



Ιόνιο Πανεπιστήμιο
Σχολή Επιστήμης Της Πληροφορίας & Πληροφορικής
Τμήμα Πληροφορικής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανάπτυξη εφαρμογής Crowdfunding με την χρήση Smart Contracts

Υποψήφιος: Αριστείδης Κοντίνης (Π2017144)

Επιβλέπων: Χριστόφορος Νταντογιάν (Επίκουρος Καθηγητής)

Κέρκυρα

2022

Η παρούσα Πτυχιακή εργασία εγκρίθηκε ομόφωνα από την τριμελή εξεταστική επιτροπή, η οποία ορίστηκε σύμφωνα με το νόμο και τον εγκεκριμένο οδηγό σπουδών του τμήματος.

Χριστόφορος Νταντογιάν (Επίκουρος Καθηγητής)	Εμμανουήλ Μάγκος (Αναπληρωτής Καθηγητές)	Άννα Σωτηροπούλου (Μέλος ΕΔΙΠ)
(Υπογραφή)	(Υπογραφή)	(Υπογραφή)

Περιεχόμενα

Περιεχόμενα.....	4
Ευχαριστίες.....	6
Περίληψη	7
Εισαγωγή.....	8
2 Η τεχνολογία του Blockchain.....	11
2.1 Τι είναι το Blockchain;.....	11
2.2 Θεμελιώδεις ιδιότητες	12
2.3 Τύποι Συστημάτων.....	13
2.3.1 Κεντριοποιημένα συστήματα	13
2.3.2 Κατανεμημένα συστήματα	14
2.3.3 Αποκεντρωμένα συστήματα	14
2.4 Πλεονεκτήματα του Blockchain.....	15
2.5 Προκλήσεις του Blockchain.....	16
2.6 Το Πρόβλημα των Βυζαντινών Στρατηγών.....	16
3 Η Αρχιτεκτονική του Blockchain	19
3.1 Αλγόριθμος Συναίνεσης Proof of Work	19
3.2 Δομή ενός Μπλοκ.....	19
3.3 Αλυσίδα μπλοκ.....	21
3.4 Forks	22
3.5 Κατηγοριοποίηση Blockchain	23
3.5.1 Public	23
3.5.2 Permissioned	24
3.5.3 Private	24
3.6 Επιθέσεις και απειλές	24
4 Κρυπτογραφία.....	27
4.1 Συμμετρική κρυπτογραφία	27
4.2 Ασύμμετρη κρυπτογραφία.....	28
4.3 Κρυπτογραφική Συνάρτηση (Hash)	29
4.4 Ψηφιακή Υπογραφή.....	29
4.5 Παραγωγή διευθύνσεων	30
4.6 Αποθήκευση ιδιωτικών κλειδιών	30
4.7 Ασφάλεια και κίνδυνοι Απώλειας κλειδιών.....	30
5 Ethereum & Smart Contracts	33
5.1 Το δίκτυο του Ethereum.....	33

5.2 Τι είναι τα <i>Smart Contracts</i> ;	34
5.3 EVM	35
5.4 Dapps	35
6 Σχεδιασμός του Συστήματος και εργαλεία	37
6.1 Υπάρχουσες Προσεγγίσεις <i>Crowdfunding</i>	37
6.2 Διαγραμμα Ροής	39
6.3 Αρχιτεκτονικής του Dapp.	40
6.4 Εργαλεία που θα χρειαστούν για την ανάπτυξη	42
6.4.1 Metamask	42
6.4.2 Hardhat	43
6.4.3 Solidity	44
6.4.4 Δίκτυο Testnet	44
6.4.5 Remix	45
6.4.6 IPFS	46
6.4.7 Node.js	46
6.4.8 React & Next.js	46
7 Υλοποίηση του Συστήματος	49
Βιβλιογραφικές αναφορές	55
Παράρτημα 1: Οδηγίες εγκατάστασης	57
Παράρτημα 2: Κώδικας <i>Smart Contracts</i>	59

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της εργασίας μου, Χριστόφορος Νταντογιάν για την ευκαιρία που μου έδωσε να. Τον ευχαριστώ για την εμπιστοσύνη που μου έδειξε, για την υποστήριξη, την υπομονή και την προτροπή του στην δημιουργία Smart Contracts και σε αντίθεση με μια βιβλιογραφική εργασία όπως είχα αρχικά ως στόχο στην αρχή του ακαδημαϊκού έτους.

Τέλος, ιδιαίτερα θερμές ευχαριστίες θέλω να δώσω στην μητέρα μου Αφροδίτη για την συνεχή συμπαράσταση της, για τις πολύτιμες συμβουλές της και για όλα όσα μου έχει προσφέρει όλα αυτά τα χρόνια της ζωής μου αλλά και των σπουδών μου. Επίσης θέλω να ευχαριστήσω την αδερφή μου Ιωάννα που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της πτυχιακής μου εργασίας.

A.Κοντίνης
Κέρκυρα, Σεπτέμβριος 2022

Περίληψη

Η τεχνολογία Blockchain λύνει το πρόβλημα της σύγχρονης καταγραφής δεδομένων σε ένα κατανεμημένο δίκτυο διασφαλίζοντας ότι τα δεδομένα που αποθηκεύονται κάθε φορά είναι ακριβώς τα ίδια. Αυτό αποτρέπει τους κόμβους στο δίκτυο να διαφωνούν σχετικά με την ακρίβεια των δεδομένων, κάτι που διαφορετικά θα οδηγούσε σε ασυνέπειες. Κάθε υπολογιστής που συμμετέχει σε ένα δίκτυο Blockchain αποθηκεύει τα ίδια δεδομένα, τα οποία δεν μπορούν να αλλαχθούν ή να τροποποιηθούν και είναι ασφαλισμένα με την χρήση της κρυπτογραφίας.

Η ανατρεπτική τεχνολογία του Blockchain αρχίζει να απομακρύνεται από την αρχική της εφαρμογή (κρυπτονομίσματα) και αρχίζει να αλλάζει τον τρόπο με τον οποίο οι άνθρωποι χρησιμοποιούν το διαδίκτυο. Το Blockchain είναι ένας ψηφιακός κατανεμημένος και δημόσιος κατάλογος (ledger) στον οποίο καταγράφονται οι συναλλαγές και οι συμφωνίες με τρόπο αδιάβλητο και υποστηρίζεται από ένα δίκτυο ομότιμων κόμβων.

Αυτό οδήγησε στην ανάπτυξη αποκεντρωμένων εφαρμογών (DApps), οι οποίες επιτρέπουν στους συμμετέχοντες σε ένα Blockchain να επικοινωνούν μεταξύ τους χωρίς την ανάγκη εμπιστοσύνης, αφού αυτό διασφαλίζεται από την ίδια την τεχνολογία. Βασίζεται σε ένα δίκτυο ομότιμων κόμβων και θωρακίζεται με τεχνικές ομοφωνίας (consensus) μεταξύ των κόμβων, ώστε να διασφαλίζεται η ορθότητα και εγκυρότητα των δεδομένων που αποθηκεύονται στην αλυσίδα.

Για τις ανάγκες της παρούσας πτυχιακής, αναπτύχθηκε, πάνω στο testnet του Polygon, μία αποκεντρωμένη εφαρμογή, που δίνει στους χρήστες της τη δυνατότητα να προσφέρουν να δημιουργήσουν καμπάνιες Crowdfunding και χρηματοδοτηθεί από άλλους χρήστες. Στην παρούσα εργασία, θα γίνει εκτενής αναφορά στα θεωρητικά θεμέλια τα οποία χρειάζονται για την ανάπτυξη της προαναφερθείσας εφαρμογής, καθώς και μια παρουσίαση της εφαρμογής καθαυτής, με περιγραφή του τρόπου με τον οποίο αναπτύχθηκε, αλλά και κάποιων από τα βασικότερα use-cases.

Λέξεις-Κλειδιά: Smart Contracts, Blockchain, Crowdfunding, Web3.0, Αποκεντρωμένη Εφαρμογή, Solidity, Polygon

1

Εισαγωγή

Στις αρχές της δεκαετίας του 90' εμφανίζεται το διαδίκτυο με την μορφή του Web 1.0 το οποίο ξεκίνησε ως ένα τρόπος επικοινωνίας μεταξύ άλλων ανθρώπων με την χρήση στατικών ιστοσελίδων. Αυτή η ραγδαία ανταλλαγή πληροφοριών άλλαξε την μορφή του συγχρόνου κόσμου. Στην πορεία οι ανάγκες και οι απαιτήσεις του κόσμου οδήγησαν το διαδίκτυο να μετεξελιχθεί σε μια άλλη μορφή ώστε να θεωρούμε από το 2004 και υστέρτα το παγκόσμιο ιστό ως Web 2.0, το οποίο έφερε πληθώρα από νέες εφαρμογές όπως τα κοινωνικά δίκτυα, το ηλεκτρονικό εμπόριο κ.λπ., έτσι ο παγκόσμιος ιστός άρχισε να αλλάζει από τις απλές στατικές ιστοσελίδες σε πιο δυναμικές και να γίνεται όλο και πιο προσβάσιμες σε κινητές συσκευές.

Το διαδίκτυο έδωσε την δυνατότητα να φτιαχτούν πολλές εφαρμογές μια από αυτές ήταν η εναλλακτική μορφή χρηματοδότησης crowdfunding, που συνδέει εκείνους που μπορούν να δώσουν, να δανείσουν ή να επενδύσουν τα χρήματα απευθείας με εκείνους που χρειάζονται χρηματοδότηση για ένα συγκεκριμένο έργο. Έτσι στα τέλη της δεκαετίας του 2000 δημιουργούνται διάφοροι διαδικτυακοί ιστότοποι που στόχο την συγκέντρωση ποσών για διάφορους σκοπούς και λειτουργεί ως μεσάζοντας. Οι πιο γνωστοί στο ισόχωρο crowdfunding είναι το Kickstarter και το Indiegogo τα οποία έδιναν την δυνατότητα να συγκεντρώσουν χρήματα.

Το 2009 ο Satoshi Nakamoto προτείνει ένα πρωτόκολλο τεχνολογίας για το πρώτο κρυπτονόμισμα με όνομα Bitcoin για την εκτέλεση ψηφιακών οικονομικών συναλλαγών μεταξύ άλλων χρηστών που λειτουργεί ακόμα και σήμερα. Το Bitcoin είναι ένα σύνολο τεχνολογιών και δημιουργήθηκε ως μια απάντηση για την προστασία του κόσμου από τον πληθωρισμό. Το Bitcoin είναι στην ουσία ένα κατανεμημένο peer-to-peer σύστημα το οποίο μοιράζεται και δημιουργείται από πολλούς διαφορετικούς ομότιμους χρήστες (peers) και ως εκ τούτου, δεν υπάρχει κάποιος κεντρικός διακομιστής που μπορεί να παρεμβεί ή να τροποποιήσει τις συναλλαγές.

Έτσι ξεκίνησε το Blockchain δηλαδή μια αλυσίδα συναλλαγών που μεταφέραν αξία ένας χρήστης σε έναν άλλο. Η μεγάλη απήχηση και καινοτομίες που έφερε το Bitcoin έδωσε το ερέθισμα και σε άλλους προγραμματιστές να δημιουργήσουν τους δικούς τους κλώνους (fork) που είχαν διαφορετικές προτεραιότητες από το Bitcoin. Έτσι το 2014 ο Vitalik Buterin προτείνει την δημιουργία ενός νέου πρωτόκολλου με όνομα Ethereum στο οποίο θα ήταν μια πλατφόρμα που

υποστηρίζει την δημιουργία αποκεντρωμένων εφαρμογών με την χρήση των έξυπνων συμβολαίων (Smart Contracts).

Τα έξυπνα συμβόλαια είναι μια σύμβαση που χρησιμοποιείται για να περιγράψει μερικές γραμμές κώδικα που στόχο έχει την διευκόλυνση των συναλλαγών χρήματων, περιεχομένου και οτιδήποτε έχει αξία. Όταν εκτελείται ένα έξυπνο συμβόλαιο λειτουργεί σαν ένα πρόγραμμα στο Blockchain το οποίο δεν μπορεί να επηρεαστεί από κάποιον τρίτο και είναι φτιαγμένο με τέτοιο τρόπο να λειτουργεί ακριβώς όπως έχει προγραμματιστεί.

Στην εξέλιξη του διαδικτύου δημιουργήθηκε ένας γενικός όρος για το όραμα ενός νέου Διαδικτύου με το όνομα Web3 (ή αλλιώς Web 3.0). Στον πυρήνα του, το Web3 χρησιμοποιεί το blockchain, τα κρυπτονομίσματα και τα NFT (Non-fungible token) για να δώσει ισχύ στους χρήστες με τη μορφή ιδιοκτησίας. Το Web3 είναι στην ουσία αποκεντρωμένο και αντί για μεγάλα τμήματα του Διαδικτύου που ελέγχονται και ανήκουν σε κεντρικές οντότητες, η ιδιοκτησία κατανέμεται μεταξύ των δημιουργών και των χρηστών του. Αφού το Web3 υποστηρίζει πληρωμές με την χρήση κρυπτονομισμάτων για να ξοδεύει και να στέλνει χρήματα στο διαδίκτυο αντί να βασίζεται στην απαρχαιωμένη υποδομή των τραπεζών και των επεξεργαστών πληρωμών.

Οι περισσότερες σημερινές web 2.0 πλατφόρμες crowdfunding όπως το Kickstarter και το Indigogo υστερούν στο τρόπο λειτουργίας τους. Αυτές οι πλατφόρμες δουλεύουν με ένα πρότυπο εμπορευματοποίησης της διαδικασίας ελέγχεται κάτω από μια κεντρική αρχή και έχει δυο κυρία προβλήματα στο τρόπο της χρηματοδότησης. Το πρώτο αφορά την περιορισμένη πρόσβαση σε συγκεκριμένες ομάδες ανθρώπων όπως μεγάλα τμήματα του κόσμου που στερούνται υποδομές οικονομικών πληρωμών, ενώ το δεύτερο αφορά το πρόβλημα κεντροποίησης και του περιορισμούς που μπορεί να θέσει η πλατφόρμα εμποδίζοντας πολλούς χρηματοδότες να στηρίξουν το έργο.

1.1 Αντικείμενο της Πτυχιακής Εργασίας Ιδέα και στόχοι

Το αντικείμενο της παρακάτω εργασίας είναι να παρέχει τις βασικές πληροφορίες για την λειτουργία του Blockchain για την καλύτερη κατανόηση των εννοιών που θα αναλυθούν στο δεύτερο σκέλος στο οποίο δημιουργηθεί μια αποκεντρωμένη εφαρμογή για την δημιουργία καμπανιών ώστε να συγκεντρωθεί ένα ποσό για ένα σκοπό (crowdfunding). Ένα σύστημα το οποίο θα μπορεί να χρησιμοποιείται από τον καθένα χωρίς περιορισμούς με αμεσότητα, χωρίς ενδιάμεσους ώστε να χρονοτριβούν ή να επιβαρύνουν την διαδικασία. Χρησιμοποιώντας την ήδη υπάρχουσα δομή από το

δίκτυο του Polygon ως μεσάζοντα για την αλληλεπίδραση των χρηστών αφού η προσπέλαση των δεδομένων θα μπορεί να γίνεται τον καθένα χωρίς να χρειάζεται να υπάρχει εμπιστοσύνη από καμία κεντρική αρχή.

1.2 Οργάνωση και Δομή της Πτυχιακής

Το κείμενο της παραπάνω πτυχιακής εργασίας στα πρώτα 5 Κεφάλαια αφορούν πληροφορίες για το πώς λειτουργεί το Blockchain και στην συνέχεια στα επόμενα 2 κεφάλαια επεξηγείται πως αναπτύχθηκε η αποκεντρωμένη εφαρμογή (Dapp).

Το παρόν Κεφάλαιο, το οποίο αποτελεί την εισαγωγή γίνεται επεξήγηση του αντικειμένου που θα πραγματευτεί στην παρακάτω πτυχιακή καθώς και την οργάνωση και δομή που γίνεται σε αυτή την ενότητα. Στο Κεφάλαιο 2 της εργασίας γίνεται μια πρώτη παρουσίαση για την τεχνολογία του Blockchain, και ακόμη πως λειτουργεί. Το Κεφάλαιο 3 γίνεται ανάλυση διάφορων σχετικών εννοιών και καταστάσεις που μπορούν να δημιουργηθούν με την χρήση του Blockchain. Το Κεφάλαιο 4 αφορά τους αλγορίθμους κρυπτογραφία, Δημοσίων και ιδιωτικών κλειδιών και πως πρέπει να φυλάσσονται γίνεται επίσης αναφορά στα είδη των Blockchain και στην συνέχεια στο Κεφάλαιο 5 περιγράφεται πως λειτουργεί το Ethereum και τα έξυπνα συμβόλαια που θα χρησιμοποιηθούν στην ανάπτυξη της εφαρμογής.

Στο Κεφάλαιο 6 παρουσιάζονται τα απαραίτητα εργαλεία και προγράμματα που θα χρειαστούν να γίνουν εγκατάσταση για την υλοποίηση της αποκεντρωμένης εφαρμογής. Στο Κεφάλαιο 7 γίνεται μια λεπτομερής ανάλυση για την ανάπτυξη και την υλοποίηση της εφαρμογής καθώς και για την λειτουργικότητα της.

Η τεχνολογία του Blockchain

2.1 Τι είναι το Blockchain;

Ο όρος blockchain επινοήθηκε για πρώτη φορά επίσημα το 2008, όταν ένας προγραμματιστής ή μια ομάδα προγραμματιστών, με το όνομα Satoshi Nakamoto, στο οποίο δημοσίευσε μέσα από το White Paper του Bitcoin ένα ψηφιακό νόμισμα το οποίο δεν είχε τον έλεγχο κάποια κεντρική αρχή όπως για παράδειγμα μια τράπεζα αλλά ήταν εξολοκλήρου ελεγχόμενο από ομότιμους χρήστες του δικτύου του.

Το blockchain είναι μια κατανεμημένη βάση δεδομένων που καταγράφει τις συναλλαγές με επαληθεύσιμο τρόπο και δημιουργήθηκε για να υποστηρίξει το πρωτόκολλο του Bitcoin, ωστόσο στην πορεία χρησιμοποιήθηκε και για άλλους σκοπούς. Μια αλυσίδα μπλοκ όπως υποδηλώνει και το όνομά της είναι μια σειρά από μπλοκ με χρονική σήμανση, το καθένα από τα οποία προσδιορίζεται από μια κρυπτογραφική συνάρτηση κατακερματισμού και αναφορές σε προηγούμενους κατακερματισμούς έτσι οι σύνδεσμοι δημιουργούν αλυσίδες μεταξύ τους με κάθε προηγούμενο και επομένο μπλοκ.

