ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών

UNIVERSITY of WEST ATTICA
FACULTY OF ENGINEERING
Department of Electrical & Electronics Engineering

Πρόγραμμα Μεταπτυχιακών Σπουδών
Διαδικτυωμένα Ηλεκτρονικά Συστήματα

Master of Science in
Internetworked Electronic Systems

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Το Διαδίκτυο της ενέργειας και οι τεχνολογίες Διαδικτύωσης Αντικειμένων:
Μελέτη Υλοποίησης διάταξης επίδειξης

Μεταπτυχιακός Φοιτητής: Κουναλάκης Νικόλαος, Α.Μ. IES-0038
Επιβλέπων: Παπαγέωργας Παναγιώτης, Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΝΟΕΜΒΡΙΟΣ 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
Τμήμα Ηλεκτρολόγων & Ηλεκτρονικών Μηχανικών

UNIVERSITY of WEST ATTICA
FACULTY OF ENGINEERING
Department of Electrical & Electronics Engineering

Πρόγραμμα Μεταπτυχιακών Σπουδών
Διαδικτυωμένα Ηλεκτρονικά Συστήματα

Master of Science in
Internetworked Electronic Systems

MSc Thesis

Internet of Energy and IoT technologies:
Study of a demonstration platform

Student: Kounalakis Nikolaos, Reg. Nr. IES-0038
MSc Thesis Supervisor: Papageorgas Panagiotis, Professor

ATHENS-EGALEO, NOVEMBER 2019

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία έχει ως αντικείμενο την μελέτη και ανάπτυξη τεχνολογιών του Διαδικτύου των Πραγμάτων και της Ενέργειας (IoT & IoE) σε επίπεδο υλοποίησης smart grid βασισμένο σε Blockchain πρωτόκολλο. Αρχικά περιγράφονται σε θεωρητικό επίπεδο οι Τεχνολογίες Κατανεμημένου Μητρώου (DLT- Distributed Ledger technologies) , τα Blockchain και οι κατηγορίες που υπάγονται σε αυτά, οι τεχνολογίες IoT και η χρήση αυτών για την πραγματοποίηση Home Area Networks (HAN) . Έμφαση θα δοθεί στις αποκεντρωμένες εφαρμογές (DApps- Decentralized Applications) και πώς μέσω των τεχνολογιών διαδικτύωσης των Αντικειμένων εφαρμόζεται ένα μικροδίκτυο, έναντι του καθιερωμένου client-server grid, δίνοντας την δυνατότητα σε όλους τους συμμετέχοντες-χρήστες να είναι ομότιμοι (P2P) έχοντας την ιδιότητα και του πωλητή και του αγοραστή ταυτόχρονα, χωρίς να είναι απαραίτητη η παρουσία διαμεσολαβητών.

Στη συνέχεια, υλοποιείται ένα πραγματικό Ethereum Private Blockchain με τα εργαλεία του Ethereum και τη βοήθεια δύο τερματικών συσκευών σε Linux λογισμικό, μία εκ των δύο είναι το RPi, βασισμένο στις θεωρητικές προδιαγραφές, όπως περιγράφονται στο πρώτο μέρος. Στόχος είναι η επίδειξη διάταξης στα πρότυπα ενός Microgrid και η ολοκλήρωση μιας μικροπληρωμής μεταξύ δύο ομότιμων χρηστών αναδεικνύοντας την σημαντικότητα της εφαρμογής των Blockchain για την βιωσιμότητα της αγοράς ενέργειας. Η εργασία αυτή αποσκοπεί στην αξιολόγηση των τεχνολογιών που ήδη υπάρχουν για την επίτευξη αποκεντρωμένων ενεργειακών συστημάτων και την πρόοδο τους στην ασφάλεια και ταχύτητα, την ανάδειξη projects που έχουν ήδη τεθεί σε εφαρμογή, καθώς και τις δυνατότητες των αποκεντρωμένων εφαρμογών στην δόμηση μιας ευέλικτης και προσβάσιμης σε όλους αγορά ενέργειας.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: Διαδίκτυο των Πραγμάτων, Διαδίκτυο της Ενέργειας, Smart Grid, Blockchain, Τεχνολογίες Κατανεμημένου Μητρώου, Αποκεντρωμένες Εφαρμογές, Home Area Networks, μικροδίκτυο, P2P, Ethereum, Μικροπληρωμή

ABSTRACT

The purpose of the present thesis is to study and develop Internet of Things and Energy (IoT & IoE) technologies at smart grid implementation level, based on Blockchain protocol. To begin with, Distributed Ledger Technologies (DLT – Distributed Ledger Technologies) are described in a theoretical level, the Blockchain and the categories that fall under it, the IoT technologies and their use for the actualization of Home Area Networks (HAN). Emphasis will be given to decentralized applications (DApps) and how a Microgrid is applied through the technology of the internetworking of Objects, instead of the standard client – server grid, enabling all participants – users to be peers (P2P) having the capacity of both seller and buyer at the same time, without the need of brokers.

Subsequently, a real Ethereum Private Blockchain is implemented with the use of Ethereum tools and the help of two terminals in Linux software using Raspberry, based on the theoretical specifications as described in the first part. The aim is to demonstrate the layout of a Microgrid template and to complete a micropayment between two peers highlighting the importance of Blockchain's application to the viability of the energy market. This operation aims to evaluate technologies that already exist for achieving decentralized energy systems and their progress in security and speed, highlighting projects that have already been implemented, as well as the possibilities of decentralized application in building a flexible and accessible energy market for everyone.

Keywords: Internet of Things (IoT), Internet of Energy (IoE), Smart Grid, Blockchain, Distributed Ledger Technologies (DLT), Decentralized Apps (DApps), Home Area Networks, Microgrid, P2P, Ethereum, Micropayments

ΕΥΧΑΡΙΣΤΙΕΣ

Η συγκεκριμένη εργασία πραγματοποιήθηκε στα πλαίσια των μεταπτυχιακών μου σπουδών στο τμήμα «Διαδικτυωμένα Ηλεκτρονικά Συστήματα» του Πανεπιστημίου Δυτικής Αττικής. Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή του τμήματος «Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών» του Πανεπιστημίου Δυτικής Αττικής κ. Παναγιώτη Παπαγέωργα για την συμβολή και την στήριξη του, την καθοδήγηση του σε επιστημονικά ζητήματα και τον χρόνο του για την εκπόνηση της διπλωματικής μου εργασίας.

Επίσης θα ήθελα να ευχαριστήσω τους Υποψήφιους Διδάκτορες του Τμήματος Η&ΗΝ Μηχανικών του Πανεπιστημίου Δυτικής Αττικής Ιωάννη Δόγα και Δημήτριο Καλύβα για το χρόνο που αφιέρωσαν και τις γνώσεις που μου μετέδωσαν για την ολοκλήρωση του πρακτικού κομματιού της εργασίας. Θα ήθελα να επίσης να ευχαριστήσω όλους τους καθηγητές του τμήματος για τις γνώσεις που μου μετέδωσαν, τον πολύτιμο χρόνο που αφιέρωσαν και το έργο που άσκησαν για να φτάσω σε αυτό το σημείο. Πολλές ευχαριστίες στους συναδέλφους και φίλους που είχαμε κοινή πορεία και με στηρίξανε τα όλα αυτά τα χρόνια.

Τέλος θα ήθελα ιδιαιτέρως να ευχαριστήσω την οικογένεια μου που για τη δύναμη και τη στήριξη τους να συνεχίζω στην ζωή μου εκπληρώνοντας τους στόχους μου.

ΠΙΝΑΚΑΣ ΣΥΜΒΟΛΩΝ-ΑΚΡΟΝΥΜΙΩΝ-ΣΥΝΤΟΜΓΡΑΦΙΩΝ

AMI	Advanced Metering Infrastructure
BMG	Brooklyn Microgrid Project
BFT	Byzantine Fault Tolerance
DAG	Directed Acyclic Graph
DApps	Decentralized Applications
DER	Distributed Energy Resources
DES	Distributed Energy Systems
DHT	Distributed Hash Table
DLT	Distributed Ledger Technologies
DPOS	Delegated Proof of Stake
DRES	Distributed Renewable Energy Systems
EOAs	Externally Owned Accounts
ESS	Energy Storage Systems
EV	Electric Vehicle
HAN	Home Area Network
IoE	Internet of Energy
IoT	Internet of Things
IT	Information Technology
KSI	Keyless Signature Infrastructure
P2P	Peer to Peer
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoC	Proof of Concept
PoET	Proof of Elapsed Time
PoS	Proof of Stake
PoW	Proof of Work
PV	Photovoltaic
RES	Renewable Energy Sources
RPi	Raspberry Pi
SG	Smart Grid
SM	Smart Meter
TEE	Trusted Execution Environment
TPS	Transactions Per Second
TSO	Transmission System Operator
UHV	Ultra High Voltage
WAN	Wide Area Network

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΕΙΣΑΓΩΓΗ:

Αντικείμενο, ερευνητικά ερωτήματα και διάρθρωση της εργασίας

Η αγορά εμπορίας ενέργειας είναι συνέπεια της εξέλιξης των Ηλεκτρικών δικτύων, η οποία έχει ρυθμιστεί σε μεγάλο βαθμό με αποτέλεσμα να έχει πρόσβαση μόνο μια μικρή ομάδα ενδιαφερόμενων μέχρι στιγμής. Η αυξανόμενη ενσωμάτωση των κατανεμημένων ενεργειακών πόρων (DER- Distributed Energy Resources) στο επίπεδο μικρομετατροπής, μεταβάλλει την εξάρτηση της υποδομής δικτύου από ορυκτά και πυρηνικά σε ανανεώσιμες πηγές ενέργειας, στοχεύοντας την έξυπνη διαχείριση και αποθήκευση της ενέργειας, αποτελώντας ένα νέο αντικείμενο έντονων ερευνών και πειραματισμών.

Τα παραδοσιακά ενεργειακά συστήματα είναι κεντρωμένης αρχιτεκτονικής· ένας μεγάλος αριθμός πελατών βρίσκεται σε μια ευρεία περιοχή, όπως ένα νησί ή μια χώρα. Η ενέργεια παρέχεται από μεγάλους σταθμούς ηλεκτροπαραγωγής που λειτουργούν σύμφωνα με έναν κεντρικό μηχανισμό συντονισμού. Αντιθέτως, ένα σύστημα αποκεντρωμένου ελέγχου αποτελείται από συσκευές που λειτουργούν ανεξάρτητα, βελτιώνοντας την ταχύτητα επικοινωνίας και την αντοχή σφάλματος. Η ανάγκη εφαρμογής ενός επιχειρηματικού μοντέλου διανομής ενέργειας στο Έξυπνο Δίκτυο (Smart Grid) αλλάζει ταχύτατα την εισαγωγή ανανεώσιμων πηγών ενέργειας (RES- Renewable Energy Sources) στο ηλεκτρικό δίκτυο.

Μια βασική ιδέα για το σχεδιασμό ενός SG είναι η εισαγωγή μικροδικτύων (Microgrids). Παράλληλα η ενεργοποίηση ενεργειακών συναλλαγών εντός / μεταξύ των Μικροδικτύων, θωρείται ένα από τα κυριότερα στοιχεία για την επίτευξη του επιθυμητού αποκεντρωμένου συστήματος, καθώς βελτιστοποιείται η ενσωμάτωση των Κατανεμημένων Ενεργειακών Πόρων (DER), ιδιαίτερα των RES, συμβάλλοντας παράλληλα στη σταθερότητα του δικτύου . Γενικά, ένα Μικροδίκτυο μπορεί να περιγραφεί ως συστοιχία φορτίων, όπως είναι οι αποκεντρωμένοι ενεργειακοί πόροι (DER) (π.χ. φωτοβολταϊκά πάνελ, γεννήτριες ντίζελ, συνδυασμένες θερμότητες κτλ.) και συστήματα αποθήκευσης ενέργειας (ESS- Energy Storage Systems) (π.χ. μπαταρία, EV- Electric Vehicles Κτλ.), τα οποία λειτουργούν με συντονισμό για την αξιόπιστη παροχή ηλεκτρικής ενέργειας. Το Μικροδίκτυο έχει δύο κύριες ιδιότητες: ενεργεί ως μία ενιαία ελεγχόμενη οντότητα με σαφή ηλεκτρικά όρια και μπορεί να

λειτουργήσει σε τέσσερις συνθήκες (σύνδεση με το δίκτυο, αποσύνδεση, αυτόνομη λειτουργία και επανασύνδεση) . Στην αυτόνομη λειτουργία, η ισχύς ανταλλάσσεται μόνο τοπικά μεταξύ φορτίων, DER και ESS. Τα Μικροδίκτυα θεωρούνται ως μια προσέγγιση για τη μείωση της αποκεντρωμένης ευελιξίας που εισάγεται από τις ανανεώσιμες πηγές ενέργειας μέσω νέων εννοιών ελέγχου .

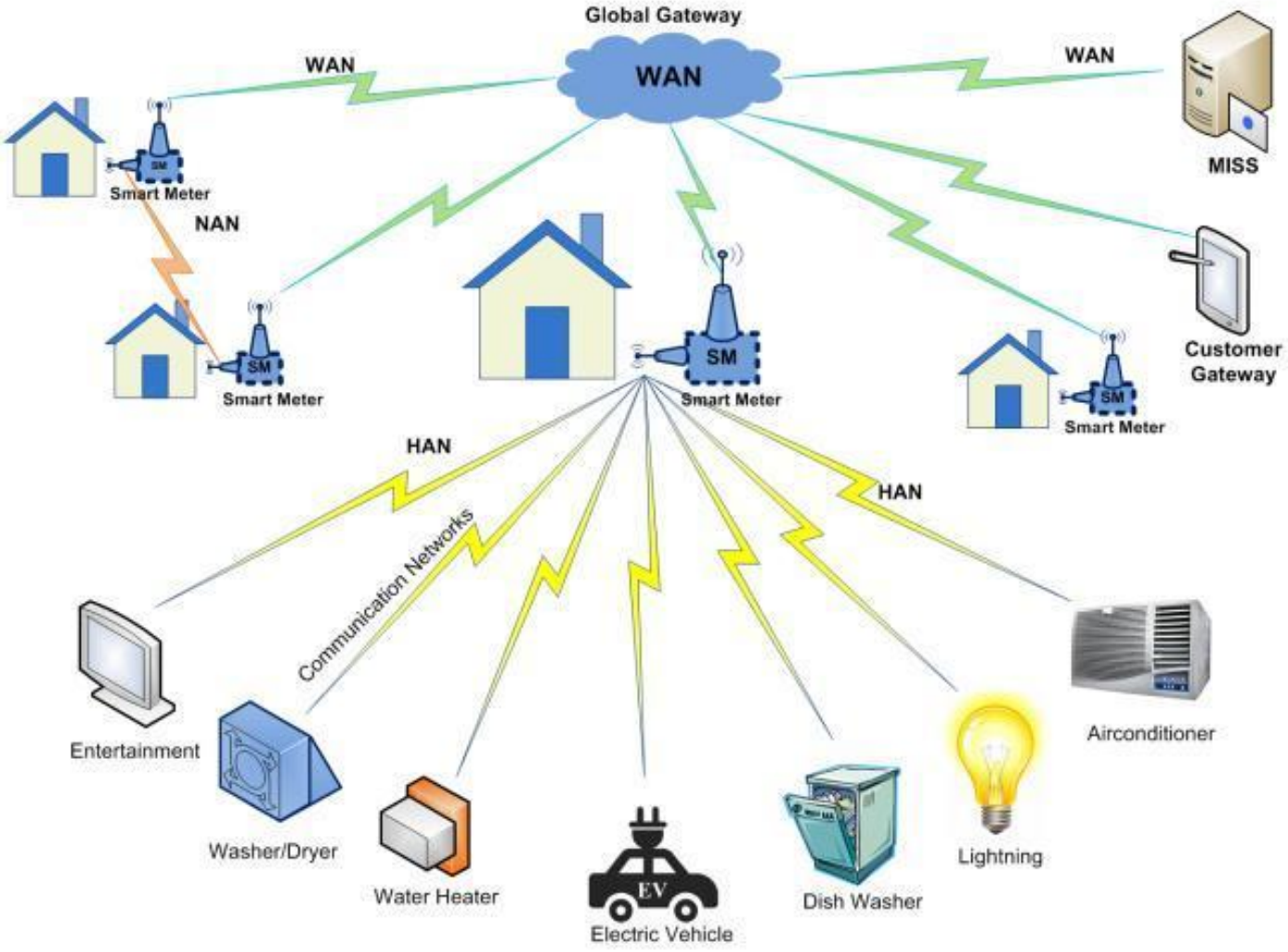
Το πρόβλημα που επικρατεί στις σύγχρονες κοινωνίες, είναι οι μεγάλες διακυμάνσεις στο ηλεκτρικό δίκτυο που προκαλούνται από την κατανεμημένη ολοκληρωμένη παραγωγή, λύση που έρχεται να δώσει η τοπική κατανάλωση ενέργειας του Μικροδικτύου. Εξαιτίας της ενεργειακής κρίσης, η κατανεμημένη παραγωγή και τα Μικροδίκτυα έχουν σημαντική άνοδο τα τελευταία χρόνια. Η τοπική κατανάλωση ενέργειας στο Μικροδίκτυο εξασφαλίζει την προώθηση της κατανεμημένης παραγωγής, ανάπτυξη του οποίου βασίζεται στην οικονομία. Η εισαγωγή του Μικροδικτύου στην αγορά μπορεί να αυξήσει τα έσοδα του παραγωγού και να μειώσει τα κόστη του καταναλωτή. Η τεχνολογία και η αγορά ενέργειας του μεγάλου πλέγματος δεν είναι κατάλληλες για το Μικροδίκτυο. Ως εκ τούτου, πολλοί ειδήμονες που σχετίζονται με την βιομηχανία της ενέργειας, προτείνουν την χρήση Blockchain για την διαχείριση των συναλλαγών ενέργειας και μικροπληρωμών, ώστε να πραγματοποιηθεί η τοπική κατανάλωση κατανεμημένης παραγωγής και η ανταλλαγή ηλεκτρικής ενέργειας από ομότιμους χρήστες στα πλαίσια ενός Μικροδικτύου. Με το Blockchain επιτυγχάνεται μια P2P (Peer-2-Peer) πλατφόρμα συναλλαγών, η οποία χρησιμοποιείται για την αποκεντρωμένη καταγραφή όλων των συναλλαγών που πραγματοποιούνται σε αυτό.

Οι προαναφερόμενες εφαρμογές ποικίλουν σε δυνατότητες και δεν αποσκοπούν στην επωφέληση σε συγκεκριμένη ομάδα ανθρώπων. Η ιδέα είναι, το Έξυπνο Δίκτυο (SG - Smart Grid) , επέκταση του Μικροδικτύου, να επιλύσει όλες τις μελλοντικές προκλήσεις στην παροχή ρεύματος. Το Smart grid θα εγκατασταθεί σε κάθε σπίτι για να συλλέξει δεδομένα κατανάλωσης ηλεκτρικής ενέργειας σε πραγματικό χρόνο και να τα αποστέλλει σε υπηρεσίες κοινής ωφέλειας, έτσι ώστε να προσφέρονται καλύτερες έξυπνες υπηρεσίες στο σπίτι.

Οι έξυπνες κοινότητες έχουν πολλά τυπικά παραδείγματα, όπως το έξυπνο σπίτι, το έξυπνο κτίριο ακόμη και την έξυπνη πανεπιστημιούπολη. Είναι κτισμένες πάνω από έξυπνη παροχή ρεύματος, βασισμένη σε Smart grid, η Δομή ενός έξυπνου

σπιτιού εξαρτάται από την προηγμένη υποδομή μέτρησης (AMI- Advanced Metering Infrastructure), η οποία αποτελεί μία από τις βασικές τεχνολογίες του SG δικτύου. Στην AMI, η αμφίδρομη επικοινωνία μεταξύ πελατών και υπηρεσίας επιτυγχάνεται με δύο τρόπους: με την υποστήριξη της ενημέρωσης και τις τεχνολογίες επικοινωνίας. Οι έξυπνοι μετρητές (SM- Smart Meters) έχουν αναπτυχθεί με σκοπό την παροχή αξιόπιστων ηλεκτρικών υπηρεσιών ενέργειας. Προκειμένου να επιτευχθεί ο βέλτιστος προγραμματισμός, SM εγκαθίστανται σε κάθε σπίτι προς συλλογή δεδομένων κατανάλωσης ηλεκτρικής ενέργειας σε πραγματικό χρόνο. Με βάση τα δεδομένα που συλλέγονται, μπορεί να σχεδιαστεί και το προφίλ κατανάλωσης ηλεκτρικής ενέργειας και στη συνέχεια να προσφερθεί δυναμική τιμολόγηση η οποία θα επιτρέπει στους χρήστες να επωφεληθούν ειδοποιώντας τους για τις αλλαγές στην συμπεριφορά ηλεκτρικής κατανάλωσης. Οι τρεις βασικές προκλήσεις που απορρέουν από την παραπάνω εφαρμογή σε ένα Smart grid, είναι η διαθεσιμότητα ενός αξιόπιστου μέρους για συγκέντρωση των δεδομένων του χρήστη, η απόκρυψη της σύνδεσης μεταξύ της πραγματικής ταυτότητας του χρήστη και του ψευδωνύμου του και τέλος η ταχύτητα με την οποία επιτυγχάνεται η εξακρίβωση της γνησιότητας. Προς αποφυγή των παραπάνω επιπλοκών, προτείνεται η χρήση της τεχνολογίας Blockchain στην οποία κάθε φορά ένας χρήστης θα επιλέγεται τυχαία για την συγκέντρωση των δεδομένων όλων των χρηστών και την καταγραφή αυτών στο Blockchain για την ακεραιότητα των μηνυμάτων. Ακόμη και ένας κακόβουλος χρήστης να επιλεγεί και να αλλοιώσει τα αρχεία, οι υπόλοιποι χρήστες θα μπορούν να τα βρουν εφόσον έχουν πρόσβαση σε όλα τα δεδομένα. Για την απόκρυψη της σύνδεσης μεταξύ ταυτότητας και ψευδωνύμου, προσφέρεται η δυνατότητα δημιουργίας πολλών ψευδωνύμων και η υποβολή της κατανάλωσης ηλεκτρικής ενέργειας δεδομένων υπό διαφορετικά ψευδώνυμα. Τέλος για την ταχύτερη εξακρίβωσης της αυθεντικότητας της ταυτότητας και την προστασία της ιδιωτικότητας χρησιμοποιείται το Bloom Filter για την έγκριση πραγματικών ψευδωνύμων και τον έλεγχο των πλαστών.

Κατ’ επέκταση όλων των παραπάνω, αναπτύσσεται η διαδικτυακή πύλη της τοπικής περιοχής δικτύου (HAN – Home Area Network) η οποία παρέχει ένα κανάλι επικοινωνίας μεταξύ της κύριας μονάδας μέτρησης και των μικροελεγτών, σχηματικό του οποίου φαίνεται παρακάτω.



Εικόνα 1 – Αρχιτεκτονική επικοινωνίας έξυπνης μέτρησης-HAN αλληλένδετα συνδεδεμένα με NAN και ανέβασμα δεδομένων στο WAN [16]

Ως αποτέλεσμα, οι μικροεπεξεργαστές και η διαχείριση φορτίου μπορούν να επεκταθούν σε μετρητή φορτίου για τη χρήση συστημάτων φόρτισης ηλεκτρικών οχημάτων (EV – Electric Vehicles) και άλλων φορτίων κατανάλωσης ενέργειας. Η πύλη του Δικτύου Γειτονικών Δικτύων (NAN) ενεργεί ως ενδιάμεσο επίπεδο που συνδέει πολλαπλά HAN στο Smart grid, με σκοπό τη συσσώρευση πληροφοριών κατανάλωσης ενέργειας και μετάδοσης τους στο ευρύ δίκτυο πληροφοριών (WAN – Wide Area Network) για παρακολούθηση και χρέωση αυτών.

Η σημερινή αγορά είναι κεντρωμένης αρχιτεκτονικής με ποικίλα μειονεκτήματα, καθιστώντας αναγκαία την ανάπτυξη μιας αποκεντρωμένης αρχιτεκτονικής, αποτελούμενη από Μικροδίκτυα, επιχειρήσεις κοινής ωφέλειας, χρηματοπιστωτικά ιδρύματα και από τους καταναλωτές-χρήστες. Οι Τεχνολογίες Κατανεμημένου

Μητρώου ((DLT – Distributed Ledger Technologies) μία από αυτές είναι και τα Blockchains) παρέχουν έναν αμετάβλητο, ασφαλή και απρόσκοπτο τρόπο αυτοματοποίησης και καταγραφής πολλαπλών συναλλαγών, όπως προαναφέρθηκε. Μπορούν να χρησιμοποιηθούν σε συνδυασμό με έξυπνους μετρητές ενέργειας για τη δημιουργία επιχειρηματικών μοντέλων οικονομίας στην ενέργεια έτσι ώστε οι μετρήσεις στην κατανάλωση ενέργειας να μπορούν να πιστοποιηθούν με ασφαλή τρόπο.

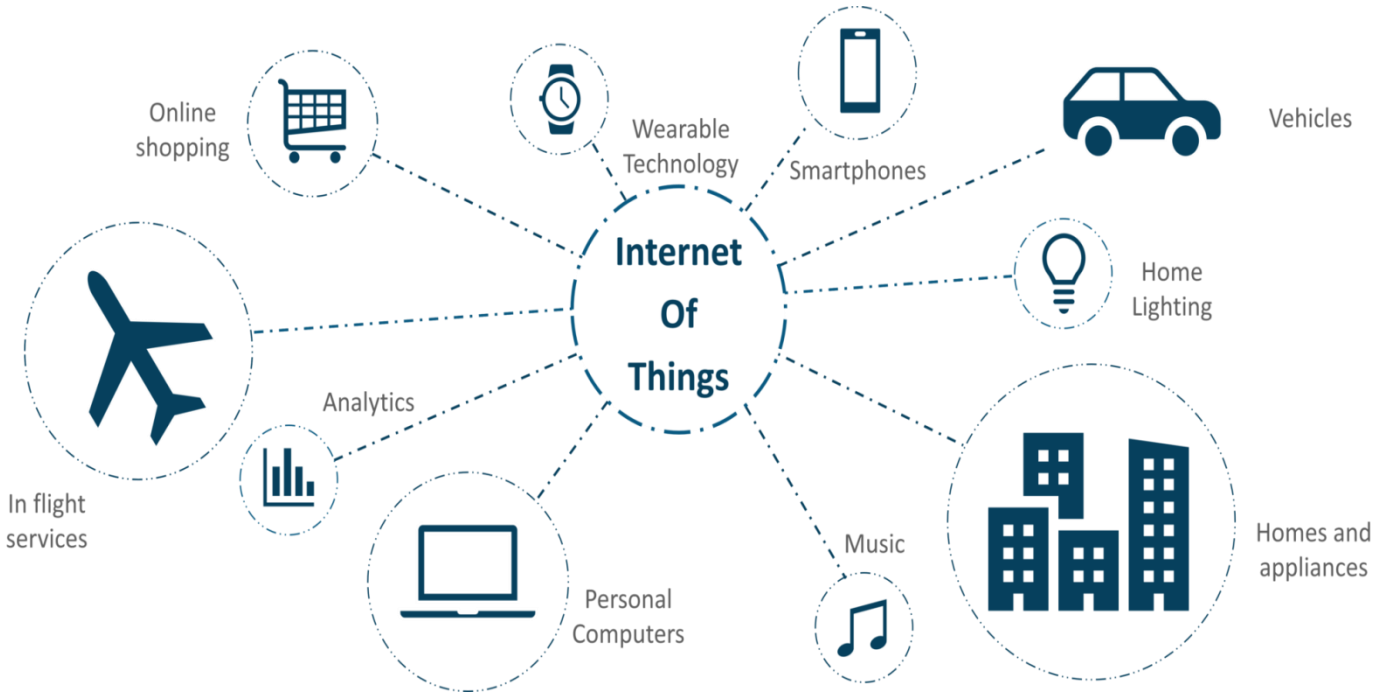
Αυτή η απαίτηση φαίνεται να ταιριάζει απόλυτα με την τεχνολογία Distributed Ledger και συγκεκριμένες αρχιτεκτονικές Blockchain, των οποίων η φύση είναι αποκεντρωμένη, και τα καθιστά κατάλληλα για την εφαρμογή αποδιοργανωτικών επιχειρηματικών διαδικασιών χρησιμοποιώντας έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές (DApps – Decentralized Applications).

Σε αυτή την πτυχιακή υποστηρίζεται ότι αυτή η μετατόπιση, η οποία σηματοδοτεί τη μετάβαση προς την επόμενη βιομηχανική εποχή, θέτει στο προσκήνιο της αγοράς μεγάλο αριθμό μικρότερων παραγωγών και, τελικά, όλους τους τελικούς χρήστες, με τη μορφή ενεργά απασχολούμενων προσώπων. Επιπλέον, αποδεικνύεται ότι οι υπολογιστικοί πόροι και η τεχνολογία για την υποστήριξη μιας ανοικτής, ευρέως προσβάσιμης και δίκαιης αγοράς ανταλλαγής από ομότιμους, είναι ήδη διαθέσιμες όπως το Διαδίκτυο των Αντικειμένων και οι τεχνολογίες επικοινωνιών καθώς και οι τεχνολογίες Blockchain για την υλοποίηση των πληρωμών που δεν θα βασίζονται σε κεντρικά ελεγχόμενα ιδρύματα όπως οι τράπεζες (διαμεσολαβητές). Στην πτυχιακή αυτή γίνεται βιβλιογραφική ανασκόπηση των τεχνολογιών που θα επιτρέψουν την εξέλιξη των Smart Grids στο Internet of Energy. Έμφαση δίνεται σε τεχνολογίες IoT και στην χρήση τους για την υλοποίηση Home Area Network, οι τεχνολογίες Smart meters και τα αντίστοιχα πρότυπα Αρχιτεκτονικής που έχουν επικρατήσει στα Smart Grids καθώς και οι τεχνολογίες Blockchain για την πραγματοποίηση μικροπληρωμών. Θα προταθεί και θα μελετηθεί διάταξη υλοποίησης πειραματικής διάταξης που θα ενσωματώνει τις προαναφερθείσες τεχνολογίες βασισμένη σε open-source projects.

1. Θεωρητικό Υπόβαθρο

1.1 Εισαγωγή στο Διαδίκτυο των Πραγμάτων (IoT)

Το Διαδίκτυο των Πραγμάτων είναι ένα αναδυόμενο σύνολο τεχνικών, κοινωνικών και οικονομικών παραγόντων. Τα καταναλωτικά προϊόντα, τα αυτοκίνητα και τα φορτηγά, τα βιομηχανικά εξαρτήματα, οι αισθητήρες και άλλα καθημερινά αντικείμενα συνδυάζονται με το Διαδίκτυο και με ισχυρές αναλυτικές δυνατότητες δεδομένων υποσχόμενα να μεταμορφώσουν τον τρόπο που ζούμε και εργαζόμαστε. Μέσω της πρόσβασης στο διαδίκτυο δίνεται η δυνατότητα απομακρυσμένου ελέγχου τους και επίβλεψής τους από οποιοδήποτε σημείου του κόσμου. Συνεπώς, προσφέρουν σύνδεση του φυσικού κόσμου με υπολογιστικά συστήματα, το οποίο αυξάνει την αποτελεσματικότητα, την ακρίβεια και την αποδοτικότητα. Οι προβλέψεις για τον αντίκτυπο του IoT στο Internet και στην οικονομία είναι εντυπωσιακοί, με ορισμένες να ξεπερνούν τις 100 δισεκατομμύρια συνδεδεμένες συσκευές IoT και με παγκόσμιο οικονομικό αντίκτυπο άνω των 11 τρισεκατομμυρίων δολαρίων μέχρι το 2025. [4] [5]



Εικόνα 2- Εφαρμογές Διαδικτύου των Πραγμάτων/Παραδείγματα IoT [5]

Ταυτόχρονα, όμως, το Διαδίκτυο των πραγμάτων εγείρει σημαντικές προκλήσεις που θα μπορούσαν να παρεμποδίσουν την αξιοποίηση των δυνατοτήτων του. Η διάδοση του IoT και η απήχηση στο ευρύ κοινό, προσελκύει κακόβουλους χρήστες για την πειρατεία των συσκευών που συνδέονται με το Διαδίκτυο, προκαλώντας την ανησυχία των υπολοίπων χρηστών σχετικά με την προστασία της ιδιωτικής τους ζωής. Οι τεχνικές προκλήσεις παραμένουν και ως εκ τούτου εμφανίζονται νέες πολιτικές, νομικές και αναπτυξιακές εμφανίζονται για την αντιμετώπιση τους**.**

Το Διαδίκτυο των πραγμάτων ασχολείται με ένα εκτεταμένο σύνολο ιδεών που είναι πολύπλοκες και αλληλένδετες από διαφορετικές οπτικές γωνίες. Βασικές έννοιες που χρησιμεύουν ως βάση για τη διερεύνηση των ευκαιριών και των προκλήσεων του IoT περιλαμβάνουν:

IoT διευκρινίσεις του όρου: Ο όρος IoT (Internet of Things) αναφέρεται στις ενσωματωμένες συσκευές που αλληλεπιδρούν με τον φυσικό κόσμο μέσω σύνδεσης στο Internet, προκειμένου να παρακολουθούν και να εκτελούν συγκεκριμένες εργασίες σε αυτούς που τις χρησιμοποιούν. Ένας πιο χαρακτηριστικός ορισμός από το ITU έργο XX1 2015 στο Διαδίκτυο των Πραγμάτων, δηλώνει ότι είναι μία παγκόσμια υποδομή της πληροφορίας για την κοινωνία που επιτρέπει προηγμένες υπηρεσίες μέσω της διασύνδεσης (φυσικών και εικονικών) πραγμάτων που βασίζονται σε υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών. Ο όρος Διαδίκτυο των Πραγμάτων επινοήθηκε από τον Kevin Ashton το 1999 για να περιγράψει ένα σύστηνα όπου το Διαδίκτυο συνδέεται με τον φυσικό κόσμο μέσω πανταχού παρόντων αισθητήρων.

Τεχνολογίες ενεργοποίησης: Η έννοια του συνδυασμού υπολογιστών, αισθητήρων και δικτύων για την παρακολούθηση και τον έλεγχο των συσκευών υπάρχει εδώ και δεκαετίες. Η πρόσφατη συρροή αρκετών τάσεων στην τεχνολογική αγορά, ωστόσο, φέρνει το Διαδίκτυο των Πραγμάτων πιο κοντά στην διαδεδομένη πραγματικότητα. Αυτό περιλαμβάνει τη δυνατότητα σύνδεσης στο διαδίκτυο, τη διαδεδομένη υιοθέτηση δικτύων βασισμένων σε

IP, υπολογιστικών οικονομικών , προόδου στην ανάλυση δεδομένων και της ανόδου του Cloud Computing.

Μοντέλα συνδεσιμότητας: Οι εφαρμογές IoT χρησιμοποιούν διαφορετικά μοντέλα τεχνικών επικοινωνιών, τα οποία έχουν τα δικά τους χαρακτηριστικά. Τέσσερα κοινά μοντέλα επικοινωνιών που περιγράφονται από το Συμβούλιο Αρχιτεκτονικής Διαδικτύου είναι: Συσκευή-συσκευή (device), Συσκευή-προς-νέφος(cloud), Συσκευή προς πύλη (gateway) και κοινή χρήση δεδομένων. Αυτά τα μοντέλα υπογραμμίζουν την ευελιξία στους τρόπους με τους οποίους οι συσκευές IoT μπορούν να συνδεθούν και να δώσουν αξία στον χρήστη.

Δυνατότητα μετασχηματισμού:. Η δυνητική πραγματοποίηση αυτού του αποτελέσματος - ένας "υπερσυνδεδεμένος κόσμος" - αποδεικνύει τη γενικότερη φύση της ίδιας της αρχιτεκτονικής του Διαδικτύου, η οποία δεν θέτει εγγενείς περιορισμούς στις εφαρμογές ή τις υπηρεσίες που μπορούν να κάνουν χρήση της τεχνολογίας.

Πέντε τομείς βασικών θεμάτων IoT εξετάζονται για να διερευνηθούν μερικές από τις πιο βασικές προκλήσεις και ζητήματα που σχετίζονται με την εκάστοτε τεχνολογία. Αυτοί οι τομείς περιλαμβάνουν 1) την ασφάλεια, 2) την ιδιωτικότητα, 3) την διαλειτουργικότητα και τα πρότυπα, 4) νομικά, ρυθμιστικά και δικαιωματικά πλαίσια, 5) αναδυόμενη οικονομία και ανάπτυξη.

1) Ασφάλεια

Ενώ οι εκτιμήσεις ασφάλειας δεν είναι καινούργιες στο πλαίσιο της τεχνολογίας των πληροφοριών, τα χαρακτηριστικά πολλών εφαρμογών του IoT παρουσιάζουν νέες και μοναδικές προκλήσεις σε επίπεδο ασφαλείας. Η ασφάλεια και η αντιμετώπιση των προκλήσεων αυτών πρέπει να αποτελεί θεμελιώδη προτεραιότητα στις υπηρεσίες του διαδικτύου. Οι χρήστες πρέπει να εμπιστεύονται ότι οι συσκευές IoT και οι σχετικές υπηρεσίες δεδομένων είναι ασφαλείς από τρωτά σημεία, ειδικά καθώς η τεχνολογία αυτή γίνεται όλο

και πιο διαδεδομένη και ενσωματώνεται σθεναρά στην καθημερινότητά μας. Οι μη ασφαλείς συσκευές και υπηρεσίες IoT μπορούν να χρησιμεύσουν ως πιθανά σημεία εισόδου για επιθέσεις στον κυβερνοχώρο και να εκθέσουν τα δεδομένα χρήστη αφήνοντας τις ροές δεδομένων ανεπαρκώς προστατευμένα.

Κατ' αρχήν, οι προγραμματιστές και οι χρήστες συσκευών και συστημάτων IoT έχουν συλλογική υποχρέωση να διασφαλίσουν ότι δεν εκθέτουν τους χρήστες και το Διαδίκτυο σε δυνητική ζημιά. Ως συνέπεια, χρειάζεται μια συλλογική προσέγγιση για την ασφάλεια και την ανάπτυξη αποτελεσματικών και κατάλληλων λύσεων για την κλίμακα και την πολυπλοκότητα των προκλήσεων αυτών.

2) Ιδιωτικότητα

Το πλήρες δυναμικό του IoT εξαρτάται από στρατηγικές που σέβονται τις επιμέρους επιλογές απορρήτου σε ένα ευρύ φάσμα προσδοκιών. Οι ροές δεδομένων και η εξειδίκευση των χρηστών που παρέχονται από συσκευές IoT μπορούν να ξεκλειδώσουν την απίστευτη και μοναδική αξία των χρηστών του Διαδικτύου, αλλά οι ανησυχίες σχετικά με την ιδιωτικότητα τους ενδέχεται να εμποδίσουν την πλήρη υιοθέτηση του Διαδικτύου των Πραγμάτων. Αυτό σημαίνει ότι τα δικαιώματα απορρήτου και ο σεβασμός της ιδιωτικής ζωής των χρηστών αποτελούν αναπόσπαστο μέρος της διασφάλισης της εμπιστοσύνης των χρηστών στο Διαδίκτυο, τις συνδεδεμένες συσκευές και τις περαιτέρω υπηρεσίες. Πράγματι, το Διαδίκτυο των πραγμάτων επαναπροσδιορίζει τη συζήτηση σχετικά με τα ζητήματα ιδιωτικής ζωής, καθώς πολλές εφαρμογές μπορούν να αλλάξουν δραματικά τους τρόπους συλλογής, ανάλυσης, χρήσης και προστασίας των προσωπικών δεδομένων. θα πρέπει να αναπτυχθούν στρατηγικές που σέβονται τις επιμέρους επιλογές προστασίας της ιδιωτικής ζωής σε ένα ευρύ φάσμα προσδοκιών, ενώ ταυτόχρονα θα ενθαρρύνεται η καινοτομία στις νέες τεχνολογίες και υπηρεσίες.

3) Διαλειτουργικότητα/Πρότυπα

Ένα κατακερματισμένο περιβάλλον ιδιόκτητων τεχνικών υλοποιήσεων IoT θα εμποδίσει την αξία για τους χρήστες και τη βιομηχανία. Ενώ η πλήρης διαλειτουργικότητα μεταξύ των προϊόντων και των υπηρεσιών δεν είναι πάντοτε εφικτή ή απαραίτητη, οι αγοραστές ενδέχεται να διστάζουν να αγοράζουν προϊόντα και υπηρεσίες IoT εάν υπάρχει έλλειψη ευελιξίας, υψηλή πολυπλοκότητα ιδιοκτησίας και ανησυχία σχετικά με την εξασφάλιση του πωλητή.

