ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

“Εφαρμογή Αλυσίδας Καταγραφών σε περιβάλλοντα Διαδικτύου των Πραγμάτων”

Μαρτίνης Λουκάς

ΜΜ4160011

ΑΘΗΝΑ, ΟΚΤΩΒΡΙΟΣ 2019

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ευχαριστίες

Αρχικά, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον εποπτεύοντα της παρούσας εργασίας, κ. Βασίλειο Σύρη, αναπληρωτή καθηγητή στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών και διευθυντή του Τομέα Συστημάτων Υπολογιστών και Επικοινωνιών, τόσο για την πολύτιμη καθοδήγησή του παρά τις πολλές ερευνητικές υποχρεώσεις του όσο και για τη δυνατότητα να ασχοληθώ με ένα πολύ επίκαιρο και ενδιαφέρον θέμα, το οποίο ευελπιστώ να αξιοποιήσω στη συνέχεια της ακαδημαϊκής και εργασιακής μου καριέρας.

Τέλος, είμαι απεριόριστα ευγνώμων στην οικογένειά μου και τους στενούς μου φίλους για την υποστήριξη και τη συμπαράσταση που μου παρείχαν κατά τη διάρκεια των σπουδών μου. Ιδιαίτερη μνεία στην αδερφή μου Ξένια, το Δήμο και τον Δημήτρη.

Περίληψη

Το Διαδίκτυο των πραγμάτων ή αλλιώς IoT, μια παγκόσμια υποδομή για την κοινωνία της πληροφορίας ψηφιοποιεί τον κόσμο ενσωματώνοντας τα "έξυπνα αντικείμενα" στο διαδίκτυο και παρέχοντας στους χρήστες πολυάριθμες και ποικίλες εφαρμογές, πχ. έξυπνα προϊόντα, έξυπνη υγεία, έξυπνες μεταφορές κα. Το IoT μπορεί να εκληφθεί ως ένα εκτεταμένο όραμα με τεχνολογικές και κοινωνικές επιπτώσεις.

Τα IoT συστήματα παρουσιάζουν προκλήσεις και ανοικτά ζητήματα όπως ότι τα κεντρικοποιημένα δίκτυα δεν θα μπορούν να υποστηρίξουν τη συνδεσιμότητα δισεκατομμυρίων συσκευών και ότι υπάρχει ανομοιογένεια στις συσκευές που αλληλοεπιδρούν. Οι IoT συσκευές εμφανίζουν αδυναμία εφαρμογής πολύπλοκων συστημάτων ασφάλειας λόγω χαμηλών δυνατοτήτων ενέργειας και υπολογιστικής ισχύς, λειτουργούν χωρίς επίβλεψη και υπόκεινται σε υποκλοπές. Παρουσιάζουν προβλήματα εμπιστευτικότητας των δεδομένων, ιδιωτικότητας και τίθεται ζήτημα εμπιστοσύνης στις αλληλεπιδράσεις μεταξύ οντοτήτων και στο σύστημα. Η κεντρικοποιημένη αρχιτεκτονική απαιτεί τη σύνδεση και την πιστοποίηση των συσκευών μέσω ενός διακομιστή, εντούτοις, ορισμένες εφαρμογές είναι δυναμικές και δεν μπορεί να καλύψει τις μελλοντικές τους ανάγκες ούτε να διαχειριστεί τον όγκο των δεδομένων ενώ λειτουργεί και ως ένα μοναδικό σημείο αστοχίας. Επομένως, γεννάται η ανάγκη μίας αποκεντρωμένης δομής που να καλύπτει επαρκώς και με αποδεκτό κόστος αυτές τις ανάγκες.

Μία δημοφιλής λύση των προαναφερθέντων ζητημάτων αποτελεί η αλυσίδα καταγραφών, αλλιώς blockchain (BC), η τεχνολογία πίσω από τα κρυπτονομίσματα αρχής γενομένης του Bitcoin. Σύντομα όμως εξελίχθηκε και επεκτάθηκε και σε άλλους τομείς και εφαρμογές. Αποτελεί μία βάση δεδομένων που διαμοιράζεται μεταξύ των συμμετεχόντων μερών στο δίκτυο. Οι συναλλαγές ομαδοποιούνται σχηματίζοντας μπλοκ (block) με χρονοσήμανση. Κάθε μπλοκ αναγνωρίζεται από το κρυπτογραφικό του αποτύπωμα (hash) και παραπέμπει στο αντίστοιχο αποτύπωμα του μπλοκ που προηγούνταν, δημιουργώντας έτσι μια αλυσίδα (chain). Περιέχει όλες τις συναλλαγές που έχουν εκτελεστεί σε ένα κατανεμημένο μητρώο καταγραφών (distributed ledger) το οποίο διαμοιράζεται στο δίκτυο.