Τα Blocks περιέχουν συναλλαγές που καταγράφουν την μεταφορά δεδομένων μεταξύ δύο διευθύνσεων. Ένας κόμβος σε ένα δίκτυο blockchain μπορεί να έχει πρόσβαση στο blockchain για να ανακτήσει την τρέχουσα κατάσταση της αλυσίδας. Αυτό επιτρέπει σε αυτόν τον κόμβο να περάσει σε μια άλλη αλυσίδα για να ανακατασκευάσει την τρέχουσα κατάσταση αυτής της αλυσίδας. Οι κόμβοι σε ένα δίκτυο blockchain λειτουργούν παρόμοια μεταξύ τους και σχηματίζουν ένα δίκτυο peer-to-peer όπου κάθε κόμβος παίζει κάποιο ρόλο στο blockchain. Για την επαλήθευση των συναλλαγών στο blockchain, κάθε κόμβος χρησιμοποιεί ένα ζεύγος δημόσιων και ιδιωτικών κλειδιών. Ο κόμβος κατασκευάζει και υπογράφει μια συναλλαγή και τη μεταδίδει στους ομότιμους του. Κάθε κόμβος επικυρώνει τις συναλλαγές που λαμβάνει, απορρίπτοντας μη έγκυρες συναλλαγές πριν τις μεταβιβάσει στους ομότιμους του. Αυτές οι συναλλαγές είναι ένα σύνολο έγκυρων εκκρεμών συναλλαγών που είναι έτοιμες να συμπεριληφθούν σε ένα μελλοντικό μπλοκ.

Οι miners είναι κόμβοι στο δίκτυο που είναι υπεύθυνοι για την δημιουργία νέων μπλοκ, τα οποία στη συνέχεια επαληθεύονται και προσθέτονται στην αλυσίδα συναλλαγών και μεταβιβάζονται στους ομότιμους τους. Έτσι αυτή η διαδικασία επαναλαμβάνεται συνεχώς επ' αόριστου και η αλυσίδα αυξάνεται κάθε φορά προσθέτετε ένα νέο μπλοκ.

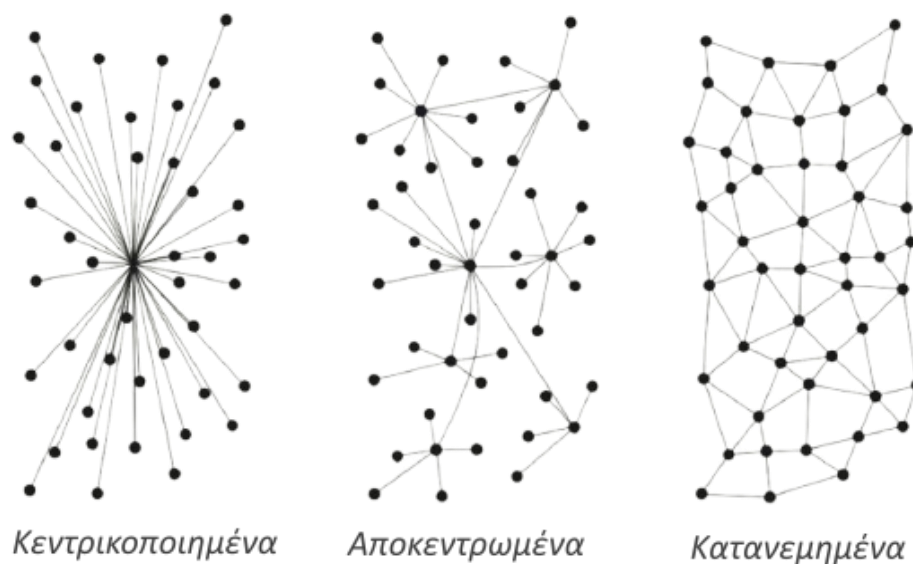
2.2 Θεμελιώδεις ιδιότητες

Η τεχνολογία του Blockchain έχει μερικά μοναδικά χαρακτηριστικά, τα οποία την καθιστούν τεχνολογία αιχμής. χωρίς να επικεντρωθούμε σε χιλιάδες υπάρχουσες εφαρμογές και στις δυνατότητές τους, εκείνα τα θεμελιώδη που χαρακτηρίζουν την τεχνολογία στο σύνολό της είναι τα παρακάτω:

- **Κατανομή:** Σε αντίθεση με τα κεντροποιημένα δίκτυα όπου πρέπει να μεταφέρονται όλες οι πληροφορίες από τον αποδεκτή σε μια κεντρική οντότητα του συστήματος, την οποία πρέπει να εμπιστεύονται και να χρησιμοποιούν ως διαμεσολαβητή. Στην περίπτωση του blockchain δεν χρειάζεται εμπιστοσύνη μεταξύ των άλλων χρηστών του δικτύου. Αφού αυτό το πρόβλημα λύνεται χρησιμοποιώντας αλγόριθμους συναίνεσης για να διασφαλίσει την ασφάλεια όλων των πληροφοριών που είναι αποθηκευμένες σε αυτό, τότε ο ρόλος του διαμεσολαβητή είναι περιττός.
- **Ανθεκτικότητα:** Κάθε συναλλαγή επικυρώνεται γρήγορα εάν είναι έγκυρη, ενώ οι ειλικρινείς ομότιμοι θα απορρίψουν κατά τυχόν μη έγκυρων συναλλαγών. Είναι πρακτικά αδύνατο να διαγράψουν ή να τροποποιηθούν οι συναλλαγές από τη στιγμή που αποθηκεύτηκαν στο Blockchain.
- **Ανωνυμία:** Το ζεύγος κλειδιών επιτρέπει στους χρήστες του δικτύου να συμμετέχουν σε μια συναλλαγή με τα κλειδιά που έχουν στην κατοχή τους. το δημόσιο κλειδί αντιπροσωπεύει τον χρήστη, αλλά το όνομά του δεν εμφανίζεται πουθενά. Φυσικά το blockchain δεν εγγυάται πλήρη ανωνυμία, αφού υπάρχουν ενδογενείς περιορισμοί.
- **Επαληθευσιμότητα:** Κάθε φορά που ο χρήστης συμμετέχει σε μια συναλλαγή, το υπόλοιπό του και οι πληροφορίες σχετικά με τη συναλλαγή αποθηκεύονται στο μπλοκ που περιέχει τη συναλλαγή. Με αυτόν τον τρόπο, είναι εύκολο να εντοπιστεί και να αξιολογηθεί οποιαδήποτε συναλλαγή εντός του δικτύου.

2.3 Τύποι Συστημάτων

Η επικοινωνία μεταξύ των κόμβων που συμμετέχουν σε ένα blockchain πραγματοποιείται φυσικά μέσω ενός δικτύου. Αν και μπορούμε να δημιουργήσουμε μια ποικιλία δικτύων, τα κύρια, όσον αφορά τον έλεγχο και τις αποφάσεις αρχιτεκτονικής λήψης, είναι κεντριοποιημένα και τα κατανεμημένα. Με την διαδικασία λήψης αποφάσεων και τις μεθόδους επικοινωνίας, τα συστήματά είναι ανάλογα με το σκοπό και τις διαφορετικές εργασίες που θα εκτελεστούν. Στην πραγματικότητα, συνήθως χρησιμοποιείται μια μικτή αρχιτεκτονική. Σαφώς γίνεται μια αναφορά στις ιδιαιτερότητες των άλλων τύπων δικτύων με σκοπό να γίνει πιο κατανοητά πως λειτουργούν τα δίκτυα Blockchain.



Εικόνα 2.1: Σύγκριση τύπων συστημάτων

2.3.1 Κεντριοποιημένα συστήματα

Τα κεντριοποιημένα συστήματα δικτύων έχουν σχεδιαστεί με γνώμονα μια κεντρική αρχή, η οποία έχει πλεονεκτήματα και αδυναμίες που είναι εμφανή στην ικανότητά τους να ελέγχουν τα δεδομένα. Ωστόσο, η καταστροφή του κεντρικού κόμβου θα οδηγήσει σε ολική απώλεια επικοινωνίας σε όλους τους κόμβους του δικτύου. Το μοντέλο αυτό συγκεντρώνει όλους του δικτυακούς πόρους σε ένα κεντρικό σημείο. Η αρχιτεκτονική προσφέρει μεγάλα οφέλη για τους διαχειριστές, συμπεριλαμβανομένης της εύκολης και γρήγορης πρόσβασης στα συστήματα καθώς και την καλύτερης δικτύωσης και φυσικής ασφάλειας. Το κύριο μειονέκτημα αυτού του

τύπου δικτύων είναι το γεγονός ότι ο κεντρικός διακομιστής πολύ πιθανόν να αποτύχει να ανταπεξέλθει σε μεγάλο και απρόσμενο φόρτο εργασίας.

2.3.2 Κατανεμημένα συστήματα

Τα κατανεμημένα συστήματα είναι εκείνα τα συστήματα όπου μεμονωμένοι υπολογιστές λειτουργούν ως «διακομιστής» ή ως «μεσάζων» όταν δύο ή περισσότερα άτομα θέλουν να επικοινωνήσουν. Δεν υπάρχει ένα συγκεκριμένο τμήμα του συστήματος που συνδέει τα άλλα μέλη και λειτουργεί ως συντονιστής. Οι αποφάσεις στα κατανεμημένα συστήματα λαμβάνονται με την ανταλλαγή γνώσεων στους κόμβους του δικτύου και η συλλογική απόφαση βασίζεται στην πλήρη κατανόηση του συστήματος. Αυτό εξαρτάται από τη συνολική λειτουργία του συστήματος.

Αντίθετα, η έλλειψη κεντρικού σημείου λήψης όπως τα κεντροποιημένα συστήματα σημαίνει ότι τα κατανεμημένα συστήματα λαμβάνουν πιο αξιόπιστες και αποτελεσματικές αποφάσεις στο δίκτυο. Κάθε κόμβος συνεισφέρει στο δίκτυο και όλοι συνεργάζονται για να δημιουργήσουν τη συνολική δομή του συστήματος. Αυτό διασφαλίζει ότι όλες οι αποφάσεις και οι συμπεριφορές λαμβάνονται υπόψη προκειμένου να δημιουργηθεί ένα συνεκτικό σύστημα.

2.3.3 Αποκεντρωμένα συστήματα

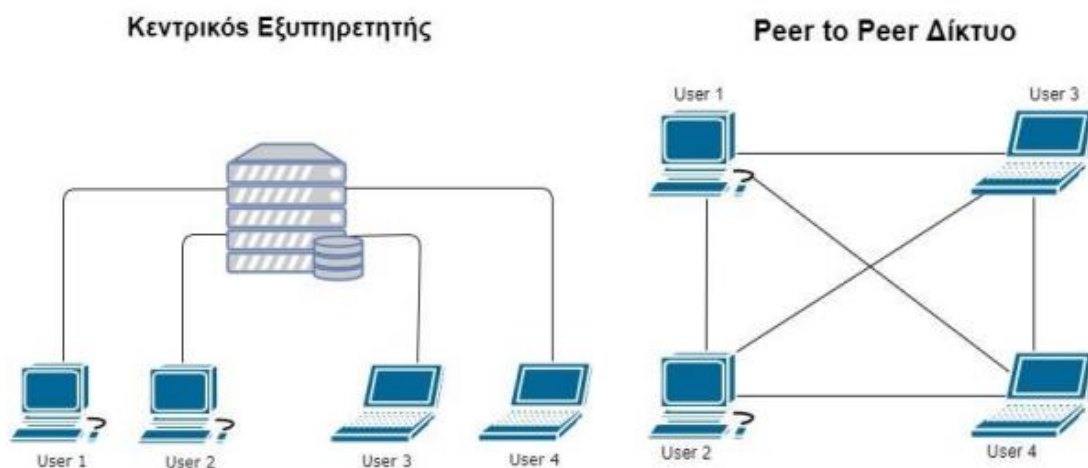
Τα αποκεντρωμένα συστήματα είναι παρόμοια με τα κατανεμημένα συστήματα, με τη διαφορά ότι ο έλεγχος εκτελείται από διαφορετικά στοιχεία και επιπλέον η εμπιστοσύνη δεν είναι διάχυτη. Στα αποκεντρωμένα συστήματα, η συμπεριφορά του συστήματος καθορίζεται από τις αποφάσεις των κόμβων. Κάθε κόμβος παίρνει τη δική του ανεξάρτητη απόφαση, επομένως δεν βασίζεται σε μια συγκεκριμένη οντότητα για την αποστολή αιτημάτων και τη λήψη απαντήσεων. Οι κόμβοι δεν εξαρτώνται ο ένας από τον άλλον, επομένως ο καθένας έχει το δικό του ρολόι. Υπάρχουν περισσότερες από μία κεντρικές μονάδες σε αυτό το σύστημα και οι κάθε κεντρική μονάδα ακούει συνεχώς τις συνδέσεις από άλλους κόμβους. Έτσι κάθε κόμβος παίρνει τις δικές του αποφάσεις, οπότε όταν ένας κόμβος αποτυγχάνει δεν προκαλεί πρόβλημα στο υπόλοιπο δίκτυο. Στην *εικόνα 2.1* που είδαμε νωρίτερα βλέπουμε ένα δείγμα αυτού του δικτύου.

Τα αποκεντρωμένα συστήματα είναι πιο ανθεκτικά στη συμφόρηση του δικτύου, επειδή το φορτίο κατανέμεται στους κόμβους του δικτύου. Το δίκτυο είναι πάντα διαθέσιμο, διασφαλίζοντας ότι οι χρήστες παραμένουν πάντα συνδεδεμένοι. Κάθε κόμβος στο δίκτυο έχει τη δική του μοναδική συμπεριφορά που επιτρέπει την αυτονομία και τον έλεγχο των πόρων. Υπάρχουν ορισμένα μειονεκτήματα στα αποκεντρωμένα συστήματα, όπως η δυσκολία στην επίτευξη μεγάλων έργων λόγω της αυτονομίας των κόμβων, καθώς και η έλλειψη ιεραρχίας και

διαχείρισης, μπορεί να οδηγήσει σε προβλήματα. Επιπλέον είναι σχετικά δύσκολο να εφαρμοστούν σε μικρά συστήματα λόγω του υψηλού κόστους και της αποτελεσματικότητάς τους.

2.4 Πλεονεκτήματα του Blockchain

Το πλεονέκτημα της χρήσης ενός Blockchain δικτύου είναι ότι για την αποθήκευση και την επιβεβαίωση της ορθότητας της κάθε συναλλαγής δεν χρειάζεται κάποιος ενδιάμεσος ή κάποια κεντρική αρχή για την επαλήθευση των συναλλαγών, κάτι το οποίο κάνει το δίκτυο πιο ασφαλές από κακόβουλες επιθέσεις.



Εικόνα 2.2: i) Η δομή ενός Κεντρικού Εξυπηρετητή ii) Η δομή ενός P2P δικτύου.

Αφού η αποκέντρωση έχει ένα προφανές πλεονέκτημα με τα δίκτυα να γίνονται πιο ανθεκτικά έναντι στις επιθέσεις, καθώς δεν υπάρχει κεντρικό κόμβος ως κέντρο βάρους. Αφού από όσους περισσότερους κόμβους-επαληθευτές αποτελείται ένα δίκτυο τόσο πιο ισχυρό γίνεται καταφέρνοντας να λύσει ένα από τα βασικά προβλήματα της κρυπτογραφίας την **ακεραιότητα** (Integrity). Επιπλέον, η διατήρηση του αντιγράφου όλων των κόμβων οδηγεί επίσης σε μόνιμη διαθεσιμότητα των δεδομένων καταφαίρνοντας να λύσει και το πρόβλημα της **διαθεσιμότητας** (Availability) αφού το δίκτυο θα είναι συνεχώς διαθέσιμο.

Η δομή blockchain προσφέρει πρόσθετα οφέλη στην αναζήτηση και τον έλεγχο πληροφοριών, καθώς το σχέδιο των μπλοκ και η ανοιχτή δομή τους επιτρέπουν την μη αναγνωρισμένη ταυτοποίηση των συνεπειών όλων των επιβεβαιωμένων συναλλαγών και όταν είναι απαραίτητο, να τα μεταδώσει από τους χρήστες. Αυτή η προσέγγιση φυσικά, παρέχει διαφάνεια για τα δεδομένα και τις συναλλαγές του δικτύου με την προϋπόθεση ότι γίνεται χρήση

κάποιου δημοσίου και ανοιχτού Blockchain όπως θα αναλύσουμε στο Κεφάλαιο 3 για την διάκριση των Blockchain. Φυσικά όπως σε όλα τα πράγματα υπάρχουν και οι δυο πλευρές του νομίσματος έτσι και το Blockchain έχει τις δίκες του προκλήσεις που θα αναλύσουμε στην επόμενη ενότητα.

2.5 Προκλήσεις του Blockchain

Ένα από τα κύρια μειονεκτήματα στην χρήση blockchain είναι η μεγάλη ηλεκτρική και υπολογιστή ισχύ που απαιτείται για να δημιουργηθεί ένα τέτοιο δίκτυο. Στην πλειονότητα των δικτύων η κατανάλωση ενέργειας είναι μεγάλη, αφού το κύριο πρόβλημα οφείλεται στον αλγόριθμο συναινέσεις που χρησιμοποιείται για την επαλήθευση του δικτύου. Ωστόσο η εξέλιξη των δικτύων Blockchain οδήγησε στην δημιουργία νέων αλγορίθμων συναίνεσης οι οποίοι απαιτούν πολύ χαμηλότερη κατανάλωση ενέργειας σε σχέση με τον αλγόριθμο Proof-of-Work που θα αναλύσουμε στο επόμενο κεφάλαιο.

Επίσης μια σημαντική πρόκληση που έχουν να αντιμετωπίσουν τα δίκτυα αυτά είναι ασφάλεια αφού λόγω του ανοικτού χαρακτήρα τους, ο πηγαίος κώδικας του δικτύου είναι διαθέσιμος στο καθένα να τον διαβάσει και αυτό το κάνει πιο ευάλωτο σε απειλές αφού κάποιος κακόβουλος χρήστης μπορεί να εντοπίσει μια ευπάθεια στην κρυπτογραφία και να το εκμεταλλευτεί προς όφελος του.

2.6 Το Πρόβλημα των Βυζαντινών Στρατηγών

Το πρόβλημα των Βυζαντινών Στρατηγών είναι ένα πρόβλημα συναίνεσης το οποίο εξετάζει την αξιοπιστία των συμμετεχόντων στο δίκτυο. Το σκεπτικό του περιγράφει μια ομάδα στρατηγών με αντίστοιχα στρατιωτικά τμήματα που περιβάλλουν μια εχθρική χώρα, οι οποίοι προσπαθούν να συμφωνήσουν σε μια στρατηγική μέσω των αγγελιοφόρων, αλλά επηρεάζονται εν μέρει από εγωιστικά κίνητρα. Αυτό υποδηλώνει ότι το σημείο καμπής είναι όταν ο αριθμός των στρατηγών που προωθούν εγωιστικά κίνητρα υπερτερεί σημαντικά του αριθμού των στρατηγών που προωθούν το κοινό καλό.

