ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ & ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Know-Your-Employee: Μια αποκεντρωμένη εφαρμογή αντιστοίχισης δεδομένων εργαζομένων σε NFT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεόδωρος Παπαγεωργίου

Επιβλέπουσα: Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π

Αθήνα, Οκτώβριος 2024

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ & ΣΥΣΤΗΜΑΤΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ

Know-Your-Employee: Μια αποκεντρωμένη εφαρμογή αντιστοίχισης δεδομένων εργαζομένων σε NFT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεόδωρος Παπαγεωργίου

Επιβλέπουσα: Θεοδώρα Βαρβαρίγου
Καθηγήτρια Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 17η Οκτωβρίου 2024.

.....	.....	.....
Θεοδώρα Βαρβαρίγου	Συμεών Παπαβασιλείου	Εμμανουήλ Βαρβαρίγος
Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2024

.....
Θεόδωρος Δ. Παπαγεωργίου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Στην εποχή της πληροφορίας, η αύξηση των φαινομένων πλαστογραφίας και ηλεκτρονικής απάτης αποτελεί σημαντικό πρόβλημα και κίνδυνο για τις σύγχρονες κοινωνίες. Είναι, λοιπόν, αναγκαία η διασφάλιση της διαφάνειας και της εγκυρότητας των δεδομένων που ανεβαίνουν και ανταλλάσσονται στο διαδίκτυο ή σε άλλα επιμέρους δίκτυα. Η παρούσα διπλωματική εργασία πραγματεύεται τη δημιουργία μιας αποκεντρωμένης εφαρμογής με σκοπό την κατοχύρωση και εξασφάλιση της αξιοπιστίας δεδομένων που ανήκουν σε εργαζόμενους ή άτομα που αναζητούν εργασία. Αυτό επιτυγχάνεται με την έκδοση ενός κρυπτοπαραστατικού (Non Fungible Token ή NFT) για κάθε εργαζόμενο. Συγκεκριμένα, ένας ορισμένος από την κυβέρνηση ελεγκτικός φορέας συμπληρώνει τα πεδία με τα στοιχεία του ενδιαφερόμενου και ανεβάζει τα απαιτούμενα αρχεία στο προσκήνιο (front-end) της εφαρμογής. Εμπνευσμένοι από την ήδη εδραιωμένη αποθήκευση δεδομένων πελατών χρηματοοικονομικών συστημάτων που είναι ευρέως γνωστά ως KYC (Know Your Customer) δεδομένα, ονομάζουμε τα δεδομένα που διαχειρίζεται η εφαρμογή μας KYE (Know Your Employee). Για να επιτευχθεί η αποκέντρωση της εφαρμογής μας το παρασκήνιο (back-end) είναι στην πλειοψηφία του γραμμένο με τη μορφή ενός έξυπνου συμβολαίου. Οι μέθοδοι του έξυπνου συμβολαίου εκτελούνται εντός ενός περιβάλλοντος αλυσίδας-κορμού (blockchain) Ethereum. Ο αρχικός κόμβος του δικτύου είναι ο ελεγκτικός φορέας ενώ στο δίκτυο εντάσσονται οι εργαζόμενοι (υποψήφιοι ή μη) καθώς και ενδιαφερόμενες επιχειρήσεις. Χάρη στην αμεταβλητότητα και την ασφάλεια που διέπουν τις συναλλαγές σε ένα δίκτυο blockchain, η εφαρμογή εξασφαλίζει την επαλήθευση της ταυτότητας των εργαζομένων, τη δυνατότητα ελέγχου του ιστορικού τους και την επιβεβαίωση των πιστοποιήσεών τους. Για να έχουν πρόσβαση οι επιχειρήσεις στα δεδομένα του εκάστοτε εργαζομένου θα πρέπει να πληρώσουν ένα προκαθορισμένο αντίτιμο. Το ποσό αυτό μεταφέρεται εξ ολοκλήρου στον εργαζόμενο στον οποίον ανήκουν τα δεδομένα. Η ενσωμάτωση αυτής της νομισματοποίησης αποτελεί κίνητρο για την ανάρτηση των δεδομένων από τους εργαζόμενους. Παράλληλα, τα δεδομένα αυτά αποθηκεύονται κρυπτογραφημένα σε ένα Διαπλανητικό Σύστημα Αρχείων (IPFS) ενώ στο blockchain αποθηκεύεται μόνο ο σύνδεσμος που οδηγεί σε αυτά. Με τον τρόπο αυτό διασφαλίζεται η ικανότητα κλιμάκωσης της εφαρμογής.

Λέξεις κλειδιά: περιβάλλον αλυσίδας-κορμού, κρυπτοπαραστατικό, ιδιωτικότητα, προστασία δεδομένων, έξυπνο συμβόλαιο, νομισματοποίηση, αποκεντρωμένη εφαρμογή, KYE, Διαπλανητικό Σύστημα Αρχείων (IPFS), κρυπτογράφηση

Abstract

In the information age, the rise of forgery and electronic fraud poses a significant problem and threat to modern societies. It is therefore essential to ensure the transparency and validity of the data uploaded and exchanged on the internet or other networks. This thesis deals with the creation of a decentralized application aimed at securing and ensuring the reliability of data belonging to employees or job seekers. This is achieved through the issuance of a Non-Fungible Token (NFT) for each employee. Specifically, a government-appointed auditing body fills in the fields with the interested party's details and uploads the required files to the application's front-end. Inspired by the already established data storage systems in financial systems, commonly known as KYC (Know Your Customer) data, we call the data managed by our application KYE (Know Your Employee). To achieve the decentralization of our application, most of the back-end is written in the form of a smart contract. The methods of the smart contract are executed within an Ethereum blockchain environment. The initial node of the network is the auditing body, and employees (whether candidates or not), as well as interested businesses, join the network. Thanks to the immutability and security governing transactions on a blockchain network, the application ensures the verification of employees' identities, the ability to check their history, and the confirmation of their certifications. For businesses to access an employee's data, they must pay a predetermined fee. This amount is transferred entirely to the employee who owns the data. The integration of this monetization serves as an incentive for employees to upload their data. At the same time, this data is encrypted and stored in an InterPlanetary File System (IPFS), while only the link to this data is stored on the blockchain. This ensures the scalability of the application.

Keywords: blockchain, Non-Fungible Token (NFT), privacy, data protection, smart contract, monetization, decentralized application, KYE (Know Your Employee), InterPlanetary File System (IPFS), cryptography

Ευχαριστίες

Με την παρούσα διπλωματική εργασία ολοκληρώνονται οι σπουδές μου στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Πρωτίστως, θα ήθελα να ευχαριστήσω όλους τους καθηγητές που στην συνολική μου εκπαιδευτική πορεία με εφοδίασαν με το σύνολο των γνώσεων που κατέχω.

Ιδιαίτερα επιθυμώ να ευχαριστήσω την Καθηγήτρια ΕΜΠ, κα. Βαρβαρίγου και επιβλέπουσα της παρούσας Διπλωματικής Εργασίας, για την εμπιστοσύνη και ευκαιρία που μου έδωσε να αναπτύξω ένα τόσο ενδιαφέρον θέμα. Επιπλέον, θα ήθελα να ευχαριστήσω τον ερευνητή Αντώνιο Λίτκε για τη βοήθεια και καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια της εργασίας.

Τέλος, ευχαριστώ ιδιαίτερα τους γονείς μου, Δήμο και Χαρά, τις αδερφές μου Κατερίνα και Νικολέττα και τους φίλους μου που στάθηκαν δίπλα μου όλα αυτά τα χρόνια.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος Διαγραμμάτων

Κατάλογος Συντμήσεων

NFT	Non-Fungible Token
KYC	Know Your Customer
eKYC	electronic Know Your Customer
KYE	Know Your Employee
VASPS	Virtual Asset Providers
FI	Financial Institution
IoT	Internet of Things
GHOST	Greedy Heaviest Observed Subtree
EVM	Ethereum Virtual Machine
EIP	Ethereum Improvement Proposals
IP	Intellectual Property
DApp	Decentralized App
AES	Advanced Encryption Standard
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
USB	Universal Serial Bus
VPN	Virtual Private Network
PoS	Proof of Stake
PoH	Proof of History
UI	User Interface
Geth	Go Ethereum
CLI	Command Line Interface
HTML	HyperText Markup Language
CSS	Cascading Style Sheets
API	Application Programming Interface
IPC	Inter-Process Communication
SHA	Secure Hash Algorithm
IPFS	Interplanetary File System
CID	Content Identifier
ID	Identity
PDF	Portable Document Format
TVL	Total Value Locked
BLOB	Binary Large Object
FIPS	Federal Information Processing Standard
ΚΕΠ	Κέντρο Εξυπηρέτησης Πολιτών

1 Εισαγωγή

Με την αύξηση της δημοφιλίας των ηλεκτρονικών συναλλαγών αυξήθηκαν και τα περιστατικά απάτης. Η πλαστογράφηση προσωπικών στοιχείων και οι κυβερνοεπιθέσεις μπορούν να οδηγήσουν σε απώλεια μεγάλου ποσού χρημάτων για έναν ή και περισσότερους οργανισμούς ή ιδιώτες. Συγκεκριμένα, στα πλαίσια των τραπεζικών συστημάτων καταγράφονται εκατοντάδες υποκλοπές χρημάτων τα τελευταία έτη [1]. Ταυτόχρονα, τα ποσά αυτά συνήθως χρηματοδοτούν παράνομες δραστηριότητες όπως πώληση λαθραίων προϊόντων, ληστείες, απαγωγές, δολοφονίες και δραπετεύσεις.

Η απάντηση των τραπεζών στα προβλήματα αυτά είναι πολύπλευρη. Ωστόσο, μία από τις πιο υποσχόμενες λύσεις που αναδύεται τα τελευταία χρόνια είναι η ενσωμάτωση τεχνολογιών blockchain στα τραπεζικά συστήματα και η σύσταση υπηρεσιών KYC. Με τη χρήση των KYC δεδομένων στον χρηματοοικονομικό τομέα μπορούν να αποφευχθούν οικονομικά εγκλήματα και περιπτώσεις ξεπλύματος χρημάτων χάρη στην αξιοπιστία και την διαφάνεια των δεδομένων που εξασφαλίζεται.

Δεν είναι τυχαίο ότι την περίοδο συγγραφής της παρούσας διπλωματικής προτείνεται νέο μέτρο από την κυβέρνηση της Ελλάδος που προσφέρει τη δυνατότητα παροχής KYC υπηρεσιών στις τράπεζες σε συνεργασία με την Εθνική βάση δεδομένων προσωπικών στοιχείων (gov) [2],[3].

Η πλαστογραφία αποτελεί ένα σοβαρό κοινωνικό και νομικό πρόβλημα που δεν συναντάται μόνο στον χρηματοοικονομικό τομέα. Στον τομέα της εκπαίδευσης, η πλαστογραφία πτυχίων ή άλλων πιστοποιητικών μπορεί να υπονομεύσει την αξιοπιστία των εκπαιδευτικών ιδρυμάτων. Η χρήση τους δε στερεί μόνο ευκαιρίες σε θέσεις εργασίας, σπουδές και υποτροφίες από ανθρώπους που εργάζονται σκληρά για να πετύχουν τους στόχους τους, αλλά μπορεί να οδηγήσει σε τραυματισμό ή ακόμα και θάνατο. Αρκετές είναι οι ειδήσεις που έχουν προβληθεί στα ελληνικά μέσα ενημέρωσης για ανθρώπους που χειρουργούσαν ασθενείς χωρίς να έχουν καν πτυχίο από την Ιατρική Σχολή [4]. Επιπλέον, στις περισσότερες χώρες υπάρχουν αυστηρές προϋποθέσεις (πχ λευκό ποινικό μητρώο) που πρέπει να τηρούνται σε θέσεις εργασίας που έχουν άμεση επαφή με παιδιά και άλλες ευαίσθητες κοινωνικές ομάδες.

Από τα παραπάνω, είναι φανερό ότι είναι επιτακτική η ανάγκη για την άμεση και έγκυρη επαλήθευση όλων των στοιχείων των υποψηφίων υπαλλήλων πριν την πρόσληψή τους στον Ιδιωτικό ή τον Δημόσιο τομέα.

1.1 Σκοπός Εργασίας

Η παρούσα εργασία πραγματεύεται την ανάπτυξη μιας αποκεντρωμένης εφαρμογής (decentralized app) βασισμένης σε δίκτυο αλυσίδας-κορμού Ethereum (Ethereum blockchain). Κύριος στόχος της εφαρμογής είναι να επιτρέπει στους χρήστες της να διαχειρίζονται δεδομένα υπό πλήρη ασφάλεια και μυστικότητα, αλλά και με πλήρη διαφάνεια και αξιοπιστία. Συγκεκριμένα, εντός του δικτύου όλοι οι χρήστες μπορούν – εάν επιθυμούν - να αιτηθούν την κοπή (mint) ενός μη-εναλλάξιμου κρυπτοπαραστατικού (non-fungible token ή NFT), το οποίο μετά την κοπή θα τους ανήκει. Ορισμένοι χρήστες που έχουν δικαίωμα κοπής (minters), μπορούν να κόψουν NFT και να ορίσουν τον ιδιοκτήτη που αιτήθηκε την κοπή του.

Με το κόψιμο (minting) ενός NFT, ο χρήστης που ορίζεται ως ιδιοκτήτης του, αναρτά στο δίκτυο Blockchain κάποια υψηλής σημασίας δεδομένα του, υπό κρυπτογραφημένη μορφή. Ο ίδιος μετά την ολοκλήρωση της κοπής λαμβάνει και το μοναδικό κλειδί που μπορεί να χρησιμοποιηθεί για να αποκαλυφθούν τα δεδομένα του. Επιπλέον, κερδίζει κάποια κρυπτονομίσματα λόγω της ανάρτησης των δεδομένων του στο δίκτυο. Πριν εξηγηθεί η υπόλοιπη λειτουργικότητα της εν λόγω εφαρμογής, είναι σκόπιμο να γίνει λόγος για το είδος των δεδομένων που αναρτώνται στο blockchain με τη χρήση της.

Τα δεδομένα που αναρτώνται από τους χρήστες που το επιθυμούν ονομάζονται δεδομένα Know-Your-Employee (KYE). Θυμίζουν την περίπτωση των δεδομένων Know-Your-Customer (KYC), τα οποία απαντώνται συχνά στη βιβλιογραφία όπως φαίνεται και στην παράγραφο 1.2. Η διαφορά είναι ότι δεν αποτελούν απλώς κάποια γενικά προσωπικά στοιχεία για τον χρήστη που τα αναρτά, αλλά περιγράφουν το εργασιακό προφίλ του. Εν ολίγοις, τα δεδομένα αυτά περιλαμβάνουν την προηγούμενη εργασιακή του εμπειρία, τις σπουδές του, τα έργα στα οποία έχει συμμετάσχει κλπ.

Όταν ο χρήστης αναρτά τα KYE δεδομένα του στο blockchain, αυτά παγιώνονται και η συναλλαγή καταγράφεται ονομαστικά και αμετάβλητα. Τα πιστοποιητικά και τα έγγραφα που συνοδεύουν το κείμενο που αναρτά είναι και αυτά αμετάβλητα και οποιαδήποτε αλλαγή σε αυτά καταγράφεται ως συναλλαγή στο blockchain. Η εκτέλεσή της κάθε συναλλαγής είναι εμφανής στους χρήστες του δικτύου.

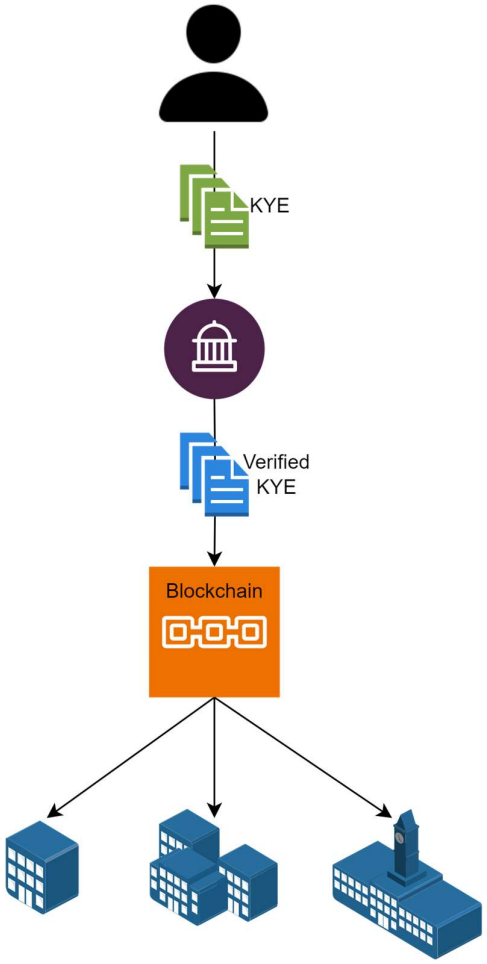
Επομένως, αν μια εταιρεία επιθυμεί να μάθει το επαγγελματικό ιστορικό ενός υποψήφιου εργαζομένου της ή αν ένα πανεπιστήμιο επιθυμεί να εξετάσει την ακαδημαϊκή δραστηριότητα ενός υποψήφιου μεταπτυχιακού φοιτητή, δεν έχει παρά να εισέλθει στο δίκτυο και να ζητήσει από τον εν λόγω χρήστη το μοναδικό κλειδί που δίνει πρόσβαση στα δεδομένα του. Αν ο χρήστης το επιθυμεί, αποκαλύπτει το κλειδί στον ενδιαφερόμενο φορέα που το αιτήθηκε (εταιρεία, πανεπιστήμιο κλπ) και έτσι ο φορέας αποκτά πρόσβαση στα δεδομένα.

Η είσοδος λοιπόν, στην αποκεντρωμένη εφαρμογή και, επομένως, στο δίκτυο blockchain στο οποίο η ίδια στηρίζεται, είναι ωφέλιμη και για τους εργαζόμενους, αλλά και για τις ίδιες τις εταιρείες, τα πανεπιστήμια ή άλλους φορείς που απαιτούν προσωπικό για να λειτουργήσουν. Οι μεν εργαζόμενοι επωφελούνται με τρεις τρόπους:

1. Η ανάρτηση των KYE δεδομένων τους στο δίκτυο αμείβεται με νομίσματα ether.
2. Η ανάρτηση του επαγγελματικού ιστορικού τους με τη μορφή KYE δείχνει ότι δεν έχουν να κρύψουν τίποτα και ότι αποδέχονται την πλήρη διαφάνεια.
3. Τα εργασιακά τους δεδομένα είναι κρυπτογραφημένα στο δίκτυο και αποκαλύπτονται μόνο στους φορείς στους οποίους οι ίδιοι επιθυμούν να τα αποκαλύψουν, με την αποστολή του μοναδικού κλειδιού που τους αντιστοιχεί.

Οι δε εταιρείες και φορείς επωφελούνται με το να έχουν πρόσβαση σε έγκυρα και έμπιστα δεδομένα του υποψήφιου προσωπικού τους, αποφεύγοντας τις κακόβουλες ενέργειες όπως αποκρύψεις και πλαστογραφίες.

Επιστρέφοντας στην λειτουργία και τον σκοπό της εφαρμογής, εν συντομία, η ίδια επιτρέπει στους κόμβους-μέλη του δικτύου που δημιουργεί να ανταλλάσσουν δεδομένα σχετικά με το επαγγελματικό τους ιστορικό μέσω κοπής NFT. Επομένως, οι συναλλαγές αυτές καταγράφονται και τα δεδομένα είναι αδιάβλητα μέσω των διαδικασιών εξασφάλισης πιστότητας του blockchain. Να σημειωθεί ότι την είσοδο των φορέων και των εργαζομένων στο δίκτυο, την εγκυρότητα των δεδομένων πριν την πρώτη ανάρτησή τους, καθώς και το δικαίωμα κοπής NFT, καθορίζει ένας τρίτος φορέας, ο οποίος θα μπορούσε να είναι κάποιο κρατικό όργανο ή η εταιρεία-συντηρητής της εφαρμογής.



Εικόνα 1-1 Συνοπτική παρουσίαση της Ιδέας

1.2 Βιβλιογραφική Ανασκόπηση

Τα τελευταία χρόνια όσο αναπτύσσονται οι ηλεκτρονικές συναλλαγές τόσο σημαντικότερη γίνεται η διασφάλιση και η επαλήθευση των δεδομένων για να αποφευχθούν οικονομικά και όχι μόνο εγκλήματα. Σύμφωνα με τις Patil και M. Sangeetha η επαλήθευση KYC είναι κρίσιμη για την αποτροπή χρήσης των τραπεζών από κακόβουλα άτομα, για δραστηριότητες όπως το ξέπλυμα χρήματος, η διακίνηση ναρκωτικών, η τρομοκρατία και άλλα εγκλήματα. Οι συγγραφείς του [5] προτείνουν μια αποκεντρωμένη διαδικασία επαλήθευσης KYC σε Ethereum blockchain, στην οποία όλες οι τράπεζες του δικτύου μπορούν να επαληθεύουν και να ψηφίζουν για τη νομιμότητα των δεδομένων που παρέχει ο πελάτης, αλλά και να ψηφίζουν ποιές τράπεζες αποσκοπούν στην αλλοίωση των δεδομένων KYC. Εφόσον υπερψηφιστούν ως έγκυρα και νόμιμα τα δεδομένα του πελάτη, αυτά αποθηκεύονται στο blockchain. Αντίστοιχα όποια τράπεζα ψηφιστεί ότι παρακινεί και επιβεβαιώνει παράνομα και λανθασμένα δεδομένα θα αφαιρείται από το blockchain [5].

Η χρήση δεδομένων Know-Your-Cutomer (KYC) από χρηματοπιστωτικά ιδρύματα (π.χ. τράπεζες) έχει διευρυνθεί σημαντικά τα τελευταία χρόνια, σε μια έντονη προσπάθεια των ιδρυμάτων αυτών να διατηρούν αξιόπιστα δεδομένα για τους πελάτες τους στις βάσεις τους και να θεμελιώνουν μια επιχειρηματική σχέση εμπιστοσύνης με αυτούς [6]. Στο παρελθόν για να επιτευχθεί αυτό ήταν απαραίτητο τα χρηματοπιστωτικά ιδρύματα (Financial Institutions ή FI), όπως οι τράπεζες, να επαληθεύουν τις ταυτότητες και να ελέγχουν τις συναλλακτικές συμπεριφορές των πελατών τους, για να διευκολύνουν την ανίχνευση ύποπτων δραστηριοτήτων (π.χ. ξέπλυμα χρήματος). Τυπικές εφαρμογές συμμόρφωσης με το KYC απαιτούσαν από τους πελάτες να παρέχουν πληροφορίες αυτοπροσώπως σε κάθε ένα από τα χρηματοπιστωτικά ιδρύματα με τα οποία συνεργάζονταν. Αλλιώς, μεσολαβούσε μια τρίτη επιχείρηση-εγγυητής που επικύρωνε τα δεδομένα μέσω χρονοβόρων και συχνά κοστοβόρων διαδικασιών. Το ίδιο ίσχυε και για την επακόλουθη ενημέρωση των δεδομένων τους, όσο διαρκούσε η επιχειρηματική τους σχέση με τα χρηματοπιστωτικά ιδρύματα [7].

Με την άνθιση του νέου πρότυπου διαδικτύου Web3.0 και την ενσωμάτωση των τεχνολογιών αλυσίδας κορμού σε πληθώρα εφαρμογών της καθημερινότητας, η ιδέα ότι η επικύρωση της αξιοπιστίας των δεδομένων KYC μπορεί να βελτιωθεί με την αξιοποίηση τεχνολογιών blockchain έχει εδραιωθεί πλήρως στην βιβλιογραφία [8]. Τα NFTs έχουν εμπλακεί σε αυτήν την εξίσωση, κυρίως με διαφορετικό τρόπο από αυτόν που θα παρουσιάσουμε στην παρούσα εργασία. Δηλαδή, οι περισσότεροι ερευνητές επιχειρούν είτε να χρησιμοποιήσουν τα δεδομένα KYC για να παρέχουν ασφάλεια στους παρόχους ψηφιακών περιουσιακών στοιχείων (Virtual Asset Providers ή VASPS) [9] είτε να εξασφαλίσουν ότι τα πνευματικά δικαιώματα των καλλιτεχνών που δημιουργούν κομμάτια ψηφιακής τέχνης και τα ενσωματώνουν σε NFTs [10] [11].

Η έκδοση των ίδιων των NFT με σκοπό την αποθήκευση δεδομένων KYC σε δίκτυα αλυσίδας κορμού - πράγμα που αποτελεί και βασικό στοιχείο της παρούσας εργασίας - δεν φαίνεται να αποτελεί θέμα εκτεταμένης μελέτης προς το παρόν. Παρ' όλα αυτά υπάρχουν ερευνητές και επιχειρήσεις που αναφέρουν ρητά την εν λόγω ιδέα, αλλά και κάποιοι που έχουν προχωρήσει σε μια αρχική υλοποίησή της [12]. Το γεγονός αυτό δίνει έναυσμα για την επιτυχή υλοποίηση της ιδέας αυτής με τη μορφή μιας αποκεντρωμένης εφαρμογής.

Βέβαια, η εφαρμογή που αναπτύχθηκε περιλαμβάνει και μια περαιτέρω πτυχή της διαχείρισης ταυτότητας μέσα στο blockchain: Αντί για δεδομένα KYC, διαχειρίζεται δεδομένα KYE (Know-Your-Employee). Στην εκδοχή αυτή, τη θέση των χρηματοπιστωτικών ιδρυμάτων καταλαμβάνουν επιχειρήσεις, ενώ στη θέση των πελατών έρχονται οι υπάλληλοι (μελλοντικοί ή νυν). Η διάρθρωση αυτή εξυπηρετεί - όπως και στην περίπτωση των χρηματοπιστωτικών ιδρυμάτων - και τα δύο μέρη της επιχειρηματικής σχέσης. Στη βιβλιογραφία η ιδέα των δεδομένων KYE εμφανίζεται πολύ πρόσφατα και σε περιορισμένο αριθμό εφαρμογών και υλοποιήσεων [13]. Η θεματολογία αυτή αποτελεί μια εξαιρετική ευκαιρία για περαιτέρω μελέτη.

1.3 Δομή Εργασίας

Η παρούσα διπλωματική εργασία διαρθρώνεται σε 6 Κεφάλαια ως εξής:

Στο Κεφάλαιο 1 γίνεται μία εισαγωγή στο θέμα, περιγράφονται οι πρακτικές εφαρμογές και εξηγούνται οι λόγοι που καθιστούν αναγκαία την έρευνα και βαθύτερη ανάλυση στο

συγκεκριμένο αντικείμενο. Ταυτόχρονα, γίνεται μία βιβλιογραφική ανασκόπηση και παρουσιάζονται οι μελέτες που έχουν γίνει μέχρι τη στιγμή της συγγραφής της παρούσας διπλωματικής εργασίας.

Στο Κεφάλαιο 2 αναλύονται βασικές έννοιες και το θεωρητικό υπόβαθρο που είναι απαραίτητο για την κατανόηση της εργασίας. Εξηγούνται θεμελιώδεις όροι, όπως τι είναι blockchain, KYC, KYE και κρυπτογράφηση.

Στο Κεφάλαιο 3 παρουσιάζονται οι τεχνολογίες και τα εργαλεία που απαιτούνται για τη μελέτη του συγκεκριμένου αντικειμένου. Επιπλέον, συγκρίνουμε τα εργαλεία μεταξύ τους και εξηγούμε την τελική μας επιλογή.

Στο Κεφάλαιο 4 περιγράφεται η αποκεντρωμένη εφαρμογή που δημιουργήθηκε για τους σκοπούς της διπλωματικής εργασίας. Παρουσιάζονται οι λειτουργίες της, η αρχιτεκτονική της αλλά και ο τρόπος χρήσης της.

Στο Κεφάλαιο 5 παρατίθενται τα αποτελέσματα των πειραμάτων, αναλύεται αν τα αποτελέσματα ήταν αναμενόμενα και παρέχονται οι σχετικές παρατηρήσεις.

Τέλος, στο Κεφάλαιο 6 η εργασία ολοκληρώνεται με την παρουσίαση των τελικών συμπερασμάτων και τις πιθανές μελλοντικές κατευθύνσεις στις οποίες μπορεί να επεκταθεί η μελέτη.

2 Στοιχεία Θεωρίας

2.1 Blockchain

Η τεχνολογία blockchain μπορεί να θεωρηθεί ως ένας δημόσιος λογιστικός κατάλογος (public ledger), όπου όλες οι καταγεγραμμένες συναλλαγές αποθηκεύονται σε μια λίστα με μπλοκ (blockchain). Αυτή η αλυσίδα μεγαλώνει καθώς νέα μπλοκ προστίθενται συνεχώς. Κάθε block περιέχει στην κεφαλίδα του (header) την ταυτότητα του προηγούμενου block, κρυπτογραφημένη με μια συνάρτηση hash. Κάθε block έχει μόνο ένα προηγούμενο block (parent block). Αξίζει να σημειώσουμε ότι σε κάποια blockchain - όπως στο Ethereum blockchain - αποθηκεύονται επιπλέον και τα hash των uncle blocks, δηλαδή των παιδιών των προγόνων του κάθε block.

Μέσω της χρήσης κρυπτογραφίας και αλγορίθμων συναίνεσης επιτυγχάνεται ασφάλεια των χρηστών και συνέπεια-αξιοπιστία στον λογιστικό κατάλογο (ledger). Η τεχνολογία blockchain , έχει ως βασικά χαρακτηριστικά την αποκέντρωση (decentralization), την συνέπεια (persistency), την ανωνυμία (anonymity) και τη δυνατότητα πλήρους ελέγχου (auditability). Με αυτά τα χαρακτηριστικά, το blockchain μπορεί να μειώσει σημαντικά το κόστος και να βελτιώσει την αποδοτικότητα των συναλλαγών [14].

Δεδομένου ότι επιτρέπει την ολοκλήρωση πληρωμών χωρίς οποιαδήποτε τράπεζα ή μεσάζοντα, το blockchain μπορεί να χρησιμοποιηθεί σε διάφορες χρηματοοικονομικές υπηρεσίες όπως ψηφιακά περιουσιακά στοιχεία, εμβάσματα και online πληρωμές. Επιπλέον, μπορεί να εφαρμοστεί και σε άλλους τομείς συμπεριλαμβανομένων των δημόσιων υπηρεσιών, του Internet of Things (IoT), των συστημάτων φήμης (reputation systems) και των υπηρεσιών ασφάλειας. Αυτοί οι τομείς ευνοούνται από την τεχνολογία του blockchain με πολλούς τρόπους. Πρώτα απ' όλα, το blockchain είναι αμετάβλητο. Οι συναλλαγές δεν μπορούν να παραποιηθούν μόλις ενσωματωθούν στο blockchain. Οι επιχειρήσεις που απαιτούν υψηλή αξιοπιστία και εγκυρότητα μπορούν να χρησιμοποιήσουν το blockchain για να προσελκύσουν πελάτες. Τέλος, το blockchain είναι διανεμημένο και μπορεί να αποφεύγει αδυναμίες που οφείλονται σε μοναδικά σημεία αποτυχίας. Επιπλέον, το έξυπνο συμβόλαιο (smart contract) μπορεί να εκτελείται αυτόματα από τους miners μόλις έχει αναπτυχθεί (deployed) στο blockchain .

