρμόσουν επιτυχημένα μοντέλα που χρησιμοποιούνται ήδη αλλού και, στη συνέχεια, να τα προσαρμόσουν για τοπική χρήση, έτσι ώστε να μπορούν να επωφεληθούν από την αυξημένη αποτελεσματικότητα που προσφέρει η αλυσίδα των μπλοκ, η οποία βελτιώνει επίσης τα επίπεδα διαφάνειας εκτός από την εξασφάλιση διαφόρων λειτουργιών που αναλαμβάνονται εντός των οργανισμών. Σε αυτήν την περίπτωση, καθίσταται απαραίτητο για μελλοντικούς κανονισμούς να τεθούν σε εφαρμογή διαδικασίες ανάπτυξης μελλοντικών κανονισμών που αποσκοπούν στην εξισορρόπηση της καινοτομίας έναντι της προστασίας των συμφερόντων των καταναλωτών παράλληλα με την ακεραιότητα της αγοράς, επειδή είναι πιθανό να διαμορφώσουν περαιτέρω αυτόν τον κλάδο, δεδομένης της τρέχουσας κατάστασής του που χαρακτηρίζεται από ταχείες αλλαγές σε συνδυασμό με αβεβαιότητα σχετικά με τα νομικά πρότυπα που εφαρμόζονται σε αυτά.

Κεφάλαιο 4: Εφαρμογές των Smart Contracts στο Online Αθλητικό Στοίχημα

4.1 ΕΡΓΑΛΕΙΑ

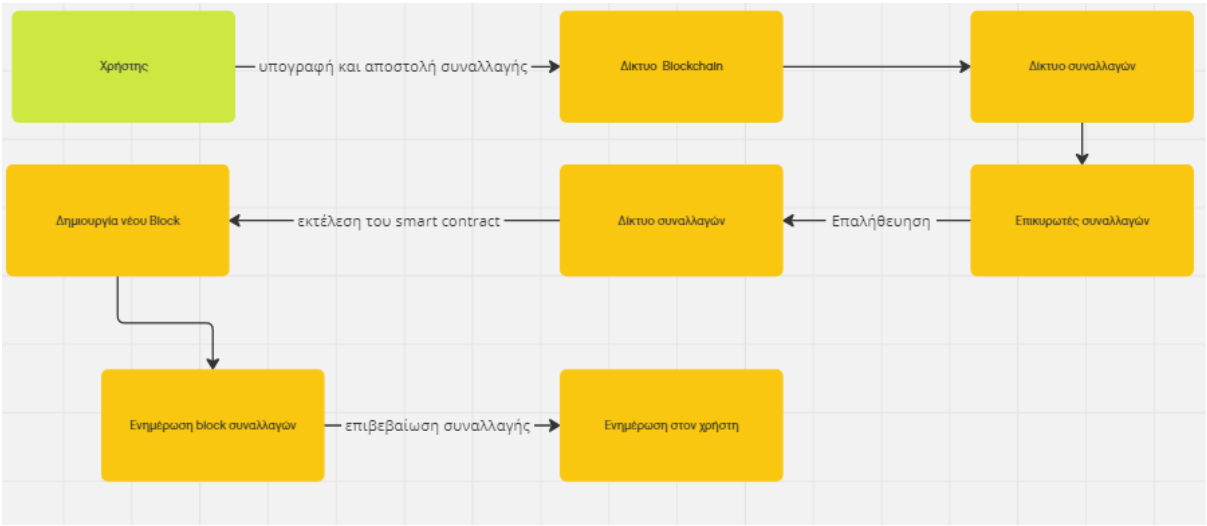
Η παρούσα ενότητα παρουσιάζει την αρχιτεκτονική ενός συστήματος για την ανάπτυξη των smart contracts καθώς και των εργαλειών που χρησιμοποιήθηκαν μέσα σε ένα τοπικό δίκτυο.

Solidity: Η υλοποίηση του smart contract έγινε με τη χρήση της γλώσσας προγραμματισμού Solidity. Η Solidity παρέχει τη δυνατότητα να καθοριστούν έξυπνα συμβόλαια που περιλαμβάνουν όλες τις απαραίτητες λειτουργίες για την τοποθέτηση, τη διαχείριση και την επίλυση στοιχημάτων.

Node.js: Είναι απαραίτητο εργαλείο για την εγκατάσταση του Truffle. Το node.js είναι απαραίτητο για συνδεθούμε στο blockchain και να αλληλεπιδράσουμε με το δίκτυο.

Truffle Framework: Το Truffle χρησιμοποιήθηκε ως το κύριο πλαίσιο ανάπτυξης για τη δημιουργία και την ανάπτυξη του smart contract. Το Truffle προσφέρει ένα περιβάλλον που υποστηρίζει τη διαχείριση smart contract, από την ανάπτυξη έως και τη μεταφορά στο δίκτυο.

Ganache: Το Ganache, αποτελεί ένα προσωπικό blockchain και χρησιμοποιήθηκε για την τοπική ανάπτυξη και δοκιμή του smart contract. Παρέχει ένα περιβάλλον στο οποίο μπορούν να εκτελεστούν συναλλαγές (transactions) και να δοκιμαστούν όλες οι λειτουργίες του συμβολαίου, προτού προχωρήσει η ανάπτυξή του σε ένα δημόσιο δίκτυο.



Εικόνα 1: Ροή μέσα στο Δίκτυο του Blockchain

Ο **χρήστης** είναι αυτός που ξεκινά τη διαδικασία μέσω μιας αποκεντρωμένης εφαρμογής. Το **δίκτυο blockchain** αποτελείται από ένα αποκεντρωμένο δίκτυο κόμβων, που αλληλεπιδρούν μεταξύ τους για να επαληθεύουν και να καταγράφουν συναλλαγές. Οι συναλλαγές μεταδίδονται στο pool των συναλλαγών, όπου περιμένουν μέχρι να επαληθευτούν και να εκτελεστούν. Οι **εξορύκτες** ή **επικυρωτές** είναι οι κόμβοι που αναλαμβάνουν να επαληθεύσουν τη συναλλαγή, ελέγχοντας την εγκυρότητά της και προσθέτοντάς την στο blockchain. Το **έξυπνο συμβόλαιο** είναι ένα πρόγραμμα που εκτελείται όταν η συναλλαγή θεωρηθεί έγκυρη, αυτόματα και χωρίς

την ανάγκη μεσολαβητή. Η επιβεβαιωμένη συναλλαγή καταγράφεται μόνιμα στην **αλυσίδα μπλοκ** (blockchain), όπου δεν μπορεί να τροποποιηθεί (βλέπε Εικόνα 1).

4.2 ΑΝΑΠΤΥΞΗ ΤΩΝ SMART CONTRACTS

Τοποθέτηση στοιχήματος σε μια διαδικτυακή εφαρμογή στοιχήματος (BetPlacement)

```
contract BetPlacement {
    struct Bet {
        address user;
        uint256 amount;
        bool placed;
    }

    mapping(uint256 => Bet) public bets;
    uint256 public betCounter;

    event BetPlaced(uint256 betId, address indexed user, uint256 amount);

    function placeBet() external payable {
        require(msg.value > 0, "Bet amount must be greater than zero");

        Bet memory newBet = Bet({
            user: msg.sender,
            amount: msg.value,
            placed: true
        });

        bets[betCounter] = newBet;
        emit BetPlaced(betCounter, msg.sender, msg.value);
        betCounter++;
    }

    function getBet(uint256 betId) external view returns (Bet memory) {
        return bets[betId];
    }
}
```

Εικόνα 2: Τοποθέτηση στοιχήματος σε μια διαδικτυακή εφαρμογή στοιχήματος (BetPlacement)

Το smart contract BetPlacement επιτρέπει σε χρήστες να τοποθετούν στοιχήματα μέσω της συναρτήσεως placeBet. Η αλληλεπίδραση με το συμβόλαιο βασίζεται στη χρήση μιας δομής η οποία αποθηκεύει τα στοιχήματα με βάση ένα μοναδικό betId.