Επειδή ο χρόνος είναι λίγος, οι αγγελιοφόροι πρέπει να διασχίσουν κρυφά την πόλη για να μεταφέρουν τις πληροφορίες στους άλλους στρατηγούς. Σε αυτό το σημείο, προκύπτουν δύο πιθανά προβλήματα. Σε περίπτωση σύλληψης των ταχυμεταφορών κατά την αποστολή τους, η πόλη θα ειδοποιηθεί αμέσως και εγγράφως εάν παραληφθεί ένας ταχυμεταφοράς. Εάν επιτευχθεί μια τέτοια αναλογία, τότε υπάρχει λύση στο πρόβλημα και επομένως, είναι δυνατή η κατάληξη σε

συναίνεση για μια απόφαση. Το Blockchain είναι ένα κατανεμημένο δίκτυο, επομένως δεν υπάρχει κεντρικός υπεύθυνος λήψης αποφάσεων. Η προϋπόθεση είναι ότι τουλάχιστον τα δύο τρίτα των κόμβων δεν είναι ελαττωματικά.

3

Η Αρχιτεκτονική του Blockchain

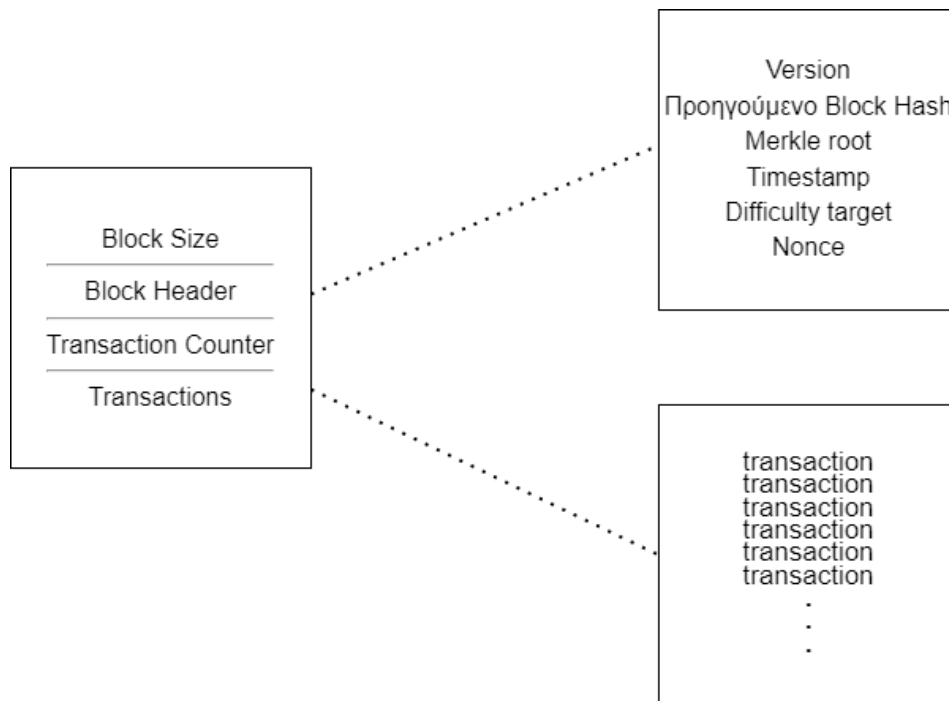
3.1 Αλγόριθμος Συναίνεσης Proof of Work

Ο μηχανισμός Απόδειξη Εργασία Proof-of-Work που εισήγαγε ο Nakamoto βασίζονταν σε ένα παλιότερο αλγόριθμο του Hashcash και χρησιμοποιούταν για τον περιορισμό ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Έτσι ο Satoshi χρησιμοποίησε το αλγόριθμο απόδειξης εργασίας με σκοπό το δίκτυο του Bitcoin να συμφωνεί ομόφωνα στις αποφάσεις και να προστατεύει τα δεδομένα από επιθέσεις. Ο αλγόριθμος βασίζονταν στις πρωτοποριακές ιδέες και σε μεταγενέστερες προσεγγίσεις που είχαν προταθεί ως τότε.

Ένας miner δημιουργεί το επόμενο δυνατό block στην αλυσίδα προσπαθώντας να είναι ο πρώτος που θα βρει και θα δώσει τη λύση σε έναν δύσκολο και απαιτητικό υπολογισμό. Ο μόνος τρόπος για να λύσουμε αυτό το πρόβλημα είναι οι επαναλαμβανόμενες δοκιμές του αλγόριθμου. Οι κομβοί λαμβάνουν το πλαίσιο της κεφαλή του επόμενου block με τις κατακερματισμένες τιμές και της τιμής nonce. Η δυσκολία του προβλήματος συνεχώς αυξάνεται καθώς όλο και περισσότεροι miners χρησιμοποιούν ισχυρότερους υπολογιστές για την διαδικασία της επίλυσης του.

3.2 Δομή ενός Μπλοκ

Η αλυσίδα μπλοκ είναι ένα αποθεματικό όλων των πρόσφατων συναλλαγών. Επομένως, ένα μπλοκ είναι μια μόνιμη εγγραφή δεδομένων που δεν μπορεί να τροποποιηθεί ή να αφαιρεθεί μόλις γραφτεί. Αλλά οι διαφορετικές Blockchain προσφέρουν μια ποικιλία διαφορετικών χαρακτηριστικών, καθιστώντας τους την τέλεια επιλογή για διαφορετικές συναλλαγές. Τα μπλοκ όμως διαφέρουν από σε κάθε Blockchain και εκτός από τις συναλλαγές περιέχουν κι, άλλα δεδομένα όπως θα αναλύσουμε παρακάτω.



Εικόνα 3.1: Η δομή ενός μπλοκ της αλυσίδας.

Κάθε μπλοκ αποτελείται από 4 κατηγορίες δεδομένων.

- Η πρώτη αφορά **Block Size**: Είναι το μέγεθος του παρόν μπλοκ σε bytes που διαθέτει η κεφαλίδα.
- Η δεύτερη κατηγορία είναι το **Block Header** δηλαδή η κεφαλίδα η οποία αποτελείται από τα παρακάτω μεταδομένα:

Version: Είναι η έκδοση του παρόν μπλοκ που κατασκευάζεται.

Previous Block Hash: Είναι το Hash του προηγούμενου μπλοκ.

Merkle root: Είναι μια τιμή hash η οποία δημιουργείται από όλες τις συναλλαγές που περιλαμβάνονται σε αυτό το μπλοκ.

Timestamp: Είναι η χρονοσφραγίδα και δείχνει το χρόνο που δημιουργήθηκε το μπλοκ.

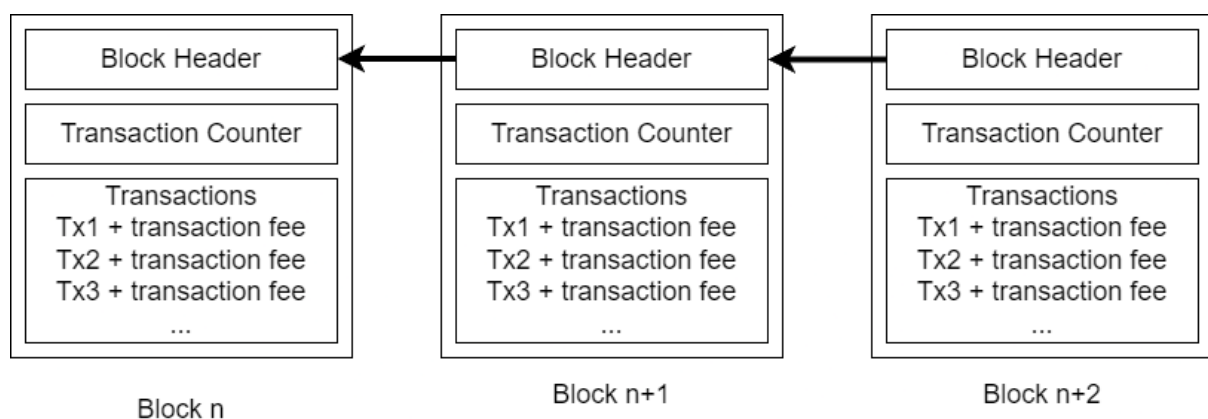
Difficulty target: Είναι η δυσκολία που χρειάζεται για να επικυρωθεί αυτό το μπλοκ.

Nonce: Είναι ένας τυχαίος αριθμός ο οποίος χρησιμοποιείται από τον αλγόριθμο Proof-of-Work που θα αναλυθεί στο επόμενο κεφάλαιο της κρυπτογραφίας.

- Η τρίτη αφορά **Transaction Counter** το οποίο δείχνει τον συνολικό αριθμό των συναλλαγών στο μπλοκ.
- Ενώ η τελευταία αφορά όλες τις συναλλαγές (**Transactions**) του μπλοκ. Μία συναλλαγή (transaction) είναι στην ουσία, ένα μήνυμα που περιέχει το δημόσιο κλειδί του παραλήπτη, το επισυναπτόμενο ποσό που μεταφέρεται και είναι υπογεγραμμένο από το ιδιωτικό κλειδί του αποστολέα.

3.3 Αλυσίδα μπλοκ

Ο όρος αλυσίδα αναφέρεται στον τρόπο που θεωρητικά είναι συνδεδεμένα μεταξύ τους τα block του δικτύου, εφόσον το ένα συνδέεται με το αμέσως προηγούμενο-επόμενο μέσω των μετα-δεδομένων είναι σαν να αποτελούν μια αλυσίδα, όπου οι κρίκοι συνδέονται μεταξύ τους. Ο τρόπος που τα block συνδέονται μεταξύ τους αφορά τα δεδομένα που παρουσιάζονται στην κεφαλή του καθενός. Ειδικότερα στην κεφαλή υπάρχει το parent block hash που συνδέει το παρόν block n με το αμέσως προηγούμενο block $n-1$. Αυτή η τιμή προκύπτει μέσω της διαδικασίας κατακερματισμού σε συγκεκριμένα δεδομένα της κεφαλής και με τη χρήση των κρυπτογραφικών αλγορίθμων που προαναφέρθηκαν για την προστασία δεδομένων του δικτύου.



Εικόνα 3.2: Η σύνδεση νέων μπλοκ με προηγούμενα μπλοκ συναλλαγών.

3.4 Forks

Η διαδικασία πραγματοποίησης αλλαγών και ενημερώσεων στο Blockchain δεν είναι μια τόσο εύκολη διαδικασία. Η συγκεκριμένη διαδικασία στον κόσμο του Blockchain ονομάζεται forking. Το επίπεδο δυσκολίας διαφέρει. Καθώς τα forks που μπορούν να εκτελεστούν είναι δύο ειδών, τα soft forks και τα hard forks ανάλογα με το είδος της αλλαγής που πρόκειται να φέρουν στο δίκτυο. Τα forks πραγματοποιούνται για την διόρθωση σφαλμάτων, την προσθήκη νέων χαρακτηριστικών στο σύστημα ή ακόμη για την γρήγορη διακοπή κυβερνοεπιθέσεων που πραγματοποιούνται.

Τα **Soft Forks** είναι μια διαδικασία που παρέχει αλλαγές στην εφαρμογή που είναι συμβατή με προηγούμενες εκδόσεις της εφαρμογής (backwards compatible). Συνήθως πρόκειται για κάτι απλό και είναι συνήθως να διαρθρώνει ένα σφάλμα στο δικτυό. Μετά τη διαδικασία, εάν κάποιος κόμβος δεν έχουν πραγματοποιήσει την αναβάθμιση, θα μπορούν να επικοινωνούν με το δίκτυο και να πραγματοποιούν συναλλαγές με τους ενημερωμένους κόμβους. Στην περίπτωση που ένα μικρό ποσοστό των κόμβων έχουν πραγματοποιήσει την αναβάθμιση, το δίκτυο δεν θα λειτουργεί με τους νέους κανόνες αλλά με τους παλιούς που υπερισχύουν στο δίκτυο αφού δεν τηρείται από την πλειοψηφία του δικτύου.

Ενώ τα **Hard Forks** πρόκειται για μια τελείως διαφορετική διαδικασία. Αρχικά η ενημέρωση συνήθως δεν είναι συμβατή με προγενέστερες εκδόσεις της εφαρμογής (non-backwards compatible). Το hard fork προγραμματίζεται τότε πρόκειται να συμβεί, είτε μία συγκεκριμένη χρονική στιγμή ή πιο συχνά μετά τη δημιουργία ενός προκαθορισμένου block. Έπειτα από αυτή την αλλαγή στο Blockchain έρχονται ριζικές αλλαγές στο τρόπο λειτουργίας του δικτύου και προκαλείται διάσπαση της αλυσίδας που υπήρχε έως εκείνη τη χρονική στιγμή. Στη συνέχεια δημιουργείται ακόμη μια καινούρια αλυσίδα από την οποία θα συνεχιστεί η λειτουργία του δικτύου. Επίσης να σημειωθεί ότι η παλιά αλυσίδα θα συνεχίσει να υφίσταται, αλλά πλέον στην παλαιά αλυσίδα δεν επιτρέπεται η πραγματοποίηση επιπλέον αλλαγών. Υπάρχει το περιθώριο ελευθερίας και όποιος δεν πραγματοποιήσει την ενημέρωση θα μπορεί, εάν θέλει, να συνεχίσει τη συμμετοχή του στην παλαιά αλυσίδα. Στην παλαιά αλυσίδα οι αλλαγές θα γίνονται αποδεκτές μόνο από κόμβους που τρέχουν την παλιά έκδοση.

Για παράδειγμα ένα hard fork αποτελεί το συμβάν του 2016, όταν στο δίκτυο του Ethereum δημιουργήθηκε ένα προβληματικό έξυπνο συμβόλαιο με όνομα DAO (Decentralized Autonomous Organization) στο οποίο είχαν επενδυθεί περίπου \$150 εκατομμύρια. Λόγω κενών ασφάλειας που

υπήρχαν στη λειτουργία των έξυπνων συμβολαίων, μια ομάδα κατάφερε και εξόρυξε από το δίκτυο περίπου 50 εκατομμύρια Αμερικανικά δολάρια αξίας σε Ether. Για την καταπολέμηση αυτής της επίθεσης προτάθηκε να πραγματοποιηθεί ένα Hard Fork και να σπάσει η αλυσίδα. Η καινούρια αλυσίδα συνέχισε κανονικά τη λειτουργία του Ethereum, ενώ διατηρήθηκε και η παλιά, η οποία έλαβε το όνομα Ethereum Classic. Υστέρα από αυτήν την αλλαγή, στην καινούρια αλυσίδα δεν υπήρχε το κενό ασφαλείας και τα χρήματα κατάφεραν να επιστρέφουν στους αρχικούς κατόχους, χάρις στην βοήθεια των δημιουργών του Ethereum.

3.5 Κατηγοριοποίηση Blockchain

3.5.1 Public

Τα Public Blockchain δίκτυα είναι ένας τύπος blockchain που επιτρέπεται να συμμετέχει στο δίκτυο από τον οποιονδήποτε, είτε ως χρήστη, είτε ως developer ή να δημιουργήσει ένα κόμβο του δικτύου. Οι συναλλαγές που γίνονται μεταξύ των χρηστών αποτελούν δημοσιά δεδομένα και γίνονται με διαφάνεια, με σαφήνεια και μπορεί ο καθένας να ελέγξει ως προς το περιεχόμενο και την εγκυρότητα των δεδομένων που ανταλλάζουν. Παράδειγμα τέτοιων blockchain είναι το Bitcoin και το Ethereum είναι τα μεγαλύτερα σε όγκο συναλλαγών καθημερινά. Αξίζει να σημειωθεί ότι οι δημόσιες αλυσίδες blockchain τείνουν να είναι πιο ασφαλής σε σχέση με του άλλους δυο τύπους blockchain που θα αναλυθούν στην συνέχεια, επειδή δεν υπάρχει κάποιος οργανισμός να ελέγχει το δίκτυο και η συμμετοχή είναι ανώνυμη.

Βασικό χαρακτηριστικό της συμμετοχής των miners στη διαδικασία συνάθροισης των συναλλαγών σε block, στον μηχανισμό συναίνεσης στα public blockchains, είναι η παροχή κινήτρου που συνήθως είναι το οικονομικό όφελος που λαμβάνουν έναν προκαθορισμένο αριθμό κρυπτονομισμάτων μαζί με την είσπραξη των τελών επί των συναλλαγών που εγκρίθηκαν, για τις υπηρεσίες επαλήθευσης των μπλοκ που προφέραν στο δίκτυο.

Φυσικά πρέπει να αναγνωρίσουμε ότι στα μειονεκτήματα των δημόσιων Blockchains καθίσταται φανερό ότι απαιτείται σημαντικό ποσό υπολογιστικής ισχύος για να επιτευχθεί ο συγχρονισμός και η διατήρηση του κατανεμημένων μπλοκ που χρειάζεται για να συνεχιστεί η αλυσίδα. Επίσης το δημόσιο Blockchain είναι συχνά πιο αργό από τους υπόλοιπους τύπους Blockchain και με τη συνεχόμενη αύξηση των συναλλαγών να αντιμετωπίζουν προβλήματα στον τρόπο διατήρησης της αλυσίδας και στον αποθηκευτικό χώρο συνεχώς η αλυσίδα γίνεται όλο και μεγαλύτερη αφού ολοένα και περισσότερα blocks προθέτονται.

3.5.2 Permissioned

Ένα Permissioned Blockchain διατηρεί και αυτό καταναμεμένα τα δεδομένα των μπλοκ, όμως η συμμετοχή σε αυτό ελέγχεται από μια κεντρική αρχή. Η κεντρική αυτή αρχή γνωρίζει τους συμμετέχοντες και δίνει το δικαίωμα επικύρωσης των συναλλαγών σε άτομα που εμπιστεύεται. Αυτό το χαρακτηριστικό διευκολύνει την αύξηση του όγκου των συναλλαγών που πραγματοποιούνται ημερησίως και ταυτόχρονα τα εξουσιοδοτημένα δίκτυα μπορούν να είναι πολύ γρήγορα με μεγαλύτερη αποθηκευτική χωρητικότητα. Επίσης ο βασικός κώδικας του κάθε Permissioned Blockchain συχνά εκδίδεται ανοιχτά προς όλους για να τον επιθεωρήσουν αλλά όχι απαραίτητα πάντα.