2.1.1 Τύποι Blockchain

Τα τρέχοντα συστήματα blockchain κατατάσσονται γενικά σε τρεις τύπους [15]:

- **Δημόσιο Blockchain** (Public blockchain): όλα τα αρχεία είναι ορατά στο κοινό και όλοι μπορούν να συμμετάσχουν στη διαδικασία συναίνεσης. Το δημόσιο Blockchain είναι πλήρως ανεξαρτητοποιημένο από κεντρικούς οργανισμούς ελέγχου και επομένως μπορεί να λειτουργεί χωρίς την παρουσία κάποιας ρυθμιστικής αρχής, δεν μπορεί να χειραγωγηθεί ή να μειωθεί η διαφάνειά του από μια κεντρική αρχή.

- **Ιδιωτικό Blockchain** (Private blockchain): μόνο οι κόμβοι που προέρχονται από μία συγκεκριμένη οργάνωση επιτρέπεται να συμμετάσχουν στη διαδικασία συναίνεσης.

Ένα ιδιωτικό blockchain θεωρείται ως συγκεντρωτικό (centralized) δίκτυο, καθώς ελέγχεται πλήρως από μία οργάνωση. Επιπλέον, αν ένας σημαντικός κόμβος του δικτύου εμφανίσει ρήξη ασφάλειας, μπορεί να κινδυνέψει η λειτουργικότητα ολόκληρου του δικτύου.

- **Blockchain Κοινοπραξίας** (Consortium blockchain): μόνο μια ομάδα προκαθορισμένων κόμβων (nodes) συμμετέχει στη διαδικασία συναίνεσης. Το consortium blockchain που έχει κατασκευαστεί από πολλές οργανώσεις είναι μερικώς αποκεντρωμένο, καθώς μόνο μια μικρή ποσότητα κόμβων θα επιλεγεί για να καθορίσει την επικύρωση.

Τέλος, εκτός από τους παραδοσιακούς τύπους blockchain υπάρχουν και τα Υβριδικά Blockchains (Hybrid Blockchain) που είναι ένας συνδυασμός δημόσιου και ιδιωτικού blockchain και προσφέρουν καλύτερο έλεγχο ώστε να επιτευχθούν υψηλότεροι στόχοι. Το Υβριδικό Blockchain χρησιμοποιείται σε συγκεντρωτικά και αποκεντρωμένα συστήματα και δεν είναι ανοιχτό. Ωστόσο, προσφέρει ακεραιότητα, διαφάνεια, καθώς και ασφάλεια.

Ιδιότητα	Public Blockchain	Consortium Blockchain	Private Blockchain
Καθορισμός Συναίνεσης	Όλοι οι miners	Επιλεγμένοι κόμβοι	Ένας οργανισμός
Δικαιώματα ανάγνωσης	Δημόσιο	Δημόσιο ή περιορισμένο	Δημόσιο ή περιορισμένο
Αμεταβλητότητα	Σχεδόν αδύνατο να αλλοιωθεί	Θα μπορούσε να αλλοιωθεί	Θα μπορούσε να αλλοιωθεί
Αποτελεσματικότητα	Χαμηλή	Υψηλή	Υψηλή
Κεντρικοποίηση	Όχι	Μερική	Ναι
Διαδικασία συναίνεσης	Χωρίς άδεια	Με άδεια	Με άδεια

Πίνακας 2-1: Σύγκριση βασικών τύπων blockchain [14]

2.1.2 Πρωτόκολλα Συναίνεσης (Consensus Protocols)

Σκοπός των πρωτόκολλων συναίνεσης (Consensus protocols) είναι η εγκυρότητα και η ασφάλεια κάθε συναλλαγής στο blockchain. Μέσω των πρωτοκόλλων οι κόμβοι ενός blockchain επικυρώνουν τις αλλαγές που έχουν γίνει στον Λογιστικό Κατάλογο πριν προστεθούν στο blockchain.
Στα συγκεντρωτικά δίκτυα η ύπαρξη ενός κεντρικού εξυπηρετητή (server) διευκολύνει την ομαλή λειτουργία και διασφαλίζει την αξιοπιστία του συστήματος, αφού οι άλλοι κόμβοι χρειάζεται μόνο να συμφωνούν με τον κεντρικό εξυπηρετητή (server). Ωστόσο, σε ένα αποκεντρωμένο δίκτυο όπως το blockchain, κάθε κόμβος χρειάζεται να επικοινωνήσει με άλλους κόμβους για να επιτευχθεί συναίνεση. Μερικές φορές, ορισμένοι κόμβοι θα είναι εκτός λειτουργίας ή εκτός σύνδεσης, ενώ θα υπάρχουν και κακόβουλοι κόμβοι (malicious nodes), με σκοπό να επηρεάσουν ή να ματαιώσουν πλήρως τη διαδικασία συναίνεσης. Συνεπώς, ένα πρωτόκολλο συναίνεσης πρέπει να μπορεί να ελέγξει τέτοια φαινόμενα και να ελαχιστοποιήσει τους κινδύνους, ώστε να μην επηρεαστεί η αξιοπιστία του συστήματος [16].

Δεν ταιριάζουν όλα τα πρωτόκολλα συναίνεσης σε όλους τους τύπους blockchain και για αυτό θα πρέπει να γίνεται κάθε φορά η σωστή επιλογή πρωτοκόλλου ανάλογα με τις απαιτήσεις και τις ανάγκες κάθε δικτύου.

2.1.3 Έξυπνο Συμβόλαιο (Smart Contract)

Το Έξυπνο Συμβόλαιο (Smart Contract) αποτελεί ένα βασικό στοιχείο των blockchain. Είναι ένα σύνολο συμβάσεων που καθορίζουν το λειτουργικό μοντέλο που διέπει όλες τις συναλλαγές που λαμβάνουν χώρα στο blockchain. Δηλαδή, το έξυπνο συμβόλαιο ορίζει τους κανόνες, τα δεδομένα και τις διαδικασίες που θα ακολουθηθούν σε κάθε περίπτωση. Τα έξυπνα συμβόλαια χρησιμοποιούνται συνήθως για να αυτοματοποιούν την εκτέλεση μιας συμφωνίας, έτσι ώστε όλοι οι συμμετέχοντες να είναι άμεσα βέβαιοι για το αποτέλεσμα, χωρίς την εμπλοκή μεσάζοντα ή την απώλεια χρόνου. Μπορούν επίσης να αυτοματοποιήσουν μια ροή εργασίας, ενεργοποιώντας την επόμενη ενέργεια όταν πληρούνται προκαθορισμένες συνθήκες.

2.1.4 Ethereum

Το Ethereum αντιπροσωπεύει ένα blockchain με ενσωματωμένη γλώσσα προγραμματισμού Turing-complete. Παρέχει ένα αφηρημένο επίπεδο που επιτρέπει σε οποιονδήποτε να δημιουργήσει τους δικούς του κανόνες για την κυριότητα, τις μορφές συναλλαγών και τις λειτουργίες μετάβασης κατάστασης. Αυτό επιτυγχάνεται μέσω έξυπνων συμβολαίων (smart contracts), ένα σύνολο κρυπτογραφικών κανόνων που εκτελούνται μόνο εάν πληρούνται ορισμένες προϋποθέσεις.[5]

Η συναίνεση στο δίκτυο του Ethereum βασίζεται στο τροποποιημένο πρωτόκολλο GHOST (Greedy Heaviest Observed Subtree). Αυτό δημιουργήθηκε για να αντιμετωπίσει το πρόβλημα των παρωχημένων μπλοκ στο δίκτυο. Τα παρωχημένα μπλοκ μπορούν να προκύψουν εάν μία ομάδα από miners, συνδυασμένη σε ένα mining pool, έχει περισσότερη υπολογιστική ισχύ από τις άλλες, πράγμα που σημαίνει ότι τα μπλοκ του πρώτου mining pool θα συμβάλλουν περισσότερο στο δίκτυο, δημιουργώντας έτσι το πρόβλημα της συγκέντρωσης. Το πρωτόκολλο GHOST περιλαμβάνει αυτά τα παρωχημένα μπλοκ στους υπολογισμούς της μεγαλύτερης αλυσίδας.

Ethereum Virtual Machine (EVM)

Το Ethereum Virtual Machine (EVM) είναι ένα αποκεντρωμένο εικονικό περιβάλλον που εκτελεί κώδικα με συνέπεια και ασφάλεια σε όλους τους κόμβους του Ethereum. Οι κόμβοι εκτελούν έξυπνα συμβόλαια μέσω του EVM, χρησιμοποιώντας καύσιμο (gas) για να μετρήσουν την υπολογιστική προσπάθεια που απαιτείται για τις λειτουργίες. Έτσι, εξασφαλίζεται αποδοτική κατανομή πόρων και ασφάλεια δικτύου.[17]

2.1.5 NFT

Το NFT (Non-Fungible Token) είναι ένας τύπος κρυπτονομίσματος που προκύπτει από τα έξυπνα συμβόλαια (smart contracts) του Ethereum. Το NFT προτάθηκε αρχικά στην Πρόταση Βελτίωσης του Ethereum (Ethereum Improvement Proposals) EIP-721 και αναπτύχθηκε περαιτέρω στην EIP-1155. Το NFT διαφέρει από τα κλασικά κρυπτονομίσματα, όπως το Bitcoin, στις εσωτερικές του ιδιότητες.

Το Bitcoin είναι ένα τυπικό νόμισμα στο οποίο όλα τα νομίσματα είναι ισοδύναμα και δεν μπορούν να διακριθούν μεταξύ τους. Αντίθετα, το NFT είναι μοναδικό και μη εναλλάξιμο, καθιστώντας το κατάλληλο για την ταυτοποίηση ενός αντικειμένου ή ενός ατόμου με μοναδικό τρόπο. Συγκεκριμένα, χρησιμοποιώντας NFTs σε έξυπνα συμβόλαια (στο Ethereum), ένας δημιουργός μπορεί εύκολα να αποδείξει την ύπαρξη και την κυριότητα ψηφιακών περιουσιακών στοιχείων με τη μορφή βίντεο, εικόνων, έργων τέχνης, εισιτηρίων εκδηλώσεων κλπ. Επιπλέον, ο δημιουργός μπορεί να κερδίσει δικαιώματα (royalties) κάθε φορά που πραγματοποιείται μια επιτυχημένη συναλλαγή σε οποιαδήποτε αγορά NFT ή μέσω ανταλλαγής σε ομότιμο δίκτυο (peer-to-peer).

Το πλήρες ιστορικό στις συναλλαγές, η υψηλή ρευστότητα και η εύκολη διαλειτουργικότητα επιτρέπουν στο NFT να γίνει μια υποσχόμενη λύση για την προστασία της πνευματικής ιδιοκτησίας (IP, intellectual property). Παρόλο που, στην ουσία, τα NFTs αντιπροσωπεύουν κάτι περισσότερο από κώδικα, αυτός ο κώδικας αποκτά αξία για τον αγοραστή, όταν λαμβάνεται υπόψη η σπανιότητά του ως ψηφιακό αντικείμενο. Έτσι, διασφαλίζονται οι τιμές πώλησης των προϊόντων που σχετίζονται με την πνευματική ιδιοκτησία, κάτι το οποίο σε άλλη περίπτωση θα φαινόταν αδιανόητο.[18]

2.2 Decentralized App (DApp)

Οι αποκεντρωμένες εφαρμογές (DApp) προσελκύουν περισσότερη προσοχή με την ανάπτυξη και την ευρεία εφαρμογή των τεχνολογιών blockchain. Οι τυπικές εφαρμογές συνήθως ελέγχονται και λειτουργούν από μια κεντρική οντότητα, όπως μια εταιρεία ή έναν οργανισμό. Από την άλλη, οι DApp που εκτελούνται σε ένα blockchain λειτουργούν αυτόνομα, καθώς βασίζονται στις συλλογικές προσπάθειες των κόμβων του δικτύου και στους κωδικοποιημένους κανόνες των έξυπνων συμβολαίων [19]. Χρησιμοποιούνται ευρέως στην εκπαίδευση, οικονομία, στα μέσα κοινωνικής δικτύωσης, στην Υγεία αλλά και σε άλλους τομείς.

Οι αποκεντρωμένες εφαρμογές προσφέρουν [20]:

- **Ασφάλεια:** Αξιοποιώντας την τεχνολογία blockchain, συμβάλλουν στη βελτίωση της ασφάλειας σε πολλές επιχειρηματικές και προσωπικές διαδικασίες. Τα blockchain καθιστούν τα δεδομένα αμετάβλητα, χρησιμοποιώντας κρυπτογραφικές τεχνικές και μηχανισμούς κατανεμημένης αυτοματοποιημένης συναίνεσης. Ο αποκεντρωμένος Λογιστικός Κατάλογος (decentralized Ledger) μοιράζεται και συγκρίνεται μεταξύ όλων των χρηστών, με αποτέλεσμα τα δεδομένα να μην μπορούν να τροποποιηθούν.

- **Κόστος και Αποτελεσματικότητα:** Η απουσία μεσάζοντα έχει ως αποτέλεσμα τη μείωση του κόστους, την αύξηση της αποδοτικότητας και τη μεγαλύτερη προσβασιμότητα.

- **Προσβασιμότητα:** Πρόσβαση στην αποκεντρωμένη εφαρμογή (DApp) έχει οποιοσδήποτε διαθέτει σύνδεση στο διαδίκτυο. Αυτή η παγκόσμια προσβασιμότητα εκδημοκρατίζει την πρόσβαση σε πολλούς διαφορετικούς τύπους υπηρεσιών, ψηφιακών περιουσιακών στοιχείων και πληροφοριών ανεξάρτητα από την τοποθεσία από την οποία γίνεται η σύνδεση.

- **Διαφάνεια και Αξιοπιστία:** Διατηρούν διαφανή αρχεία συναλλαγών, επιτρέποντας στους χρήστες να επαληθεύουν την ακεραιότητα των δεδομένων χωρίς να βασίζονται σε κεντρικές αρχές.

2.3 KYC

Η διαδικασία KYC (Know Your Customer) είναι απαραίτητη στα χρηματοπιστωτικά ιδρύματα για την επαλήθευση των πελατών τους , την προστασία από οικονομικά εγκλήματα και το ξέπλυμα χρήματος αλλά και για την καλύτερη εξυπηρέτηση ανάλογα με τις ανάγκες τους [21]. Τύποι KYC:

- **KYC μέσω φυσικής παρουσίας (KYC):** Ο πελάτης υποβάλλει τα έγγραφα και την ταυτότητα σε φυσική μορφή προς επικύρωση σε εξουσιοδοτημένα κέντρα ή υποκαταστήματα.

- **Ηλεκτρονικό KYC (eKYC) :** Ο πελάτης υποβάλλει τα έγγραφα σε ψηφιακή μορφή. Σε αυτή την περίπτωση μπορεί να είναι απαραίτητη για επαλήθευση η βιομετρική ταυτοποίηση, η αναγνώριση προσώπου και η χρήση των κυβερνητικών βάσεων δεδομένων.

Τα δεδομένα KYC που ζητάει κάθε χρηματοπιστωτικό ίδρυμα μπορεί να διαφέρουν. Συνήθως αποδέχονται κάποιο από τα παρακάτω έγγραφα:

- Ταυτότητα
- Δίπλωμα οδήγησης
- Διαβατήριο
- Λογαριασμό Ρεύματος/Ύδρευσης
- Έγγραφο έκδοσης πιστωτικής κάρτας
- Έγγραφο ανοίγματος λογαριασμού σε τράπεζα

Τα παραπάνω έγγραφα περιέχουν πληροφορίες για το όνομα, επίθετο, διεύθυνση, ημερομηνία γέννησης, πατρώνυμο, μητρώνυμο, υπογραφή, υπηκοότητα κλπ. Δεδομένα δηλαδή που είναι απαραίτητα για την σωστή ταυτοποίηση του πελάτη των χρηματοπιστωτικών ιδρυμάτων. Επιπλέον αυτών, μπορεί να ζητηθούν έγγραφα που να αποδεικνύουν την προέλευση των χρημάτων τους αλλά και το επάγγελμά τους.

2.3.1 KYE

Όπως αναφέρθηκε και στην εισαγωγή της παρούσας εργασίας, τα KYE μοιάζουν στα KYC δεδομένα αφού και αυτά χρησιμεύουν στην επαλήθευση της ταυτότητας του εργαζομένου. Ωστόσο, είναι προσανατολισμένα κυρίως προς τις γνώσεις και τις πιστοποιήσεις που κατέχει ο εργαζόμενος. Επομένως, εκτός από τα προσωπικά στοιχεία του εργαζομένου, τα KYE δεδομένα πρέπει να περιέχουν:

- Απολυτήριο Λυκείου
- Διπλώματα σπουδών
- Πιστοποιητικά Σεμιναρίων που έχει παρακολουθήσει
- Πτυχία Ξένων Γλωσσών
- Προηγούμενες θέσεις εργασίας

Αλλά και οτιδήποτε άλλο μπορεί να θεωρηθεί σημαντικό για την πρόσληψη του ατόμου (π.χ. ποινικό μητρώο για τις δουλείες που έχουν άμεση επαφή με παιδιά ή άλλες ευαίσθητες κοινωνικές ομάδες).

2.4 Μηχανισμοί κρυπτογράφησης

2.4.1 Κρυπτογράφηση

Τα δεδομένα πριν μοιραστούν ή αποθηκευτούν κρυπτογραφούνται για να παραμείνει ασφαλές το περιεχόμενό τους. Η κρυπτογράφηση λειτουργεί κωδικοποιώντας το «απλό κείμενο» (plain text) σε «κρυπτογραφημένο κείμενο» (ciphertext), συνήθως μέσω της χρήσης αλγορίθμων.

Με την κρυπτογράφηση τα δεδομένα μετατρέπονται σε μία μορφή μη αναγνώσιμη από μη εξουσιοδοτημένα άτομα. Αποτρέπονται έτσι κυβερνοεγκλήματα, αφού παρόλο που μπορεί να έχουν χρησιμοποιήσει αρκετά εξελιγμένα μέσα για να αποκτήσουν πρόσβαση σε ένα εταιρικό δίκτυο, τα δεδομένα είναι πρακτικά μη αναγνώσιμα και συνεπώς άχρηστα.

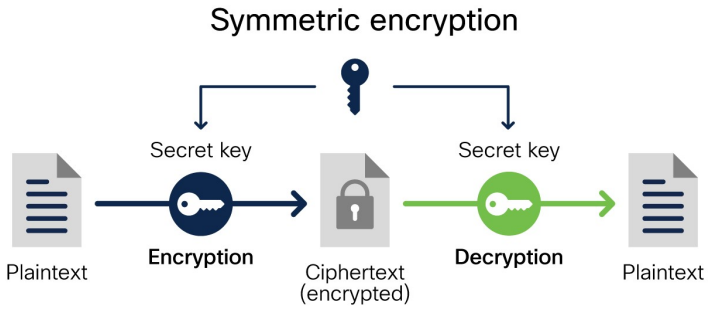
Για να αποκωδικοποιηθούν τα δεδομένα και να επιστρέψουν σε απλό κείμενο απαιτείται η χρήση ενός κλειδιού αποκρυπτογράφησης, δηλαδή, μιας σειράς αριθμών/χαρακτήρων ή ενός κωδικού πρόσβασης που δημιουργείται επίσης από έναν αλγόριθμο.

Οι ασφαλείς μέθοδοι κρυπτογράφησης διαθέτουν τόσο μεγάλο αριθμό κρυπτογραφικών κλειδιών που ένας μη εξουσιοδοτημένος χρήστης δεν μπορεί ούτε να μαντέψει ποιο είναι το σωστό, ούτε να χρησιμοποιήσει έναν υπολογιστή για να υπολογίσει εύκολα τη σωστή ακολουθία χαρακτήρων δοκιμάζοντας κάθε πιθανό συνδυασμό (γνωστό ως επίθεση “brute force”). Με αυτόν τον τρόπο διασφαλίζεται η εμπιστευτικότητα αλλά και η ακεραιότητα των δεδομένων αφού τα μηνύματα δεν μπορούν να αλλοιωθούν στην κρυπτογραφημένη μορφή και όταν αποκρυπτογραφηθούν επανέρχονται στην αρχική τους κατάσταση.

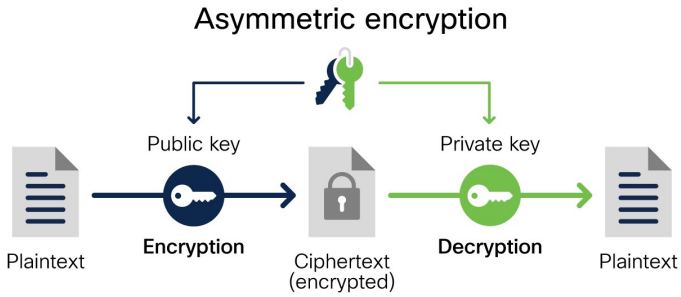
Τύποι αλγορίθμων κρυπτογράφησης [22]:

- **Συμμετρική κρυπτογράφηση:** Χρησιμοποιείται το ίδιο κλειδί (key) και για κρυπτογράφηση και για αποκρυπτογράφηση.

- **Ασύμμετρη κρυπτογράφηση:** Χρησιμοποιούνται δύο κλειδιά. Το κλειδί που χρησιμοποιείται για την κρυπτογράφηση ονομάζεται συνήθως «δημόσιο κλειδί» (public key) ενώ το κλειδί για την αποκρυπτογράφηση ονομάζεται «ιδιωτικό κλειδί» (private key). Πρόσβαση στο ιδιωτικό κλειδί έχουν μόνο εξουσιοδοτημένα άτομα.



Εικόνα 2-1 Διαδικασία Συμμετρικής Κρυπτογράφησης και Αποκρυπτογράφησης[22]



Εικόνα 2-2 Διαδικασία Ασύμμετρης Κρυπτογράφησης και Αποκρυπτογράφησης [22]

Advanced Encryption Standard AES [23]

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ξεκίνησε την ανάπτυξη του AES το 1997. Τον Ιούνιο του 2003, το AES έγινε ο προεπιλεγμένος αλγόριθμος κρυπτογράφησης για την προστασία διαβαθμισμένων πληροφοριών, συμπεριλαμβανομένων κυβερνητικών

δεδομένων [24]. Έγινε επίσης το πρώτο δημόσια προσβάσιμο και ανοιχτό σύστημα κρυπτογράφησης που εγκρίθηκε από την Υπηρεσία Εθνικής Ασφάλειας (NSA) για την προστασία πληροφοριών «Άκρως Απόρρητου» χαρακτήρα και εθνικών συστημάτων ασφαλείας.

Το AES περιλαμβάνεται επίσης στο πρότυπο ISO/IEC 18033-3 του Διεθνούς Οργανισμού Τυποποίησης, το οποίο καθορίζει αλγόριθμους κρυπτογράφησης μπλοκ για την ενίσχυση της εμπιστευτικότητας των δεδομένων.

Σήμερα, το AES είναι ένας από τους πιο δημοφιλείς αλγόριθμους συμμετρικής κρυπτογραφίας για ένα ευρύ φάσμα εφαρμογών, τόσο για κυβερνητική όσο και για εμπορική χρήση. Μερικά παραδείγματα περιλαμβάνουν τα εξής:

- Δεδομένα σε μέσα αποθήκευσης, όπως σκληροί δίσκοι και USB drives.
- Εφαρμογές ηλεκτρονικής επικοινωνίας.
- Βιβλιοθήκες προγραμματισμού.
- Περιηγητές διαδικτύου.
- Συμπίεση αρχείων και δίσκων.
- Ασύρματα δίκτυα.
- Βάσεις δεδομένων.
- Διαπιστευτήρια σύνδεσης, όπως κωδικοί πρόσβασης.
- Εικονικά ιδιωτικά δίκτυα (VPN).

Ο AES είναι αλγόριθμος συμμετρικού κλειδιού δηλαδή, χρησιμοποιεί το ίδιο μυστικό κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Επομένως τόσο ο αποστολέας όσο και ο παραλήπτης των δεδομένων πρέπει να έχουν αντίγραφο αυτού του μυστικού κλειδιού. Οι αλγόριθμοι συμμετρικού κλειδιού, όπως το AES, είναι ταχύτεροι και πιο αποδοτικοί, καθώς απαιτούν λιγότερη υπολογιστική ισχύ σε σύγκριση με τους αλγόριθμους ασύμμετρου κλειδιού.

Στον AES χρησιμοποιείται αλγόριθμος κρυπτογράφησης μπλοκ (cipher block). Κρυπτογραφεί τα δεδομένα σε μπλοκ των 128bits το καθένα. Το κρυπτογραφημένο μπλοκ έχει επίσης μήκος 128bits. Υπάρχουν τρεις κύριοι τύποι [25]:

- **AES-128:** Αυτή η μέθοδος χρησιμοποιεί μήκος κλειδιού 128-bit για κρυπτογράφηση και αποκρυπτογράφηση, που έχει ως αποτέλεσμα 10 γύρους κρυπτογράφησης με $3,4 \times 10^{38}$ διαφορετικούς πιθανούς συνδυασμούς

- **AES-192:** Αυτή η μέθοδος χρησιμοποιεί μήκος κλειδιού 192-bit για κρυπτογράφηση και αποκρυπτογράφηση, που έχει ως αποτέλεσμα 12 γύρους κρυπτογράφησης με 6.2×10^{57} διαφορετικούς πιθανούς συνδυασμούς

- **AES-256:** Αυτή η μέθοδος χρησιμοποιεί μήκος κλειδιού 256-bit για κρυπτογράφηση και αποκρυπτογράφηση, που έχει ως αποτέλεσμα 14 γύρους κρυπτογράφησης με $1,1 \times 10^{77}$ διαφορετικούς πιθανούς συνδυασμούς

Το AES είναι ένα δίκτυο υποκατάστασης-μεταθέτησης που χρησιμοποιεί μια διαδικασία επέκτασης κλειδιού, όπου το αρχικό κλειδί χρησιμοποιείται για την παραγωγή νέων κλειδιών

που ονομάζονται κλειδιά γύρων. Τα κλειδιά γύρων παράγονται μέσω πολλαπλών γύρων τροποποίησης. Κάθε γύρος κάνει πιο δύσκολο το σπάσιμο της κρυπτογράφησης. Σε κάθε γύρο έχουμε 4 βήματα. Για την αποκρυπτογράφηση πραγματοποιείται η αντίστροφη διαδικασία. Η μαθηματική διαδικασία που ακολουθείται δεν έγκειται στον σκοπό της παρούσας διπλωματικής και για αυτό δε θα αναλυθεί περαιτέρω.

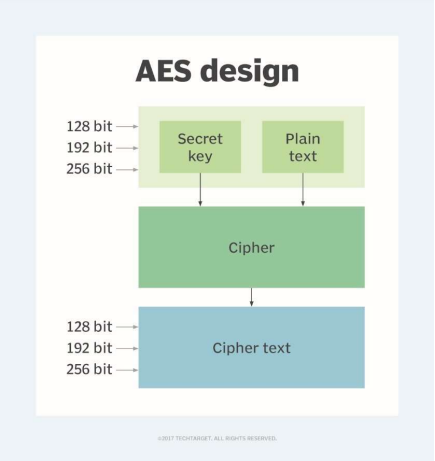


Figure 2-1 AES αλγόριθμος κρυπτογράφησης [24]

3 Εργαλεία και Τεχνολογίες

3.1 Πλατφόρμα Blockchain

3.1.1 Ethereum

Ως πλατφόρμα λογισμικού Blockchain επιλέχθηκε το Ethereum καθώς είναι ένα από τα πιο εδραιωμένα blockchain. Δημιουργήθηκε το 2015 και η δημοτικότητά του ανεβαίνει έκτοτε. Για τον λόγο αυτό κατέχει μεγάλο ιστορικό αξιοπιστίας. Επιπλέον, παρά την παλαιότητά του σε σχέση με άλλα, νεότερα blockchain, το Ethereum ενσωματώνει αρκετές νέες τεχνολογίες στον χώρο των αποκεντρωμένων λογισμικών:

1. Επιτρέπει τη δημιουργία και την εκτέλεση έξυπνων συμβολαίων, δίνοντας τη δυνατότητα επιτέλεσης περίπλοκων λειτουργιών με τη μορφή ασφαλών συναλλαγών.

2. Τα έξυπνα συμβόλαια επεξεργάζονται μέσω του Ethereum Virtual Machine (EVM) [17], ενός αποκεντρωμένου εικονικού περιβάλλοντος που εκτελεί κώδικα με ασφάλεια και υπολογίζει την υπολογιστική «προσπάθεια» (computational effort) που απαιτείται για την εκτέλεσή του. Η υπολογιστική προσπάθεια μετριέται σε «gas».

3. Proof of Stake (PoS): Το Ethereum μετά την έκδοση του Ethereum 2.0 μετέβη από τη χρήση Proof of Work ως μηχανισμού συναίνεσης (consensus mechanism) στη χρήση του Proof of Stake. Ο αλγόριθμος Proof of Stake είναι αρκετά πιο κλιμακώσιμος, γρήγορος αλλά και αποδοτικός.

Εκτός των παραπάνω, το Ethereum υποστηρίζει δύο από τα πιο δημοφιλή πρότυπα διαχείρισης NFT: το ERC-721 [26] και το ERC-1155 [27].

ERC-721

Το πρότυπο ERC-721, το οποίο συντάχθηκε το 2017, είναι ένα επαναστατικό πρότυπο διαχείρισης κρυπτοπαραστατικών (tokens) που πυροδότησε το φαινόμενο NFT και έγινε πυλώνας δημιουργίας NFT στο οικοσύστημα του Ethereum. Το πρότυπο ERC-721 παρέχει μια τυπική διεπαφή για NFT και εξασφαλίζει ότι όλα τα tokens είναι μοναδικά. Το ERC-721 επιτρέπει τη μεταφορά NFT μεταξύ λογαριασμών, αλλά και την ανταλλαγή NFT με άλλα νομίσματα.

Μία από τις πρακτικές λειτουργίες του ERC-721 είναι ότι επιτρέπει στους χρήστες να προσδιορίζουν το σύνολο των NFT που διατίθενται σε ένα δίκτυο. Άλλες λειτουργίες περιλαμβάνουν τη λήψη του τρέχοντος υπολοίπου NFT ενός λογαριασμού και τον υπολογισμό του αριθμού των tokens που μπορεί να μεταφέρει ένας λογαριασμός σε έναν άλλον.

Τα NFT που βασίζονται στο ERC-721 χρησιμοποιούνται πιο συχνά για ψηφιακά έργα τέχνης, αλλά οι περιπτώσεις χρήσης επεκτείνονται επίσης σε μουσική, παιχνίδια που βασίζονται σε blockchain και αποκεντρωμένες εφαρμογές.

ERC-1155

Το ERC-1155, το οποίο δημιουργήθηκε το 2018, είναι ένα πρότυπο που υποστηρίζει πολλά είδη token και το οποίο παρέχει μια διεπαφή για έξυπνα συμβόλαια που διαχειρίζονται πολλαπλούς τύπους token. Η αρχική πρόθεση πίσω από τη δημιουργία του ERC-1155 περιελάμβανε την επίλυση των προβλημάτων που αντιμετωπίζουν οι προγραμματιστές στον κόσμο των ηλεκτρονικών παιχνιδιών που βασίζονται σε blockchain.