Επιπλέον, οι κακώς σχεδιασμένες και διαμορφωμένες συσκευές IoT ενδέχεται να έχουν αρνητικές συνέπειες για τους πόρους δικτύωσης. Τα κατάλληλα πρότυπα, τα μοντέλα αναφοράς και οι βέλτιστες πρακτικές θα βοηθήσουν επίσης στον περιορισμό του πολλαπλασιασμού των συσκευών που ενδέχεται να λειτουργούν με διαταραγμένους τρόπους στο Διαδίκτυο. Η χρήση γενικών, ανοικτών και ευρέως διαθέσιμων προτύπων ως τεχνικών δομικών στοιχείων για συσκευές και υπηρεσίες IoT (όπως το πρωτόκολλο του Διαδικτύου) θα υποστηρίξει τα μεγαλύτερα οφέλη για τους χρήστες, την καινοτομία και τις οικονομικές ευκαιρίες.

4) Νομικά/Ρυθμιστικά/Δικαιωματικά Πλαίσια

Η χρήση συσκευών διαδικτύου εγείρει πολλά νέα ρυθμιστικά και νομικά ζητήματα καθώς και ενισχύει τα υφιστάμενα νομικά ζητήματα γύρω από το Διαδίκτυο. Οι ερωτήσεις ποικίλουν και ο ταχύς ρυθμός αλλαγής στην τεχνολογία του Διαδικτύου υπερβαίνει συχνά την ικανότητα προσαρμογής των συνδεδεμένων πολιτικών, νομικών και ρυθμιστικών δομών.

Ένα σύνολο ζητημάτων περιβάλλει τις ροές δεδομένων, οι οποίες συμβαίνουν όταν οι συσκευές του Διαδικτύου συλλέγουν δεδομένα σχετικά με άτομα που ανήκουν σε μία δικαιοδοσία και τα μεταδίδουν σε άλλη δικαιοδοσία με διαφορετικούς νόμους προστασίας δεδομένων. Επιπλέον, τα δεδομένα που συλλέγονται από συσκευές IoT είναι μερικές φορές ευαίσθητα σε κατάχρηση, ε προκαλώντας διακρίσεις για ορισμένους χρήστες.

Ενώ οι νομικές και κανονιστικές προκλήσεις είναι ευρείες και πολύπλοκες, η υιοθέτηση των κατευθυντήριων αρχών της κοινωνίας του Διαδικτύου για την προώθηση της ικανότητας του χρήστη να συνδέει, να μιλάει, να καινοτομεί, να μοιράζεται, να επιλέγει και να εμπιστεύεται είναι βασικοί παράγοντες για την εξέλιξη νόμων και κανονισμών του IoT που επιτρέπουν τα δικαιώματα του χρήστη.

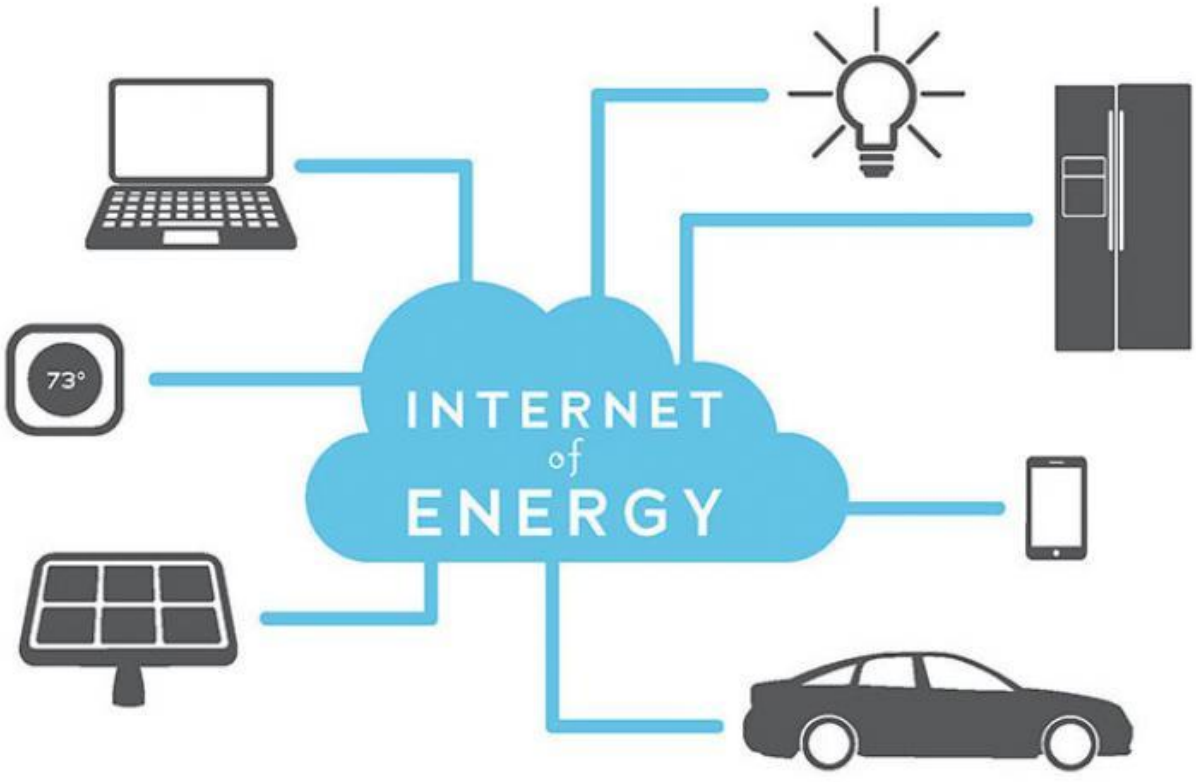
5) Αναδυόμενη Οικονομία και Ανάπτυξη

Το IoT υπόσχεται την παροχή κοινωνικών και οικονομικών οφελών στις αναδυόμενες και αναπτυσσόμενες οικονομίες. Αυτό περιλαμβάνει τομείς όπως η βιώσιμη γεωργία, η ποιότητα των υδάτων και η χρήση τους, η υγειονομική περίθαλψη, η εκβιομηχάνιση και η περιβαλλοντική διαχείριση. Οι αναπτυσσόμενες περιφέρειες θα πρέπει επίσης να ανταποκριθούν για να συνειδητοποιήσουν τα πιθανά οφέλη. Επιπρόσθετα, θα πρέπει να αντιμετωπιστούν οι μοναδικές ανάγκες και προκλήσεις της εφαρμογής σε λιγότερο ανεπτυγμένες περιφέρειες, συμπεριλαμβανομένης της υποδομής που υπάρχει, των κινήτρων για την αγορά και τις επενδύσεις, των τεχνικών απαιτήσεων και των πόρων πολιτικής.

Το Διαδίκτυο των πραγμάτων προσφέρει έναν επαναστατικό, πλήρως συνδεδεμένο "έξυπνο" κόσμο, καθώς οι σχέσεις μεταξύ αντικειμένων, περιβάλλοντος και ανθρώπων γίνονται πιο στενά συνδεδεμένες.

1.2 Εισαγωγή στο Διαδίκτυο της Ενέργειας (IoE)

Το Διαδίκτυο της Ενέργειας (IoE) είναι η εφαρμογή της τεχνολογίας Internet of Things (IoT) σε κατανεμημένα ενεργειακά συστήματα (DES – Distributed Energy Systems) για τη βελτιστοποίηση της αποδοτικότητας των ενεργειακών υποδομών και τη μείωση της σπατάλης. Αυτό σημαίνει ότι έχει τεράστιο αντίκτυπο στον τομέα της τεχνολογίας. Το IoE αναφέρεται στην αναβάθμιση και αυτοματοποίηση των υποδομών ηλεκτρικής ενέργειας για τους παραγωγούς. Ο όρος προέρχεται από την ολοένα και πιο εξέχουσα αγορά της τεχνολογίας του Διαδικτύου των Πραγμάτων, η οποία βοήθησε στην ανάπτυξη των κατανεμημένων ενεργειακών συστημάτων που συνθέτουν το Διαδίκτυο της Ενέργειας. Ένα παράδειγμα της τεχνολογίας IoE περιλαμβάνει τη χρήση έξυπνων αισθητήρων, κοινών μεταξύ άλλων εφαρμογών τεχνολογίας IoT, που επιτρέπουν την παρακολούθηση της ισχύς, την έξυπνη αποθήκευση και την ενσωμάτωση ανανεώσιμης ενέργειας.



Εικόνα 3 – Κατανεμημένη μεταφορά ενεργείας μέσω του Διαδικτύου των Πραγμάτων (IoT) , το Διαδίκτυο της Ενέργειας (IoE) [12]

1.2.1 Από το Smart Grid στο Διαδίκτυο της Ενέργειας

Ο στόχος του IoE είναι να συλλέξει, να οργανώσει και να μετατρέψει τις πληροφορίες από τις μεμονωμένες συσκευές του μεγάλου πλέγματος σε όλο το δίκτυο, διαθέσιμες σε όλους τους άλλους συμμετέχοντες στη διαχείρισή του, απλά και γρήγορα. Το μείζων ζήτημα είναι ο όγκος των δεδομένων και ο χρόνος που απαιτείται για την ανάλυση των πληροφοριών, καθώς αυξάνεται ο αριθμός των συσκευών και η ποσότητα πληροφοριών για τα δίκτυα διανομής. Ο όγκος και η κλίμακα των δεδομένων μπορούν να ξεπεραστούν χρησιμοποιώντας ασφαλή επικοινωνιακή δικτύωση των συσκευών, καθώς και IT (Information Technology) τελευταίας τεχνολογίας, όπως το cloud computing. Καθώς οι πληροφορίες των συσκευών καταναλώνονται από μια πλατφόρμα που βασίζεται σε cloud, η ενοποίηση και η ανταλλαγή πληροφοριών μπορεί να απλοποιηθεί χρησιμοποιώντας εφαρμογές λογισμικού που εκτελούνται στην πλατφόρμα cloud. Το cloud αυτομάτως θα γίνει μία βάση δεδομένων για τις διάφορες εφαρμογές που θα μπορούν να τα χρησιμοποιήσουν. Αυτό μπορεί να εξαλείψει την ανάγκη για υπηρεσίες ενοποίησης μεταξύ εφαρμογών. Ένα έξυπνο σύστημα διαχείρισης ενέργειας θα διατηρήσει σταθερό το δίκτυο εξισορροπώντας την παραγόμενη ενέργεια από όλες τις πηγές με την ηλεκτρική ενέργεια που καταναλώνεται.

Επιπλέον, το IoE θα επιτρέψει στους καταναλωτές και τους πελάτες να συντονίσουν την προσφορά και τη ζήτηση αυτόνομα μεταξύ τους. Επίσης είναι εξοπλισμένο με έξυπνα συστήματα πρόγνωσης που χρησιμοποιούν προβλέψεις καιρού, αναμενόμενες ροές κυκλοφορίας και άλλες πληροφορίες για την πρόβλεψη της μελλοντικής ενεργειακής ζήτησης.

Εικόνα 4 – Η χρήση του IoE για τη βέλτιστη διαχείριση του Smart Grid [13]

1.2.2 Ενεργειακά Προβλήματα που λύνει το Διαδίκτυο της Ενέργειας

Το αμερικανικό Συμβούλιο για μια ενεργειακά αποτελεσματικότερη οικονομία, κάθε δύο χρόνια απελευθερώνει την διεθνή scorecard η οποία κατατάσσει τους σημαντικότερους ενεργειακούς χρήστες παγκοσμίως με βάση την αποδοτικότητά τους. Καθώς η ζήτηση για ενέργεια συνεχίζει να αυξάνεται, όλες οι χώρες θα χρειαστεί να καταβάλουν προσπάθειες για να μεγιστοποιήσουν την ενεργειακή τους αποδοτικότητα και να σταματήσουν τις σημαντικές απώλειες ενέργειας που βιώνουμε αυτήν την περίοδο.

Το πρόβλημα της σπατάλης είναι ιδιαίτερα εμφανές στο πλαίσιο της βιομηχανίας ανανεώσιμων πηγών ενέργειας. Για παράδειγμα, το 2016 η Κίνα σπατάλησε τόση ενέργεια που θα μπορούσε να τροφοδοτήσει ολόκληρη την πόλη του Πεκίνου για ένα ολόκληρο έτος.

Το IoE βοηθά τις χώρες να διαχειριστούν τη ζήτηση ενέργειας, επιτρέποντας στους σταθμούς ηλεκτροπαραγωγής να παράγουν περισσότερη ηλεκτρική ενέργεια σε ώρες αιχμής και λιγότερο όταν οι απαιτήσεις κατανάλωσης είναι χαμηλές. Η ευρεία εξάπλωση αυτής της τεχνολογίας θα μπορούσε να αποτρέψει τις χώρες που αντιμετωπίζουν διακοπές ρεύματος στο μέλλον. Η βρετανική εταιρεία κοινής ωφέλειας National Grid δήλωσε ότι μεταξύ 30% και 50% των διακυμάνσεων στο δίκτυο θα μπορούσε να λυθεί τόσο από τα

νοικοκυριά όσο και από τις επιχειρήσεις που προσαρμόζουν τη ζήτηση τους σε ώρες αιχμής.[6]

Είναι αυτονόητο ότι η αποδοτική χρήση της ενέργειας είναι κρίσιμη για μια βιώσιμη πόλη. Κάτι που συχνά θεωρείται δεδομένο, αλλά η αυξανόμενη ζήτηση για ενέργεια χρήζει απαραίτητη την βελτίωση στον τρόπο με τον οποίο την διαχειριζόμαστε. Όχι μόνο η ζήτηση στα σπίτια μας αυξάνεται καθώς αυξάνεται ο πληθυσμός (σύμφωνα με τον ΟΗΕ, σχεδόν το ένα τρίτο του παγκόσμιου πληθυσμού θα ζει σε αστικούς οικισμούς μέχρι το 2030) και ο αριθμός των συσκευών που χρησιμοποιούμε είναι μεγαλύτερος, αλλά άλλες θεμελιώδεις πτυχές της καθημερινής ζωής αλλάζει τη σχέση μας με την ενέργεια. Για παράδειγμα, τα ηλεκτρικά αυτοκίνητα που θεωρούνται βασικό μέρος της καταπολέμησής από την αλλαγή του κλίματος - συμβάλλοντας στη μείωση των εκπομπών διοξειδίου του άνθρακα. Όμως, αν όλοι οι ιδιοκτήτες ενός οχήματος το μετέτρεπαν σε μια ηλεκτρική εναλλακτική λύση και στη συνέχεια όλοι τους το συνέδεαν στο δίκτυο φόρτισης, η προκύπτουσα αύξηση θα ήταν πολύ μεγαλύτερη της τρέχουσας υποδομής για να μπορεί να χειριστεί. Έτσι, η έξυπνη τεχνολογία IoT συμβάλλει στην επίλυση προβλημάτων όπως αυτά, καθώς και στην παροχή μεγαλύτερης γνώσης και ελέγχου στους καταναλωτές σχετικά με την ποσότητα ενέργειας που καταναλώνουν.[11]

Πολλοί καταναλωτές σε όλο τον κόσμο θα γνωρίσουν την έννοια των έξυπνων μετρητών (SM – Smart Meters). Οι συσκευές έχουν σχεδιαστεί για να επικοινωνούν απευθείας μεταξύ του ηλεκτρικού ρεύματος ή του μετρητή αερίου του σπιτιού π.χ. και του προμηθευτή ενέργειας. Αυτή η σύνδεση σε πραγματικό χρόνο σημαίνει ότι οι καταναλωτές μπορούν να δουν ακριβώς πόση ενέργεια καταναλώνουν και το κόστος που προκύπτει. Έτσι, είτε ενεργοποιείται η θέρμανση είτε απλά απενεργοποιώντας τα φώτα που δεν χρησιμοποιούνται, οι καταναλωτές μπορούν να λάβουν μια τεκμηριωμένη απόφαση για το τι πρέπει να χρησιμοποιήσουν και πώς μπορούν να συμπεριφέρονται για το χαμηλότερο δυνατό κόστος. Ταυτόχρονα, οι επιχειρήσεις κοινής ωφέλειας μπορούν να προσφέρουν ακριβή χρέωση ανάλογα με την κατανάλωση ενέργειας σε πραγματικό χρόνο και να ελέγχουν προσεκτικά και να εξισορροπούν τη ζήτηση και την προσφορά.

Αυτή η πολυπλοκότητα απαιτεί έξυπνη λύση και εδώ, μπαίνουν τα Smart Grids. Συνδέοντας κάθε έξυπνο μετρητή, ηλιακό πάνελ, ηλεκτρικό όχημα και κάθε άλλο ενεργειακό στοιχείο, ένα Smart Grid μπορεί να αναλύσει αμέτρητα σημεία δεδομένων για να βοηθήσει στη διαχείριση της ροής ενέργειας - διαθέσιμη και αναγκαία - την κατάλληλη στιγμή, στα σωστά σημεία , για την τελική διαχείριση έτσι ώστε να γίνει αποδοτικότερο στον καταναλωτή.

1.2.3 Έξυπνα Κτίρια

Η απόδοση της ισχύος είναι ένα μεγάλο μέρος του IoT στην οικοδόμηση της ενέργειας. Ο περιορισμός των φορτίων είναι ένας αποτελεσματικός τρόπος στην δόμηση της ενέργειας, αλλά η αυτοματοποίηση και ο έλεγχος των κτιρίων είναι μια άλλη μεγάλη λύση. Ορισμένες επιλογές αύξησης της ενεργειακής απόδοσης ενός κτιρίου είναι: [10]

- Την αποδοτική χρήση του HVAC (Heating Venting Air Condition) συστήματος
- Αυτόματη απενεργοποίηση φώτων όταν ένα δωμάτιο δεν είναι κατειλημμένο
- Εξισορρόπηση της ροής του αέρα για χρήση αυτού όταν χρειάζεται
- Επιβεβαίωση της ελάχιστης δυνατής ισχύος των συσκευών

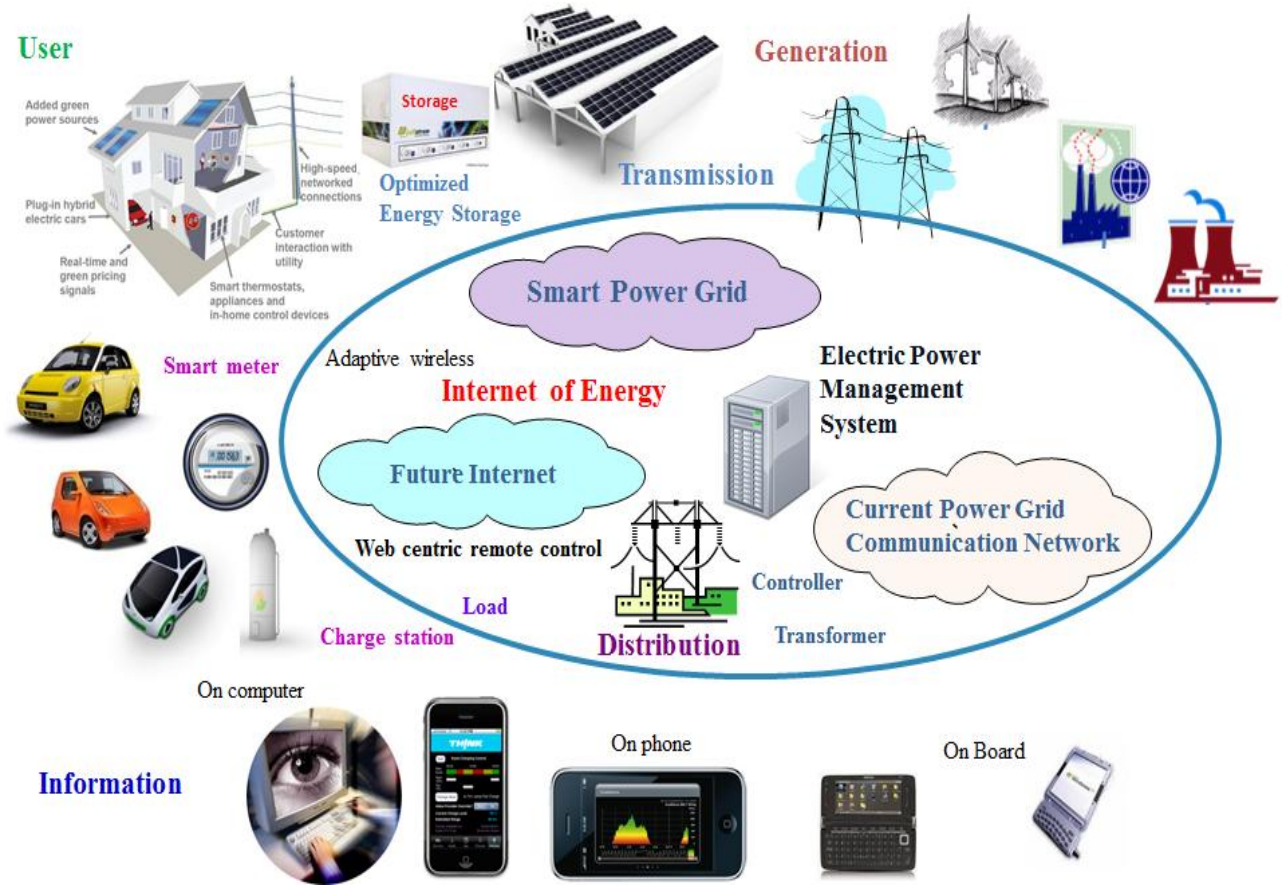
1.2.4 Το Μέλλον του Διαδικτύου της Ενέργειας (IoE)

Μια πιθανή λύση στο πρόβλημα της αναποτελεσματικότητας της ενέργειας είναι η μετάδοση εξαιρετικά υψηλής τάσης (UHV – Ultra High Voltage), ένα σύστημα που επιτρέπει την ταχεία μετάδοση ενέργειας σε μεγάλες αποστάσεις. Το UHV λύνει το πρόβλημα της παραγωγής ενέργειας που βρίσκεται πολύ μακριά από τα κέντρα φορτίου. Η Κίνα εφάρμοσε για πρώτη φορά το UHV το 2009, αλλά η ανάπτυξή της συνεχώς επεκτείνεται για να καλύψει όλη τη ζήτηση.

Η Κίνα προσπαθεί να αυτοματοποιήσει τη διανομή και να προσθέσει περισσότερους πόρους για να καλύψει τη ζήτηση, συμπεριλαμβανομένων περισσότερων σταθμών φόρτισης για ηλεκτρικά αυτοκίνητα. Κατασκευάζει επίσης τοποθεσίες αποθήκευσης, δίνοντας βάση σε εκείνες τις πόλεις που

χρησιμοποιούν το μεγαλύτερο μέρος της ενέργειας, προκειμένου να αποθηκεύουν την πλεονάζουσα ενέργεια αποτελεσματικά. Αυτό θα έχει οικονομικά οφέλη για τις εταιρείες που προμηθεύουν ανανεώσιμες πηγές ενέργειας, όπως είναι η ηλιακή και η αιολική, εξαιτίας του γεγονότος ότι περισσότερη ενέργεια θα διατηρηθεί και θα πουληθεί και αυτό θα έχει ως αποτέλεσμα χαμηλά κόστη αποθήκευσης.

Τα επόμενα χρόνια, καθώς ο κόσμος εργάζεται για τη εύρεση ανανεώσιμων πηγών ενέργειας, αναμένεται να μειωθεί η χρήση μη ανανεώσιμων πόρων, πράγμα που σημαίνει ότι θα μειωθεί η ανάγκη για παρωχημένες υποδομές που χειρίζονται πόρους όπως ο άνθρακας και το πετρέλαιο.[7]



Εικόνα 5 – Η αρχιτεκτονική του IoE στη δόμηση έξυπνης πόλης [14]

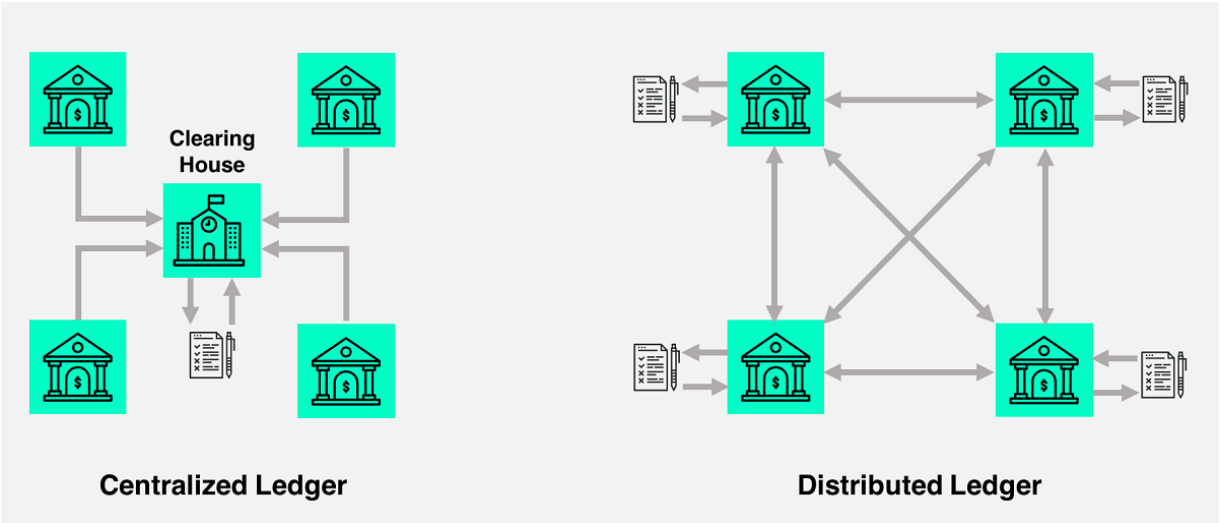
1.3 Εισαγωγή στις Τεχνολογίες Κατανεμημένου Μητρώου (DLT)

Η υλοποίηση ενός Smart Grid των προαναφερόμενων προδιαγραφών, χρήζει απαραίτητης εφαρμογής Τεχνολογιών Κατανεμημένου Μητρώου(DLT – Distributed Ledger Technologies), μέσω της οποίας θα δημιουργηθεί αρχικά ένα μικροδίκτυο ομότιμων χρηστών και συνδικαιούχων στην συναλλαγή της ενέργειας, έναντι του Large grid.

Όλες οι Blockchain τεχνολογίες είναι DLT, αλλά δεν είναι όλες οι DLT τεχνολογίες Blockchain. Παρακάτω εξηγείται η έννοια των DLT τεχνολογιών και θα παρουσιαστούν κάποιες βασικές τεχνολογίες κατανεμημένου μητρώου που υπάρχουν όπως είναι αντίστοιχα τα Blockchain. Η πτυχιακή αυτή εστιάζει στην τεχνολογία Blockchain πάνω στην οποία θα γίνει και η προσομοίωση ενός μικροδικτύου βασισμένο στα εργαλεία του Ethereum, οι άλλες αναφέρονται εγκυκλοπαιδικά για εκπαιδευτικούς λόγους.

1.3.1 Προσδιορισμός DLT

Η DLT τεχνολογία είναι πρακτικά μία βάση δεδομένων η οποία μοιράζεται δεδομένα μεταξύ υπολογιστών και χρηστών σε όλο τον κόσμο, δημιουργώντας ένα αποκεντρωμένο περιβάλλον έναντι του κεντρικού που ήδη υπάρχει. Η βάση αυτή δεδομένων υπάρχει δηλαδή μεταξύ πολλών τοποθεσιών και συμμετεχόντων. Εν αντιθέσει, οι περισσότερες εταιρείες σήμερα χρησιμοποιούν κεντρική βάση δεδομένων με σταθερή τοποθεσία. Αυτό έχει ως κύριο μειονέκτημα να υφίσταται ένα μόνο σημείο αποτυχίας του συστήματος. Δεδομένου ότι αποτυγχάνει το σημείο αυτό, όλο το σύστημα μετά δεν θα είναι ενεργό μέχρι το σημείο αυτό να ξαναγίνει λειτουργικό.



Εικόνα 6 – Διαφορά Κεντρικής και Τεχνολογίας Κατανεμημένου Μητρώου [21]

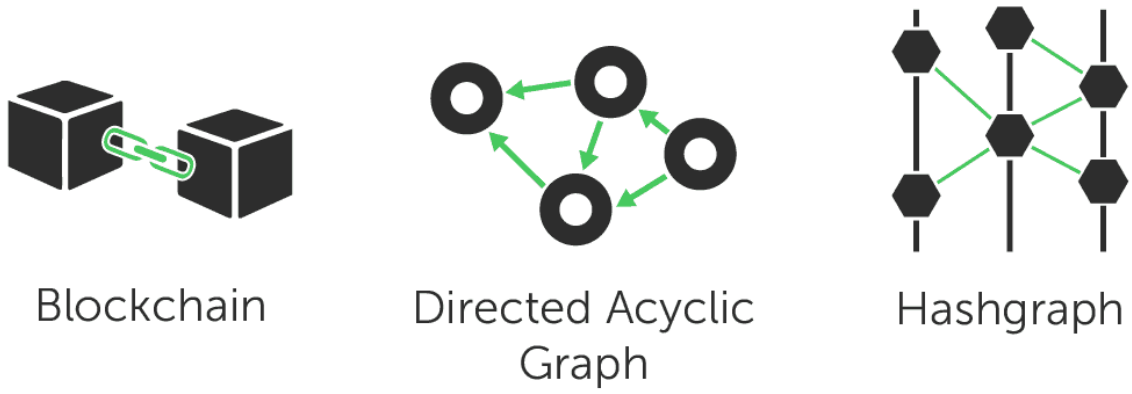
Ωστόσο, οι τεχνολογίες κατανεμημένου μητρώου είναι αποκεντρωμένες με σκοπό την εξάλειψη της ανάγκης για κεντρική αρχή ή για διαμεσολαβητή ο οποίος επεξεργάζεται, επικυρώνει η πιστοποιεί συναλλαγές. Οι επιχειρήσεις χρησιμοποιούν την κατανεμημένη τεχνολογία για την διεκπεραίωση, την επικύρωση ή την πιστοποίηση συναλλαγών ή άλλων τύπων ανταλλαγών δεδομένων. Συνήθως, αυτά τα αρχεία αποθηκεύονται μόνο στον καθολικό, όταν επιτευχθεί συναίνεση από τα εμπλεκόμενα μέλη.

Στη συνέχεια όλα τα αρχεία στην DLT καταχωρούνται και φέρουν μία μοναδική κρυπτογραφική υπογραφή. Όλοι οι συμμετέχοντες των τεχνολογιών Κατανεμημένου Μητρώου μπορούν να δουν τα εν λόγω αρχεία. Η τεχνολογία παρέχει ένα επαληθεύσιμο και ελέγξιμο ιστορικό όλων των πληροφοριών που είναι αποθηκευμένες σε αυτό το συγκεκριμένο σύνολο δεδομένων. Ο στόχος των DLT τεχνολογιών είναι να προσφέρει μια βέβαιη και ασφαλέστερη εναλλακτική λύση στις κεντρικές υπηρεσίες.

Για την επίτευξη ενός αποκεντρωμένου περιβάλλοντος ίδιας λειτουργικότητας ενός κεντρικού, απαιτούνται κάποιες διαφορετικές τεχνολογίες και διαδικασίες.

1.3.2 Τύποι DLT

Υπάρχουν μερικοί διαφορετικοί τύποι Τεχνολογιών Κατανεμημένου Μητρώου και διαρκώς συνεχίζουν να επινοούνται περισσότερα για τη βελτίωση των υφιστάμενων. Προς το παρόν, θα παρουσιαστούν οι τρεις δημοφιλέστεροι τύποι που είναι: Blockchain, DAG και Hashgraph. Αυτές οι τρεις τεχνολογίες είναι ο πυρήνας για την κατανόηση των DLT και της αρχής λειτουργίας της κατανεμημένης δομής.



Εικόνα 7 – Αρχιτεκτονική Δομής των 3 τύπων DLT [22]

Blockchain

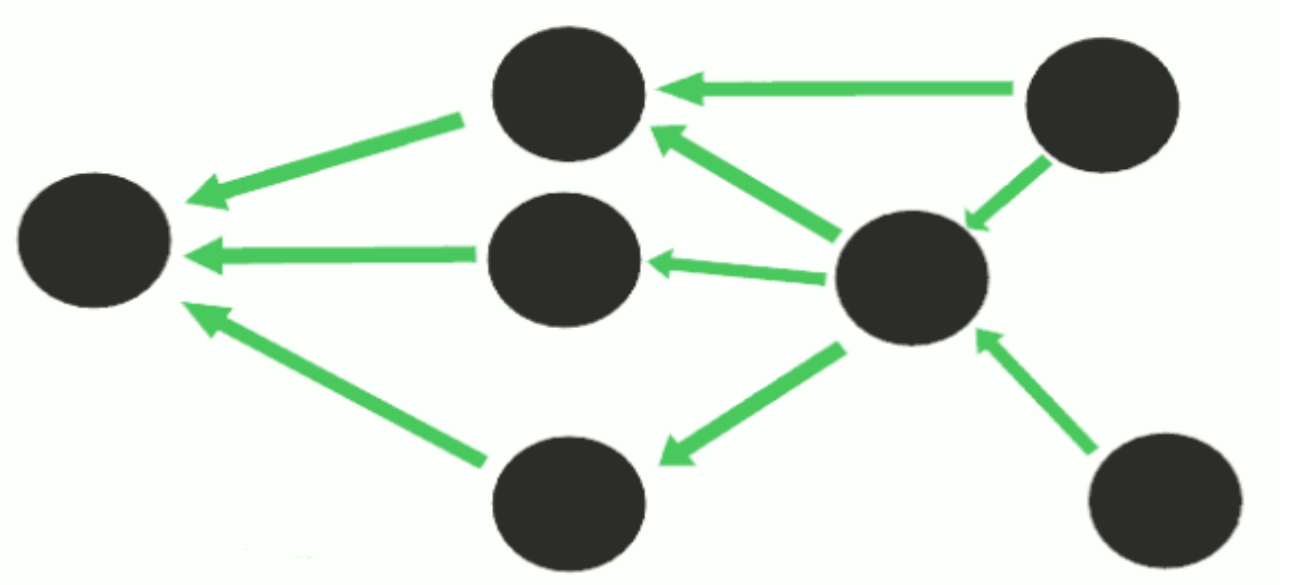
Πάνω στο Blockchain θα δομηθεί και θα πραγματοποιηθεί η διάταξη της εκάστοτε διπλωματική και όλα όσα έχουν περιγραφεί βασίζονται στις Τεχνολογίες Κατανεμημένο Μητρώου, περιγραφή του οποίου θα δοθεί εκτενώς παρακάτω. Το Blockchain είναι η πιο ευρεία και διαδεδομένη τεχνολογία των DLT, Είναι κάτι περισσότερο από μια βάση δεδομένων, καθώς αποτελείται από ένα ολοκληρωμένο σύστημα με δυναμικά μέρη και συστήματα που πρέπει να συνεργάζονται. Είναι ένα σύστημα κατανεμημένου μητρώου και ένα σύστημα επιλύσεων/συναλλαγών. Η τεχνολογία Blockchain άρχισε να γίνεται ευρέως γνωστή με την εμφάνιση του Bitcoin, ενός ομότιμου ηλεκτρονικού νομίσματος.

Αξίζει επίσης να σημειωθεί ότι ορισμένα Blockchains εξυπηρετούν διαφορετικούς σκοπούς. Ορισμένες μπλοκ αλυσίδες, μπορούν να φιλοξενήσουν εφαρμογές, όπως του App Store της Apple ή του Google Play Store της Google, κομμάτι του αποκεντρωμένου κόσμου. Αυτό συμβαίνει επειδή κάποια εργαλεία του είναι Turing Complete, [68] πράγμα που σημαίνει ότι το δίκτυο μπορεί να λειτουργεί και να ερμηνεύεται/υλοποιείται απο πλήρεις γλώσσες προγραμματισμού. Με άλλα λόγια, οι προγραμματιστές μπορούν στην πραγματικότητα να ξεκινήσουν εφαρμογές που μπορούν να χρησιμοποιηθούν στο δίκτυο. Το Ethereum, ένας τύπος Blockchain, λειτουργεί σαν ένα λογισμικό σύστημα το οποίο μπορεί να “τρέξει” αποκεντρωμένες εφαρμογές (DApps – Decentralized Applications) . Ένας από τους βασικούς σκοπούς του Bitcoin είναι η χρήση ψηφιακών μετρητών. Η χρήση του Ethereum είναι ευρύτερη, επιτρέποντας στους προγραμματιστές να εκκινήσουν εφαρμογές σε αυτό το στήσιμο του Μικροδικτύου σε αυτή την πτυχιακή θα βασίζονται στα εργαλεία που προσφέρει.

Ενώ το Blockchain είναι επαναστατικό στην ανάπτυξη του πρώτου ομότιμου αποκεντρωμένου συστήματος εμπιστοσύνης για ηλεκτρονικά νομίσματα, υπάρχουν ελλείψεις όπως με οποιαδήποτε τεχνολογία. Τα δύο μεγαλύτερα προβλήματα με την τεχνολογία Blockchain είναι η επεκτασιμότητα και τα τέλη. Ωστόσο, αποτελούν προβλήματα τα οποία με την πάροδο του χρόνου τείνουν να λυθούν και κυρίως το πρώτο. [21] [22]

DAG – Directed Acyclic Graph

Ο δεύτερος τύπος DLT είναι το DAG. Σε απάντηση στα ζητήματα επεκτασιμότητας του Blockchain, ήρθε στην επιφάνεια το DAG. Το DAG σημαίνει "κατευθυνόμενο ακυκλικό γράφημα" και έχει διαφορετικό μηχανισμό από το Blockchain. Η πιο δημοφιλής πλατφόρμα για τη χρήση μιας υποδομής DAG (ή όπως αποκαλείται Tangle) είναι το IOTA. [24] Το IOTA είναι ένας εξίσου τύπος κατανεμημένης τεχνολογίας συνδυασμένος με το IoT, του οποίου η πλατφόρμα χρησιμοποιεί αποκλειστικά DAG, σε αντίθεση με τα Blockchains, και το κρυπτονόμισμα που έχει λέγεται mIOTA. Μέσω των mIOTA πραγματοποιούνται ψηφιακές συναλλαγές.



Εικόνα 8 – Αρχιτεκτονική Δομής των DAG [22]

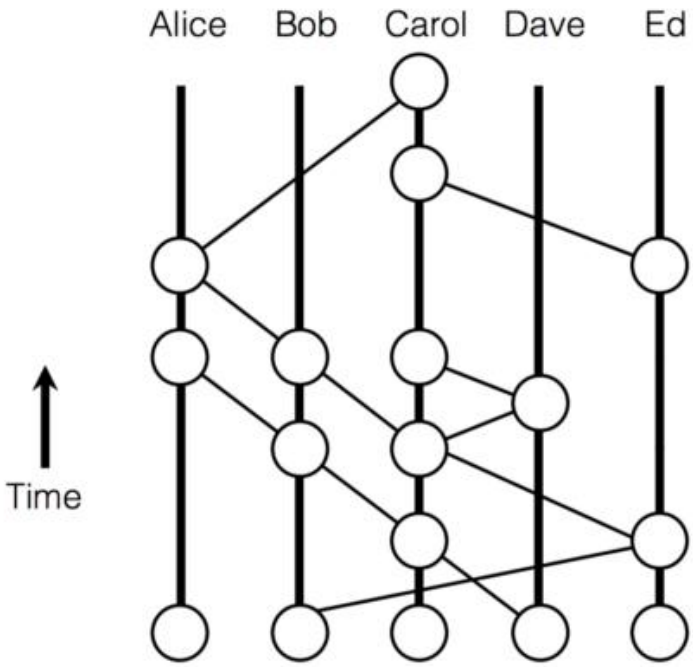
Σε αντίθεση με τα Blockchain, το DAG δεν έχει blocks, αλυσίδες, miners ή τέλη συναλλαγών. Η συνολική προσφορά κερμάτων είτε εκδίδεται στους χρήστες είτε "προ-εξορύσσεται" και η συναίνεση γίνεται πολύ γρήγορα. Το DAG έχει ένα εξαιρετικά υψηλό θεωρητικό όριο στις συναλλαγές ανά δευτερόλεπτο (TPS – Transactions Per Second) λόγω του τρόπου με τον οποίο επιτυγχάνεται η συναίνεση.[22]

Πρώτο μειονέκτημα του DAG είναι ότι στη σημερινή και δημοφιλέστερη μορφή της με το IOTA υπάρχει ένας κεντρικός κόμβος συντονισμού, ο οποίος διοικείται από το ίδρυμα IOTA και χρησιμοποιείται για την αναμετάδοση συναλλαγών. Στο μέλλον, καθώς το δίκτυο επεκτείνεται και γίνεται πιο ασφαλές, αναμένεται ότι η πλατφόρμα θα είναι πλήρως αποκεντρωμένη. Ένα καθαρά αποκεντρωμένο σύστημα DAG δεν έχει δοκιμαστεί ποτέ πλήρως ή χρησιμοποιηθεί σε σύγκριση με το Blockchain. Δεύτερον, δεν υπάρχουν αποκεντρωμένες εφαρμογές (DApps) που χρησιμοποιούνται με το DAG, ενώ για το Blockchain υπάρχουν εκατοντάδες. [22] [69]

Hashgraph

Το Hashgraph είναι ένας άλλος τύπος DLT και ο τελευταίος που θα αναφερθεί στην τεχνολογία Κατανεμημένου Μητρώου στο σημείο αυτό. Είναι γνωστό ότι είναι μια κατοχυρωμένη με δίπλωμα ευρεσιτεχνίας τεχνολογία και σκοπεύεται να χρησιμοποιηθεί σαν permissioned Blockchain, σε αντίθεση με Bitcoin που ανήκει στην κατηγορία permissionless Blockchain. [22]

Το Hashgraph μπορεί να χειριστεί 250.000 συναλλαγές ανά δευτερόλεπτο και να επιτύχει συναίνεση των συμμετεχόντων, έχοντας τα ⅔ του δικτύου σύμφωνα στις έγκυρες συναλλαγές. Η συναίνεση επιτυγχάνεται μέσω ενός συστήματος ψηφοφορίας σε συνδυασμό με ένα σύστημα "gossip", το οποίο είναι ουσιαστικά ένας τρόπος επικοινωνίας των κόμβων με την ανταλλαγή πληροφοριών με γειτονικούς κόμβους. Το gossip είναι το πώς οι συναλλαγές κατανέμονται σε όλο το δίκτυο και μόλις πάνω από τα ⅔ των κόμβων λάβουν τις πληροφορίες αυτές και δουν τα γεγονότα να είναι αληθή, τότε το δίκτυο επικυρώνεται.