3.5.3 Private

Τα ιδιωτικά δίκτυα blockchain είναι διαφορετικά από τα δημόσια δίκτυα blockchain ως προς την πρόσβαση των χρηστών, αφού το ιδιωτικό blockchain (private blockchain), συνήθως η κατασκευαστές θέτουν ένα διαχειριστή για το δίκτυο ή ένα αυστηρό πρωτόκολλο κανόνων για την παροχή αυθεντικοποίησης και επικύρωσης, αφού γίνεται πρόσκληση συμμετοχής σε υποψήφιους κόμβους. Με άλλα λόγια, το blockchain καθίσταται ελεγχόμενο ως προς το ποιοι μπορούν να συμμετέχουν και να αναγνώσουν τη βάση δεδομένων. Με αποτέλεσμα να είναι συνήθως κεντριοποιημένο δίκτυο, τοποθετημένο σε ιδιωτικούς διακομιστές, το οποίο φυσικά επιλύει το πρόβλημα της ιδιωτικότητας. Σε αυτόν τον τύπο blockchain μόνο οι οντότητες που συμμετέχουν στη συναλλαγή έχουν γνώση σχετικά με τη συναλλαγή που εκτελείται, ενώ άλλοι δεν θα έχουν πρόσβαση σε αυτήν, δηλαδή οι συναλλαγές είναι ιδιωτικές.

3.6 Επιθέσεις και απειλές

Ένας από τους σημαντικότερους κινδύνους που αντιμετωπίζουν τα Blockchain με τον αλγόριθμο Proof-of-Work είναι οι επιθέσεις 51% αφού μπορούν να προκληθούν επιθέσεις κατά της ακαιραιότητας του δικτύου. Λόγω τη φύσης της τεχνολογίας του Blockchain που έχει την βάση της στην δημοκρατική και αποκεντρωμένη διακυβέρνηση, δηλαδή οι αποφάσεις παίρνονται από την πλειοψηφία, αν το μεγαλύτερο ποσοστό χρηστών οδηγηθεί από την αυθεντική αλυσίδα σε κάποια άλλη η οποία περιέχει διαφορετικές συναλλαγές, τότε οι συναλλαγές της πρώτης αλυσίδας

θα αναιρεθούν και οι χρηματικές ποσότητες που διακινήθηκαν θα επιστραφούν στους αρχικούς κατόχους. Για να πετύχει τον σκοπό του η κακόβουλη πλευρά μπορεί είτε να αγοράσει εξοπλισμό ο οποίος θα έχει μεγαλύτερη επεξεργαστική ισχύ από το 51% του υπόλοιπου δικτύου υπολογιστών, είτε να βρει κάποια ευπάθεια στο πρωτόκολλο δημιουργίας των block και να επιταχύνει την προσθήκη στην δική του προσωπική αλυσίδα. Όταν η δική του αλυσίδα θα είναι μεγαλύτερη από την αυθεντική αλυσίδα τότε θα μεταδώσει τις αλλαγές στο δίκτυο προσπαθώντας να τις εδραιώσει.

Για κάθε συναλλαγή θα πρέπει να πληρωθεί ένα μικρό τέλος στο δίκτυο (fees). Αυτό προστατεύει το δίκτυο από αχρείαστες συναλλαγές που απαιτούν κάποιο κόστος υπολογισμού καθώς αποτρέπει τις κακόβουλες επιθέσεις, όπως τις επιθέσεις άρνησης υπηρεσίας (DDoS) από την υπερβολική κίνηση του δικτύου. Η πληρωμή αυτών των τελών συμπεριλαμβάνεται μαζί με την επιβράβευση της εξόρυξης του μπλοκ για τον υπολογισμό και την μνήμη που έχει χρησιμοποιήθηκε για την πραγματοποίηση των συναλλαγών. Το τέλος αυτό πληρώνεται στο εκάστοτε νόμισμα του δικτύου.

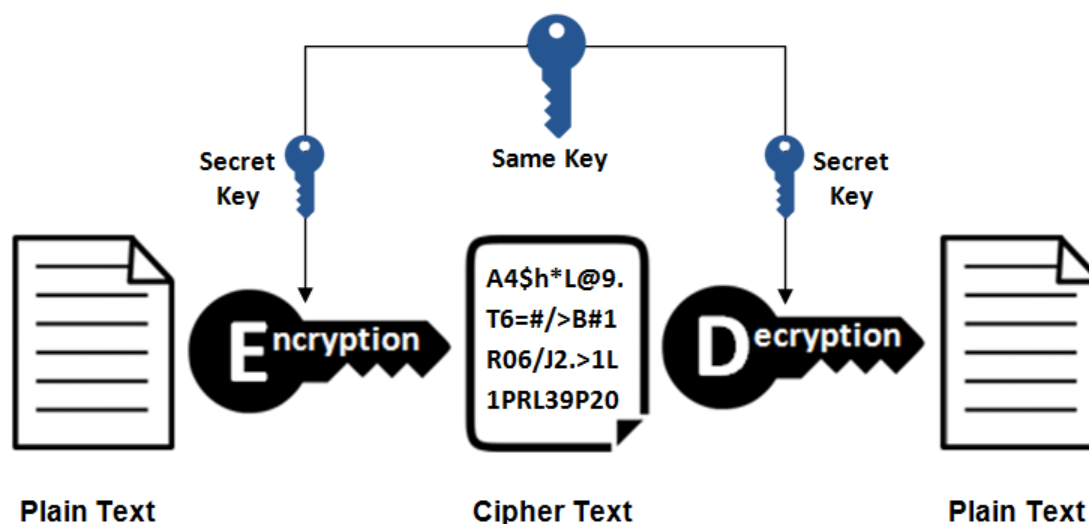
Επίσης θα πρέπει να υπολογίζουμε πάντα ότι ανα πασά στιγμή με την χρήση κάποιου κενού ασφάλειας στον αλγόριθμο Proof-of-Work μπορεί να γίνει το σπάσιμο της κρυπτογραφίας αφού είναι δυνατό η κρυπτογραφία που χρησιμοποιεί το blockchain να σπάσει με την χρήση κβαντικών αλγορίθμων και της αντίστροφής μηχανικής για να βρεθεί το ιδιωτικό κλειδί του στόχου.

Κρυπτογραφία

Η κρυπτογραφία των δεδομένων δημιουργήθηκε ώστε να μην έχουν πρόσβαση μη εξουσιοδοτημένα άτομα. Η κρυπτογράφηση στην ουσία μετασχηματίζει τα δεδομένα σε κείμενο cyphertext δηλαδή ένα κρυπτογραφημένο κείμενο το οποίο είναι αδύνατο να αποκρυπτογραφηθεί από τη στιγμή που δεν υπάρχει γνώση για το είδος της κρυπτογράφησης. Η διαδικασία της αποκρυπτογράφησης είναι ο μετασχηματισμός του κρυπτογραφημένου κειμένου στο αρχικό κείμενο. Με την χρήση της κρυπτογραφίας επιτυγχάνουμε την ταυτοποίηση ότι ένας άνθρωπος είναι όντως αυτός που λέει, και μέσω της πιστοποίησης (authentication), δηλαδή η απόδειξη ότι είναι πράγματι αυτός που ισχυρίζεται ότι είναι, έχει την δυνατότητα πρόσβασης σε συγκεκριμένους πόρους εφόσον πρώτα έχει πιστοποιηθεί.

4.1 Συμμετρική κρυπτογραφία

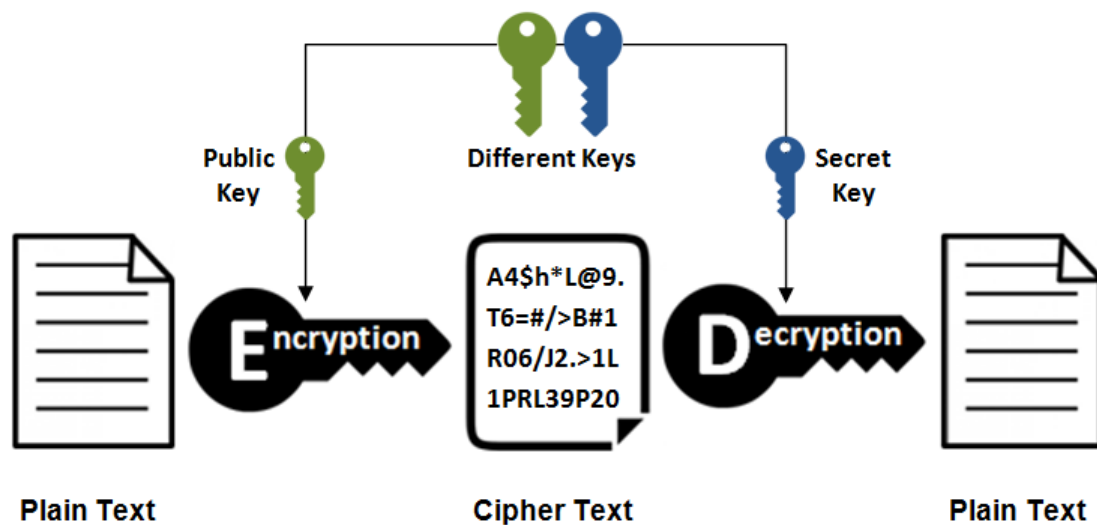
Η συμμετρική κρυπτογραφία είναι μια λιγότερη διαδεδομένη μορφή κρυπτογραφίας και χρησιμοποιεί ένα κλειδί που είναι σημαντικό για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση των δεδομένων. Ο λόγος που δεν χρησιμοποιείται πλέον συχνά είναι λόγω προβλημάτων που δημιουργούνται στη διαχείριση των κλειδιών και την αδυναμία ανάλυσης του κλειδιού με κάποιο ασφαλές τρόπο.



Εικόνα 4.1: Συμμετρική Κρυπτογραφία.

4.2 Ασύμμετρη κρυπτογραφία

Η τεχνολογία του Blockchain χρησιμοποιεί κρυπτογραφία ασύμμετρου κλειδιού. Η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιεί ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί που σχετίζονται κρυπτογραφικά μεταξύ τους. Το δημόσιο κλειδί δημοσιοποιείται χωρίς να δημιουργεί προβλήματα ασφαλείας στην διαδικασία, αλλά το ιδιωτικό κλειδί πρέπει να παραμείνει μυστικό εάν τα δεδομένα πρόκειται να διατηρηθούν ασφαλείς. Παρόλο που υπάρχει σχέση μεταξύ των δύο κλειδιών, το ιδιωτικό κλειδί δεν μπορεί να προσδιοριστεί αποτελεσματικά με βάση τη γνώση του δημόσιου κλειδιού. Για παράδειγμα μπορεί κάποιος να κρυπτογραφήσει με το ιδιωτικό κλειδί και στη συνέχεια αποκρυπτογραφήσει με το δημόσιο κλειδί.



Εικόνα 4.2: Ασύμμετρη κρυπτογραφία.

Η κρυπτογραφία ασύμμετρου κλειδιού επιτρέπει μια σχέση εμπιστοσύνης μεταξύ χρηστών που δεν γνωρίζουν, και δεν χρειάζεται να εμπιστευθεί ο ένας τον άλλον, παρέχοντας έναν μηχανισμό επαλήθευσης της ακεραιότητας και της γνησιότητας των συναλλαγών ενώ ταυτόχρονα επιτρέπει στις συναλλαγές να παραμένουν δημόσιες. Για να γίνει αυτό, οι συναλλαγές χρειάζεται να είναι «ψηφιακά υπογεγραμμένες». Αυτό σημαίνει ότι ένα ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση μιας συναλλαγής έτσι ώστε οποιοσδήποτε έχει το δημόσιο κλειδί να μπορεί να το αποκρυπτογραφήσει. δεδομένου ότι το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο, η κρυπτογράφηση της συναλλαγής με το ιδιωτικό κλειδί αποδεικνύει ότι ο υπογράφων της συναλλαγής έχει πρόσβαση στο ιδιωτικό κλειδί.

Εναλλακτικά, μπορεί κανείς να κρυπτογραφήσει δεδομένα με το δημόσιο κλειδί ενός χρήστη έτσι ώστε μόνο οι χρήστες που έχουν το ιδιωτικό κλειδί να μπορούν να το αποκρυπτογραφήσουν. Ένα μειονέκτημα που έχει το ασύμμετρο κλειδί είναι ότι η κρυπτογραφία είναι συχνά αργή στον υπολογισμό και απαιτεί μεγαλύτερο υπολογιστικό κόστος.

4.3 Κρυπτογραφική Συνάρτηση (Hash)

Η δημιουργία ενός ζεύγους κλειδιών είναι ανάλογη με τη δημιουργία ενός λογαριασμού στο blockchain, καθώς το λογισμικό που δημιουργεί τον λογαριασμό, ουσιαστικά δημιουργεί ένα ιδιωτικό και ένα δημόσιο κλειδί για τον χρήστη, τα οποία συσχετίζονται με τον ανωτέρω μαθηματικό τρόπο. Επίσης, κάθε συναλλαγή που εκτελείται στο blockchain υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί του. Αυτή η ψηφιακή υπογραφή διασφαλίζει ότι μόνο ο κάτοχος του λογαριασμού μπορεί να πραγματοποιήσει συναλλαγές από τον λογαριασμό αυτόν.

4.4 Ψηφιακή Υπογραφή

Η δημιουργία μιας συναλλαγής στο blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο ταυτότητας της συναλλαγής. Μια ψηφιακή υπογραφή είναι στην ουσία η κρυπτογράφηση της σύνοψης του μηνύματος. Μια τυπική ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις: τη φάση υπογραφής και τη φάση επαλήθευσης, ακριβώς όπως συμβαίνει με την ασύμμετρη κρυπτογραφία, τη λειτουργία της οποίας περιγράψαμε παραπάνω.

Η δημιουργία ενός ζεύγους κλειδιών είναι ανάλογη με τη δημιουργία ενός λογαριασμού στο blockchain, καθώς το λογισμικό που δημιουργεί τον λογαριασμό, ουσιαστικά δημιουργεί ένα ιδιωτικό και ένα δημόσιο κλειδί για τον χρήστη, τα οποία συσχετίζονται κρυπτογραφικά. Επίσης, κάθε συναλλαγή που εκτελείται στο blockchain υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί του. Αυτή η υπογραφή διασφαλίζει ότι μόνο ο κάτοχος του λογαριασμού μπορεί να πραγματοποιήσει συναλλαγές από τον λογαριασμό αυτόν.

Πιο συγκεκριμένα, αρχικά υπολογίζεται η σύνοψη του του μηνύματος (checksum) με την συνάρτηση κατακερματισμού. Η σύνοψη κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα και πλέον αποτελεί την ψηφιακή υπογραφή, η οποία επισυνάπτεται στο μήνυμα. Κατά την διαδικασία ελέγχου, η ψηφιακή υπογραφή διαχωρίζεται από το μήνυμα και αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα. Με την αποκρυπτογράφηση να εξάγεται το checksum του μηνύματος ενώ παράλληλα υπολογίζεται και το checksum του ληφθέντος μηνύματος. Αν οι δυο συνόψεις είναι ίδιες συνεπάγεται πως το μήνυμα υπογράφηκε από τον αποστολέα και δεν παραποιήθηκε στη συνέχεια.

4.5 Παραγωγή διευθύνσεων

Τα δίκτυα blockchain χρησιμοποιούν μια διεύθυνση, η οποία είναι μια σύντομη, αλφαριθμητική συμβολοσειρά από χαρακτήρες που προέρχονται από το δημόσιο κλειδί του χρήστη. Χρησιμοποιώντας ένα κρυπτογραφικό κατακερματισμό (Hash Function), μαζί με δεδομένα όπως των αριθμός έκδοσης και το checksum. Τα περισσότερα blockchain στις υλοποιήσεις τους χρησιμοποιούν διευθύνσεις ως τελικά σημεία "προς" και "από" σε μια συναλλαγή. Οι διευθύνσεις είναι μικρότερες από τα δημόσια κλειδιά και δεν είναι μυστικές. Για την δημιουργία μιας νέας διεύθυνσης δημιουργείται από το δημόσιο κλειδί, υστέρτα το δημόσιο κλειδί περνάει από μια κρυπτογραφική συνάρτηση κατακερματισμού (hash function) και το αποτέλεσμα του είναι διεύθυνση που θα χρειαστεί κάποιος για να λάβει ή να στείλει κάτι μέσα στο δίκτυο. Η διαδικασία που ακολουθείτε είναι η παρακάτω:

public key -> cryptographic hash function -> address

4.6 Αποθήκευση ιδιωτικών κλειδιών

Σε ορισμένα δίκτυα blockchain οι χρήστες πρέπει να διαχειρίζονται και να αποθηκεύουν με ασφάλεια τα δικά τους ιδιωτικά κλειδιά. Αντί να τα καταγράφουν χειροκίνητα, αυτοί συχνά χρησιμοποιούν λογισμικό για την ασφαλή αποθήκευσή τους. Αυτό το λογισμικό αναφέρεται συχνά ως πορτοφόλι και υπάρχουν δυο κυρία είδη όπως το hardware wallet που αποτελούνται από μια συσκευή καθώς και τα software wallet που είναι κυρίως λογισμικό που λειτουργεί ή στο browser ή τοπικά στον υπολογιστή ή το κινητό του χρήστη. Το πορτοφόλι μπορεί να αποθηκεύσει ιδιωτικά κλειδιά, δημόσια κλειδιά και τις σχετικές διευθύνσεις με ασφάλεια. Μπορεί επίσης να εκτελέσει και άλλες λειτουργίες, όπως ο υπολογισμός του συνολικού αριθμού ψηφιακών στοιχείων που έχει ο χρήστης στο πορτοφόλι του.

4.7 Ασφάλεια και κίνδυνοι Απώλειας κλειδιών

Εάν ένας χρήστης χάσει το ιδιωτικό του κλειδί, τότε κάθε ψηφιακό στοιχείο που σχετίζεται με αυτό το κλειδί χάνεται, επειδή είναι υπολογιστικά ανέφικτη η ανάκτηση του ίδιου ιδιωτικού κλειδιού. Εάν κλαπεί ένα ιδιωτικό κλειδί, τότε ο εισβολέας θα έχει πλήρη πρόσβαση σε όλα τα ψηφιακά στοιχεία που ελέγχονται από αυτό το ιδιωτικό κλειδί. Η ασφάλεια των ιδιωτικών κλειδιών

είναι τόσο σημαντική που πολλοί χρήστες συνήθως καταφεύγουν στην λύση των hardware wallets, τα οποία είναι πιο ασφαλείς λύση αυτή την στιγμή.