Επιπλέον δυνατότητες έρχεται να προσθέσει η χρήση έξυπνων συμβολαίων ή αλλιώς smart contracts (SC). Ένα έξυπνο συμβόλαιο είναι κώδικας που τρέχει σε ένα BC και μπορεί να θεωρηθεί ως ένα σύστημα που απελευθερώνει ψηφιακά αγαθά σε όλα ή σε ορισμένα από τα εμπλεκόμενα μέρη μόλις επιτευχθούν αυθαίρετοι προκαθορισμένοι κανόνες. Η βασική ιδέα πίσω από την χρησιμότητά του στο IoT είναι η ανάπτυξη αυτόνομων αντικειμένων ή συσκευών IoT, τα οποία θα είναι σε θέση να μισθώνουν ή να πουλούν τα δεδομένα τους καθώς και να διατηρήσουν την λειτουργικότητά τους πληρώνοντας υπηρεσίες συντήρησης. Ο συνδυασμός των τριών αυτών τεχνολογιών είναι ισχυρός και έχει ως στόχο να μετασχηματίσει πολλούς κλάδους.

Λόγω των οφελών της αποκεντρωμένης αρχιτεκτονικής του και της μη μεταβλητότητας οι ερευνητές και οι αναλυτές ασφαλείας σε όλο τον κόσμο επικεντρώνονται στο BC για την επίλυση των

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

προκλήσεων του IoT. Είναι ζωτικής σημασίας για το μέλλον του IoT, το λειτουργικό του μοντέλο να μεταπηδήσει από την δαπανηρή κεντρική αρχιτεκτονική σε ένα αυτορρυθμιζόμενο και αυτοδιαχειριζόμενο αποκεντρωμένο μοντέλο. Ένας τέτοιος μετασχηματισμός θα προσφέρει μειωμένο κόστος υποδομής, αυτονομία, ασφαλείς λειτουργίες. Το BC με σωστή και μελετημένη εφαρμογή στο IoT περιβάλλον μπορεί μεταξύ άλλων να προσφέρει διαφάνεια και ελεγξιμότητα, ανθεκτικότητα, ταχύτητα, εξοικονόμηση δαπανών, ταυτοποίηση συσκευής και ασφαλή ανάπτυξη κώδικα. Οι εφαρμογές είναι πολλές και μεταξύ άλλων διακρίνονται η ασφαλής λειτουργία έξυπνης πόλης, η αυτόνομη αγορά ενέργειας, η διαφανής διαχείριση εφοδιαστικής αλυσίδας κα.

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η ενοποίηση των τεχνολογιών BC και IoT και σκοπός της η επισκόπηση των οφελών, των εφαρμογών και των μελλοντικών τάσεων που απορρέουν. Ένας από τους βασικούς στόχους είναι ο εντοπισμός, η καταγραφή και ομαδοποίηση των προκλήσεων που προκύπτουν σε πέντε βασικούς άξονες ενώ πραγματοποιείται μία απόπειρα ανάλυσης της απόδοσης σε μετρικές. Αυτό καθώς και η υπόλοιπη ανάλυση θα μπορούσε να βοηθήσει έναν ενδιαφερόμενο να μελετήσει τρόπους εξυγίανσης. Έπεται η ανάδειξη ενδεικτικών μέτρων αντιμετώπισης. Σε επόμενο στάδιο, θα εστιάσουμε στην υλοποίηση ενός SC για τον τομέα της εφοδιαστικής αλυσίδας το οποίο θα αντιμετωπίζει το ζήτημα της εμπιστοσύνης και διαφάνειας κατά την μεταφορά ευπαθών προϊόντων με έμφαση στην αυτόματη επίλυση οικονομικών διενέξεων. Οι συμμετέχοντες πρέπει να εξασφαλίζονται ως προς την αποζημίωσή τους σε περίπτωση αλλοίωσης ενός εμπορεύματος από τον υπαίτιο. Η διαδικασία απαιτεί έλεγχο του ποιος συμμετέχει στη διαδικασία και τί επιτρέπεται να κάνει και διαρκή καταγραφή της θερμοκρασίας μέσω συσκευών IoT.