Περιγραφή της Δομής του Συμβολαίου

- Η Δομή Bet: Περιέχει τα εξής πεδία:
  - user: Η διεύθυνση του χρήστη που τοποθετεί το στοίχημα.
  - amount: Το ποσό του στοιχήματος σε Ether.

- placed: Boolean που δείχνει αν το στοίχημα τοποθετήθηκε επιτυχώς.
- Το Mapping bets: Διατηρεί όλα τα στοιχήματα με ένα μοναδικό αναγνωριστικό betId για κάθε στοίχημα, που είναι ο δείκτης στη λίστα.
- Ο Μετρητής betCounter: Αυξάνεται κατά ένα κάθε φορά που τοποθετείται ένα νέο στοίχημα, εξασφαλίζοντας μοναδικά betId για κάθε στοίχημα.
- Το Event BetPlaced: Εκπέμπεται κάθε φορά που τοποθετείται ένα νέο στοίχημα, περιλαμβάνοντας το betId, τη διεύθυνση του χρήστη και το ποσό του στοιχήματος.

Συμπέρασμα: Το συμβόλαιο BetPlacement προσφέρει μια δομημένη μέθοδο τοποθέτησης και παρακολούθησης στοιχημάτων μέσω του Ethereum blockchain. Η χρήση του mapping bets επιτρέπει την αποθήκευση πολλαπλών στοιχημάτων με μοναδικά αναγνωριστικά, ενώ τα events διευκολύνουν την παρακολούθηση των συναλλαγών (βλέπε Εικόνα 2).

Όριο κατάθεσης σε μια διαδικτυακή εφαρμογή στοιχήματος (DepositLimit)

```
contract DepositLimit {
    uint256 public constant MAX_DEPOSIT_LIMIT = 50 ether;

    mapping(address => uint256) private balances;

    event Deposited(address indexed user, uint256 amount);

    function deposit() external payable {
        require(msg.value > 0, "Deposit amount must be greater than zero");
        require(msg.value <= MAX_DEPOSIT_LIMIT, "Deposit exceeds maximum limit");

        balances[msg.sender] += msg.value;
        emit Deposited(msg.sender, msg.value);
    }

    function checkBalance() external view returns (uint256) {
        return balances[msg.sender];
    }
}
```

Εικόνα 3: Όριο κατάθεσης σε μια διαδικτυακή εφαρμογή στοιχήματος (DepositLimit)

Περιγραφή της Δομής του Συμβολαίου:

- **Σταθερά (Constant):** Ορίζεται το μέγιστο όριο κατάθεσης (MAX_DEPOSIT_LIMIT = 50 ether), το οποίο δεν μπορεί να αλλάξει.
- **Mapping**: Αποθηκεύει τα υπόλοιπα των χρηστών, συνδέοντας κάθε διεύθυνση χρήστη με το ποσό που έχει καταθέσει.
- **Event**:
  - Το event Deposited καταγράφει τις καταθέσεις των χρηστών στο blockchain.
- **Συναρτήσεις**:
  - deposit(): Επιτρέπει στους χρήστες να καταθέτουν Ether, με όριο 50 ether ανά συναλλαγή.
  - checkBalance(): Επιτρέπει στους χρήστες να δουν το υπόλοιπό τους.

Η δομή του συμβολαίου παρέχει έναν ασφαλή και περιορισμένο μηχανισμό κατάθεσης Ether, με τη χρήση σταθερών, mapping και events για την καταγραφή συναλλαγών και την παρακολούθηση υπολοίπων χρηστών (βλέπε Εικόνα 3).

Ανάληψη σε μια διαδικτυακή εφαρμογή στοιχήματος Withdrawal

```
contract Withdrawal {

    mapping(address => uint256) private balances;

    event Deposited(address indexed user, uint256 amount);
    event Withdrawn(address indexed user, uint256 amount);

    function deposit() external payable {
        require(msg.value > 0, "Deposit amount must be greater than zero");

        balances[msg.sender] += msg.value;
        emit Deposited(msg.sender, msg.value);
    }

    function withdraw() external payable{
        require(msg.value > 0, "Withdraw amount must be greater than zero");
        require(balances[msg.sender] >= msg.value, "Insufficient balance");

        balances[msg.sender] -= msg.value;
        (bool success, ) = msg.sender.call{value: msg.value}("");
        require(success, "Transfer failed");

        emit Withdrawn(msg.sender, msg.value);
    }
```

Εικόνα 4: Ανάληψη σε μια διαδικτυακή εφαρμογή στοιχήματος Withdrawal

Περιγραφή της Δομής του Συμβολαίου:

Το συμβόλαιο διαχειρίζεται καταθέσεις και αναλήψεις των χρηστών με ασφάλεια, χρησιμοποιώντας ελέγχους μέσω των εντολών require για να διασφαλιστεί ότι οι χρήστες έχουν επαρκή υπόλοιπα για τις αναλήψεις τους. (βλέπε Εικόνα 4). Επίσης, τα γεγονότα βοηθούν στην παρακολούθηση των συναλλαγών καταθέσεων και αναλήψεων μέσω των λογαριασμών των χρηστών.

Το συμβόλαιο αυτό επιτρέπει στους χρήστες να καταθέτουν και να αποσύρουν Ether με ασφάλεια, χρησιμοποιώντας την ενσωματωμένη λογική και δομή του Ethereum για συναλλαγές.

Ασφαλής διαχείριση CasinoRound

```
contract CasinoRound {
    struct Round {
        uint256 startTime;
        bool isActive;
    }

    Round public currentRound;

    event RoundStarted(uint256 startTime);
    event RoundEnded(bool wasActive);

    function startRound() external {
        require(!currentRound.isActive, "A round is already in progress");

        currentRound = Round({
            startTime: block.timestamp,
            isActive: true
        });

        emit RoundStarted(currentRound.startTime);
    }

    function endRound() external {
        require(currentRound.isActive, "No active round");
        require(block.timestamp >= currentRound.startTime + 5, "Round must last at least 5
seconds");

        emit RoundEnded(currentRound.isActive);

        currentRound.isActive = false;
    }

    function getCurrentRound() external view returns (Round memory) {
        return currentRound;
    }
```

Εικόνα 5: Ασφαλης διαχειριση CasinoRound

Περιγραφή της Δομής του Συμβολαίου:

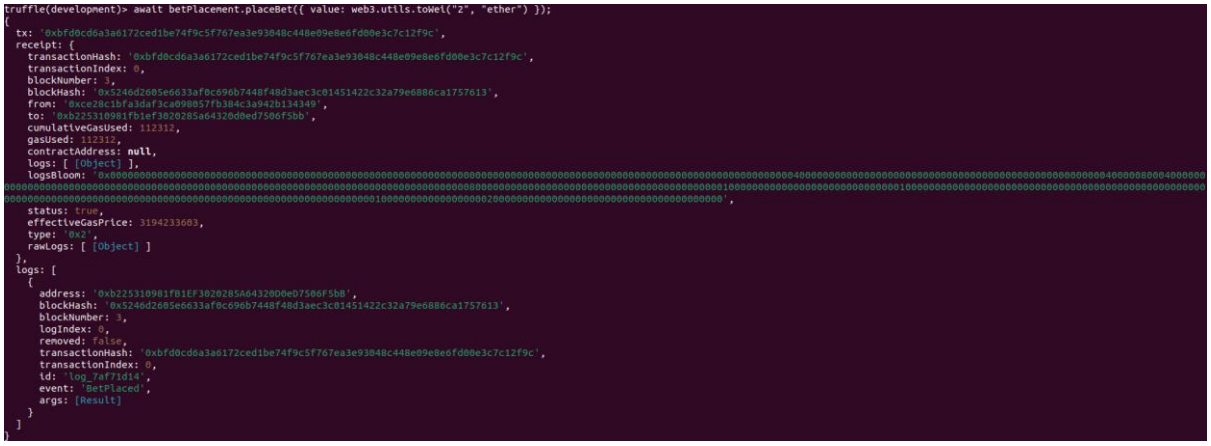
Το συμβόλαιο αυτό επιτρέπει τη διαχείριση γύρων σε ένα καζίνο, με σαφείς κανόνες για το πότε μπορεί να ξεκινήσει και να λήξει ένας γύρος.