Ethereum & Smart Contracts

5.1 Το δίκτυο του Ethereum

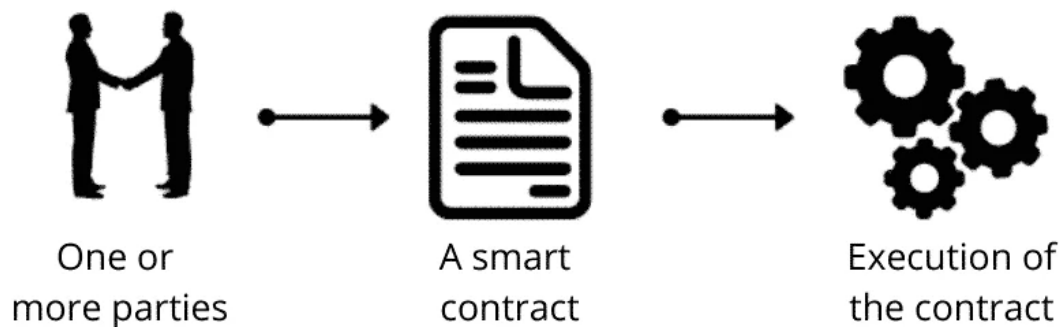
Το Ethereum είναι μια πλατφόρμα ανοιχτού κώδικα, που αναπτύχθηκε έπειτα από μια ομάδα προγραμματισμών το 2014 από τον ιδρυτή του τον Vitalik Buterin, με σκοπό την βελτίωση κάποιων περιορισμών του Bitcoin και άλλων κρυπτονομισμάτων. Το Ethereum χρησιμοποιεί την τεχνολογία του Blockchain για να δημιουργήσει αποκεντρωμένες εφαρμογές, γνωστές και ως “Dapps” (Decentralized Applications). Αυτές οι εφαρμογές επιτρέπουν στους χρήστες να συνάπτουν συμφωνίες και συναλλαγές απευθείας μεταξύ των χρηστών και να αγοράζουν, να πωλούν και να εμπορεύονται αγαθά και υπηρεσίες χωρίς μεσάζοντα. Η κύρια προσθήκη σε σχέση με το Bitcoin είναι η αποκεντρωμένη εικονική μηχανή Ethereum Virtual Machine (EVM), όπου ο καθένας μπορεί να αναπτύξει και να εκτελέσει κώδικα χρησιμοποιώντας τη γλώσσα προγραμματισμού Solidity που αναπτύχθηκε για να υποστηρίξει την τεχνολογία των Smart Contracts.

Οι διευθύνσεις στο Ethereum είναι δυο τύπων. Στην περίπτωση του Bitcoin είχαμε τις διευθύνσεις που χρησιμοποιούσαν ένα ιδιωτικό κλειδί για να εκτελέσουν τις συναλλαγές τους στο Blockchain. Ο άλλος τύπο διευθύνσεων είναι διευθύνσεις συμβολαίων (Contract Address). Οι διευθύνσεις συμβολαίων ελέγχονται από τον κώδικα των έξυπνων συμβολαίων. Ενώ οι συμβατικές διευθύνσεις δεν έχουν κώδικα και απλά παράγουν συναλλαγές, σε αντίθεση με τις διευθύνσεις συμβολαίων, οι οποίες κάθε φορά που λαμβάνουν κάποιο μήνυμα ενεργοποιείται ο κώδικας και έχει τη δυνατότητα να διαβάζει και να γράφει στο χώρο αποθήκευσης, να στέλνει άλλα μηνύματα ή ακόμα και να δημιουργεί άλλα συμβόλαια.

Το Ethereum είναι στην ουσία ένα προγραμματιζόμενο Blockchain και αντί να δίνει στους χρήστες ένα σύνολο προκαθορισμένων λειτουργιών (π.χ. συναλλαγές Bitcoin), το Ethereum επιτρέπει στους χρήστες να δημιουργούν τις δικές τους λειτουργίες οι οποίες ποικίλουν ανάλογα με τις ανάγκες τους. Με τον τρόπο αυτό, χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους αποκεντρωμένων εφαρμογών Blockchain, συμπεριλαμβανομένων, μεταξύ άλλων διάφορες αποκεντρωμένες εφαρμογές όπως εφαρμογές DeFi (Decentralized Finance) καθώς και αυτή που θα αναπτυχθεί στην παρούσα εργασία.

5.2 Τι είναι τα Smart Contracts;

Ο όρος έξυπνα συμβόλαια (Smart Contracts) χρονολογείται από το 1994, ο οποίος ορίστηκε από τον Nick Szabo ως «πρωτόκολλο για ηλεκτρονικές συναλλαγές» που εκτελεί τους όρους μιας σύμβασης. Οι στόχοι των έξυπνων συμβολαίων είναι για την ικανοποίηση συμβάσεων τόσο για τις ηλεκτρονικές πληρωμές όσο και για την εμπιστευτικότητα και την επιβολή των συμβάσεων αυτών. Ωστε να ελαχιστοποιήθουν οι εξαιρέσεις τόσο από κακόβουλες όσο και από εξωτερικούς παράγοντες με σκοπό την μείωση της ανάγκης για έμπιστους μεσάζοντες.



Εικόνα 5.1: Η λειτουργία των Smart Contracts.

Ο κώδικας ενός έξυπνου συμβολαίου μπορεί να αντιπροσωπεύει μια συναλλαγή πολλών μερών, συνήθως στο πλαίσιο μιας διαδικασίας. Το δίκτυο συγκεντρώνει και εκτελεί τα έξυπνα συμβόλαια που θεωρητικά είναι ανεξάρτητα από τυχόν παρεμβολές τρίτων, καθώς είναι ανθεκτικό έναντι παραβιάσεων. Τα έξυπνα συμβόλαια λειτουργούν ακριβώς όπως έχουν προγραμματιστεί, μειώνοντας σημαντικά τον κίνδυνο δυσλειτουργίας και αυτο-εκτελούνται συνεχώς χωρίς κάποια παρεμβολή.

Μία ιδιαιτερότητά των έξυπνων συμβολαίων είναι πως ο κώδικάς τους είναι οριστικός και δεν μπορεί να αλλαχθεί. Από την στιγμή που ενεργοποιηθεί κάποιο συμβόλαιο στο blockchain, τότε δεν υπάρχει τρόπος να αλλάξει η συμπεριφορά του, ούτε να διορθωθεί κάποιο σφάλμα όσο μικρό και αν αυτό διότι, όπως έχει ήδη αναφερθεί, τα περιεχόμενα του blockchain δεν μπορούν να μεταβληθούν. Στην περίπτωση που, κατά την διάρκεια λειτουργίας της εφαρμογής διαπιστωθεί κάποιο κρίσιμο σφάλμα στα συμβόλαια της, ο μόνος τρόπος διόρθωσής του θα ήταν η δημιουργία κάποιου εντελώς νέου συμβολαίου. Αφού είναι εύκολο κάποιος νέος προγραμματιστής στην Solidity (η γλώσσα συγγραφής των συμβολαίων) να υποπέσει σε σφάλματα, διότι η Solidity εκ κατασκευής είναι μια γλώσσα πολύ υψηλού επιπέδου και κάθε γραμμή κώδικα μπορεί να περιέχει πολλές λειτουργίες.

5.3 EVM

Το EVM είναι το κομμάτι του Ethereum που διαχειρίζεται την ανάπτυξη και την εκτέλεση έξυπνων συμβολαίων στο δίκτυο του Ethereum. Ουσιαστικά το EVM είναι ένας παγκόσμιος και αποκεντριοποιημένος υπολογιστής, κατανεμημένος σε όλους τους υπολογιστές που συμμετέχουν στο δίκτυο του Ethereum, ο οποίος περιέχει εκατομμύρια εκτελέσιμα αντικείμενα τα οποία έχουν το καθένα τον δικό του μόνιμο αποθηκευτικό χώρο. Αυτός ο παγκόσμιος υπολογιστής εκτελεί οποιαδήποτε υπολογιστική διεργασία η οποία αλλάζει την κατάσταση ενός δεδομένου εκτός από απλές συναλλαγές μεταξύ λογαριασμών. Το EVM είναι μία σχεδόν Turing πλήρης μηχανή καταστάσεων λόγω ότι υπάρχει περιορισμός των υπολογιστικών βημάτων στις εκτελέσιμες διεργασίες από το ποσό του gas που είναι διαθέσιμο για την εκτέλεση οποιουδήποτε έξυπνου συμβολαίου.

Όπως και τα άλλα blockchain, το Ethereum περιλαμβάνει ένα πρωτόκολλο δικτύου ομότιμων κόμβων. Το πρωτόκολλο αυτό είναι υπεύθυνο για τον συντονισμό των συνδεδεμένων κόμβων, με σκοπό την απρόσκοπτη λειτουργία του δικτύου. Κάθε κόμβος τρέχει το EVM και εκτελεί τις ίδιες εντολές. Η μεγάλη αυτή παραλληλοποίηση των υπολογισμών δεν έχει σκοπό την απόδοση, αφού οι υπολογισμοί είναι πολύ πιο αργοί και ακριβοί απ' ότι θα γινόταν σε έναν απλό υπολογιστή, σκοπό έχει την ύπαρξη ομοφωνίας/συναίνεσης (consensus). Αυτό το χαρακτηριστικό δίνει στο Ethereum πολύ μεγάλη αντοχή σε σφάλματα, αδιάλειπτη λειτουργία και εγγυάται ότι τα δεδομένα μέσα στο blockchain θα μείνουν για πάντα (σχεδόν) αμετάβλητα.

Όπως αναφέρθηκε και πριν, το Ethereum δεν παρέχει στους χρήστες απλά ένα προκαθορισμένο σύνολο λειτουργιών, όπως κάνει το Bitcoin, αλλά αντιθέτως τους παρέχει την δυνατότητα να ορίσουν δικές τους λειτουργίες και κατ' επέκταση έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές DApps, είναι δηλαδή ένα προγραμματιζόμενο blockchain. Το Ethereum είναι κατά μία έννοια μία σουίτα πρωτοκόλλων που καθορίζουν μία πλατφόρμα για την ανάπτυξη και την λειτουργία αποκεντρωμένων εφαρμογών.

5.4 Dapps

Τα DApps (Decentralized Apps) είναι διαδικτυακές εφαρμογές που είναι μερικώς ή τελείως αποκεντριοποιημένες. Τα στοιχεία μίας εφαρμογής που μπορούν να αποκεντριοποιηθούν είναι το backend λογισμικό, το frontend λογισμικό, ο αποθηκευτικός χώρος δεδομένων, η επικοινωνία μηνυμάτων και η Διευθυνσιοδοτηση ονόματος (Decentralized Domains). Στα dapps, η αποκεντριοποίηση του backend γίνεται με την χρήση των έξυπνων συμβολαίων όπου βρίσκεται αποθηκευμένη η λογική της εφαρμογής και οι καταστάσεις της.

Τα DApps ή οι Αποκεντρωμένες Εφαρμογές, είναι μια νέα κατηγορία εφαρμογών blockchain που αλλάζουν τον τρόπο λειτουργίας των επιχειρήσεων. Όπως υποδηλώνει το όνομα, τα DApps είναι αποκεντρωμένα, πράγμα που σημαίνει ότι δεν ελέγχονται από καμία μεμονωμένη αρχή. Ένα DApp χρησιμοποιεί τεχνολογία blockchain και εκτελείται σε δίκτυο peer-to-peer σε αντίθεση με ένα ενιαίο δίκτυο υπολογιστών. Σε ένα δίκτυο peer-to-peer, οι πληροφορίες διανέμονται συνεχώς μεταξύ των συμμετεχόντων αντί να αποθηκεύονται σε έναν κεντρικό διακομιστή. Ενώ ένα μεγάλο δίκτυο υποφέρει από χαμηλότερη ταχύτητα και απόδοση σε σύγκριση με έναν κεντρικό διακομιστή, ένας υψηλότερος αριθμός συμμετεχόντων ενισχύει ένα δίκτυο peer-to-peer.

Οι πιθανές χρήσεις για αυτά τα blockchain DApps είναι ατελείωτες. Μπορούν να λύσουν πολλά ζητήματα του πραγματικού κόσμου σε τομείς όπως ο έλεγχος ταυτότητας, η διαχείριση προμηθειών, η παράδοση φαγητού, οι υπηρεσίες μουσικής και μια ποικιλία άλλων λειτουργιών που θα γίνουν πιο εμφανείς καθώς αναπτύσσεται η τεχνολογία. Όλες αυτές οι βιομηχανίες μπορούν να επωφεληθούν από τα DApps ενισχύοντας την ασφάλεια των εφαρμογών, ενσωματώνοντας τα κρυπτονομίσματα και χωρίς εξωτερική παρέμβαση.

6

Σχεδιασμός του Συστήματος και εργαλεία

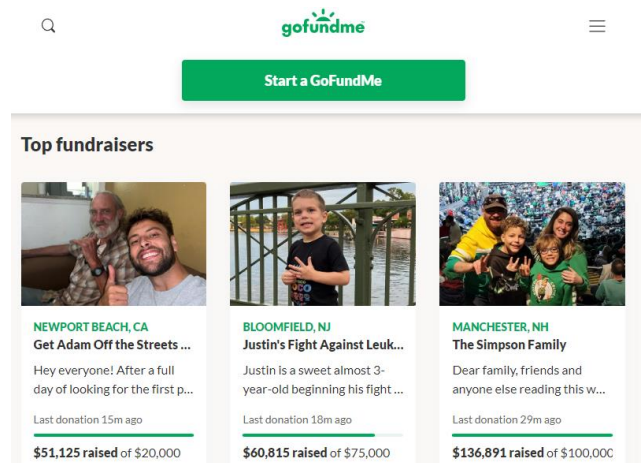
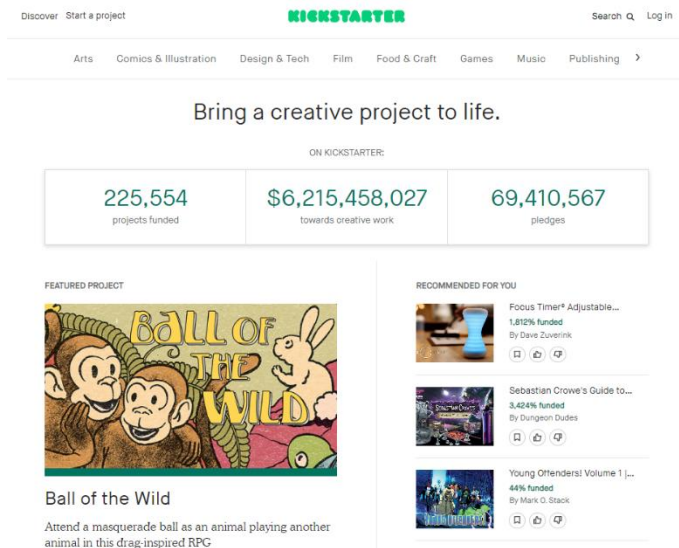
6.1 Υπάρχουσες Προσεγγίσεις Crowdfunding

Με τον όρο Crowdfunding εννοούμε την μέθοδο συγκέντρωση κεφαλαίων μέσω της συλλογικής προσπάθειας φίλων, οικογενειών, πελατών και επενδυτών με κατά κυριο μέσω τα κοινωνικά δίκτυα και διαδικτυακών πλατφορμών, αξιοποιώντας τα δίκτυά τους για μεγαλύτερη έκθεση με απώτερο σκοπό την συλλογή μεγαλύτερων ποσών. Το crowdfunding είναι ουσιαστικά το αντίθετο της γενικής προσέγγισης για τη χρηματοδότηση των επιχειρήσεων.

Παραδοσιακά στην εποχή προ του διαδικτύου, αν κάποια οντότητα ήθελε να συγκεντρώσει κάποια κεφάλαια για να ξεκινήσετε μια επιχείρηση ή ένα νέο προϊόν, θα χρειαζόταν να παρουσιάσει το επιχειρηματικό του σχέδιο και στη συνέχεια να απευθυνθείτε σε ένα περιορισμένο κύκλο επενδυτών για πηγή χρηματοδότησης περιλαμβάνουν εταιρείες επιχειρηματικών κεφαλαίων, τράπεζες κ.λπ. περιορίζοντας σημαντικά τις επιλογές του. Η βασική αρχή πίσω από τον ορισμό του crowdfunding είναι ότι μπορείτε να βοηθήσετε έναν φίλο ή να βοηθήσετε μια ολόκληρη κοινότητα. Θεωρητικά με το Crowdfunding μπορείτε να συγκεντρώσετε κάποια ποσό για τη δική σας επέμβαση μέχρι να εκπληρώσετε το όνειρο ενός μαθητή ώστε να φοιτήσει στο κολλέγιο και πολλά άλλα αφού δεν υπάρχουν περιορισμοί στην θεματολογία.

Με την εξέλιξη του διαδικτύου ο τρόπος χρηματοδότησης έργων άλλαξε με την πάροδο του χρόνου, χαρώ στα μέσα κοινωνικής δικτύωσης δίνοντας την δυνατότητα στους χρηστές να διαδίδουν πιο ευκολά την ιδέα που θέλουν να συγκεντρώσουν κεφάλαια για την ανάπτυξη της. Έτσι δημιουργήθηκαν κεντροποιημένες πλατφόρμες με σκοπό να συγκεντρώνονται χρήματα για τις καμπάνιες των χρηστών. Η απλότητα των βημάτων έκανε την ιδέα του Crowdfunding αρκετά δημοφιλή αφού τα βήματα για την υλοποίηση μια καμπάνιας ήταν αρχικά να δημιουργήσει μια σελίδα για τον έρανο να γράψει μια σχετική ιστορία με κινητήρια δύναμη να προσκαλέσουν άλλους χρήστες να συνεισφέρουν στον έρανο. Υστέρα οι χρήστες έκαναν συνεισφορές και μετά την λήξη της καμπάνιας η πλατφόρμα έστελνε το ποσό στον ιδρυτή της καμπάνιας.

Ένα από τα πιο επιτυχημένα παραδείγματα τέτοιων πλατφορμών είναι το Kickstarter και το GoFundMe. Φυσικά αυτές οι πλατφόρμες υστερούν σε κάποια κυρία σημεία και στον τρόπο λειτουργίας τους.



Εικόνα 6.1: Η αρχική σελίδα i)KickStarter ii) GoFundMe.com

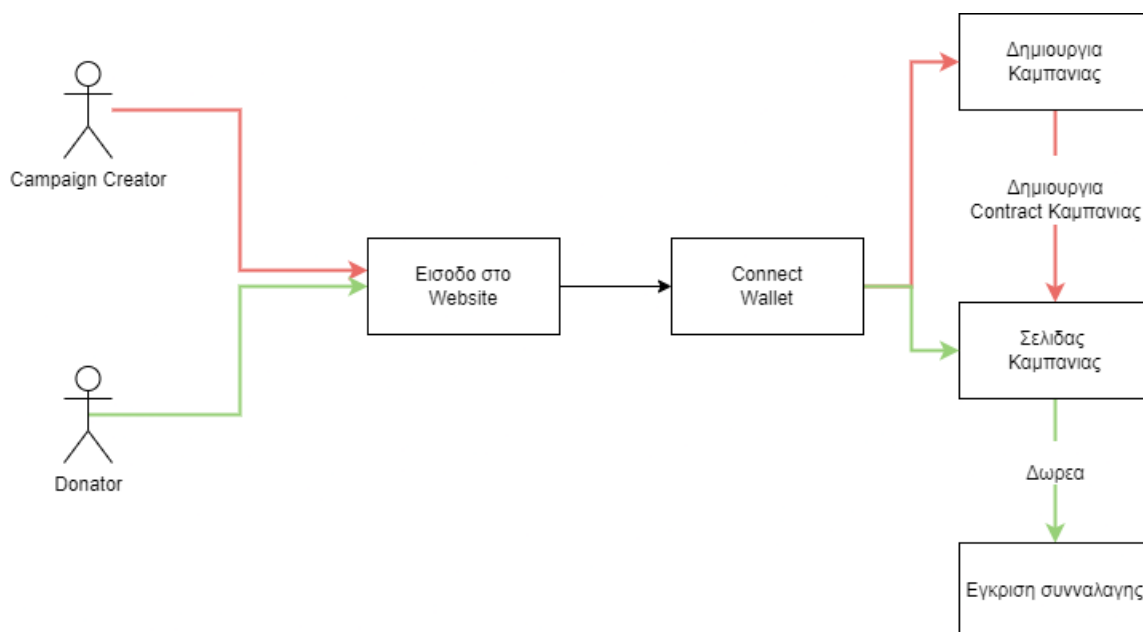
Το πρώτο πρόβλημα είναι η πρόσβαση, η οποία περιορίζει το ποσό της χρηματοδότησης σε μελλοντικά έργα που πρόκειται να δημιουργηθούν με αποτέλεσμα να αυξάνει την ανισότητα. Πολλοί επίδοξοι χρηματοδότες εμποδίζονται ώστε να έχουν πρόσβαση σε αυτές τις πλατφόρμες, συμπεριλαμβανομένων περιθωριοποιημένων ομάδων όπως για παράδειγμα κάτοικοι χωρών με κυβερνήσεις που υπόκεινται σε αυταρχικές κυβερνήσεις καθώς επίσης μεγάλα τμήματα του κόσμου που στερούνται υποδομές οικονομικών πληρωμών πχ τράπεζες.