Η δομή της εργασίας έχει ως εξής. Αρχικά γίνεται μια σύντομη περιγραφή στο IoT, πώς αυτό λειτουργεί, τα βασικά του χαρακτηριστικά, εφαρμογές και προκλήσεις *(1η ενότητα)*. Αναλύουμε το BC ως προς τη δομή των συστατικών μερών της, τη λειτουργία της αλλά και τα επικρατέστερα πρωτόκολλα συναίνεσης *(2η ενότητα)*. Κάνουμε επισκόπηση στο έξυπνο συμβόλαιο σχετικά με τη δομή και τα χαρακτηριστικά του, τον τρόπο λειτουργίας καθώς και τα οφέλη που απορρέουν από αυτό *(3η ενότητα)*. Το κύριο μέρος της εργασίας σχετίζεται με την ενοποίηση των δύο τεχνολογιών, όποτε παραθέτουμε τις βασικές ωφέλειες που αναδύονται από την αξιοποίηση της αλυσίδας καταγραφών στα περιβάλλοντα διαδικτύου των πραγμάτων και παρουσιάζονται οι κλάδοι που είναι αυτό εφικτό αλλά και κάποια σενάρια εφαρμογής που απορρέουν. Γίνεται καταγραφή των προκλήσεων και προτείνονται ορισμένα μέτρα αντιμετώπισης. Έπειτα, εξελίσσεται μία συνοπτική μελέτη δύο σεναρίων που παρουσιάζουν ιδιαίτερο ενδιαφέρον λόγω της καινοτομίας τους και της δυνατότητάς τους να τύχουν ευρείας εφαρμοσιμότητας και σε άλλους τομείς *(4η ενότητα)*. Σε επόμενο βήμα, συζητάμε πιθανές μελλοντικές κατευθύνσεις και τάσεις στον υπό εξέταση κλάδο *(5η ενότητα)*. Ακόμη, παρατίθεται η ανάπτυξη ενός έξυπνου συμβολαίου ώστε να κατανοήσουμε καλύτερα την τεχνολογία πίσω από αυτό, εξετάζονται τα αποτελέσματα και αναφέρονται ενδεχόμενες μελλοντικές προεκτάσεις *(6η ενότητα)*. Εντέλει οδηγούμαστε στα ανάλογα συμπεράσματα και ολοκληρώνουμε *(7η ενότητα)*.

Abstract

The Internet of Things or otherwise IoT, a global information infrastructure for society, is digitizing the world by integrating "smart objects" into the internet; providing users with numerous and diverse applications, e.g. smart products, smart health, smart transport and many more. IoT can be seen as a broad vision with technological and social impact.

IoT systems pose challenges and open issues such as that centralized networks will not be able to support the connectivity of billions of devices and there is heterogeneity in devices that interact with IoT. Smart devices are unable to implement complex security systems due to energy and computational power constraints; they operate unattended and are subject to espionage. They also present problems with data confidentiality, privacy, and the issue of trust in interactions between entities and trust in the system. Their centralized architecture requires all devices to be connected and authenticated through a single server, however, some applications are dynamic and cannot meet their future needs nor manage the volume of data; while it also acts as a single point of failure. Therefore, there is a need for a decentralized structure that adequately and at an acceptable cost covers these needs.

One of the most popular solutions to the above issues is the blockchain (BC), the technology behind Bitcoin cryptocurrency. Soon, however, it expanded to other industries and applications. It is a database that is shared between parties involved in a network. Transactions are grouped into timestamped blocks. Each block is recognized by its cryptographic hash and refers to the corresponding hash of the previous block, thus creating a chain. BC contains all transactions executed in a distributed ledger that it shares among the network participants.

The use of smart contracts comes with additional value. A smart contract is code running on a BC and can be considered as a system that releases digital assets to all or some of the parties involved once arbitrarily predefined conditions are met. The key idea behind its IoT usefulness is the development of autonomous IoT objects or devices that will be able to lease or sell their data as well as maintain their functionality by paying maintenance services. The combination of these three technologies is powerful and aims to transform many industries.