Ένας γύρος μπορεί να ξεκινήσει μόνο αν δεν υπάρχει άλλος ενεργός γύρος και τελειώνει αφού έχουν περάσει τουλάχιστον 5 δευτερόλεπτα από την έναρξη. Τα γεγονότα βοηθούν στην καταγραφή των σημαντικών στιγμών, όπως η έναρξη και το τέλος ενός γύρου (βλέπε Εικόνα 5).

4.3 ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΜΕ ΤΑ SMART CONTRACTS

```
truffle(development)> let betPlacement = await BetPlacement.deployed();
undefined
```

Εικόνα 6: Συμβόλαιο :BetPlacement



Εικόνα 7: Ανάθεση του αντικειμένου του smart contract BetPlacement στη μεταβλητή betPlacement.

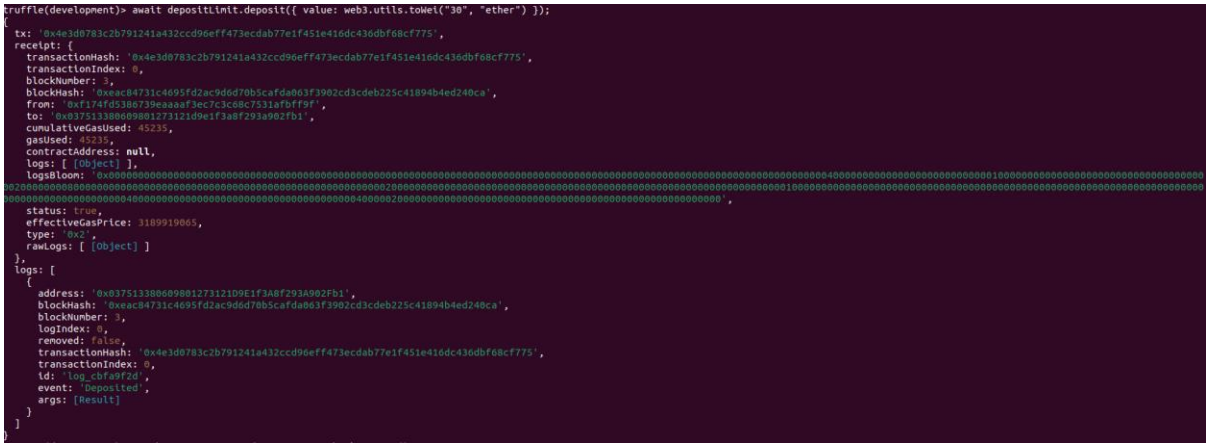
Εικόνα 8: Αλληλεπίδραση με το smart contract BetPlacement και τοποθετώ στοίχημα αξίας 2 ether.

```
truffle(development)> let bet = await betPlacement.getBet(0);
undefined
truffle(development)> console.log(bet);
[
  '0xCe28C1Bfa3DaF3cA098057FB384C3A942b134349',
  '2000000000000000000',
  true,
  user: '0xCe28C1Bfa3DaF3cA098057FB384C3A942b134349',
  amount: '2000000000000000000',
  placed: true
]
undefined
```

Εικόνα 9: Αλληλεπίδραση με το smart contract και τοποθετείται στοίχημα αξίας 5 ether. Ανάκτηση πληροφοριών του smart contract για το στοίχημα που τοποθετήθηκε.

```
truffle(development)> let depositLimit = await DepositLimit.deployed();
undefined
```

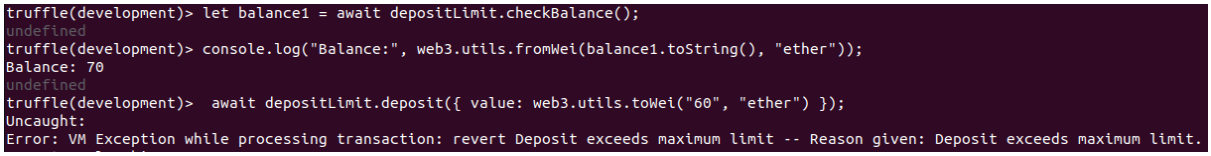
Εικόνα 10: Συμβόλαιο :DepositLimit



Εικόνα 11: Ανάθεση του αντικειμένου του smart contract DepositLimit στη μεταβλητή depositlimit.

```
truffle(development)> let balance = await depositLimit.checkBalance();
undefined
truffle(development)> console.log("Balance:", web3.utils.fromWei(balance.toString(), "ether"));
Balance: 30
undefined
```

Εικόνα 12: Ανάθεση του αντικειμένου του smart contract DepositLimit στη μεταβλητή depositlimit.



Εικόνα 13: Ανάθεση του αντικειμένου του smart contract DepositLimit στη μεταβλητή depositlimit.

Εικόνα 14: Ανάθεση του αντικειμένου του smart contract DepositLimit στη μεταβλητή depositlimit.

Εικόνα 15: Withdrawal Contract

Εικόνα 16:Withdrawal Contract

```
3_withdrawal_migration.js
=========================

   Replacing 'Withdrawal'
   ----------------------
   > transaction hash:    0x68e3862fb2c7d74e4679e33959da7cbf390a457aa9b239874a709f0da55b314c
   > Blocks: 0            Seconds: 0
   > contract address:    0x8734b2737729462adB8cBe6e6BCBF5fFea9a6EdD
   > block number:        3
   > block timestamp:     1728815985
   > account:             0x4840AD2c921567d8BeA708c4cFFE88aDE47AB0cd
   > balance:             99.996283869389429143
   > gas used:            435373 (0x6a4ad)
   > gas price:           3.189919065 gwei
   > value sent:          0 ETH
   > total cost:          0.001388804633086245 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.001388804633086245 ETH

Summary
=======
> Total deployments:   3
> Final cost:          0.003716130610570857 ETH
```