Το δεύτερο πρόβλημα με το crowdfunding που βασίζεται στο Web2 είναι η ισχύς και η λογοδοσία. Οι πλατφόρμες Crowdfunding Web2 είναι μεγάλες, κεντρικά ελεγχόμενες από εταιρείες. Το μέγεθός τους παρέχει ισχύ στην αγορά για να εξάγουν μεγάλες αμοιβές και η κεντροποιημένη φύση τους δίνει την δυνατότητα σε κυβερνητικούς φορείς ή σε στελέχη να εμποδίζουν την πρόσβαση σε πολλούς επίδοξους χρηματοδότες.

6.2 Διαγραμμα Ροής

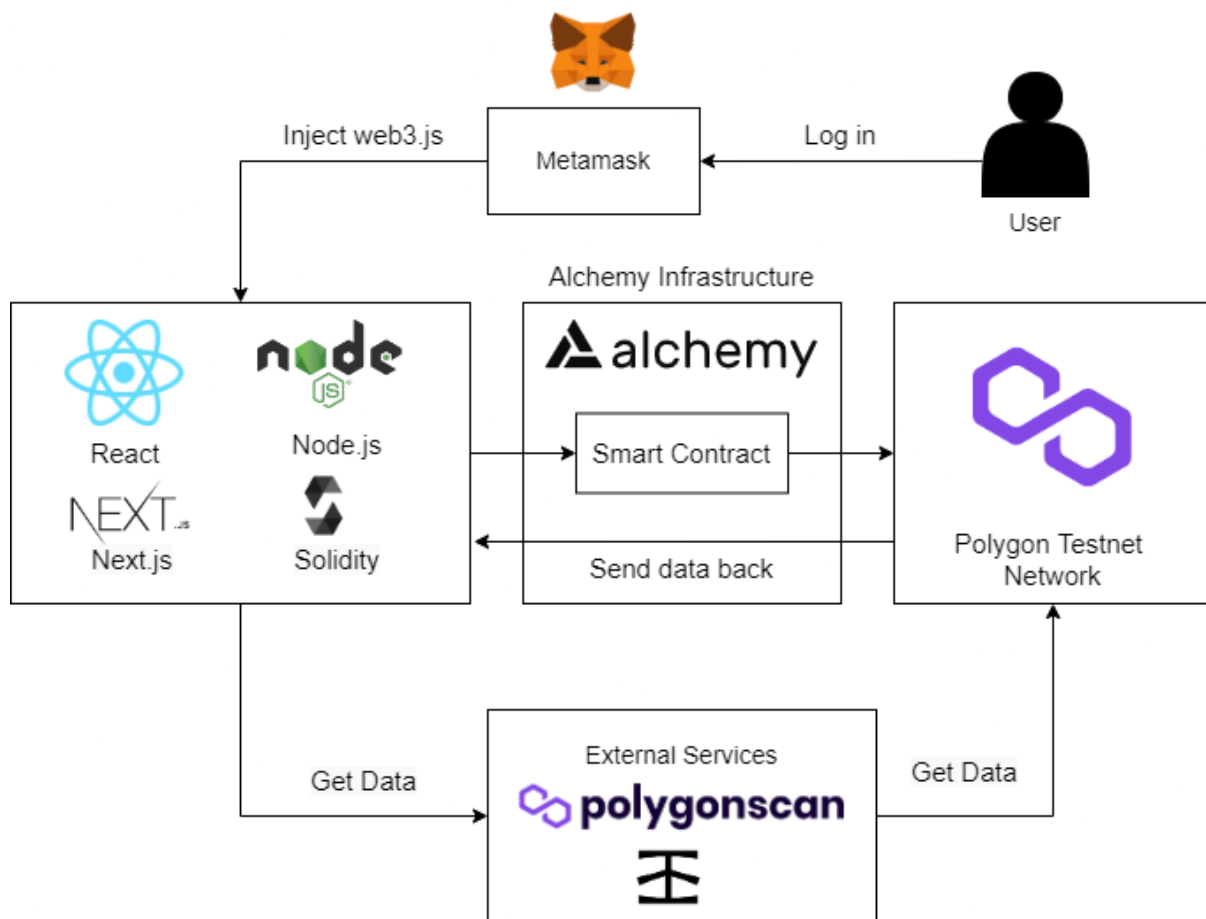
Αρχικά από την πλευρά του Campaign Creator δηλαδή τον Δημιουργό της Καμπάνιας που θέλει να συγκεντρώσει ένα ποσό για κάποιο σκοπό, εισέρχεται στην Αποκεντρωμένη εφαρμογή και συνδέεται με το πορτοφόλι του. Το πορτοφόλι μπορεί να είναι οποιοδήποτε συμβατό πορτοφόλι με το EVM όπως το Metamask, Exodus, Brave Wallet κλπ. Το πορτοφόλι αλληλοεπιδρά με το Dapp και δίνει την δυνατότητα πρόσβασης στα στοιχεία του πορτοφολιού, όπως το την δημοσιά διεύθυνση (public address) του πορτοφολιού του πχ. 0xCa9569621bD7F62387F2e31bCcCbB0bAA01f0FAF. Αφού συνδεθεί ο Campaign Creator θα προχωρήσει στην δημιουργία μια καμπάνιας και υστέρτα θα δημιουργηθεί η Σελίδα της Καμπάνιας.

Από την άλλη πλευρά είναι ο Donator δηλαδή ο δωρητής που θα χρηματοδοτήσει ένα έργο ή μια καμπανιά, σε αυτήν την περίπτωση ο δωρητής θα επαναλάβει το ίδιο βήμα με τον Campaign Creator δηλαδή θα εισέλθει στην σελίδα, θα συνδέσει το Web πορτοφόλι του με την αποκεντρωμένη εφαρμογή. Αφού συνδέσει το πορτοφόλι του στην αρχική ο χρήστης θα βρει άλλες καμπάνιες χρηστών, υστέρτα αφού βρει κάποια καμπανιά που θα θέλει να χρηματοδοτήσει θα μεταφέρεται στην καμπανιά της σελίδας και θα κάνει την δωρεά και αφού εγκριθεί η συναλλαγή η διαδικασία έχει τελειώσει.



Εικόνα 6.2: Διάγραμμα Ροής του Dapp από την πλευρά του χρήστη.

6.3 Αρχιτεκτονική του Dapp.



Εικόνα 6.3: Διάγραμμα Αρχιτεκτονικής του Dapp.

Η Αρχιτεκτονική της αποκεντρωμένης εφαρμογής αρχικά ξεκινάει από το χρήστη που κάνει χρήση του ψηφιακού του πορτοφολιού τύπου Metamask, Το Metamask είναι στην ουρία ένα plugin-in του Browser οπου αλληλεπιδρά και επικοινωνεί με την σελίδα. Αφού συνδεθεί ο χρήστης τότε γίνεται χρήση της βιβλιοθήκης του web3.js που επιτρέπει να αλληλοεπιδράει ο browser με έναν τοπικό ή απομακρυσμένο κόμβο ethereum χρησιμοποιώντας HTTP ή Websockets.

Στην συνέχεια γίνεται το πάντρεμα των τεχνολογιών που αφορά το Backend και το Frontend διαμορφώνουν την σελίδα της αποκεντρωμένης εφαρμογής. Στο Frontend κομμάτι δηλαδή πως παρουσιάζονται τα δεδομένα στο χρήστη χρησιμοποιήθηκε το framework της React και της Next.js. Ενώ για το Backend κομμάτι δηλαδή αυτά που γίνονται στο server και δεν τα βλέπει ο χρήστης ήταν η γλώσσα Node.js η οποία ήταν υπεύθυνη για το hosting της εφαρμογής και ο βασικός πυρήνας για την αλληλεπίδραση όλων των βιβλιοθηκών που χρησιμοποιήθηκαν.

Επιπλέον στο backend χρησιμοποιήθηκε η Solidity όπου ήταν υπεύθυνη για την υλοποίηση των έξυπνων συμβολαίων (Smart Contracts) της εφαρμογής. Θα γίνει εκτενέστερη ανάλυση στις επόμενες ενότητες την κάθε τεχνολογία ξεχωριστά.

Το Alchemy είναι η διόδος μεταξύ της αποκεντρωμένης εφαρμογής και των κόμβων του Blockchain του Polygon. Αφού το hosting των έξυπνων συμβολαίων απαιτεί από την πλευρά του προγραμματιστή να έχει ένα δικό του κόμβο στο blockchain αλλά αυτή η διαδικασία είναι αρκετά περιπλοκή και χρονοβόρα, αφού απαιτεί να παραμετροποιηθεί ένας server με πολλές παραμέτρους και μπορεί να οδηγήσει σε μεγάλο κόστος η συντήρηση του, αφού θα πρέπει να γίνει λήψη όλη την αλυσίδα συναλλαγών του blockchain και αυτό πιθανόν να είναι πολύ μεγάλο σε μέγεθος. Οπότε με την διεπαφή και το API που προσφέρει το Alchemy κάνει αυτό το πρόβλημα στους προγραμματιστές να γίνεται ευκολά και γρηγορά.

Επίσης χρησιμοποιείται ως εξωτερική υπηρεσία PolygonScan όπου είναι στην ουσία ο εξερευνητής (explorer) του blockchain του Polygon και βοηθάει στην ιχνηλατήση των συναλλαγών αν έχουν εγκριθεί ή απορριφθεί. Δίνει την δυνατότητα στο καθένα να εξερευνήσει το ιστορικό συναλλαγών οποιασδήποτε διεύθυνσης πορτοφολιού, βελτιώνοντας τη διαφάνεια στο blockchain και δίνοντας τη δυνατότητα στους χρήστες να πραγματοποιούν ελέγχους. Καθώς μπορεί να δει κάποιος και να επαληθεύσει τα δεδομένα και τις συναλλαγές που έχουν πραγματοποιηθεί σε κάθε μπλοκ.

Μια προσθετή εξωτερική υπηρεσία που χρησιμοποιείται είναι το Infura το οποίο είναι υπεύθυνο για την φιλοξενία των εικόνων και τον κείμενων των καμπανών. Στην ουσία το API του Infura προφέρει το πρωτόκολλο του IPFS, δηλαδή χρησιμοποιεί πολλούς κόμβους για την αποθήκευση περιεχομένου αντί να βασίζεται σε έναν μόνο διακομιστή ιστού. Δηλαδή οι εικόνες και οι λεβάντες των καμπανιών δεν αποθηκεύονται σε κάποιο CDN (Content delivery network) ή κάποια βάση δεδομένων όπως δουλεύαν με το παραδοσιακό τρόπο του HTTPS.

Αντίθετα η αρχιτεκτονική του IPFS μοιάζει με τον τρόπο που λειτουργούν τα Torrent, δηλαδή χρησιμοποιεί αναγνωριστικά περιεχομένου για να σχηματίσει μια διεύθυνση βάσει του ίδιου του περιεχομένου σε αντίθεση με τον εντοπισμό δεδομένων με γνώμονα τη διεύθυνση ενός διακομιστή και έχει σχεδιαστεί και βελτιστοποιηθεί κυρίως σε αποκεντρωμένες πλατφόρμες.

6.4 Εργαλεία που θα χρειαστούν για την ανάπτυξη

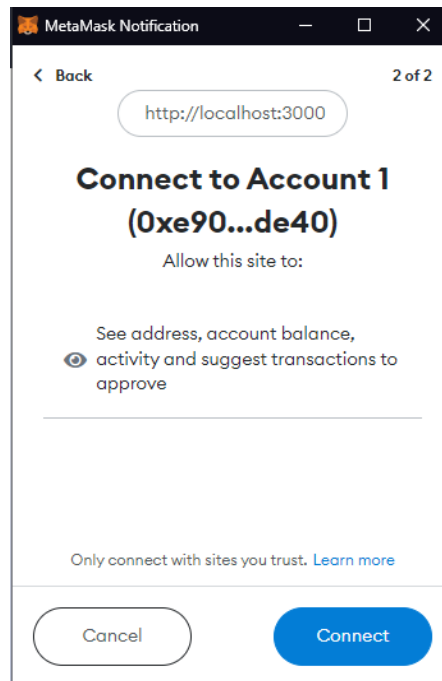
Για την υλοποίηση του DApp, αρχικά έγινε η συγγραφή του έξυπνου συμβολαίου κάνοντας για κάθε συνάρτηση κάθε φορά την αποσφαλμάτωση με την χρήση της ιστοσελίδας Remix για να γίνει σαφές ότι ο κώδικας τρέχει σωστά και χωρίς προβλήματα. Αφού ολοκληρώθηκε το παρακάτω βήμα και επιβεβαιώθηκε ότι ο κώδικας λειτουργεί όπως πρέπει στην συνέχεια προχώρησε η υλοποίηση της ιστοσελίδας με την οποία θα γίνει η διασύνδεση του έξυπνου συμβολαίου με το front end καθώς και το UI για την αλληλεπίδραση του χρήστη με την εφαρμογή μας.

Αφού έγινε εγκατάσταση όλων των απαραίτητων βιβλιοθηκών με την χρήση του npm αρχικά σε τοπικό blockchain με την χρήση του Hardhat δηλαδή σε ένα τοπικό δίκτυο αντίστοιχα DApp για ταχύτερη απόδοση και μείωση των πόρων δημιουργήθηκε ότι το front end λειτουργεί επίσης σωστά. Υστέρα τροποποιήθηκε το Dapp ώστε να είναι συμβατό με το δοκιμαστικό δίκτυο του Polygon και στην συνέχεια το Contract έγινε Deploy στο Mumbai Testnet.

6.4.1 Metamask

Ένα από τα βασικά εργαλεία που χρησιμοποιήθηκαν ήταν το MetaMask το οποίο είναι ένα plugin διαθέσιμο για τους περισσότερους φυλλομετρητές (Browsers) όπως Google Chrome, Mozilla Firefox, Opera και Brave. Είναι στην ουσία μία γέφυρα η οποία δίνει στον browser πρόσβαση στις κατανεμημένες εφαρμογές (DApps), που για την λειτουργία τους βασίζονται στο δίκτυο Polygon.

Το μεγάλο πλεονέκτημα που προσφέρει είναι το γεγονός ότι με την χρήση του, η πρόσβαση στις εφαρμογές αυτές, δεν απαιτεί την εκτέλεση ενός πλήρη κόμβου του δικτύου του Polygon στο μηχάνημα του χρήστη. Συμπεριλαμβάνει επίσης μια ασφαλή κρυπτογράφηση και παρέχει στον χρήστη μία διεπαφή, μέσω της οποίας αυτός μπορεί να διαχειρίζεται τους λογαριασμούς/διευθύνσεις του, ώστε να αλληλοεπιδρά με τις ιστοσελίδες, να στέλνει ή και να υπογράφει συναλλαγές και να υπογράφει δεδομένα.



Εικόνα 6.4: Η αλληλεπίδραση του χρήστη με το Metamask.

6.4.2 Hardhat

Το Hardhat είναι ένα περιβάλλον που χρησιμοποιούν οι προγραμματιστές για τη δοκιμή, τη μεταγλώττιση, την ανάπτυξη και τον εντοπισμό σφαλμάτων dApps που βασίζονται στο blockchain του Ethereum. Ως εκ τούτου, βοηθά τους προγραμματιστές να διαχειρίζονται πολλές από τις εργασίες που είναι εγγενείς στην ανάπτυξη dApps και έξυπνων συμβολαίων. Μαζί με την παροχή στους προγραμματιστές με τα κατάλληλα εργαλεία για τη διαχείριση αυτής της διαδικασίας, το Hardhat βοηθά επίσης στην αυτοματοποίηση ορισμένων από αυτά τα βήματα και παρέχει στους προγραμματιστές με νέες λειτουργίες.

Το Hardhat συνοδεύεται από ένα προκατασκευασμένο τοπικό δίκτυο Ethereum καθώς και όλα τα συμβατά EVM δίκτυα που έχει σχεδιαστεί με την ανάπτυξη στον πυρήνα του. Αυτό το δίκτυο εστιάζει στον εντοπισμό σφαλμάτων Solidity και παρακολουθεί αν αποτυγχάνουν οι συναλλαγές των dApps κ.λπ. Αυτό παρέχει στους προγραμματιστές βασικά εργαλεία για να κατανοήσουν πού αποτυγχάνει μια εφαρμογή και τους παρέχει την απάντηση για την επίλυσή τους.

Το περιβάλλον χαρακτηρίζεται από πρόσθετα από τα οποία προέρχεται μεγάλο μέρος της λειτουργικότητας. Αυτό σημαίνει ότι οι προγραμματιστές μπορούν να επιλέξουν ακριβώς ποια

πρόσθετα θα ήθελαν να συμπεριλάβουν στη διαδικασία ανάπτυξής τους. Ωστόσο, έρχεται με ενσωματωμένες προεπιλογές, αλλά όλες μπορούν να παρακαμφθούν.

```
npm install --save-dev hardhat
```

6.4.3 Solidity

Η Solidity είναι μια γλώσσα προγραμματισμού υψηλού επιπέδου, πλήρης Turing με παρόμοια σύνταξη σαν την JavaScript, που είναι τύπου στατική, υποστηρίζοντας την κληρονομικότητα και τον πολυμορφισμό, καθώς αποτελείται από βιβλιοθήκες με πολύπλοκους τύπους που καθορίζονται από το χρήστη. Η Solidity χρησιμοποιείται για την ανάπτυξη έξυπνων συμβολαίων, τα συμβόλαια είναι έτσι δομημένα παρόμοια με τις κλάσεις στον αντικειμενοστραφή προγραμματισμό. Ο κώδικας των Smart Contracts αποτελείται από μεταβλητές και συναρτήσεις που τα διαβάζουν και τα τροποποιούν, όπως στις παραδοσιακές γλώσσες προγραμματισμού.