Το ERC-1155 βελτιώνει τη λειτουργικότητα του ERC-721, αυξάνοντας την αποτελεσματικότητά του και διορθώνοντας προφανή σφάλματα υλοποίησης. Μπορεί να υποστηρίξει άπειρα tokens σε ένα ενιαίο συμβόλαιο, υποστηρίζοντας εναλλάξιμα (fungible), ημι-εναλλάξιμα (semi-fungible) και μη-εναλλάξιμα (non-fungible) token. Τα token μάλιστα μπορούν να αλλάξουν την ιδιότητά τους κατά τη διάρκεια του κύκλου ζωής τους [28].

Το ERC-1155 διαθέτει επίσης λειτουργίες ασφαλείας που επαληθεύουν την εγκυρότητα μιας συναλλαγής, επιτρέποντας την επιστροφή των ανάλογων tokens στον εκδότη εάν μια συναλλαγή αποτύχει. Αυτό εξαλείφει το άγχος των χρηστών για πιθανά λάθη, όπως η αποστολή tokens σε λάθος διεύθυνση. Αυτή η λειτουργία, μαζί με άλλους κανόνες του προτύπου προστατεύει από την λανθασμένη χρήση.

Τέλος, το ERC-1155 έχει υποστεί βελτιώσεις και αναφορικά με την ικανότητα διατήρησης μετα-δεδομένων (meta data), επιτρέποντας τη χρήση πληθώρας πρωτοκόλλων αποθήκευσης μετα-δεδομένων, σε αντίθεση με το ERC-721 το οποίο δέχεται μονάχα στατικά δεδομένα.

Επιλογή του ERC-721

Για την ΚΥΕ εφαρμογή επιλέχθηκε το πρότυπο ERC-721. Οι λόγοι αφορούν κυρίως την απλότητα του προτύπου αυτού. Άλλωστε, τα token που αφορούν την εφαρμογή ΚΥΕ είναι όλα μοναδικά και μη-εναλλάξιμα. Επομένως, για τους σκοπούς της εργασίας αυτής το πρότυπο ERC-1155 που επιτρέπει τη διαχείριση εναλλάξιμων ή ημι-εναλλάξιμων παραστατικών θα πρόσθετε απλά περιττή πολυπλοκότητα στην εφαρμογή. Να σημειωθεί, βέβαια, ότι λόγω των σημαντικών βελτιώσεων στο πρότυπο ERC-1155 και κυρίως αυτών που αφορούν στην αποθήκευση μετα-δεδομένων, η μετάβαση από το ERC-721 στο ERC-1155 είναι κάτι που θα άξιζε να μελετηθεί για εφαρμογές ΚΥΕ και σίγουρα αποτελεί τροφή για μελλοντική εργασία.

Criteria	ERC 721	ERC 1155
Ease of Use	Individual transactions and smart contracts are required for each token type.	Single, smart contracts of ERC-1155 tokens can support multiple functions.
Batch Transfers	No support for batch transfers.	You can use a single, smart contract for batch transfers.
Support for Semi-fungible Tokens	Only supports the creation of non-fungible tokens.	Supports the conversion of fungible tokens to NFTs and vice versa.
Security of Assets	Impossible to revert transactions after transferring assets to the wrong address.	Safe transfer function enables verification of transaction validity and reverses the transactions.

Εικόνα 3-1: Σύγκριση των προτύπων ERC-721 και ERC-1155 [28]

3.1.2 Solidity [29]

Η Solidity είναι μια αντικειμενοστραφής γλώσσα προγραμματισμού υψηλού επιπέδου με στατικούς τύπους δεδομένων. Συντακτικά και δομικά εμφανίζει ομοιότητες με τη C++ και την JavaScript. Είναι με διαφορά η δημοφιλέστερη γλώσσα προγραμματισμού που χρησιμοποιείται για τη δημιουργία έξυπνων συμβολαίων στο οικοσύστημα του Ethereum. Είναι μάλιστα σύνηθες να τη θεωρούν πολλοί προγραμματιστές ως τη μοναδική επιλογή για τον σκοπό αυτόν. Εντούτοις, υπάρχουν και άλλες γλώσσες που τυγχάνουν βέβαια λιγότερης δημοφιλίας. Μια εξ' αυτών είναι η Vyper.

3.1.3 Vyper [30]

Η γλώσσα προγραμματισμού Vyper είναι η δεύτερη πιο δημοφιλής γλώσσα για την ανάπτυξη έξυπνων συμβολαίων Ethereum. Είναι επίσης μια γλώσσα υψηλού επιπέδου και έχει παρόμοια δομή και ιδιότητες με την Python. Έχει αναπτυχθεί ειδικά για την επίλυση των προβλημάτων που είναι εμφανή στη Solidity, όπως τα θέματα ασφάλειας. Ωστόσο, η Vyper έχει αποκλείσει πολλές αντικειμενοστραφείς έννοιες που είναι χρήσιμες και συναντώνται στη Solidity, όπως η κληρονομικότητα.

Η Vyper εξελίχθηκε ως εναλλακτική λύση στη Solidity, εξαλείφοντας ορισμένες δυνατότητες, σε μια προσπάθεια να καταστούν τα συμβόλαια πιο ασφαλή και ευκολότερα στον έλεγχο. Μπορεί να διευκολύνει τους προγραμματιστές Python να ξεκινήσουν εύκολα με την επιθυμητή ασφάλεια και αναγνωσιμότητα κώδικα. Επιπλέον, πρόσφατα η Vyper έχει σημειώσει μερικές σημαντικές βελτιώσεις όσον αφορά τα εργαλεία ανάπτυξης. Από την άλλη

πλευρά, η Vyper υστερεί σε σύγκριση με τη Solidity σε ό,τι αφορά την υποστήριξη από την κοινότητα και το πλήθος διαθέσιμου υλικού στο διαδίκτυο.

Ωστόσο, η Vyper προσφέρει και κάποιες νέες ενδιαφέρουσες λειτουργιές, όπως τον καθορισμό του ακριβούς ανώτατου ορίου για την κατανάλωση gas. Τέλος, οι περιορισμοί μεγέθους σε πίνακες και συμβολοσειρές στη Vyper θα μπορούσαν να διασφαλίσουν καλύτερη προστασία για το συμβόλαιο από κυβερνο-επιθέσεις που εκμεταλλεύονται την απουσία αυτού του περιορισμού στην Solidity.

3.1.3 Ανερχόμενες γλώσσες προγραμματισμού Ethereum

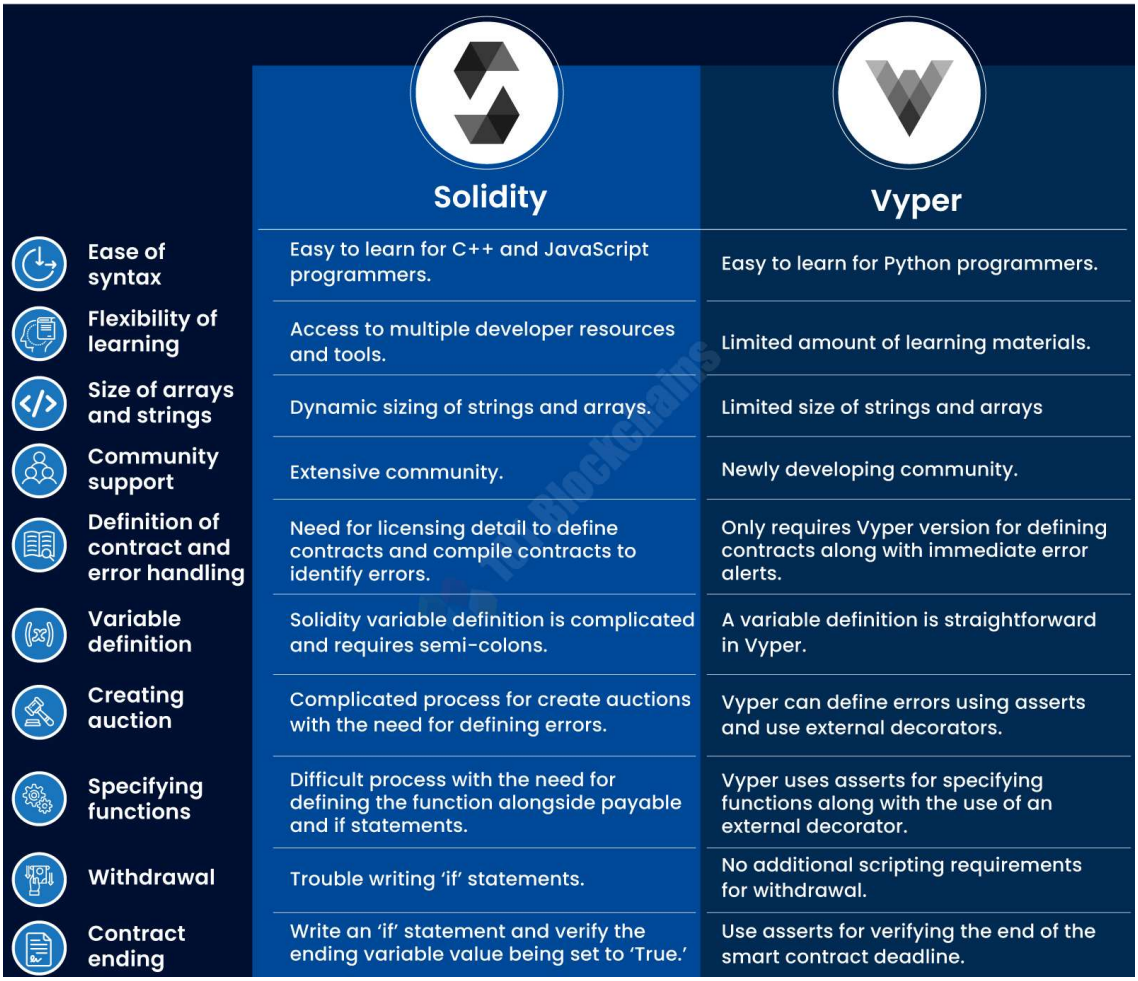
Πέραν της Solidity και της Vyper, στον χώρο του Ethereum μπορεί κανείς πλέον να συναντήσει και πληθώρα νεότερων, ανερχόμενων γλωσσών προγραμματισμού έξυπνων συμβολαίων. Αξίζει ανάμεσα σε αυτές να αναφερθούν η Yul [31] και η Fe [32].

Η Yul είναι μια γλώσσα προγραμματισμού χαμηλού επιπέδου σχεδιασμένη για το οικοσύστημα του Ethereum. Συνήθως χρησιμοποιείται για έντονες και προηγμένες βελτιστοποιήσεις σε περιπτώσεις που η επίδοση του κώδικα είναι υψηλής σημασίας. Σημαντική λειτουργία της Yul είναι ότι μπορεί να ενσωματωθεί μέσα σε κώδικα Solidity με χρήση μπλοκ κώδικα assembly (assembly {}). Αυτό βέβαια σημαίνει ότι σπάνια η Yul χρησιμοποιείται εντελώς αποκλειστικά για τη συγγραφή έξυπνων συμβολαίων.

Η Fe από την άλλη είναι μια ακόμη γλώσσα υψηλού επιπέδου. Βασίζεται στην επίσης ανερχόμενη γλώσσα προγραμματισμού Rust, ενώ εμφανίζει ομοιότητες και με την Vyper. Χρησιμοποιείται ήδη για την πλήρη συγγραφή έξυπνων συμβολαίων στο οικοσύστημα του Ethereum. Παρ' όλα αυτά, βρίσκεται στα πρώτα στάδια ανάπτυξης και ως εκ τούτου, η στήριξη από την κοινότητα και τα διαθέσιμα βοηθήματα για αυτήν στο διαδίκτυο είναι περιορισμένα σε σύγκριση με αυτά της Solidity ή της Vyper.

3.1.4 Επιλογή της Solidity

Αναφορικά με τη γλώσσα προγραμματισμού για την ανάπτυξη έξυπνων συμβολαίων στο οικοσύστημα του Ethereum, η τελική επιλογή για την παρούσα διπλωματική εργασία κρίθηκε μεταξύ της Solidity και της Vyper, καθώς αποτελούν τις δύο πλέον διαδεδομένες και αυτοτελείς γλώσσες προγραμματισμού για έξυπνα συμβόλαια Ethereum. Αν και η Vyper προσφέρει απλοποιημένη σύνταξη και επικεντρώνεται στην ενίσχυση της ασφάλειας μέσω της απομάκρυνσης ορισμένων σύνθετων χαρακτηριστικών, όπως η κληρονομικότητα, επιλέγεται η Solidity λόγω της ώριμης και εκτεταμένης υποστήριξης που προσφέρει η κοινότητα. Το πλήθος των βοηθητικών πόρων στο διαδίκτυο, η ευρεία χρήση της σε ήδη υπάρχουσες αποκεντρωμένες εφαρμογές, καθώς και τα διαθέσιμα εργαλεία και βιβλιοθήκες, καθιστούν τη Solidity την καταλληλότερη επιλογή για την ανάπτυξη έξυπνων συμβολαίων με μεγαλύτερη λειτουργικότητα και ευελιξία.



Εικόνα 3-2: Solidity και Vyper - Κύριες Διαφορές [33]

3.1.5 OpenZeppelin [34]

Το OpenZeppelin είναι ένα πλαίσιο που βοηθάει στην ανάπτυξη κώδικα για έξυπνα συμβόλαια. Η κύρια λειτουργικότητά του έγκειται στις βιβλιοθήκες που προσφέρει. Οι βιβλιοθήκες OpenZeppelin αναπτύχθηκαν αρχικά για το Ethereum blockchain, εντούτοις πλέον χρησιμοποιούνται σε οποιοδήποτε blockchain είναι συμβατό με το Ethereum Virtual Machine (EVM). Είναι σημαντικό το γεγονός ότι το μεγαλύτερο μέρος των βιβλιοθηκών είναι γραμμένο σε Solidity και η OpenZeppelin έχει αναπτυχθεί με κύριο σκοπό την υποστήριξη ανάπτυξης κώδικα Solidity για έξυπνα συμβόλαια. Ωστόσο, πρακτικά οι προγραμματιστές μπορούν να χρησιμοποιήσουν τις βιβλιοθήκες και να τις ενσωματώσουν σε κώδικα γραμμένο σε Vyper, Yul ή άλλες γλώσσες που μεταγλωττίζονται σε EVM bytecode.

Οι εν λόγω βιβλιοθήκες παρέχουν έτοιμες υλοποιήσεις για πρωτόκολλα διαχείρισης NFT όπως το ERC-721 και το ERC-1155. Περιλαμβάνουν επίσης λειτουργικότητες που αφορούν τον έλεγχο πρόσβασης και δικαιωμάτων εντός του δικτύου blockchain αλλά και εργαλεία εξασφάλισης της ασφάλειας των έξυπνων συμβολαίων.

3.2 Πλατφόρμα Ανάπτυξης Έξυπνων Συμβολαίων

Στην ανάπτυξη αποκεντρωμένων εφαρμογών (DApps), η ανάπτυξη έξυπνων συμβολαίων και η ανάρτησή τους σε δίκτυο blockchain αποτελούν τις δύο κυριότερες ίσως διαδικασίες. Υπάρχουν διάφορα εργαλεία που διευκολύνουν την ανάπτυξη αυτή, προσφέροντας μια ποικιλία δυνατοτήτων ανάλογα με τις ανάγκες της εκάστοτε εφαρμογής. Πριν αρχίσει η ανάπτυξη της εφαρμογής που πραγματεύεται η παρούσα εργασία, εξετάσθηκαν τέσσερις επιλογές αναφορικά με πλατφόρμες ανάπτυξης έξυπνων συμβολαίων. Παρακάτω παρουσιάζονται οι επιλογές και επισημαίνονται τα πλεονεκτήματα τους σχετικά με τη λειτουργικότητά τους αλλά και την υποστήριξή τους από την κοινότητα.

3.2.1 Δημοφιλείς πλατφόρμες ανάπτυξης έξυπνων συμβολαίων

Hardhat [35]

Το Hardhat είναι ένα δημοφιλές περιβάλλον ανάπτυξης για το Ethereum, που επιτρέπει στους προγραμματιστές να μεταγλωττίζουν, να δοκιμάζουν και να αναπτύσσουν έξυπνα συμβόλαια. Διαθέτει ένα ευέλικτο και επεκτάσιμο σύστημα πρόσθετων βιβλιοθηκών, γεγονός που το καθιστά πολύ προσαρμόσιμο στις απαιτήσεις ενός έργου. Επιπλέον, η ισχυρή διαχείριση σφαλμάτων και η λεπτομερής καταγραφή του Hardhat το καθιστούν ένα δημοφιλές εργαλείο για την αποσφαλμάτωση έξυπνων συμβολαίων.

Brownie – Ape [36]

Το Brownie είναι ένα πλαίσιο ανάπτυξης έξυπνων συμβολαίων βασισμένο στη γλώσσα Python και είναι ιδιαίτερα κατάλληλο για προγραμματιστές που είναι εξοικειωμένοι με το ευρύτερο οικοσύστημα της Python. Οι εκτεταμένες δυνατότητες testing που προσφέρει, σε συνδυασμό με την ενσωματωμένη υποστήριξη για βιβλιοθήκες Python, το καθιστούν μια ισχυρή επιλογή για την ανάπτυξη αποκεντρωμένων εφαρμογών. Το Brownie, ωστόσο, δεν συντηρείται πλέον ενεργά. Μελλοντικές εκδόσεις ενδέχεται να κυκλοφορήσουν σποραδικά - ή και καθόλου. Το Ape Framework είναι η εξέλιξη του πλαισίου αυτού και καλύπτει τις ίδιες ή και περισσότερες ανάγκες για ανάπτυξη Ethereum με Python. Αξίζει να σημειωθεί ότι η υποστήριξη του Ape Framework από την κοινότητα προγραμματιστών Ethereum είναι μεν υπαρκτή, ωστόσο, φαίνεται να υστερεί σε σχέση με ανταγωνιστικά εργαλεία.

Truffle [37]

Το Truffle, είναι ένα ακόμη δημοφιλές πλαίσιο ανάπτυξης για το Ethereum. Αναπτύχθηκε από την Consensys το 2016 και αποτελεί ένα από τα παλαιότερα οικοσυστήματα ανάπτυξης για το Ethereum. Λειτουργεί ως πλαίσιο ανάπτυξης και δοκιμών καθώς και ως μέσο εγκατάστασης εργαλείων για εφαρμογές blockchain, χρησιμοποιώντας την Εικονική Μηχανή του Ethereum (Ethereum Virtual Machine). Το Truffle προσφέρει πολλές δυνατότητες για ευκολότερη και αποδοτικότερη ανάπτυξη αποκεντρωμένων εφαρμογών (DApps), όπως υποστήριξη για μεταγλώττιση και διαχείριση συμβολαίων, διαδραστική κονσόλα για την άμεση επικοινωνία με συμβόλαια, και διαχείριση δικτύων.

Η Σουίτα Truffle περιλαμβάνει επίσης το Ganache, το οποίο βοηθά στη δοκιμή των συμβολαίων Solidity σε ένα τοπικό blockchain δίκτυο. Το Truffle αναδεικνύεται επίσης ως μια αξιόλογη επιλογή, λόγω του Drizzle, της συλλογής βιβλιοθηκών για το front-end. Το Drizzle μπορεί να βοηθήσει στον σχεδιασμό διαδραστικών γραφικών διεπαφών (UIs), διευκολύνοντας τους χρήστες να αλληλεπιδρούν με τις αποκεντρωμένες εφαρμογές.

Remix [38]

Το Remix είναι ένα διαδικτυακό περιβάλλον ανάπτυξης κώδικα που αφορά τη διαδικασία συγγραφής, δοκιμής και ανάπτυξης έξυπνων συμβολαίων. Είναι εξαιρετικά προσβάσιμο, καθώς δεν απαιτεί εγκατάσταση, και υποστηρίζει την άμεση αλληλεπίδραση με τα δίκτυα Ethereum. Η ευκολία χρήσης του το καθιστά δημοφιλές για μικρά έργα ή για έργα που βρίσκονται στα αρχικά στάδια ανάπτυξης.

3.2.2 Επιλογή της Πλατφόρμας Truffle

Το Truffle επιλέχθηκε ως το εργαλείο για τη μεταγλώττιση και ανάπτυξη των έξυπνων συμβολαίων στα πλαίσια της παρούσας εργασίας. Η κύρια αιτία για την επιλογή του Truffle ήταν η εκτενής υποστήριξή του από την κοινότητα, η οποία παρέχει αναλυτική καθοδήγηση για προγραμματιστές όλων των επιπέδων εμπειρίας. Η μεγάλη κοινότητα που έχει δημιουργηθεί γύρω από το Truffle εξασφαλίζει ότι ζητήματα που προκύπτουν μπορούν συχνά να επιλυθούν γρήγορα, με πλήθος πόρων και λύσεων στο διαδίκτυο. Η εκτενής αυτή υποστήριξη οφείλεται εκτός των άλλων και στο γεγονός ότι το Truffle είναι από τις παλαιότερες πλατφόρμες ανάπτυξης έξυπνων συμβολαίων αλλά παραμένει απολύτως ενεργή μέχρι και σήμερα.

Επιπλέον, ενσωματώνεται άψογα με δημοφιλή και εκτενώς υποστηριζόμενα εργαλεία ανάπτυξης όπως το Ganache και το MetaMask, τα οποία επίσης χρησιμοποιήθηκαν στο έργο αυτό, όπως θα δούμε παρακάτω.

Συνολικά, το Truffle προσφέρει μια ολοκληρωμένη λύση για την ανάπτυξη αποκεντρωμένων εφαρμογών, ενσωματώνοντας ένα ευρύ φάσμα λειτουργιών, όπως αυτοματοποιημένες δοκιμές συμβολαίων, διαχείριση δικτύων και ένα σύνολο εργαλείων για τη μετανάστευση (migration) συμβολαίων σε διάφορα δίκτυα.

3.3 Προσομοίωση δικτύου Blockchain

Πριν αναρτηθεί μια αποκεντρωμένη εφαρμογή που περιέχει έξυπνα συμβόλαια σε ένα ζωντανό δίκτυο blockchain, οι λειτουργίες της θα πρέπει να δοκιμαστούν σε ένα ελεγχόμενο περιβάλλον. Με αυτόν τον τρόπο τα έξυπνα συμβόλαια δοκιμάζονται χωρίς τον κίνδυνο απώλειας πραγματικών χρημάτων, αλλά και ενεργοποιούνται λειτουργίες αποσφαλμάτωσης (debugging) που δεν θα ήταν διαθέσιμες σε πραγματικές συνθήκες.

Υπάρχει πληθώρα εφαρμογών ανοιχτού κώδικα που επιτρέπει στον εκάστοτε προγραμματιστή να δημιουργήσει ένα τοπικό περιβάλλον blockchain στον προσωπικό του υπολογιστή και να προσομοιώσει συναλλαγές Ethereum εκεί. Το Geth, για παράδειγμα είναι ένα από τα πιο διαδεδομένα λογισμικά για την υλοποίηση ενός δικτύου στο οικοσύστημα του

Ethereum. Προσφέρει όμως και τη λειτουργία "dev mode" όπου οι προγραμματιστές μπορούν να τρέξουν έναν τοπικό κόμβο Ethereum. Αυτή η επιλογή παρέχει μια ρεαλιστική προσομοίωση ενός ζωντανού περιβάλλοντος Ethereum, με όλες τις αντίστοιχες λειτουργίες.

Για την υλοποίηση της εφαρμογής που περιγράφεται εδώ, επιλέχθηκε εντούτοις το Ganache. Το Ganache επιλέχθηκε κυρίως επειδή αποτελεί εργαλείο της σουίτας εργαλείων Truffle. Ωστόσο, θα πρέπει να σημειωθεί ότι αναφέρεται συχνά πως οι προσομοιωμένες συναλλαγές στο Ganache είναι το ίδιο γρήγορες ή και γρηγορότερες από αυτές στο Geth, καθώς και ότι το περιβάλλον του Ganache είναι γενικά πιο απλό [39]. Ως εκ τούτου, νέοι προγραμματιστές μπορούν εύκολα να πλοηγηθούν στη γραφική διεπαφή που παρέχει. Για εφαρμογές μεγαλύτερης κλίμακας, ενδεχομένως η γνώση και χρήση του Geth να ήταν η ορθή επιλογή.

3.4 Διεπαφή με το Δίκτυο Blockchain

Η αλληλεπίδραση ενός χρήστη με το Blockchain μπορεί να επιτευχθεί πλήρως με τη χρήση του Truffle console, το οποίο είναι ένα εργαλείο της σουίτας Truffle που μπορεί να λειτουργήσει ταυτόχρονα ως διεπαφή χρήστη αλλά και ως πάροχος του δικτύου. Εν ολίγοις, μέσω του Truffle console υπάρχει η δυνατότητα να τοποθετηθούν έξυπνα συμβόλαια σε ένα δίκτυο blockchain, αλλά και να αλληλεπιδράσουν χρήστες με αυτά, χωρίς την ανάγκη για κάποιο εξωτερικό πορτοφόλι ή επιπλέον λογισμικό.

Ωστόσο, ο σκοπός της παρούσας εργασίας είναι η δημιουργία μιας ολοκληρωμένης αποκεντρωμένης εφαρμογής και αυτό απαιτεί και την υλοποίηση ενός προσκήνιου (front-end), το οποίο θα εκτελείται σε περιηγητές (browsers). Οι browsers δεν επικοινωνούν με το blockchain χωρίς τη βοήθεια κάποιου τρίτου προγράμματος. Αυτή τη γεφύρωση μεταξύ browser και δικτύου έρχονται να καλύψουν προγράμματα ή επεκτάσεις διεπαφής όπως αυτά που θα αναλύσουμε παρακάτω.

3.4.1 MetaMask [40]

Το MetaMask είναι ένα ηλεκτρονικό πορτοφόλι (wallet) το οποίο είναι διαθέσιμο για δωρεάν εγκατάσταση ως επέκταση στους περισσότερους browsers. Διατίθεται πλέον και ως εφαρμογή για κινητές συσκευές. Προσθέτει πληθώρα λειτουργιών αλληλεπίδρασης του browser με δίκτυα Ethereum Blockchain. Εντός του πορτοφολιού διατηρούνται με ασφάλεια τα ether του κάθε χρήστη. Ο χρήστης συνδέεται με μοναδικό συνθηματικό και μπορεί να δει το υπόλοιπο των κρυπτονομισμάτων του αλλά και να πραγματοποιήσει συναλλαγές με άλλους χρήστες του δικτύου στο οποίο ο ίδιος ανήκει. Το MetaMask έχει γίνει δημοφιλές τα τελευταία έτη και αξιοποιείται από πληθώρα αποκεντρωμένων εφαρμογών διαδικτύου, αλλά και κινητών συσκευών (Android & iOS DApps).

3.4.2 Trust Wallet [41]

Το Trust Wallet είναι ένα λογισμικό που παρέχει αρκετά παρόμοιες λειτουργικότητες με το MetaMask. Είναι δηλαδή ένα πορτοφόλι κρυπτονομισμάτων που αναρτάται σε browsers ή εγκαθίσταται ως εφαρμογή σε κινητές συσκευές και επιτρέπει στους χρήστες να αποθηκεύουν,

να πουλούν και να αγοράζουν κρυπτονομίσματα. Ένα σημαντικό χαρακτηριστικό του είναι ότι υποστηρίζει πάνω από 100 είδη κρυπτονομισμάτων, σε αντίθεση με το MetaMask που υποστηρίζει αποκλειστικά κρυπτονομίσματα Ethereum. Η εν λόγω πλατφόρμα είναι αρκετά φιλική προς τους χρήστες και εμπεριέχει πολλές λειτουργίες διεπαφής που είναι εύκολα προσβάσιμες. Ωστόσο, το Trust Wallet προσφέρει λιγότερες επιλογές για προγραμματιστές. Αφορά κυρίως χρήστες οι οποίοι επιθυμούν να διαχειριστούν κρυπτονομίσματα σε πολλές πλατφόρμες blockchain παράλληλα.

3.4.3 Binance Web3 Wallet [42]

Το Binance Web3 Wallet είναι ένα ακόμη πορτοφόλι κρυπτονομισμάτων που μπορεί να χρησιμοποιηθεί με τη μορφή browser extension ή εφαρμογής. Υποστηρίζει και αυτό πολλά είδη κρυπτονομισμάτων και έχει παρόμοια διεπαφή με αυτήν του Trust Wallet. Συνδέεται βέβαια με πληθώρα εργαλείων της εταιρείας Binance και αποτελεί μέρος ενός ευρύτερου οικοσυστήματος, η χρήση του οποίου δεν εμπίπτει στους σκοπούς αυτής της διπλωματικής εργασίας.

3.4.4 Επιλογή του MetaMask

Υπάρχει πληθώρα χρηστικών εργαλείων για την διασύνδεση των browser με τα δίκτυα blockchain και την ανάλογη διεπαφή. Στο λογισμικό Wallet Connect [43], για παράδειγμα, μπορεί οποιοσδήποτε σχεδιαστής αποκεντρωμένων εφαρμογών - ή ακόμα και κάποιος απλός κάτοχος κρυπτονομισμάτων που επιθυμεί να τα διαχειριστεί αποτελεσματικά – να εξερευνήσει δεκάδες τέτοια λογισμικά και να επιλέξει κάποιο που ανταποκρίνεται στις ανάγκες του. Για την αποκεντρωμένη εφαρμογή KYE που αναπτύχθηκε σε αυτήν την εργασία, επιλέχθηκε η χρήση του MetaMask. Ο κύριος λόγος είναι η εστίαση του MetaMask στο Ethereum Blockchain, η απλότητά του, αλλά και η δημοφιλία του. Αποτελεί ένα εύχρηστο εργαλείο που δεν απαιτεί ιδιαίτερη εξοικείωση για την πλήρη αξιοποίησή του.

3.5 Εργαλεία για το προσκήνιο (front-end) της αποκεντρωμένης εφαρμογής

Η αλληλεπίδραση των χρηστών και των διαχειριστών με την αποκεντρωμένη εφαρμογή θα μπορούσε να υλοποιηθεί πλήρως με μια διεπαφή τερματικού (Command Line Interface). Ωστόσο, όπως αναφέρθηκε και στην παράγραφο 3.4, λόγω του μεγάλου συνόλου των λειτουργιών της KYE εφαρμογής, αλλά και της πολυπλοκότητας των δικαιωμάτων και των διαδικασιών ασφάλειας που απαιτεί η λειτουργία της, αποφασίστηκε η δημιουργία ενός προσκήνιου με πλήκτρα και πεδία εισόδου. Αυτό διευκολύνει σε μεγάλο βαθμό την κατανόηση της εφαρμογής από τους χρήστες, αλλά βοηθάει και σε θέματα οργάνωσης την συνολική ανάπτυξη (full stack) της εφαρμογής. Για να υλοποιηθεί το front-end χρειάστηκε να ενσωματωθούν κάποια επιπλέον εργαλεία και να εναρμονιστούν με αυτά που ήδη χρησιμοποιήσαμε.