Εικόνα 9 – Αλληλουχία χρηστών στο Hashgraph [25]

Τα κύρια μειονεκτήματα εδώ είναι ότι είναι κατοχυρωμένα με δίπλωμα ευρεσιτεχνίας, γνωστό ότι χρησιμοποιείται καλύτερα σε permissioned οικοσυστήματα, και δεν δοκιμάζεται εξίσου καλά με άλλα DLT, παρόλο που είναι στον χώρο αρκετά χρόνια. Ενώ οι 250.000 συναλλαγές ανά δευτερόλεπτο υπερβαίνουν κατά πολύ αυτό που τα Blockchain, δεν είναι καλά δοκιμασμένο από την άποψη της ασφάλειας, της αξιοπιστίας και της συνολικής πρακτικότητας.

1.3.3 Σύγκριση μεταξύ των DLT

Σήμερα, το Blockchain εξακολουθεί να βρίσκεται στην κορυφή των DLT. Ο ανταγωνισμός στον κλάδο μπορεί να συνοψιστεί ως Blockchain εναντίον DLT. Η τεχνολογία Blockchain είναι χωρίς αμφιβολία η πιο δοκιμασμένη, χρησιμοποιημένη και ευπροσάρμοστη DLT που έχουμε σήμερα. Δεν χρησιμοποιείται μόνο για περιπτώσεις νομισματικής χρήσης, αλλά εξουσιοδοτεί και αποκεντρωμένες εφαρμογές (DApps).

	 Blockchain	 DAG	 Hashgraph
Transactions per second	7	Potentially unlimited	250,000+
dApps support	Yes	No	No
Tested under real market conditions	Yes	Yes	No
Patented	No	No	Yes

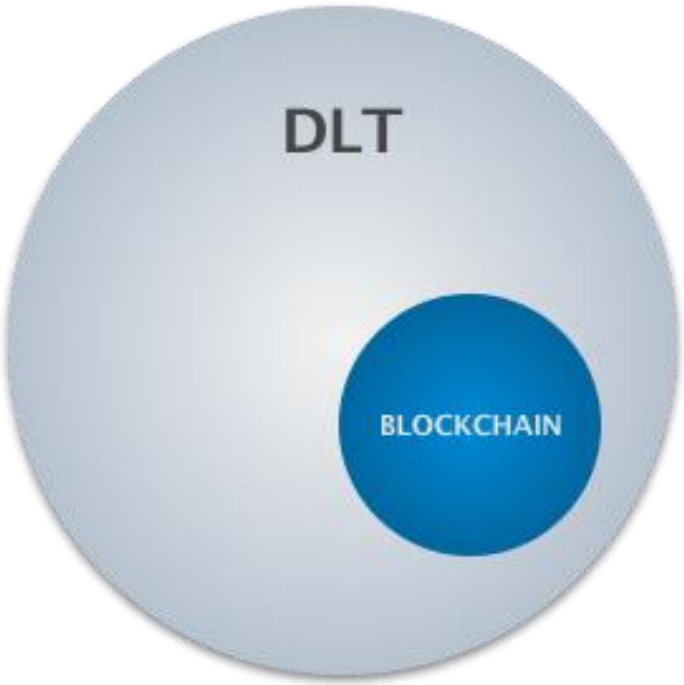
Table 1 – Σύγκριση μεταξύ των DLT [22]

1.3.4 Διαφορά τύπων DLT και Blockchain

Η πιο σημαντική διαφορά είναι ότι το Blockchain είναι μία κατηγορία κατανεμημένου μητρώου. Αν και το Blockchain είναι μια ακολουθία από blocks, σε ένα κλασσικό DLT δεν απαιτείται μια τέτοια αλυσίδα. Επιπλέον, οι DLT δεν χρειάζονται κάποιον μηχανισμό ή αλγόριθμο συναίνεσης και προσφέρουν, θεωρητικά, καλύτερες επιλογές κλιμάκωσης.

Η κατάργηση των ενδιάμεσων από τις κατανεμημένες αρχιτεκτονικές είναι αυτό που καθιστά την έννοια της Κατανεμημένης Τεχνολογίας τόσο ελκυστική. Σε αντίθεση με το Blockchain, ένα DLT δεν χρειάζεται απαραίτητα να έχει μια δομή δεδομένων σε block. Είναι απλώς ένας τύπος βάσης δεδομένων που διανέμεται σε πολλαπλούς ιστότοπους, περιοχές ή συμμετέχοντες.

Σε γενικές γραμμές, οι DLT ακούγονται ακριβώς όπως πιθανώς οραματίζεται κάποιος ένα Blockchain. Ωστόσο, όλα τα Blockchains είναι DLT αλλά δεν είναι όλα τα DLT Blockchains. Ενώ ένα Blockchain αντιπροσωπεύει έναν τύπο DLT, στην πραγματικότητα είναι απλώς ένα υποσύνολο αυτού. [23] [26]



Εικόνα 10 – Το Blockchain ως υποσύνολο των DLT [26]

1.3.5 Τα οφέλη των DLT και Blockchains

Ένα DLT δίνει τον έλεγχο όλων των πληροφοριών και συναλλαγών του στους χρήστες και προάγει τη διαφάνεια. Μπορούν να ελαχιστοποιήσουν το χρόνο συναλλαγής σε λεπτά. Η τεχνολογία διευκολύνει επίσης την αύξηση της απόδοσης γραφείου και την αυτοματοποίηση.

Οι DLT, όπως το Blockchain, είναι εξαιρετικά χρήσιμες για τις χρηματοπιστωτικές συναλλαγές. Μειώνουν τις λειτουργικές ανεπάρκειες (κάτι το οποίο εξοικονομεί χρήματα). Μεγαλύτερη ασφάλεια παρέχεται επίσης εξαιτίας του αποκεντρωμένου χαρακτήρα τους, καθώς και του γεγονότος ότι τα αρχεία είναι αμετάβλητα.

Εναλλακτικά, η τεχνολογία Blockchain προσφέρει έναν τρόπο για την ασφαλή και αποτελεσματική δημιουργία ενός αρχείου μητρώου ευαίσθητης δραστηριότητας. Αυτό περιλαμβάνει οτιδήποτε από τις διεθνείς μεταφορές χρημάτων σε αρχεία μετόχων. Οι χρηματοοικονομικές διαδικασίες αναβαθμίζονται ριζικά για να προσφέρουν στις επιχειρήσεις μια ασφαλή, ψηφιακή εναλλακτική λύση στις διαδικασίες που διεξάγονται. Αποφεύγοντας εν γένει αυτές τις συχνά γραφειοκρατικές, χρονοβόρες, χάρτινες και δαπανηρές διαδικασίες.

Όταν γράφονται τα δεδομένα σε ένα Blockchain, γίνονται χαραγμένα στο δίκτυο. Όταν υπάρχει μια σειρά συναλλαγών στην πάροδο του χρόνου, αποκτάται μια ακριβή και αμετάβλητη διαδρομή ελέγχου. Αυτό είναι πολύ χρήσιμο για τους οικονομικούς ελέγχους. Έχοντας αποθηκευμένα τα δεδομένα σε έναν τόπο όπου καμία από τις οντότητες δεν το κατέχει ή δεν το ελέγχει και κανείς δεν μπορεί να αλλάξει ό, τι έχει ήδη γραφτεί, δίνονται οφέλη παρόμοια με αυτά της διπλής λογιστικής. Τελικά, αυτό σημαίνει ότι υπάρχουν λιγότερες πιθανότητες σφάλματος ή απάτης.

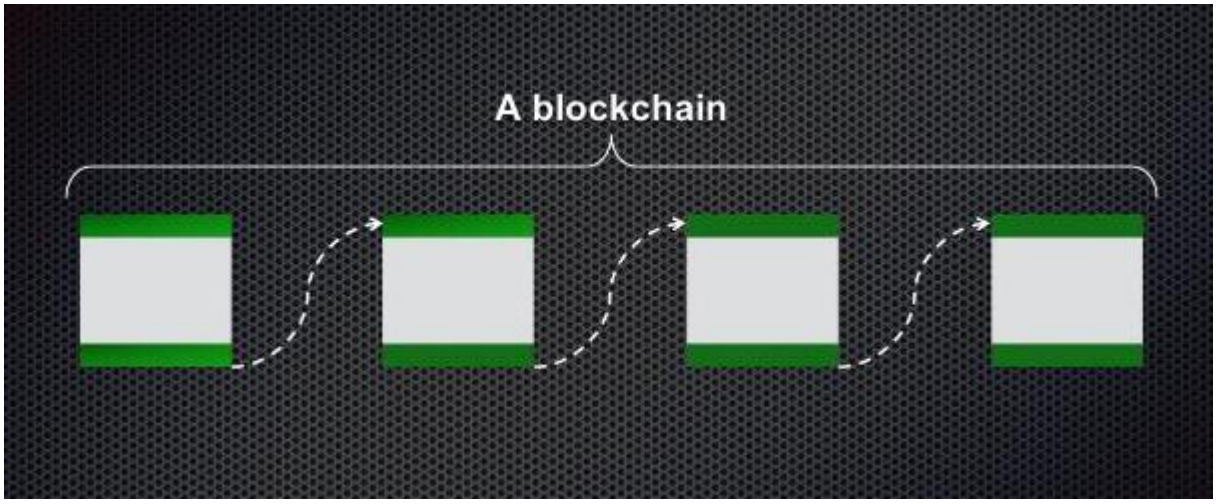
1.4 Εισαγωγή στα Blockchain

1.4.1 Τι είναι το Blockchain?

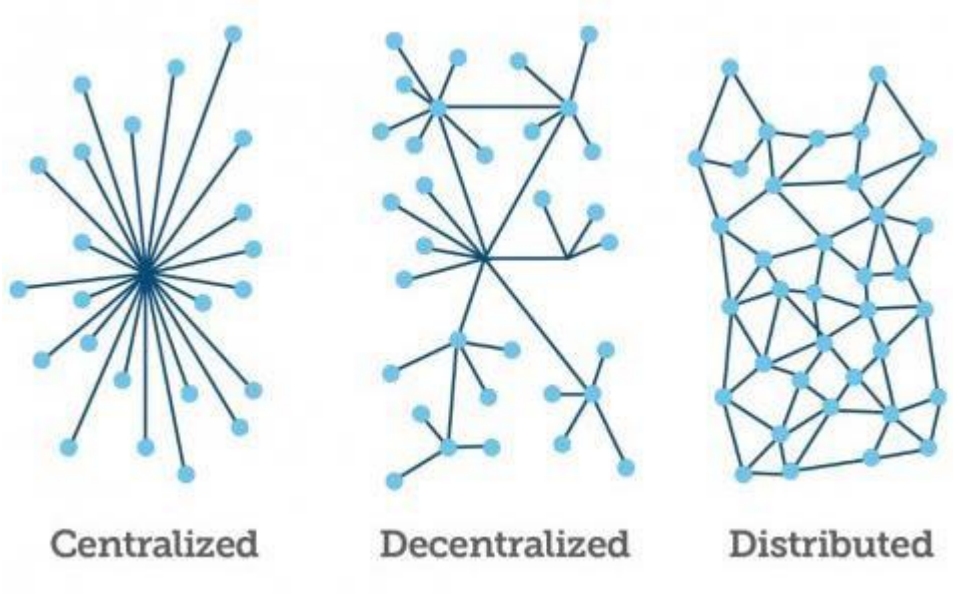
Το Blockchain είναι μία λίστα αρχείων ή "μπλοκ" που συνδέονται μεταξύ τους και είναι κρυπτογραφικά ασφαλισμένα. Κάθε συμμετέχων στο δίκτυο του Blockchain έχει αρχεία όλων των συναλλαγών και τα αρχεία αυτά αποθηκεύονται τοπικά στους υπολογιστές όλων των χρηστών που συμμετέχουν στο δίκτυο. Οποιοδήποτε πρωτόκολλο ή καθεστώς πρόκειται να αλλάξει, απαιτεί την συναίνεση όλων των συμμετεχόντων του δικτύου.

Η διαδικασία ξεκινά όταν ένας χρήστης του δικτύου Blockchain ζητά μια συναλλαγή – είτε πρόκειται για συναλλαγή που σχετίζεται με κρυπτογράφηση, σύμβαση ή άλλες πληροφορίες. Η συναλλαγή μεταδίδεται σε ομότιμο (P2P Network) δίκτυο υπολογιστών (κόμβοι). Το δίκτυο των κόμβων στη συνέχεια επαληθεύει την συναλλαγή χρησιμοποιώντας γνωστούς αλγόριθμους που επισυνάπτουν ένα μοναδικό "hash" στην συναλλαγή. Μετά την επαλήθευση, η συναλλαγή συνδυάζεται με άλλες για να δημιουργηθεί ένα μπλοκ δεδομένων για το αρχείο. Το νέο μπλοκ προστίθεται στο υπάρχον Blockchain με τρόπο μόνιμο και αναλλοίωτο.

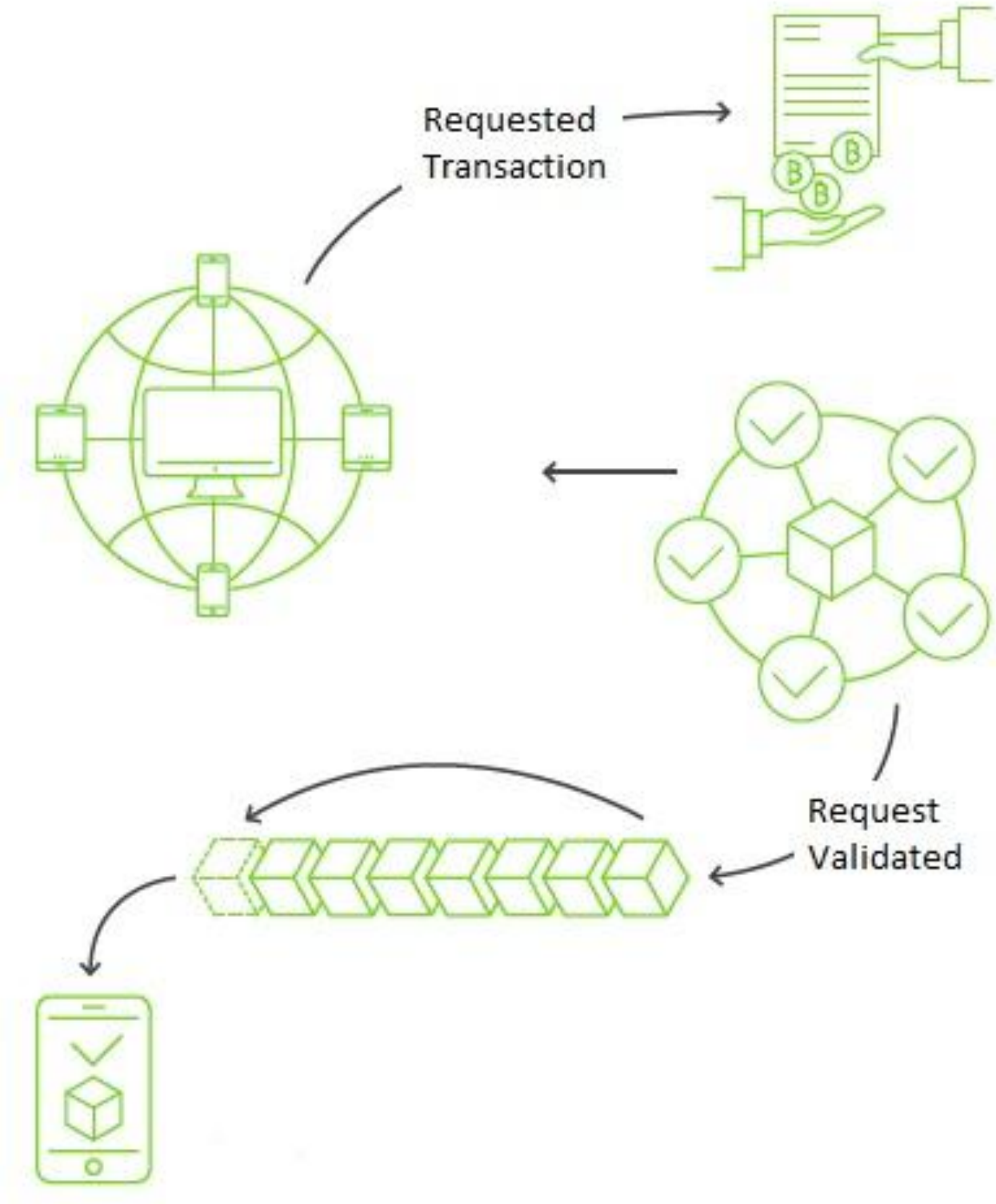
Η διαδικασία με την οποία οι κατανεμημένοι φορείς ενός Blockchain επαληθεύουν μια συναλλαγή πριν από τη μόνιμη ενσωμάτωσή τους στο σύστημα Blockchain, ονομάζεται "συναίνεση" (Consensus). Η επίτευξη συναίνεσης επιτρέπει την αλυσίδα του Blockchain να αναπτυχθεί, αποτρέποντας παράλληλα σε αντίπαλους παράγοντες να εκμεταλλευτούν και να παραμορφώσουν την αλυσίδα. Τα μπλοκ αντιπροσωπεύουν σύνολα συναλλαγών (ή σύνολα δεδομένων που πρέπει να προστεθούν στο αρχείο) και επαληθεύονται μέσω της διαδικασίας συναίνεσης σε διακριτά χρονικά διαστήματα, υπάρχει γενικά μια διάρκεια επιβεβαίωσης μεταξύ της συναλλαγής που πραγματοποιείται και της προσθήκης αυτής της συναλλαγής στο Blockchain. Ο μέσος χρόνος επιβεβαίωσης εξαρτάται από τον όγκο των συναλλαγών, τα μεγέθη των μπλοκ και τους αλγόριθμους συναίνεσης.[53]



Εικόνα 11 - Αρχιτεκτονική Blockchain [57]



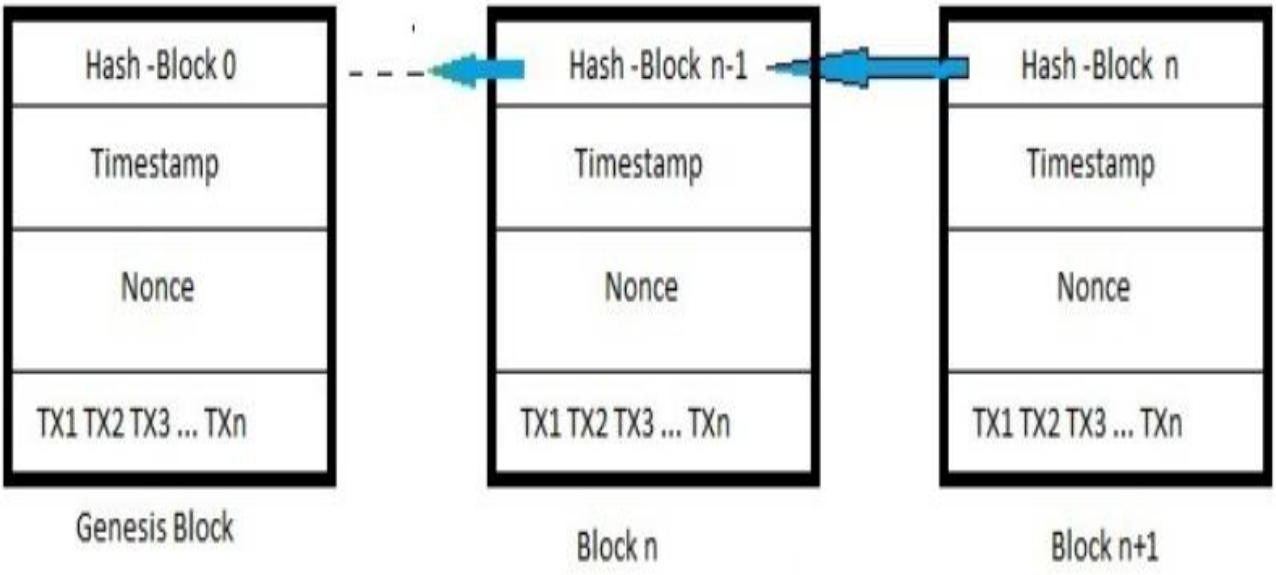
Εικόνα 12 – Διαφορές μεταξύ Κεντρικών, Αποκεντρωμένων και Κατανεμημένων τεχνολογιών στην αρχιτεκτονική, το Blockchain ανήκει στην τελευταία κατηγορία κατανεμημένης βάσης δεδομένων [57]



Εικόνα 13 – Διαδικασία Συναλλαγής στο Blockchain, από την απαίτηση για συναλλαγής μέχρι την επικύρωση αυτής και δημιουργίας block [53]

1.4.2 Αρχή λειτουργίας Blockchain

Το Blockchain, ως αρχή, περιλαμβάνει blocks τα οποία αποτελούνται από πολλά δεδομένα (συναλλαγές) συμπεριλαμβανομένων και μερικών άλλων σημαντικών πληροφοριών για να σχηματιστεί η αλυσίδα. Κάθε block δείχνει στο προηγούμενο του ότι εμπεριέχει μια σημαντική βασική τιμή για αυτό, και ονομάζεται parent block. Το πρώτο block, που δεν περιέχει κάποια σημαντική τιμή από προηγούμενο, ονομάζεται genesis block.



Εικόνα 14 – Δομή Block [70]

Ένα block αποτελείται από το block header και block body. Ο μέγιστος αριθμός συναλλαγών που μπορεί να περιέχει ένα block, εξαρτάται από το μέγεθος του block και το μέγεθος της συναλλαγής.

Header	**Block version**	0000000000010
	Parent block hash	fffff00015421256fffffffffff00000000
	Merkle tree root	dd008121256ddddddddffff11111111
	Timestamp	12e5d1985y
	Nonce	0efdef12
	Nbits	30x30x301845
Body	**Transaction counter**	TX1 TX2 TX3 TX4….. TXn

Table 2 – Περιεχόμενο ενός Block [70]

Παρακάτω αναλύονται τα επιμέρους στοιχεία του πίνακα που εμπεριέχονται σε ένα block:

Block version: Υποδεικνύει ποιο σύνολο κανόνων επικύρωσης ενός block πρέπει να ακολουθήσει.

Parent block hash: Μία 256-bit hash τιμή, που δείχνει στο προηγούμενο block

Merkle tree root: Η hash τιμή που περιέχει όλες τις συναλλαγές του block

Timestamp: Η χρονική σήμανση σε δευτερόλεπτα από 1970-01-01T00: 00 UTC

Nonce: Ένα 4-byte πεδίο, το οποίο συνήθως ξεκινά με την τιμή 0 και αυξάνει ε κάθε hash υπολογισμό.

Nbits: Τρέχων hashing στόχος, σε συμπαγής μορφή

1.4.3 Τύποι Blockchain

Τα Blockchain χωρίζονται σε 3 κατηγορίες: Public Blockchain, Private Blockchain και Hybrid Blockchain. Παρακάτω δίνεται αναλυτική επεξήγηση για το τι συνεπάγεται στον κάθε τύπο Blockchain, οι δυνατότητες και οι περιορισμούς που εμπεριέχουν.[70]

1.4.3.1 Public Blockchain

Ένα πλήρως ανοικτό Public Blockchain δεν έχει περιορισμούς όσον αφορά την άδειας ανάγνωσης και γραφής. Οποιοσδήποτε μπορεί να συνδεθεί στο δίκτυο να αποκτήσει πρόσβαση σε πληροφορίες και να έχει τη δυνατότητα προσθήκης πληροφοριών. Όποιος συνδεθεί με το δίκτυο έχει το δικαίωμα να συμμετάσχει στο πρωτόκολλο συναίνεσης, να επαληθεύσει τις νέες προσθήκες και να το διασφαλίσετε ότι δεν έρχεται σε σύγκρουση με τα προηγούμενα μπλοκ της αλυσίδας. Το πρωτόκολλο συναίνεσης είναι αναγκασμένο να βασίζεται σε κρυπτοοικονομικό μηχανισμό, λόγω της ανοικτής φύσης του συστήματος και λόγω έλλειψης εμπιστοσύνης μεταξύ των κόμβων. Ένα σύστημα Public Blockchain λειτουργεί χωρίς την απαίτηση εμπιστοσύνης μεταξύ χρηστών. Ως εκ τούτου, θεωρείται ότι είναι πλήρως

αποκεντρωμένο. Μερικά state-of-the-art πρωτόκολλα Public Blockchain ανοικτών πηγών που βασίζονται στον αλγόριθμο συναίνεσης Proof of Work (PoW) είναι το Bitcoin, το Ethereum και το Monero.Τα κύρια χαρακτηριστικά του δημόσιου Blockchain είναι τα εξής:

• Οποιοσδήποτε μπορεί να συμμετάσχει χωρίς άδεια.

• Κάθε άτομο μπορεί να κατεβάσει τον κώδικα και να ξεκινήσει να εκτελεί έναν δημόσιο κόμβο στις τοπικές συσκευές του, να επικυρώνει συναλλαγές στο δίκτυο και, συνεπώς, να συμμετέχει στη διαδικασία συναίνεσης.

• Κάθε χρήστης ανά τον κόσμο μπορεί να στείλει συναλλαγές μέσω του δικτύου και να περιμένει να συμπεριληφθούν στο Blockchain, αν είναι έγκυρες.

• Ο καθένας μπορεί να διαβάσει τις συναλλαγές στον δημόσιο εξερευνητή μπλοκ.

1.4.3.2 Private Blockchain

Ένα Private Blockchain έχει ορισμένους περιορισμούς στα δικαιώματα ανάγνωσης και γραφής και είναι πιο στενά ελεγχόμενο από ένα Public. Το δικαίωμα τροποποίησης, προσθήκης ή ανάγνωσης πληροφοριών περιορίζεται και ελέγχεται κεντρικά από μια ομάδα συμμετεχόντων, π.χ. μία οργάνωση. Σε ένα Private Blockchain, ένα πρωτόκολλο συναίνεσης συνήθως δεν είναι απαραίτητο λόγω της αξιοπιστίας των κόμβων. Τα Private Blockchain έχουν τη δυνατότητα γρήγορης πρόσβασης πληροφοριών, να κάνουν τις συναλλαγές φθηνότερες και να ελέγχουν το επίπεδο της ιδιωτικότητας .Παραδείγματα τέτοιων εφαρμογών περιλαμβάνουν τη διαχείριση βάσεων δεδομένων, τον έλεγχο κ.λπ. που είναι εσωτερικά σε μια ενιαία εταιρεία και, επομένως, πιθανόν σε πολλές περιπτώσεις η δημόσια έκθεση να μην είναι απαραίτητη. Σε άλλες περιπτώσεις είναι επιθυμητός ο δημόσιος λογιστικός έλεγχος. Τα Private Blockchain (όπως η Monaxκαι Multichain) είναι ένας τρόπος να εκμεταλλευτεί η τεχνολογία Blockchain με τη δημιουργία ομάδων και συμμετεχόντων που μπορούν να επαληθεύσουν τις συναλλαγές εσωτερικά. Αυτό εγκυμονεί κινδύνους στην ασφάλεια παραβιάζοντας το ακριβώς όπως ένα κεντρικό σύστημα, αλλά έχει πλεονεκτήματα όταν πρόκειται για την επεκτασιμότητα και την συμμόρφωση των κανόνων περί απορρήτου δεδομένων και άλλων ρυθμιστικών θεμάτων.[70]

1.4.3.3 Hybrid Blockchain

Υπάρχει και το Hybrid Blockchain που αποτελείται από ορισμένα χαρακτηριστικά ενός Public και ενός Private. Η συναίνεση συνήθως προκαθορίζεται και διοικείται από μια προκαθορισμένη ομάδα ιδρυμάτων. Ένα τέτοιο Blockchain θα μπορούσε π.χ. να έχει 20 ιδρύματα που ελέγχουν ένα κόμβο και κάθε νέα προσθήκη πρέπει να υπογραφεί από τουλάχιστον 13 ιδρύματα για να θεωρηθεί έγκυρη. Το Hybrid θεωρείται εν μέρει αποκεντρωμένο. Τα δικαιώματα ανάγνωσης μπορούν να είναι ανοιχτά στο δημόσιο ή να περιορίζονται σε μια ομάδα συμμετεχόντων. Υπάρχει μια υβριδική λύση σε αυτό, έτσι ώστε κάποια μέρη των πληροφοριών να είναι δημόσια και κάποια άλλα μέρη να μην είναι. Ομοσπονδιακά Blockchains (όπως R3 (Τράπεζες), EWF (Ενέργεια), B3i (Ασφάλειες), Corda),λειτουργούν υπό την ηγεσία μιας ομάδας χωρίς να αφήνουν κανένα πρόσωπο με πρόσβαση στο διαδίκτυο να συμμετέχει στη διαδικασία επαλήθευσης των συναλλαγών. Τα Ομοσπονδιακά Blockchain είναι ταχύτερα στην παροχή μεγαλύτερης ιδιωτικότητας συναλλαγών .Τα Blockchain της κοινοπραξίας χρησιμοποιούνται κυρίως στον τραπεζικό τομέα. Η διαδικασία συναίνεσης ελέγχεται από ένα προεπιλεγμένο σύνολο κόμβων. Το δικαίωμα να διαβαστεί το Blockchain μπορεί να είναι κοινό, ή να περιορίζεται στους συμμετέχοντες.[70]

	PUBLIC	PRIVATE
Access right	Open, anyone can write/read	Restricted "Know Your Customer" (KYC) policy
Validation	Permissionless, unknown validators (risk of "Sybil attack")	Permissioned, known validators (can ban who misbehave)
Speed	Slow clearing, fast settlement	Fast, high performances. Settlement might be slow depending on the process
Security	Immutable record	Reversible, can edit and change the history
Identity	Anonymous/pseudonymous	Known (KYC rules)
Asset	Native digital token used for mining reward	Customisable type of asset
Cost	Energy, OPEX	Development cost, CAPEX
Consensus	Proof of Work, possible Proof of Stake in the future	Proof of Stake, Delegated Proof of Stake, Proof of Elapsed Time, Byzantine Fault Tolerance algorithms

Table 3 – Διαφορές Public και Private Blockchain [53]

1.4.4 Permissioned and Permissionless Blockchains

Επιπλέον, τα Blockchain διακρίνονται το ένα από το άλλο και από το "permission model" τους, το οποίο καθορίζει τους τύπους αδειών που μπορούν να δοθούν στους συμμετέχοντες στο δίκτυο. Τα Public και Private Blockchain αναφέρονται στην ικανότητα ανάγνωσης: ποιος επιτρέπεται ή δεν επιτρέπεται να βλέπει συναλλαγές στο Blockchain. Τα Public είναι ανοιχτά σε οποιονδήποτε, ενώ οι συναλλαγές που πραγματοποιούνται στα Private περιορίζονται σε ένα υποσύνολο εγκεκριμένων συμμετεχόντων. Τα "permissioned" και "permissionless" Blockchain αναφέρονται στις δυνατότητες "εγγραφής" και "δέσμευσης" των Blockchains: ποιος μπορεί να στείλει

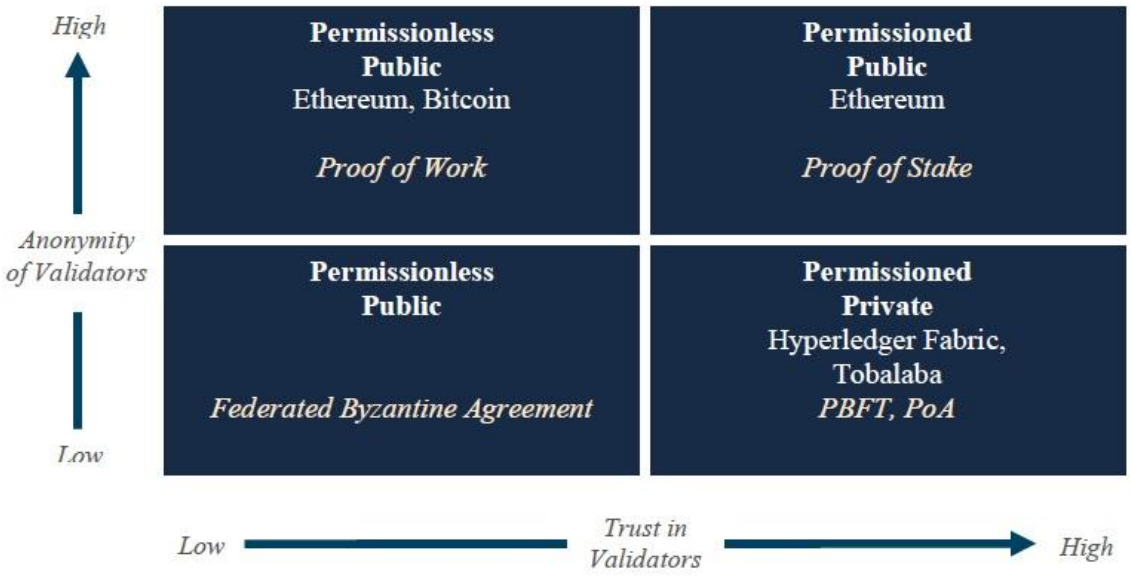
συναλλαγές και πραγματοποιήσει επαλήθευση, αντίστοιχα. Όπως υποδηλώνουν τα ονόματά τους, τα permissionless Blockchains επιτρέπουν στον καθένα να γράψει η να δεσμευτεί σε αυτό, ενώ στα permissioned Blockchains απαιτείται εξουσιοδότηση.

Βάσει των παραπάνω προκύπτουν τέσσερις πιθανές κατηγορίες Blockchain:

- Permissionless Public
- Permissioned Public
- Permissionless Private
- Permissioned Private

Όταν επιλέγεται ένα Blockchain θα πρέπει να ληφθούν υπ' όψιν 3 βασικοί παράγοντες:

- Αποκέντρωση – είναι το σενάριο του συστήματος στο οποίο κάθε συμμετέχοντας έχει πρόσβαση σε συγκεκριμένες πηγές.
- Επεκτασιμότητα – αναφέρεται στο χαρακτηριστικό του συστήματος να επεκτείνει τις εκτελεστικές του δυνατότητες, προσθέτοντας και άλλες λειτουργίες
- Ασφάλεια – Η δυνατότητα που έχει το σύστημα να ανταποκρίνεται σε κακόβουλους χρήστες



Εικόνα 15 – Επίπεδα ανωνυμίας και εμπιστοσύνης μεταξύ των επικυρωτών στο δίκτυο βάσει του τύπου Blockchain [67]

Characteristics	Permissionless/ Public	Permissionless/ Public	Permissioned/ Public	Permissioned/ Private
Consensus	PoW	FBA	PoS	PBFT/ Multi-signature
Anonymity of the user	🟢	🟡	🟢	🟡
Immutability	🟢	🟡	🟡	🟡
Scalability	🔴	🟡	🟡	🟡
Privacy	🔴	🟡	🔴	🟡
Examples of Platform	Bitcoin, Ethereum	Ripple Stellar	Ethereum Casper	Hyperledger Fabric Tobalaba Tendermint
Energy Use Case	✓	✗	✗	✓

High 🟢 Medium 🟡 Low 🔴

Table 4 – Παραδείγματα Blockchain, τι τύποι είναι, τι αλγόριθμους συναίνεσης χρησιμοποιούν και ποια τα χαρακτηριστικά αυτών [67]

1.4.5 Αλγόριθμοι Συναίνεσης (Consensus Algorithms)

Μία από τις μεγαλύτερες δυσκολίες που αντιμετωπίζεται στην τεχνολογία Blockchain είναι ποιο είναι το βέλτιστο πρωτόκολλο συναίνεσης ανα περίπτωση για τους χρήστες στο P2P δίκτυο. Χρησιμοποιούνται αλγόριθμοι συναίνεσης για να διασφαλιστεί ότι οι συμμετέχοντες στο δίκτυο ακολουθούν τους κανόνες και οι συναλλαγές επικυρώνονται με τη σωστή σειρά. Χρησιμοποιούνται επίσης για να επιβεβαιωθεί ότι οι πληροφορίες εντός ενός block είναι σωστές, ότι οι κόμβοι λαμβάνουν μια δίκαιη αποζημίωση και αποφεύγουν ζητήματα όπως το πρόβλημα της διπλής δαπάνης. Δύο βασικές προσεγγίσεις που υπάρχουν είναι η "Nakamoto συναίνεση "και η Ανοχή Βυζαντινού Σφάλματος (BFT – Byzantine Fault Tolerance). Η πρώτη προσέγγιση εκλέγει τον ηγέτη, μέσω κάποιας μορφής "κλήρωσης", ο οποίος στη συνέχεια προτείνει ένα block προστίθεται στην αλυσίδα των ήδη υπαρχόντων Blocks. Η δεύτερη προσέγγιση βασίζεται στον αλγόριθμο του BFT και χρησιμοποιεί πολλαπλούς γύρους ρητών ψήφων για να επιτευχθεί η απαραίτητη συναίνεση.

Έχουν αναπτυχθεί πολλοί τύποι κατανεμημένων αλγορίθμων συναίνεσης, καθένας από τους οποίους παρέχει πλεονεκτήματα και μειονεκτήματα. Η μεθοδολογία που χρησιμοποιείται για την επίτευξη συναίνεσης στα δίκτυα Blockchain καθορίζει πολλά χαρακτηριστικά επιδόσεων, όπως επεκτασιμότητα, ταχύτητα συναλλαγής, το αμετάκλητο των συναλλαγών, ασφάλεια και δαπάνη πόρων όπως η ηλεκτρική ενέργεια. Οι εφαρμογές συστημάτων Blockchain, όπως οι βιομηχανίες, απαιτούν διάφορες απαιτήσεις ανάλογα με τις συγκεκριμένες περιπτώσεις. Πολλές εφαρμογές απαιτούν εκκαθάριση συναλλαγών σε πραγματικό χρόνο και χαμηλή πιθανότητα σφάλματος. Άλλες εφαρμογές πρέπει να έχουν καλή δυνατότητα επεκτασιμότητας. Παρακάτω παρουσιάζονται κάποιοι από τους σημαντικότερους αλγόριθμους συναίνεσης , με πιο διαδεδομένους και σύνηθες στην χρήση του Proof of Work (Pow) και Proof of Stake (PoS).

1.4.5.1 Proof of Work (PoW)

Είναι ο μηχανισμός συναίνεσης που χρησιμοποιείται πιο συχνά σε συνδυασμό με την τεχνολογία Blockchain, και βασίζεται στους "miners". Οι miners επιλύουν δύσκολα κρυπτογραφημένα παζλ για να έχουν το δικαίωμα προσθήκης επόμενου block στην αλυσίδα, δημιουργώντας τους το κίνητρο να ανταγωνίζονται μεταξύ τους για την πιο πρόσφατη κρυπτογράφηση. Τρέχοντα δίκτυα Blockchain που λειτουργούν με PoW είναι το Bitcoin, το Ethereum, και άλλα permissionless δίκτυα. Η χρήση PoW σε μεγάλα αποκεντρωμένα δίκτυα συνοδεύεται με βραδύτερες ταχύτητες συναλλαγών. Οι χρόνοι επιβεβαίωσης για το Bitcoin είναι της τάξεως των οκτώ έως δέκα λεπτών, ενώ στο Ethereum είναι περίπου 15 δευτερόλεπτα.