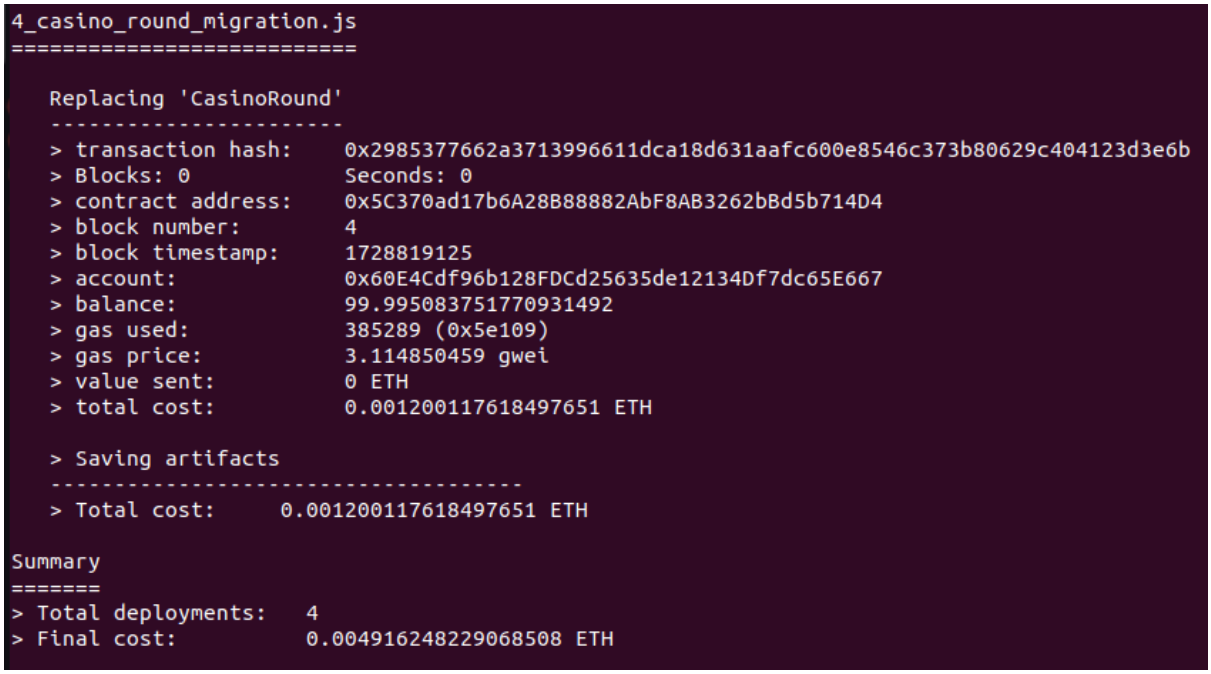
Εικόνα 17: Withdrawal Contract

Εικόνα 18: CasinoRound

Εικόνα 19: CasinoRound

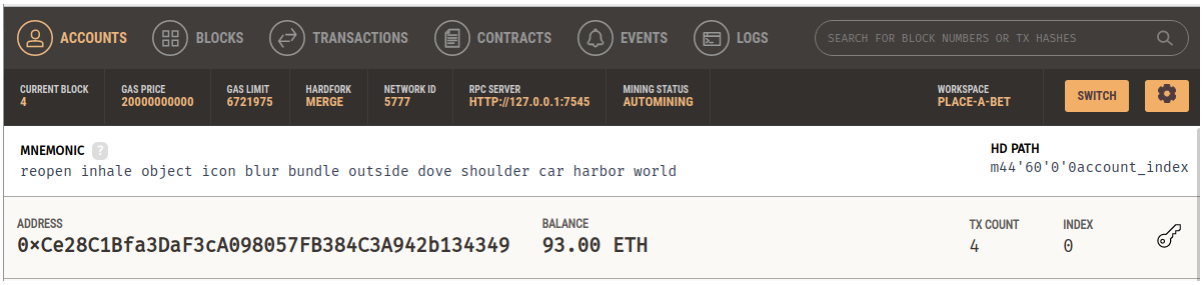
Εικόνα 20: CasinoRound

Εικόνα 21: CasinoRound



Εικόνα 22: CasinoRound

4.4 ΓΡΑΦΙΚΗ ΔΙΕΠΑΦΗ ΤΩΝ SMART CONTRACTS ΜΕΣΩ ΤΟΥ GANACHE



Εικόνα 23: Γραφική Διέπαφη των Smart Contracts μέσω του Ganache

Accounts: Η καρτέλα όπου φαίνονται οι διαθέσιμοι λογαριασμοί στο δίκτυο.

Blocks: Τα μπλοκ που έχουν δημιουργηθεί στο τοπικό blockchain, περιλαμβάνοντας πληροφορίες όπως το ύψος του μπλοκ και συναλλαγές.

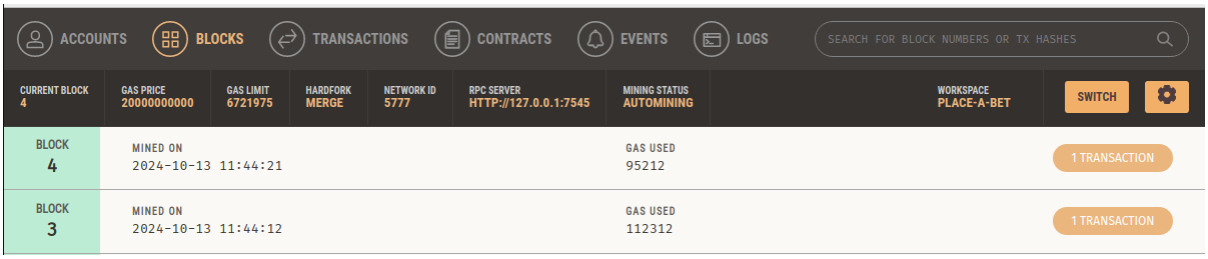
Transactions: Όλες οι συναλλαγές που έχουν πραγματοποιηθεί, με λεπτομέρειες για τον αποστολέα, τον παραλήπτη, το gas, και το ποσό.

Contracts: Διαχείρισω των έξυπνων συμβολαίων που έχουν αναπτυχθεί στο τοπικό δίκτυο.

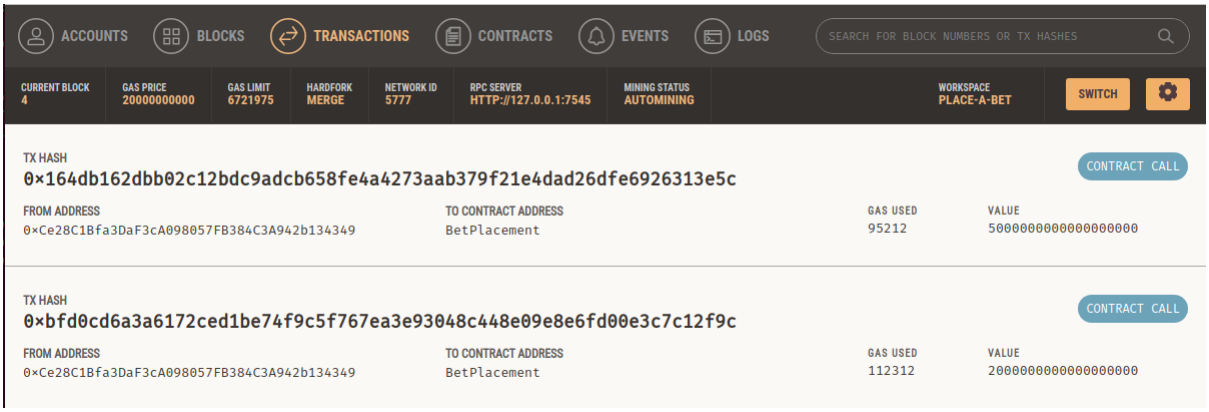
Events: Τα γεγονότα (events) που έχουν καταγραφεί από τα έξυπνα συμβόλαια που έχουν εκτελεστεί στο δίκτυο.

Logs: Τα logs των συναλλαγών και των συμβολαίων.