3.5.1 Hypertext Markup Language (HTML) [44] & Cascading Style Sheets (CSS) [45]

Η HTML (HyperText Markup Language) είναι η βασική γλώσσα που χρησιμοποιείται για τη δομή και την οργάνωση του περιεχομένου σε ιστοσελίδες, ενώ η CSS (Cascading Style Sheets) είναι η γλώσσα που καθορίζει την εμφάνιση και τη μορφοποίηση του περιεχομένου της ιστοσελίδας. Με την CSS προσθέτει κανείς γραμματοσειρές, στυλ και μορφές διάταξης στο κείμενο και στα κουμπιά της εφαρμογής. Στην ανάπτυξη του front-end της αποκεντρωμένης εφαρμογής, επιλέχθηκαν και οι δύο γλώσσες, καθώς επιτρέπουν την αποτελεσματική διάταξη των στοιχείων της σελίδας και την εξατομίκευση της αισθητικής της εφαρμογής. Μέσω της HTML δημιουργήθηκε το πλαίσιο για την οργάνωση των λειτουργιών της εφαρμογής, ενώ η CSS χρησιμοποιήθηκε για τη βελτίωση της εμφάνισης και της αλληλεπίδρασης των χρηστών με την εφαρμογή. Η χρήση αυτών των τεχνολογιών συμβάλλει στην καλύτερη κατανόηση του τρόπου λειτουργίας της εφαρμογής.

3.5.2 Το Web3.js [46] στο Front-End και ως API

Το Web3.js είναι μια συλλογή βιβλιοθηκών που επιτρέπουν την αλληλεπίδραση με έναν κόμβο ενός δικτύου blockchain μέσω των πρωτοκόλλων HTTP, IPC ή WebSocket. Στις αποκεντρωμένες εφαρμογές, το Web3.js χρησιμοποιείται ώστε να αλληλεπιδράσει ο browser με το Ethereum blockchain μέσω ενός front-end. Ενώ το front-end τρέχει στον browser, οι ενέργειες του χρήστη θα πρέπει να καλέσουν κάποιες συναρτήσεις από το smart contract, το οποίο στην περίπτωσή μας αποτελεί το παρασκήνιο (back-end). Αυτές οι ενέργειες θα έχουν και την ανάλογη επίδραση στο πορτοφόλι (wallet) του χρήστη. Όπως περιγράφεται και στην παράγραφο 3.4.4, η τεχνολογία wallet που χρησιμοποιείται στην αποκεντρωμένη εφαρμογή ΚΥΕ είναι το MetaMask. Το Web3.js είναι λοιπόν ο τρόπος διασύνδεσης του MetaMask με τα έξυπνα συμβόλαια που είναι αναρτημένα στο Ethereum Blockchain. Ως εκ τούτου, ο χρήστης της εφαρμογής μπορεί να κάνει συναλλαγές πιέζοντας πλήκτρα στο front-end, να ενεργοποιεί συναρτήσεις του Web3.js, οι οποίες με τη σειρά τους ενεργοποιούν συναρτήσεις του έξυπνου συμβολαίου και διαχειρίζονται τα κόστη αυτών για το πορτοφόλι του χρήστη. Τις αλλαγές στο πορτοφόλι του ο χρήστης μπορεί να τις δει μέσω του MetaMask.

Υπό αυστηρότερη έννοια θα λέγαμε ότι το Web3.js δρα ως ένα API (Application Programming Interface) για την αποκεντρωμένη εφαρμογή μας. Όπως ένα API φροντίζει για την αλληλεπίδραση του front-end με έναν παραδοσιακό server που εκτελεί λειτουργίες του back-end, έτσι και στην περίπτωσή μας, τα σενάρια που τρέχουν με χρήση του Web3.js φροντίζουν για την αλληλεπίδραση του front-end με το Blockchain και το MetaMask.

Crypto.js [47]

Θα πρέπει σε αυτό το σημείο να σημειωθεί ότι εντός των σεναρίων που χρησιμοποιούν το Web3.js, αξιοποιείται και η βιβλιοθήκη crypto.js. Η τελευταία είναι μια βιβλιοθήκη γραμμένη σε JavaScript και επιτρέπει στους προγραμματιστές να ενσωματώσουν σχετικά προηγμένες λειτουργίες κρυπτογράφησης στις διαδικτυακές εφαρμογές τους. Η βιβλιοθήκη προσφέρει εργαλεία για την κρυπτογράφηση, αποκρυπτογράφηση, κατακερματισμό και παραγωγή υπογραφών για δεδομένα, κάνοντας τη διαδικασία κρυπτογραφίας προσβάσιμη απευθείας στον browser. Υποστηρίζει συμμετρικούς αλγόριθμους όπως AES (Advanced Encryption

Standard) και περαιτέρω γνωστούς αλγόριθμους όπως SHA-256, SHA-512, MD5, για τον κατακερματισμό δεδομένων. Στην εφαρμογή μας, η Cypto.js χρησιμοποιείται για την κρυπτογράφηση των δεδομένων των χρηστών πριν αυτά κωδικοποιηθούν με τη μορφή NFT και αναρτηθούν στο IPFS.

3.6 IPFS

Το Διαπλανητικό Σύστημα Αρχείων (IPFS) είναι ένα σύνολο ομότιμων πρωτόκολλων (peer-to-peer) για τη δεικτοδότηση, δρομολόγηση και μεταφορά δεδομένων σε ένα αποκεντρωμένο σύστημα αρχείων. Πολλά δημοφιλή έργα Web3 είναι βασισμένα πάνω στο IPFS [48]. Κάθε αρχείο που προστίθεται στο IPFS λαμβάνει μια μοναδική διεύθυνση. Η διεύθυνση αυτή είναι μία συμβολοσειρά, ονομάζεται Αναγνωριστικό Περιεχομένου (Content Identifier-CID) και προκύπτει από τον συνδυασμό του hash του αρχείου και ενός μοναδικού αναγνωριστικού για τον αλγόριθμο hash που χρησιμοποιήθηκε.

3.6.1 Pinata

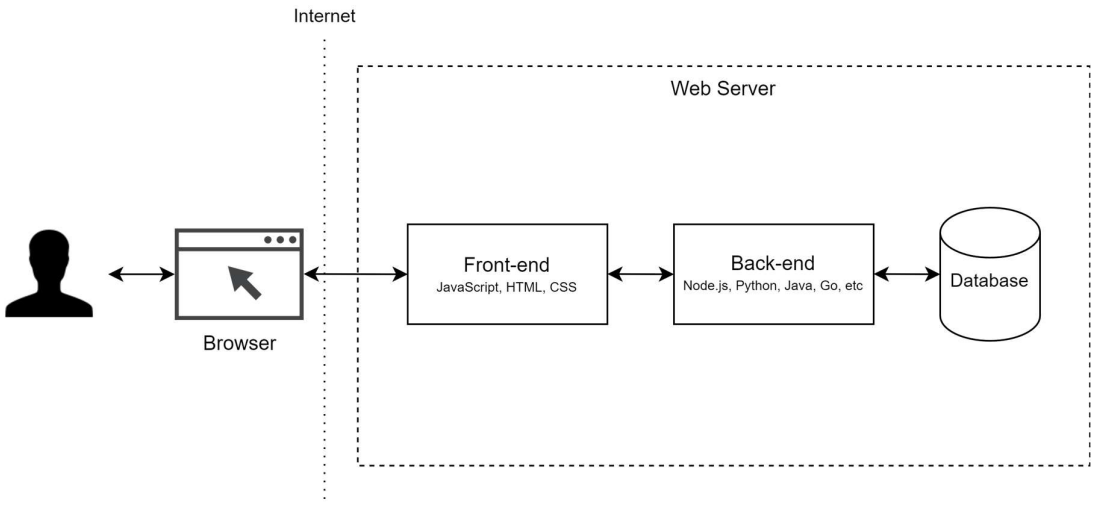
Για τους σκοπούς της εργασίας μας χρησιμοποιήσαμε το Pinata το οποίο είναι μια υπηρεσία ανάρτησης στο IPFS (IPFS pinning service). Το Pinata παρέχει ένα API το οποίο επιτρέπει το ανέβασμα αρχείων στο IPFS και το κατέβασμα αρχείων από αυτό. Επιπλέον, προσφέρει μια διεπαφή με τον χρήστη (UI) για την εύκολη εποπτεία των δεδομένων που έχουν αναρτηθεί στο IPFS και των ταυτοτήτων τους.

4 Σχεδίαση και Υλοποίησης της Αποκεντρωμένης Εφαρμογής

4.1 Εισαγωγή

Οι αποκεντρωμένες εφαρμογές που αξιοποιούν το Ethereum blockchain αλλά και γενικότερα όλες οι αποκεντρωμένες εφαρμογές αποτελούν κομμάτι της νέας γενιάς διαδικτυακών πρωτοκόλλων που στο σύνολό τους ονομάζονται Web 3.0. Το Web 3.0 έχει επικρατήσει τις τελευταίες δύο δεκαετίες έναντι του Web 2.0 και μία σύγκριση μεταξύ των δύο θα ήταν αρκετά χρήσιμη για να γίνουν αντιληπτές οι διαφορές τους αλλά και για να γίνει πιο κατανοητή η αρχιτεκτονική μίας εφαρμογής Web 3.0 και η χρησιμότητα αυτής.

Σε μία αρχιτεκτονική Web 2.0 ο χρήστης επικοινωνεί μέσω μιας διεπαφής προσκηνίου (front-end) στέλνοντας εντολές σε έναν εξυπηρετητή (server) ο οποίος περιέχει τα δεδομένα που απαιτούνται για την αλληλεπίδραση του χρήστη και τη λειτουργία της Web 2.0 εφαρμογής συγκεντρωμένα όλα στο ίδιο σημείο ή έστω ανάμεσα σε ένα σύνολο server που είναι τοποθετημένοι σε συγκεκριμένες τοποθεσίες. Δεν υπάρχει δηλαδή ουσιαστική αποκέντρωση καθώς τα δεδομένα είναι αποθηκευμένα σε συγκεκριμένους φυσικούς χώρους. Το ίδιο ισχύει και την επεξεργαστική δύναμη, αφού τα αιτήματα των χρηστών και η εξυπηρέτησή τους γίνονται από μία συγκεντρωμένη μονάδα επεξεργασίας δηλαδή κάποιους συγκεντρωμένους υπολογιστές οι οποίοι εξυπηρετούν τα αιτήματα. Όταν για παράδειγμα ένας χρήστης εκτελεί μία αναζήτηση μέσα στην εφαρμογή πληκτρολογεί τις λέξεις κλειδιά της αναζήτησης , τις στέλνει στον server, ο server ψάχνει στη βάση δεδομένων, επεξεργάζεται τα δεδομένα και τα επιστρέφει στον χρήστη.

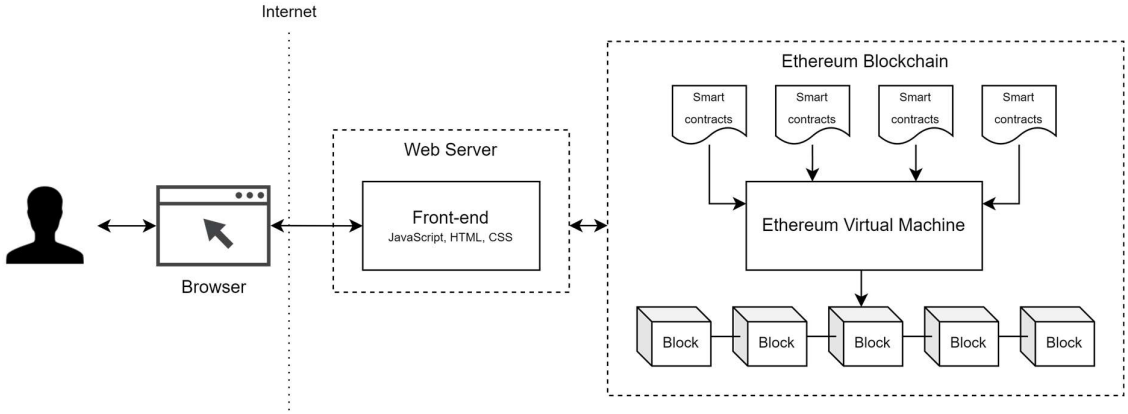


Εικόνα 4-1 Σχεδιάγραμμα Αρχιτεκτονικής Web 2.0 εφαρμογής

Αντίθετα, σε μία Web 3.0 εφαρμογή συναντάμε αποκέντρωση των δεδομένων αλλά και της επεξεργαστικής δύναμης που χρειάζονται για να λειτουργήσει η εφαρμογή. Στην

περίπτωση των αποκεντρωμένων εφαρμογών που βασίζονται στην τεχνολογία του blockchain και συγκεκριμένα σε αυτές που βασίζονται στο Ethereum υπάρχει το EVM (Ethereum Virtual Machine) το οποίο διατηρεί την κατάσταση όλου του δικτύου, η οποία μάλιστα είναι ορατή από όλους τους κόμβους του. Έτσι, οποιαδήποτε αλλαγή κατάστασης του δικτύου καταγράφεται στο EVM. Την καταγραφή και την επεξεργασία αλλαγής κατάστασης την εκτελούν οι κόμβοι που ονομάζονται «minters», προσφέρει δηλαδή και αποκέντρωση επεξεργαστικής ισχύος. Επειδή η κατάσταση του EVM είναι αποθηκευμένη και ορατή σε όλους τους κόμβους, έχουμε απουσία κεντρικού μέρους αποθήκευσης πληροφοριών. Αντίθετα από τις παραδοσιακές εφαρμογές, λόγω της χρήσης του EVM, δεν υπάρχει η δυνατότητα ουσιαστικής διαγραφής δεδομένων αφού όλες οι αλλαγές καταγράφονται και δεν μπορούν να αφαιρεθούν.

Από τη στιγμή που δεν υπάρχει διαγραφή των δεδομένων-συναλλαγών, με το πέρασμα του χρόνου συσσωρεύεται μεγάλος όγκος πληροφορίας στο EVM και οι κόμβοι δυσκολεύονται να το υποστηρίξουν. Επομένως, είναι αναγκαίο δεδομένα μεγάλου όγκου να αποθηκεύονται σε κάποιο εξωτερικό σύστημα. Τη λειτουργία αυτή την εξυπηρετούν αποκεντρωμένες βάσεις δεδομένων όπως το IPFS.



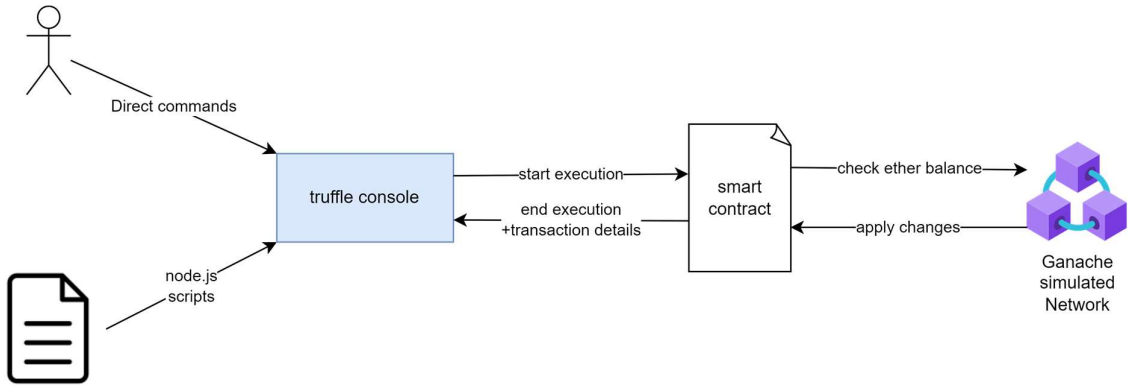
Εικόνα 4-2 Σχεδιάγραμμα Αρχιτεκτονικής Web 3.0 εφαρμογής

Αξίζει να σημειωθεί ότι οι αποκεντρωμένες εφαρμογές εκτός από την αποκέντρωση δίνουν έμφαση στην αξιοπιστία και την κρυπτογράφηση των στοιχείων, αφού δεν υπάρχει κάποιος κεντρικός οργανισμός να ελέγχει τις συναλλαγές όπως γίνεται στις παραδοσιακές εφαρμογές. Άρα, για να εξασφαλιστεί η ασφάλεια εμπιστεύονται κάποιους παρόχους (π.χ. MetaMask) οι οποίοι φροντίζουν για την υπογραφή των συναλλαγών με ιδιωτικές υπογραφές αλλά και για την ομαλή διασύνδεση του front end με το blockchain.

Επιπλέον, ο κώδικας σε Web 3.0 εφαρμογές δεν είναι γραμμένος σε παραδοσιακές γλώσσες προγραμματισμού (π.χ javascript) αλλά σε γλώσσες όπως η Solidity που μπορούν να μεταγλωττιστούν και να τρέξουν στο EVM. Τέλος, το smart contract δεν μπορεί να αλλάξει.

4.2 Σχεδιασμός Εφαρμογής

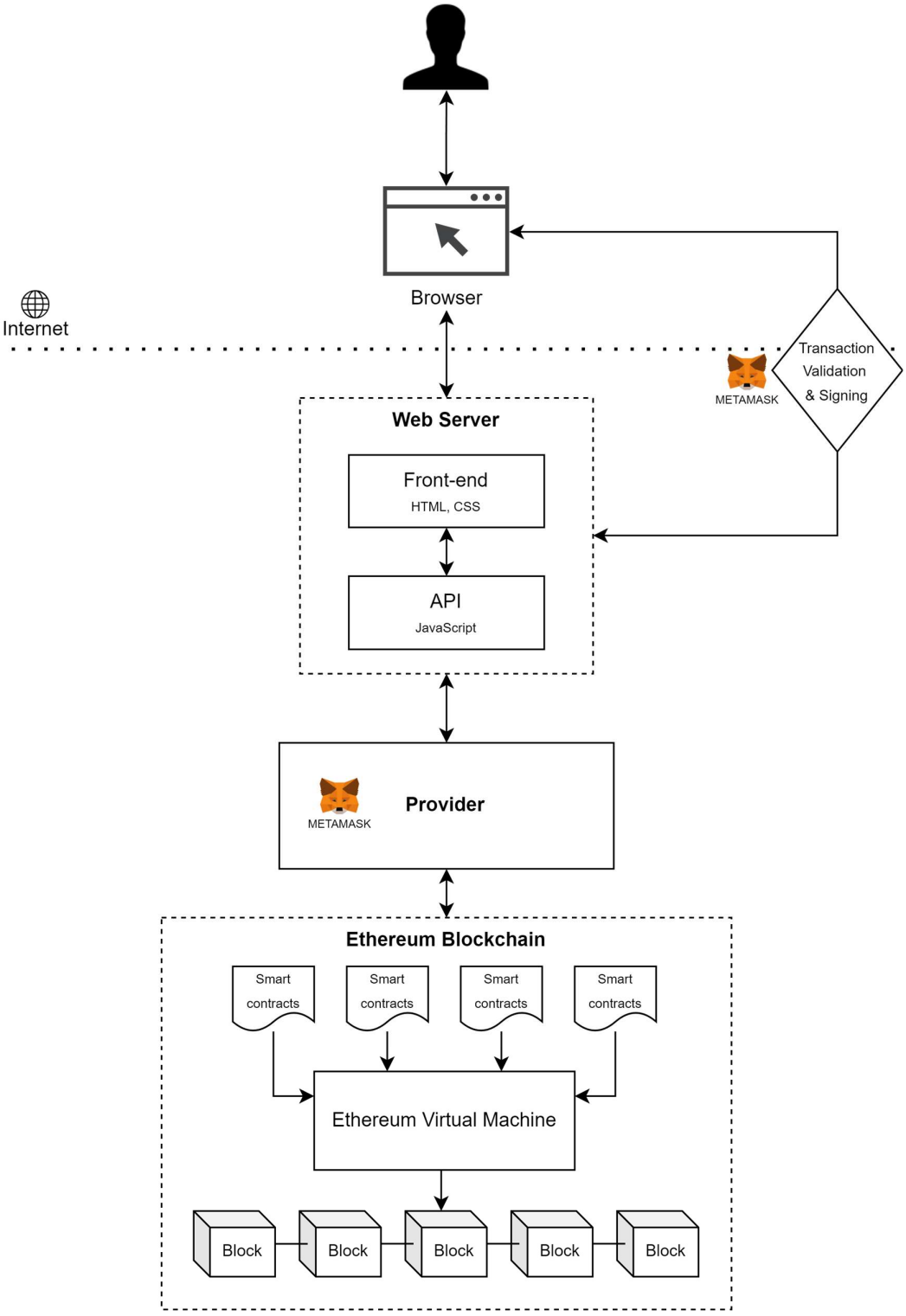
Οι περισσότερες αποκεντρωμένες εφαρμογές ακολουθούν έναν παρόμοιο τρόπο διαχείρισης της ροής της πληροφορίας. Ο χρήστης μπορεί να εκτελέσει μεθόδους του έξυπνου συμβολαίου πληκτρολογώντας εντολές σε μία κονσόλα ή ομαδοποιώντας τις εντολές αυτές στη μορφή ενός σεναρίου (script). Το έξυπνο συμβόλαιο μεταγλωττίζεται σε γλώσσα μηχανής και διαβάζεται από το Ethereum Virtual Machine ή το αντίστοιχο εργαλείο σε άλλα είδη blockchain. Με τον τρόπο αυτόν ελέγχονται οι παράμετροι του δικτύου που αφορούν τη μέθοδο που κάλεσε ο χρήστης και αν η κατάσταση του δικτύου ικανοποιεί κάποιες προϋποθέσεις τότε η εντολές του χρήστη εκτελούνται, η κατάσταση του δικτύου ανανεώνεται και στον χρήστη επιστρέφονται τα αποτελέσματα της εκτέλεσης. Η παραπάνω διαδικασία αποτυπώνεται στην Εικόνα 4-3.



Εικόνα 4-3: Η αποκεντρωμένη εφαρμογή στην αρχική μορφή της.

Για τη μελέτη αυτής της εργασίας επιλέξαμε να διευρύνουμε αυτήν την αρχιτεκτονική ώστε να διευκολύνουμε την διεπαφή των χρηστών με το δίκτυο blockchain, να ενσωματώσουμε περισσότερες λειτουργίες και να εξασφαλίσουμε ότι η εφαρμογή μπορεί να κλιμακωθεί και να φιλοξενήσει έναν μεγάλο αριθμό χρηστών.

4.2.1 Αρχιτεκτονική Αποκεντρωμένης Εφαρμογής



Εικόνα 4-4 Αρχιτεκτονική της αποκεντρωμένης εφαρμογής χωρίς τη χρήση IPFS

Αρχικά, προσθέσαμε προσκήνιο (front-end) στην εφαρμογή μας ώστε να γίνει πιο εύκολη και γρήγορη η χρήση της. Το προσκήνιο εκτελείται σε φυλλομετρητές (browsers) και ως εκ τούτου χρειάστηκε να δημιουργήσουμε ένα API ώστε οι μέθοδοι που ο χρήστης καλεί στο προσκήνιο να καλούν με τη σειρά τους τις αντίστοιχες μεθόδους του έξυπνου συμβολαίου. Ωστόσο, για να γίνει αυτή η σύνδεση απαιτείται ένας πάροχος (provider) ο οποίος επικοινωνεί και με τον φυλλομετρητή και με το δίκτυο blockchain. Στην περίπτωσή μας, επιλέξαμε για πάροχο το MetaMask.

Το MetaMask εκτός από ως πάροχος λειτουργεί και ως σύστημα διαχείρισης των πορτοφολιών των χρηστών (wallet management system). Η πιο σημαντική λειτουργία του, ωστόσο, είναι ότι υπογράφει και επιβεβαιώνει τις συναλλαγές που εκτελούνται μέσω του έξυπνου συμβολαίου με τη βοήθεια των δημόσιων (public) και ιδιωτικών (private) κλειδιών των χρηστών. Τα παραπάνω φαίνονται στην Εικόνα 4-4.

Συνοπτικά η εφαρμογή μας αποτελείται από:

- **Browser:** Φιλοξενεί το προσκήνιο της εφαρμογής εκτελώντας τον κώδικα που είναι γραμμένος σε CSS και HTML.

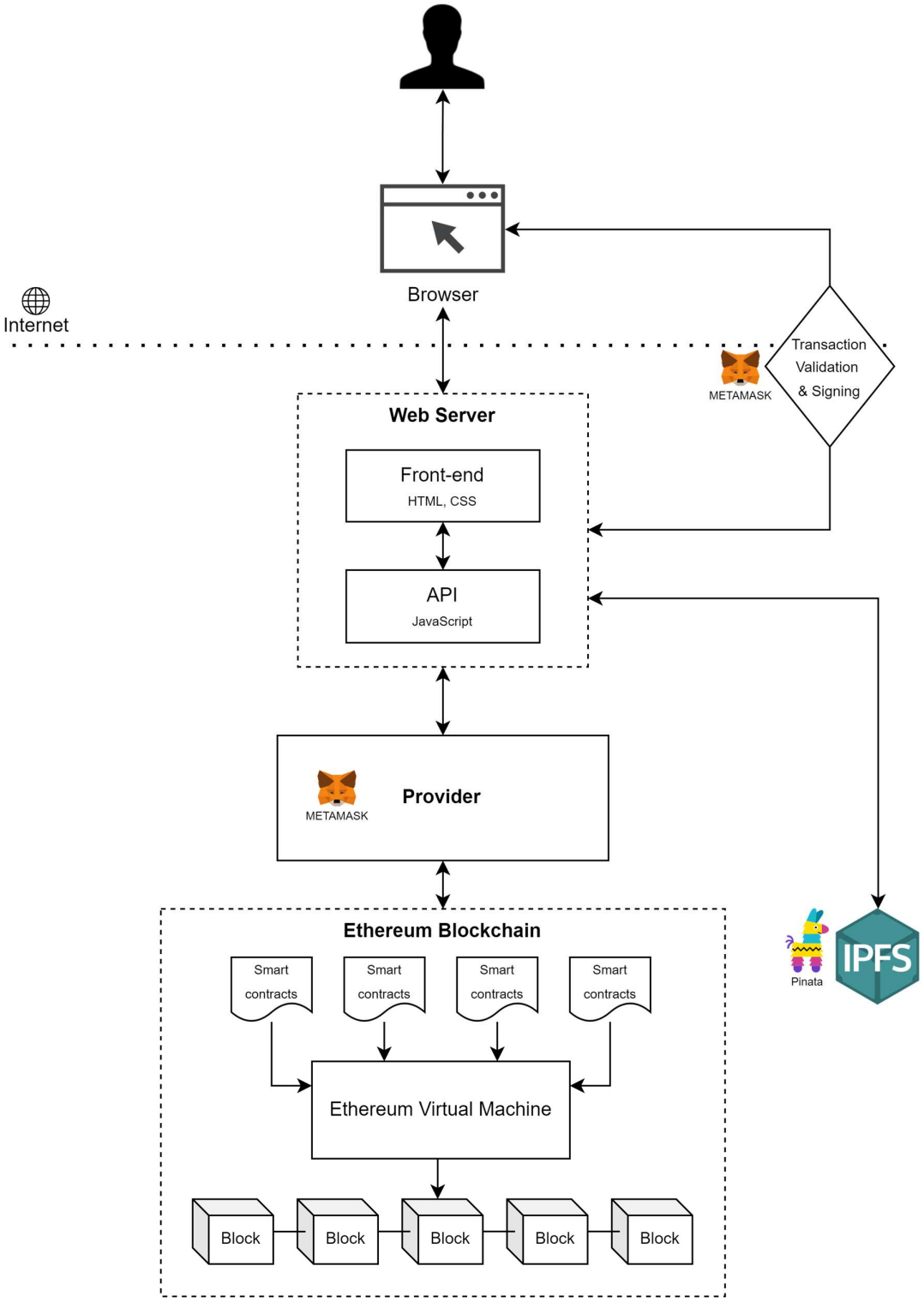
- **Web Server:** Περιέχει το front-end με τα αρχεία της HTML και CSS. Επιπλέον, περιέχει τα αρχεία που είναι γραμμένα σε JavaScript δηλαδή, αυτά που συντελούν το API (app.js κλπ.).

- **Πάροχο** (provider) : Βοηθάει στην επικοινωνία μεταξύ Web Server και Ethereum. Επιπλέον, βοηθάει στην επικύρωση και υπογραφή των συναλλαγών. Επιλέχθηκε το MetaMask.

- **Blockchain:** Πιο συγκεκριμένα Ethereum Blockchain. Στο blockchain υπάρχει το έξυπνο συμβόλαιο που καθορίζει όλες τις συναλλαγές που γίνονται. Αναπτύχθηκε με τη βοήθεια του Truffle και της εφαρμογής Ganache.

Η τελική μορφή της εφαρμογής έχει ένα επιπλέον στάδιο εκτός από τα παραπάνω: τη σύνδεση με μια υπηρεσία IPFS. Τα δεδομένα πριν αποθηκευτούν κρυπτογραφούνται και ύστερα αναρτώνται σε ένα κατανεμημένο σύστημα αρχείων με τη βοήθεια της εφαρμογής “Pinata”, ενός παρόχου υπηρεσιών IPFS. Δηλαδή, όπως έχουμε προαναφέρει η εφαρμογή μας αποθηκεύει τα δεδομένα ΚΥΕ των εργαζομένων με αποκεντρωμένο τρόπο και όχι σε έναν κεντρικό server ή ένα σύνολο από servers. Η ολοκληρωμένη αρχιτεκτονική της αποκεντρωμένης εφαρμογής φαίνεται στην Εικόνα 4-5.

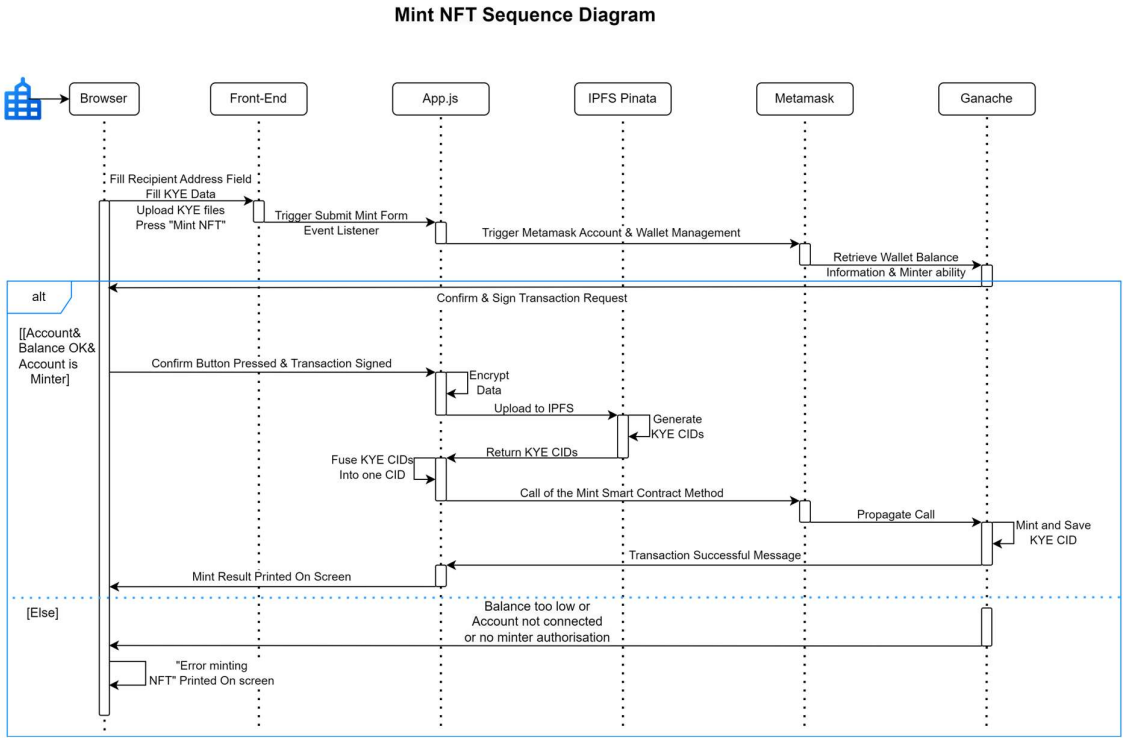
Στα sequence διαγράμματα της επόμενης ενότητας φαίνονται αναλυτικά τα βήματα που ακολουθούνται σε κάθε μέθοδο της αποκεντρωμένης εφαρμογής.