Ένας τρόπος διασφάλισης της αυθεντικότητας είναι να αφεθεί σε κάθε χρήστη μέσα στο δίκτυο να πάρει μία ψήφο και να αφήσει όλους τους χρήστες να ψηφίσουν την οποιαδήποτε συναλλαγή που θα πρέπει να συμπεριληφθεί στο επόμενο block. Ο αριθμός των ψήφων αποφασίζει ποιο σύνολο συναλλαγών θα πρέπει να συμπεριληφθεί. Αυτό το είδος της διαδικασίας συναίνεσης είναι ευάλωτο σε επιθέσεις Sybil, όπου ένας χρήστης θα μπορούσε να δημιουργήσει πολλαπλούς λογαριασμούς και να πάρει την μεγαλύτερη επιρροή εντός του δικτύου. Ο Nakamoto, ο δημιουργός του Bitcoin, λύνει αυτό το θέμα επιρροής προσθέτοντας ένα κόστος στην ψήφο. Η επιρροή κάθε χρήστη βασίζεται στην υπολογιστική ισχύ του. Όσο περισσότερη η υπολογιστική ισχύς, τόσο μεγαλύτερη είναι η απαιτούμενη ενέργεια και τόσο υψηλότερο είναι το κόστος του hardware. Αυτή είναι η έννοια του πρωτοκόλλου συναίνεσης για το PoW.

Στην περίπτωση των bitcoins (τα οποία χρησιμοποιούν PoW), το δίκτυο συλλέγει όλες τις συναλλαγές που πραγματοποιούνται κατά τη διάρκεια μιας καθορισμένης περιόδου σε ένα block. Η δουλειά των κόμβων είναι να επιβεβαιώσουν τις συναλλαγές και να τις γράφουν στο Blockchain που έχει και τις πληροφορίες που προστατεύονται από τους εισβολείς. Οι κόμβοι παίρνουν οικονομικά κίνητρα για να κρατήσουν το mining και το hashing, όσο περισσότερα block δημιουργούνται, τόσο περισσότερα bitcoins λαμβάνονται .

Σε ένα δίκτυο Bitcoin, συνιστάται η αναμονή τουλάχιστον έξι block για να επιβεβαιωθεί ότι η συναλλαγή είναι τελική. Οι κόμβοι ανταγωνίζονται μεταξύ τους για να είναι οι πρώτοι που θα παράγουν ένα block και ένα ζευγάρι κόμβων θα μπορούσαν να εργάζονται ταυτόχρονα στην ίδια συναλλαγή. Το block που δημιουργείται πρώτα, με το μακρύτερο Bockchain πίσω του, κερδίζει και παίρνει την ανταμοιβή. Το PoW έχει αποδειχθεί εμπειρικά ότι είναι ασφαλές και ισχυρό Παρόλα αυτά, υποστηρίζεται ότι υπάρχουν κάποιες υφέσεις με το PoW, π.χ. ο κίνδυνος επίθεσης κατά 51% και το κόστος υψηλής ενέργειας την παραγωγή ενός block. Η mining κοινότητα γίνεται όλο και μικρότερη, ενώ όπου μεγάλες εταιρείες με μεγάλους πόρους θα μπορούσαν να ξεπεράσουν το mining σε ατομικό επίπεδο. Αυτή η εξειδίκευση του mining καθιστά το σύστημα πιο συγκεντρωμένο σε λίγες μεγάλες εταιρείες και ο κίνδυνος επίθεσης του 51% αυξάνεται.

1.4.5.2 Proof of Stake (PoS)

Στο Proof of Stake (PoS),δεν υπάρχει καμία διαδικασία mining. Αντιθέτως, η εργασία που απαιτείται για την διεξαγωγή της διαδικασίας επαλήθευσης κατανέμεται μεταξύ των επικυρωτών και βασίζεται στο ποσοστό συμμετοχής που έχουν στην δημιουργία ενός block. Διαφορετικοί αλγόριθμοι συναίνεσης PoS υπάρχουν για να επιβραβεύονται ειλικρινείς επικυρωτές ανάλογα με την συμμετοχή τους. Αυτή η προσέγγιση μειώνει την πολυπλοκότητα των αποκεντρωμένων διαδικασιών επαλήθευσης και έτσι μπορεί να αποφέρει μεγάλη οικονομία στην ενέργεια και τα λειτουργικά έξοδα. Μπορεί επίσης να συμβάλει στη μείωση των κινδύνων συγκέντρωσης που σχετίζονται με το PoW , λόγω της υψηλής κλίμακας οικονομιών στις επενδύσεις του mining, κάνοντας τις επενδύσεις στο δίκτυο περισσότερο ακριβές .

Μειώνεται ο κίνδυνος κατά 51% και μειώνεται και η κατανάλωση ενέργειας κατά αυτόν τον τρόπο. Στην περίπτωση της PoS χρειάζονται νομίσματα για να δημιουργηθεί ένα νέο block και ο κόμβος με τα περισσότερα νομίσματα παίρνει και την μεγαλύτερη επιρροή.

1.4.5.3 Delegated Proof of Stake (DPOS)

Το Delegated Proof of Stake είναι παρόμοιο με το POS, οι miners έχουν προτεραιότητα να δημιουργούν block σύμφωνα με την συμμετοχή τους. Η μεγάλη διαφορά μεταξύ του POS και του DPOS είναι ότι το POS έχει άμεση δημοκρατία ενώ το DPOS είναι αντιπροσωπευτικά δημοκρατικό .Οι ενδιαφερόμενοι εκλέγουν τους αντιπροσώπους τους για να δημιουργήσουν και να επικυρώσουν ένα block. Με σημαντικά λιγότερους κόμβους για την επικύρωση του block, το block θα μπορούσε να επιβεβαιωθεί γρήγορα, κάνοντας και τις συναλλαγές να επιβεβαιωθούν γρήγορα. Επιπλέον, οι παράμετροι του δικτύου, όπως το μέγεθος του block και τα διαστήματα των block που μεσολαβούν θα μπορούσαν να συντονιστούν. Επιπλέον, οι χρήστες δεν χρειάζεται να ανησυχούν για ανέντιμους αντιπροσώπους διότι αυτοί του εξελέγουν εύκολα. Το DPOS έχει ήδη εφαρμοστεί και είναι η βάση του Bitshares.

1.4.5.4 Proof of Authority (PoA)

Σύμφωνα με το Proof of Authority (PoA), εγκεκριμένοι λογαριασμοί ή οι επικυρωτές “τρέχουν” λογισμικό που τους επιτρέπει να τοποθετήσουν συναλλαγές σε block. Αν και η διαδικασία είναι αυτοματοποιημένη και δεν απαιτεί την συνεχή παρακολούθηση της επικύρωσής στους υπολογιστές, η διατήρηση της ασφάλειας του PoA απαιτεί από τους υπολογιστές των επικυρωτών να συμμετέχουν χωρίς συμβιβασμούς. Η προσέγγιση του PoA είναι πιο συγκεντρωτική και επιρρεπής στην επίθεση από άλλους, αλλά συνδέεται με γρηγορότερες ταχύτητες συναλλαγών. Ένα παράδειγμα ενός δικτύου που βασίζεται σε PoA είναι το δοκιμαστικό δίκτυο Tobalaba Energy Web Foundation του οποίου οι επικυρωτές περιλαμβάνουν εταιρείες ενέργειας / ηλεκτρικής ενέργειας όπως την Shell, Engie,Statoil, Centrica, Tepco και άλλες. Το δίκτυο αυτό έχει μέσο όρο χρόνου επιβεβαίωσης περίπου τρία με τέσσερα δευτερόλεπτα.

1.4.5.5 Practical Byzantine Fault Tolerance (PBFT)

Το Blockchain στοχεύει στην επίλυση του λεγόμενου προβλήματος "Byzantine Generals' Problem" , που προκύπτει όταν μια ομάδα προσπαθεί να πάρει μια συλλογική απόφαση για το πώς θα ενεργήσει και θα αντιμετωπίσει τον κίνδυνο κακόβουλων χρηστών εντός της ομάδας, που στέλνουν μικτά μηνύματα σχετικά με τις προτιμήσεις τους. Στα δίκτυα Blockchain, αν ορισμένα μέλη στέλνουν άσχετα στοιχεία σε άλλους σχετικά με τις συναλλαγές, τότε η αξιοπιστία του Blockchain καταρρέει, και δεν υπάρχει κάποιος εξουσιοδοτημένος που να μπορεί το διορθώσει. Ο PBFT επιδιώκει την επίτευξη συναίνεσης ενάντια σε τέτοια λάθη. Το PBFT χρησιμοποιεί την έννοια των πρωτευόντων και των δευτερευόντων «αντιγράφων», όπου τα δευτερεύοντα αντίγραφα αξιολογούν αυτόματα τις αποφάσεις που λαμβάνονται από το πρωτεύοντα και μπορούν συλλογικά να μεταβούν σε μια νέα κατάσταση πρωτευόντων δεδομένου ότι συμβιβάζεται με τις προδιαγραφές του δικτύου. Το Hyperledger, ένας ανοιχτός πόρος όπου η συνεισφορά του οδήγησε στο Linux Foundation, είναι ένα παράδειγμα project που βασίζεται σε PBFT.

1.4.5.6 Proof of Elapsed Time (PoET)

Το Proof of Elapsed Time (PoET) απελευθερώθηκε αρχικά στο Hyperledger χρησιμοποιώντας ένα TEE (Trusted Execution Environment). Όσον αφορά τη λειτουργικότητα το PoET εκλέγει ομότιμους για να εκτελέσει αιτήματα σε ένα συγκεκριμένο στόχο. Οι μεμονωμένοι ομότιμοι δοκιμάζουν μια εκθετικά κατανεμημένη τυχαία μεταβλητή και περιμένουν ένα χρονικό διάστημα που υπαγορεύεται από το δείγμα. Ο ομότιμος με το μικρότερο δείγμα κερδίζει την εκλογή. Η εξαπάτηση εμποδίζεται μέσω της χρήσης ενός TEE.

1.4.5.7 Ripple Protocol

Το πρωτόκολλο συναλλαγών Ripple (Ripple Transaction Protocol-RTXP), εκδόθηκε το 2012 και σκοπός του είναι να διευκολύνει τις χρηματοπιστωτικές συναλλαγές καθορίζοντας ένα σύνολο κανόνων που επιτρέπουν στους χρήστες να πραγματοποιήσουν ηλεκτρονικές συναλλαγές με οποιοδήποτε νόμισμα, κρυπτογράφηση ή άλλο μέσο. Ο Ripple Schwartz είναι ένας αλγόριθμος συναίνεσης που χρησιμοποιεί αξιόπιστα υπο-δίκτυα στα πλαίσια

ενός ευρύτερου δικτύου. Στο δίκτυο, οι κόμβοι χωρίζονται σε δύο τύπους: στον server για την συμμετοχή στη διαδικασία συναίνεσης και στον client για τη μεταφορά κεφαλαίων.

1.4.5.8 Tendermint

Το Tendermint είναι ένας αλγόριθμος βυζαντινής συναίνεσης όπου ένα block καθορίζεται σε ένα γύρο.. Η διαδικασία χωρίζεται σε τρία βήματα:

- Prevote : οι επικυρωτές επιλέγουν αν θα εκπέμπουν ένα prevote για το προτεινόμενο block.
- Precommit : Εάν ο κόμβος έχει λάβει περισσότερα από τα 2/3 των prevotes του προτεινόμενου block, εκπέμπει μία δέσμευση για αυτό το block. Αν ο κόμβος έχει λάβει περισσότερα από τα 2/3 των precommit πάει στο τελευταίο βήμα.
- Commit : Ο κόμβος επικυρώνει το block και μεταδίδει ένα commit για αυτό το block. Αν ο κόμβος έχει λάβει τα 2/3 των commit, δέχεται το block.

Property	PoW	PoS	PBFT	DPoS	PoET	Ripple	Tendermint
Node identity management	open	open	permissioned	open	-	open	permissioned
Tolerated power of the adversary	<25,0% computing power	<51,0% stake	<33,3% fault replicas	<51,0% validators	-	<20,0% faulty nodes in UNL	<33,3% byzantine voting power
Energy saving	No	Partial	Yes	Partial	Yes	Yes	Yes
Known apps or platforms	Bitcoin	Ethereum (next version)	Hyperledger Fabric	Bitshares	Sawtooth Lake	Ripple	Tendermint

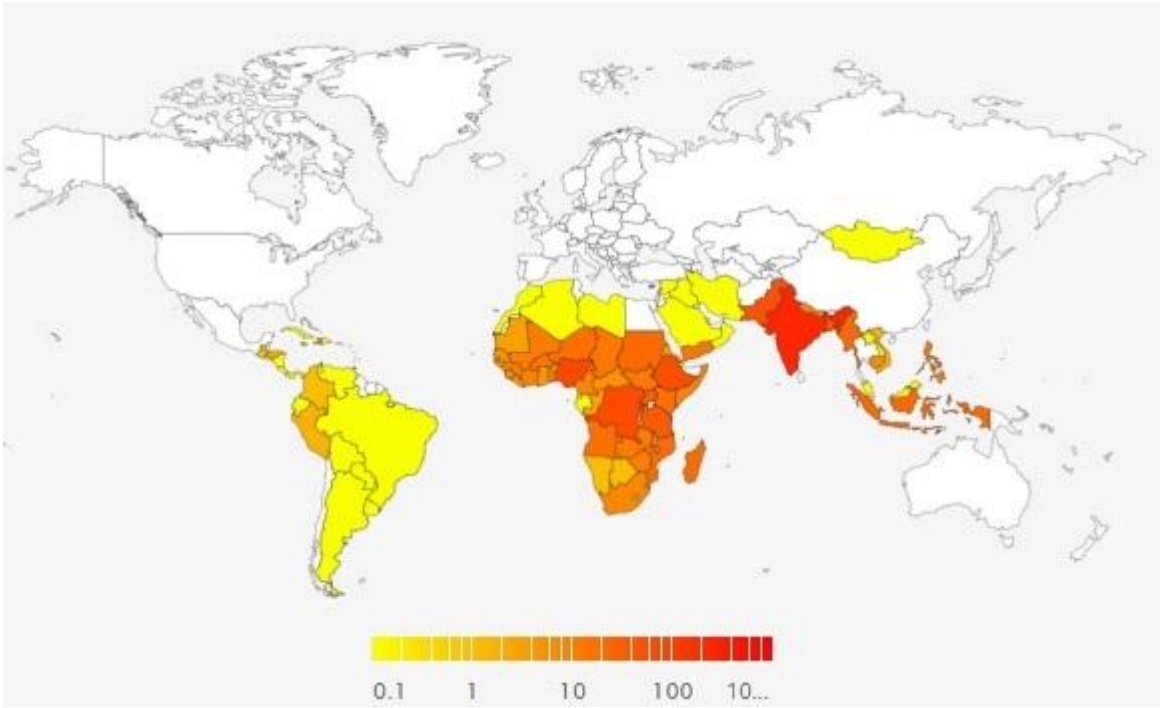
Table 5 – Σύγκριση των ιδιοτήτων μεταξύ των αλγόριθμων συναίνεσης [70]

2. Ανάπτυξη και Οφέλη της Έρευνας

2.1 Σκοπός της εργασίας

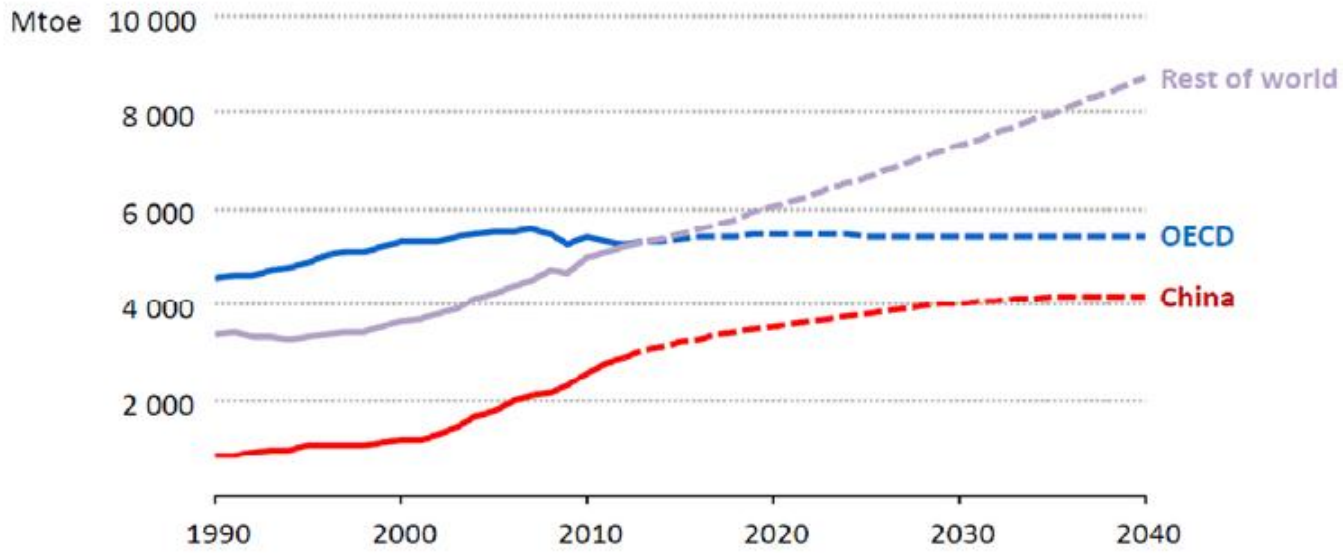
Ο βασικός στόχος στην εκπόνηση της εργασίας, είναι η βιβλιογραφική ανασκόπηση σε κατανεμημένες τεχνολογίες (DLT) και η εφαρμογή μιας τέτοιας διάταξης η οποία θα βασίζεται σε τεχνολογίες Blockchain για την υλοποίηση ενός ομότιμου δικτύου. Κάποια από τα προβλήματα που δημιουργούνται στο Large grid και στην τωρινή κατάσταση διανομής ενέργειας έχουν ήδη επισημανθεί, όπως επίσης και η σημαντικότητα χρήσης Μικροδικτύων. Έτσι όπως είναι ο δομημένος ο κόσμος, η ενέργεια δεν προσφέρεται σε ένα μεγάλο ποσοστό των πολιτών ακόμη και σε ολόκληρων πόλων.

Βάσει ερευνών που διεξήγαγε και δημοσιεύτηκαν στο Energy Access Outlook το 2017, εκτιμάται ότι το 1.1 δισεκατομμύριο του συνολικού πληθυσμού της γης δεν έχει πρόσβαση στην ηλεκτρική ενέργεια. Το 84% εξ αυτών κατοικούν στις αγροτικές περιοχές και περισσότερο από το 95% των κατοίκων χωρίς πρόσβαση στην ηλεκτρική ενέργεια βρίσκονται στην Αφρική και την ανεπτυγμένη Ασία. Παρακάτω φαίνεται στον χάρτη που ενδείκνυται ποιες χώρες δεν έχουν πρόσβαση στην ηλεκτρική ενέργεια.[28]



Εικόνα 16- Χώρες χωρίς ηλεκτρική ενέργεια σε κλίμακα 0.1 εκ έως 1000 εκ. [28]

Η ζήτηση για ενέργεια στον κόσμο θα συνεχίσει να αυξάνεται καθώς ο πληθυσμός στις αναδυόμενες χώρες μεγαλώνει. Η εστίαση σε αυτές τις χώρες είναι να βελτιωθεί η ποιότητα ζωής και να μειωθεί η φτώχεια, κάτι το οποίο απαιτεί οικονομική ανάπτυξη και περισσότερη χρήση των πόρων, και όχι λιγότερη ενέργεια. Οποιαδήποτε μείωση της κατανάλωσης ενέργειας στις ανεπτυγμένες χώρες, λόγω της βελτίωσης της απόδοσης και της συνειδητής χρήσης της ενέργειας, θα αντισταθμιστεί περισσότερο από την αύξηση της ζήτησης σε λιγότερο ανεπτυγμένες χώρες του κόσμου. Μια γενικά αποδεκτή υπόθεση είναι ότι η παγκόσμια ζήτηση ενέργειας θα αυξηθεί κατά 50% μέχρι το 2050, χωρίς αύξηση στις χώρες του OECD. [29]



Εικόνα 17 – Ζήτηση ενέργειας ανά χώρα μέχρι το 2040 [29]

Οι OECD είναι χώρες που συνεργάζονται μεταξύ τους για βασικά παγκόσμια ζητήματα σε εθνικό, περιφερειακό και τοπικό επίπεδο. Σήμερα τα μέλη-χώρες OECD είναι 36 και φαίνονται παρακάτω: Αυστραλία, Αυστρία, Βέλγιο, Καναδάς, Χιλή, Τσεχία, Δανία, Εσθονία, Φιλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ισλανδία, Ιρλανδία, Ισραήλ, Ιταλία, Ιαπωνία, Κορέα, Λετονία, Λιθουανία, Λουξεμβούργο, Μεξικό, Ολλανδία, Νέα Ζηλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Σλοβακία, Σλοβενία, Ισπανία, Σουηδία, Ελβετία, Τουρκία, Αγγλία, Αμερική. [29]

Αυτό είναι ένα από τα επιμέρους προβλήματα που επιλύεται με την εφαρμογή Μικροδικτύου και κατ' επέκταση Smart grid στο δίκτυο ενέργειας που επικρατεί τώρα. Με την χρήση υποδίκτυων στο Large grid, όλοι οι χρήστες γίνονται server, οπότε δεν έχουν πλέον την ιδιότητα μόνο του καταναλωτή αλλά και του παραγωγού και δεν εξαρτώνται πλέον από ένα και μόνο πάροχο, δίνοντας έτσι την δυνατότητα διανομής ενέργειας από κεντρικό πάροχο σε οποιονδήποτε χρήστη που συμμετέχει στο δίκτυο αυτό. Κατ' αυτό τον τρόπο η ενέργεια θα μπορεί να διαδοθεί, χωρίς την εγκατάσταση επιπλέον υποδομών από τον πάροχο που τν προσφέρει. Επιπλέον άλλα προβλήματα που επιλύονται είναι η ασφάλεια στις συναλλαγές, καθώς ότι συναλλαγή πραγματοποιείται αποθηκεύεται στο Blockchain και δεν μπορεί να χαθεί, ταχύτητα και ευελιξία στην επέκταση του.

Στο προηγούμενο κεφάλαιο έγινε αναφορά στις βασικές αρχές των DLT τεχνολογιών, με ιδιαίτερο ενδιαφέρον στα Blockchain, στα είδη που υπάρχουν και στην αρχή λειτουργίας τους. Σε αυτό το κεφάλαιο θα επισημανθούν κάποια Projects που τα οποία είναι βασισμένα σε Blockchain τεχνολογία, το πρόβλημα που επικρατεί και χρήζει εφαρμογής των Projects, θα αναλυθούν εκτενώς κάποιες απαραίτητες έννοιες όπως είναι το P2P δίκτυο, το Μικροδίκτυο, το Ethereum και τα Smart Contracts τα οποία χρειάζονται στην ανάπτυξη της διάταξης του συστήματος αυτής της πτυχιακής και τα βήματα που θα πραγματοποιηθούν.

Η μεθοδολογία που θα ακολουθηθεί είναι η υλοποίηση ενός ομότιμου δικτύου P2P βασισμένο σε τεχνολογία Blockchain μέσω των εργαλείων που προσφέρονται από το Ethereum. Θα δημιουργηθεί ένα δίκτυο δύο ομότιμων χρηστών Private Blockchain στα πλαίσια ενός πραγματικού Μικροδικτύου και θα ολοκληρωθεί μία συναλλαγή. Το δίκτυο που θα δομηθεί είναι ιδιωτικό παρέχοντας την δυνατότητα συμμετοχής εξωτερικών χρηστών δεδομένου ότι θα τους δίνεται εξουσιοδότηση.

2.2 Τρέχοντα Projects με Blockchain

Ποικίλα Projects έχουν εφαρμογή σε επίπεδο διακίνησης της ηλεκτρικής ενέργειας βασισμένα σε Blockchain τεχνολογίες. Οι μεγάλες εταιρείες, τείνουν να επενδύουν στην ανάπτυξη και εφαρμογή τέτοιων Projects με απώτερο σκοπό στην πλήρη αυτοματοποίηση των συναλλαγών χωρίς την παρέμβαση του ανθρώπου. Η λογική είναι, το ρεύμα να ταξιδεύει στην χαμηλότερη δυνατή απόσταση μεταξύ των χρηστών σε ένα αποκεντρωμένο Smart grid δίκτυο ενσωματώνοντας μία ολοκληρωμένη Κατανεμημένη Ανανεώσιμη Πηγή Ενέργειας (DREs- Distributed Renewable Energy sources). Μερικά από τα σημαντικότερα Projects και τα πεδία δράσης τους περιγράφονται παρακάρω.

2.2.1 Enerchain

Το Enerchain Project αναπτύχθηκε από την Ponton τον Ιούνιο του 2016. Η Ponton αναζητούσε μία πλατφόρμα μέσω τα οποίας θα μείωνε το κόστος που συσχετίζεται με το χονδρικό εμπόριο στην διακίνηση της ενέργειας, επιτρέποντας στους συμμετέχοντες να ανταλλάζουν ισχύς και καύσιμα με ένα αποκεντρωμένο τρόπο χωρίς την παρεμβολή διαμεσολαβητών. Το Enerchain επιτρέπει στους έμπορος να στέλνουν ανώνυμα παραγγελίες σε ένα αποκεντρωμένο “βιβλίο παραγγελιών” στο οποίο έχουν πρόσβαση όλοι οι έμποροι του δικτύου. Το Enerchain χρησιμοποιεί τον αλγόριθμο Proof-of-Concept (PoC) και συναρτήσει με τεστ που έχουν πραγματοποιηθεί μαζί με τους συμμετέχοντες, έχει καταλήξει να είναι το πιο γρήγορο Blockchain οριστικοποιώντας κάθε δευτερόλεπτο block και ολοκληρώνοντας μία συναλλαγή σε λιγότερο από ένα δευτερόλεπτο. Το Project ξεκίνησε το 2017 σαν κοινοπραξία σε 15 Ευρωπαϊκές εταιρίες ενέργειας. Έκτοτε το Enerchain έχει επεκταθεί και έχει φτάσει σε σημείο από τον Απρίλιο του 2018 να έχει επεκταθεί σε 42 εταιρείες. Μερικά χαρακτηριστικά το σε λειτουργικό και τεχνικό επίπεδο παρουσιάζονται παρακάτω: [30]

Λειτουργικά Χαρακτηριστικά

- Δημιουργία, τροποποίηση, ακύρωση και εκτέλεση εντολών
- Χρησιμοποιεί πιστωτικά όρια για να επιλέξει με ποιον θα συναλλάξεις
- Τοποθετεί παραγγελίες ανώνυμα
- Τα αρχεία συναλλαγών λαμβάνονται απευθείας στο ETRM σύστημα του χρήστη για επεξεργασία μετά την πώληση.
- Δυνατότητα εμπορίου ηλεκτρικής ενέργειας και φυσικού αερίου, σε χονδρική και περιφερειακή ενέργεια
- Υποστήριξη μη τοπικών προϊόντων όπως καμπύλες φορτίου κτλ.
- Υποστήριξη συνεχούς διαπραγμάτευσης
- Άμεση πρόσβαση στην αποκεντρωμένη αγορά

Τεχνικά Χαρακτηριστικά

- Permissioned Blockchain χρησιμοποιώντας public key πιστοποιητικά για έλεγχο ταυτότητας συμμετεχόντων και κρυπτογράφηση end-to-end
- Εξαιρετικά γρήγορο: το block δημιουργείται σε ένα δευτερόλεπτο, αποστολή μηνυμάτων end-to-end σε λιγότερο από ένα δευτερόλεπτο
- Έλεγχος διείσδυσης, έλεγχος φορτίου, έλεγχος ασφάλειας
- Υποστηρίζει περιβάλλον πολλαπλών cloud
- Αρχιτεκτονική αποτυχίας : σε περίπτωση αποτυχίας ενός κόμβου, ο χρόνος αποτυχίας περιορίζεται σε λίγα δευτερόλεπτα
- Ανοικτό API για αποστολή και λήψη συναλλαγών Blockchain

2.2.2 Grid+

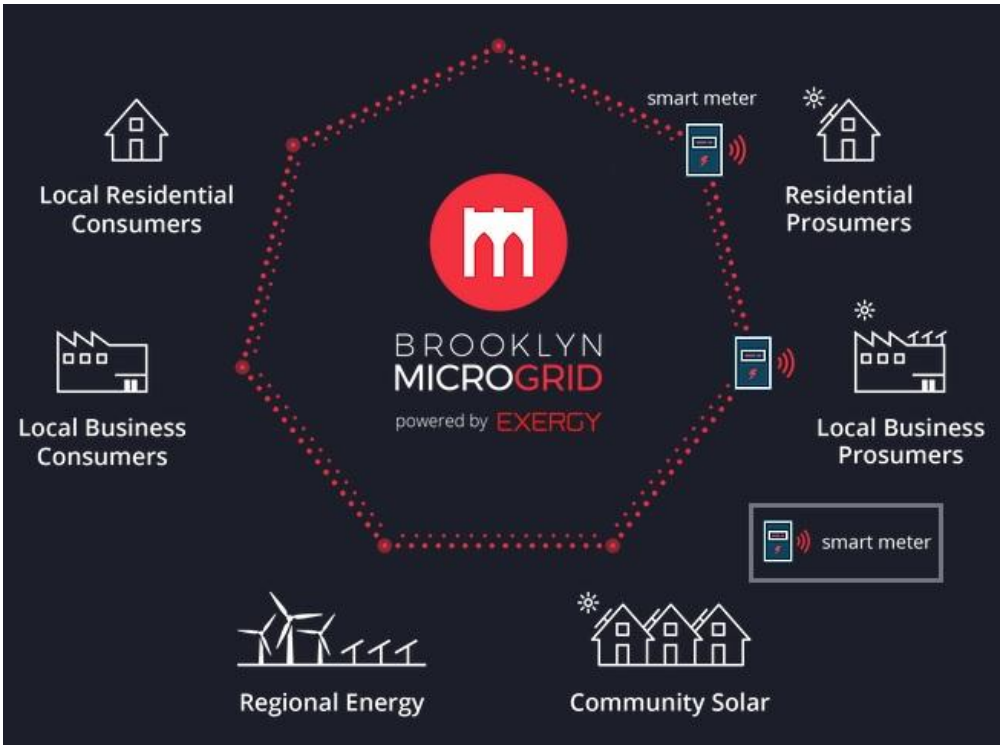
Παρομοίως, με το εμπόριο χονδρικής, το Blockchain ενισχύει και το λιανικό εμπόριο της αγοράς ηλεκτρικής ενέργειας, χρησιμοποιώντας κρυπτονομίσματα για την εξόφληση λογαριασμών και άλλων διαδικασιών που εμπεριείχαν μετρητά. Το Blockchain, μειώνει το μεταβλητό κόστος των πληρωμών επεξεργασίας και λογιστικής εκτελώντας ένα έξυπνο συμβόλαιο (smart contract). Μερικοί οραματίζονται ήδη την οριστική αυτοματοποίηση των μετρητών και την κατάργηση διαμεσολαβητών από λιανικούς ή χονδρικούς έμπορους. Το Blockchain εμπλουτίζει περισσότερο τους πελάτες λιανικής, από την μεγαλύτερη διαφάνεια στα ενεργειακά τέλη, την ικανότητα να εισάγει και να αφήνει τα ενεργειακά συμβόλαια πιο ρευστά, και την προσφορά περισσότερων επιλογών στον ενεργειακό εφοδιασμό.

Το Grid+ ξεκίνησε στο Austin, Texas και αναπτύσσει μία αυτοματοποιημένη πλατφόρμα βασισμένη στο Ethereum που θα λειτουργεί σαν λιανοπωλητής στην αγορά ενέργειας. Με την αυτοματοποίηση των λογαριασμών και του διακανονισμού, το Grid+ στοχεύει στο να παρέχει είσοδο στους πελάτες που δεν έχουν πρόσβαση στο χονδρικό εμπόριο. Το project βασίζεται σε δύο μοντέλα ψηφιακών νομισμάτων και τον πελάτη, ενεργοποιημένο μέσω μιας ενεργειακής πύλης συνδεδεμένης στο διαδίκτυο που καλείται Grid+ “Smart Agent”. Μακροπρόθεσμα, αυτό θα χρησιμοποιηθεί ως μία αυτοματοποιημένη μονάδα επεξεργασίας πληρωμών, διαβάζοντας τα δεδομένα του έξυπνου μετρητή που έχει το σπίτι και πληρώνοντας σε πραγματικό χρόνο την χρήση του ηλεκτρικού ρεύματος (σε διάστημα 15 λεπτών έως μία ώρα, ανάλογα με την κίνηση της αγοράς). Αυτό θα πραγματοποιηθεί με την εκτέλεση των έξυπνων συμβολαίων πάνω στο Blockchain του Ethereum χρησιμοποιώντας το ψηφιακό νόμισμα “BOLT” , τα οποία με ασφάλεια αποθηκεύονται στο ewallet (το BOLT είναι ένα σταθερό νόμισμα που η αντιπροσωπευτική του αξία είναι 1 δολάριο της ενέργειας από το Grid+). Αυτή η τεχνολογία θα ανοίξει το δρόμο για τη χρήση της τεχνητής νοημοσύνης και άλλων αναδυόμενων τεχνολογιών για να προσφέρει στους καταναλωτές μεγαλύτερο έλεγχο του κόστους ηλεκτρικής ενέργειας [31]

2.2.3 Brooklyn Microgrid Project (BMG)

LO3 Energy ονομάζεται η εταιρεία που βρίσκεται πίσω από την ανάπτυξη του πρώτου P2P Blockchain βασισμένο στο εμπόριο ενέργειας, το BMG (Brooklyn Microgrid), το οποίο χρησιμοποιεί την δική το πλατφόρμα το Exergy. Το BMG επιτρέπει στους συμμετέχοντες να ανταλλάξουν ενέργεια χρησιμοποιώντας τα Smart contracts του Blockchain. Είναι δομημένο σε μία Ethereum πλατφόρμα εξειδικευμένης ενεργειακής αγοράς, που επιτρέπει στους καταναλωτές και τους παραγωγούς να ανταλλάσουν ηλεκτρική ενέργεια τοπικά. Τα Smart Contracts ψηφιοποιούν τα πράσινα πιστοποιητικά, αναδεικνύοντας το πλεόνασμα της ενέργειας που παράχθηκε από τους παραγωγούς όπως αυτά καταγράφηκαν στο Blockchain μέσων των έξυπνων μετρητών, και δημιουργούν το P2P δίκτυο αγοράς στο οποίο αυτά τα πιστοποιητικά ανταλλάσσονται. Η πρώτη συναλλαγή του Project εκτελέστηκε το 2016, συνδέοντας 5 σπίτια που υποστήριζαν Ηλιακή Φωτοβολταϊκή (PV – Photovoltaic) παραγωγή με 5 πελάτες. Στα τέλη του 2017, υπήρχαν ήδη 60 ηλιακές εγκαταστάσεις και 500 πελάτες. [32]

.



Εικόνα 18 – Το δίκτυο του BMG με Smart meters για την συλλογή δεδομένων [32]

2.2.4 TenneT

Σε πολλές ενεργειακές αγορές, μεταβλητές στην αιολική και ηλιακή παραγωγή δημιουργούν προκλήσεις στους ικανότητα των διαχειριστών συστημάτων, να εξισορροπήσουν βραχυπρόθεσμα την προσφορά και ζήτηση της παροχής χωρίς να περιορίζουν την παραγωγή ανανεώσιμων πηγών ενέργειας. Η δυνατότητα επίτευξης ενός ισχυρού ευέλικτου συστήματος ενέργειας είναι μεγάλη. Το 2016, πελάτες στη Γερμανία εξυπηρετούνται από το Διαχειριστή Συστήματος Μεταφοράς (TSO – Transmission System Operator) οι οποίοι πληρώνουν περίπου 800 εκατομμύρια ευρώ σε μέτρα (επανεπεξεργασία, αποθέματα πλέγματος, μείωση της ισχύος ανέμου) για να εξασφαλίσουν ότι η μεταφορά ηλεκτρικής ενέργειας ήταν εντός των ορίων και δυνατοτήτων του grid. Το Blockchain θα μπορούσε να βοηθήσει προμηθεύοντας υπηρεσίες ευελιξίας καταγράφοντας την διαθεσιμότητα πόρων και αυτοματοποιώντας την απάντηση της ζήτησης και τη δραστηριότητα των DER σε πραγματικό χρόνο.

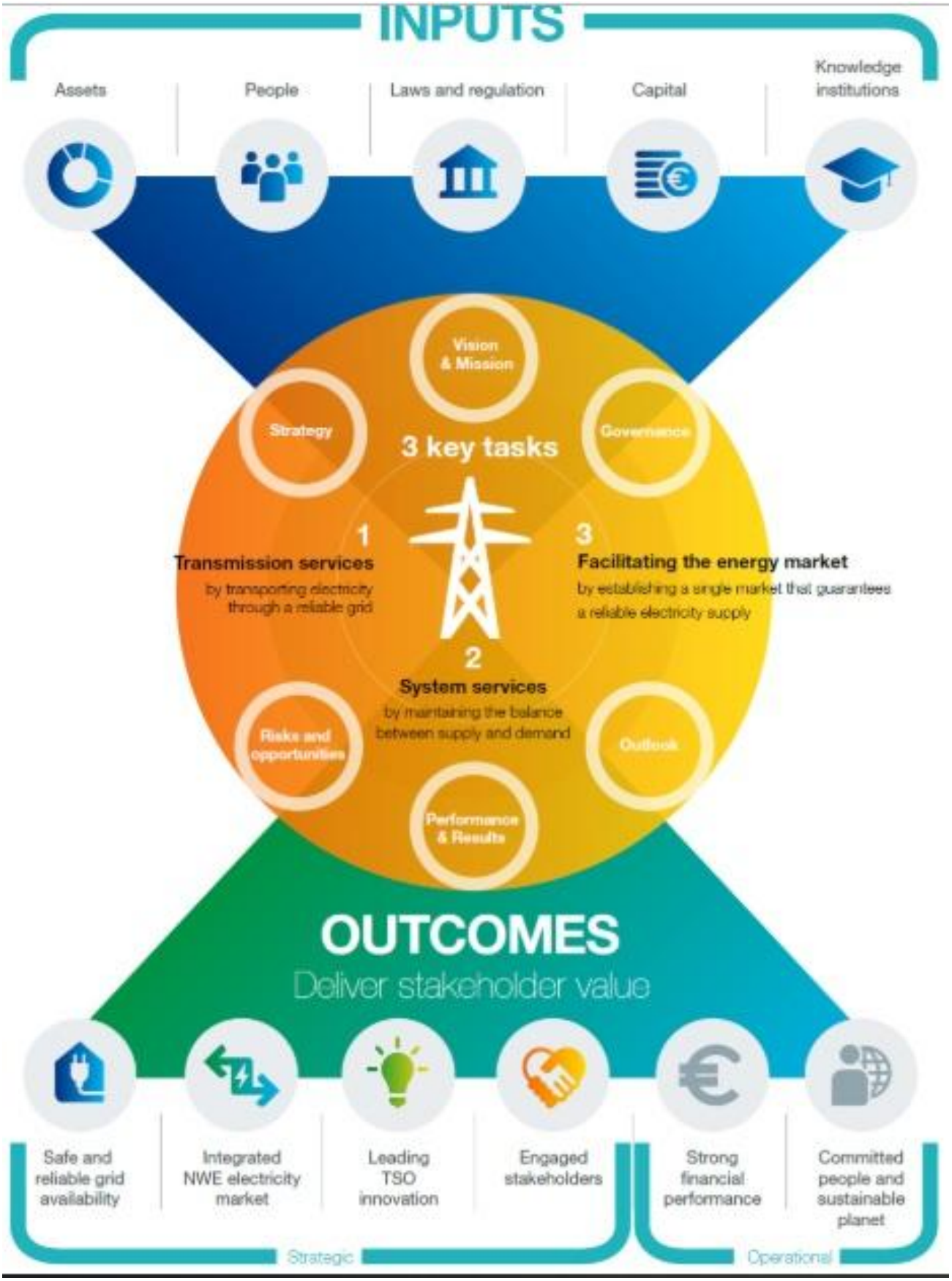
Το TenneT Project, είναι ένα TSO και έχει συνεργαστεί με τις Vandebron, Sonnen και IBM σε projects που βασίζονται σε Blockchains και προορίζονται να ενισχύσουν την διαθεσιμότητα ευέλικτων υπηρεσιών στον διαχειριστή. Η Vandebron θα συνεργαστεί με τους ιδιοκτήτες Ηλεκτρικών Οχημάτων (EV) για να κάνουν διαθέσιμη την χωρητικότητα της μπαταρίας των EV διαθέσιμη στο να ενισχύσουν το TenneT να ισορροπήσει το grid. Η Vandebron θα προμηθεύσει την υπηρεσία αυτοί στους ιδιώτες χωρίς συμβιβασμούς στη διαθεσιμότητα των ιδιοκτητών μπαταριών των EV. Τα Blockchain ενεργοποιούν τα EV να συμμετάσχουν καταγράφοντας την διαθεσιμότητα τους και τις ενέργειες τους από τις απαντήσεις των σημάτων του TenneT. [33]

Το TenneT μετασχηματίζεται για βιώσιμη ανάπτυξη βασισμένη σε τέσσερις στρατηγικούς πυλώνες:

- Ενεργοποιεί τους ανθρώπους της και την οργάνωσή της, σε ένα περιεκτικό και ασφαλές περιβάλλον όπου οι άνθρωποι απολαμβάνουν να έρχονται στην εργασία. Χτίζουν ένα μοντέλο ηγεσίας που ενδυναμώνει, εμπνέει και δημιουργεί ευκαιρίες ανάπτυξης, έτσι ώστε όλοι να μπορούν να αποδώσουν το καλύτερο δυνατό έργο τους και να εργαστούν ως ένα.
- Οδηγεί την ενεργειακή μετάβαση ως διαχειριστής πράσινου δικτύου και επισκεπτόμενου ηγέτη, αναπτύσσοντας καινοτόμα μέσα και καθιερώνοντας έναν καίριο ρόλο στον κόσμο των ενεργειακών δεδομένων.
- Ασφαλίζει τον εφοδιασμό του σήμερα και του αύριο, διατηρώντας το δίκτυο για να εκπληρώνονται οι στόχοι αξιοπιστίας και να το λειτουργεί με τις μέγιστες δυνατότητές του.
- Διασφαλίζει την οικονομική υγεία, εφαρμόζοντας ένα ρυθμιστικό πλαίσιο για να στηρίξει τη στρατηγική της και να παρέχει απόδοση σύμφωνα με το τι προσδοκούν οι προμηθευτές κεφαλαίου.