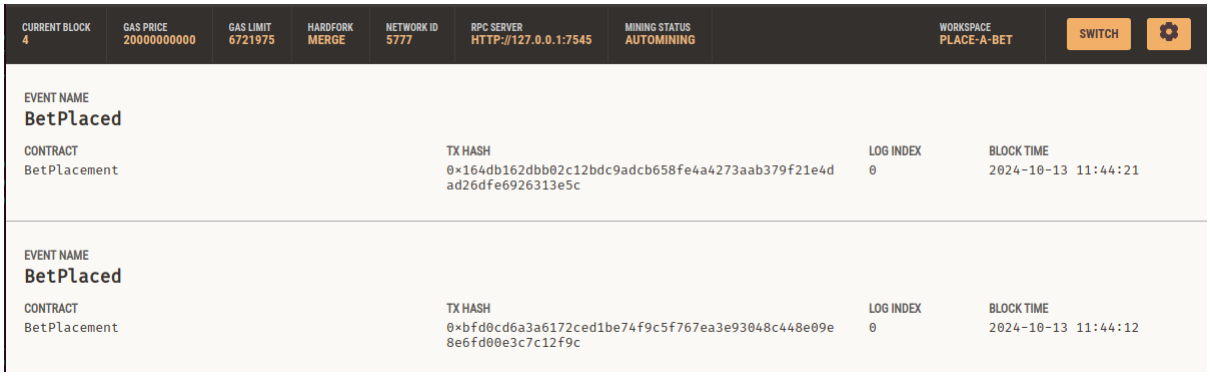
BetPlacement



Εικόνα 24: BetPlacement



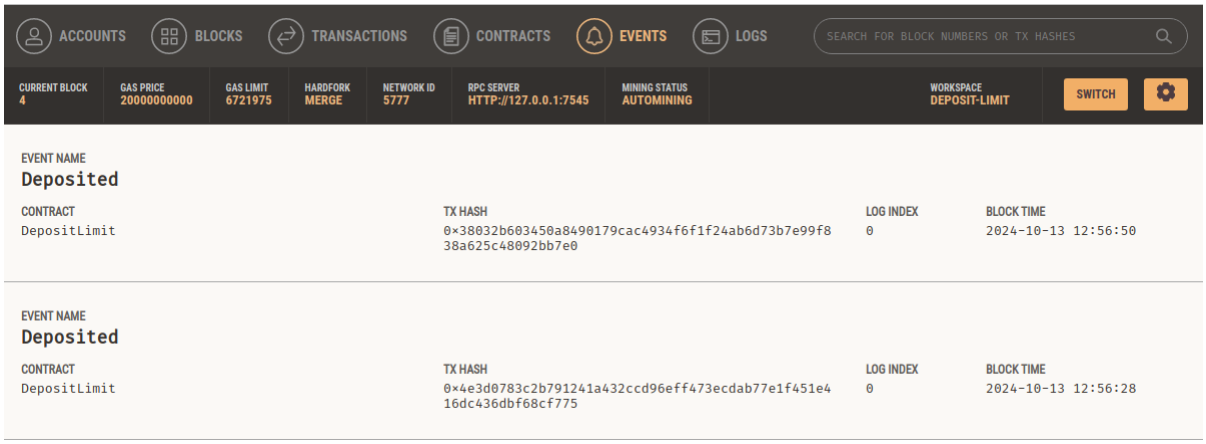
Εικόνα 25: BetPlacement



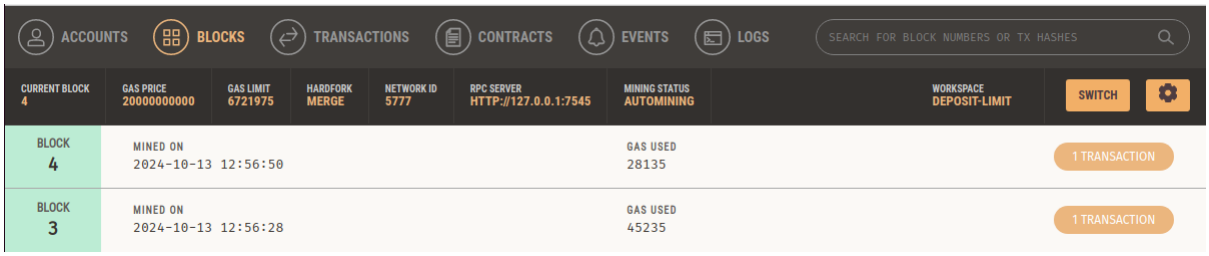
Εικόνα 26: BetPlacement

Deposit

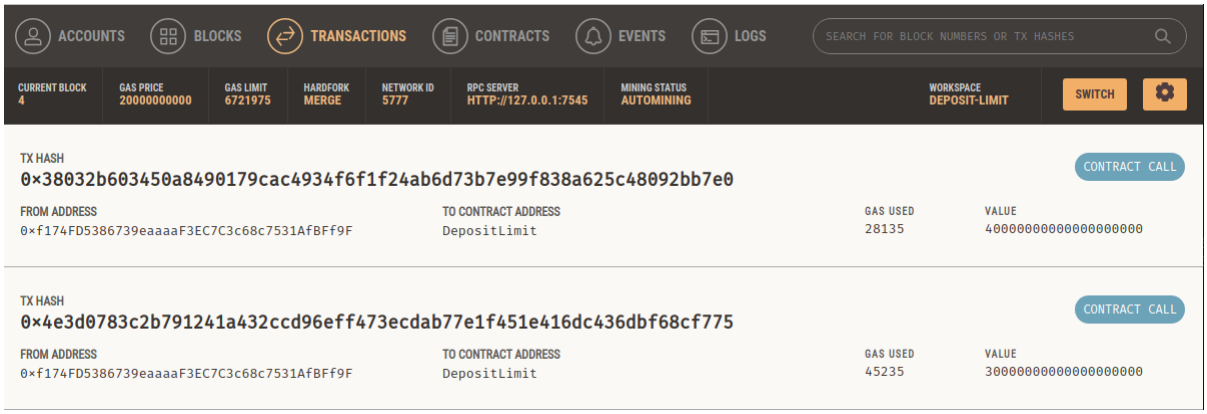
Εικόνα 27: Deposit



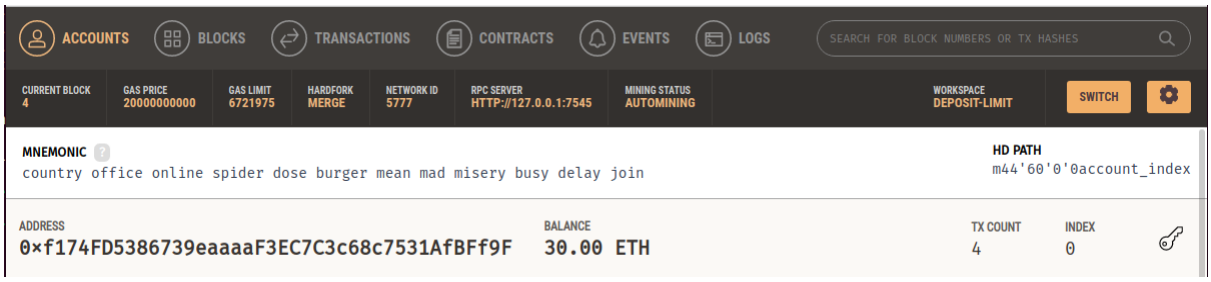
Εικόνα 28: Deposit



Εικόνα 29: Deposit

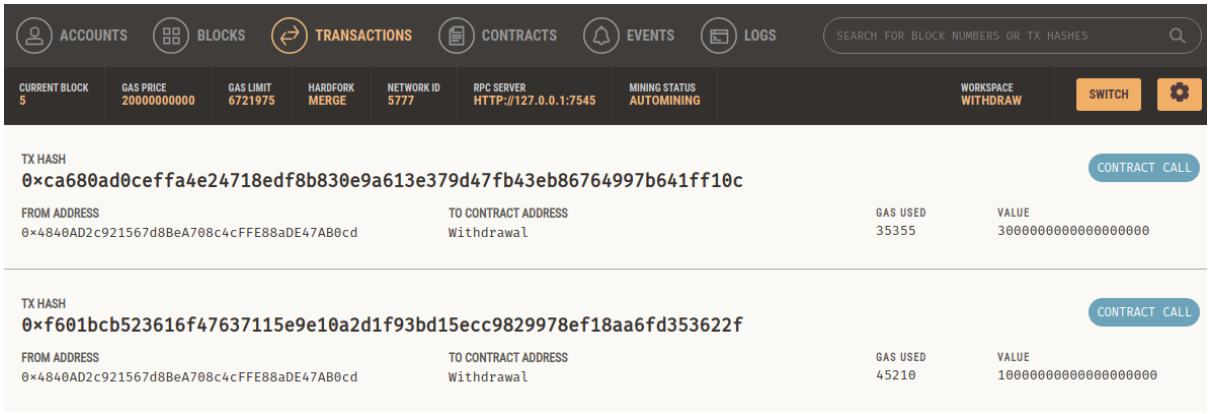


Εικόνα 30: Deposit

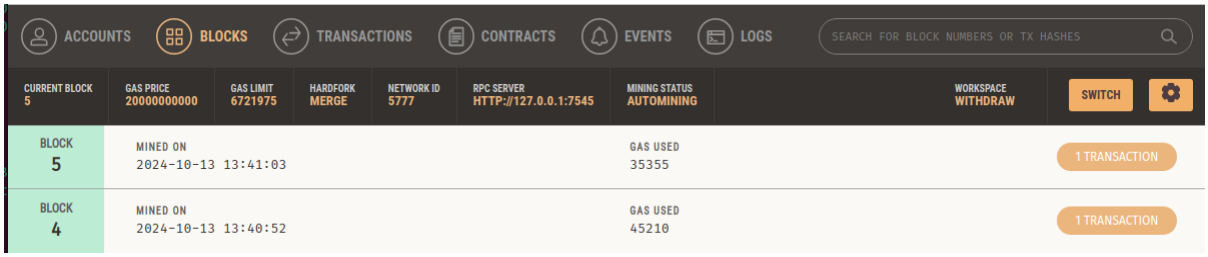


Εικόνα 31: Deposit

Withdrawal

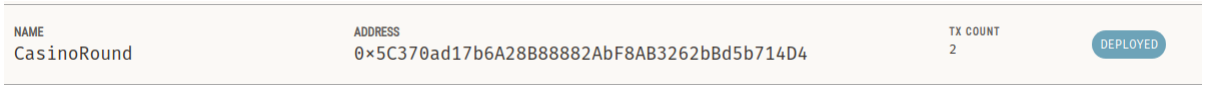


Εικόνα 32: Withdrawal

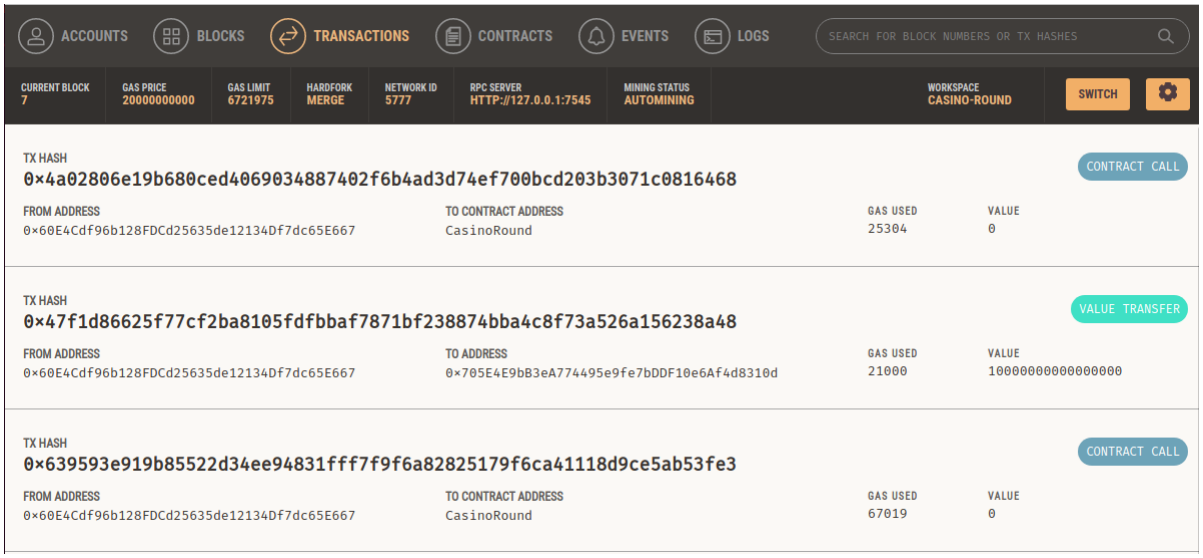


Εικόνα 33: Withdrawal

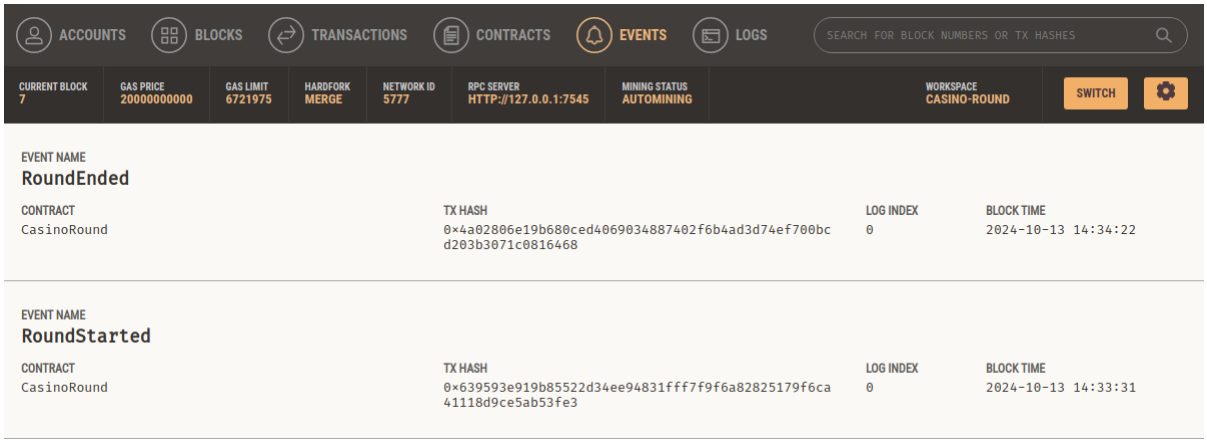
CasinoRound



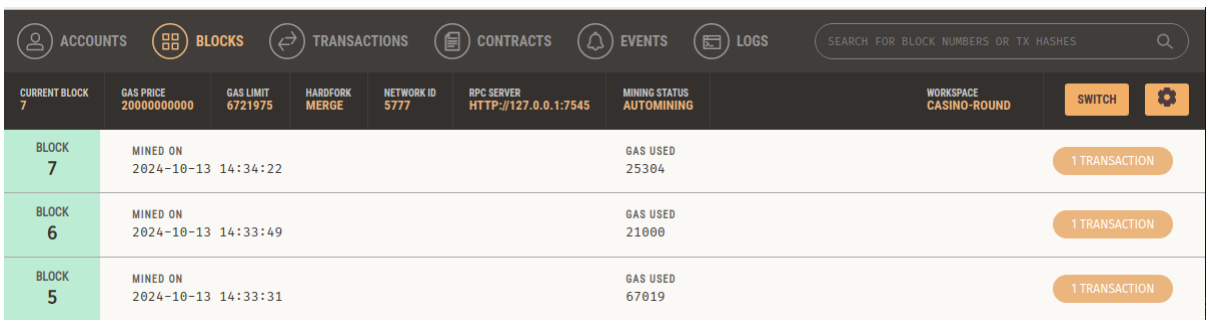
Εικόνα 34: CasinoRound



Εικόνα 35: CasinoRound



Εικόνα 36: CasinoRound



Εικόνα 37: CasinoRound

4.5 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