6.4.4 Δίκτυο Testnet

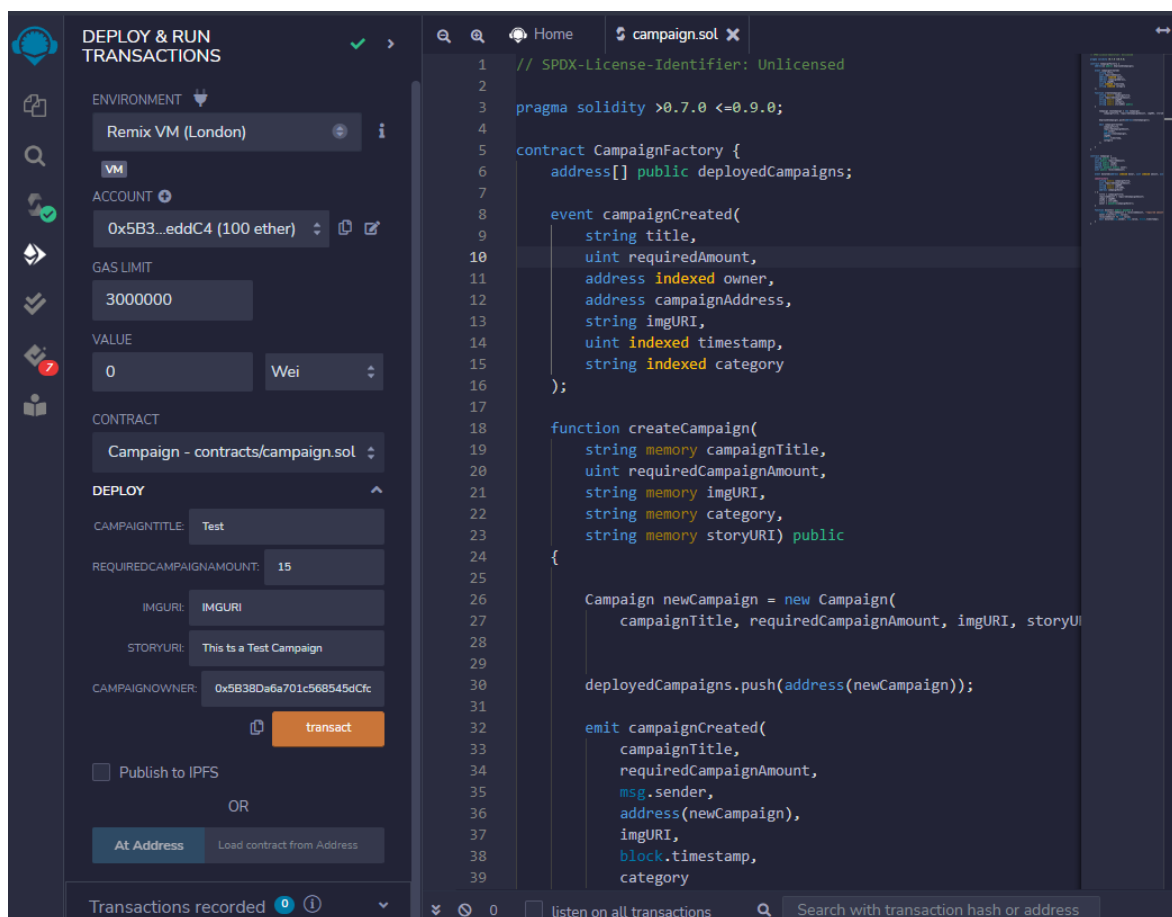
Το Mainnet είναι το κύριο δίκτυο στο οποίο εκτελείται ένα έργο blockchain. Αυτό είναι το στάδιο που λογικά έρχεται αφού έχουν ολοκληρωθεί όλες οι απαραίτητες δοκιμές στο testnet. Το mainnet είναι ένα πλήρως ανεπτυγμένο δίκτυο όπου οι συναλλαγές κρυπτονομισμάτων μπορούν να επεξεργαστούν αποτελεσματικά, να επαληθευτούν με ακρίβεια και να καταγραφούν με ασφάλεια. Ένα πλήρως λειτουργικό blockchain, τα mainnets χρησιμοποιούνται για την αποστολή και λήψη οποιασδήποτε συναλλαγής, με τη μορφή κρυπτονομισμάτων ή μη ανταλλακτικών μαρκών (NFT), μεταξύ άλλων, ή μεταφοράς πληροφοριών.

Πρώτον, η εκτέλεση δοκιμών σε ένα κεντρικό δίκτυο μπορεί να είναι πολύ ακριβή αφού τα τέλη Blockchain θα πρέπει να καταβάλλονται για κάθε συναλλαγή που πραγματοποιείται, για κάθε αλλαγή και κάθε φορά που κυκλοφορεί ένα έργο - οι οποίες κατά τη διάρκεια μιας φάσης δοκιμών είναι πολλαπλές και επαναλαμβάνονται. Αυτό θα σήμαινε ότι για να δοκιμαστεί αποτελεσματικά ένα έργο και να διερευνηθούν οι πιθανές επιλογές του, θα απαιτηθούν απίστευτα υψηλά τέλη. Εάν παρουσιαστεί πρόβλημα κατά τη διάρκεια μιας δοκιμαστικής φάσης στο mainnets δίκτυο, μπορεί να διαταραχθεί ολόκληρο το δίκτυο, με αποτέλεσμα να διαταραχθούν και να κινδυνεύσουν τα περιουσιακά στοιχεία και οι συναλλαγές των χρηστών του, και να οδηγήσει τους χρήστες να χάσουν τα χρήματά τους. Αυτό μπορεί να είναι πολύ δαπανηρό, τόσο για προγραμματιστές όσο και για τη φήμη του κρυπτονομίσματος στο σύνολό του.

Επίσης τεθείτε ένα ζήτημα συμβατότητας, τα δοκιμαστικά δίκτυα δεν χρησιμοποιούν τίποτα πραγματικής αξίας και αντίθετα χρησιμοποιούν ψεύτικα νομίσματα. Τα δοκιμαστικά νομίσματα δεν είναι συμβατά με τα κύρια δίκτυα και το αντίστροφο, πράγμα που σημαίνει ότι θα πρέπει να κοπούν νέα νομίσματα ή μέθοδοι, με αποτέλεσμα μια πολύ μεγαλύτερη, περίπλοκη και δαπανηρή διαδικασία.

6.4.5 Remix

Ότι γράφετε στο blockchain παραμένει εκεί για πάντα για αυτό είναι πολύ σημαντικό να ελέγξουμε ότι τα smart contract λειτουργούν σωστά. Για τον έλεγχο της λειτουργικότητας των smart contracts χρησιμοποιήθηκε η ιστοσελίδα του Remix (<https://remix.ethereum.org/>) εκεί δημιουργήθηκε ένα .sol αρχείο με τον κώδικα επίσης, αρχικά έγινε compile και στην συνέχεια deploy. Έτσι έχουμε το UI επίσης της εικόνας 6.2 και χρησιμοποιώντας επίσης συναρτήσεις μέσω του remix μπορούμε να ελέγξουμε αν οι συναρτήσεις επίσης λειτουργούν όπως θα έπρεπε



Εικόνα 6.5 User interface του Remix.

6.4.6 IPFS

Το InterPlanetary File System, IPFS είναι μια αποκεντρωμένη πλατφόρμα κοινής χρήσης αρχείων που προσδιορίζει τα αρχεία μέσω του περιεχομένου τους. Βασίζεται σε έναν κατακερματισμένο πίνακα κατακερματισμού για την ανάκτηση της τοποθεσίας του αρχείου. Για παράδειγμα όταν ένα αρχείο μεταφορτώνεται στο IPFS, χωρίζεται σε κομμάτια, το καθένα περιέχει το πολύ 256 kilobyte δεδομένων ή/και συνδέσμων σε άλλα κομμάτια. Κάθε κομμάτι προσδιορίζεται από ένα κρυπτογραφικό hash, που ονομάζεται επίσης αναγνωριστικό περιεχομένου, που υπολογίζεται από το περιεχόμενο. Οι σύνδεσμοι περιέχουν αναγνωριστικά περιεχομένου, σχηματίζοντας έτσι ένα άκυκλο γράφημα κατευθυνόμενο από τη Merkle (Merkle DAG) που περιγράφει το αρχείο ως σύνολο και μπορεί να χρησιμοποιηθεί για ανακατασκευή οποιoδήποτε αρχείο από τα κομμάτια του.

6.4.7 Node.js

Η Node.js είναι μία server-side πλατφόρμα, η οποία έχει αναπτυχθεί πάνω στο Google Chrome JavaScript Engine (V8 Engine) το 2009. Είναι ανοιχτού κώδικα (Opensource), cross-platform περιβάλλον ανάπτυξης και εκτέλεσης της γλώσσας προγραμματισμού JavaScript, κατάλληλο για εύκολη και γρήγορη ανάπτυξη κλιμακώσιμων Web εφαρμογών. Θεωρείται ιδανικό για εφαρμογές πραγματικού χρόνου (real-time), υπολογιστικά έντονες που τρέχουν σε κατακερματισμένα περιβάλλοντα. Επίσης, το Node.js παρέχει μία μεγάλη βιβλιοθήκη από JavaScript modules, γεγονός που απλοποιεί ουσιαστικά τη διαδικασία ανάπτυξης διαδικτυακών εφαρμογών.

6.4.8 React & Next.js

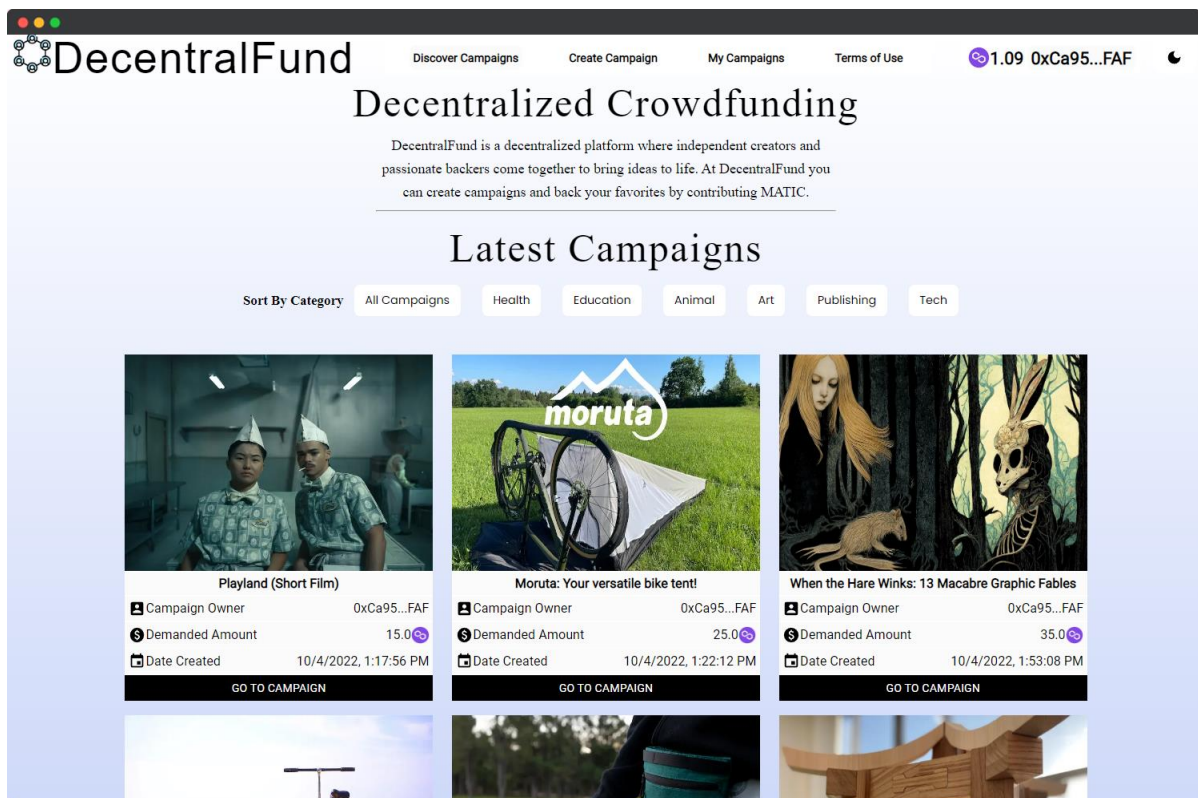
Η React είναι μια βιβλιοθήκη JavaScript που δημιουργήθηκε από την Facebook . Είναι η πιο δημοφιλής βιβλιοθήκη για τη δημιουργία μονοσέλιδων εφαρμογών και διαδραστικών διεπαφών χρήστη. Η ύπαρξη ανοιχτού κώδικα βοηθά τη βιβλιοθήκη να παραμένει στην κορυφή των λιστών δημοτικότητας. Η React είναι μια δωρεάν και ανοιχτού κώδικα βιβλιοθήκη JavaScript front-end για τη δημιουργία διεπαφών χρήστη που βασίζονται σε στοιχεία διεπαφής χρήστη και συντηρείται από τη Meta και από την κοινότητα των προγραμματιστών και εταιρειών.

Η βιβλιοθήκη του Next.js είναι ένα πλαίσιο της React που επιτρέπει πολλές επιπλέον δυνατότητες, συμπεριλαμβανομένης της απόδοσης από την πλευρά του διακομιστή και της

δημιουργίας στατικών ιστότοπων. Το κύριο χαρακτηριστικό της Next.js είναι η χρήση της απόδοσης από την πλευρά του διακομιστή για τη μείωση του φόρτου στα προγράμματα περιήγησης ιστού και την παροχή βελτιωμένης ασφάλειας. Αυτό μπορεί να γίνει για οποιοδήποτε μέρος της εφαρμογής ή ολόκληρου του έργου, επιτρέποντας την επιλογή σελίδων με πλούσιο περιεχόμενο για απόδοση από την πλευρά του διακομιστή.

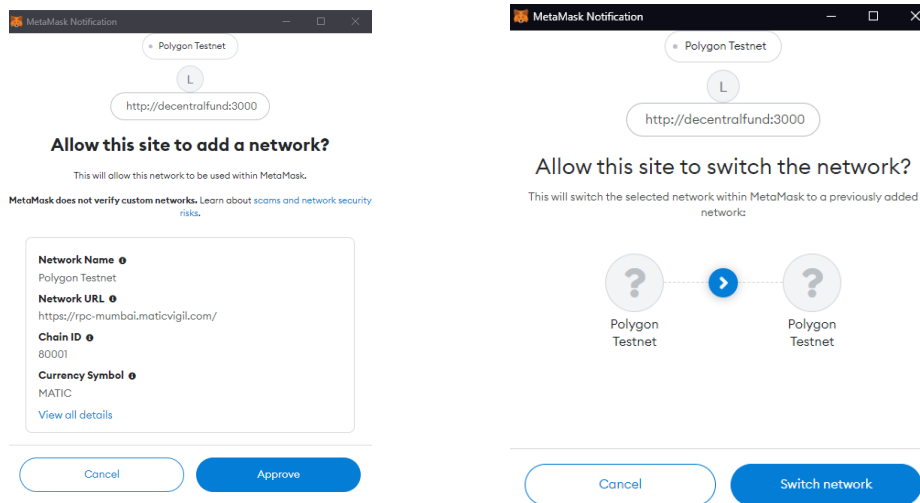
Υλοποίηση του Συστήματος

Αφού ολοκληρώσουμε την παραπάνω βήματα μπορούμε να ξεκινήσουμε την παρουσίαση του DApp. Αρχικά θα πρέπει να εισέλθουμε στην ιστοσελίδα της αποκεντρωμένης εφαρμογής, για εξοικονόμηση κόστους και πόρων την ιστοσελίδα θα τρέχει τοπικά στο υπολογιστή μέσω του server που υλοποιεί η node.js. Στην συνέχεια επισκεπτόμαστε την σελίδα localhost:3000. Με το που εισερχόμαστε στην ιστοσελίδα βλέπουμε την αρχική σελίδα του Dapp και την περιγραφή του Dapp καθώς πιο κάτω βλέπουμε όλες τις καμπάνιες που έχουν δημιουργηθεί από άλλους χρήστες ταξινομημένες με χρονολογική σειρά.



Εικόνα: Η αρχική σελίδα της Αποκεντρωμένης Εφαρμογής

Αφού προηγηθεί στην σελίδα πάνω δεξιά υπάρχει το κουμπί για την σύνδεση του πορτοφολιού. Μόλις πατήσει ο χρήστης αρχικά του ζητάει να αλλάξει το δίκτυο που χρησιμοποιεί και του ζητάει να μεταβεί στο δίκτυο του Polygon Testnet. Αφού πατήσει **Αποδοχή** στην συνέχεια του ζητάει αν επιθυμεί να έχει πρόσβαση στην διεύθυνση του με σκοπό να δει την δημοσιά διεύθυνση και στην συνέχεια το Dapp να βρει το ποσό που έχει σε Matic Tokens (Testnet) μέσω του PolygonScan.



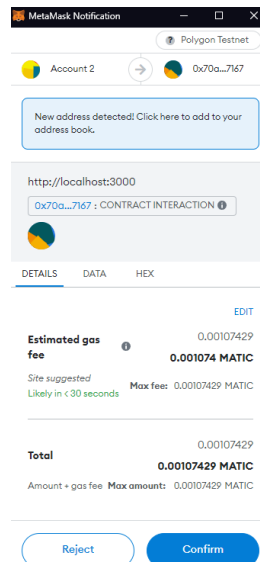
Εικόνα: Η αλλαγή δικτύου Testnet

Κατόπιν ο χρήστης βρει μια καμπανιά που θέλει να χρηματοδοτήσει μπορεί να δει ποτέ έχει δημιουργηθεί από ποια διεύθυνση και τι ποσό στοχεύει να μαζέψει προς χρηματοδότηση στην συνέχεια μπορεί να πατήσει στο κουμπί Go to Campaign για να μεταφερθεί στην σελίδα της καμπάνιας ώστε να χρηματοδοτήσει. Στην συνέχεια θα δείξουμε πως φαίνεται η σελίδα της καμπάνιας.

Στην κορυφή υπάρχει η επιλογή Create Campaign για να δημιουργήσει καποιος την δικια του καμπανιά. Αφού το πατήσει θα μεταφερθεί στην παρακάτω σελίδα. Όπου θα ζητάει από το χρήστη να συμπληρώσει έναν τίτλο για την καμπανιά. Μια περιγραφή της καμπάνιας για το τι πρόκειται να κάνει. Ένα απαιτούμενο ποσό για την υλοποίηση της καμπάνιας. Να επιλέξει μια κατηγορία και να ανεβάσει μια φωτογραφία που θα αντιπροσωπεύει την καμπανιά και αφού ολοκληρώσει τα παραπάνω βήματα να πατήσει Start Campaign.