Το TenneT έχει ένα επιχειρησιακό μοντέλο στην Ευρώπη που “τρέχει” δύο TSO στην Γερμανία και Ολλανδία και απαρτίζεται από τέσσερις διεργασίες για να εξασφαλίσει την προμήθεια υπηρεσιών μεταφοράς ενεργείας:

- Η διασφάλιση μιας ασφαλούς συνεχούς παροχής ενέργειας
- Η παροχή υπηρεσιών μετάδοσης, μεταφέροντας ενέργεια από το Large grid δίκτυο υψηλής τάσης από όπου παράγεται μέχρι εκεί που καταναλώνεται
- Η παροχή υπηρεσιών για εξασφάλιση της ροής της ηλεκτρικής ενέργειας στην Ολλανδία και σε μεγάλα τμήματα της Γερμανίας
- Η ομαλή και σταθερή λειτουργία της αγοράς ηλεκτρικής ενέργειας για την υποστήριξη της μετάβασης από την μεγάλη κλίμακα στις ανανεώσιμες πηγές ενέργειας



Εικόνα 19 – Το Επιχειρησιακό μοντέλο της TenneT [33]

2.2.5 Share and Charge

Καθώς τα EV γίνονται πιο διακριμένα, οι διαχειριστές συστημάτων αντιμετωπίζουν προκλήσεις στην παροχή νέου EV που σχετίζεται με κινητό φορτίο και , ενδεχομένως στην χρήση αποθηκευμένου πλεονάσματος ενέργειας για βελτίωση της ευελιξίας του συστήματος. Με την τεχνολογία Blockchain βελτιώνεται ο συντονισμός χρέωσης στα EV, διευκολύνοντας τις ενεργειακές πληρωμές σε σταθμούς φόρτισης και ενεργοποιώντας τους οδηγούς πάρουν αποφάσεις που αφορούν την φόρτιση βασιζόμενοι στον χάρτη των σταθμών και στα δεδομένα τιμολόγησης σε πραγματικό χρόνο.

Ένα ενεργό Project σε αυτό τον χώρο, είναι της MotionWErk το Share & Charge που αναπτύχθηκε στο Innogy της Γερμανίας. Σε συνεργασία με το γερμανικό Blockchain του Slock.it, δημιουργήσανε ένα P2P δίκτυο υπηρεσιών επιτρέποντας στα EV και στους ιδιοκτήτες των σημείων φόρτισης, να νοικιάζουν τις υποδομές φόρτισης αυτόνομα στον οποιονδήποτε, χωρίς την ανάγκη διαμεσολαβητή. Είναι το πρώτο Project, το Share & Charge, που επέτρεψε στους ιδιώτες των EV, να φορτίσουν το όχημα τους πραγματοποιώντας ψηφιακή πληρωμή χρησιμοποιώντας μία εφαρμογή κινητού.

Οι ιδιώτες των σημείων φόρτισης χρησιμοποιούσαν την εφαρμογή για να κάνουν την υποδομή τους διαθέσιμη, να ορίσουν δομές τιμολόγησης και να συλλέξουν αμοιβές. Μέχρι τον Απρίλιο του 2018, η υπηρεσία ήταν διαθέσιμη σε 1.000 ιδιοκτήτες EV με 1.250 ιδιωτικά και δημόσια σημεία φόρτισης εγγεγραμμένα στην Γερμανία. Το σύστημα χρησιμοποιούσε ένα e-wallet και smart contracts σε public Ethereum Blockchain σαν ένα P2P στρώμα συναλλαγής. Συμπεριλάμβανε το κρυπτονόμισμα “Mobility Token”. Το Share & Charge ήταν η πρώτη πλατφόρμα συναλλαγών e-mobility που χρησιμοποιούσε Blockchain.

Το Share & Charge μετατρέπεται σε μια ανοικτή πηγή και ένα αποκεντρωμένο ψηφιακό πρωτόκολλο για την φόρτιση των EV.

2.2.6 Keyless Signature Infrastructure (KSI)

Το κατανεμημένο σύστημα γίνεται όλο και πιο σύνθετο εξαιτίας της συμπερίληψης των DER και των ψηφιακών τεχνολογιών. Τα μοντέρνα DSO (Distributed System Operators) και TSO (Transmission System Operators) αντιμετωπίζουν προκλήσεις κατανόησης της παρούσας κατάστασης του συστήματος, αποθήκευσης και ανάλυσης μεγάλου όγκου δεδομένων. Ταυτόχρονα η ψηφιοποίηση έχει μειώσει την ασφάλεια τους συστήματος ενέργειας κάνοντας στο ευπαθές σε κακόβουλους χρήστες.

Τα Blockchain βοηθούν στην ενίσχυση της διαχείρισης του δικτύου διατηρώντας αυτόματα τα επαληθεύσιμα στοιχεία της κατάστασης των δεδομένων στο δίκτυο. Επιπλέον, η Blockchain τεχνολογία προστατεύει το δίκτυο από σχετικές απειλές λόγω του εγγενή πλεονασμού του και του γεγονότος ότι δεν έχει κάποιο σημείο επίθεσης, θεωρείται tamper-proof.

Υπάρχουν λίγα ενεργά Projects που χρησιμοποιούν Blockchain τεχνολογία για να ενισχύσουν την διαχείριση του δικτύου και την ασφάλεια. Ένα εξ αυτών είναι υπό την αιγίδα της Guardtime και ονομάζεται Keyless Signature Infrastructure (KSI) και χρησιμοποιεί permissioned Blockchain για την προστασιών υποδομών κρίσιμης σημασίας. Το KSI επιτρέπει την επαλήθευση του χρόνου, της τοποθεσίας και της αυθεντικότητας των υπογεγραμμένων δεδομένων, και την συνεχή παρακολούθηση των συστημάτων διαχείρισης.

Το KSI Blockchain ξεπερνά δύο σημαντικές αδυναμίες των παραδοσιακών Blockchain, καθιστώντας το χρήσιμο στην βιομηχανική κλίμακα: [34]

- Επεκτασιμότητα: οι παραδοσιακές προσεγγίσεις Blockchain κλιμακώνονται στην πολυπλοκότητα O (n) δηλαδή αυξάνονται γραμμικά με τον αριθμό των συναλλαγών. Σε αντίθεση με την κλίμακα KSI στην κλίμακα O (t) - αναπτύσσεται γραμμικά με το χρόνο και ανεξάρτητα από τον αριθμό των συναλλαγών.
- Χρόνος διακανονισμού: Με τον περιορισμό του αριθμού των συμμετεχόντων καθίσταται δυνατή η ταυτόχρονη επίτευξη συναίνεσης, εξαλείφοντας την ανάγκη για Proof of Work και εξασφαλίζοντας ότι η διευθέτηση μπορεί να συμβεί μέσα σε ένα δευτερόλεπτο.

2.2.7 SolarCoin

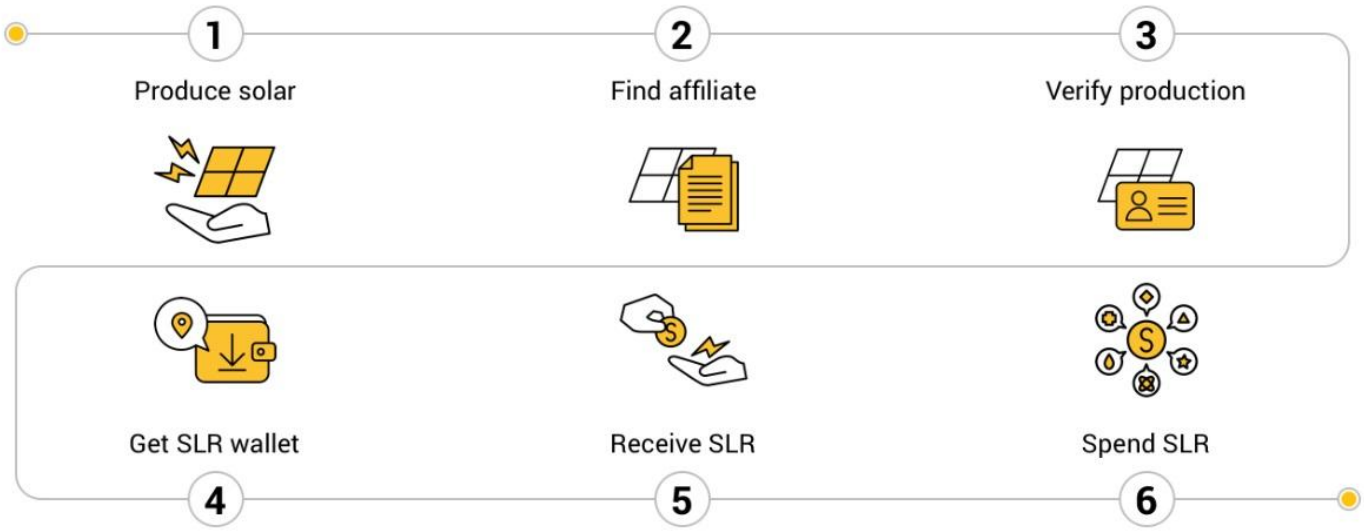
Συστήματα βασισμένα στην αγορά για την προώθηση της ανάπτυξης ανανεώσιμων πηγών ενέργειας και τις μειώσεις των εκπομπών αερίων θερμοκηπίου υπάρχουν σε πολλές χώρες. Αυτά περιλαμβάνουν μηχανισμούς αντιστάθμισης άνθρακα, φόρων άνθρακα και των κεφαλαιακών και εμπορικών συστημάτων. Κοινές προκλήσεις με αυτά τα συστήματα περιλαμβάνουν ην δαπανηρή εξάρτηση από πρακτικές χειρωνακτικού ελέγχου, περιορισμένη γεωγραφική κλίμακα και κεντρική και αδιαφανή διαχείριση. Τέτοιες προκλήσεις μπορούν να οδηγήσουν σε υψηλό κόστος συναλλαγών, ακόμη και σε απάτες. Κάποιες από αυτές τις προκλήσεις μπορούν να αντιμετωπιστούν με την ψηφιοποίηση των χαρακτηριστικών ανανεώσιμων πηγών και την αποθήκευση αυτών σε Blockchain. Τα δεδομένα που αποθηκεύονται σε ένα Blockchain αποτυπώνονται ασφαλή και ακριβή, έτσι με αυτό τον τρόπο οι συναλλαγές πραγματοποιούνται εξαλείφοντας την ανάγκη κεντρικής υπηρεσίας επαλήθευσης.

Ένα παράδειγμα σε αυτόν τον χώρο είναι το SolarCoin, ένα ηλιακό κίνητρο κρυπτογράφησης του οποίου οι στόχοι είναι να μειωθεί το κόστος ελέγχου, να βελτιωθεί η διαφάνεια, και να βελτιωθεί και η ρευστότητα για πιστώσεις που προέρχονται από την ηλιακή ενέργεια. Το SolarCoin αποστέλλεται σε ηλιακές γεννήτριες μετά από αιτήματα για παραγωγή από καταχωρημένες εγκαταστάσεις, τα οποία με την σειρά τους αποστέλλονται στο Ίδρυμα SolarCoin η σε κάποια θυγατρική. Οι απαιτήσεις μπορούν επίσης να παραχθούν αυτόματα από έξυπνους μετρητές, και όλες οι συναλλαγές να είναι ορατές στο SolarCoin Blockchain. Από τον Μάρτιο του 2018, SolarCoins έχουν χορηγηθεί σε 58 χώρες και η αυξανόμενη ζήτηση για κρυπτονομίσματα αποσκοπεί στην παροχή κινήτρων για παραγωγή ανανεώσιμης ενέργειας. Το SolarCoin αποτελεί ανταμοιβή για τους παραγωγούς ηλιακής ενέργειας. Το Ίδρυμα SolarCoin ανταμείβει τους παραγωγούς ενέργειας με ψηφιακά νομίσματα που βασίζονται σε Blockchain, με αναλογία ένα SolarCoin (SLR) ανά Megawatt-Hour (MWh) ηλιακής ενέργειας που παράγεται. [35]

2.2.7.1 Κερδίζοντας SolarCoins

Οποιοσδήποτε παραγωγός ηλιακής ενέργειας υποβάλλει ελεύθερα αίτηση με έναν συνεργάτη της SolarCoin για την καταχώριση της ηλιακής του εγκατάστασης. Οι αιτούντες κατεβάζουν χωρίς χρέωση ένα ψηφιακό πορτοφόλι SolarCoin για να δημιουργήσουν μια διεύθυνση παραλαβής που λειτουργεί ως τραπεζικός λογαριασμός. Αυτή η διεύθυνση και μερικά στοιχεία της ηλιακής εγκατάστασης μοιράζονται με τον εκάστοτε συνεργάτη.

Το Ίδρυμα SolarCoin αποστέλλει στη συνέχεια το SolarCoins στο πορτοφόλι του αιτούντα με αναλογία 1 SolarCoin ανά 1 MWh επαληθευμένης παραγόμενης ηλεκτρικής ενέργειας. Οι αιτούντες μπορούν να αποθηκεύσουν, να ανταλλάξουν ή να ξοδέψουν το SolarCoins όπως επιθυμούν και να λαμβάνουν συνεχείς επιχορηγήσεις για τα επόμενα 20-30 χρόνια που παράγουν ενέργεια. Έχουν δημιουργηθεί 97,5 δισεκατομμύρια μη κυκλοφορημένα SolarCoins για τους παραγωγούς ενέργειας.



Εικόνα 20 – Σχεδιάγραμμα ανταμοιβής ενός SolarCoin [35]

2.2.7.2 Ξοδεύοντας SolarCoins

Τα SolarCoins αποστέλλονται στις διευθύνσεις (λογαριασμούς) σε ψηφιακά πορτοφόλια και χρησιμοποιούνται ως νόμισμα ή μπορούν να αποθηκευτούν μακροπρόθεσμα σε offline πορτοφόλια. Το SolarCoin μπορεί να αποτελέσει αντικείμενο διαπραγμάτευσης για κυβερνητικά νομίσματα σε κρυπτογραφικές ανταλλαγές ή σε επιχειρήσεις που τα αποδέχονται.

2.3 Δυναμική του Blockchain στην Ηλεκτρική ενέργεια

Το συμβατικό ηλεκτρικό σύστημα, είναι μία διαμόρφωση μονής κατεύθυνσης που παραδίδει ενέργεια από το εργοστάσιο παραγωγής στον καταναλωτή, αλλά όπως αναδύεται από τον ρόλο των πωλητών (prosumers), το Μικροδίκτυο επιτρέπει τη διαμόρφωση πολλαπλής κατεύθυνσης και έχει αρχίσει ήδη να αναπτύσσεται. Με την εφαρμογή Blockchain τεχνολογία στο Μικροδίκτυο, εξοικονομείται χρόνος και χρήματα συγκριτικά με ένα συμβατικό Μικροδίκτυο.

Η ενεργειακή βιομηχανία μεταβάλλεται συνεχώς, και υπάρχει η τάση καθιέρωσης περισσότερων ενεργειακών, αποκεντρωμένων και ψηφιακών συστημάτων. Η κατανεμημένη και αμετάβλητη φύση του Blockchain θα μπορούσε ενδεχομένως να αξιοποιηθεί για να επιταχύνει αυτό το μετασχηματισμό και να αντιμετωπίσει μερικές από τις κρίσιμες προκλήσεις που αντιμετωπίζει η βιομηχανία. Ωστόσο, η εμφάνιση μιας νέας και ενδεχομένως ανατρεπτικής τεχνολογίας παρουσιάζει την αβεβαιότητα και την απειρία ως προς προκλήσεις που εκτιμούνται ότι θα προκύψουν, και έως ένα βαθμό η υλοποίηση του Blockchain στον ενεργειακό τομέα εξακολουθεί να είναι σε μεγάλο βαθμό άγνωστη.

Η Blockchain τεχνολογία έχει τη δυνατότητα να είναι πιο άμεσα επιτυχημένη σε τομείς που δεν υπάρχουν φυσικές συναλλαγές. Σε τέτοιους τομείς, παρέχουν αξιόπιστα αρχεία δοσοληψιών, χωρίς την ανάγκη επαλήθευσης φυσικής συναλλαγής. Από όλους τους τομείς φυσικών συναλλαγών, αυτός του ηλεκτρισμού είναι πιο επιρρεπής για την ενσωμάτωση Blockchain. Τα τελευταία χρόνια η εμφάνιση των Blockchain και η επιτακτική ανάγκη εύρεσης projects , μερικά εκ των οποίων αναφέρθηκαν παραπάνω, για την ενίσχυση της αγοράς της ηλεκτρικής ενέργειας διαρκώς επεκτείνεται. Παρά τις δυνατότητες όμως που έχει η εμφάνιση αυτής της νέας τεχνολογίας, το μέλλον του στα συστήματα ηλεκτρισμού είναι αβέβαιο. Οι ιδέες που παρουσιάζονται είναι καινοτόμες, αλλά υστερούν σε κλιμάκωση τα τωρινά Project και η εφαρμογή που έχουν. [53]

2.3.1 Το Blockchain ως κατανεμημένο και αποκεντρωμένο σύστημα στην αγορά

Το Blockchain παρέχει ένα αποκεντρωμένο και κατανεμημένο περιβάλλον επεξεργασίας για τη διασύνδεση της υποδομής IoT. Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, το Blockchain είναι μία κατανεμημένη τεχνολογία της οικογένειας των DLT, όπου συναρτήσει με το IoT δίνεται η δυνατότητα δημιουργίας Μικροδικτύου ομότιμων χρηστών. Παρέχει τις ακόλουθες θεμελιώδεις υπηρεσίες για να χειριστεί τα δεδομένα IoT και να υποστηρίξει τις αλληλεπιδράσεις διαφόρων ενεργειακών οντοτήτων.

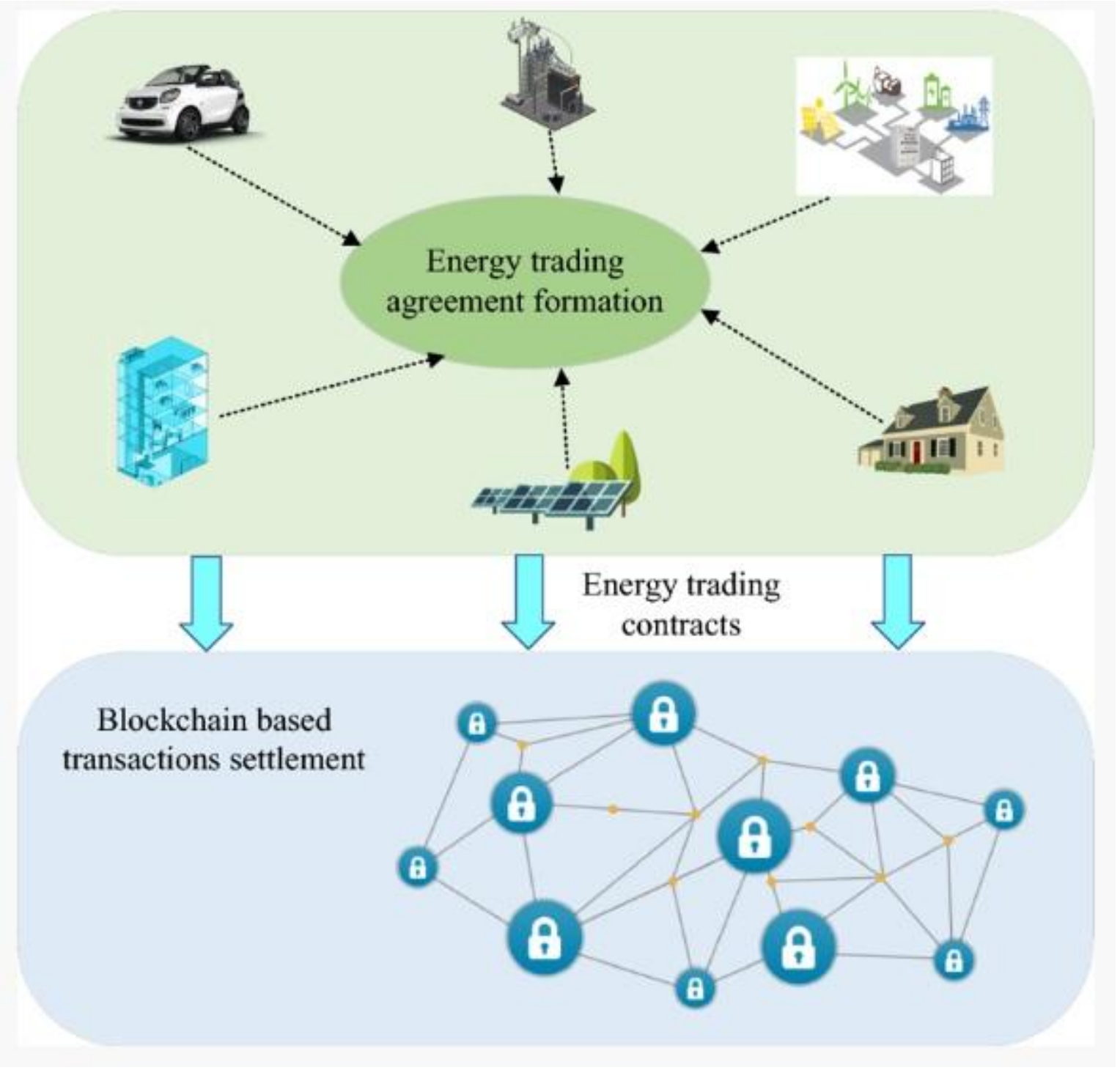
- Αποκεντρωμένη αποθήκευση δεδομένων. Με τη δομή της αλυσίδας και τον μηχανισμό συναίνεσης, το Blockchain δημιουργεί αντίγραφα των δεδομένων σε δικτυωμένους κόμβους και συγχρονίζει δεδομένα μέσω του Διαδικτύου. Η δομή της αλυσίδας εξασφαλίζει ότι τα δεδομένα είναι ανιχνεύσιμα και μη παραβιάσιμα. ο μηχανισμός συναίνεσης διασφαλίζει την επαλήθευση και συγχρονισμό των δεδομένων. Αυτό παρέχει ένα ασφαλές περιβάλλον για την αποθήκευση των δεδομένων IoT για υποστήριξη των εφαρμογών ανώτερου επιπέδου. Τα αντίγραφα πολλαπλών δεδομένων στο Blockchain μπορούν επίσης να αποφύγουν αποτελεσματικά την αποτυχία ενός σημείου ολόκληρου του συστήματος.
- Προγραμματιζόμενα smart contracts. Το smart contract στο Blockchain αναφέρεται σε ένα σύνολο κωδικών λογισμικού που καθορίζει τις ευθύνες κάθε συμμετέχοντα στο συμβόλαιο και τους όρους εκτέλεσης της σύμβασης. Ως εκ τούτου, το Blockchain παρέχει μια πλατφόρμα για τον προγραμματισμό smart contracts που βασίζονται σε διαφορετικές λογικές εφαρμογών.
- Εξουσιοδότηση. Οι πληροφορίες που αποθηκεύονται στο Blockchain είναι ανιχνεύσιμες και μη παραβιάσιμες, γεγονός που σημαίνει ότι παρέχει έναν αξιόπιστο μηχανισμό για την επαλήθευση και την εξουσιοδότηση για περιουσιακά στοιχεία, συμφωνίες, δικαιώματα πνευματικής ιδιοκτησίας κ.ο.κ.

2.3.2 Αρχιτεκτονική Αγοράς Ενέργειας

Η τεράστια επιτυχία των Blockchain στον τομέα της χρηματοδότησης συνεπάγεται ότι διαθέτει επίσης μεγάλη δυνατότητα ανασυγκρότησης της αγοράς ενέργειας. Η τρέχουσα αγορά ενέργειας υιοθετεί μια κεντρική δομή συναλλαγών. Δηλαδή, οι συμμετέχοντες στην αγορά υποβάλλουν προσφορές εμπορίας ενέργειας στον φορέα της αγοράς και ο τελευταίος διευθετεί και διαχειρίζεται τις συναλλαγές.

Η δομή του τωρινού κεντρικού συστήματος αγοράς ενέργειας, απαρτίζεται από τρεις αξιοσημείωτους περιορισμούς: [39]

- Πρώτον, είναι ευάλωτη στις επιθέσεις στον κυβερνοχώρο. Στην Ουκρανία το 2015, συνέβη η πρώτη συσκότιση στον κόσμο που προκλήθηκε από κακόβουλο λογισμικό, αποδεικνύοντας ότι οι σύγχρονοι επιδρομείς του κυβερνοχώρου έχουν τη δυνατότητα να καταστρέψουν ένα εθνικό κέντρο ελέγχου. Οι επιθέσεις στον κυβερνοχώρο κατά του κέντρου ελέγχου της αγοράς οδηγούν σε διακοπή της λειτουργίας της αγοράς ή, τουλάχιστον, θα παραπλανήσουν σημαντικά τη διαδικασία λήψης αποφάσεων του διαχειριστή της αγοράς.
- Δεύτερον, η κεντρική διαχειριζόμενη δομή της αγοράς καθιστά δύσκολη τη δημιουργία ενός ανοικτού, διασυνοριακού συστήματος ενεργειακής αγοράς. Παρά την επιτυχή επίδειξη της Σκανδιναβικής Ενεργειακής Αγοράς, ενός διασυνοριακού συστήματος εμπορίας ενέργειας για τις σκανδιναβικές χώρες, το πρόβλημα της εμπιστοσύνης παραμένει και είναι το πιο αυστηρό εμπόδιο για τη δημιουργία διασυνοριακής αγοράς.
- Τρίτον, η κεντρική δομή της αγοράς είναι δύσκολο να κλιμακωθεί για την υποδοχή μεγάλου αριθμού παραγόντων της αγοράς, ιδίως όσον αφορά τους μικρούς παραγωγούς ενέργειας. Στο πλαίσιο αυτό, το Blockchain μπορεί να παράσχει ουσιαστικά τεχνικές υποστηρίξεις για τη δημιουργία ανοικτών, αποκεντρωμένων, ασφαλών αγορών ενέργειας σε διάφορα επίπεδα.

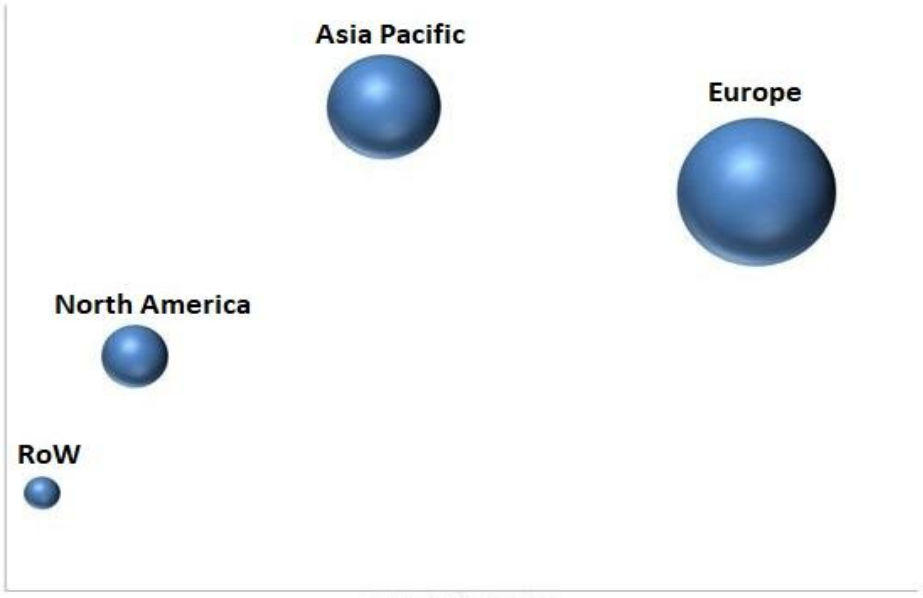


Εικόνα 21 – Σχηματικό του συστήματος εμπορίου ενέργειας στην κατανεμημένη πλευρά [39]

2.3.3 Το μέγεθος του Blockchain στην αγορά

Το Blockchain σε παγκόσμια κλίμακα στον τομέα ενέργειας αναμένεται να φθάσει το μέγεθος των αγορών ύψους 7,110.1 εκατομμυρίων δολαρίων μέχρι το 2023. Η αύξηση αυτή μπορεί να αποδοθεί στην δημοτικότητα της τεχνολογίας των Blockchain στον ενεργειακό τομέα, στην ανάγκη διαχείρισης υποδομών και άλλων επιχειρηματικών λειτουργιών για υψηλές ταχύτητες και αμερόληπτες συναλλαγές, και στα αυξανόμενα προβλήματα ασφάλειας σε ολόκληρο τον πλανήτη. Το Private Blockchain αναμένεται να κατέχει το μεγαλύτερο μερίδιο αγοράς έως το 2023, καθώς είναι πιο ασφαλές από το Public. Επίσης, το Public θα χρειαζόταν μεγαλύτερα ολοκληρωμένα συστήματα όπως υποδομές και συνδεσιμότητα, ενώ το Private μπορεί να εφαρμοστεί σε μικρότερη κλίμακα.

Έχει αναλυθεί το Blockchain στην αγορά 4 περιφερειών, συγκεκριμένα της Βόρειας Αμερικής, της Ευρώπης, της Ασίας του Ειρηνικού και στον υπόλοιπο κόσμο (RoW – Rest of World). Η αγορά στην Ευρώπη εκτιμάται ότι έχει τν μεγαλύτερη ύφεση, από το 2018 έως το 2023. Χώρες όπως είναι η Γερμανία, το Ηνωμένο Βασίλειο και η Ολλανδία, επενδύουν σε μεγάλο βαθμό στην υιοθέτηση Blockchain για την επίλυση των παγκοσμίων συναλλαγών μεταξύ πολλαπλών συμμετεχόντων. [40]



Εικόνα 22 – Το μέγεθος της αγοράς των Blockchain από το 2023 [40]

2.4 Περιορισμοί και Προκλήσεις του Blockchain

2.4.1 Τεχνολογικοί Περιορισμοί και Κίνδυνοι

Παρόλο που το Blockchain παρουσιάζει τεράστιο δυναμικό μιας ασφαλής, κατανεμημένης υποδομής στον κυβερνοχώρο για μελλοντικά ενεργειακά συστήματα, υπάρχουν ακόμη πιθανοί περιορισμοί και πρακτικές προκλήσεις. [53]

2.4.1.1 Πλεονασμός Πληροφοριών

Το Blockchain δημιουργεί πολλαπλά αντίγραφα δεδομένων σε δικτυωμένους κόμβους, οι οποίοι μπορούν να υποστηρίξουν την ασφαλή διαχείριση δεδομένων στο grid. Ωστόσο, δημιουργεί επίσης περιττές πληροφορίες. Οι μεμονωμένοι κόμβοι πρέπει να συμμετέχουν στη διαδικασία επαλήθευσης κάθε συναλλαγής και συνεπώς θα χρειάζονται επιπλέον αποθηκευτικό χώρο και θα καταναλώνουν περισσότερη ισχύ. Επιπλέον, θα ήταν βολικό για τους επιδρομείς να ξεκινήσουν μια στοχευόμενη επίθεση στον κυβερνοχώρο σε έναν μόνο κόμβο για να κατανοήσουν τις δυναμικές πληροφορίες ολόκληρου του δικτύου. Στο μέλλον εικάζεται ότι θα εμφανιστούν ιοί υπολογιστών ή επιθέσεις με στόχο το Blockchain. Επομένως, η εφαρμογή του Blockchain στα μελλοντικά ενεργειακά συστήματα απαιτεί πιο αποτελεσματικές τεχνολογίες για την ανακούφιση του προβλήματος της απόλυσης πληροφοριών.

2.4.1.2 Εξέλιξη Απόδοσης

Όπως το P2P σύστημα, το Blockchain κάνει ένα εγγενές εμπόριο μεταξύ αποκέντρωσης και απόδοσης του συστήματος. Τα τυπικά συστήματα Blockchain διεκπεραιώνουν τις συναλλαγές με μια ταχύτητα η οποία είναι μία ή περισσότερες φορές βραδύτερη από τις συγκεντρωτικές αντίστοιχες. Σε αντίθεση με άλλα κατανεμημένα συστήματα, η προσθήκη περισσότερων κόμβων υπολογιστών σε ένα δίκτυο Blockchain ενδέχεται να μην αυξήσει τη διακίνηση του δικτύου. Ανάλογα με το πρωτόκολλο συναίνεσης, η προσθήκη περισσότερων κόμβων θα μπορούσε ακόμη και να επιβραδύνει σημαντικά το σύστημα. Επί του παρόντος, ο ακαδημαϊκός κόσμος και η βιομηχανία εργάζονται για το σχεδιασμό νέων πρωτοκόλλων συναίνεσης για να μετριάσουν αυτό το πρόβλημα κλιμάκωσης.

2.4.1.3 Ασφάλεια του Smart Contract

Τα smart contract πρακτικά είναι προγράμματα γραμμένα από ανθρώπους. Ως αποτέλεσμα, ενδέχεται να περιέχουν ελαττώματα και σφάλματα σχεδίασης. Στη βιομηχανία λογισμικού, μια κοινή πρακτική αντιμετώπισης αυτών των αδυναμιών και σφαλμάτων είναι η απελευθέρωση αναβαθμίσεων λογισμικού ή διόρθωσης σφαλμάτων. Ωστόσο, οι αμετάβλητες και μη αναστρέψιμες φύσεις του Blockchain καθιστούν τη διαδικασία αυτή δυσκίνητη και αναποτελεσματική, αν όχι αδύνατη. Επιπλέον, τα smart contract συνήθως ασχολούνται άμεσα με πολύτιμα ψηφιακά στοιχεία, πράγμα που τους καθιστά ελκυστικούς στόχους εκμετάλλευσης. Τα εργαλεία επαλήθευσης θα πρέπει να αναπτυχθούν και να χρησιμοποιηθούν για την ανίχνευση ελλείψεων σχεδιασμού και σφαλμάτων σε smart contracts πριν από την πραγματική ανάπτυξη.

2.4.1.4 Συντονισμός του Blockchain με άλλα μέρη

Το Blockchain στα μελλοντικά ενεργειακά συστήματα δεν είναι τόσο απλό, θα απαιτήσει μη τετριμμένες προσπάθειες για τον συντονισμό του με άλλες υποδομές πληροφόρησης, όπως το IoT, cloud κλπ. Τα cloud και οι συσκευές του διαδικτύου έχουν συνήθως περιορισμένο εύρος ζώνης, ενώ τα πρωτόκολλα Blockchain παράγουν συχνή κυκλοφορία στο δίκτυο υπολογιστών. Αυτό συνεπάγεται προβλήματα σχετικά με τη συμβατότητα του Blockchain και άλλων τεχνολογιών πληροφορικής. Το πιο σημαντικό είναι ότι οι εφαρμογές που βασίζονται σε Blockchain απαιτούν τη συνεργασία διαφόρων λειτουργικών ενεργειακών οργανώσεων (ανεξάρτητους διαχειριστές συστημάτων, επιχειρήσεις λιανικής πώλησης ενέργειας, εταιρείες διανομής, χρήστες ενέργειας κ.λπ.), κάτι που αποτελεί μη τετριμμένο έργο.

2.4.1.5 Ενσωμάτωση του Blockchain και της φυσικής ενεργειακής υποδομής

Στο κυβερνοχώρο, το Blockchain και το smart contract προσφέρουν ασφάλεια και διαχρονικό εμπόριο ενέργειας. Ωστόσο, οι μεταβολές της κατανομής ενέργειας που προκαλείται από τη διαπραγμάτευση, επηρεάσουν τις ενεργειακές ροές στα φυσικά δίκτυα, γεγονός που οδηγεί σε ορισμένα προβλήματα, όπως η συμφόρηση του δικτύου και η υπερφόρτωση του. Συνεπώς, πρέπει να αναπτυχθούν αντίστοιχες λύσεις για τον συντονισμό των φυσικών υποδομών στον κυβερνοχώρο και την ενέργεια και να εξασφαλίσει την ασφαλή, αξιόπιστη και αποτελεσματική λειτουργία των ενεργειακών δικτύων.

2.4.2 Πιθανοί Περιορισμοί στη Δομή της Ηλεκτρικής Βιομηχανίας

Η λειτουργία των δικτύων ηλεκτρικής ενέργειας θεωρείται ευρέως μονοπωλιακή δραστηριότητα. Με απλά λόγια, αυτό σημαίνει ότι η μετάδοση και η διανομή των υπηρεσιών ηλεκτρικής ενέργειας παρέχεται τουλάχιστον με το κόστος μιας ενιαίας οντότητας - είτε ενός TSO είτε ενός DSO - αντί να ανταγωνίζονται επιχειρήσεις. Οι "οικονομίες κλίμακας" λέγεται ότι υπάρχουν στη λειτουργία του δίκτυα μεταφοράς και διανομής: το μέσο κόστος λειτουργίας του δικτύου για τον διαχειριστή του grid, απορρίπτεται λειτουργίας ενός διαχειριστή δικτύου απορρίπτεται όσο το μέγεθος των λειτουργικών δικτύων αυξάνεται. [53]

Σαν φυσικά μονοπώλια, οι διαχειριστές δικτύων είναι οι μοναδικοί υπεύθυνοι για ορισμένες λειτουργίες. Το TSO για παράδειγμα, είναι το μοναδικό σύστημα που είναι υπεύθυνο για την ισορροπία μεταξύ της παροχής ηλεκτρικού ρεύματος και των απαιτήσεων που προκύπτουν ανά πάσα στιγμή. Όλες οι συναλλαγές ηλεκτρικής ενέργειας, συμπεριλαμβανομένου και του P2P εμπορίου, πρέπει να συμβαδίζουν με το TSO, το οποί φέρει την ευθύνη της διατήρησης της ασφάλειας του δικτυού. Αποτέλεσμα αυτού είναι ότι ακόμα και αν προκύψουν ισχυρές P2P κοινότητες, είναι αδύνατο να λειτουργήσουν ανεξάρτητες από τους φορείς εκμετάλλευσης δικτύου, καθώς είναι συνδεδεμένες στο κεντρικό grid.

Εκτός από τις οικονομίες κλίμακας, υπάρχουν οι οικονομίες του πεδίου εφαρμογής που βρίσκονται σε υπηρεσίες οι οποίες σχετίζονται με τη λειτουργία του δικτύου. Λόγω της οικειότητας με τα δικά τους λειτουργικά χαρακτηριστικά και προγραμματιστικών απαιτήσεων, οι διαχειριστές δικτύου είναι πιθανό να παρέχουν μια σειρά υπηρεσιών σε χαμηλότερο κόστος από ότι εάν αυτές οι υπηρεσίες ανταγωνιστικά προσφερόμενες. Για παράδειγμα, τα DSOs μπορεί να είναι σε θέση να συντονιστούν πιο αποτελεσματικά με τις παροχές υπηρεσιών DER συστημάτων σε χαμηλότερο κόστος, από ότι οργανισμοί που είναι λιγότεροι εξοικειωμένοι με το δίκτυο ή πλατφόρμες που βασίζονται σε Blockchain. [53]

2.4.3 Ανταγωνιστικές Πιέσεις και Προκλήσεις Δημόσιας Αντίληψης

Υπάρχουν διάφορες τεχνολογικές λύσεις για πολλές δυνατότητες των εφαρμογών που διευρύνονται μέσω των Blockchain Projects. Για παράδειγμα, όσον αναφορά τη δυνατότητα συμμετοχής πελατών και των DER στη χονδρική πώληση, τα τηλεπικοινωνιακά συστήματα επικοινωνίας έχουν αναδυθεί ως μία πιθανή λύση. Δεν είναι ξεκάθαρο ότι οι προτεινόμενες Blockchain λύσεις για την ενίσχυση της συμμετοχής των DER στην αγορά και των πελατών, υπερβαίνουν τις ήδη υπάρχουσες τεχνολογίες τηλεμετρίας. Επιπλέον, υπάρχουν πολλοί τρόποι να προστατευτούν από κυβερνητικές επιθέσεις. Τα DSOs και TSOs, έχουν κάποιες καθιερωμένες πρακτικές διασφάλισης και διαχείρισης του δικτύου τους. Δεν είναι συνεπώς βέβαιο ότι οι προτεινόμενες λύσεις των Blockchain προσφέρουν βελτίωση σε εναλλακτικές λύσεις.