4.5.1Κύρια συμπεράσματα

Αυξημένη Ασφάλεια μέσω Αποκέντρωσης

Τα smart contracts παρέχουν ασφάλεια μέσω του αποκεντρωμένου χαρακτήρα τους, καθώς βασίζονται στο blockchain και εκτελούνται αυτόματα, χωρίς την ανάγκη μεσολαβητών. Αυτό μειώνει τον κίνδυνο ανθρώπινων λαθών ή παραβιάσεων από τρίτους.

Οι όροι των συμβολαίων αποθηκεύονται μόνιμα στο blockchain και δεν μπορούν να τροποποιηθούν αφού αναπτυχθούν, κάτι που διασφαλίζει τη διαφάνεια και την ακεραιότητα των επιχειρηματικών συμφωνιών.

Αποτροπή Απάτης

Η διαφάνεια του blockchain, σε συνδυασμό με την αμετάβλητη φύση των smart contracts, αποτρέπει την απάτη, αφού όλες οι πράξεις είναι δημόσια καταγεγραμμένες και επαληθεύσιμες από όλους τους εμπλεκόμενους.

Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν smart contracts για την αυτοματοποιημένη επιβολή όρων και την εκτέλεση συναλλαγών, με αποτέλεσμα να μειώνεται ο κίνδυνος από κακόβουλες συμπεριφορές.