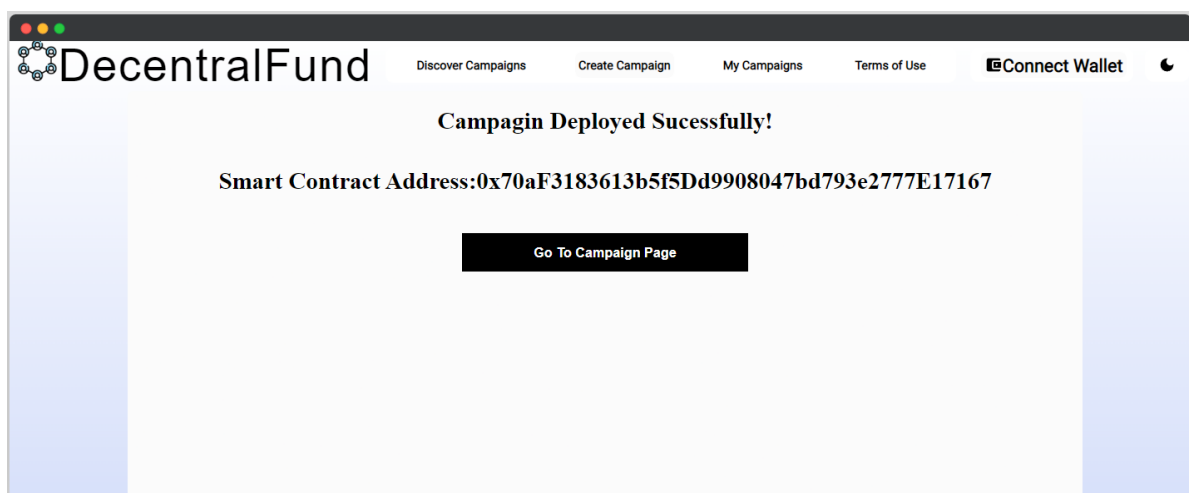
Εικόνα: Η σελίδα δημιουργίας καμπάνιας.

Να σημειωθεί ότι όταν ο χρήστης γραφεί μια περιγραφή στο πεδίο Description of Campaign τα δεδομένα αυτά ανεβαίνουν στο IPFS του Infura και δημιουργείται ένα μοναδικό αναγνωριστικό στο οποίο μετά ο Browser του χρήστη κάνει fetch από το IPFS και λαμβάνει από τις αποκεντρωμένες οντότητες. Το ίδιο γίνεται και στην περίπτωση των φωτογραφιών των καμπανιών ανεβαίνουν στο IPFS και όχι σε κάποιο τοπικό server. Υστέρα αφού πατήσουμε το κουμπί Start Campaign ανοίγει ένα Pop-Up του Metamask ώστε εγκρίνει την συναλλαγή για την δημιουργία της καμπάνιας.



Εικόνα: Η αλληλεπίδραση του Metamask για την δημιουργία της καμπάνιας.

Αφού πατήσουμε έγκριση θα περιμένουμε κάποια δευτερόλεπτα (εξαρτάται από την κίνηση που υπάρχει στο δίκτυο την δεδομένη στιγμή) και αφού εγκριθεί θα δούμε ότι καμπανιά μας δημιουργηθεί με μια δική της διεύθυνση.



Εικόνα: Η επιτυχημένη δημιουργία της καμπάνιας

Η διεύθυνση αποτελεί το μοναδικό αναγνωριστικό της καμπάνιας με σκοπό να συλλεχθούν χρήματα αφού ότι συναλλαγές γίνονται θα στέλνονται στο Smart Contract της καμπάνιας και υστέρτα το Smart Contract θα στέλνει τα χρήματα στην διεύθυνση του δημιουργού.

Η μαγεία του Blockchain είναι ότι μας δίνει την ευκαιρία να εξερευνήσουμε τα δεδομένα με διαφάνεια και να ελέγξουμε περί τίνος πρόκειται. Αφού μπορούμε να δούμε τα δεδομένα που στάλθηκαν στο Blockchain κατά την δημιουργία της καμπάνιας καθώς και τα gas fees που δαπανήθηκαν για αυτή την συναλλαγή. Επίσης υπάρχει το πεδίο imURL και storyURL που έχουν τα μοναδικά αναγνωριστικά για τα δεδομένα της καμπάνιας και την εικόνα της καμπάνιας.

The screenshot shows the 'Transaction Details' page on PolygonScan. The transaction is a PoS Testnet transaction. Key details include:

- Transaction Hash: 0xce816b289de3fb8c0eed3f2a6266f22d5e6726b21fc022d5414057ad1aeb7431
- Status: Success
- Block: 28441929 (1 Block Confirmation)
- Timestamp: 24 secs ago (Oct-04-2022 12:32:57 PM +UTC)
- From: 0xca9569621bd7f523872e31bccccb0baa0110faf
- To: Contract 0x70af3183613b5f5dd9908047bd793e2777e17167
- Value: 0 MATIC (\$0.00)
- Transaction Fee: 0.0016267506410998 MATIC (\$0.00)
- Txn Type: 2 (EIP-1559)
- Gas Limit: 670,825
- Gas Used by Transaction: 670,825 (100%)
- Base Fee Per Gas: 26 wei (0.000000026 Gwei)

Εικόνα: Το μπλοκ συναλλαγής της δημιουργίας της Καμπάνιας.

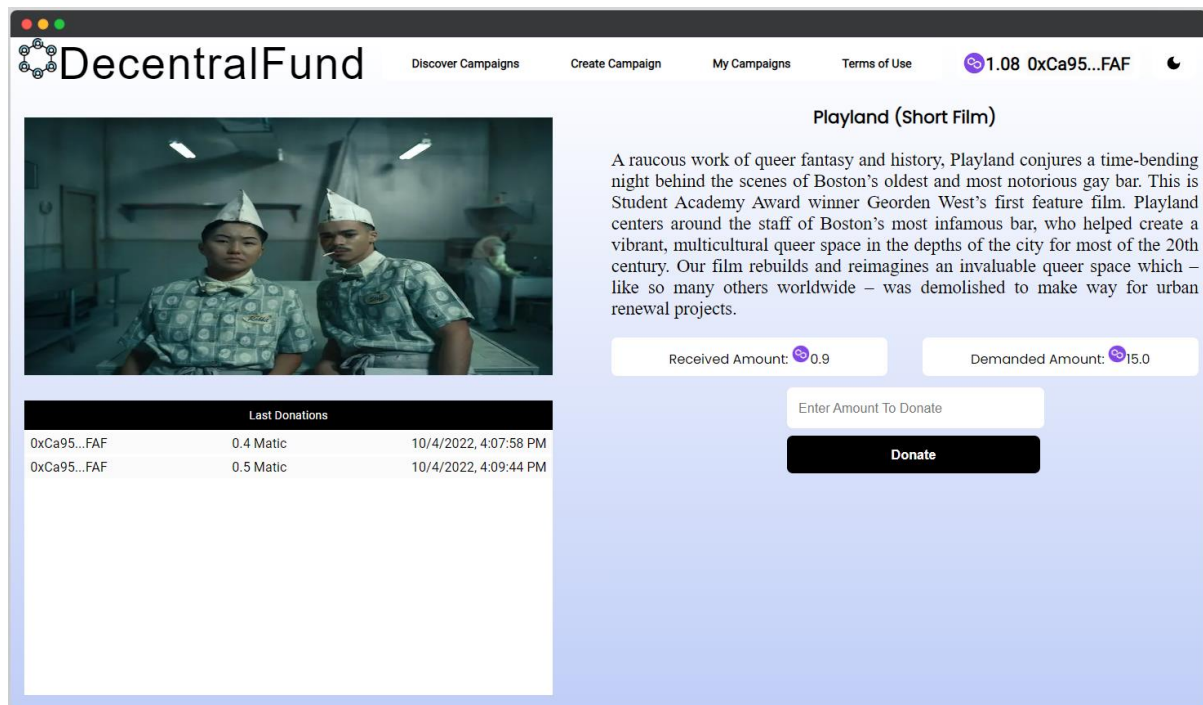
The screenshot shows the 'Input Data' section of the transaction details. It lists various fees and the input data for the transaction.

#	Name	Type	Data
0	campaignTitle	string	All-Water Bike
1	requiredCampaignAmount	uint256	1000000000000000000
2	imgURI	string	QmPg8QeL1P8QKPC67hcKzh5M2yT2VvXh8LW8U9FTby
3	category	string	Tech
4	storyURI	string	QmQ8uWlyYSPeg72wtCdJpyQmTfpcCkxGvWk35orzyqHKG7

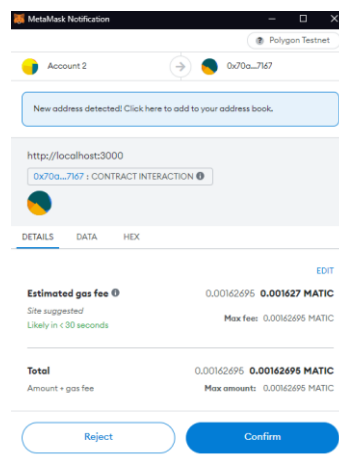
Εικόνα: Τα δεδομένα του μπλοκ συναλλαγής.

Παρακάτω βλέπουμε πως φαίνεται η σελίδα μια καμπάνιας. Αριστερά βλέπουμε την εικόνα της καμπάνιας και από κάτω βλέπουμε τους χρηματοδότες που έχουν στηρίξει το έργο πάνω δεξιά βλέπουμε τον τίτλο της Καμπάνιας και από κάτω την περιγραφή της Καμπάνιας. Στο Received Amount αφορά την ποσότητα Matic Tokens που έχει δεχθεί η καμπάνια ενώ στο Demanded Amount είναι ο στόχος που έχει βάλει ο δημιουργός της Καμπάνιας.

Από κάτω στο πεδίο είναι το ποσό που θέλει να βάλει ο δωρητής και αφού συμπλήρωση το ποσό πατάει το κουμπί Donate και προχωράει στην δωρεά. Αφού πατήσει το Donate θα ανοίξει το pop-up του Metamask για να εγκρίνει την συναλλαγή.



Εικόνα: Η σελίδα για την δημιουργία μιας νέας καμπάνιας.



Εικόνα: Η αλληλεπίδραση του Metamask για την δωρεά στην καμπάνια.

Φυσικά αν προχωρήσουμε στον εξερευνητή (explorer) θα δούμε αναλυτικά τις συναλλαγές που έχουν δημιουργηθεί με το αναγνωριστικό της μεθόδου (method) δηλαδή αν πρόκειται για δημιουργία καμπάνιας ή για δωρεά και την ακριβή ώρα και σε ποιο μπλοκ συναλλαγών έγινε οι συναλλαγές.

Txn Hash	Method ⓘ	Block	Age	From	
 0x1254478f7561d782caf...	Donate	28442369	18 hrs 46 mins ago	0xca9569621bd7f62387f...	OUT
 0x16534e25655e5b3e23...	Donate	28442348	18 hrs 48 mins ago	0xca9569621bd7f62387f...	OUT
 0xe2be6f95ac4f57f9bf7a...	Create Campaign	28442075	19 hrs 11 mins ago	0xca9569621bd7f62387f...	OUT

Εικόνα: Οι συναλλαγές από το PolygonScan.

Επίσης έχει δημιουργηθεί μια σελίδα με τους ορους της εφαρμογής αλλά και μια πιο αναλυτική περιγραφή για το τι είναι το DecentralFund.



Εικόνα: Σελίδα Terms Of Use.

Βιβλιογραφικές αναφορές

- [1] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. Available: <https://bitcoin.org/bitcoin.pdf>.
- [2] Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).
- [3] What is the Web3? The Decentralized Web - Blockchain <https://blockchainhub.net/web3-decentralized-web/>.
- [4] Antonopoulos, A.M. (2015). Mastering Bitcoin. United States of America: O'Reilly Media Inc.
- [5] Jimi S., (2018) 'Blockchain: how a 51% attack works (double spend attack)', <https://medium.com/@JimiS/what-is-a-51-attack-or-double-spend-attack-aa108db63474>,
- [6] Meier, J., & Schuppli, B. (2019). The DAO Hack and the Living Law of Blockchain. Digitalisierung–Gesellschaft–Recht: Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich, 27-43.
- [7] Public key cryptography. [Online]. Available: https://en.wikipedia.org/wiki/Public-key_cryptography (visited on 01/13/2019).
- [8] Srivastav, K. (2019). A Guide to Blockchain Immutability and Challenges - DZone Security. Retrieved 26 October 2020, from <https://dzone.com/articles/a-guide-to-blockchainimmutability-and-chief-chall>
- [9] G. Wood, «Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain,» [Ηλεκτρονικό]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>.
- [10] Ethereum. What is ethereum? Ανάκτηση Ιούλιος 15, 2022, από Ethereum.org: <https://ethereum.org/en/what-is-ethereum/>
- [11] Antonopoulos, A., Wood, G. (2019). Mastering Ethereum. O'Reilly Media, Inc
- [12] William Metcalfe, 2020. Ethereum, Smart Contracts, Dapps. Springer. E-journal. In book: Blockchain and Crypt Currency.

- [13] «What is the Web3? The Decentralized Web - Blockchain». Website: <https://blockchainhub.net/web3-decentralized-web/>.
- [14] What Is Crowdfunding? The Clear and Simple Answer. GoFundMe.com [online] <https://www.gofundme.com/c/crowdfunding>
- [15] Web3.js. [Online]. Available: <https://web3js.readthedocs.io/en/v1.8.0/>.
- [16] MetaMask. (2021). Retrieved 26 January 2021, from <https://metamask.io/>
- [17] Remix - Solidity IDE. Ανακτήθηκε από <http://remix.readthedocs.io/en/latest/>
- [18] Nodejs Documentation. Website: <https://nodejs.org/en/docs>
- [19] Chrome V8 | Google Developers Available: <https://developers.google.com/v8/>.
- [20] What Is Solidity? What Are Its Use Cases? - Top Digital Agency. (2019). Retrieved 26 January 2021, from <https://topdigital.agency/what-is-solidity-what-are-its-use-cases/>
- [21] Johnston, David, et al. "TheGeneralTheoryofDecen-tralizedApplications, DApps." (2014).
- [22] Metcalfe, William. "Ethereum, smart contracts, DApps." *Blockchain and Crypt Currency* (2020): 77.

Παράρτημα 1: Οδηγίες εγκατάστασης

Εγκατάσταση

Στο παράρτημα αυτό θα γίνει παρουσίαση οδηγιών για την εγκατάσταση του συστήματος σε Windows Server και για την χρήση του συστήματος.

Εδώ παρουσιάζονται αναλυτικά τα προγράμματα που χρειάζονται για την εγκατάσταση και λειτουργία της εφαρμογής. Τα βήματα που παρουσιάζονται πραγματοποιήθηκαν για την επιτυχή εγκατάσταση της εφαρμογής σε Windows 10 Pro χωρίς πρόβλημα.

Βήμα 1: Θα χρειαστεί το σύστημα διαχείρισης πακέτων NPM. Ο installer του npm (συμπεριλαμβάνεται ο Node.js) βρίσκεται εδώ: <https://nodejs.org/>

Βήμα 2: Θα χρειαστεί να κατεβάσουμε τοπικά το project μέσω του Github

- `C:\Users\p17kont1> git clone https://github.com/p17kont1/thesis`

Βήμα 3: Θα χρειαστεί να εγκαταστήσουμε τις απαραίτητες βιβλιοθήκες

- `C:\Users\p17kont1> cd thesis`
- `C:\Users\p17kont1> npm install -i`

Βήμα 4: Θα χρειαστεί να κάνουμε compile το Smart Contract που δημιουργήσαμε στο Remix εκτελούμε την παρακάτω εντολή:

- `npx hardhat compile`

Βήμα 5: Στην συνέχεια δημιουργούμε το αρχείο `env.local` και προσθέτουμε τις παρακάτω γραμμές:

- `NEXT_PUBLIC_RPC_URL=` (Με το RPC URL του Alchemy).
- `NEXT_PUBLIC_PRIVATE_KEY=` (Το ιδιωτικό κλειδί του Metamask).

Βήμα 5: Στην συνέχεια κάνουμε το contract deploy στο Blockchain με την παρακάτω εντολή:

- `npx hardhat run scripts/deploy.js`

Και στην συνέχεια θα δημιουργηθεί το contract της εφαρμογής που θα έχει την μορφή: 0xAc6b5a11f9897905cbb1fAc5B4e1816d5Fb243B7.

Βήμα 6: Στην συνέχεια προσθέτουμε στο αρχείο env.local

- NEXT_PUBLIC_ADDRESS= την προηγούμενη διεύθυνση που λάβαμε από το deployer.

Βήμα 7: εκτελούμε την web εφαρμογή με την εντολή npm run dev και θα μετάβουμε στην διεύθυνση localhost:3000.

Παράρτημα 2: Κώδικας Smart Contracts

Σε αυτήν την ενότητα βρίσκεται ο κώδικας των έξυπνων συμβολαίων (smart contracts) γραμμένος στην γλώσσα Solidity.

```
// SPDX-License-Identifier: Unlicensed

pragma solidity >0.7.0 <=0.9.0;

contract CampaignFactory {
    address[] public deployedCampaigns;
    event campaignCreated(
        string title,
        uint requiredAmount,
        address indexed owner,
        address campaignAddress,
        string imgURI,
        uint indexed timestamp,
        string indexed category
    );

    function createCampaign(
        string memory campaignTitle,
        uint requiredCampaignAmount,
        string memory imgURI,
        string memory category,
        string memory storyURI) public
    {
        Campaign newCampaign = new Campaign(
            campaignTitle, requiredCampaignAmount, imgURI, storyURI,
            msg.sender);

        deployedCampaigns.push(address(newCampaign));
        emit campaignCreated(
            campaignTitle,
            requiredCampaignAmount,
            msg.sender,
            address(newCampaign),
            imgURI,
            block.timestamp,
            category
        );
    }
}
```

```

contract Campaign {
    string public title;
    uint public requiredAmount;
    string public image;
    string public story;
    address payable public owner;
    uint public receivedAmount;

    event donated(address indexed donar, uint indexed amount, uint indexed
timestamp);

    constructor(
        string memory campaignTitle,
        uint requiredCampaignAmount,
        string memory imgURI,
        string memory storyURI,
        address campaignOwner
    ) {
        title = campaignTitle;
        requiredAmount = requiredCampaignAmount;
        image = imgURI;
        story = storyURI;
        owner = payable(campaignOwner);
    }

    function donate() public payable {
        require(requiredAmount > receivedAmount, "required amount
fullfilled");
        owner.transfer(msg.value);
        receivedAmount += msg.value;
        emit donated(msg.sender, msg.value, block.timestamp);
    }
}

```