Τελικά, παράλληλα με τις ανταγωνιστικές πιέσεις, τα Blockchain αντιμετωπίζουν προκλήσεις δημόσιας αντίληψης. Οι Blockchain τεχνολογίες είναι κοινώς συσχετιζόμενες με την “σκιώδη οικονομία” και μόλις πρόσφατα έχουν αρχίσει να κερδίζουν την δημόσια νομιμότητα. Όπως αποδεικνύεται και από τις πτώσεις στην τιμή του κρυπτονομίσματος, ακόμη και η πιο ώριμη εφαρμογή του Blockchain αγωνίζεται να διατηρήσει την εμπιστοσύνη των χρηστών. [53]

2.5 Μεθοδολογία της Εργασίας

Η μεθοδολογία που ακολουθείται στην παρούσα εργασία για την ανάδειξη της πληρότητας του Μικροδικτύου συγκριτικά με του συμβατικού και η ευχρηστία των αποκεντρωμένων εφαρμογών στην παρούσα υποδομή της τεχνολογίας, είναι η ανάπτυξη και η εφαρμογή ενός Blockchain. Με τη βοήθεια των εργαλείων που προσφέρει το Ethereum για δημιουργία DApps, θα παραχθεί ένα δίκτυο μεταξύ δύο ομότιμων χρηστών-κόμβων, καθένας εξ αυτών θα συνδέεται με ένα λογαριασμό μηδενικού αρχικού ποσού, και θα πραγματοποιηθεί μία συναλλαγή μεταξύ των κόμβων σε πραγματικό χρόνο.

Το δίκτυο που θα υλοποιηθεί, είναι τύπου Private Blockchain, που σημαίνει ότι οποιοσδήποτε άλλος χρήστης θελήσει να συμμετάσχει πρέπει να λάβει εξουσιοδότηση. Για την εγκατάσταση του δικτύου των παραπάνω προδιαγραφών, χρησιμοποιείται το Geth εργαλείο του Ethereum, το οποίο μαζί με τη διαδικασία κατασκευής του P2P πλέγματος αναλύεται εκτενώς στις επόμενες ενότητες της εργασίας.

Επιπλέον, θα επεξηγηθεί ο τρόπος λειτουργίας ενός Μικροδικτύου και τι επιτυγχάνεται όταν εφαρμόζεται στο τωρινό Large συμβατικό δίκτυο. Θα αναλυθεί το Ethereum πρωτόκολλο, χρήσιμο για την επίτευξη των απαιτήσεων μας, θα επεξηγηθούν τα smart contracts (απαραίτητα για την ανταλλαγή δεδομένων μεταξύ των χρηστών) και τέλος τα χαρακτηριστικά που φέρει ένα P2P δίκτυο. Έμφαση δίνεται στις αποκεντρωμένε εφαρμογές (DApps) και πως συναρτήσει με το IoT δίνουν μίας τελείως διαφορετική διάσταση τόσο στον τομέα αγοράς της ηλεκτρικής ενέργειας όσο και σε επίπεδο ανταλλαγής δεδομένων, οποιασδήποτε πληροφορίας μεταξύ των συμμετεχόντων.

2.5.1 Ethereum

Το Ethereum είναι μια ανοικτή πλατφόρμα Blockchain η οποία παρουσιάστηκε στο ευρύ κοινό από τον Vitalik Buterin το 2013 που επιτρέπει σε οποιονδήποτε να δημιουργεί και να χρησιμοποιεί smart contracts και αποκεντρωμένες εφαρμογές (DApps) που λειτουργούν με την εκάστοτε τεχνολογία. Όπως και ο Bitcoin, έτσι και το Ethereum είναι αυτόνομο και δεν ελέγχεται από κανέναν - είναι ένα έργο ανοιχτού κώδικα που κατασκευάστηκε από πολλούς ανθρώπους σε όλο τον κόσμο. Αντίθετα με το πρωτόκολλο Bitcoin, το Ethereum σχεδιάστηκε για να είναι προσαρμόσιμο και ευέλικτο. Είναι εύκολο να δημιουργήσετε νέες εφαρμογές στην πλατφόρμα Ethereum και με την έκδοση Homestead είναι πλέον ασφαλές για οποιονδήποτε να χρησιμοποιεί αυτές τις εφαρμογές. Το Ethereum χρησιμοποιεί το PoS, ενώ είχε ξεκινήσει με PoW, για αλγόριθμο συναίνεσης και είναι βασισμένο στο RLPx, ένα TCP πρωτόκολλο που επιτρέπει την επικοινωνία μεταξύ των κόμβων.

2.5.1.1 Πλεονεκτήματα PoS

Αν εφαρμοστεί σωστά, το PoS ποικίλει σε πλεονεκτήματα. Ιδιαίτερη έμφαση δίνονται στα 3 παρακάτω:

1. Δεν σπαταλάει σημαντική ποσότητα ηλεκτρικής ενέργειας. Βέβαια, υπάρχει η ανάγκη να συνεχίσουν οι παραγωγοί να προσπαθούν να παράγουν blocks, αλλά κανείς δεν επωφελείται πιο πολύ επιχειρώντας από περισσότερες από μία προσπάθειες ανά λογαριασμό ανά δευτερόλεπτο.
2. Μπορεί αναμφισβήτητα να προσφέρει ένα πολύ υψηλότερο επίπεδο ασφάλειας. Στο PoW, το κόστος επίθεσης από το 51% των συμμετεχόντων αντιστοιχεί στην υπολογιστική ισχύ όλου του δικ΄τυου. Στο PoS είναι αρκετά μεγαλύτερο το ποσοστό του 51% της συνολικής προσφοράς του νομίσματος
3. Ανάλογα με τον αλγόριθμο που θα χρησιμοποιηθεί, μπορεί να επιτρέψει μεγαλύτερες ταχύτητες δημιουργίας block στο Blockchain. Για παράδειγμα, Το NXT παράγει ένα μπλοκ κάθε λίγα δευτερόλεπτα, το Ethereum ένα ανά λεπτό και το Bitcoin ένα ανά 10 λεπτά)

2.5.1.2 Αρχή Λειτουργίας Ethereum

Το Ethereum ενσωματώνει πολλά χαρακτηριστικά και τεχνολογίες παρεμφερή με αυτά του Bitcoin, ενώ παράλληλα εισάγει πολλές δικές του τροποποιήσεις και καινοτομίες. Ενώ το Bitcoin ήταν καθαρά ένας κατάλογος συναλλαγών, η βασική μονάδα του Ethereum είναι ο λογαριασμός. Το Ethereum παρακολουθεί την κατάσταση κάθε λογαριασμού, και όλες οι καταστάσεις μετάβασης του Ethereum είναι μεταφορές αξίας και πληροφοριών μεταξύ λογαριασμών. Υπάρχουν δύο τύποι λογαριασμών:

- Οι Εξωτερικοί Ιδιόκτητοι Λογαριασμοί (EOAs – Externally Owned Accounts), οι οποίοι ελέγχονται από ιδιωτικά κλειδιά
- Λογαριασμοί Συμβολαίων, οι οποίοι ελέγχονται από τον συμβατικό τους κώδικα και μπορούν να ενεργοποιηθούν μόνο από έναν EOA

Η βασική διαφορά είναι ότι οι χρήστες του ανθρώπινου δυναμικού ελέγχουν τους EOAs. Οι λογαριασμοί των συμβολαίων, από την άλλη πλευρά, διέπονται από τον εσωτερικό κώδικα τους. Ο δημοφιλής όρος "smart contracts" αναφέρεται σε κώδικα Λογαριασμού Συμβολαίου - προγράμματα που εκτελούνται όταν μια συναλλαγή αποστέλλεται στον λογαριασμό αυτό.

Οι λογαριασμοί των συμβολαίων εκτελούν μια ενέργεια μόνο όταν τους έχει δοθεί σχετική εντολή από έναν EOA. Επομένως, δεν είναι δυνατό για έναν λογαριασμό συμβολαίου να εκτελεί μη αυτόματες λειτουργίες. Αυτό συμβαίνει επειδή το Ethereum απαιτεί από τους κόμβους να είναι σε θέση να συμφωνήσουν για το αποτέλεσμα του υπολογισμού, το οποίο απαιτεί εγγύηση αυστηρά εξουσιαστικής εκτέλεσης.

Όπως και στο Bitcoin, οι χρήστες πρέπει να πληρώνουν μικρές αμοιβές συναλλαγών στο δίκτυο. Αυτό προστατεύει το Ethereum από επιπόλαιες ή κακόβουλες υπολογιστικές εργασίες, όπως επιθέσεις DDoS. Ο αποστολέας μιας συναλλαγής πρέπει να πληρώνει για κάθε βήμα του "προγράμματος" που ενεργοποίησε, συμπεριλαμβανομένου του υπολογισμού και της αποθηκευόμενης μνήμης. Αυτά τα τέλη πληρώνονται σε ποσότητες από του Ethereum το φυσικό ειδικό νόμισμα, το ether.

Αυτά τα τέλη συναλλαγών συλλέγονται από τους κόμβους που επικυρώνουν το δίκτυο. Οι miners είναι κόμβοι στο δίκτυο Ethereum που λαμβάνουν, διαδίδουν, επαληθεύουν και εκτελούν συναλλαγές. Οι miners ομαδοποιούν τότε τις συναλλαγές - οι οποίες περιλαμβάνουν πολλές ενημερώσεις για την "κατάσταση" των λογαριασμών στο Blockchain του Ethereum - και ανταγωνίζονται τότε μεταξύ τους για να είναι το μπλοκ τους το επόμενοι που θα προστεθεί στην αλυσίδα. Ανταμείβονται με ether για κάθε επιτυχημένο block που εξάγουν. Αυτό παρέχει το οικονομικό κίνητρο για τους ανθρώπους να αφιερώσουν hardware και ηλεκτρισμό στο δίκτυο Ethereum.

2.5.1.3 Μηχανισμός Δημιουργίας Block

Το block στο Ethereum είναι η συλλογή σχετικών πληροφοριών (γνωστή ως block header), όπου οι πληροφορίες του αντιστοιχούν στις συναφείς συναλλαγές. Το block header εμπεριέχει αρκετά κομμάτια πληροφοριών τα οποία αναγράφονται παρακάτω:

parentHash: 256-bit του parent block header, Hp

ommersHas: 256-bit hash της ommers λίστας του block, Ho

beneficiary: 160-bit διεύθυνση, εκεί αποθηκεύονται όλα τα τέλη από το mining, Hc

transactionRoots: 256-bit hash του root κόμβου που συσχετίζεται με όλες τις συναλλαγές, Hr

receiptsRoot: 256-bit hash του root κόμβου που συσχετίζεται με τις αποδείξεις των συναλλαγών, He

logsBloom: το Bloom Filter δημιουργείται από τις πληροφορίες που εμπεριέχονται στο log των αποδείξεων κάθε συναλλαγής, Hb

difficulty: αναφέρεται στην δυσκολία επιπέδου ενός block, υπολογίζεται από την δυσκολία του προηγούμενου block και από το timestamp, Hd

number: ο αριθμός των block, το genesis block έχει τον αριθμό 0, Hi

gasLimit: αναφέρεται στο όριο των δαπανών gas του block, Hl

gasUsed: αναφέρεται στο πόσο gas χρησιμοποιήθηκε στη συναλλαγή αυτού του block, Hg

timestamp: αναφέρεται στο χρόνο για την αρχή ενός block, Hs

extraData: μία αυθαίρετη παράταξη από byte που σχετίζεται με τα δεδομένα του block. Πρέπει να είναι 32 byte η λιγότερα, Hx

mixHash: 256-bit hash, συναρτήσει με το nonce, αποδεικνύει ότι ένα σημαντικό ποσό υπολογιστικής ισχύς έχει εξέλθει από το εκάστοτε block, Hm

nonce: 64-bit, συναρτήσει με το mixHash, αποδεικνύει ότι ένα σημαντικό ποσό υπολογιστικής ισχύς έχει εξέλθει από το εκάστοτε block, Hn

Τα block στο Ethereum δεν έχουν σταθερό μέγεθος και ούτε δημιουργούνται ανά τακτά χρονικά διαστήματα. Κάθε block έχει όριο στο gas. Έτσι λοιπόν και το gasLimit περιορίζει του block, αλλά και την υπολογιστική ισχύ που χρειάζεται για την δημιουργία του. Το όριο του gas σε κάθε block προκύπτει ύστερα από ψηφοφορία μεταξύ των miners, αυτό σημαίνει ότι είναι τιμή μεταβλητή και κατά συνέπεια αλλάζει και το μέγεθος του block στην πάροδο του χρόνου. Το gas δηλαδή, είναι η μονάδα που χρησιμοποιεί το Ethereum για την μέτρηση της υπολογιστικής προσπάθειας.

Το χρονικό διάστημα που μεσολαβεί στη δημιουργία μεταξύ δύο διαδοχικών block είναι σταθερό και εξαρτάται από το επίπεδο δυσκολίας του δικτύου. Ισχύουν οι σχέσεις:

$$block\_time = current\_block\_timestamp - parent\_block\_timestamp$$

$$currentBlockDifficulty = parentBlockDifficulty + \frac{parentBlockDifficulty}{2048} * \max\left[\left(1 - \frac{blockTime}{10}\right), -99\right] + \text{floor}\left(\frac{currentBlockNumber}{100000} - 2\right)$$

Ο floor είναι ο μεγαλύτερος ακέραιος αλλά μικρότερος από τον περιεχόμενο αριθμό. Η παραπάνω σχέση δείχνει ότι αν ο χρόνος που μεσολαβεί της δημιουργίας δύο διαδοχικών block είναι μικρότερος από 10 δευτερόλεπτα, τότε η δυσκολία θα αυξηθεί. Μεταξύ 10 και 19 η δυσκολία δεν θα μεταβληθεί, ενώ μεγαλύτερο του 19 η δυσκολία μειώνεται. Το floor (…) αναφέρεται στην σταδιακή αύξηση της δυσκολίας παράλληλα με την αύξηση του αριθμού των block. Η παραπάνω σχέση βοηθάει να παραμένει το κάθε block στον προκαθορισμένο χρονικό διάστημα, από 10 έως 19 δευτερόλεπτα.

2.5.1.4 Μηνύματα και Συναλλαγές

Ο όρος συναλλαγή στο Ethereum αναφέρεται στο εγκεκριμένο πακέτο δεδομένων, που εμπεριέχει το μήνυμα που αποστέλλεται από ένα EOA. Η συναλλαγή περιλαμβάνει:

- Τον παραλήπτη του μηνύματος
- Την υπογραφή εξακρίβωσης του αποστολέα
- Το πόσο που αποστέλλεται από τον αποστολέα στον παραλήπτη
- Ένα προαιρετικό πεδίο δεδομένων
- Μία StarGas τιμή, που παρουσιάζει τον μέγιστο αριθμό υπολογιστικών βημάτων που επιτρέπεται να κάνει η συναλλαγή κατά την εκτέκεση
- Μία GasPrice τιμή, που παρουσιάζει τα τέλη που πληρώνει ο αποστολέας για κάθε υπολογιστικό βήμα

Τα συμβόλαια έχουν την ικανότητα να στέλνουν μηνύματα σε άλλα συμβόλαια. Τα μηνύματα είναι εικονικά αντικείμενα που υπάρχουν μόνο στο περιβάλλον του Ethereum. Το μήνυμα περιλαμβάνει:

- Τον αποστολέα του μηνύματος
- Τον παραλήπτη του μηνύματος
- Το ποσό των ether που μεταφέρεται μαζί με το μήνυμα
- Ένα προαιρετικό περιβάλλον δεδομένων
- Μία StarGas τιμή

2.5.1.5 Ethereum Λογαριασμοί

Το Ethereum αποτελείται από αντικείμενα που ονομάζονται “λογαριασμοί”, καθένας εξ αυτών έχει μία διεύθυνση των 20-byte και οι μεταφορές των πληροφοριών τους πραγματοποιούνται άμεσα μεταξύ των λογαριασμών. Ένας Ethereum λογαριασμό περιλαμβάνει:

- Το nonce, έναν μετρητή που χρησιμοποιείται για να βεβαιωθεί ότι κάθε συναλλαγή μπορεί να επεξεργαστεί μόνο μία φορά
- Τα τρέχοντα ether του λογαριασμού
- Τον κώδικα του συμβολαίου
- Τον αποθηκευτικό χώρο του λογαριασμού (Στην προεπιλογή είναι άδειος)

2.5.1.6 Εκτέλεση Κώδικα στο Ethereum

Ο κώδικας στα συμβόλαια του Ethereum γράφεται σε γλώσσα χαμηλού επιπέδου, που αναφέρεται ως "κωδικός εικονικής μηχανής Ethereum" ή "κώδικας EVM". Ο κώδικας αποτελείται από μια σειρά από bytes, όπου κάθε byte αντιπροσωπεύει μια λειτουργία. Γενικά, η εκτέλεση κώδικα είναι ένας άπειρος βρόχος που αποτελείται από την επανειλημμένη διεξαγωγή της λειτουργίας στον τρέχοντα μετρητή προγράμματος (ο οποίος ξεκινά από το μηδέν) και στη συνέχεια την αύξηση του μετρητή προγράμματος κατά ένα, μέχρι να φτάσει το τέλος του κώδικα ή σε ένα σφάλμα, ή να ανιχνευθεί η εντολή STOP ή εντολή RETURN. Οι λειτουργίες έχουν πρόσβαση σε τρεις τύπους χώρου στον οποίο αποθηκεύονται τα δεδομένα:

- Τον stack, ένας κατανεμητής στον οποίο γίνονται push και pop εντολές
- Την μνήμη, μία απείρως διευρυνόμενη συστοιχία από bytes
- Τον μακροχρόνιο αποθηκευτικό χώρο του συμβολαίου, ένα key/value μέρος. Σε αντίθεση με τον stack αι την μνήμη, τα οποία επαναφέρονται μετά το τέλος της υπολογιστικής κατάστασης, ο αποθηκευτικός χώρος του συμβολαίου παραμένει για αρκετό χρονικό διάστημα.

2.5.2 Αποκεντρωμένες Εφαρμογές – DApps

Οι χρήστες του Διαδικτύου δεν έχουν αποκλειστικό έλεγχο των δεδομένων που μοιράζονται στους σημερινούς ιστότοπους. Το Ethereum προσπαθεί να διορθώσει ένα σημείο στο σημερινό διαδίκτυο, το οποίο για πολλούς χρήστες θεωρείται ελαττωματικό. Είναι σαν ένα αποκεντρωμένο appstore, στο οποίο καθένας θα μπορεί να δημοσιεύσει τις αποκεντρωμένες εφαρμογές του, όπου σε αντίθεση με μεγάλες εφαρμογές (Gmail, Uber κλτ.) δεν θα χρειάζονται κάποιον μεσάζοντα για να λειτουργήσουν. Οι DApps θα συνδέουν τους χρήστες και τους πάροχους άμεσα.

Ένα τρανταχτό παράδειγμα, είναι η εφαρμογή ενός τέτοιου σχεδιασμού σε κάποιο Social Media (π.χ. Twitter) ώστε να μετατραπεί σε αποκεντρωμένο και να είναι ανθεκτικό στην λογοκρισία. Αφού δημοσιευτεί ένα μήνυμα στο Blockchain θα είναι αδύνατο να διαγραφεί ακόμη και από την εταιρεία.

Οι DApps καθορίζονται από δύο βασικά χαρακτηριστικά, ότι είναι ανοικτού κώδικα και ότι δεν έχουν κεντρικό σημείο αποτυχίας.

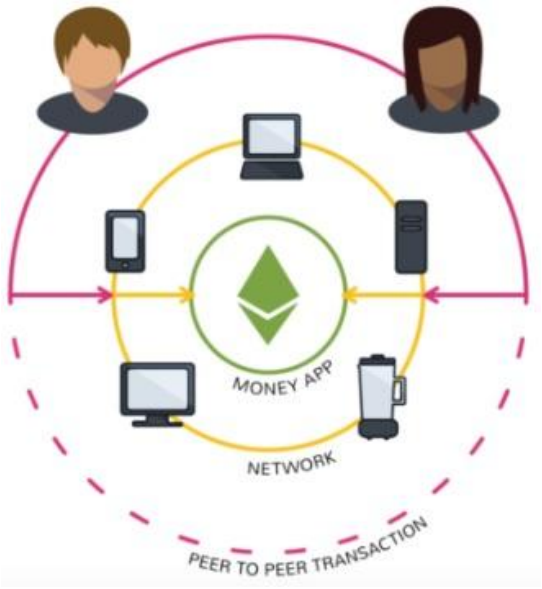
2.5.2.1 Τύποι DApps

Υπάρχουν 3 τύποι στους οποίους διαχωρίζονται τα DApps:

- Εφαρμογές που διαχειρίζονται λεφτά
- Εφαρμογές που εμπεριέχονται λεφτά
- Εφαρμογές ψηφοφορίας και διακυβερνητικών συστημάτων

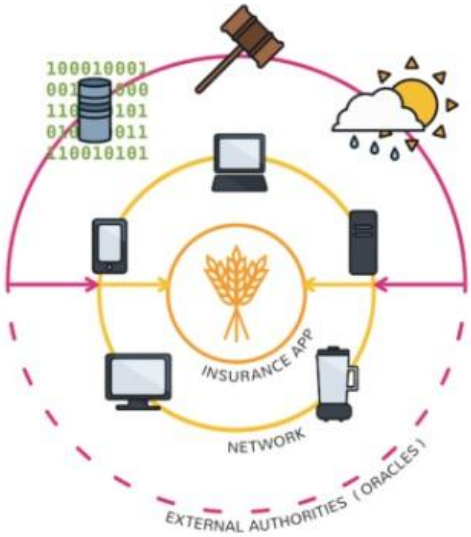
1^{ος} τύπος Dapp: Στον πρώτο τύπο εφαρμογής, ο χρήστης μπορεί να χρειαστεί να ανταλλάξει το ether ως ένα τρόπο λύσης μιας σύμβασης με άλλο χρήστη, χρησιμοποιώντας τα κατανεμημένα δίκτυα υπολογιστών κόμβων για να διευκολύνει τη διανομή αυτών των δεδομένων.

.



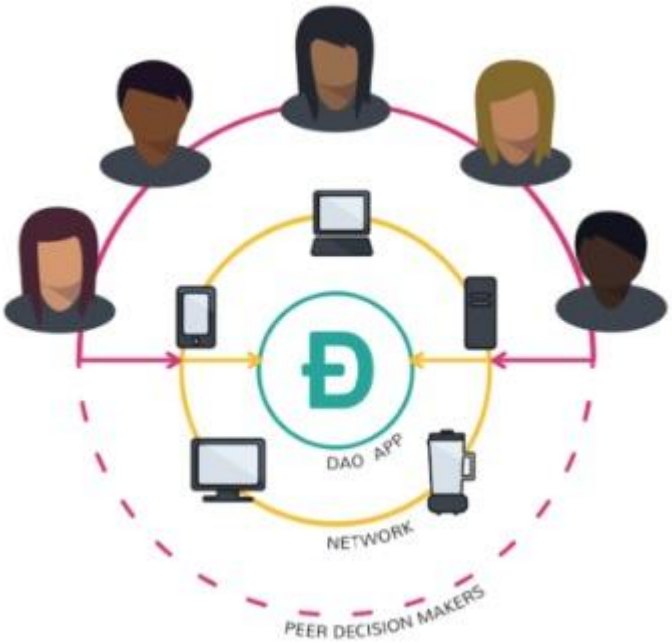
Εικόνα 23 – Money Dapp διαχείριση χρημάτων μέσω αποκεντρωμένης εφαρμογής [17]

2ος Τύπος DApp: Ο δεύτερος τύπος εφαρμογής αναμιγνύει χρήματα με πληροφορίες εκτός του Blockchain. Για παράδειγμα, μια εφαρμογή ασφάλισης καλλιέργειας που εξαρτάται από μια εξωτερική καιρική ενημέρωση. Για να εκτελεστούν, αυτά τα smart contracts βασίζονται σε λεγόμενα "oracles" που αναμεταδίδουν ενημερωμένες πληροφορίες για τον έξω κόσμο.



Εικόνα 24 – Insurance Dapp αυτόματη πληρωμή μια υπηρεσίας, όταν αυτή χρειαστεί βάσει των δεομένων που λαμβάνονται από τον έξω κόσμο [17]

3ος τύπος DApp: Ο στόχος είναι να σχηματιστεί μια εταιρεία χωρίς ηγέτες, κανόνες προγράμματος για το πώς τα μέλη μπορούν να ψηφίσουν και πώς να απελευθερώσουν κεφάλαια της εταιρείας. Οι αποκεντρωμένες αυτόνομες οργανώσεις (Decentralized Autonomous Organizations – DAO) είναι ένα ιδιαίτερα φιλόδοξο αντικείμενο DApp.



Εικόνα 25 – DAO App σχηματισμός αυτόνομου οργανισμού εν μέσω αποκεντρωμένης εφαρμογής[17]

2.5.3 Smart Contracts

Τα έξυπνα συμβόλαια ή smart contracts είναι μια από τις εφαρμογές της τεχνολογίας Blockchain που επιτρέπει στους οργανισμούς, στην κυβέρνηση, στα νομικά όργανα και ακόμη και σε ιδιώτες να ανταλλάσσουν χρηματικές αξίες, περιουσίες, μετοχές, ομόλογα με αξία με τρόπο σαφή, αποφεύγοντας οποιαδήποτε σύγκρουση χωρίς την ανάγκη μεσάζοντος. Ο παράγοντας που διατηρεί την ανάπτυξη του smart contract είναι η τάση του να καθορίζει τους κανόνες και τους κανονισμούς μιας συμφωνίας, αλλά και να επιβάλλει αυτόματα οποιαδήποτε από τις υποχρεώσεις. Το έξυπνο συμβόλαιο μπορεί να χρησιμοποιηθεί για οποιαδήποτε καταστάση όπως χρηματοοικονομικά, ασφάλιστρα, παραβιάσεις συμβάσεων, ιδιοκτησιακό δίκαιο και πολλά άλλα.

Για κυβερνητικές έξυπνες συμβάσεις μπορεί να αποδειχθεί ένα επόμενο βήμα προς την ψηφοφορία και άλλες νομικές διατυπώσεις και προσφορές που εκδίδονται από την κυβέρνηση. Αυτά μπορεί να περιλαμβάνουν οποιαδήποτε συμφωνία γίνεται μεταξύ της κυβέρνησης και των ιδιωτικών ή δημόσιων επιχειρήσεων. [70]

2.5.3.1 Χαρακτηριστικά Smart Contracts

Ένα έξυπνο συμβόλαιο είναι μια ψηφιακά υπογεγραμμένη, αξιόπιστη συμφωνία μεταξύ δύο ή περισσοτέρων συμβαλλόμενων μελών. Στο πλαίσιο του Blockchain, ένα έξυπνο συμβόλαιο είναι ένα πρόγραμμα καθοδηγούμενο , που τρέχει σε ένα επαναλαμβανόμενο κοινό μητρώο και το οποίο μπορεί να πάρει την επιμέλεια επί περιουσιακών στοιχείων σε αυτό το μητρώο. Τα έξυπνα συμβόλαια στο Blockchain, δημιουργήθηκαν από προγραμματιστές υπολογιστών, είναι εξ ολοκλήρου ψηφιακά και γραμμένα σε γλώσσες προγραμματισμού κώδικα. Οι έξυπνος κώδικες έχουν ορισμένα μοναδικά χαρακτηριστικά: [70]

- **Ντετερμινιστικοί:** Δεδομένου ότι ένας έξυπνος συμβατικός κώδικας εκτελείται σε πολλαπλούς κατανεμημένους κόμβους ταυτόχρονα, πρέπει να είναι καθοριστικός, δηλ. όλοι οι κόμβοι πρέπει να παράγουν την ίδια έξοδο. Αυτό σημαίνει ότι ο έξυπνος συμβατικός κώδικας δεν πρέπει να είναι τυχαία γραμμένος, θα πρέπει να είναι ανεξάρτητος από το χρόνο και έχει την δυνατότητα εκτέλεσης του κώδικα πολλές φορές.
- **Αμετάβλητοι:** Ο έξυπνος συμβατικός κώδικας είναι αμετάβλητος. Αυτό σημαίνει ότι μόλις εγκατασταθεί, αυτό δεν μπορεί να αλλάξει. Αυτό φυσικά είναι επωφελές από την άποψη της εμπιστοσύνης, αλλά δημιουργεί ορισμένες προκλήσεις.
- **Επιβεβαιωμένοι:** Μόλις εγκατασταθεί, το έξυπνος συμβόλαιο αποκτά μια μοναδική διεύθυνση. Πριν αρχίσει να χρησιμοποιείται το έξυπνο συμβόλαιο, τα ενδιαφερόμενα μέλη έπρεπε να δουν ή να επαληθεύσουν τον κώδικα.

2.5.3.2 Κύρια Μέρη του Smart Contract

Ένα smart contract υποδιαιρείται σε 2 βασικές κατηγορίες: [70]

- **Smart contract Code:** ο κώδικας που αποθηκεύεται, επαληθεύεται και εκτελείται στο Blockchain
- **Smart Legal Contracts:** το είδος του smart contract που χρησιμοποιείται ως συμπλήρωμα ή υποκατάστατο για νόμιμα συμβόλαια.

Τα smart contracts βάσει της δουλειάς που παράγουν χωρίζονται σε τρία κομμάτια:[70]

- **Coding:** Επειδή τα έξυπνα συμβόλαια λειτουργούν όπως προγράμματα ηλεκτρονικών υπολογιστών, είναι πολύ σημαντικό να κάνουν ακριβώς αυτό που επιθυμούν οι συμμετέχοντες. Αυτό επιτυγχάνεται με την εισαγωγή της κατάλληλης λογικής κατά τη σύνταξη ενός έξυπνου συμβολαίου. Ο κώδικας συμπεριφέρεται με προκαθορισμένους τρόπους και τις διαδικασίες σύνταξης των παραδοσιακών συμβάσεων
- **Distributed Ledgers: Ο** κωδικός είναι κρυπτογραφημένος και αποστέλλεται στους άλλους υπολογιστές μέσω ενός κατανεμημένου δικτύου κόμβων “τρέχοντας” ένα κατανεμημένο καθολικό
- .**Execution:** Μόλις οι υπολογιστές του κατανεμημένου δικτύου λάβουν τον κώδικα, καθένας από αυτούς έρχεται σε συμφωνία για τα αποτελέσματα της εκτέλεσης του κώδικα. Το δίκτυο τότε θα ενημερώσει το κατανεμημένο καθολικό να καταγράψει και να παρακολουθήσει τη σωστή διεξαγωγή του κώδικα βάσει των όρων του έξυπνου συμβολαίου.

2.5.3.3 Ταξινόμηση του Smart Contract

Παρακάτω κατηγοριοποιούνται τα smart contracts ανά τομέα εφαρμογής όσον τα συμβόλαια Ethereum. Από τα αποτέλεσμα της έρευνας σχετικά με την εφαρμογή των έξυπνων συμβολαίων, προκύπτουν πέντε κατηγορίες οι οποίες περιγράφονται παρακάτω: [46]

1. **Financial:** Τα συμβόλαια αυτής της κατηγορίας διαχειρίζονται, συγκεντρώνουν ή διανέμουν χρήματα ως πρωταρχικό χαρακτηριστικό. Μερικά συμβόλαια πιστοποιούν την κατοχή ενός περιουσιακού στοιχείου σε πραγματικό κόσμο, επικυρώνουν την αξία του και παρακολουθούν τις συναλλαγές. Τα επενδυτικά προγράμματα υψηλής απόδοσης είναι συμβόλαια που συλλέγουν χρήματα από τους χρήστες υπό την υπόσχεση ότι θα λάβουν πίσω τα κεφάλαιά τους με τόκους εάν νέοι επενδυτές θα ενταχθούν στο σύστημα. Άλλα συμβόλαια παρέχουν ασφάλιση για αποτυχίες οι οποίες είναι ψηφιακά αποδεδειγμένες (π.χ. το Etherisc πουλάει ασφάλιση για πτήσεις).
2. **Notary:** Τα συμβόλαια αυτής της κατηγορίας, εκμεταλλεύονται την αμετάβλητη κατάσταση για να αποθηκεύσει κάποια δεδομένα, και σε ορισμένες περιπτώσεις την ιδιοκτησία και την προέλευση τους. Κάποια από τα συμβόλαια αυτά, επιτρέπουν στον χρήστη να γράψει το hash ενός εγγράφου στο Blockchain, έτσι ώστε να μπορεί να αποδείξει την ύπαρξη του εγγράφου και την ακεραιότητα του (Proof of Existence αλγόριθμος). Άλλα επιτρέπουν την δήλωση δικαιωμάτων σε ένα αρχείο ψηφιακής τέχνης, όπως είναι φωτογραφίες ή μουσική και άλλα απλώς επιτρέπουν στου χρήστες να γράφουν μηνύματα τα οποία αποθηκεύονται στο Blockchain και μπορεί ο καθένας που συμμετέχει στο δίκτυο να τα διαβάσει.
3. **Game:** Οι συμβάσεις σε αυτή την κατηγορία περιλαμβάνουν τυχερά παιχνίδια και παιχνίδια δεξιοτήτων που οι χρήστες επιθυμούν να συμμετάσχουν.
4. **Wallet:** Τα συμβόλαια αυτής της κατηγορίας χειρίζονται κλειδιά, αποστέλλουν συναλλαγές, διαχειρίζονται χρήματα, αναπτύσσουν και

παρακολουθούν συμβάσεις, προκειμένου να απλοποιηθεί η αλληλεπίδραση με το Blockchain. Τα πορτοφόλια μπορούν να διαχειρίζονται από έναν ή περισσότερους ιδιοκτήτες, στην τελευταία περίπτωση απαιτείται πολλαπλή έγκριση.

5. **Library:** Αυτά τα συμβόλαια υλοποιούν πράξεις γενικού σκοπού, που θα χρησιμοποιηθούν από άλλα συμβόλαια

Πριν από μερικούς μήνες ίσχυε ο παρακάτω πίνακας όσον αναφορά τα Smart contracts και τον αριθμό των συναλλαγών που έχουν πραγματοποιηθεί ανά κατηγορία, βάσει της πλατφόρμας που έχουν χρησιμοποιηθεί. Φυσικά, τα νούμερα αλλάζουν με ταχύτατους ρυθμούς καθώς τα Blockchain βρίσκουν όλο και περισσότερες εφαρμογές εισαχθούν.

Category	Platform	Number of Detected Contracts	Total Number of Transactions
Financial	Bitcoin	6	470.391
	Ethereum	373	624.046
Notary	Bitcoin	17	443.269
	Ethereum	79	35.253
Game	Bitcoin	0	0
	Ethereum	158	58.257
Wallet	Bitcoin	0	0
	Ethereum	17	1.342
Library	Bitcoin	0	0
	Ethereum	29	37.034
Unclassified	Bitcoin	0	0
	Ethereum	155	3.679
Total	**Bitcoin**	**23**	**913.66**
	Ethereum	**811**	**759.611**
Overall	**Overall**	**834**	**1.673.271**

Table 6 – Συναλλαγές Έξυπνων συμβολαίων ανά κατηγορία [46]

2.5.3.4 Τα κόστη Συναλλαγής

Σε αυτή την ενότητα, δίνεται τα κόστη που έχει μία συναλλαγή ενός απλού Ethereum έξυπνου συμβολαίου. Το κόστος τελικά μίας απλής συναλλαγής σε Ether (κρυπτονόμισμα του Ethereum) πραγματοποιείται σε τρεις διαδοχικές συναλλαγές και φαίνεται παρακάτω:

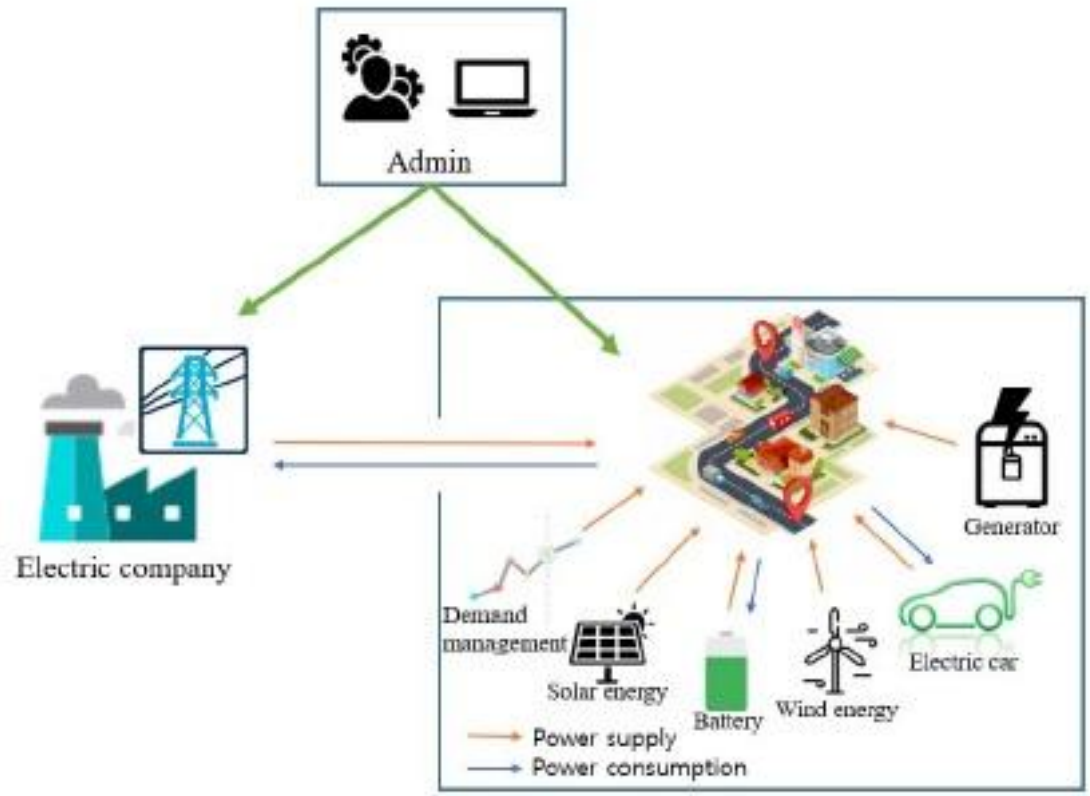
- Η πρώτη συναλλαγή αρχικοποιεί το συμβόλαιο και καταθέτει 0,5 Ether σε αυτό. Η συναλλαγή κοστίζει: 0.01072934 Ether ($3.21 at $300/ETH)
- Στη δεύτερη συναλλαγή ο αποστολέας δήλωνει επιβεβαίωση . Η συναλλαγή κοστίζει: 0.00093492 Ether ($0.28 at $300/ETH)
- Στη τρίτη συναλλαγή ο επιβλέποντας δηλώνει επιβεβαίωση. Η συναλλαγή κοστίζει: 0.00164754 Ether ($0.49 at $300/ETH)

Σε αυτό το σημείο, θα πρέπει να αναφερθεί ότι το κόστος **1 Ethereum** σε **Gas** είναι **97,617285 Gas,** δεδομένα που προκύπτουν από τον Ιούλιο του 2019 και παρακάτω φαίνονται οι αλλαγές που έχει υποστεί το 1 Ether σε βάθος 7 ημερών, την δεύτερη βδομάδα του Ιουλίου. [47] [48]

Εικόνα 26 - Αλλαγές στην τιμή του Ethereum σε Gas [48]

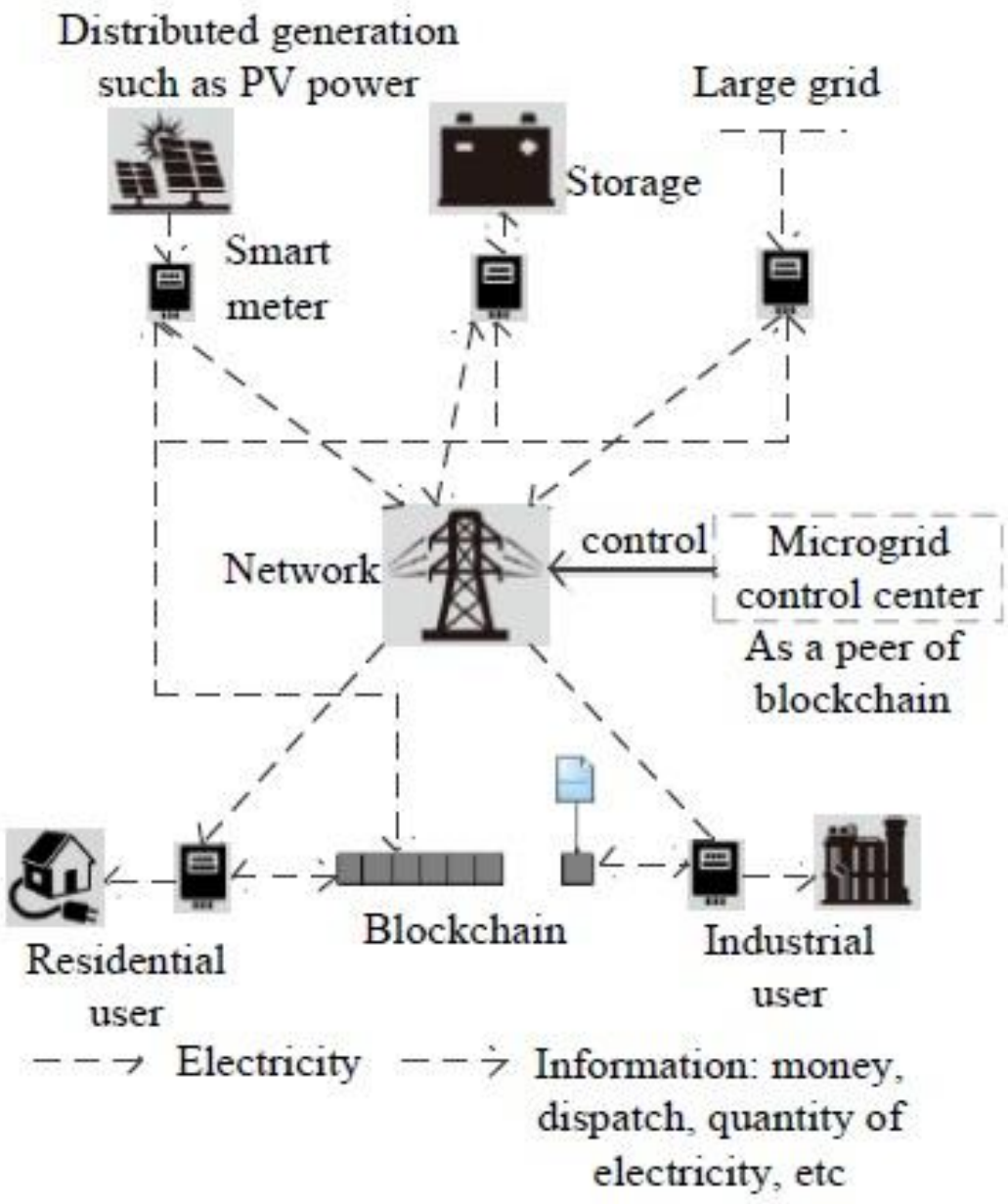
2.5.4 Μικροδίκτυο

Το Μικροδίκτυο αναφέρεται σε ένα τοπικό σύστημα τροφοδοσίας βασισμένο σε μια κατανεμημένη πηγή ισχύος ανεξάρτητη από το συμβατικό σύστημα ευρείας ισχύος. Όπως φαίνεται παρακάτω, ο αριθμός των καταναλωτών (Prosumers), όχι μόνο στο εργοστάσιο παραγωγής ηλεκτρικής ενέργειας, θα λάβει χρέωση της παραγωγής ηλεκτρικής ενέργειας του δικτύου με βάση τα δύο τρόπων μετάδοσης και διανομής. Σημαίνει να χρησιμοποιεί κατανεμημένες- πηγές ενέργειας όπως είναι οι ανανεώσιμες πηγές ενέργειας (ηλιακή ενέργεια, αιολική ενέργεια κτλ.), σαν δικές τους πηγές παραγωγής ενέργειας. Είναι εφικτό, να παρέχει, κάποιος καταναλωτής-παραγωγός εκτός του κεντρικού πάροχου, σταθερά ηλεκτρική ενέργεια και να μεταφέρει αποτελεσματικά ανανεώσιμη ενέργεια.