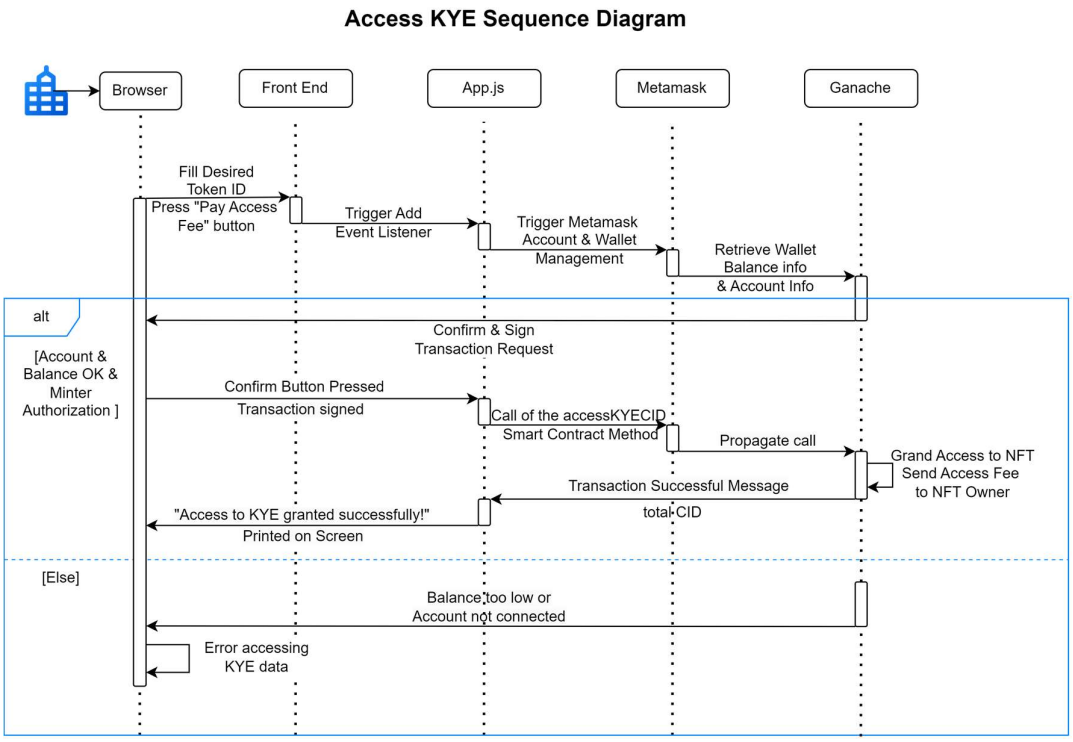
Εικόνα 4-5 Αρχιτεκτονική της αποκεντρωμένης εφαρμογής μας με τη χρήση IPFS

4.2.2 Περιπτώσεις Χρήσης

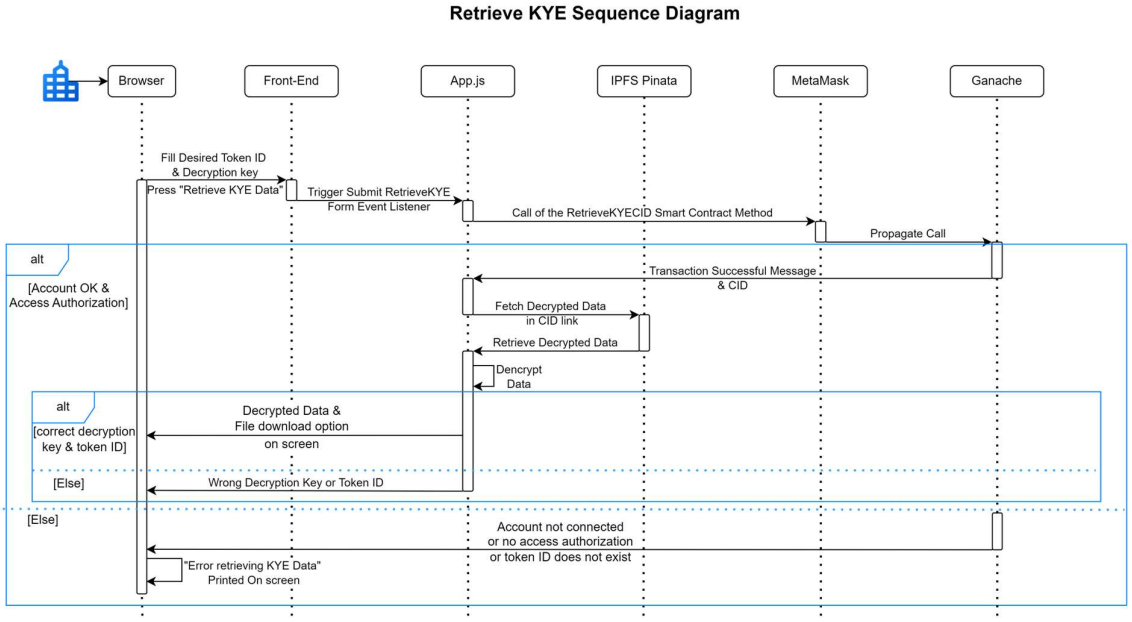
Παρακάτω παρουσιάζονται Sequence Διαγράμματα για κάθε διαδικασία της αποκεντρωμένης εφαρμογής. Φαίνεται βήμα-βήμα πώς γίνεται η επικοινωνία και η σύνδεση όλων των ξεχωριστών κομματιών της αρχιτεκτονικής που παρουσιάστηκε παραπάνω. Καταγράφεται η ροή της πληροφορίας κατά την αλληλεπίδραση των υποσυστημάτων της αποκεντρωμένης εφαρμογής. Τέλος, γίνονται πιο ξεκάθαρες οι προϋποθέσεις επιτυχούς εκτέλεσης των λειτουργιών της εφαρμογής.



Διάγραμμα 4-1 Mint NFT Sequence

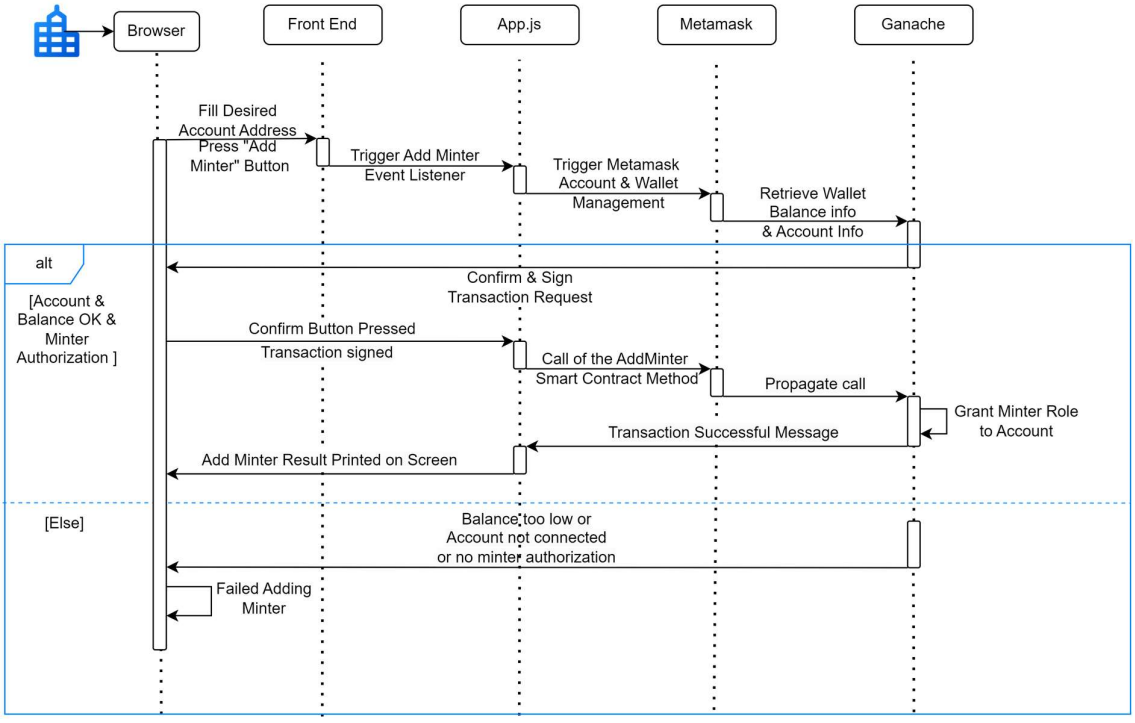


Διάγραμμα 4-2 Access KYE sequence



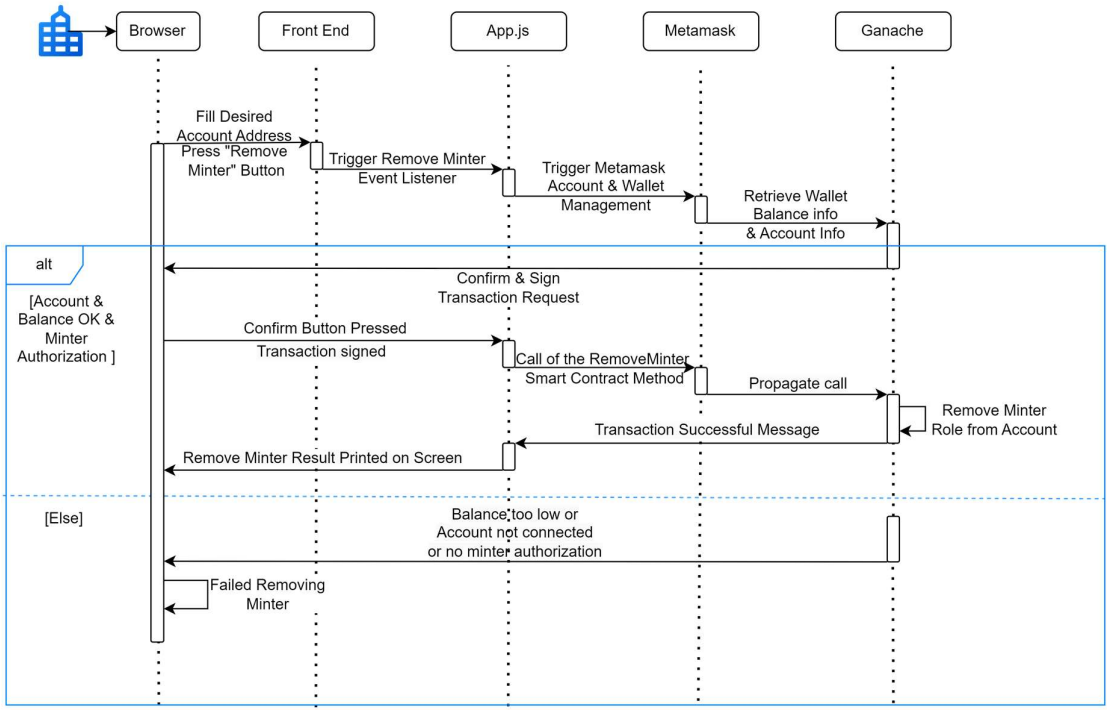
Διάγραμμα 4-3 Retrieve KYE Sequence

Add Minter Sequence Diagram

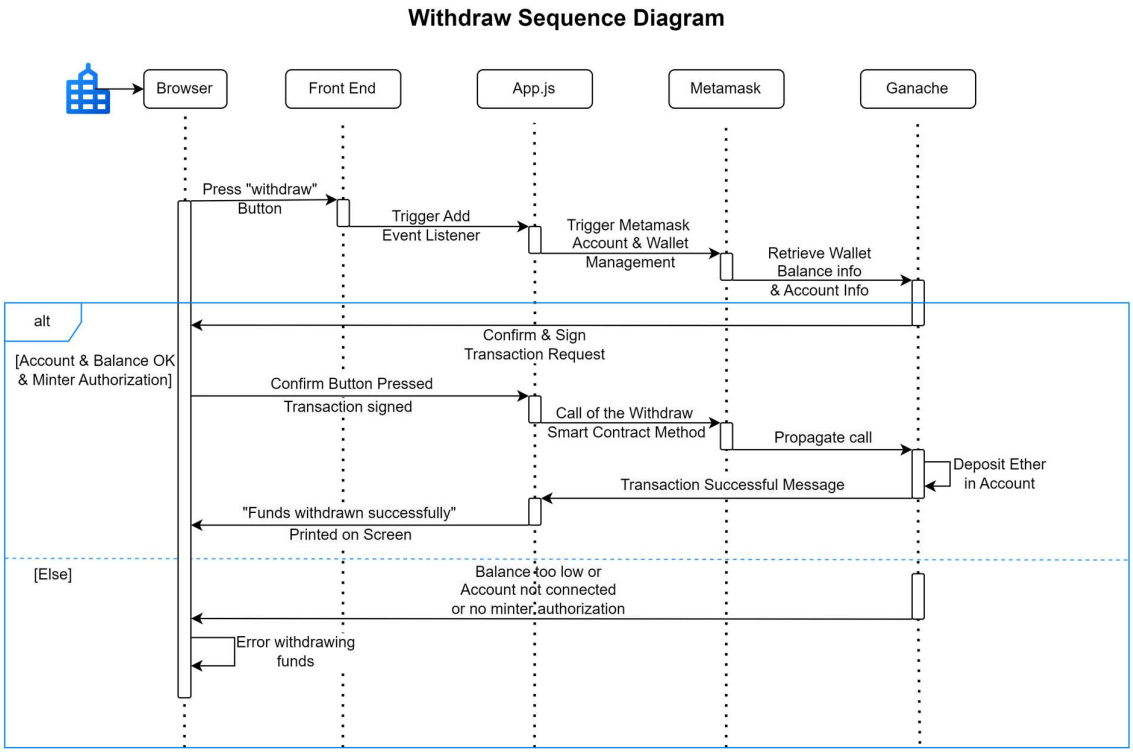


Διάγραμμα 4-4 Add Minter Sequence

Remove Minter Sequence Diagram



Διάγραμμα 4-5 Remove Minter Sequence



Διάγραμμα 4-6 Withdraw Funds Sequence

4.3 Υλοποίηση Συστήματος

Στην υλοποίησή μας έχουμε επιλέξει να έχουμε 5 λογαριασμούς. Ο πρώτος λογαριασμός με index 0 αντιπροσωπεύει έναν Κυβερνητικό Φορέα (πχ Αστυνομία, ΚΕΠ). Είναι υπεύθυνος για την σωστή και έγκυρη δημοσίευση δεδομένων στο blockchain. Έχει την δυνατότητα να κόψει ένα κρυπτοπαραστατικό (Mint NFT). Επίσης, μπορεί να ορίσει άλλους λογαριασμούς να έχουν το παραπάνω δικαίωμα ή και να τους το αφαιρέσει. Οι λογαριασμοί με index 1 και 2 αντιπροσωπεύουν απλούς πολίτες των οποίων τα ΚΥΕ ανεβάζει ο Φορέας στο blockchain. Ο Λογαριασμός με index 4 αντιπροσωπεύει έναν άλλον κυβερνητικό φορέα που δεν έχει εξ αρχής δυνατότητα να κάνει mint ενώ ο λογαριασμός με index 3 αντιπροσωπεύει τον λογαριασμό που θέλει να πάρει τα ΚΥΕ.

4.3.1 Δημιουργία περιβάλλοντος αλυσίδας κορμού (blockchain).

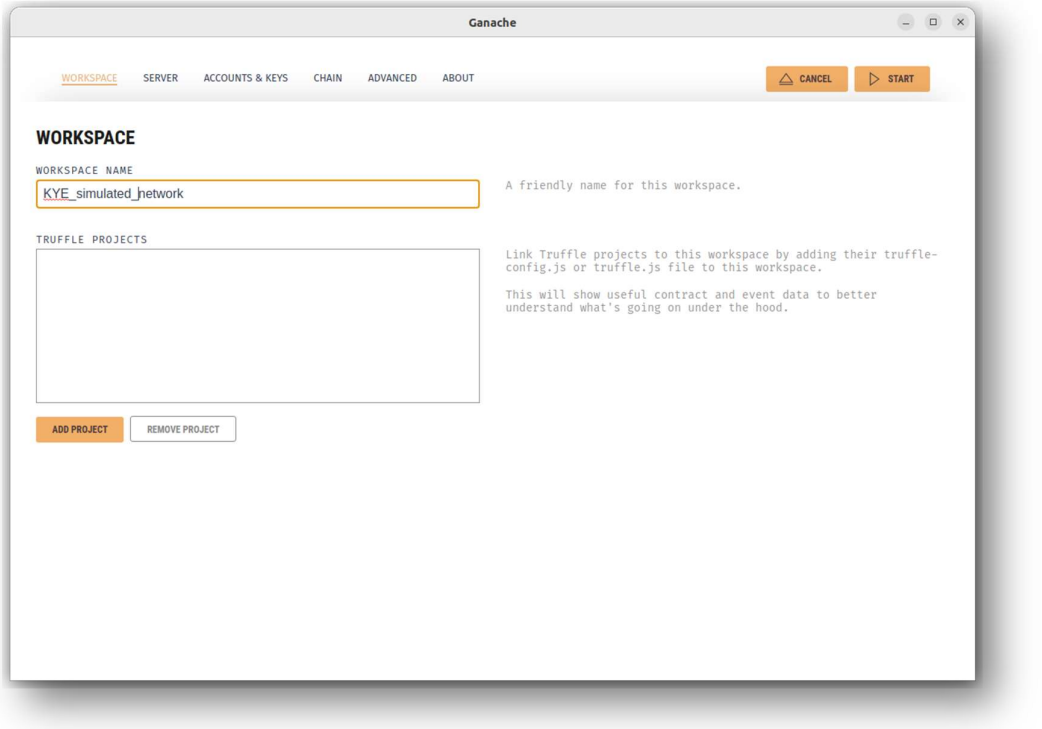
Truffle

Το EVM δεν μπορεί να εκτελέσει κώδικα που είναι γραμμένος σε υψηλού επιπέδου γλώσσα (π.χ. Solidity, Vyper), αλλά εκτελεί κώδικα σε γλώσσα μηχανής. Απαραίτητο εργαλείο για τη μεταγλώττιση του κώδικα των έξυπνων συμβολαίων σε γλώσσα μηχανής είναι το Truffle.

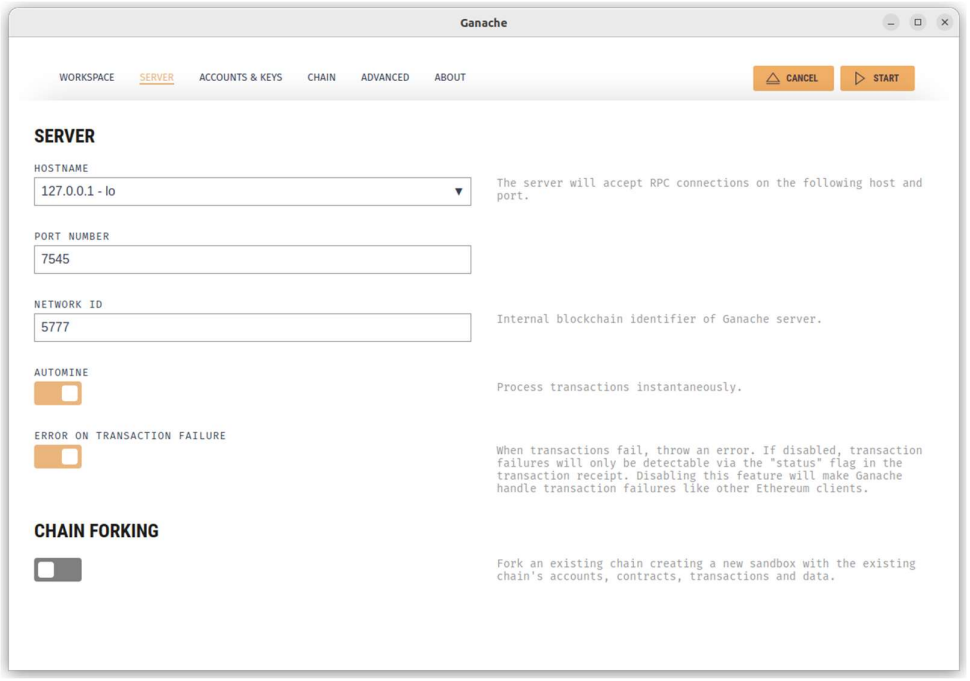
Για την εγκατάσταση του Truffle χρησιμοποιήθηκε η εντολή «npm install -g truffle». Το Truffle είναι επίσης υπεύθυνο για την ανάρτηση του έξυπνου συμβολαίου στο δίκτυο που φιλοξενείται από το Ganache («truffle migrate»). Τέλος, το Truffle επιτρέπει την εκτέλεση σεναρίων (scripts) και εντολών node.js μέσω της κονσόλας (truffle console).

Ganache

Για να δημιουργήσουμε την εφαρμογή μας πρέπει να προσομοιώσουμε ένα περιβάλλον αλυσίδας-κορμού (blockchain) Ethereum, έτσι, διαλέξαμε την εφαρμογή Ganache. Αρχικά, διαλέγουμε το όνομα που θα δώσουμε στον χώρο εργασίας (workspace). Όπως φαίνεται και στην Εικόνα 4-6 δόθηκε το όνομα «KYE_Simulated_network». Έπειτα, δηλώνουμε ότι το περιβάλλον εργασίας τρέχει στην πόρτα (portal number) *7545* στο τοπικό δίκτυο *127.0.0.1* και network id το *5777* (Εικόνα 4-7).

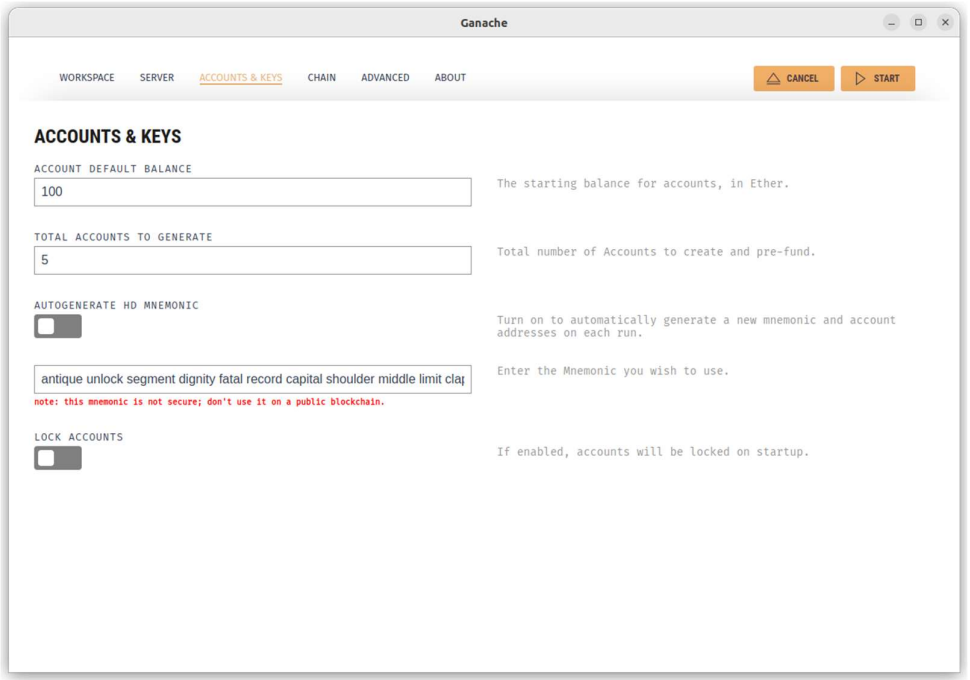


Εικόνα 4-6 Ονοματοδοσία του χώρου εργασίας (workspace) που θα χρησιμοποιήσουμε.

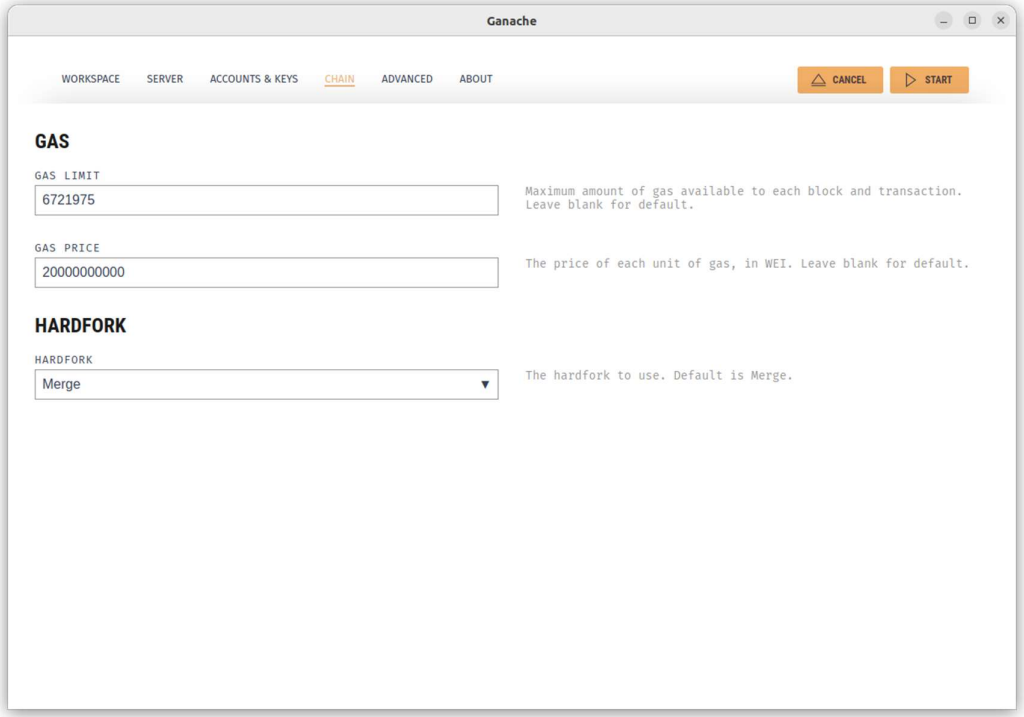


Εικόνα 4-7 Επιλογή Hostname και Port Number

Για λόγους ευκολίας και ανάπτυξης επιλέξαμε να δημιουργηθούν 5 λογαριασμοί (accounts) με αρχικό ποσό 100 ETH στον καθένα. Το μνημονικό ήταν αυτό που προτάθηκε από την εφαρμογή Ganache δηλαδή «antique unlock segment dignity fatal record capital shoulder middle limit clap key». Οι επιλογές για gas limit, gas price και hard fork έμειναν όπως προτείνονται από την εφαρμογή Ganache.

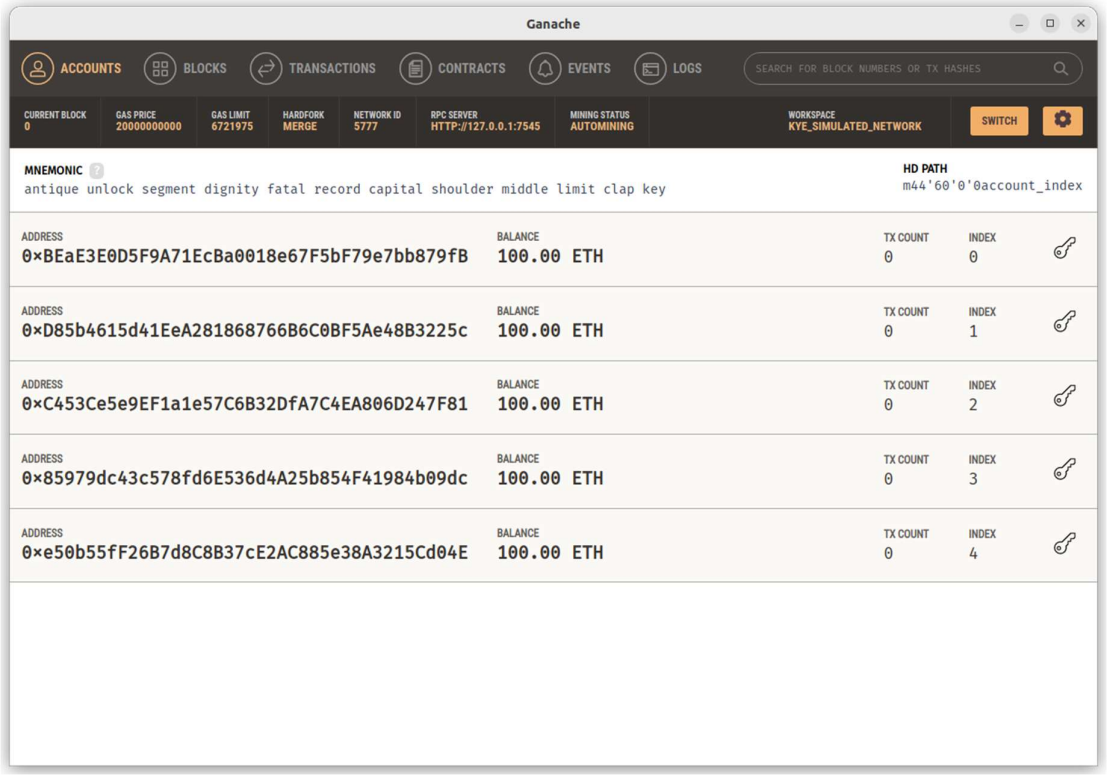


Εικόνα 4-8 Επιλογή αριθμού λογαριασμών και αρχικού ποσού που θα δίνεται στον καθένα



Εικόνα 4-9 Επιλογή gas limit, gas price, hardfork

Αφού γίνουν όλα τα παραπάνω, επιλέγουμε το κουμπί «Start» και δημιουργείται το περιβάλλον του blockchain. Μέσα από την εφαρμογή Ganache μπορούμε ανά πάσα στιγμή να δούμε το υπόλοιπο των λογαριασμών σε ETH, πόσες συναλλαγές έχουν γίνει , τη διεύθυνση και το ιδιωτικό κλειδί (address and private key) κάθε λογαριασμού, τα blocks που έχουν δημιουργηθεί, τη διεύθυνση του έξυπνου συμβολαίου (smart contract) αλλά και άλλες πληροφορίες για το περιβάλλον μας όπως φαίνονται στην Εικόνα 4-10.



Εικόνα 4-10 Περιβάλλον Ganache Blockchain

4.3.2 Δημιουργία Έξυπνου Συμβολαίου

Στη συνέχεια γράφουμε το έξυπνο συμβόλαιο (smart contract) με τις επιθυμητές συναρτήσεις. Οι συναρτήσεις είναι οι εξής:

- **mint :** Παίρνει σαν είσοδο τη διεύθυνση του παραλήπτη και τον σύνδεσμο CID που οδηγεί στα δεδομένα KYE στο IPFS. Η συνάρτηση μπορεί να κληθεί μόνο από χρήστες που έχουν τον ρόλο «minter» και ο καλών της συνάρτησης χρεώνεται ένα προκαθορισμένο ποσό για την κλήση της. Ουσιαστικά, η mint κόβει ένα NFT και του αντιστοιχίζει ένα μοναδικό αναγνωριστικό το token ID. Αλλάζει το state του EVM ανεβάζοντας το συνολικό αριθμό NFT κατά ένα και αποθηκεύει το KYECID σύνδεσμο (link) μέσα σε αυτό. Τέλος, επιστρέφει το token ID του NFT που κόπηκε.