Μείωση Ανθρώπινων Λαθών

Με τη χρήση smart contracts, οι επιχειρηματικές διαδικασίες εκτελούνται αυτόματα όταν πληρούνται οι προκαθορισμένοι όροι. Αυτό ελαχιστοποιεί την πιθανότητα λαθών ή παραλείψεων που θα μπορούσαν να προκύψουν από ανθρώπινο παράγοντα σε συμβατικές διαδικασίες.

Επιπλέον, τα έξυπνα συμβόλαια εκτελούν τις διαδικασίες χωρίς την ανάγκη διαρκούς επιτήρησης, διασφαλίζοντας την απρόσκοπτη ροή των εργασιών.

Ιχνηλασιμότητα Συναλλαγών

Όλες οι συναλλαγές μέσω smart contracts καταγράφονται μόνιμα στην αλυσίδα μπλοκ, επιτρέποντας την εύκολη παρακολούθηση και επαλήθευση. Αυτή η πλήρης ιχνηλασιμότητα ενισχύει την ασφάλεια των επιχειρηματικών διαδικασιών και δίνει στις επιχειρήσεις ένα εργαλείο για την καταπολέμηση της διαφθοράς ή την παρακολούθηση της συμμόρφωσης με κανονισμούς.

Ασφάλεια Δεδομένων

Τα smart contracts μπορούν να ενσωματώσουν κρυπτογράφηση και άλλες τεχνικές προστασίας δεδομένων, διασφαλίζοντας την προστασία των ευαίσθητων επιχειρηματικών πληροφοριών. Επειδή όλα τα δεδομένα και οι όροι είναι καταγεγραμμένα στο blockchain, οι συμμετέχοντες έχουν πρόσβαση μόνο στις απαραίτητες πληροφορίες, προστατεύοντας παράλληλα την εμπιστευτικότητα.

Ανθεκτικότητα

Τα smart contracts και το blockchain ως υποδομή είναι σχεδιασμένα για να είναι ανθεκτικά σε κυβερνοεπιθέσεις. Λόγω της αποκεντρωμένης φύσης του δικτύου, η παραβίαση ή αλλοίωση δεδομένων είναι εξαιρετικά δύσκολη, καθώς δεν υπάρχει κεντρικό σημείο αποτυχίας που θα μπορούσε να αποτελέσει στόχο επίθεσης.

Συμμόρφωση και Διακυβέρνηση

Τα smart contracts μπορούν να διασφαλίσουν ότι οι επιχειρηματικές διαδικασίες συμμορφώνονται αυτόματα με τους κανονισμούς και τους όρους που έχουν καθοριστεί, ελαχιστοποιώντας την ανάγκη για επιπρόσθετο έλεγχο ή επιτήρηση. Αυτό εξασφαλίζει ότι οι διαδικασίες ακολουθούν τα πρότυπα διακυβέρνησης και δεν υπάρχουν παρακάμψεις στους κανόνες.

4.5.2 Μελλοντικές επεκτάσεις

Η τεχνολογία των smart contracts συνεχώς εξελίσσεται και ανοίγει νέες δυνατότητες για εφαρμογές σε διάφορους τομείς. Παρά τα σημαντικά πλεονεκτήματα που προσφέρουν στον τομέα της ασφάλειας, της διαφάνειας και της αυτοματοποίησης, υπάρχουν ακόμη πολλές ευκαιρίες για βελτίωση και εξέλιξη. Στο μέλλον, η τεχνολογία αυτή μπορεί να διευρύνει τη χρήση της και να επηρεάσει πολλούς κλάδους, ενώ παράλληλα ενδέχεται να δημιουργηθούν νέες προκλήσεις και ανάγκες έρευνας. Ακολουθούν μερικά βασικά σημεία που θα μπορούσαν να αποτελέσουν κατευθύνσεις για μελλοντική ανάπτυξη:

Επέκταση σε Βιομηχανικές και Επιχειρηματικές Εφαρμογές: Τα smart contracts μπορούν να φέρουν επανάσταση σε διάφορους τομείς, όπως η εφοδιαστική αλυσίδα, οι μεταφορές και η ενέργεια. Η αυτοματοποίηση διαδικασιών μέσω έξυπνων συμβολαίων μπορεί να μειώσει σημαντικά το κόστος, να ενισχύσει την ταχύτητα των συναλλαγών και να διασφαλίσει την ακριβή παρακολούθηση των συμφωνιών σε πραγματικό χρόνο. Για παράδειγμα, στον τομέα των μεταφορών, τα smart contracts μπορούν να διαχειρίζονται αυτοματοποιημένα τις διαδικασίες πληρωμών και αποστολών, προσφέροντας μεγαλύτερη ακρίβεια και διαφάνεια.

Ανάπτυξη για Σύνθετες Συναλλαγές και Συμφωνίες: Αν και τα smart contracts ήδη χρησιμοποιούνται σε βασικές συναλλαγές, η ανάγκη για πιο σύνθετες νομικές και χρηματοοικονομικές συμφωνίες αναμένεται να ενισχυθεί. Μελλοντικά, έξυπνα συμβόλαια θα μπορούσαν να ενσωματώνουν πιο περίπλοκες ρήτρες και να υποστηρίζουν σύγχρονα χρηματοοικονομικά προϊόντα, όπως τα σύνθετα δανειακά προϊόντα, συμβόλαια ασφάλισης και άλλες επενδυτικές συμφωνίες. Η ανάπτυξη αυτών των εφαρμογών θα απαιτήσει τεχνολογικές βελτιώσεις για να εξασφαλιστεί η ευχρηστία και η νομική εγκυρότητα των έξυπνων συμβολαίων σε αυτές τις περιπτώσεις.

Συνεργασία με Τεχνολογίες Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης: Η ενσωμάτωση τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) στα smart contracts θα μπορούσε να οδηγήσει σε σημαντικές εξελίξεις. Οι τεχνολογίες αυτές θα μπορούσαν να επιτρέψουν την προσαρμογή των συμφωνιών σε πραγματικό χρόνο, βάσει μεταβαλλόμενων συνθηκών και δεδομένων. Αυτό θα έκανε τα smart contracts πιο δυναμικά και προσαρμόσιμα, επιτρέποντας την αυτοματοποιημένη λήψη αποφάσεων και την ανίχνευση κινδύνων, όπως η ενδεχόμενη απάτη ή παρατυπίες στις συναλλαγές.

Ενσωμάτωση Δεδομένων από Εξωτερικές Πηγές (Oracles): Ένα άλλο σημαντικό ζήτημα είναι η σύνδεση των smart contracts με δεδομένα από τον έξω κόσμο. Τα oracles παρέχουν εξωτερικές πληροφορίες, όπως καιρικά δεδομένα ή τιμές χρηματοοικονομικών αγαθών, που είναι αναγκαίες για την εκτέλεση των συμβολαίων. Παρά τις τεχνικές προόδους, η ανάπτυξη αξιόπιστων, ασφαλών και ακριβών oracles παραμένει πρόκληση. Η έρευνα σε αυτόν τον τομέα μπορεί να συμβάλει σημαντικά στην αύξηση της ευελιξίας και της αξιοπιστίας των έξυπνων συμβολαίων.