Εικόνα 27 – Σύστημα Μικροδικτύου [55]

Ένα αντιπροσωπευτικό σχηματικό της συμβολής που έχει το Μικροδικτυακό σύστημα, στο Large συμβατικό δίκτυο ισχύος φαίνεται παρακάτω. Με το Μικροδίκτυο, πετυχαίνεται η συμμετοχή καταναλωτών στο δίκτυο ως παραγωγοί, οι οποίοι διαμοιράζουν την ενέργεια όπου δεν το κάνει ο κεντρικός πάροχος. Τα Blockchain χρησιμοποιούνται για τις συναλλαγές στο δίκτυο μεταξύ παραγωγών και καταναλωτών.



Εικόνα 28 – Ροή πληροφοριών και έλεγχος του Μικροδικτυακού συστήματος στο συμβατικό δίκτυο ισχύος [59]

2.5.5 P2P Δίκτυο

Η αρχή λειτουργίας των δικτύων ομότιμων κόμβων είναι η απευθείας επικοινωνία ανάμεσα σε ζεύγη συνδεδεμένων υπολογιστών, που καλούνται ομότιμοι (peers). Οι ομότιμοι δεν ανήκουν σε κάποιον οργανισμό, αλλά είναι κατά κανόνα υπολογιστές που ελέγχονται από χρήστες. Όπως υποδηλώνει και η λέξη, οι ομότιμοι κόμβοι έχουν τα ίδια προνόμια, τις ίδιες δυνατότητες και τον ίδιο ρόλο στο δίκτυο. Οι κόμβοι λοιπόν διαθέτουν έναν μέρος των υπολογιστικών τους πόρων για την λειτουργία του δικτύου, απαλείφοντας έτσι την ανάγκη ύπαρξης μίας κεντρικής αρχής υπεύθυνης για τον συντονισμό και λειτουργία του δικτύου. Οι κόμβοι αυτοί του δικτύου βλέπουμε πως έχουν διπλό ρόλο, αυτόν του πελάτη (που προσφέρει πόρους-Prosumer) και αυτόν του εξυπηρετητή (που καταναλώνει πόρους-Consumer). Το Blockchain είναι τελικά μία εφαρμογή η οποία υποστηρίζεται στην αρχιτεκτονική ομότιμων (P2P Δίκτυο).

Τα δίκτυα ομότιμων χωρίζονται σε δύο κατηγορίες, τα **αδόμητα** και τα **δομημένα**: [71]

Τα **αδόμητα** δίκτυα δεν επιβάλλουν κάποια συγκεκριμένη δομή στο ανώτερο επίπεδο του δικτύου, αλλά σχηματίζονται μέσω κόμβων οι οποίοι πραγματοποιούν συνδέσεις τυχαία μεταξύ τους. Τα πλεονεκτήματα αυτού, είναι η εύκολη δημιουργία δικτύου, η δυνατότητα τοπικών βελτιστοποιήσεων σε διαφορετικές περιοχές τοπολογίας και η ακμή σε συνθήκες υψηλού ρυθμού αύξησης και αναχώρησης κόμβων. Βασικό μειονέκτημα, ο πλημμυρισμός δικτύου σε κάθε αναζήτηση δεδομένων.

Στα **δομημένα** δίκτυα, το ανώτερο επίπεδο του δικτύου οργανώνεται σχηματίζοντας μια ορισμένη τοπολογία σύμφωνα με κάποιο πρωτόκολλο, γεγονός που εξασφαλίζει την αποδοτική αναζήτηση οποιωνδήποτε δεδομένων, από οποιονδήποτε κόμβο. Έτσι η αναζήτηση αρχείων (δεδομένων) διεξάγεται αποτελεσματικά από κάθε κόμβο, με την χρήση του DHT (Distributed Hash Table) , δίνοντας μεγαλύτερο πλεονέκτημα στα δομημένα δίκτυα έναντι των αδόμητων.

3. Προδιαγραφές και Σχεδίαση της Εφαρμογής

Στην αυτή την ενότητα θα περιγραφούν οι προδιαγραφές υλοποίησης του συστήματος, καθώς και η σχεδίαση που θα ακολουθηθεί για την υλοποίηση ενός δικτύου ομότιμων χρηστών των δικών μας απαιτήσεων. Πρακτικά, αυτό που θα πραγματοποιηθεί θα είναι ένα δίκτυο των χαρακτηριστικών του Μικροδικτύου, βασισμένο στο Ethereum Blockchain με ευελιξία συμμετοχής παραπάνω από δύο χρήστες. Θα δημιουργηθεί στα πλαίσια της ανάπτυξης της εργασίας ένα Private Blockchain και θα διεξαχθεί μία συναλλαγή ή μικροπληρωμή μεταξύ των δύο αρχικών χρηστών που συμμετέχουν στο δίκτυο. Με την ολοκλήρωση της συναλλαγής, ένα Led συνδεδεμένο στο GPIO του RPi θα ανάψει ενδεικτικά προς ενημέρωσης μας ότι η διαδικασία εκτελέστηκε επιτυχώς.

3.1 Περιβάλλον Εφαρμογής

3.1.1 Hardware

Για την ανάπτυξη της εργασίας , το Hardware που χρησιμοποιήθηκε είναι:

- Ένα φορητός υπολογιστής (Laptop0
- Ένα Raspberry Pi 3 (RPi)

Δύο miners θα παρευρίσκονται στο δίκτυο ταυτόχρονα και θα έχουν τον ρόλο των Nodes (κόμβων), ένας στο Laptop και ένας στο RPi. Στην προκειμένη περίπτωση ο πρώτος miner θα είναι αυτός που θα κάνει mining για Ethers στο δίκτυο, για λόγους περιορισμού του RPi, και ο δεύτερος θα είναι ο παραλήπτης.

3.1.2 Software

Το Laptop που θα χρησιμοποιηθεί έχει λογισμικό Windows 10- 64 bit, απαιτείται ελάχιστη μνήμη RAM 4GB και επεξεργαστική ισχύς δύο πυρήνων στα 1.8 GHz, και εγκαθίσταται το VMware Workstation Pro (Virtual Machine) προκείμενου να προσαρμοστεί και να λειτουργήσει Linux λογισμικό παράλληλα. Το λογισμικό Linux που φορτώνεται στο VMware είναι του Raspbian Buster Lite, η έκδοση Debian 9x-64bit. Στο RPi εγκαθίσταται εξίσου η ίδια έκδοση Linux. Επιπλέον θα χρησιμοποιηθεί το **Geth** εργαλείο του Ethereum, το οποίο μας επιτρέπει την δημιουργία κόμβων στις εκάστοτε συσκευές.

3.2 Raspberry Pi

3.2.1 Περιγραφή

Το μοντέλο που χρησιμοποιείται είναι το Raspberry Pi 3 Model B+, είναι το τελευταίο προϊόν της σειράς 3 των RPi με επεξεργαστή 4 πυρήνων στα 64 – Bit στα 1.4 GHz, διπλό εύρος ζώνης Wireless LAN στα 2.4 GHz και στα 5 GHz, Bluetooth 4.2/BLE και θύρα Ethernet.

Το ασύρματο LAN διπλής ζώνης έρχεται με πιστοποιημένη διαμόρφωση, επιτρέποντας τη σχεδίαση του σε τελικά προϊόντα με σημαντικές μειωμένες δοκιμές συμμόρφωσης σε ασύρματο LAN, βελτιώνοντας τόσο το κόστος όσο και το χρόνο αγοράς.

Το Raspberry Pi 3 Μοντέλο B + διατηρεί το ίδιο μηχανικό αποτύπωμα με τα δύο προηγούμενα μοντέλα, το Raspberry Pi 2 Μοντέλο B και το Raspberry Pi 3 Μοντέλο B.

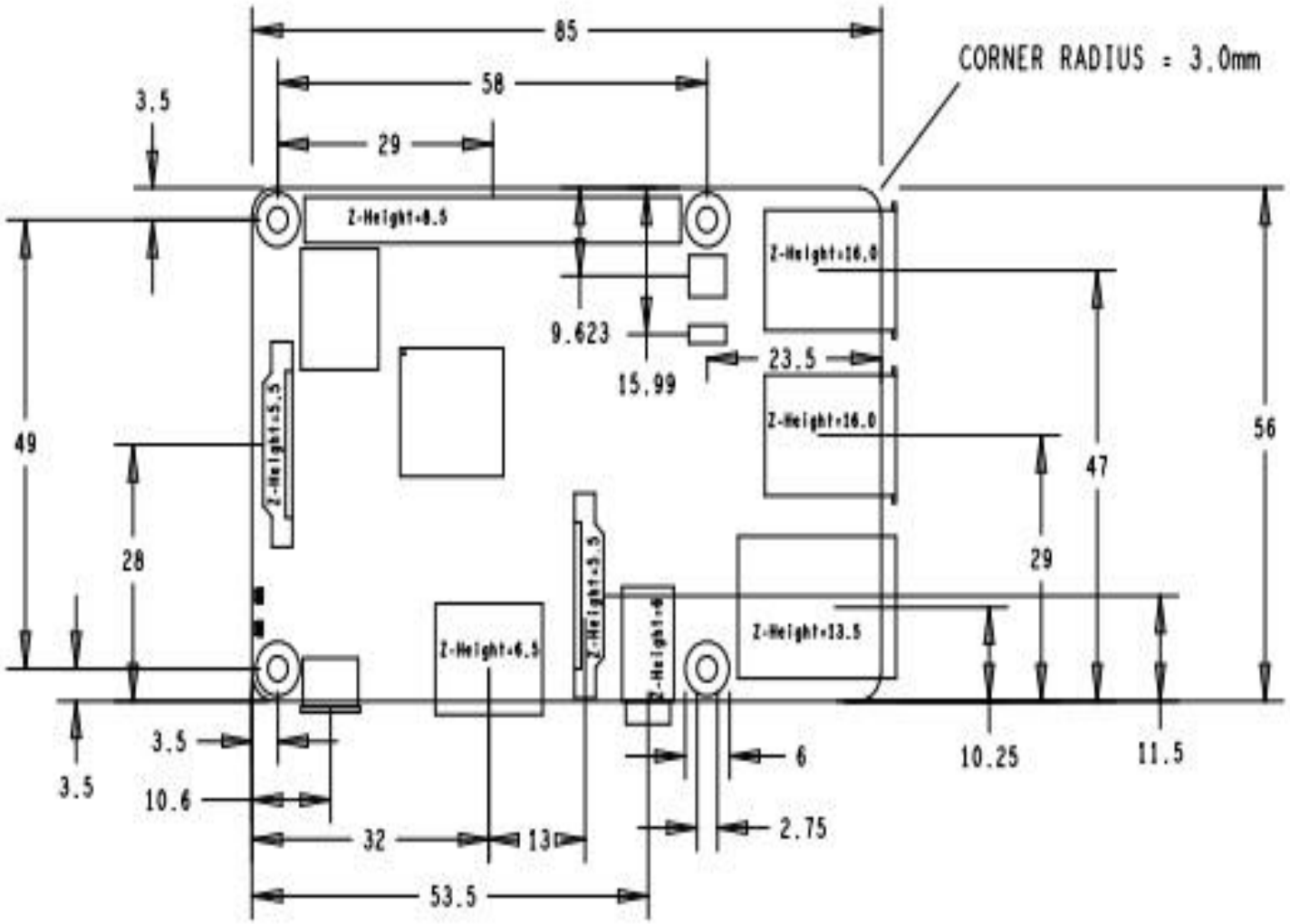
Εικόνα 29 – Το Raspberry Pi 3 Model B + [49]

3.2.2 Datasheet RPi

Processor:	Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz
Memory:	1GB LPDDR2 SDRAM
Connectivity:	■ 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE ■ Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps) ■ 4 × USB 2.0 ports
Access:	Extended 40-pin GPIO header
Video & sound:	■ 1 × full size HDMI ■ MIPI DSI display port ■ MIPI CSI camera port ■ 4 pole stereo output and composite video port
Multimedia:	H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES 1.1, 2.0 graphics
SD card support:	Micro SD format for loading operating system and data storage
Input power:	■ 5V/2.5A DC via micro USB connector ■ 5V DC via GPIO header ■ Power over Ethernet (PoE)–enabled (requires separate PoE HAT)
Environment:	Operating temperature, 0–50°C
Compliance:	For a full list of local and regional product approvals, please visit www.raspberrypi.org/products/raspberry-pi-3-model-b+
Production lifetime:	The Raspberry Pi 3 Model B+ will remain in production until at least January 2023.

Table 7 – Datasheet of Raspberry Pi 3 Model B+ [49]

3.2.3 Φυσικές Προδιαγραφές



Εικόνα 30 – Μηχανικό σχέδιο Raspberry Pi 3 Model B+ [49]

3.2.4 Εγκατάσταση Raspbian στο RPi

Για την εγκατάσταση του Raspbian στον RPi ακολουθήθηκαν τα παρακάτω βήματα:

- Κατεβάσαμε το iso αρχείο Raspbian Buster Lite, link : [https://www.raspberrypi.org/downloads/raspbian/]
- Διαμόρφωση της SD Card του RPi, η οποία είναι στα 64 Gb
- Προκειμένου να εγκατασταθεί το iso αρχείο στην SD card για Windows λογισμικό, χρησιμοποιήθηκε το Win32DiskImager, download link : [https://sourceforge.net/projects/win32diskimager/]
- Εισαγωγή SD card στην υποδοχή ανάγνωσης καρτών SD Card (θα μπορούσε να συνδεθεί και σε USB θύρα με τον ανάλογο adapter)
- Εκτέλεση Win32DiskImager από το menu των Windows
- Επιλογή του αποσυμπιεσμένου αρχείου iso
- Στο πλαίσιο συσκευής, επιλέγουμε το γράμμα μονάδας δίσκου της κάρτας SD
- Επιλέγουμε το 'Write' και περιμένουμε να ολοκληρωθεί η εγγραφή
- Βγαίνουμε από το Win32DiskImager, εξάγουμε την SD card από τον υποδοχέα καρτών και την εισάγουμε στο RPi

Οι παραπάνω οδηγίες για την εγκατάσταση του iso στην SD card με Windows λογισμικό δίνονται από τον οδηγό του παρακάτω link: [https://www.raspberrypi.org/documentation/installation/installing-images/windows.md]

3.3 Geth

Το Geth είναι η διεπαφή γραμμής εντολών για την εκτέλεση ενός πλήρους κόμβου Ethereum που υλοποιείται στο Go. Υπάρχει ελεύθερο στο διαδίκτυο και προσφέρεται δωρεάν, ενδεικτικά χρησιμοποιήθηκε αυτό το link: [https://geth.ethereum.org/downloads/] και η έκδοση Geth 1.8.27 στα 64 Bit Με το εργαλείο αυτό θα δημιουργήσουμε τους δύο κόμβους με μία σειρά εντολών στο Terminal (γραμμή εντολών Linux) με μία διαδικασία η οποία περιγράφεται εκτενώς στο επόμενο κεφάλαιο.

Σημείωση: Η τελευταία έκδοση του Geth 1.9.6 δεν είναι συμβατή για τον λόγο αυτό χρησιμοποιήθηκε παλαιότερη.

3.3.1 Δυνατότητες Geth

Εγκαθιστώντας και εκτελώντας το Geth, δίνεται η επιλογή συμμετοχής στο ζωντανό δίκτυο του Ethereum και επιπλέον οι δυνατότητες να:

- Διεξαχθεί mining για αληθινά Ethers
- Μεταφερθούν κεφάλαια μεταξύ διευθύνσεων/κόμβων
- Δημιουργηθούν contracts και να σταλούν συναλλαγές
- Εξερευνηθεί το ιστορικό των Block

3.3.2 Η Εγκατάσταση

Οι πλατφόρμες που υποστηρίζονται είναι Linux, Mac OS και Windows. Για τους κοινούς χρήστες διατίθενται δύο είδη εγκατάστασης:

- Binary installation
- Scripted installation

3.3.3 Interfaces

- JavaScript Console: το Geth μπορεί να ξεκινήσει με μια διαδραστική κονσόλα, η οποία παρέχει ένα περιβάλλον εκτέλεσης JavaScript εκθέτοντας ένα JavaScript API για να αλληλεπιδράσει με τον κόμβο. Η JavaScript κονσόλα API περιλαμβάνει το web3 JavaScript DApp API καθώς και ένα πρόσθετο admin API

- JSON-RPC server: το Geth μπορεί να ξεκινήσει με ένα JSON-RPC server που εκθέτει το JSON-RPC API
- Οι επιλογές της γραμμής εντολών εγγράφονται στις παραμέτρους της γραμμής εντολών καθώς και στις δευτερεύουσες εντολές

3.3.4 Βασική Τεκμηρίωση Χρήσης

- **Διαχείριση Λογαριασμών:** Η διαχείριση λογαριασμών επιτρέπει την δημιουργία νέων λογαριασμών, την καταγραφή όλων των υπαρχόντων λογαριασμών, την εισαγωγή ενός ιδιωτικού κλειδιού σε νέο λογαριασμό, την μεταφορά στη νέα μορφή κλειδιού και την αλλαγή του κωδικού πρόσβασής. Υποστηρίζει τη διαδραστική λειτουργία, όταν ζητηθεί κωδικός πρόσβασης καθώς και μη διαδραστική λειτουργία, όπου οι κωδικοί πρόσβασης παρέχονται μέσω ενός δωσμένου αρχείου κωδικού πρόσβασης. Η μη διαδραστική λειτουργία προορίζεται μόνο για συγγραφή σε δίκτυα δοκιμών ή γνωστά ασφαλή περιβάλλοντα.
- **Mining:** Προς το παρόν, η Geth περιλαμβάνει μόνο CPU miner, το GPU miner δοκιμάζεται ακόμη, αλλά αυτό δεν θα είναι μέρος του Frontier. Η εφαρμογή C ++ του Ethereum προσφέρει επίσης έναν GPU miner, τόσο ως μέρος του Eth (CLI) του και του AlethZero (του GUI) όσο και του EthMiner (του αυτόνομου miner). Κατά την εκκίνηση του Ethereum κόμβου με το Geth, το mining δεν υφίσταται από προεπιλογή. Για να ξεκινήσει η λειτουργία mining, χρησιμοποιείται η επιλογή της γραμμής εντολών --mine. Η παράμετρος -minerthreads μπορεί να χρησιμοποιηθεί για τον ορισμό των αριθμών των παράλληλων threads mining (θέτοντας τον συνολικό αριθμό πυρήνων του επεξεργαστή). Μπορεί επίσης, να ξεκινήσει και να σταματήσει το CPU mining κατά τον χρόνο εκτέλεσης χρησιμοποιώντας την κονσόλα. Η –miner.start εντολή έχει μια προαιρετική παράμετρο για την εισαγωγή του αριθμό των miner threads π.χ. miner.start (5) , 5 threads. Το mining για πραγματικό ether έχει νόημα μόνο αν υπάρχει συγχρονισμός με το δίκτυο. Το mining θα καθυστερήσει μέχρι να γίνει συγχρονισμός και μετά ξεκινά αυτόματα το mining μέχρι να επιλεγεί να σταματήσει με την εντολή miner.stop()

4. Διαμόρφωση και Εγκατάστασης Εφαρμογής

Για την υλοποίηση της μεθόδου ενός ομότιμου P2P δικτύου στα πρότυπα ενός Μικροδικτύου (των προαναφερόμενων προδιαγραφών), χρησιμοποιείται το εργαλείο Geth του Ethereum και η βιβλιοθήκη Genesis.json για την δημιουργία του αρχικού Block της αλυσίδας του Blockchain.

4.1 Genesis Block

Το ίδιο Genesis.json αρχείο εφαρμόζεται και στους δύο κόμβους, στην δική μας περίπτωση στο Raspberry Pi και τον φορητό υπολογιστή που φέρουν το ίδιο λογισμικό, έτσι ώστε και οι δύο χρήστες να έχουν το ίδιο Genesis block το οποίο είναι και το αρχικό block της αλυσίδας του δικτύου. Η βιβλιοθήκη Genesis.json που χρησιμοποιήθηκε και για τους δύο κόμβους φαίνεται παρακάτω:

```
"config": {
"chainId": 15,
"homesteadBlock": 0,
"eip155Block": 0,
"eip158Block": 0
},
"nonce": "0x0000000000000042",
"mixhash":
"0x0000000000000000000000000000000000000000000000000000000000000000",
"difficulty": "0x200",
```

```
"alloc": {},

"coinbase": "0x0000000000000000000000000000000000000000",

"timestamp": "0x00",

"parentHash":
"0x0000000000000000000000000000000000000000000000000000000000000000",

"gasLimit": "0xffffffff",

"alloc": {

}

}
```

Table 8 – Παράμετροι Genesis Block [63]

4.1.1 Genesis Block: Επεξήγηση Παραμέτρων

Παρακάτω επεξηγούνται κάποιες από τις παραμέτρους του Genesis Block:

mixhash: Ένα hash 256-bit που αποδεικνύει, σε συνδυασμό με το nonce, ότι έχει πραγματοποιηθεί ένας επαρκής αριθμός υπολογισμών σε αυτό το μπλοκ: το Proof of Work (PoW). Ο συνδυασμός nonce και mixhash πρέπει να ικανοποιεί μια μαθηματική κατάσταση που περιγράφεται στο Yellow Paper, 4.3.4. Έγκυρη επικεφαλίδα μπλοκ, (44). Επιτρέπει την επαλήθευση ότι το Block έχει πραγματικά εξορυχτεί κρυπτογραφικά, επομένως είναι έγκυρο.

nonce: Ένα hash 64-bit, που αποδεικνύει, σε συνδυασμό με το hash mix, ότι έχει πραγματοποιηθεί επαρκής υπολογισμός σε αυτό το μπλοκ: το Proof-of-Work (PoW). Ο συνδυασμός nonce και mixhash πρέπει να ικανοποιεί μια μαθηματική κατάσταση που περιγράφεται στο Yellow Paper, 4.3.4. Blank Header Validity, (44), και επιτρέπει να επαληθεύσουμε ότι το Block έχει πραγματικά εξορυχτεί κρυπτογραφικά και επομένως, από αυτή την άποψη, είναι έγκυρο. Το nonce είναι η κρυπτογραφικά ασφαλής απόδειξη της

εργασίας για εξόρυξη που αποδεικνύει πέρα από κάθε εύλογη αμφιβολία ότι ένα συγκεκριμένο ποσό υπολογισμών έχει δαπανηθεί για τον προσδιορισμό αυτής της συμβολικής αξίας.

difficulty: Μια βαθμωτή τιμή που αντιστοιχεί στο επίπεδο δυσκολίας που εφαρμόζεται κατά τη διάρκεια της nonce ανακάλυψης αυτού του block. Ορίζει το Target για εξόρυξη, το οποίο μπορεί να υπολογιστεί από το επίπεδο δυσκολίας του προηγούμενου μπλοκ και το timestamp. Όσο μεγαλύτερη είναι η δυσκολία, τόσο περισσότερους υπολογισμούς πρέπει να εκτελέσει ένας miner για να ανακαλύψει ένα έγκυρο block. Αυτή η τιμή χρησιμοποιείται για τον έλεγχο του χρόνου δημιουργίας block ενός Blockchain, διατηρώντας τη συχνότητα δημιουργίας Block σε μια περιοχή στόχου. Στο δοκιμαστικό δίκτυο διατηρούμε αυτήν την τιμή χαμηλή για να αποφύγουμε την αναμονή κατά τη διάρκεια των δοκιμών, καθώς απαιτείται η ανακάλυψη ενός έγκυρου block για την εκτέλεση μιας συναλλαγής στο blockchain.

alloc: Επιτρέπει τον καθορισμό μιας λίστας ήδη γεμισμένων πορτοφολιών. Αυτή είναι μια ειδική λειτουργικότητα του Ethereum για να χειριστεί την περίοδο "Ether πριν την πώληση".

coinbase: Η διεύθυνση 160-bit στην οποία μεταφέρθηκαν όλες οι ανταμοιβές (σε Ether) που συλλέχθηκαν από την επιτυχή εξόρυξη αυτού του Block. Πρόκειται για ένα ποσό της ίδιας της ανταμοιβής εξόρυξης και των επιστροφών εκτέλεσης της σύμβασης. Συχνά ονομάζεται "δικαιούχος" στις προδιαγραφές, μερικές φορές "etherbase" στην ηλεκτρονική τεκμηρίωση. Αυτό μπορεί να είναι οτιδήποτε στο Genesis Block αφού η τιμή καθορίζεται από τη ρύθμιση του Miner όταν δημιουργείται ένα νέο block.

timestamp: Μια βαθμωτή τιμή ίση με τη λογική έξοδο της λειτουργίας του χρόνου Unix () στην αρχή του Block. Ο μηχανισμός αυτός επιβάλλει μια ομοιοστασία από την άποψη του χρόνου μεταξύ των Block. Μία μικρότερη περίοδος μεταξύ των δύο τελευταίων Block έχει ως αποτέλεσμα την αύξηση του επιπέδου δυσκολίας και συνεπώς επιπλέον υπολογισμό που απαιτείται για να βρεθεί το επόμενο έγκυρο Block. Εάν η περίοδος είναι πολύ μεγάλη, μειώνεται η δυσκολία και ο αναμενόμενος χρόνος στο επόμενο Block.

parentHash: Ο Keccak 256-bit hash ολόκληρου του parent block header (συμπεριλαμβανομένου του nonce και του mixhash). Δείκτης του parent block, δημιουργώντας έτσι την αλυσίδα των block. Στην περίπτωση του Block Genesis, και μόνο στην περίπτωση αυτή, είναι 0.

gasLimit: Μια βαθμωτή τιμή ίση με το τρέχον όριο της συνολικής αλυσίδας της δαπάνης gas ανά block. Υψηλή στην περίπτωσή μας για να αποφευχθεί να περιοριστεί αυτό το όριο κατά τη διάρκεια των δοκιμών. Σημείωση: αυτό δεν δείχνει ότι δεν πρέπει να δίνεται προσοχή στην κατανάλωση gas των συμβολαίων.

config: Διαμόρφωση για την περιγραφή της ίδιας της αλυσίδας. Συγκεκριμένα, περιγράφεται το cchain ID και οι μηχανές συναίνεσης που θα χρησιμοποιηθούν.

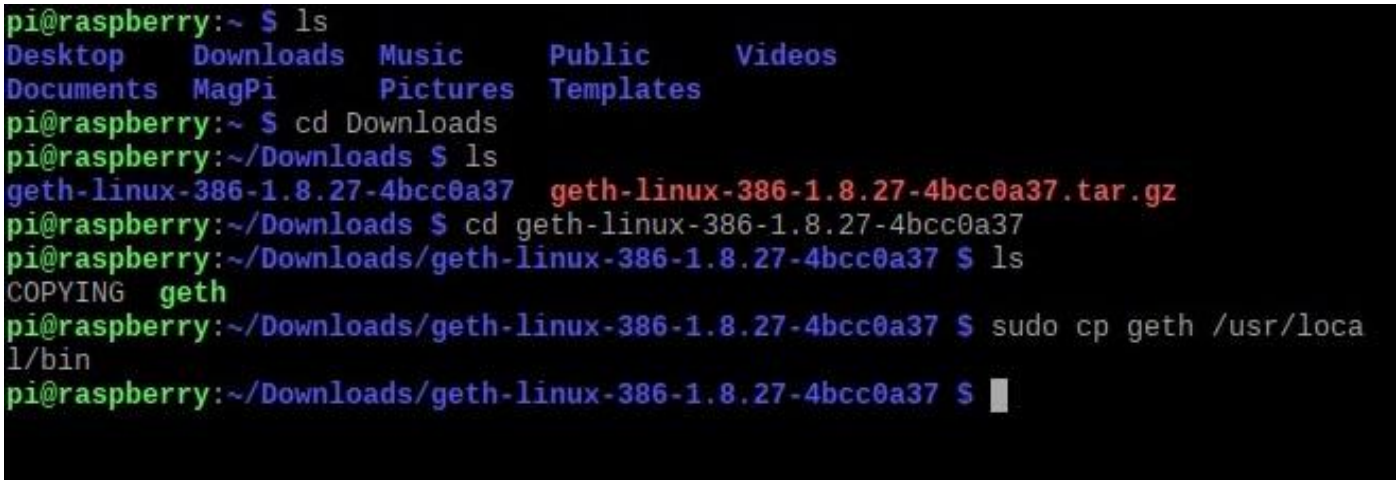
4.2 Εγκατάσταση των Nodes

Έχοντας εγκατεστημένο το Debian ver.9-64bit, λογισμικό βασισμένο σε Linux, και στις δυο τερματικές συσκευές (Φορητός Υπολογιστής και Raspberry Pi 3 B+) , το επόμενο βήμα είναι η εγκατάσταση του Geth εκτελέσιμου αρχείου για την δημιουργία κόμβων και στα δύο τερματικά.

Εν συνεχεία, με κατεβασμένο το Geth αρχείου από το link που προαναφέρθηκε σε προηγούμενη ενότητα, από το terminal και των δύο συσκευών θα πρέπει να γίνει η εγκατάσταση του Geth στο bin directory τους. Η εντολή που ακολουθείται είναι η παρακάτω:

```
$ sudo cp geth /usr/local/bin
```

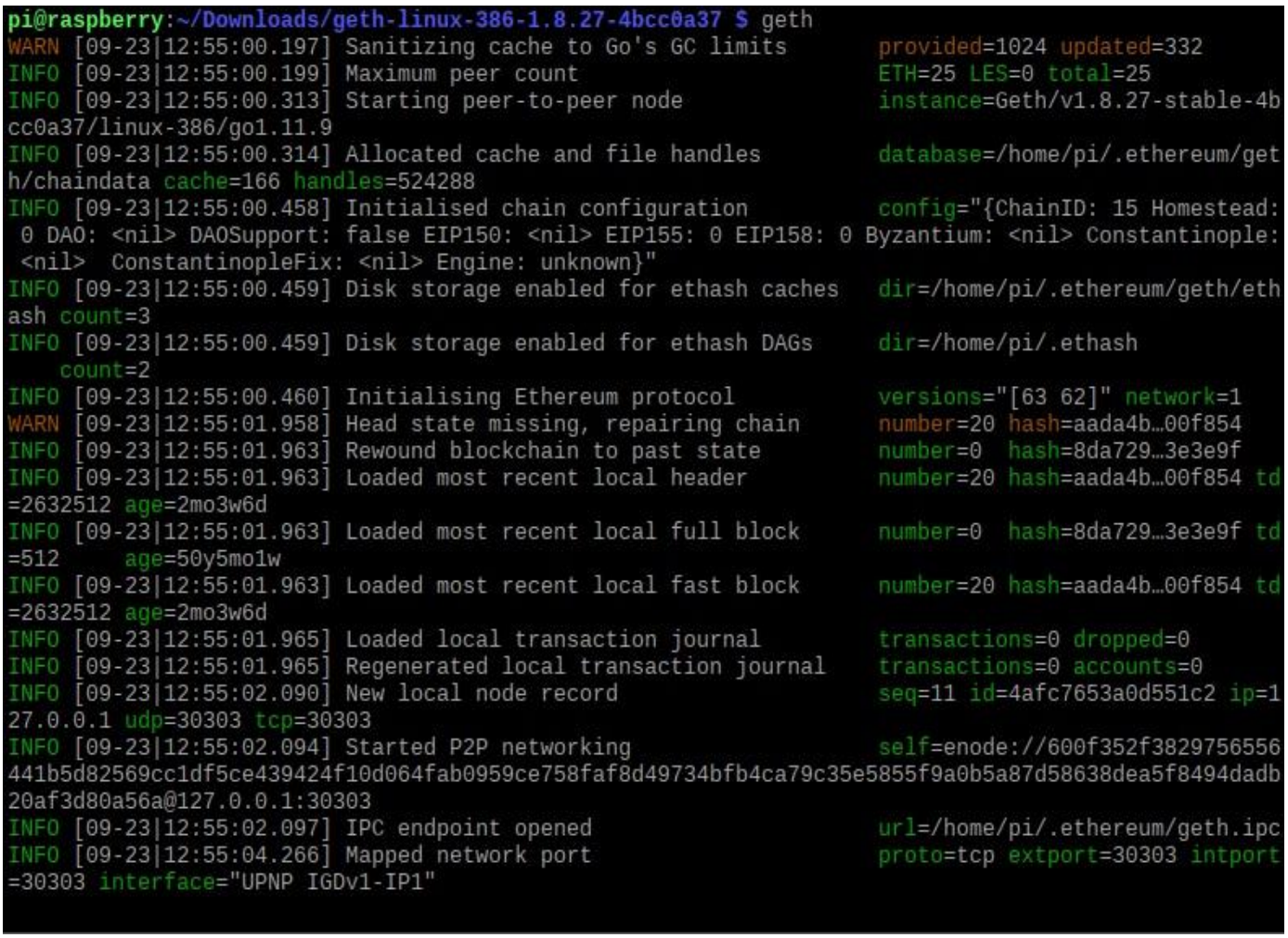
Δεδομένου ότι έχουμε ήδη εισέλθει στο σωστό directory, όπου βρίσκεται το geth αρχείο, από το Terminal ώστε να εγκατασταθεί στο παραπάνω Directory. (*Η ίδια διαδικασία επαναλαμβάνεται και στα δύο τερματικά).*



Εικόνα 31: Εγκατάσταση geth αρχείου στις Τερματικές συσκευές

Επαλήθευσης εγκατάστασης Geth αρχείου με την εντολή:

$ geth



Εικόνα 32: Επαλήθευση Εγκατάστασης geth αρχείου

4.3 Εγκατάσταση Genesis Block

Με την ολοκλήρωση της εγκατάστασης του Geth θα πρέπει σε αυτό το σημείο να οριστεί αρχικό Block και να εγκατασταθεί το αρχείο που θα πληροί τις προϋποθέσεις του αρχικού block του δικτύου και των δύο κόμβων. Το αρχείο αυτό είναι το Genesis.json το οποίο περιέχει όλες τις παραμέτρους του πρώτου Block και με την εντολή που φαίνεται παρακάτω το εγκαθιστάμε:

$ geth init Genesis.json

Δεδομένου ότι και στα δύο Terminal των συσκευών βρισκόμαστε στο directory που υπάρχει το Genesis αρχείο.

```
pi@raspberry:~ $ cd Desktop
pi@raspberry:~/Desktop $ ls
Genesis.json
pi@raspberry:~/Desktop $ geth init Genesis.json
WARN [09-24|11:24:19.675] Sanitizing cache to Go's GC limits       provided=1024
 updated=332
INFO [09-24|11:24:19.700] Maximum peer count                       ETH=25 LES=0
total=25
INFO [09-24|11:24:19.701] Allocated cache and file handles         database=/hom
e/pi/.ethereum/geth/chaindata cache=16 handles=16
INFO [09-24|11:24:19.717] Persisted trie from memory database      nodes=0 size=
0.00B time=3.573µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [09-24|11:24:19.717] Successfully wrote genesis state         database=chai
ndata                             hash=8da729…3e3e9f
INFO [09-24|11:24:19.717] Allocated cache and file handles         database=/hom
e/pi/.ethereum/geth/lightchaindata cache=16 handles=16
INFO [09-24|11:24:19.764] Persisted trie from memory database      nodes=0 size=
0.00B time=2.69µs  gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [09-24|11:24:19.765] Successfully wrote genesis state         database=ligh
tchaindata                        hash=8da729…3e3e9f
pi@raspberry:~/Desktop $
```

Εικόνα 33: Εγκατάσταση του Genesis Block για αρχικοποίηση του πρώτου block του δικτύου και των δύο χρηστών

4.4 Δημιουργία Log Αρχείων

Σε αυτό το σημείο δημιουργούνται και για τους δύο χρήστες log αρχεία για την καταγραφή των κινήσεων τους στο δίκτυο, το οποίο θα μας βοηθήσει στην παρακολούθηση της μεταξύ τους συναλλαγής παρακάτω. Οι εντολές για την δημιουργία κονσόλας και log αρχείων είναι οι εξής:

$ geth --nodiscover console 2>> eth.log

```
pi@raspberry:~/Desktop $ geth --nodiscover console 2>> eth.log
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.27-stable-4bcc0a37/linux-386/go1.11.9
coinbase: 0x52e8387720136d060de95f8eead46a7b452eb672
at block: 0 (Thu, 01 Jan 1970 01:00:00 BST)
 datadir: /home/pi/.ethereum
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.
0 txpool:1.0 web3:1.0
```