- **_setKYECID:** Καλείται εσωτερικά (internal function). Αποθηκεύει τον σύνδεσμο KYECID αντιστοιχίζοντας το με το token ID. Παίρνει σαν είσοδο το KYECID, και token ID.

- **accessKYECID:** Παίρνει σαν είσοδο το μοναδικό αναγνωριστικό (token ID) και επιτρέπει σε αυτόν που την καλεί να έχει στο εξής πρόσβαση στα δεδομένα που είναι αντιστοιχισμένα σε αυτό το token ID. Επιστρέφει τα δεδομένα KYE. Τα παραπάνω γίνονται εφόσον πληρωθεί ένα προκαθορισμένο αντίτιμο.

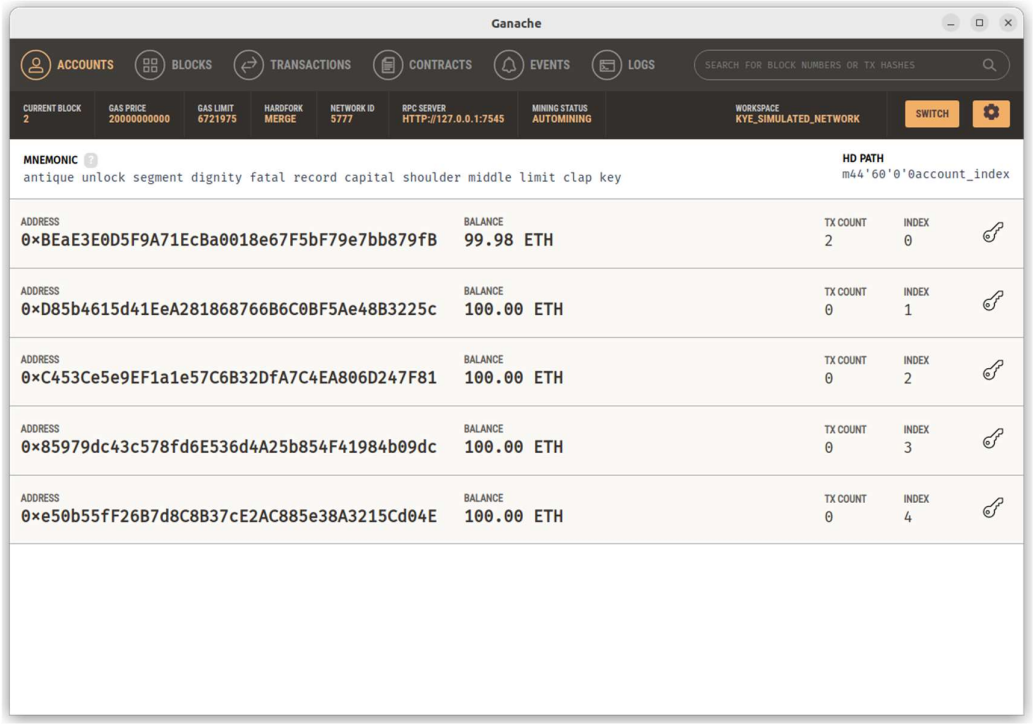
- **retrieveKYECID:** Παίρνει ως είσοδο το token ID. Επιστρέφει τον σύνδεσμο KYECID που οδηγεί στα δεδομένα που αντιστοιχούν σε αυτό το αναγνωριστικό (token ID). Τα παραπάνω προϋποθέτουν να έχει ήδη κληθεί επιτυχώς η accessKYECID οπότε ο καλών να έχει πρόσβαση στα δεδομένα.

- **addMinter:** Έχει ως παράμετρο τη διεύθυνση του λογαριασμού που επιθυμούμε να δώσουμε το δικαίωμα να κάνει mint.

- **removeMinter:** Έχει ως παράμετρο τη διεύθυνση του λογαριασμού από τον οποίο επιθυμούμε να αφαιρέσουμε το δικαίωμα να κάνει mint.

- **withdraw:** Μπορεί να κληθεί μόνο από τον Κυβερνητικό Φορέα που είναι υπεύθυνος για το blockchain και την εγκυρότητα των δεδομένων. Με την κλήση της τα κρυπτονομίσματα ether που έχουν συλλεχθεί μέσω των gas costs επιστρέφονται στον λογαριασμό του.

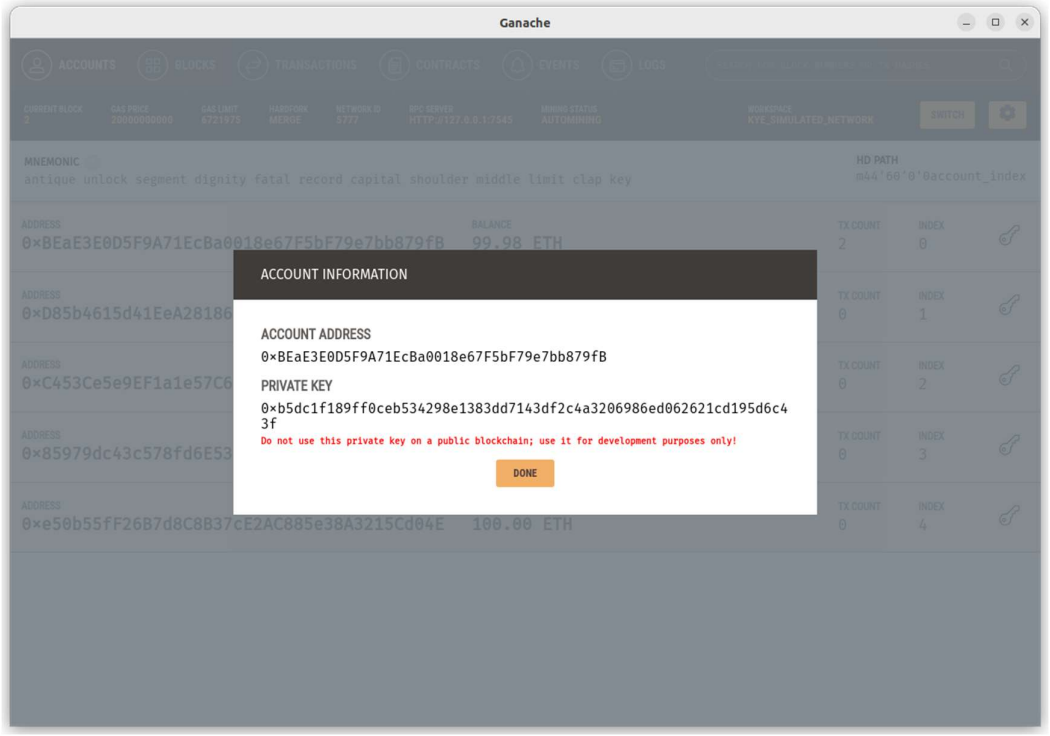
Αφού ολοκληρώσουμε το smart contract εκτελούμε την εντολή truffle migrate και βλέπουμε ότι γίνεται η πρώτη χρέωση στο blockchain μας. Ο λογαριασμός με index 0 έχει χρεωθεί και πλέον δε διαθέτει 100 ETH αλλά περίπου 99.98 ETH (Η εφαρμογή Ganache κάνει στρογγυλοποιήσεις ως προς τα ETH που έχει κάθε λογαριασμός αφού τα παρουσιάζει με ακρίβεια εκατοστού). Ταυτόχρονα, το smart contract βρίσκεται πλέον στο blockchain.



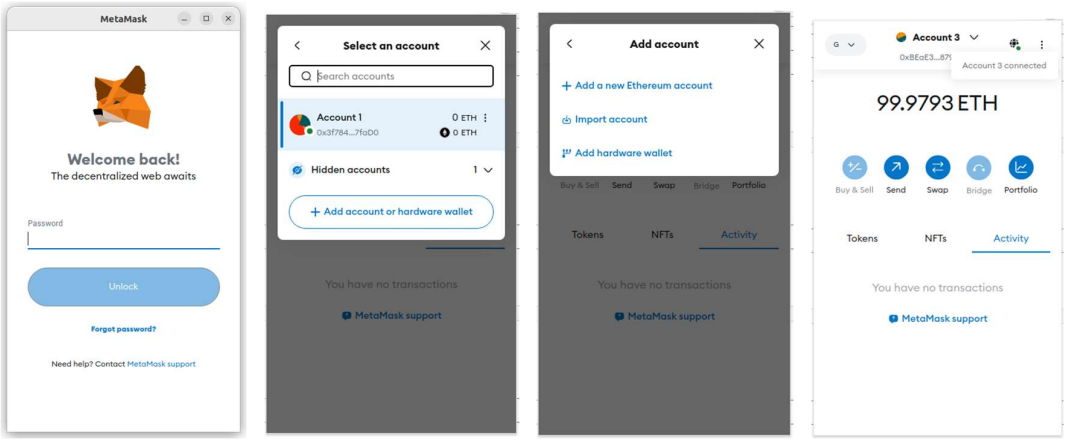
Εικόνα 4-11 Αλλαγή στο ποσό που έχει ο λογαριασμός με index = 0 μετά από το ανέβασμα του smart contract στο blockchain.

4.3.3 Σύνδεση με MetaMask

Έχοντας κατεβάσει το απαραίτητο chrome extension της MetaMask συνδεόμαστε βάζοντας τον κωδικό στο αντίστοιχο πεδίο. Αρχικά, προσθέτουμε το Ganache στα δίκτυα του MetaMask. Έπειτα, πατάμε το κουμπί «Add account or hardware wallet» και μετά «Import account». Στο πεδίο που εμφανίζεται βάζουμε το private key του λογαριασμού με index 0. Το private key το βρίσκουμε στην εφαρμογή Ganache πατώντας το εικονίδιο με το κλειδί. Αφού το πατήσουμε εμφανίζεται η διεύθυνση του λογαριασμού και το private key όπως φαίνεται στην Εικόνα 4-12. Στη συνέχεια πατάμε «Import» και ύστερα «connect account». Με αυτόν τον τρόπο καταφέρνουμε να συνδέσουμε τον λογαριασμό του Ganache με το MetaMask και πλέον βλέπουμε και εκεί το υπόλοιπο του λογαριασμού με μεγαλύτερη ακρίβεια.



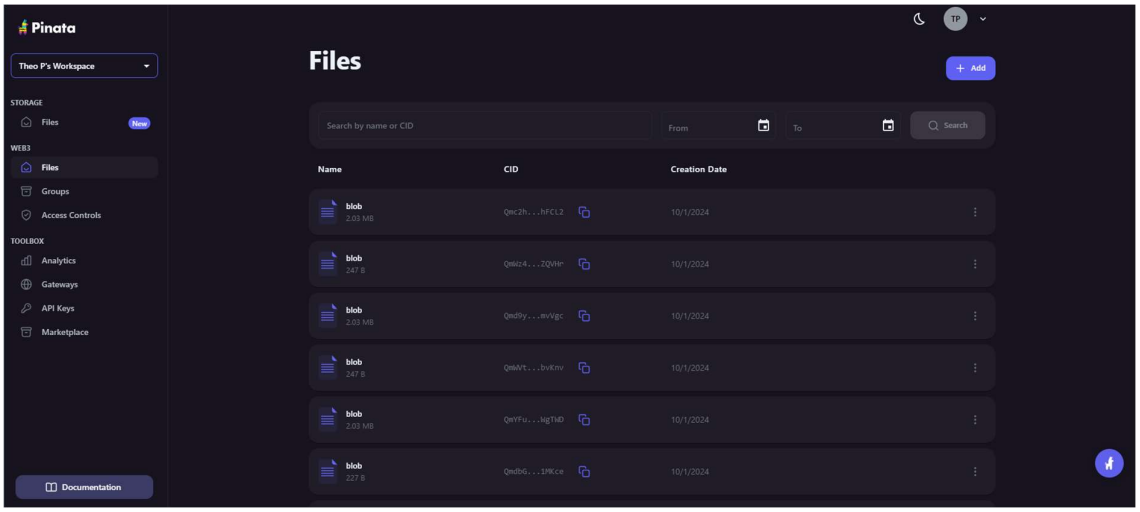
Εικόνα 4-12 Η διεύθυνση και το ιδιωτικό κλειδί του λογαριασμού εμφανίστηκαν αφού πατήσαμε το εικονίδιο με το κλειδί



Εικόνα 4-13 Διαδικασία προσθήκης λογαριασμού στο MetaMask

4.3.4 Υπηρεσία Σύνδεσης με IPFS

Για την αξιοποίηση τεχνολογιών IPFS απαιτείται η χρήση κάποιας υπηρεσίας ανάρτησης δεδομένων στο IPFS. Μια γνωστή τέτοια υπηρεσία είναι το INFURA IPFS. Ωστόσο, η συγκεκριμένη εταιρία ανακοίνωσε πρόσφατα ότι θα τερματίσει την παροχή υπηρεσιών IPFS. Μόνο ορισμένοι χρήστες θα έχουν αυτή τη δυνατότητα. Ως εκ τούτου, επιλέχθηκε ως εναλλακτική το Pinata. Μετά τη δημιουργία λογαριασμού στο Pinata, δημιουργήσαμε ένα IPFS workspace στο οποίο θα ανέβουν αρχεία και δεδομένα.



Εικόνα 4-14 Το IPFS workspace στο Pinata

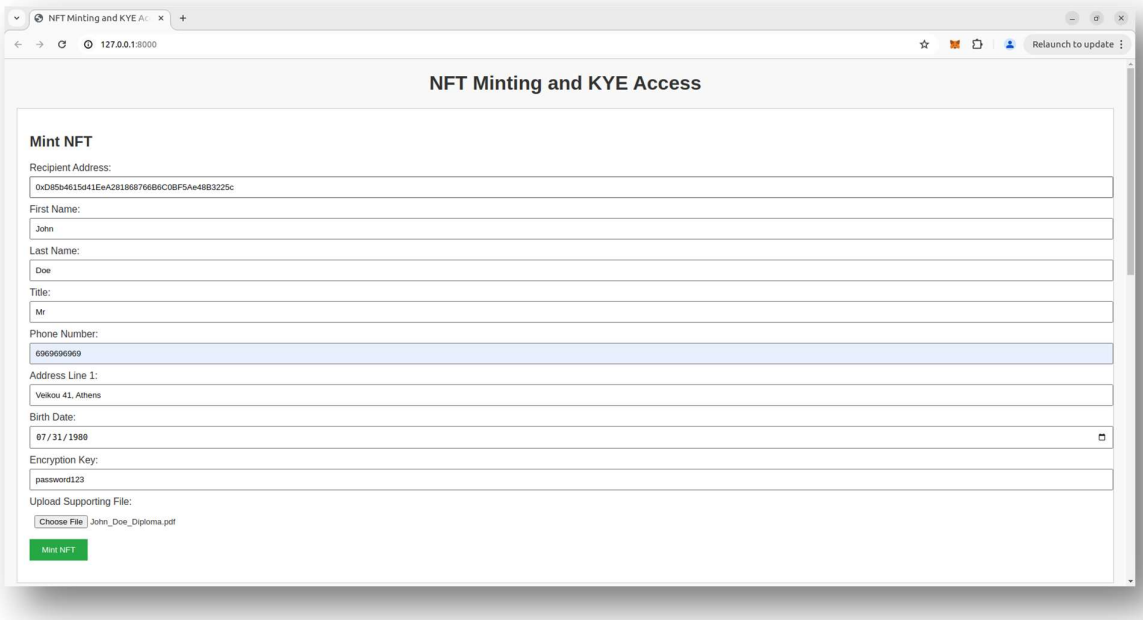
Στον κώδικα της αποκεντρωμένης εφαρμογής που υλοποιούμε συνδεόμαστε στο workspace που έχουμε δημιουργήσει και ανεβάζουμε αρχεία χρησιμοποιώντας το JavaScript API του Pinata.

4.3.5 Front-end

Mint NFT

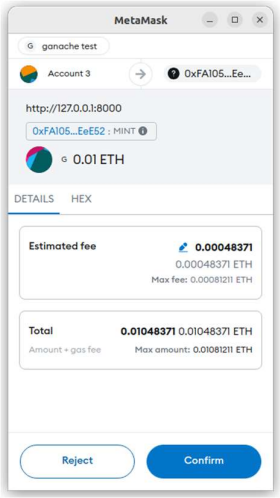
Μόνο όσοι έχουν την εξουσιοδότηση μπορούν να κάνουν mint NFT. Για προγραμματιστικούς σκοπούς επιλέξαμε τα KYE να αποτελούνται από τα εξής στοιχεία:

- Διεύθυνση του λογαριασμού που ανήκουν τα KYE (Recipient Adress)
- Όνομα (First Name)
- Επίθετο (Last Name)
- Τίτλος (Title)
- Κινητό (Phone Number)
- Διεύθυνση (Address Line 1)
- Ημερομηνία Γέννησης (Birth Date)
- Κλειδί Κρυπτογράφησης (Encryption Key)
- Ανέβασμα Αρχείου (Upload File): Ο χρήστης ανεβάζει το επιθυμητό PDF αρχείο.



Εικόνα 4-15 Συμπλήρωση Στοιχείων KYE και ανέβασμα αρχείου διπλώματος

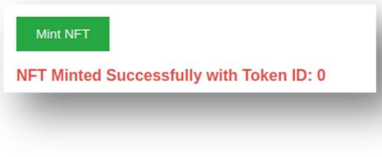
Αφού συμπληρωθούν τα πεδία με τα αντίστοιχα στοιχεία όπως φαίνεται και στην Εικόνα 4-15 πατάμε το κουμπί «Mint NFT» και ανοίγει το παράθυρο της MetaMask για να αποδεχτούμε το αίτημα και να γίνει η πληρωμή. Στο παράθυρο εμφανίζεται η χρέωση για την διαδικασία Mint αλλά και το ποσό που υπολογίζει το blockchain ότι θα κοστίσει η συναλλαγή (estimated gas). Τέλος, εμφανίζεται και το συνολικό ποσό που θα καλεστεί να πληρώσει ο χρήστης.
Δηλαδή: *Total cost = estimated cost + mint cost*



Εικόνα 4-16 Αναμονή επιβεβαίωσης για να ολοκληρωθεί η διαδικασία Mint NFT

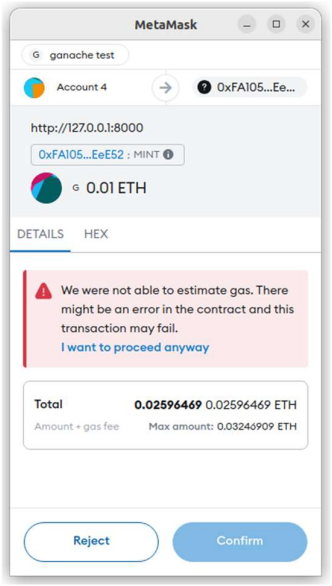
Εάν όλα τα στοιχεία έχουν συμπληρωθεί με τους κατάλληλος τύπους και ο λογαριασμός που κάνει mint έχει την ιδιότητα minter , αφού πατηθεί το κουμπί «Confirm» θα πραγματοποιηθεί η συναλλαγή. Πιο συγκεκριμένα:

1. Θα χρεωθεί ο λογαριασμός που έκανε Mint NFT. Το ποσό που αφαιρείται από τον minter για τους σκοπούς τις εργασίας είναι 0,01 ETH .
2. Τα δεδομένα αφού κρυπτογραφηθούν ανεβαίνουν στο IPFS.
3. Θα εκτυπωθεί στην οθόνη το αντίστοιχο μήνυμα επιβεβαίωσης «NFT minted successfully with token ID *x*» , με *x* το αντίστοιχο token Id που δημιουργείται κάθε φορά.



Εικόνα 4-17 Μήνυμα ότι το Mint NFT ολοκληρώθηκε με επιτυχία

Στην περίπτωση που κάποιος δεν έχει την ιδιότητα «minter» και επιχειρήσει να κάνει «mint NFT» το MetaMask θα βγάλει το μήνυμα που φαίνεται στην Εικόνα 4-18.



Εικόνα 4-18 Μήνυμα MetaMask όταν ο λογαριασμός δεν έχει το δικαίωμα να κάνει Mint NFT

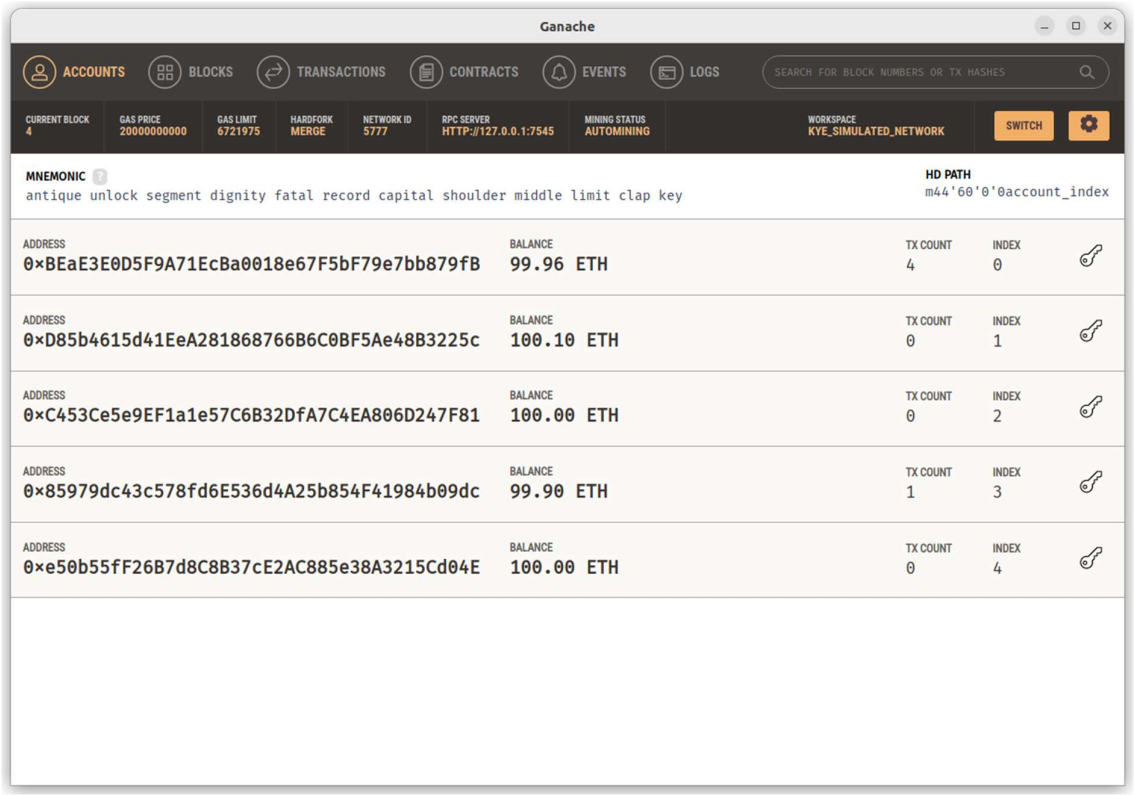
Τέλος, στις περιπτώσεις που δεν συμπληρωθούν τα πεδία με τον σωστό τύπο δεδομένων ή προσπαθήσει να κάνει mint κάποιος λογαριασμός που δεν έχει το δικαίωμα, ή για οποιαδήποτε λόγο δεν ολοκληρωθεί η πληρωμή στην οθόνη θα εμφανιστεί μήνυμα «Error minting NFT».

Εικόνα 4-19 Μήνυμα που εμφανίζεται όταν δεν πληρούνται όλες οι προϋποθέσεις για να γίνει Mint NFT

Access KYE Data (Pay Access Fee)

Οι Οργανισμοί-Επιχειρήσεις για να έχουν πρόσβαση στα KYE δεδομένα του εργαζομένου τους πρέπει να πληρώσουν έναν αντίτιμο (fee) το οποίο για τις ανάγκες της παρούσας εργασίας είναι 0.1 ETH. Το ποσό αυτό πάει εξ ολοκλήρου στον εργαζόμενο.
Για την πρόσβαση στα δεδομένα χρειάζονται 2 στοιχεία:

- Token Id
- Encryption Key: που γνωρίζει και διαχειρίζεται ο εργαζόμενος.



Εικόνα 4-20 Αλλαγή των ποσών των λογαριασμών μετά την εκτέλεση της Access

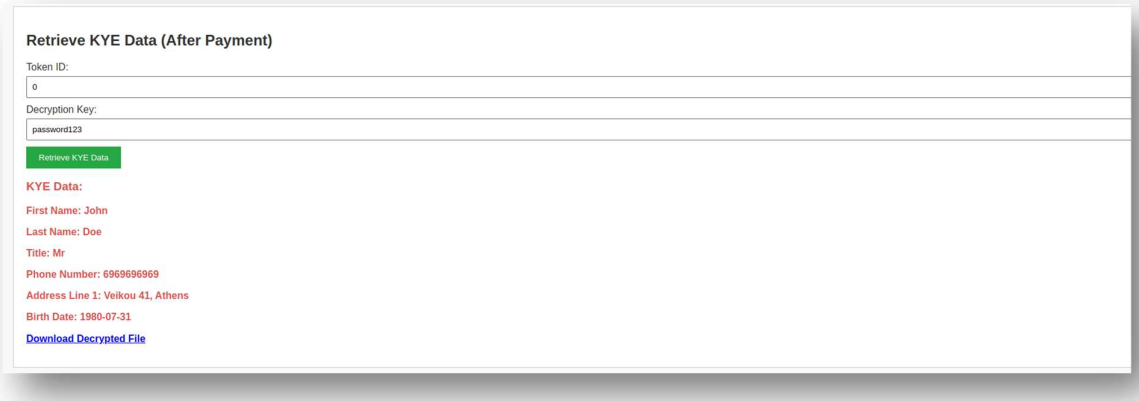
Για την πληρωμή απαιτείται μόνο το token ID. Ο Οργανισμός-Επιχείρηση συμπληρώνει το απαιτούμενο Token ID στο αντίστοιχο πεδίο και πατάει το κουμπί «Pay Access Fee». Πραγματοποιείται παρόμοια διαδικασία με αυτή του Mint NFT. Αφού πληρούνται όλες οι προϋποθέσεις και ο Οργανισμός-Επιχείρηση πατήσει το κουμπί Confirm ολοκληρώνεται η διαδικασία και εκτυπώνεται το μήνυμα «Access to KYE granted successfully» όπως φαίνεται στην Εικόνα 4-21. Αν δεν υπάρχει το αντίστοιχο token ID, ή τα απαραίτητα χρήματα στο Wallet εκτυπώνεται το μήνυμα «Error accessing KYE». Στην Εικόνα 4-20 φαίνονται οι αλλαγές στα χρήματα των λογαριασμών με index 1 και 3.

Εικόνα 4-21 Επιτυχής πληρωμή για πρόσβαση στα KYE

Retrieve KYE Data (After Payment)

Αφού ολοκληρωθεί σωστά η διαδικασία «Access KYE Data» ο Οργανισμός-Επιχείρηση έχει πρόσβαση στα δεδομένα. Σημειώνεται εδώ ότι η διαδικασία «Retrieve KYE» δεν έχει κάποια

χρέωση και μπορεί να πραγματοποιηθεί πολλές φορές. Το μόνο που χρειάζεται είναι το Token ID και το Encryption Key. Όπως φαίνεται και στην Εικόνα 4-22, εμφανίζονται όλα τα στοιχεία και δίνεται η δυνατότητα για να κατεβάσουν το αρχείο πατώντας το «Download Decrypted File». Τα δεδομένα (στοιχεία και αρχείο) πριν εμφανιστούν στην οθόνη έχουν αποκρυπτογραφηθεί. Εάν δεν έχει τοποθετηθεί το σωστό token ID, encryption Key ή δεν έχει πραγματοποιηθεί πρώτα η πληρωμή εκτυπώνεται το αντίστοιχο μήνυμα λάθους.

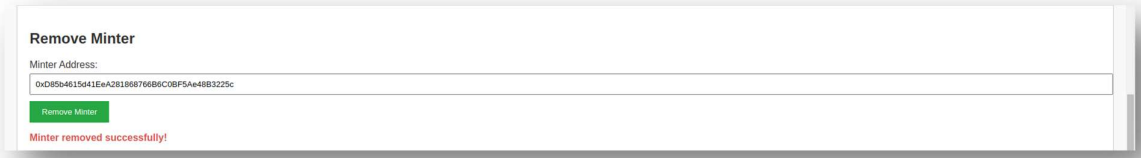


Εικόνα 4-22 Εμφάνιση KYE δεδομένων

Add Minter-Remover Minter

Μέσα από τις διαδικασίες «Add Minter» και «Remove Minter» μπορούμε να προσθέσουμε και να αφαιρέσουμε αντίστοιχα το δικαίωμα από κάποιον λογαριασμό να κάνει «Mint NFT». Μόνο ο λογαριασμός που ανέβασε το smart contract στο blockchain μπορεί υλοποιήσει αυτές τις δύο διαδικασίες. Ακολουθείται παρόμοια διαδικασία με τα παραπάνω, δηλαδή πρέπει να γίνει πληρωμή των estimated gas μέσω MetaMask για να έχουμε το επιθυμητό αποτέλεσμα. Εφόσον γίνει η πληρωμή στην οθόνη εμφανίζονται τα μηνύματα «Minter added successfully» και «Minter removed successfully» αντίστοιχα. Το ποσό που καλείται να πληρώσει ο χρήστης για να προσθέσει ή να αφαιρέσει κάποιον άλλον είναι μόνο το estimated gas.

Εικόνα 4-23 Διαδικασία Add Minter και μήνυμα μετά την πετυχημένη προσθήκη



Εικόνα 4-24 Διαδικασία Remove Minter και μήνυμα μετά την πετυχημένη αφαίρεση

Withdraw

Κάθε φορά που γίνεται μια συναλλαγή καταναλώνεται ένα ποσό καυσίμου (gas). Αυτό το ποσό υπάρχει στο blockchain και αυξάνεται όσο περισσότερες συναλλαγές γίνονται. Με τη διαδικασία «withdraw» αυτά τα λεφτά στέλνονται στον λογαριασμό που έχουμε ορίσει. Στην περίπτωσή μας ο λογαριασμός με index = 0 θα καρπωθεί τα λεφτά που έχουν συσσωρευτεί στο blockchain. Επομένως, μόνο ο λογαριασμός αυτός μπορεί να εκτελέσει withdraw και να δει το μήνυμα «Funds withdraw successfully», οι υπόλοιποι θα λάβουν μήνυμα «Error withdrawing funds». Είναι σημαντικό να αναφέρουμε ότι ενώ υπάρχει «Add Minter», δεν υπάρχει «Add Withdrawer».