Βιβλιογραφία

1. Iansiti, M., & Lakhani, KR (2017). Η αλήθεια για το Blockchain. Επιχειρηματική Επιθεώρηση του Χάρβαρντ.https://hbr.org/2017/01/the-truth-about-blockchain
2. Swan, M. (2015). Blockchain: Σχέδιο για μια νέα οικονομία. O'Reilly Media.
3. Nakamoto, S. (2008). Bitcoin: Ένα Peer-to-Peer ηλεκτρονικό σύστημα μετρητών.https://bitcoin.org/bitcoin.pdf
4. Drescher, D. (2017). Βασικά στοιχεία του Blockchain: Μια μη τεχνική εισαγωγή σε 25 βήματα. Apress.
5. Buterin, V. (2013). Έξυπνο συμβόλαιο επόμενης γενιάς και αποκεντρωμένη πλατφόρμα εφαρμογών.https://github.com/ethereum/wiki/wiki/White-Paper
6. Szabo, N. (1997). Η Ιδέα των Έξυπνων Συμβάσεων.http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
7. Tapscott, D., & Tapscott, A. (2016). Επανάσταση Blockchain: Πώς η τεχνολογία πίσω από το Bitcoin αλλάζει τα χρήματα, τις επιχειρήσεις και τον κόσμο. Πιγκουίνος.
8. Kiayias, A., Russell, A., & David, B. (2016). Ouroboros: Ένα αποδεδειγμένα ασφαλές πρωτόκολλο blockchain απόδειξης στοιχήματος. Ετήσιο Διεθνές Συνέδριο Κρυπτολογίας, 357-388.
9. Engelhardt, MA (2017). Hitching Healthcare to the Chain: Μια εισαγωγή στην τεχνολογία Blockchain στον τομέα της υγειονομικής περίθαλψης. Ανασκόπηση Διαχείρισης καινοτομίας τεχνολογίας, 7(10), 22-34.
10. Peters, GW, & Panayi, E. (2016). Κατανόηση των σύγχρονων τραπεζικών λογιστικών βιβλίων μέσω τεχνολογιών blockchain: Το μέλλον της επεξεργασίας συναλλαγών και των έξυπνων συμβολαίων στο διαδίκτυο του χρήματος. Στο Banking Beyond Banks and Money (σελ. 239-278). Πηδών.
11. Pilkington, M. (2016). Τεχνολογία Blockchain: Αρχές και Εφαρμογές. In Research Handbook on Digital Transformations.
12. Castro, M., & Liskov, B. (1999). Πρακτική βυζαντινή ανοχή σφαλμάτων. Πρακτικά Τρίτου Συμποσίου Σχεδιασμού και Εφαρμογής Λειτουργικών Συστημάτων.
13. Χρηστίδης, K., & Δεβετσικιώτης, M. (2016). Blockchains και έξυπνες συμβάσεις για το Διαδίκτυο των πραγμάτων. IEEE Access, 4, 2292-2303.
14. Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). Μια έρευνα για θέματα ασφάλειας και απορρήτου του Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.
15. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Τεχνολογία Blockchain: Πέρα από το Bitcoin. Applied Innovation Review, 2, 6-19.
16. Dannen, C. (2017). Παρουσιάζοντας το Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress.
17. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). Έρευνα επιθέσεων σε έξυπνα συμβόλαια Ethereum (SoK). Πρακτικά 6ου Διεθνούς Συνεδρίου για τις Αρχές Ασφάλειας και Εμπιστοσύνης (POST), 164-186.
18. Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gordon, AD, Maffeis, S., & Pironti, A. (2016). Επίσημη επαλήθευση έξυπνων συμβολαίων. Πρακτικά του 2016 ACM SIGSAC Conference on Computer and Communications Security, 431-448.
19. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, JA, & Felten, EW (2015). SoK: Ερευνήστε προοπτικές και προκλήσεις για το Bitcoin και τα κρυπτονομίσματα. 2015 IEEE Symposium on Security and Privacy, 104-121.
20. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: Ένα κατανεμημένο λειτουργικό σύστημα για εξουσιοδοτημένες αλυσίδες μπλοκ. Πρακτικά Δέκατος τρίτου Συνεδρίου EuroSys, 1-15.
21. Αντωνόπουλος, A.M. (2017). Mastering Bitcoin: Ξεκλείδωμα ψηφιακών κρυπτονομισμάτων. O'Reilly Media.

22. Buterin, V. (2018). Vyper: Μια γλώσσα που εστιάζει στην ασφάλεια για το Ethereum. Ιστολόγιο του Ιδρύματος Ethereum.
23. Haber, S., & Stornetta, WS (1991). Τρόπος χρονοσήμανσης ενός ψηφιακού εγγράφου. Journal of Cryptology, 3(2), 99-111.
24. Harvey, CR, Ramachandran, A., & Santoro, J. (2021). Το DeFi και το μέλλον των οικονομικών. Ηλεκτρονικό Περιοδικό SSRN.
25. IOHK. (2017). Plutus: Η έξυπνη πλατφόρμα συμβάσεων για το Cardano.https://iohk.io/research/papers/#plutus-the-smart-contract-platform-for-cardano
26. King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency με απόδειξη στοιχήματος. https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf
27. Larimer, D. (2014). Εξουσιοδοτημένη απόδειξη συμμετοχής (DPoS). Λευκή Βίβλος Bitshares.
28. Douceur, JR (2002). Η επίθεση στη Σίμπιλ. International Workshop on Peer-to-Peer Systems, 251-260.
29. Ellis, S., Juels, A., & Nazarov, S. (2017). ChainLink: Ένα αποκεντρωμένο δίκτυο μαντείου. https://link.smartcontract.com/whitepaper
30. Finck, M. (2018). Κανονισμός και Διακυβέρνηση Blockchain στην Ευρώπη. Cambridge University Press.
31. Goodman, L. (2014). Tezos — ένα Self-Amending Crypto-Ledger.https://tezos.com/static/papers/white_paper.pdf
32. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs Proof-of-Authority: Εφαρμογή του Θεωρήματος CAP σε Permissioned Blockchain. Ιταλική Διάσκεψη για την Ασφάλεια στον Κυβερνοχώρο (ITASEC).
33. Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Βήμα προς βήμα προς τη δημιουργία ενός ασφαλούς έξυπνου συμβολαίου: Μαθήματα και γνώσεις από ένα εργαστήριο κρυπτονομισμάτων. Χρηματοοικονομική Κρυπτογραφία και Ασφάλεια Δεδομένων, 79-94.
34. Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). Μια Ταξονομική Προσέγγιση για την Κατανόηση των Αναδυόμενων Συστημάτων Διαχείρισης Ταυτότητας Blockchain. Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας.
35. Luu, L., Chu, DH, Olickel, H., Saxena, P., & Hobor, A. (2016). Κάνοντας τα έξυπνα συμβόλαια πιο έξυπνα. Πρακτικά του 2016 ACM SIGSAC Conference on Computer and Communications Security, 254-269.
36. Merkle, RC (1980). Πρωτόκολλα για κρυπτοσυστήματα δημόσιου κλειδιού. Συμπόσιο IEEE για την ασφάλεια και το απόρρητο.
37. Merkle, RC (1980). Πρωτόκολλα για κρυπτοσυστήματα δημόσιου κλειδιού. Συμπόσιο IEEE για την ασφάλεια και το απόρρητο.
38. Cassano, J. (2014). Smart contracts could be cryptocurrencys killer app. Hentet fra Fastcolabs.com: http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys- killer-app
39. Coinprism. (2015). Openchain. Hentet fra Openchain: https://www.openchain.org/
40. Cortis, D. (2015). Expected values and variances in bookmaker payouts: A theoretical approach towards setting limits on odds. The journal of predicting markets, s. 1-14.
41. Danova, H. (2015). what is bitcoin fork. Hentet fra CEX IO Blog: http://blog.cex.io/bitcoin-dictionary/what- is-bitcoin-fork-14622
42. Giancarlo Daniele, A. O. (2011). Bitcoin - Decentralized, Peer-to-Peer, Cryptocurrency. Hentet fra Stanford.edu: http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/DigitalCurrencies/disadvantages/index.html
43. Hobson, D. (2013). What is Bitcoin? XRDS, s. 40-44.
44. Rob Gleasure, J. F. (2012). Procedurally transparent design Science research: A design process model. Thirty Third International Conference on Information Systems.
45. Shirley Gregor, A. R. (2013). Positioning and presenting design science research for maximum impact. MiS Quarterly Vol. 37, 337-355.

46. State of the DApps. (2016). Hentet fra http://dapps.ethercasts.com/
47. Sull, D. (2009 Vol. 87). How to thrive in turbulent markets. Harvard Business Review. Szabo, N. (1994). Smart Contracts. s. http://szabo.best.vwh.net/smart.contracts.html.
48. Taylor, S. (2015). Blockchain: understanding the potential. Barclays.