Εικόνα 34: Δημιουργία Javascript Console για παρακολούθηση κινήσεων δικτύου

$ tail -F eth.log

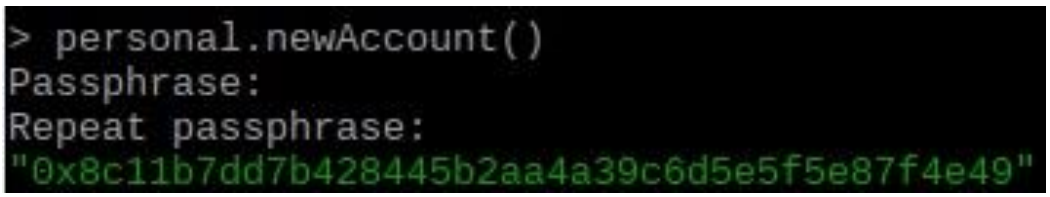
```
pi@raspberry:~/Desktop $ tail -F eth.log
INFO [09-24|11:45:13.147] Loaded most recent local header          number=20 has
h=aada4b…00f854 td=2632512 age=2mo4w15h
INFO [09-24|11:45:13.147] Loaded most recent local full block      number=0  has
h=8da729…3e3e9f td=512     age=50y5mo1w
INFO [09-24|11:45:13.147] Loaded most recent local fast block      number=20 has
h=aada4b…00f854 td=2632512 age=2mo4w15h
INFO [09-24|11:45:13.148] Loaded local transaction journal         transactions=
0 dropped=0
INFO [09-24|11:45:13.148] Regenerated local transaction journal    transactions=
0 accounts=0
INFO [09-24|11:45:13.162] New local node record                    seq=15 id=4af
c7653a0d551c2 ip=127.0.0.1 udp=0 tcp=30303
INFO [09-24|11:45:13.162] IPC endpoint opened                      url=/home/pi/
.ethereum/geth.ipc
INFO [09-24|11:45:13.162] Started P2P networking                   self="enode:/
/600f352f3829756556441b5d82569cc1df5ce439424f10d064fab0959ce758faf8d49734bfb4ca7
9c35e5855f9a0b5a87d58638dea5f8494dadb20af3d80a56a@127.0.0.1:30303?discport=0"
INFO [09-24|11:45:13.273] Etherbase automatically configured       address=0x52e
8387720136d060de95F8eEaD46A7B452Eb672
INFO [09-24|11:45:15.378] Mapped network port                      proto=tcp ext
port=30303 intport=30303 interface="UPNP IGDv1-IP1"
```

Εικόνα 35: παρακολούθηση του Log αρχείου που δημιουργήθηκε και των κινήσεων του δικτύου

4.5 Δημιουργία Λογαριασμού στους Κόμβους

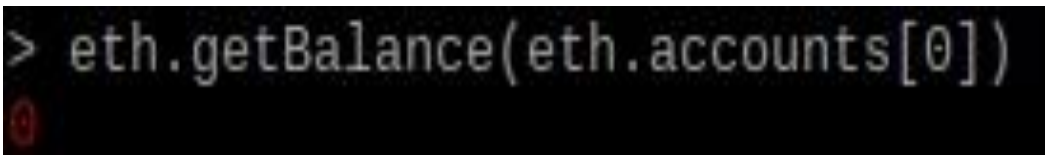
Σε αυτό το σημείο, θα δημιουργηθούν λογαριασμοί και στους δύο κόμβους με μηδενικό αρχικό ποσό σε tokens για να είναι εφικτές οι συναλλαγές μεταξύ τους. Για την δημιουργία λογαριασμών και επαλήθευσης μηδενικού ποσού σε αυτούς οι εντολές που χρησιμοποιήθηκαν φαίνονται παρακάτω:

> personal.newAccount()



Εικόνα 36: Δημιουργία Λογαριασμού ενός εκ ων κόμβων

> eth.getBalance(eth.accounts[0])



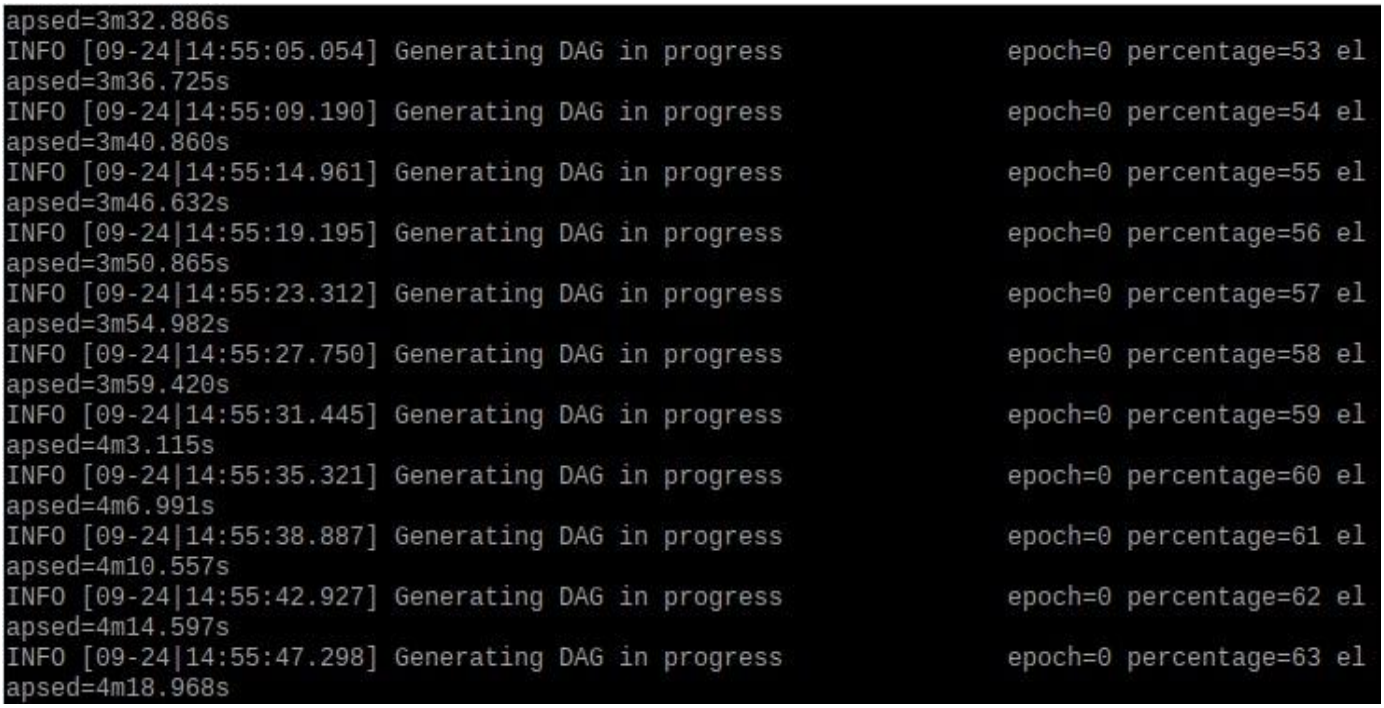
Εικόνα 37: Ορισμός 0 ποσού στον λογαριασμό που δημιουργήθηκε και επίβλεψη ποσού που υπάρχει μέσα στο λογαριασμό με την ίδια εντολή

4.6 Mining

Εφόσον και στους δύο κόμβους ολοκληρώθηκαν οι λογαριασμοί, ένας εξ αυτών (φορητός υπολογιστής) θα κάνει mining για token προσφέροντας στο δίκτυο επεξεργαστική ισχύ, και ο άλλος (Raspberry Pi) θα δεχτεί στον λογαριασμό του όσα tokens αποφασίσει ο πρώτος χρήστης ολοκληρώνοντας έτσι μια συναλλαγή. Η εντολή φαίνεται παρακάτω:

> miner.start()

Εικόνα 38: Εντολή έναρξης mining

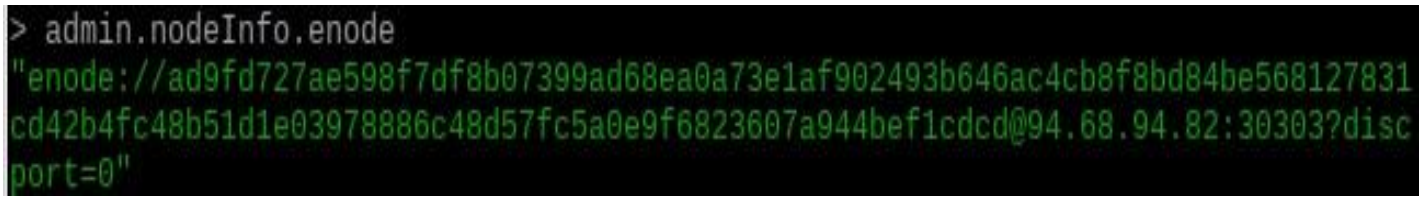


Εικόνα 39: Αρχείο log κατά τη διάρκεια του mining

4.7 Ζεύξη μεταξύ των δύο Κόμβων (Peering)

Ολοκληρώνοντας το mining ο πρώτος κόμβος (node 1) θα μεταφέρουμε κάποια Ethers στον δεύτερο κόμβο (node 2). Ο κόμβος 1 θα κάνει mining μέχρι να του δοθεί η εντολή να σταματήσεις, > miner.stop(). Παρακάτω φαίνεται ποιες εντολές χρησιμοποιήθηκαν για την ζεύξη των κόμβων και την ολοκλήρωση της συναλλαγής:

Node 1: > admin.nodeInfo.enode



Εικόνα 40- Πληροφορίες της διεύθυνσης του Node 1

Με την εντολή ifconfig σε ξεχωριστό terminal εξετάζουμε ποια είναι η ip του Node 1, και την αντικαθιστούμε στην παραπάνω εντολή του nodeInfo στη θέση του @94.68.94.82 και περνάμε την καινούρια εντολή στον Node 2.

Node 2: > admin.addPeer("enode://c667fdf1f6846af74ed14070ef9ffeee33e98ff8ab0dd43f67415868974d8205e0fb7f55f6f37e9e1ebb112adfc0b88755714c7bc83a7ac47d30f8eb53118687@192.168.1.10:30303?discport=0")

Η επαλήθευση της ζεύξης και στους δύο κόμβους πραγματοποιείται με την εντολή:

> admin.peers

Η localAddresss ανήκει στον Node 1

Η remoteAddress ανήκει στον Node 2

Εικόνα 41-Node 1: Επαλήθευση Ζεύξης των δύο κόμβων

4.8 Συναλλαγή μεταξύ των δύο κόμβων

Για την μεταφορά tokens (στην προκειμένη περίπτωση ethers) από τον node 1 που έκανε το mining στον node 2 εισάγονται διαδοχικά οι παρακάτω εντολές:

Node 1:

> web3.fromWei(eth.getBalance(eth.coinbase), “ether”) -> εμφανίζεται το υπόλοιπο του λογαριασμού του Node 1

> personal.unlockAccount(eth.coinbase) -> ζητείται κωδικός του λογαριασμού του Node 1

>eth.sendTransaction({from:eth.coinbase,to: "0x790a995c356a96ededcb0b9fb4f8727b5a96dc8d", value: web3.toWei(10, “ether”)}) -> βάζουμε το coinbase του Node 2 με τον οποίο θέλουμε να συναλλάξουμε και το ποσό, ενδεικτικά έχουμε αφήσει το ποσό των 10 ethers

> miner.start() -> γίνεται mine το block της συναλλαγής

Node 2:

> web3.fromWei(eth.getBalance(eth.coinbase), “ether”) –>ελέγχεται το υπόλοιπο του Node 2, το οποίο αρχικά είναι 0

Από το mining που πραγματοποιήθηκε στον Node 1 το ποσό που προέκυψε φαίνεται παρακάτω:

```
pi@raspberry:~ $ cd Desktop
pi@raspberry:~/Desktop $ geth init Genesis.json
INFO [10-25|20:47:43.803] Maximum peer count                       ETH=25 LES=0
total=25
INFO [10-25|20:47:43.804] Allocated cache and file handles         database=/hom
e/pi/.ethereum/geth/chaindata cache=16 handles=16
INFO [10-25|20:47:43.809] Persisted trie from memory database      nodes=0 size=
0.00B time=2.855µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [10-25|20:47:43.810] Successfully wrote genesis state         database=chai
ndata                            hash=8da729…3e3e9f
INFO [10-25|20:47:43.810] Allocated cache and file handles         database=/hom
e/pi/.ethereum/geth/lightchaindata cache=16 handles=16
INFO [10-25|20:47:43.816] Persisted trie from memory database      nodes=0 size=
0.00B time=2.883µs gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [10-25|20:47:43.817] Successfully wrote genesis state         database=ligh
tchaindata                         hash=8da729…3e3e9f
pi@raspberry:~/Desktop $ geth --nodiscover console 2>> eth.log
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.27-stable-4bcc0a37/linux-386/go1.11.9
coinbase: 0xb203a12848064b5236721aa95b0b5888fea2bcba
at block: 182 (Tue, 22 Oct 2019 17:37:07 BST)
 datadir: /home/pi/.ethereum
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0
rpc:1.0 txpool:1.0 web3:1.0

> personal.newAccount()
Passphrase:
Repeat passphrase:
"0xb339fdb7c4ec0f53f283db2adb60bec3361f5743"
> eth.getBalance(eth.accounts[0])
91000000000000000000
```

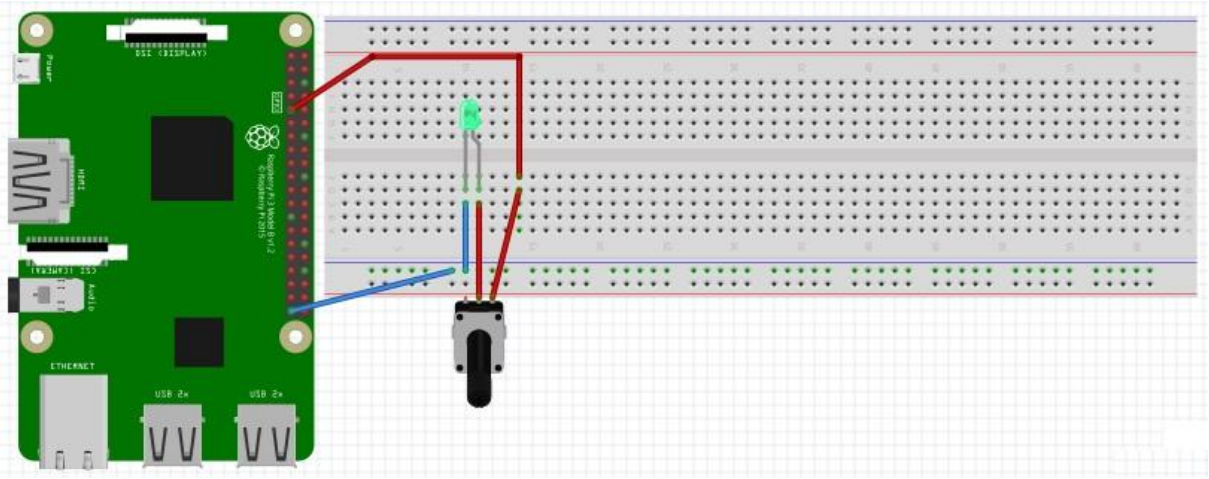
Εικόνα 42 - Υπόλοιπο Ethers στον λογαριασμό του Node 1

Ενδεικτικά επιλέγεται να μεταφερθούν από τον λογαριασμό του Node 1 στον λογαριασμό του Node 2 10 Ethers.

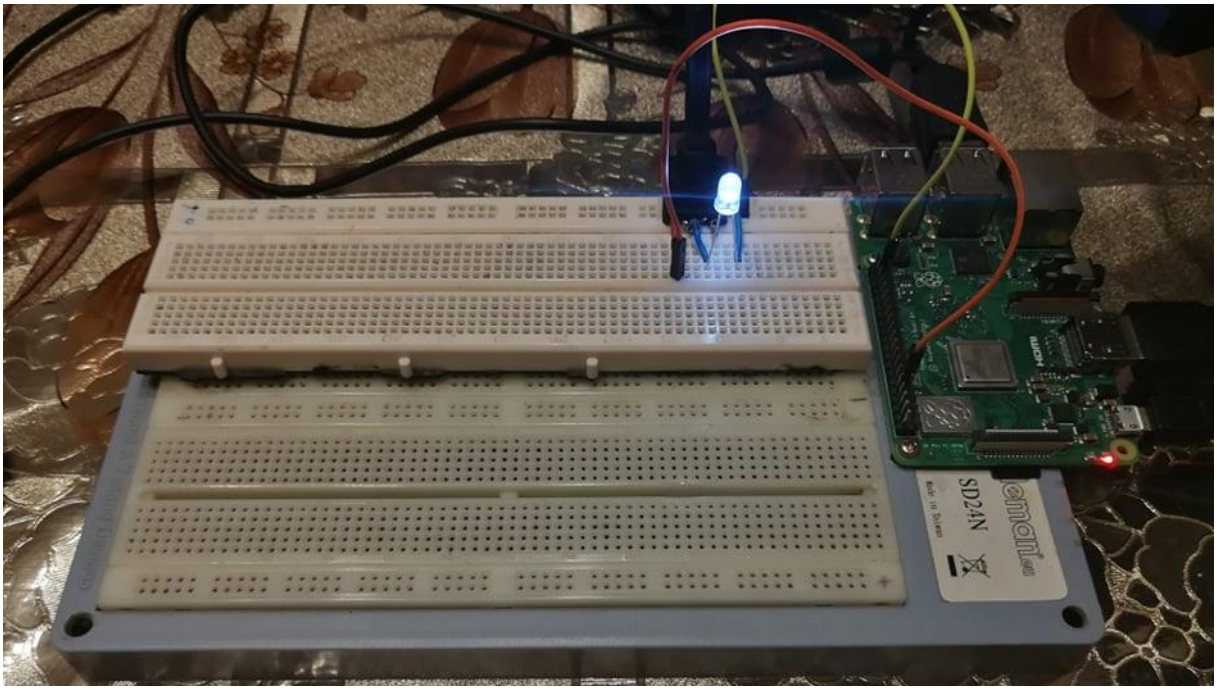
4.9 Ολοκλήρωση Συναλλαγής

Με την ολοκλήρωση της συναλλαγής και με τον κατάλληλο κώδικα γραμμένο σε Python έχουμε δημιουργήσει ένα Smart Contract του οποίου ένα LED, σε σειρά συνδεδεμένο με το RPi, όταν το GPIO 17 γίνει HIGH θα ανάψει. Τον κώδικα τον καλούμε από ξεχωριστό Terminal με την εντολή > sudo python TC.py, TC.py (Transaction Completed) είναι το όνομα του αρχείου του κώδικα το οποίο αποθηκεύεται σε .py μορφή για να διαβαστεί και να τρέξει από τον compiler της python του Linux με την παραπάνω εντολή. Η συνδεσμολογία του LED με το RPi φαίνεται παρακάτω καθώς και η ενδεικτική φωτογραφία του αναμένου LED κατά την ολοκλήρωση της συναλλαγής:

Εικόνα 43 – GPIO RPi Model A+, B+ & Pi2



Εικόνα 44 – Συνδεσμολογία ενδεικτικού LED με RPi



Εικόνα 45 – Ενδεικτικό LED ολοκλήρωσης συναλλαγής στη θέση HIGH

5. Συμπεράσματα - Προτάσεις

Στην παρούσα εργασία μελετήθηκαν και αναπτύχθηκαν τεχνολογίες του Διαδικτύου των Πραγμάτων και της Ενέργειας (IoT & IoE) για την δημιουργία ενός έξυπνου και ευέλικτου προς όλους τους χρήστες δικτύου. Το τωρινό δίκτυο ενέργειας που επικρατεί (γνωστό και ως Large Grid) λειτουργεί στα πλαίσια του client- server πρωτόκολλου έχοντας τα χαρακτηριστικά κεντρωμένου δικτύου. Στην διπλωματική αυτή περιγράφεται και υλοποιείται μία διάταξη αποκεντρωμένου δικτύου με δικαίωμα πρόσβασης προς όλους τους χρήστες. Το δίκτυο καθιερώνεται σε P2P ζεύξη δίνοντας την ιδιότητα σε όλους τους χρήστες να είναι ομότιμοι, δημιουργώντας ένα εντελώς καινούριο πρωτόκολλο από το καθιερωμένο, το server-server.

Για την ανάδειξη μίας τέτοιας εφαρμογής, αναλύονται εκτενώς οι Τεχνολογίες Κατανεμημένου Μητρώου (DLT) με μεγαλύτερη ευχρηστία να έχει το Blockchain. Το Blockchain ως η πιο διαδεδομένη DLT τεχνολογία, επιλέγεται εν αντιθέσει των DAG και Hashgraph τεχνολογιών διότι:

- είναι πλήρως αποκεντρωμένο σύστημα υποστηρίζοντας εξίσου Αποκεντρωμένες εφαρμογές (DApps)
- έχει δοκιμαστεί σε πραγματικές συνθήκες στην ευρύ αγορά

Στο πρακτικό κομμάτι της εργασίας, το Μικροδίκτυο που στήνεται είναι ένα Permissioned Private Ethereum περιορίζοντας τους εκάστοτε χρήστες στα δικαιώματα ανάγνωσης συναλλαγών στο δίκτυο και αποστολής ή επαλήθευσης συναλλαγών σε αυτό. Αυτό που τελικά επιτυγχάνεται είναι η ανταλλαγή ψηφιακών νομισμάτων (Ethers/Tokens) μεταξύ των δύο κόμβων χωρίς όμως να σημαίνει ότι οι δυνατότητες δόμησης ενός τέτοιου δικτύου περιορίζονται εδώ. Πέραν από τη μεταφορά δεδομένων και πληροφοριών, προσφέρεται η ευελιξία χρήσης για μεταφορά ηλεκτρικής ενέργειας μεταξύ των συμμετεχόντων, δεδομένης της ύπαρξης της ανάλογης διάταξης στο δίκτυο.

Η δόμηση ενός τέτοιου δικτύου ποικίλει σε πλεονεκτήματα και συνίσταται εφαρμογής προσφέροντας:

- αποκεντρωμένη αποθήκευση δεδομένων. Τα δεδομένα που αποθηκεύονται στο Blockchain είναι ανιχνεύσιμα και μη προσβάσιμα.

Δημιουργούνται αντίγραφα στους κόμβους συγχρονίζοντας τα δεδομένα όλων των χρηστών μέσω του Διαδικτύου.

- Ασφάλεια στα δεδομένα και την ταυτότητα του κάθε χρήστη στο δίκτυο, παρέχοντας του ένα τέτοιο περιβάλλον καταχώρησης δεδομένων, στο οποί ακόμη και αν ένας χρήστης χαθεί από το δίκτυο οι πληροφορίες συναλλαγών του παραμένουν ανεξίτηλες στο δίκτυο.
- Ευελιξία στον καθορισμό ευθυνών κάθε χρήστη και τους όρους εκτέλεσης της σύμβασης τους. Τα smart contracts είναι προγραμματιζόμενα προσφέροντας την δυνατότητα διαφορετικών λογικών εφαρμογών ανάλογων των προτιμήσεων του δικτύου.
- Ταχύτητα και αμεσότητα στη συναλλαγή πληροφοριών, με την συμβολή των αποκεντρωμένων εφαρμογών οι ανταλλαγές πληροφοριών πραγματοποιούνται από οπουδήποτε και οποιαδήποτε χρονική στιγμή
- Κατάργηση των διαμεσολαβητών, οι οποίοι πιθανόν να είναι τράπεζες, πολυεθνικές ή ακόμη και κεντρικοί πάροχοι ηλεκτρικής ενέργειας. Πλέον στο προτεινόμενο δίκτυο δεν υφίσταται το Client-Server πρωτόκολλο αλλά το Server-Server και για την πραγματοποίηση μιας συναλλαγής δεν χρειάζεται η έγκριση εξωτερικού παράγοντα.

Με το Blockchain ένας χρήστης έχει την δυνατότητα να διαμοιράσει ηλεκτρική ενέργεια στο υπόλοιπο δίκτυο, με την απαραίτητη διάταξη. Υφίστανται ήδη υλοποιημένα projects μεταφοράς διαμοιρασμού ηλεκτρικής ενέργειας μέσα στο δίκτυο, μερικά εξ αυτών έχουν αναφερθεί παραπάνω. Η εφαρμογή αυτή προτείνεται και ποικίλει σε πλεονεκτήματα έχοντας σημαντικό αντίκτυπο στον τομέα στης ηλεκτρική ενέργειας, τόσο στην διάδοση της όσο και στην μείωση τελικά του κόστους κατασκευής ενός συμβατικού δικτύου.

Βιβλιογραφία – Πηγές

[1] J. Mattila, "The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures," ETLA - The Research institute of the Finnish Economy, 2016.

[2] Green, Jemma and Newman, Peter, "Citizen utilities: The emerging power paradigm," Energy Policy, vol. 105, no. June 2017, pp. 283-293, 2017.

[3] T. S. C. N. R. S. M. T. A. B. J. S. Juri Mattila, "Industrial Blockchain Platforms. An Exercise in Use Cases in the Energy Industry," Research Institute of the Finnish Economy, 2016

[4] Karen Rose, Scott Eldridge, Lyman Chapin, «THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World», Internet of society, 2015. [Ηλεκτρονικό]. Available: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[5] Upasana, «Real World IoT Applications in Different Domains», 2019. [Ηλεκτρονικό]. Available: https://www.edureka.co/blog/iot-applications/ IoT

[6] NES Global Talent, «What is The Internet Of Energy?», nesgt,2019. [Ηλεκτρονικό]. Available: https://www.nesgt.com/blog/2019/05/what-is-the-internet-of-energy

[7] James Chen, Internet of Energy (IoE), 2019. [Ηλεκτρονικό]. Available: https://www.investopedia.com/terms/i/internet-energy-ioe.asp

[8] «What does the internet of things means for energy», 2017. [Ηλεκτρονικό]. Available: https://www.drax.com/technology/internet-things-mean-energy/

[9] «From a smart grid o Internet of Energy», 2019. [Ηλεκτρονικό]. Available: https://www.smart-energy.com/industry-sectors/smart-grid/from-a-smart-grid-to-the-internet-of-energy/

[10] Glenn Schatz, «What's Going On With The Internet Of Energy?», LinkLabs.2016. [Ηλεκτρονικό]. Available: https://www.link-labs.com/blog/internet-of-energy

[11] Sophie Bessin-Py, «The Internet of Energy: delivering safe, smart energy in the smart city era», IoT, 2019. [Ηλεκτρονικό]. Available:

https://blog.gemalto.com/iot/2019/01/31/the-internet-of-energy-delivering-safe-smart-energy-in-the-smart-city-era/

[12] Michael Chagala
Manager of Marketing Technology, «What Is the Internet of Energy?», San Diego Business Journal, 2016. [Ηλεκτρονικό]. Available:

https://www.bakerhomeenergy.com/blog/2016-10-17/what-is-the-internet-of-energy

[13] Pamela Largue, «Partnership uses revolutionary IoE to optimise grid management», 2018. [Ηλεκτρονικό]. Available:
https://www.smart-energy.com/regional-news/north-america/partnership-ioe-grid-management/ IoE

[14] «Internet of Energy for Electric Mobility». [Ηλεκτρονικό]. Available:http://www.artemis-ioe.eu/ Ioe (image 5)

[15] Internet Society, «Blockchain», 2018. [Ηλεκτρονικό]. Available: https://www.internetsociety.org/issues/blockchain/?gclid=Cj0KCQjwu-HoBRD5ARIsAPIPendVv8hRmgyomAkY6WZAYou6dO0ec_eCDEDIpEss5JtOKZ1OEfvFoREaAvX4EALw_wcB

[16] Samuel Tweneboah-Koduah, «Evaluation of Cybersecurity Threats on Smart Metering System», ResearchGate, 2018. [Ηλεκτρονικό]. Available: https://www.researchgate.net/figure/Smart-Metering-Communication-Architecture-vii-The-Home-Area-Network-HAN-Gateway-It_fig1_318601090

[17] *Alyssa Hertig, «*What is a Decentralized Application?». [Ηλεκτρονικό]. Available:
https://www.coindesk.com/information/what-is-a-decentralized-application-dapp

[18] EEGI, **« European Electricity Grid Initiative** (EEGI)», 2019. [Ηλεκτρονικό]. Available: https://www.edsoforsmartgrids.eu/policy/eu-steering-initiatives/eegi/

[19] Vitalik Buterin, «A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM». [Ηλεκτρονικό]. Available" https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[20] Vitalik Buterin, «On Public and Private Blockchains», 2015. [Ηλεκτρονικό]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[21] Oliver Belin, «The Difference Between Blockchain & Distributed Ledger Technology». [Ηλεκτρονικό]. Available: https://tradeix.com/distributed-ledger-technology/

[22] Michael R., «Distributed Ledger Technology for Dummies», CryptoManiaks. [Ηλεκτρονικό]. Available: https://cryptomaniaks.com/guides/distributed-ledger-technology-for-dummies

[23] ConsenSys, «Blockchain vs. Distributed Ledger Technologies», 2018. [Ηλεκτρονικό]. Available: https://media.consensys.net/blockchain-vs-distributed-ledger-technologies-1e0289a87b16

[24] JAKE FRANKENFIELD, «IOTA Definition», 2018. [Ηλεκτρονικό]. Available: https://www.investopedia.com/terms/i/iota.asp

[25] Charlie Crisp, «Building with HashGraph Part 1: Introduction», Hackers at Cambridge, 2018. [Ηλεκτρονικό]. Available: https://medium.com/hackers-at-cambridge/building-with-hashgraph-part-1-introduction-3232f9ea89ef

[26] Shawn Dexter. «Blockchain vs DLT (Distributed Ledger Technology)», 2018. [Ηλεκτρονικό]. Available: https://www.mangoresearch.co/blockchain-vs-distributed-ledger-technology-dlt/

[27] SE4ALL Global Tracking Framework, «Access to electricity», WORLD BANK GROUP, 2019. [Ηλεκτρονικό]. Available: https://data.worldbank.org/indicator/eg.elc.accs.zs

[28] «Energy Access», Energy Access outlook 2017, 2017. [Ηλεκτρονικό]. Available: https://www.iea.org/energyaccess/database/

[29] «World Energy Situation», Thorium Energy World, 2018. [Ηλεκτρονικό]. Available: http://www.thoriumenergyworld.com/energy.html

[30] Michael Merz, «ENERCHAIN- DECENTRALLY TRADED DECENTRAL ENERGY, Enerchain, 2019. [Ηλεκτρονικό]. Available: https://enerchain.ponton.de/

[31] «GRID + SELECTS SMARTGRIDCIS FOR BILLING AND CUSTOMER COMMUNICATIONS IN TEXAS», 2018. [Ηλεκτρονικό]. Available: http://www.smartgridcis.com/news/grid-selects-smartgridcis-for-billing-and-customer-communications-in-texas/

[32] «BROOKLYN MICROGRID», 2019. [Ηλεκτρονικά]. Available: https://www.brooklyn.energy/

[33] «About TenneT», TenneT Corporate Review 2018-2019, 2019. [Ηλεκτρονικό]. Availble: https://www.tennet.eu/company/profile/about-tennet/

[34] Themelsle, «Keyllesss Signature Infastracture», Hestia. [Ηλεκτρονικό]. Available: https://www.guardtime-federal.com/ksi/

[35] «Produce One Megawatt Hour. Get One Free SolarCoin.», WORLD ECONOMIC FORUM, 2019. [Ηλεκτρονικό]. Available:https://solarcoin.org/

[36] Dr. Gavin Wood, «ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM VERSION», aeeda84, 2019. [Ηλεκτρονικό]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[37] Felix Lange, «Geth», GitHub. Inc, 2019. [Ηλεκτρονικό]. Available: https://github.com/ethereum/go-ethereum/wiki/geth

[38] Ethereum community, «What is Ethereum», GitHub, 2016. [Ηλεκτρονικό]. Available: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

[39] Zhaoyang DONG, Fengji LUO, Gaoqi LIANG, «Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems», Springer Nature Switzerland AG. Part of Springer Nature, 2019. [Ηλεκτρονικό]. Available:

https://link.springer.com/article/10.1007/s40565-018-0418-0

[40] «Blockchain in Energy Market by Type (Private, Public),

(Platform, Services), End-user (Power, Oil & Gas), Application (Energy Trading, Grid Management, Payment Schemes, Supply Chain Management), and Region - Global Forecast to 2023», 2018 . [Ηλεκτρονικό]. Available: https://www.marketsandmarkets.com/Market-Reports/blockchain-energy-market-186846353.html?gclid=Cj0KCQjw3uboBRDCARIsAO2XcYAfeNRnbVR5akWMMfdJiaDRCM74fs2DJJKY64sLXm2KUVQqSlmxrBQaAuTTEALw_wcB

[41] Alex Leverington, «The RLPx Transport Protocol», GitHub, Inc., 2019. [Ηλεκτρονικό]. Available:

https://github.com/ethereum/devp2p/blob/master/rlpx.md

[42] Vitalik Buterin, «On Stake», Ethereum Foundation, 2019. [Ηλεκτρονικό]. Available: https://blog.ethereum.org/2014/07/05/stake/

[43] Philemon Viennas, **«**Ethereum Consensus and Scalability (Blockchain series — Part III)», A Medium Corporation, 2018. [Ηλεκτρονικό]. Available: https://medium.com/bethereum/ethereum-consensus-and-scalability-blockchain-series-part-iii-4acd78d0eb41

[44] Chris Chinchilla, «A Next-Generation Smart Contract and Decentralized Application Platform», GitHub, Inc., 2019. [Ηλεκτρονικό]. Available:

https://github.com/ethereum/wiki/wiki/White-Paper#ethereum

[45] WantStats Research And Media Pvt.LTD, « Smart Contracts Market Research Report – Global Forecast to 2023», Market Reasearch Future, 2018. [Ηλεκτρονικό]. Available: https://www.marketresearchfuture.com/reports/smart-contracts-market-4588

[46] Massimo Bartoletti and Livio Pompianu, « An empirical analysis of smart contracts: platforms, applications, and design patterns», Universit`a degli Studi di Cagliari, Cagliari, Italy, 2018. [Ηλεκτρονικό]. Available: http://fc17.ifca.ai/wtsc/An%20empirical%20analysis%20of%20smart%20contracts%20-%20platforms,%20applications,%20and%20design%20patterns.pdf

[47] Danny Ryan, « Costs of a Real World Ethereum Contract», 2017. [Ηλετρκονικό]. Available:

https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214

[48] *Wallet Investor, **«** How much is 1 Ethereum in Gas?», 2019. [Ηλεκτρονικό]. Available:*

https://walletinvestor.com/converter/ethereum/gas/1

[49] Raspberry Pi Foundation, «Raspberry Pi 3 Model B +». [Ηλεκτρονικό]. Available: https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf

[50] Dimitrios Kalyvas, Panagiotis Papageorgas, Kyriakos Agavanakis, Ioannis Dogas, Georgios Sarigiannis and Dimitrios Piromalis, «Building the Internet of Energy infrastructure: The Distributed Ledger Technologies approach», Department of Electrical and Electronics Engineering, University of West Attica

and *Department of Industrial Design and Production Engineering, University of West Attica, 2019.*

[51] Lawrence Orsini, Bill Collins, Molly Webb, Cian Montgomery, Ben Conte, Melanie Adamson, Paul Heitmann, Scott Kessler, Matt Brown, «EXERGY BUSINESS WHTEPAPER», LO3 Energy, 2018.

[52] Magda Foti, Dimitrios Greasidis and Manolis Vavalis, «Viability analysis of a decentralized energy market based on blockchain», Department of Electrical and Computer Engineering, University of Thessaly, 2018

[53] Max N. Luke, Consultant, NERA Economic Consulting Stephen J. Lee, Affiliated Industry Expert, NERA Economic Consulting Zdenek Pekarek, PhD, Independent Expert Anna Dimitrova, Advisor, Energy Policy & Innovation, Eurelectric, «Blockchain in Electricity: a Critical Review of Progress to Date», NERA Economic Consulting.

[54] Zhitao Guan, Guanlin Si, Xiaosong Zhang, Longfei Wu, Nadra Guizani, Xiaojiang Du, and Yinglong Ma, «IMMINENT COMMUNICATION TECHNOLOGIES FOR SMART COMMUNITIES - Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities, IEEE Communications Magazine, 2018.

[55] Geunyoung Kim, Junhoo Park, Jaecheol Ryou, «A Study on Utilization of Blockchain for Electricity Trading in Microgrid», Chungnam National University Daejeon, Korea, 2018.

[56] Thomas Lundqvist, Andreas de Blanche, H. Robert H. Andersson, «Thing-to-Thing Electricity Micro Payments Using Blockchain Technology», Department of Engineering Science University West, Trollhättan, Sweden, 2017.

[57] Catarina Naucler, « How can Blockchainchange the energy market», Fortum Sweden.

[58] MORGEN E. PECK & DAVID WAGMAN, «Energy Trading for Fun and Profit - Buy your neighbor's rooftop solar power or sell your own — it'll all be on a blockchain, ORIGIN 2017 Graphing and Analysis, 2017.

[59] Lei Xue, Yunlong Teng, Zhenyuan Zhang, Jian Li, Kunbing Wang, Qi huang, «Blockchain Technology for Electricity Market in Microgrid», School of Energy Science and Engineering University of Electronic Science and Technology of China Chengdu, Sichuan, P. R.China, 2017.

[60] Chenghua Zhang, Jianzhong Wu, Chao Long, Meng Cheng, «Review of Existing Peer-to-Peer Energy Trading Projects», aCardiff University, Cardiff, 2017.

[61] William Favre Slater, «Introduction to Setting Up Ethereum on a Small Raspberry Pi Network», Chicago, Illinois United States of America, 2018.

[62] Esther Mengelkamp , Johannes Gärttner , Kerstin Rock , Scott Kessler , Lawrence Orsini , Christof Weinhardt, «Designing microgrid energy markets A case study: The Brooklyn Microgrid», Karlsruhe Institute of Technology (KIT), Institute for Information Systems and Marketing, Karlsruhe, Germany b L03 Energy, Brooklyn, New York, NY, USA2017.

[63] Kctam, «Two-Node Setup of a Private Ethereum on AWS with Contract Deployment», 2017. [Ηλεκτρονικό]. Available: https://blockgeeks.com/two-node-setup-of-a-private-ethereum/

[64] «What does each genesis.json parameter mean?», 2016. [Ηλεκτρονικό]. Available: https://ethereum.stackexchange.com/questions/2376/what-does-each-genesis-json-parameter-mean

[65] The go-ethereum Authors, «Private-Network», 2019. [Ηλεκτρονικό]: https://geth.ethereum.org/doc/Private-network

[66] Said Eloudrhiri, «Create a private Ethereum blockchain with IoT devices », 2017. [Ηλεκτρονικό]. Available: https://chainskills.com/2017/02/24/create-a-private-ethereum-blockchain-with-iot-devices-16/

[67] Charlotta Edeland, Therese Mork, «Blockchain Technology inthe Energy TransitionAn Exploratory Study on How Electric Utilities Can Approach Blockchain Technology», Stockholm, Sweeden 2018

[68] Wikimedia Foundation, Inc., «Turing Completeness», 2019, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Turing_completeness

[69] STATE OF THE DAPPS, «Explore Decentralized Applications», 2019. [Ηλεκτρονικό]. Available: https://www.stateofthedapps.com/

[70] Sotirios Stampernas, Sokratis Katsikas, Professor, University of Piraeus, Dr. Pankaj Pandey, Research Scientist, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, Gjovik, Norway, «Blockchain technologies and smart contracts in the context of the Internet of Things», University of Piraeus School of Information and Communication Technologies Department of Digital Systems, April 2018.

[71] Georgios N. Papadodimas, «Ανάπτυξη Έξυπνων Συμβολαίων στο Blockchain και εφαρμογή στο IoT», National Technical University of Athens-School of Electrical and Computer Engineering, March 2018

6. Παραρτήματα

6.1 Κώδικας Python

```
import time
import RPi.GPIO as GPIO
import subprocess
import select


print("Preparing to tail log with subprocess..")
f = subprocess.Popen(['tail','-F',"/home/pi/Desktop/eth.log"],\
    stdout=subprocess.PIPE,stderr=subprocess.PIPE) #open and monitor eth.log
file
p = select.poll() #waiting for  i/o completion
p.register(f.stdout)

print("Setting up GPIO...")
GPIO.setmode(GPIO.BCM) #setup of LED function
GPIO.setwarnings(False)
GPIO.setup(17,GPIO.OUT) # Peer 0 White

def onTransmitComplete(): #function to switch on and switch off LED
    GPIO.output(17,GPIO.HIGH)
    time.sleep(2)
    GPIO.output(17,GPIO.LOW)
#Diagnostic LED test
GPIO.output(17,GPIO.HIGH)
time.sleep(1)
GPIO.output(17,GPIO.LOW)


print("Starting async loop...")
try: #starting main process, monitoring what is written in eth.log file
    while True:
        if p.poll(1): #pol starts from value 1, we need the value of place 1 of eth.log
            line = f.stdout.readline() #read the stream from stdout
            try:
                line = line.decode("iso8859-1") #decode the message to unicode

                if not 'Message GossipMessage: tag:EMPTY alive_msg' in line: #skip
system's messages just in case

                    if 'Imported new chain segment ' in line:#triggered-message to swith
on LED
                        onTransmitComplete() #activates LED
            except UnicodeDecodeError:#checking that input is in unicode
```

```
            print("Unicode Error")


            pass

    except KeyboardInterrupt:  #switch to stop the program, when a key is pressed
    ,during process, the program stop running
        pass
        print("Stopping")
        GPIO.output(17,GPIO.LOW)
```