Εικόνα 4-25 Διαδικασία Withdraw Funds και μήνυμα μετά από πετυχημένο withdraw

4.3.6 API

Όπως φαίνεται και στα sequence διαγράμματα όταν συμπληρωθούν τα απαραίτητα πεδία ανάλογα με το ποιο κουμπί θα πατήσουμε ενεργοποιείται το αντίστοιχο σημείο στην HTML και αυτή με τη σειρά της ενεργοποιεί το αντίστοιχο κομμάτι του σεναρίου app.js.
Πιο συγκεκριμένα έχουμε:

- **mintForm**

Συλλέγεται η διεύθυνση του «Recipient», η τιμή του «encryption key» και στην σταθερά «kyeData» τοποθετούνται τα «first name», «last name», «title», «phoneNumber», «adressLine1» και «birthdate». Με την εντολή:

JSON.stringfy(kyeData)

τα δεδομένα της kyeData μετατρέπονται σε μορφή JSON συμβολοσειράς. Έπειτα, κρυπτογραφούνται με τη βοήθεια της συνάρτησης της βιβλιοθήκης cryptojs:

CryptoJS.AES.encrypt(keyData, encryption_key)

Τα κρυπτογραφημένα δεδομένα μετατρέπονται σε συμβολοσειρά και με τη συνάρτηση:

uploadToIPFS(EncryptedData)

ανεβαίνουν στο IPFS και επιστρέφει στην σταθερά kyeCID το link . Στη συνέχεια το αρχείο κρυπτογραφείται με τον τρόπο που θα αναλυθεί στην επόμενη ενότητα. Όπως και με τα δεδομένα ανεβαίνει στο IPFS και επιστρέφεται το αντίστοιχο link. Τα δύο link ενώνονται και τοποθετούνται στη μεταβλητή totalCID.

Τέλος, καλείται η μέθοδος «mint» του έξυπνου συμβολαίου με παραμέτρους τη διεύθυνση του Recipient και το totalCID (περιέχει το CID των δεδομένων και το CID του αρχείου που ανέβηκαν στο IPFS). Στην περίπτωση που η μέθοδος εκτελεστεί επιτυχώς εκτυπώνεται το μήνυμα «NFT Minted Successfully with Token ID: » μαζί με το αντίστοιχο token διαφορετικά αν διακοπεί από κάποιο σφάλμα επιστρέφει το μήνυμα «Error minting NFT».

- **accessKYEForm**

Συλλέγεται η τιμή του token ID για το οποίο ο λογαριασμός θέλει να αποκτήσει πρόσβαση. Καλείται η μέθοδος «accessKYECID» του έξυπνου συμβολαίου με παράμετρο το token ID. Ταυτόχρονα, με το κάλεσμα καθορίζεται και το αντίτιμο που πρέπει να πληρωθεί για να ολοκληρωθεί η διαδικασία. Τέλος, στην περίπτωση που η μέθοδος διακοπεί από κάποιο σφάλμα επιστρέφει το μήνυμα «Error accessing KYE data» ενώ αν ολοκληρωθεί επιτυχώς εκτυπώνεται «Access to KYE granted successfully».

- **retrieveKYEForm**

Συλλέγει το token ID και το decryption key. Έπειτα, καλεί την μέθοδο retrieveKYECID του έξυπνου συμβολαίου. Η μέθοδος επιστρέφει το totalCID. Γίνεται ο διαχωρισμός του kyeCID από το fileCID και επικοινωνεί με το IPFS μέσω των εντολών:

fetch(https://gateway.pinata.cloud/ipfs/${keyCID})
fetch(https://gateway.pinata.cloud/ipfs/${fileCID})

Ύστερα, γίνεται αποκρυπτογράφηση με τη βοήθεια του κλειδιού. Αν έχει δοθεί λάθος κλειδί εκτυπώνεται μήνυμα «Wrong decryption key». Τα αποκρυπτογραφημένα δεδομένα εκτυπώνονται στην οθόνη του χρήστη και δίνεται η δυνατότητα να κατεβάσει το αποκρυπτογραφημένο PDF. Στην περίπτωση που η διαδικασία διακοπεί από κάποιο σφάλμα επιστρέφει το μήνυμα «Error adding minter».

- **addMinterForm**

Συλλέγει τη διεύθυνση του λογαριασμού που θέλουμε να προσθέσουμε και καλεί τη μέθοδο «addMinter» του έξυπνου συμβολαίου. Στην περίπτωση που η μέθοδος διακοπεί από κάποιο σφάλμα επιστρέφει το μήνυμα «Error adding minter» διαφορετικά τυπώνεται το μήνυμα «Minter added successfully».

- **removeMinterForm**

Συλλέγει τη διεύθυνση του λογαριασμού που θέλουμε να αφαιρέσουμε και καλεί τη μέθοδο «RemoveMinter» του έξυπνου συμβολαίου. Στην περίπτωση που η μέθοδος διακοπεί από κάποιο σφάλμα επιστρέφει το μήνυμα «Error removing minter», διαφορετικά τυπώνεται το μήνυμα «Minter removed successfully».

- **withdrawButton:**

Καλεί τη μέθοδο «withdraw» του έξυπνου συμβολαίου. Αν η μέθοδος δε διακοπεί από κάποιο σφάλμα εκτυπώνεται το μήνυμα «Funds withdrawn successfully» διαφορετικά επιστρέφει το μήνυμα «Error withdrawing funds».

4.4 Ασφάλεια και Ιδιωτικότητα

Όπως έχουμε ήδη αναφέρει στην αποκεντρωμένη εφαρμογή που δημιουργήσαμε είναι πολύ σημαντικό να υπάρχει ασφάλεια στην αποθήκευση των δεδομένων. Για να το πετύχουμε πριν τα αποθηκεύσουμε τα κρυπτογραφούμε με τη βοήθεια ενός κλειδιού που υποδεικνύει ο χρήστης και έπειτα τα ανεβάζουμε στο IPFS.

4.4.1 Κρυπτογράφηση–Αποκρυπτογράφηση Δεδομένων

Η κρυπτογράφηση των δεδομένων που συμπληρώνονται στα αντίστοιχα πεδία είναι σχετικά απλή. Έχοντας μετατρέψει τα δεδομένα σε μία συμβολοσειρά κάνουμε χρήση της βιβλιοθήκης cryptojs. Συγκεκριμένα, χρησιμοποιούμε την AES κρυπτογράφηση. Για να μπορούμε να γνωρίζουμε κάθε φορά αν το κλειδί της αποκρυπτογράφησης είναι το σωστό τοποθετούμε στο τέλος των KYE δεδομένων τη συμβολοσειρά «*_verified*» πριν κρυπτογραφηθούν. Έτσι, όταν γίνει αποκρυπτογράφηση θα ελέγξουμε τους τελευταίους χαρακτήρες αν είναι ίδιοι με την παραπάνω συμβολοσειρά. Αν διαφέρουν θα γνωρίζουμε ότι το κλειδί της αποκρυπτογράφησης δεν ήταν το σωστό και θα ενημερώσουμε τον χρήστη. Με αυτόν τον τρόπο μπορούμε να ελέγξουμε τη διαδικασία χωρίς να αποκαλυφθεί κάποιο δεδομένο.
Έτσι η εντολή είναι :

CryptoJS.AES.encrypt(kyeDataString + "_verified", encryptionKey)

Για την αποκρυπτογράφηση ακολουθείται η αντίστροφη διαδικασία.

4.4.2 Κρυπτογράφηση-Αποκρυπτογράφηση Αρχείου

Η Κρυπτογράφηση του αρχείου PDF είναι πιο περίπλοκη από αυτή των δεδομένων. Τα PDF αρχεία είναι δυαδικά δεδομένα, και αν τα κρυπτογραφήσουμε ως συμβολοσειρές όπως κάναμε παραπάνω υπάρχει κίνδυνος να αλλοιωθούν κατά τη διάρκεια της κρυπτογράφησης ή αποκρυπτογράφησης. Για να αποφευχθεί αυτό προτού τα κρυπτογραφήσουμε τα μετατρέπουμε σε συμβολοσειρά μορφής Base64.

Το Base64 μετατρέπει τα δυαδικά δεδομένα σε μια ακολουθία εκτυπώσιμων χαρακτήρων, που περιορίζεται σε ένα σύνολο 64 μοναδικών χαρακτήρων. Πιο συγκεκριμένα, τα δυαδικά δεδομένα προέλευσης λαμβάνονται 6 bit τη φορά και στη συνέχεια αυτή η ομάδα των 6 bit αντιστοιχίζεται σε έναν από τους 64 μοναδικούς χαρακτήρες. Όπως συμβαίνει με όλα τα σχήματα κωδικοποίησης δυαδικού σε κείμενο, το Base64 έχει σχεδιαστεί για να μεταφέρει δεδομένα που είναι αποθηκευμένα σε δυαδικές μορφές σε κανάλια που υποστηρίζουν αξιόπιστα μόνο περιεχόμενο κειμένου.

4.4.3 Ανέβασμα αρχείου-δεδομένων στο IPFS

Για να ανέβουν τα αρχεία στο IPFS πρώτα πρέπει να έχουμε στην κατοχή μας τα αντίστοιχα κλειδιά (pinata api key, pinata secret api key) που απαιτούνται από την εφαρμογή Pinata. Τα αρχεία ανεβαίνουν με τη μορφή ενός blob.

Η αποθήκευση Blob είναι ένας τύπος αποθήκευσης στο cloud για μη δομημένα δεδομένα. Ένα blob (Binary Large Object), είναι ένας όγκος δεδομένων σε δυαδική μορφή που δεν ακολουθεί απαραίτητα κάποιο συγκεκριμένο τύπο αρχείου.

Τα δεδομένα και το αρχείο ανεβαίνουν στο Pinata και αυτό επιστρέφει το link στο οποίο αποθηκεύτηκαν.

5 Πειραματικές Μετρήσεις και Αποτελέσματα

Στο Κεφάλαιο αυτό θα παρουσιαστούν οι μετρήσεις που έγιναν για την αξιολόγηση της επίδοσης της αποκεντρωμένης εφαρμογής. Αρχικά, μετρήθηκαν οι χρόνοι απόκρισης των συναρτήσεων της εφαρμογής χωρίς να εμπλέκεται το σύστημα IPFS για την αποθήκευση των KYE δεδομένων. Έπειτα, παρουσιάζονται οι μετρήσεις των χρόνων απόκρισης με τη συμβολή του IPFS.

Οι μετρήσεις για την κατανάλωση καυσίμων (gas) έγιναν με τη χρήση του πεδίου gas.Used. Το πεδίο αυτό επιστρέφει τον αριθμό των καυσίμων (gas) που απαιτούνται για την εκτέλεση μίας μεθόδου του έξυπνου συμβολαίου. Η μονάδα μέτρησης των καυσίμων είναι το gwei (1 gwei = 10^{-9} ether)

Για τους χρόνους εκτέλεσης, κρυπτογράφησης αλλά και ανεβάσματος αρχείου χρησιμοποιήθηκε ο συνδυασμός των «Performance.now()/Performance.end()». Επιλέχθηκαν έναντι της Date.now() διότι παρέχει αποτελέσματα μεγαλύτερης ακρίβειας. Να σημειωθεί επίσης ότι η Date.now() επιστρέφει τον χρόνο που έχει περάσει από την 1^{η} Ιανουαρίου του 1970 στις 00:00 UTC, ενώ το αποτέλεσμα της Performance.now() σχετίζεται με τη στιγμή που φορτώνεται η σελίδα (page load) και χρησιμοποιείται σε περιπτώσεις που θέλουμε να μετρήσουμε με ακρίβεια τον χρόνο εκτέλεσης ενός μέρους του κώδικα.

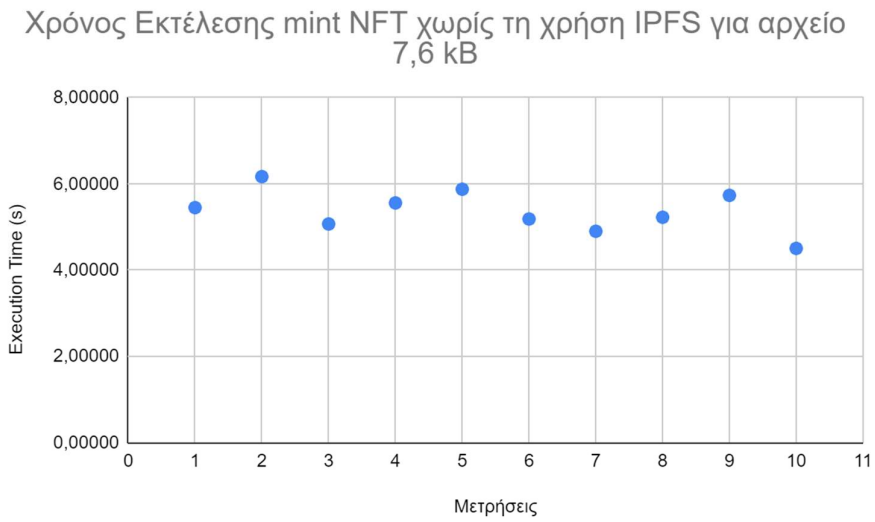
Οι χρόνοι εκτέλεσης κάθε μεθόδου που παρουσιάζονται στην υποενότητα 5.2 συνυπολογίζουν και τον χρόνο απόκρισης του χρήστη για επιβεβαίωση της συναλλαγής. Δηλαδή, τον χρόνο που απαιτείται να πατήσει το κουμπί «confirm» στην συνδεδεμένη εφαρμογή MetaMask. Ωστόσο, ο χρόνος αυτός είναι αμελητέος σε σχέση με τον συνολικό χρόνο της διαδικασίας και εντελώς ανεξάρτητος από το μέγεθος του αρχείου ή τους άλλους παράγοντες που θέλουμε να μετρήσουμε.

5.1 Μέτρηση χρόνων χωρίς IPFS

Αρχικά, γίνεται μέτρηση χωρίς τη χρήση της υπηρεσίας IPFS αξιοποιώντας το truffle console για development. Με αυτόν το τρόπο γίνεται αποθήκευση των δεδομένων πάνω στην αλυσίδα (on chain) του blockchain.

Στο Διάγραμμα 5-1 παρουσιάζονται 10 διαφορετικές μετρήσεις που έγιναν για το ίδιο μέγεθος δεδομένων. Οι τιμές κυμαίνονται ανάμεσα στα 4,5s και 6,2s . Ο μέσος όρος είναι 5,379 δευτερόλεπτα ενώ τα καύσιμα 5520208. Παρατηρούμε ότι ο χρόνος εκτέλεσης της «mint NFT» είναι αρκετά αυξημένος. Τα δεδομένα χρειάζονται πολλά καύσιμα (gas) αλλά και χρόνο για να αποθηκευτούν στην αλυσίδα.

Πρέπει να σημειωθεί ότι για να πάρουμε αυτές τις μετρήσεις αρχικοποιούσαμε κάθε φορά το σύστημα και το blockchain. Αλλιώς, θα είχαμε αύξηση του χρόνου που απαιτούσε για να εκτελεστεί η συνάρτηση «Mint NFT» κατά ένα σημαντικό ποσό κάθε φορά. Αυτό συμβαίνει λόγω της συσσώρευσης δεδομένων στο blockchain, που συνεπάγεται ότι οι κόμβοι του δικτύου χρειάζεται να εναποθέσουν περισσότερο χώρο αποθήκευσης και τα κόστη σε καύσιμα να ανέβουν.



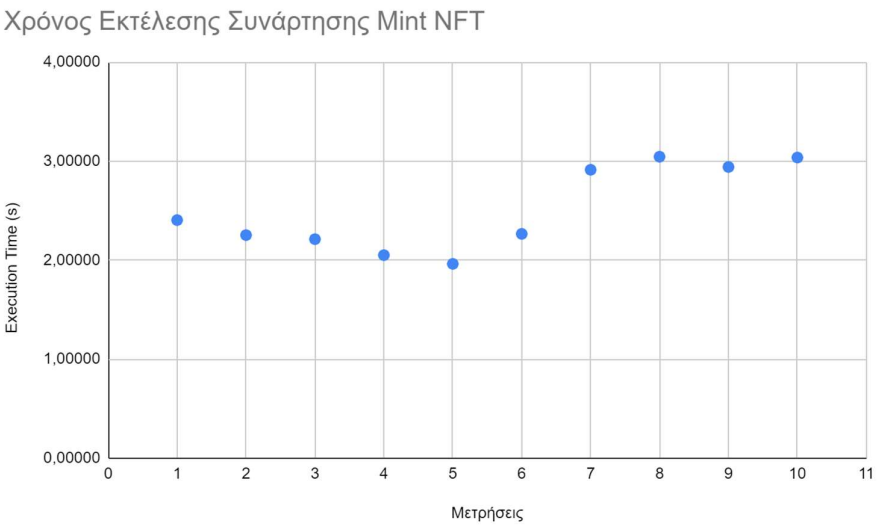
Διάγραμμα 5-1 Χρόνος Εκτέλεσης mint NFT για αρχείο 7,6KB χωρίς τη χρήση IPFS

5.2 Μέτρηση χρόνων με IPFS

Παρακάτω φαίνονται οι μετρήσεις χρόνων και καυσίμων που χρησιμοποιήθηκαν για τη συναλλαγή. Τα δεδομένα για τα οποία μετρήθηκαν οι χρόνοι είναι τα εξής:

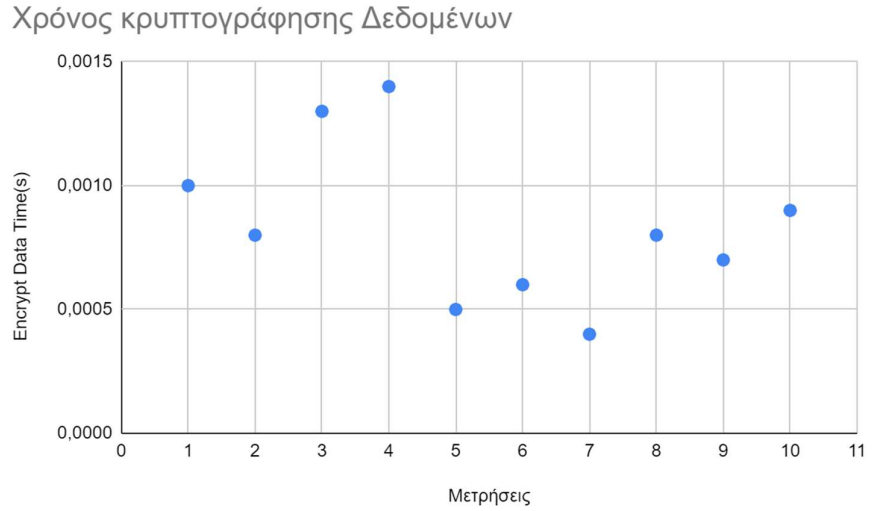
- Διεύθυνση του λογαριασμού που ανήκουν τα KYE: 0xD85b4615d41EeA281868766B6C0BF5Ae48B3225c
- Όνομα : John
- Επίθετο: Doe
- Τίτλος: Mr
- Κινητό: 6969696969
- Διεύθυνση: Veikou 41, Athens
- Ημερομηνία Γέννησης: 07/31/1980
- Κλειδί Κρυπτογράφησης: password123
- Ανέβασμα Αρχείου (Upload File): Ανέβηκε αρχείο με όνομα «John_Doe_Diploma» μεγέθους 7,6 KB (7590 bytes).

Τα δεδομένα και το αρχείο κρυπτογραφούνται όπως αναλύθηκε στο προηγούμενο κεφάλαιο. Ανεβαίνουν στο IPFS και ενεργοποιείται η αντίστοιχη μέθοδος του έξυπνου συμβολαίου.



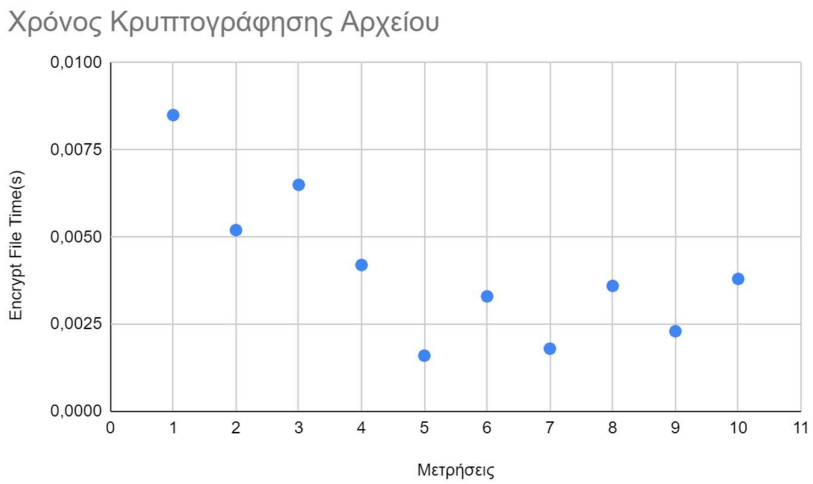
Διάγραμμα 5-2 Χρόνος εκτέλεσης συνάρτησης mint NFT για το ίδιο δείγμα 10 φορές

Στο Διάγραμμα 5-2 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης για τα ίδια δεδομένα της συνάρτησης «Mint NFT». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 2s και 3s. Οι χρόνοι για τις μετρήσεις 5,8 και 10 αποκλίνουν από το διάστημα που αναφέρθηκε. Ο μέσος όρος είναι 2,50824 δευτερόλεπτα, ενώ τα καύσιμα που χρησιμοποιήθηκαν είναι 154488.



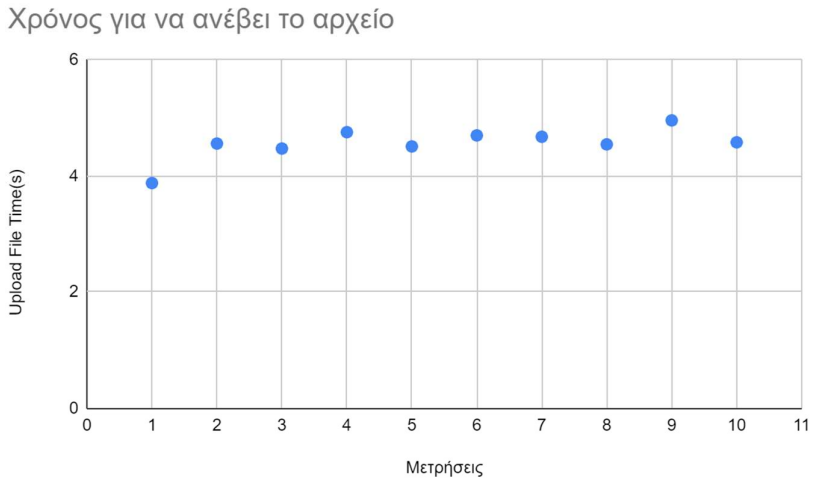
Διάγραμμα 5-3 Χρόνος Κρυπτογράφησης δεδομένων για το ίδιο δείγμα 10 φορές

Στο Διάγραμμα 5-3 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου κρυπτογράφησης για τα ίδια δεδομένα της συνάρτησης «Mint NFT». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 0,0005s και 0,0010s. Οι χρόνοι για τις μετρήσεις 3, 4 και 7 αποκλίνουν από το διάστημα που αναφέρθηκε. Ο μέσος όρος είναι 0,00084004 δευτερόλεπτα.



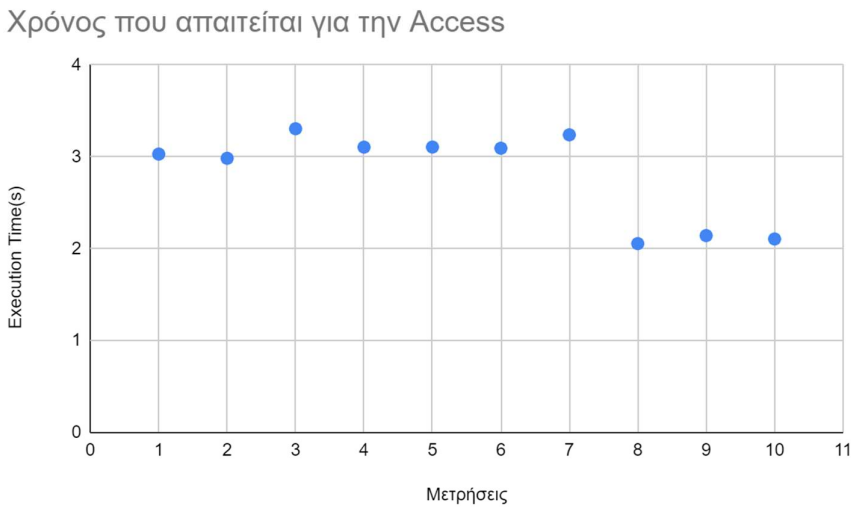
Διάγραμμα 5-4 Χρόνος Κρυπτογράφησης αρχείου για το ίδιο δείγμα 10 φορές

Στο Διάγραμμα 5-4 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου κρυπτογράφησης για το ίδιο PDF αρχείο της συνάρτησης «Mint NFT». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 0,0023s και 0,0065s. Οι χρόνοι για τις μετρήσεις 1, 5 και 7 αποκλίνουν από το διάστημα που αναφέρθηκε. Ο μέσος όρος είναι 0,00408 δευτερόλεπτα.



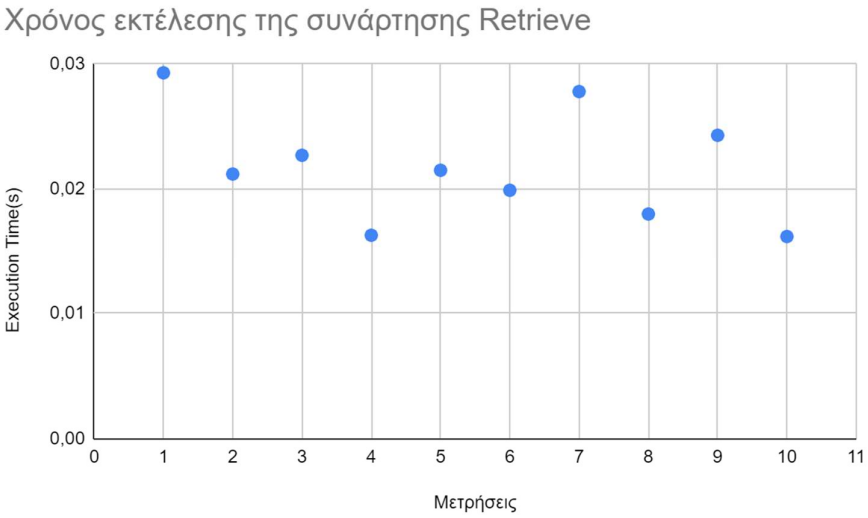
Διάγραμμα 5-5 Χρόνος για να ανέβει το ίδιο αρχείο 10 φορές

Στο Διάγραμμα 5-5 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου που απαιτείται για να γίνει ανέβασμα του αρχείου pdf της συνάρτησης «Mint NFT». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 4,4760s και 4,7569s. Οι χρόνοι για τις μετρήσεις 1 και 9 αποκλίνουν λίγο από αυτό το διάστημα. Ο μέσος όρος είναι 4,56601 δευτερόλεπτα.



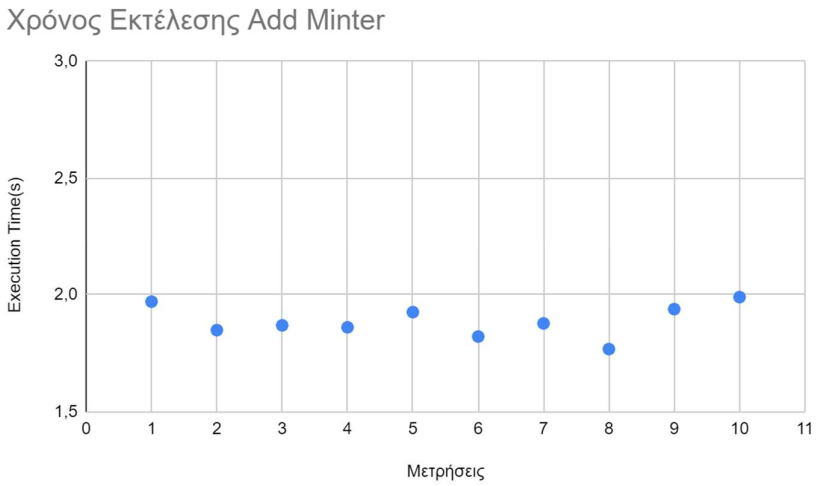
Διάγραμμα 5-6 Χρόνος Εκτέλεσης της συνάρτησης Access

Στο Διάγραμμα 5-6 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης για τη συνάρτηση «Access NFT». Οι τιμές κυμαίνονται ανάμεσα στα 2,0546s και 3,306s. Ο μέσος όρος είναι 2,81654 δευτερόλεπτα, ενώ τα καύσιμα που χρησιμοποιήθηκαν είναι 70023.



Διάγραμμα 5-7 Χρόνος Εκτέλεσης της συνάρτησης Retrieve

Στο Διάγραμμα 5-7 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης για τα ίδια δεδομένα της συνάρτησης «Retrieve». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 0,018s και 0,03s. Ο μέσος όρος είναι 0,02172 δευτερόλεπτα, ενώ δεν απαιτούνται καύσιμα για να πραγματοποιηθεί.



Διάγραμμα 5-8 Χρόνος εκτέλεσης συνάρτησης Add Minter για το ίδιο δείγμα 10 φορές

Στο Διάγραμμα 5-8 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης της συνάρτησης «Add Minter» για τη διεύθυνση:

0xD85b4615d41EeA281868766B6C0BF5Ae48B3225c.

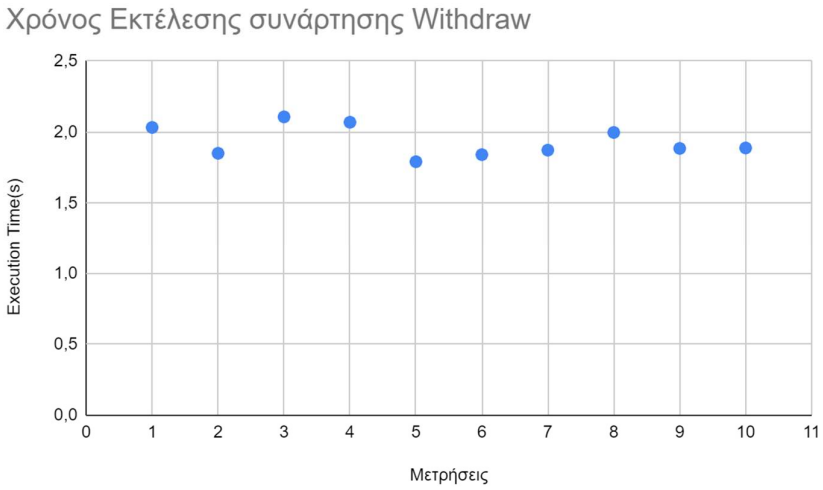
Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 1,8215 s και 1,9384 s. Οι χρόνοι για τις μετρήσεις 1, 9 και 10 αποκλίνουν λίγο από το διάστημα που αναφέρθηκε. Ο μέσος όρος είναι 1,88704 δευτερόλεπτα, ενώ τα καύσιμα που χρησιμοποιήθηκαν είναι 51860.

Διάγραμμα 5-9 Χρόνος εκτέλεσης συνάρτησης Remove Minter

Στο Διάγραμμα 5-9 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης της συνάρτησης «Remove Minter» για τη διεύθυνση:

0xD85b4615d41EeA281868766B6C0BF5Ae48B3225c.

Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 1,8282s και 1,8901s. Οι χρόνοι για τις μετρήσεις 1, 2 και 10 αποκλίνουν λίγο από το διάστημα που αναφέρθηκε. Ο μέσος όρος είναι 1,85465 δευτερόλεπτα, ενώ τα καύσιμα που χρησιμοποιήθηκαν είναι 33043.



Διάγραμμα 5-10 Χρόνος εκτέλεσης συνάρτησης Withdraw

Στο Διάγραμμα 5-10 παρουσιάζονται οι 10 διαφορετικές μετρήσεις του χρόνου εκτέλεσης της συνάρτησης «Withdraw». Οι περισσότερες τιμές κυμαίνονται ανάμεσα στα 1,7932s και 2,1082s. Ο μέσος όρος είναι 1,93501 δευτερόλεπτα, ενώ τα καύσιμα που χρησιμοποιήθηκαν είναι 33043.

Συνάρτηση	Gas used(gwei)
Mint NFT	154.488
Access	70.023
Retrieve	-
Add minter	51.860
Remove minter	29.986
Withdraw	33.043

Πίνακας 5-1 Συγκρίσεις καυσίμων για κάθε συνάρτηση

Ο Πίνακας 5-1 δείχνει τα καύσιμα (gas) που απαιτούνται για να υλοποιηθεί κάθε συνάρτηση του έξυπνου συμβολαίου. Η «mint NFT» είναι η μέθοδος που απαιτεί τα περισσότερα καύσιμα με διαφορά από τις υπόλοιπες ενώ η «Remove Minter» τα λιγότερα. Αυτό οφείλεται στο γεγονός ότι η «mint NFT» ανεβάζει δεδομένα στο blockchain (το link για τα κρυπτογραφημένα δεδομένα στο IPFS).

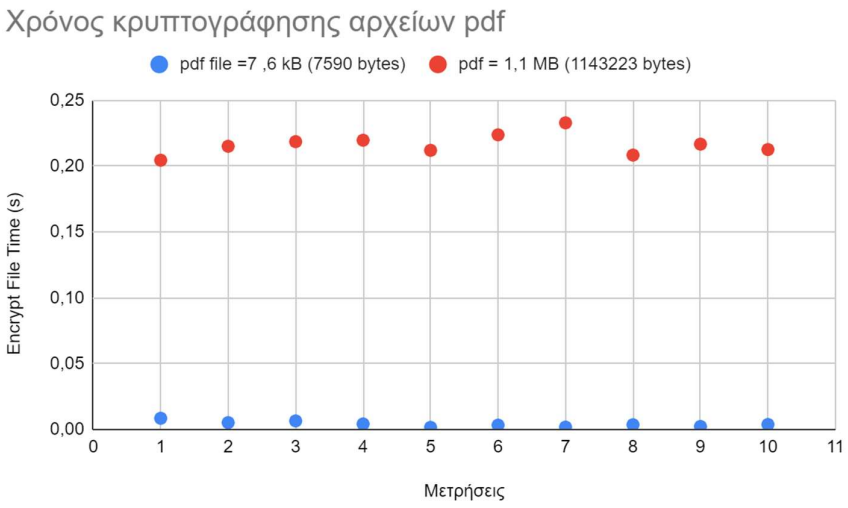
Αξίζει να σημειωθεί ότι η «Retrieve» δεν καταναλώνει κανένα καύσιμο. Αυτό οφείλεται στο γεγονός ότι δεν προκαλεί κάποια αλλαγή στην κατάσταση (state) του Ethereum Virtual Machine. Δηλαδή, η απλή προσπέλαση της κατάστασης του EVM δεν κοστολογείται σε καύσιμα.

Συνάρτηση	Μ.Ο Χρόνου Εκτέλεσης(s)
Mint NFT	2,50824
Access NFT	2,81654
Retrieve NFT	0,02172
Add Minter	1,88704
Remove Minter	1,85465
Withdraw	1,93501

Πίνακας 5-2 Μ.Ο. χρόνος εκτέλεσης για κάθε συνάρτηση

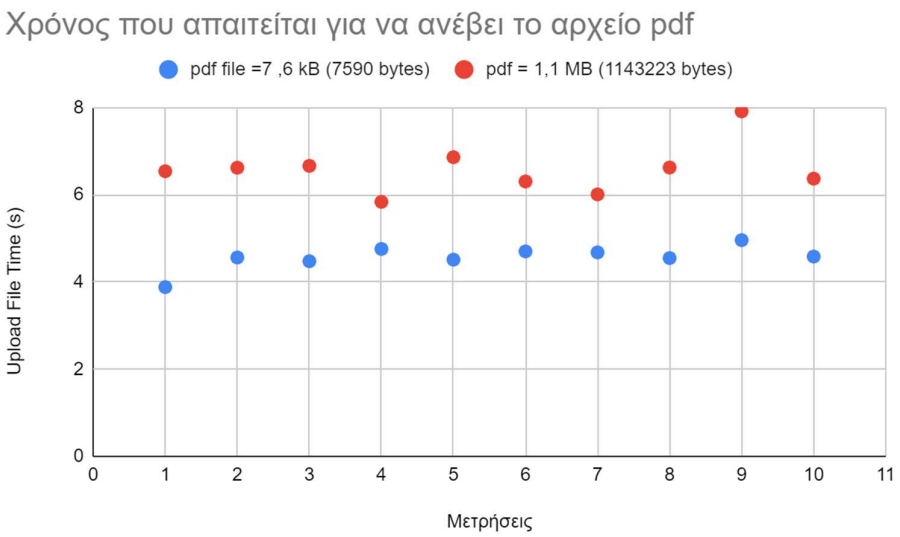
Στον Πίνακας 5-2 αναγράφεται ο μέσος όρος εκτέλεσης κάθε συνάρτησης του έξυπνου συμβολαίου. Πιο γρήγορη με διαφορά είναι η συνάρτηση Retrieve αφού δε χρειάζεται καν επιβεβαίωση από τον χρήστη μέσω του MetaMask. Παρατηρούμε ότι οι Add Minter και Remove Minter παίρνουν σχεδόν τον ίδιο χρόνο.

Ύστερα έγιναν μετρήσεις για τα ίδια δεδομένα αλλά με αρχείο PDF μεγέθους 1,1 MB (1143223 bytes). Όπως περιμέναμε οι χρόνοι εκτέλεσης των συναρτήσεων «Access», «Add Minter», «Remove Minter» και «Withdraw» δεν έχουν κάποια διαφορά αφού δεν επηρεάζει κάπου το μέγεθος του αρχείου (για αυτόν τον λόγο δεν παρουσιάζονται παρακάτω). Παρακάτω φαίνονται οι συγκρίσεις των μετρήσεων που παρουσίασαν διαφορά και εξαρτώνται από το μέγεθος του αρχείου.



Διάγραμμα 5-11 Χρόνος Κρυπτογράφησης αρχείων για διαφορετικά μεγέθη pdf

Στο Διάγραμμα 5-11 είναι εμφανές ότι το αρχείο με το μεγαλύτερο μέγεθος απαιτεί και περισσότερο χρόνο για να κρυπτογραφηθεί. Με κόκκινες κουκκίδες είναι το μεγαλύτερο αρχείο δηλαδή το 1,1 MB ενώ με μπλε το μικρότερο αρχείο, δηλαδή το 7,6KB.



Διάγραμμα 5-12 Χρόνος που απαιτείται για να ανέβει το αρχείο pdf

Στο Διάγραμμα 5-12 παρατίθενται οι χρόνοι που απαιτούνται για να ανέβει το αρχείο στο IPFS. Όπως περιμέναμε το μεγαλύτερο αρχείο παίρνει περισσότερο χρόνο για να ανέβει. Ο μέσος όρος για να ανέβει το αρχείο 7,6KB είναι 4,56601 δευτερόλεπτα, ενώ, για να ανέβει το αρχείο 1,1MB είναι 6,57507 δευτερόλεπτα.

Συνολικά, από τα παραπάνω είναι φανερό ότι η σύνδεση του blockchain με εφαρμογές υπηρεσιών IPFS είναι πολύ σημαντική για την κλιμάκωση των αποκεντρωμένων εφαρμογών. Το μέγεθος των δεδομένων δεν επηρεάζει τους χρόνους εκτέλεσης των μεθόδων του έξυπνου συμβολαίου όταν αυτά ανεβαίνουν στο IPFS αφού το NFT δεν περιέχει όλα τα δεδομένα αλλά το link για αυτά. Αντίθετα, όταν έχουμε αποθήκευση δεδομένων on-chain, καταναλώνονται μεγάλα ποσά καυσίμων και έχουμε χρονοβόρες εκτελέσεις μεθόδων. Τέλος, όταν δεν υπάρχει αλλαγή στην κατάσταση του ledger δεν καταναλώνονται και καύσιμα. Ενώ, όσο περισσότερες αλλαγές γίνονται τόσο περισσότερα είναι και τα απαιτούμενα καύσιμα.

6 Συμπεράσματα και Μελλοντικές Προεκτάσεις

6.1 Συμπεράσματα

Στην παρούσα διπλωματική εργασία υλοποιήθηκε μια αποκεντρωμένη εφαρμογή η οποία επιτρέπει τη χρήση κρυπτοπαραστατικών (NFTs) με σκοπό την αξιόπιστη και διαφανή ανταλλαγή και αποθήκευση δεδομένων. Όλοι οι κόμβοι του δικτύου επωφελούνται από την είσοδό τους σε αυτό. Συγκεκριμένα, η εφαρμογή επιτρέπει σε κόμβους του δικτύου που αντιστοιχούν σε εργαζόμενους να διαθέτουν δεδομένα που σχετίζονται με το βιογραφικό και την εργασιακή εμπειρία τους σε εταιρείες, λαμβάνοντας ένα αντίτιμο για την διάθεση των βιογραφικών αυτών. Οι εταιρείες, από την άλλη, ως κόμβοι του δικτύου έχουν τη δυνατότητα πρόσβασης σε πληθώρα αναλλοίωτων, ελεγμένων και αξιόπιστων στοιχείων KYE (Know-Your-Employee), με χρέωση ανά αγορά πρόσβασης στα δεδομένα του εκάστοτε εργαζόμενου.

Η εφαρμογή προσφέρει μια ολοκληρωμένη διεπαφή για τον χρήστη, επιτρέποντάς του να καταχωρήσει δεδομένα, να διαβάσει δεδομένα καθώς και να προσθέσει ή να αφαιρέσει δικαιώματα άλλων χρηστών, αν ο ρόλος του το επιτρέπει. Οι χρεώσεις που αντιστοιχούν για την πρόσβαση στα δεδομένα ενός χρήστη, αλλά και οι πληρωμές στους χρήστες των οποίων τα δεδομένα προσπελαύνονται, εκτελούνται αυτόματα. Οι οργανισμοί που είναι υπεύθυνοι για την ορθότητα των δεδομένων των χρηστών πριν αυτά ανέβουν στο δίκτυο blockchain – και επομένως αποκτήσουν αμεταβλητότητα -, έχουν το δικαίωμα να πραγματοποιήσουν ανάληψη χρημάτων από τα συλλεγόμενα χρήματα εντός του Blockchain, τα οποία μαζεύονται από τις λειτουργικές χρεώσεις της εκτέλεσης μεθόδων του Smart Contract (gas fees).

Αξίζει να σημειωθεί ότι ο σκοπός της εφαρμογής προϋποθέτει την ανάρτηση αρχείων στο blockchain. Τέτοια αρχεία μπορεί να είναι βιογραφικά, πιστοποιητικά, νομικά έγγραφα κλπ. Εάν τα αρχεία αυτά ανέβαιναν στο blockchain ως έχουν, τότε το μέγεθος της κατάστασης μηχανής (machine state) του EVM θα αυξανόταν με ταχύτατους ρυθμούς. Αυτό θα είχε ως αποτέλεσμα το διάβασμα και η επικύρωση τους από τους κόμβους του δικτύου να κατέληγε να είναι αργή και ακριβή. Τη λύση σε αυτό έδωσε η χρήση του συστήματος IPFS για την αποκεντρωμένη αποθήκευση δεδομένων και η ανάρτηση στο blockchain μονάχα των συνδέσμων CID που οδηγούν στα δεδομένα αυτά.

Τονίζεται, ότι το αντίκτυπο της χρήσης της πλατφόρμας IPFS στο κόστος Gas, αλλά και στον χρόνο εκτέλεσης των εντολών ανάρτησης και παραλαβής δεδομένων blockchain μετρήθηκε και σημειώθηκε. Πράγματι, η χρήση του IPFS επιφέρει αισθητή βελτίωση στην αποτελεσματικότητα της εφαρμογής, αλλά και στην ικανότητα που τη διέπει για κλιμάκωση (scaling).

Μετρήθηκαν επίσης τα κόστη και οι χρόνοι εκτέλεσης όλων των μεθόδων του έξυπνου συμβολαίου που αναπτύχθηκε για την αποκεντρωμένη εφαρμογή. Σκοπός των μετρήσεων αυτών ήταν να αποδειχθεί η βιωσιμότητα μιας τέτοιας εφαρμογής σε ένα αληθινό δίκτυο, μιας και για την παρούσα εργασία χρησιμοποιήθηκε προσομοιωμένο. Η εφαρμογή αποδείχθηκε αρκετά αποτελεσματική και δεν εμφάνισε αποτρεπτικά κόστη ή χρόνους εκτέλεσης.

Τέλος, δίνεται βάση στην κρυπτογράφηση των δεδομένων των εργαζομένων. Η κρυπτογράφηση των δεδομένων πριν από την ανάρτησή τους στο blockchain αποτελεί έναν ακόμα κλοιό ασφαλείας πέραν του ήδη υφιστάμενου που είναι η αποκέντρωση που προσφέρει

το IPFS. Οι χρόνοι κρυπτογράφησης αρχείων και δεδομένων μετρήθηκαν εκτενώς και η συμμετοχή τους στη συνολική επίδοση της εφαρμογής φαίνεται να είναι σχετικά μικρή.

6.2 Μελλοντικές Προεκτάσεις

Η αποκεντρωμένη εφαρμογή που περιγράφεται στα προηγούμενα κεφάλαια αποτελεί το έναυσμα αλλά και ένα σημαντικό θεμέλιο για περισσότερη έρευνα στον τομέα της διασφάλισης δεδομένων με χρήση NFT. Ο τομέας αυτός αναμένεται να εξελιχθεί ραγδαία τα επόμενα χρόνια και ως εκ τούτου παρόμοιες εφαρμογές θα αναπτυχθούν και θα αποκτήσουν πιο διευρυμένη λειτουργικότητα. Στα πλαίσια των εξελίξεων αυτών παρακάτω αναλύονται τρόποι επέκταση και εναλλακτικής υλοποίησης της παρούσας εργασίας

6.2.1 Χρήση διαφορετικού τύπου Blockchain

Το Ethereum blockchain το οποίο χρησιμοποιήθηκε για την εφαρμογή είναι ένα από τα πολλά είδη blockchain που χρησιμοποιούνται στις μέρες μας. Θα ήταν άξια μελέτης η υλοποίηση παρόμοιων εφαρμογών που να βασίζονται σε άλλου είδους blockchain. Το Solana είναι ένα υποψήφιο κρυπτονόμισμα-blockchain. Είναι δημοφιλές και ανερχόμενο και ως εκ τούτου πολύ συχνά συγκρίνεται με το Ethereum [49]. Εμφανίζει πρακτικά πλεονεκτήματα όπως η χαμηλότερη τιμή συναλλαγών και η ευκολότερη κλιμάκωση, χάρη στον μηχανισμό συναίνεσης PoH (Proof of History) [50], ο οποίος επιτρέπει την ταχύτερη επεξεργασία block σε σχέση με τον PoS (proof of stake). Θα είχε ωστόσο ενδιαφέρον να μην περιοριστεί κανείς στη χρήση ενός εκ των δύο αυτών αρχιτεκτονικών blockchain, αλλά να δοκιμάσει και λιγότερο γνωστά είδη δικτυών αλυσίδας-κορμού όπως το TRON blockchain [51] ή το BNB Smart Chain [52]. Ένας καλός δείκτης για την αξιολόγηση των δυνατοτήτων μιας αρχιτεκτονικής blockchain, αλλά και της απήχησης που αυτή έχει είναι ο δείκτης TVL (Total Value Locked) [53], ο οποίος θα βοηθούσε σίγουρα στην εν λόγω απόφαση.

6.2.2 Διερεύνηση διαφορετικών τρόπων κρυπτογράφησης

Για την κρυπτογράφηση των δεδομένων KYE πριν την ανάρτησή τους στο διαπλανητικό σύστημα αρχείων IPFS, χρησιμοποιήθηκε όπως αναφέραμε ο αλγόριθμος AES (Advanced Encryption Standard). Ο αλγόριθμος αυτός προέρχεται από το Αμερικανικό Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών (U.S. Federal Information Processing Standard or FIPS) και αποτελεί προϊόν προσεκτικού σχεδιασμού. Η βιβλιοθήκη CryptoJS υποστηρίζει τρεις εκδοχές του πρότυπου: Την AES-128, την AES-192 και την AES-256. Επιλέγεται κάθε φορά η ιδανική εκδοχή αυτόματα, με βάση το κλειδί που εισάγεται στον αλγόριθμο [54]. Θα ήταν δόκιμο να δοκιμαστούν και επιπλέον αλγόριθμοι, μιας και η επίδοση, αλλά και η ασφάλεια που προσφέρει ο κάθε αλγόριθμος είναι διαφορετική. Συγκεκριμένα, υποσχόμενοι φαίνονται οι αλγόριθμοι SHA-3, RC4 και Rabbit, οι οποίοι μάλιστα είναι διαθέσιμοι εντός της βιβλιοθήκης CryptoJS που χρησιμοποιούμε.

6.2.3 Μετάβαση από το πρωτόκολλο ERC-721 στο νεότερο ERC-1155

Θα ήταν σίγουρα χρήσιμο να μελετηθούν τα πλεονεκτήματα που θα επέρχονταν με την υιοθέτηση του προτύπου ERC-1155 για NFT, έναντι του ERC-721 που επιλέξαμε να χρησιμοποιήσουμε. Αξίζει να σημειωθεί ότι το ERC-721 επιλέχθηκε λόγω της δημοφιλίας του, της ευρείας χρήσης του σε πληθώρα αποκεντρωμένων εφαρμογών και της ευκολίας στην διεπικοινωνία (interoperability) που αυτό συνεπάγεται. Εντούτοις, το ERC-1155 εμφανίζει αξιόλογες ιδιότητες όπως η δυνατότητα που προσφέρει στο να εκδίδεται σε πλήθος (batch minting) που συνεπάγεται την εξοικονόμηση καυσίμου καθώς μια και μόνο συναλλαγή αρκεί για την έκδοση πολλών παραστατικών. Αν σε αυτό προσθέσει κανείς την δυνατότητα έκδοσης εναλλάξιμων κρυπτοπαραστατικών, αλλά και την αυξημένη ασφάλεια που διέπει τη χρήση των παραστατικών, διαφαίνεται η αξία της εξέτασης του νεότερου προτύπου.

6.2.4 Χρήση διαφορετικού provider

Ο πάροχος που διασυνδέει τον φυλλομετρητή με το έξυπνο συμβόλαιο στην αποκεντρωμένη εφαρμογή μας είναι το MetaMask. Μάλιστα, όπως έχει ήδη αναλυθεί, το MetaMask φροντίζει και για την υπογραφή και επικύρωση των συναλλαγών-μεθόδων που καλούν οι χρήστες-κόμβοι του δικτύου. Ωστόσο, το MetaMask είναι μια πλατφόρμα που χρησιμοποιείται κυρίως στο Ethereum Blockchain ή σε άλλα Blockchain που βασίζονται σε EVMs. Υπάρχουν άλλοι πάροχοι και πορτοφόλια των οποίων η χρήση είναι ευρύτερη. Επιπλέον, νέα ανερχόμενα Wallets έχουν συχνά λειτουργικότητες που δεν εμφανίζονται σε παλαιότερα όπως το MetaMask.

6.2.5 Δοκιμή εργαλείων κλιμάκωσης όπως side-chains (Polygon)

Όπως έχουμε ήδη αναλύσει, ένα σημαντικό πρόβλημα που εμφανίζουν τα δίκτυα αλυσίδας κορμού είναι η κλιμάκωση. Όσο πιο περίπλοκες και βεβαρημένες με δεδομένα γίνονται οι συναλλαγές - μέθοδοι που καταγράφονται στο blockchain, τόσο πιο πολύ αυξάνεται ο χρόνος απόκρισης του δικτύου αλλά και το κόστος πραγματοποίησής τους. Η λύση που δόθηκε για το πρόβλημα αυτό στην εφαρμογή KYE που παρουσιάζουμε είναι η ανάρτηση των δεδομένων σε ένα σύστημα IPFS. Υπάρχουν ωστόσο και άλλοι τρόποι να φροντίσει κανείς για την επιτυχή κλιμάκωση μιας αποκεντρωμένης εφαρμογής. Επί παραδείγματι, η τεχνολογία των side-chains, δηλαδή βοηθητικών αλυσίδων κορμού οι οποίες συνδέονται με την κύρια αλυσίδα κορμού μέσω ενός διπλού διαύλου επικοινωνίας, είναι πλέον ευρέως γνωστή για την αύξηση της κλιμάκωσης που μπορεί να επιφέρει. Αποκεντρωμένες εφαρμογές που απαιτούν κλιμάκωση πλέον καταφεύγουν σε τέτοιες λύσεις. Η σουίτα Polygon [55] είναι ένα χαρακτηριστικό παράδειγμα εργαλείου κλιμάκωσης αποκεντρωμένων εφαρμογών που θα άξιζε σίγουρα να μελετηθεί.

7 Βιβλιογραφία

[1] “Significant Cyber Incidents | Strategic Technologies Program | CSIS.” Accessed: Oct. 02, 2024. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[2] “eGov-KYC βήμα-βήμα | Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης.” Accessed: Sep. 24, 2024. [Online]. Available: https://www.gsis.gr/egov-kyc-bima-bima

[3] “Συστηθείτε - Know Your Customer (eGov- KYC),” Gov.gr. Accessed: Sep. 24, 2024. [Online]. Available: https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/stoikheia-polite-kai-tautopoietika-eggrapha/kyc

[4] “Διευθυντής κλινικής χειρουργούσε για χρόνια με πλαστό τίτλο σπουδών,” ΤΟ ΒΗΜΑ. Accessed: Sep. 23, 2024. [Online]. Available: https://www.tovima.gr/2015/11/21/society/dieythyntis-klinikis-xeiroyrgoyse-gia-xronia-me-plasto-titlo-spoydwn/

[5] P. Patil and M. Sangeetha, “Blockchain-based Decentralized KYC Verification Framework for Banks,” *Procedia Comput. Sci.*, vol. 215, pp. 529–536, Jan. 2022, doi: 10.1016/j.procs.2022.12.055.

[6] “KYC Trends in 2023 | A Global Research Report.” Accessed: Oct. 07, 2024. [Online]. Available: https://www.fenergo.com/kyc-trends

[7] C. C. Drăgan and M. Manulis, “KYChain: User-Controlled KYC Data Sharing and Certification,” in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Mar. 2020, pp. 301–307. doi: 10.1145/3341105.3373895.

[8] M. Hannan, M. Shahriar, Md. S. Ferdous, M. Chowdhury, and M. Rahman, “A systematic literature review of blockchain-based e-KYC systems,” *Computing*, vol. 105, pp. 1–30, Apr. 2023, doi: 10.1007/s00607-023-01176-8.

[9] N. Sun, Y. Zhang, and Y. Liu, “A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains,” *Sustainability*, vol. 14, p. 14584, Nov. 2022, doi: 10.3390/su142114584.

[10] “KYC for NFTs: Digital Art | Togggle.” Accessed: Oct. 07, 2024. [Online]. Available: https://www.togggle.io/blog/kyc-for-nfts-safeguarding-future-of-digital-art

[11] “KYC for NFTs: Balancing Security and Accessibility,” KYC Chain. Accessed: Oct. 07, 2024. [Online]. Available: https://kyc-chain.com/?insight=kyc-for-nfts-balancing-security-and-accessibility

[12] Serenawilliams, “NFTs: Revolutionizing Digital Identities: A Deep Dive into Blockchain Identity Management,” Coinmonks. Accessed: Oct. 07, 2024. [Online]. Available: https://medium.com/coinmonks/nfts-revolutionizing-digital-identities-a-deep-dive-into-blockchain-identity-management-d973a55771a0

[13] E. Esoimeme, “Curbing Employee Fraud and Corruption in Financial Institutions With an Effective Know Your Employee Program,” Nov. 12, 2018, *Rochester, NY*: 3287949. doi: 10.2139/ssrn.3287949.

[14] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Jun. 2017. doi: 10.1109/BigDataCongress.2017.85.

[15] P. Aithal, P. Saavedra, S. Aithal, and S. Ghoash, “Blockchain Technology and its Types-A Short Review,” *Int. J. Appl. Sci. Eng.*, vol. 9, pp. 189–200, Dec. 2021.

[16] S. Zhang and J.-H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT Express*, vol. 6, no. 2, pp. 93–97, Jun. 2020, doi: 10.1016/j.icte.2019.08.001.

[17] “Ethereum Virtual Machine (EVM),” ethereum.org. Accessed: Sep. 21, 2024. [Online]. Available: https://ethereum.org/en/developers/docs/evm/

[18] Q. Wang, R. Li, Q. Wang, and S. Chen, “Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges,” Oct. 24, 2021, *arXiv*: arXiv:2105.07447. doi: 10.48550/arXiv.2105.07447.

[19] “Αποκεντρωμένη εφαρμογή (dApp),” Binance Academy. Accessed: Sep. 21, 2024. [Online]. Available: https://academy.binance.com/el/glossary/decentralized-application

[20] “Decentralized Applications (dApps): Definition, Uses, Pros and Cons,” Investopedia. Accessed: Sep. 21, 2024. [Online]. Available: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

[21] V. U. Rajput, “Research on Know Your Customer (KYC),” vol. 3, no. 7, 2013.

[22] “What Is Encryption? Explanation and Types,” Cisco. Accessed: Sep. 21, 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/security/encryption-explained.html

[23] National Institute of Standards and Technology (US), “Advanced Encryption Standard (AES),” National Institute of Standards and Technology (U.S.), Washington, D.C., NIST FIPS 197-upd1, May 2023. doi: 10.6028/NIST.FIPS.197-upd1.
[24] “What is the Advanced Encryption Standard (AES)? | Definition from TechTarget,” Security. Accessed: Sep. 22, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[25] P. Security, “What Is Advanced Encryption Standard (AES)? - Panda Security,” Panda Security Mediacenter. Accessed: Sep. 22, 2024. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/what-is-aes-encryption/
[26] “ERC-721: Non-Fungible Token Standard,” Ethereum Improvement Proposals. Accessed: Sep. 21, 2024. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721
[27] “ERC-1155 Multi-Token Standard,” ethereum.org. Accessed: Sep. 21, 2024. [Online]. Available: https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/
[28] “ERC-721 vs ERC-1155: Which is Better for NFTs?,” Chetu. Accessed: Sep. 22, 2024. [Online]. Available: https://www.chetu.com/blogs/blockchain/erc-721-vs-erc-1155.php
[29] “Home,” Solidity Programming Language. Accessed: Sep. 22, 2024. [Online]. Available: https://soliditylang.org/
[30] “Vyper.” Accessed: Sep. 22, 2024. [Online]. Available: https://docs.vyperlang.org/en/stable/
[31] “Yul — Solidity 0.8.28 documentation.” Accessed: Sep. 22, 2024. [Online]. Available: https://docs.soliditylang.org/en/latest/yul.html
[32] “Fe - A next generation, statically typed, future-proof smart contract language for the Ethereum Virtual Machine.” Accessed: Sep. 22, 2024. [Online]. Available: https://fe-lang.org
[33] J. Howell, “Vyper vs Solidity- Key Differences Between Ethereum Smart Contract Languages,” 101 Blockchains. Accessed: Sep. 22, 2024. [Online]. Available: https://101blockchains.com/vyper-vs-solidity/
[34] “OpenZeppelin.” Accessed: Sep. 22, 2024. [Online]. Available: https://www.openzeppelin.com
[35] “Hardhat Network | Ethereum development environment for professionals by Nomic Foundation.” Accessed: Sep. 16, 2024. [Online]. Available: https://hardhat.org
[36] “ApeWorx Academy.” Accessed: Sep. 16, 2024. [Online]. Available: https://academy.apeworx.io/articles/porting-brownie-to-ape
[37] “Home - Truffle Suite.” Accessed: Sep. 16, 2024. [Online]. Available: https://archive.trufflesuite.com/
[38] “Remix - Ethereum IDE.” Accessed: Sep. 16, 2024. [Online]. Available: https://remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.26+commit.8a97fa7a.js
[39] MiDa, “Answer to ‘Difference of Geth or Ganache,’” Stack Overflow. Accessed: Sep. 21, 2024. [Online]. Available: https://stackoverflow.com/a/57511750
[40] “The Ultimate Crypto Wallet for DeFi, Web3 Apps, and NFTs | MetaMask.” Accessed: Sep. 21, 2024. [Online]. Available: https://metamask.io/
[41] “Best Crypto Wallet for Web3, NFTs and DeFi | Trust,” Trust Website. Accessed: Sep. 21, 2024. [Online]. Available: https://trustwallet.com/
[42] “Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins,” Binance. Accessed: Sep. 21, 2024. [Online]. Available: https://www.binance.com
[43] WalletConnect, “WalletConnect - Explorer,” WalletConnect. Accessed: Sep. 21, 2024. [Online]. Available: https://walletconnect.com
[44] “HTML Standard.” Accessed: Sep. 22, 2024. [Online]. Available: https://html.spec.whatwg.org/
[45] “Cascading Style Sheets.” Accessed: Sep. 22, 2024. [Online]. Available: https://www.w3.org/Style/CSS/Overview.en.html
[46] “web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation.” Accessed: Sep. 22, 2024. [Online]. Available: https://web3js.readthedocs.io/en/v1.10.0/
[47] “crypto-js,” npm. Accessed: Sep. 22, 2024. [Online]. Available: https://www.npmjs.com/package/crypto-js
[48] “IPFS Documentation | IPFS Docs.” Accessed: Oct. 10, 2024. [Online]. Available: https://docs.ipfs.tech/
[49] A. Weiler, “Ethereum vs. Solana: Which Blockchain Will Lead in the Long Run?,” Medium. Accessed: Oct. 07, 2024. [Online]. Available: https://medium.com/@13ajw12/ethereum-vs-solana-which-blockchain-will-lead-in-the-long-run-6ed5b4744a7c
[50] A. Yakovenko, “Solana: A new architecture for a high performance blockchain”.
[51] “TRON | Decentralize The Web.” Accessed: Oct. 07, 2024. [Online]. Available: https://tron.network/

[52] “BNB Smart Chain (BSC): Bring Smart Contracts to BNB Chain,” BNB Chain. Accessed: Oct. 07, 2024. [Online]. Available: https://www.bnbchain.org/en/bnb-smart-chain
[53] “Total Value Locked (TVL) in Cryptocurrency: Everything You Need to Know,” Investopedia. Accessed: Oct. 07, 2024. [Online]. Available: https://www.investopedia.com/total-value-locked-7486821
[54] “CryptoJS | CryptoJS.” Accessed: Oct. 07, 2024. [Online]. Available: https://cryptojs.gitbook.io/docs/
[55] “Web3, Aggregated.” Accessed: Oct. 07, 2024. [Online]. Available: https://polygon.technology/