Due to the benefits of its decentralized architecture and immutability, researchers and security analysts around the world are focusing on BC to address the challenges of IoT. It is vital for the future of IoT, its operating model to shift from a costly central architecture to a self-regulated and self-managed decentralized one. Such a transformation will offer reduced infrastructure costs, autonomy, secure operations. Properly designed BC applications in the IoT environment can, inter alia, provide transparency and resilience, robustness, speed, cost savings, device identification and secure code development. There are many applications, including the secure operation of the smart city, autonomous energy market, transparent supply chain management and so on.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

The main focus of this thesis is the integration of BC and IoT technologies and it aims at providing an overview of its benefits, applications and future trends. One of the key objectives is the identification, recording and classification of the challenges that arise in five key groups; while an attempt is made to analyze the performance in metrics, too. This, in addition to the rest of the analysis, could help any interested party study ways of handling them. Following, indicative countermeasures are presented. In the next phase, we focus on the implementation of a supply chain SC addressing the issue of trust and transparency during the transport of sensitive products with emphasis on the automatic resolution of financial disputes. Participants must be compensated in the occurrence of damage to the goods by the responsible party. The process requires control over who is involved in the process and what he/she can do; in addition to maintaining a temperature log through IoT devices.

The present thesis deals with the collaboration of these technologies and is structured as follows. Initially, a brief description is made on the Internet of Things, how it works, what are its key features, applications as well as its challenges *(Section 1)*. We analyze BC in terms of its key components, its main function along with the most often used consensus protocols *(Section 2)*. We review the smart contract regarding its structure and features, how it works along with its benefits *(Section 3)*. The main part of the work relates to the integration of the two technologies, consequently we quote the key benefits that come from adopting BC in IoT environments and we present the industries that this integration is feasible as well as some emerging application scenarios. Challenges are identified and some countermeasures are proposed. Afterwards, there is a brief review of two scenarios that are of particular interest because of their innovation and their potential to be widely applied in other areas *(Section 4)*. In the next step, we discuss possible future directions and trends in the sector under consideration *(Section 5)*. Furthermore, we continue with the development of a smart contract so that we can better understand the technology behind it. We discuss the outcome along with possible future work *(Section 6)*. Finally, we complete our study with conclusions *(Section 7)*.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Περιεχόμενα

Ευχαριστίες 3
Περίληψη 4
Abstract 6
Περιεχόμενα 8
Κατάλογος Εικόνων 12
Κατάλογος Πινάκων 12
Ενότητα 1: Διαδίκτυο των Πραγμάτων 13
1.1 Ορισμός του Διαδικτύου των Πραγμάτων 13
1.2 Βασικά χαρακτηριστικά 13
1.3 Εφαρμογές 14
1.4 Προκλήσεις και ανοικτά ζητήματα 15
1.5 Ασφάλεια 15
1.6 Ιδιωτικότητα 16
1.7 Εμπιστοσύνη 17
Ενότητα 2: Αλυσίδα Καταγραφών 18
2.1 Ορισμός Αλυσίδας Καταγραφών 18
2.2 Δομή Μπλοκ 19
2.3 Λειτουργία Αλυσίδας Καταγραφών 20
2.4 Διακλαδώσεις στο δίκτυο 21
2.4.1 Ελαστική και σταθερή διακλάδωση 21
2.5 Ταξινόμηση Αλυσίδων Καταγραφών 22
2.6 Συναίνεση στο δίκτυο 23
2.6.1 Ανάγκη μίας κοινής καθολικής εικόνας 23
2.6.2 Το πρόβλημα των βυζαντινών στρατηγών 23
2.6.3 Πρωτόκολλα συναίνεσης 24
2.6.3.1 Απόδειξη-του-Έργου (Proof-of-Work) 24
2.6.3.2 Απόδειξη-του-Μεριδίου (Proof-of-Stake) 25
2.6.3.3 Κατ' Εκπροσώπευση Απόδειξη-του-Μεριδίου (Delegated Proof-of-Stake) 26
2.6.3.4 Απόδειξη του Χρόνου που παρήλθε (Proof-of-Elapsed-Time) 27
2.6.3.5 Απόδειξη-της-Δραστηριότητας (Proof-of-Activity) 28
2.6.3.6 Πρακτική Ανοχής Βυζαντινού Σφάλματος (Practical Byzantine Fault Tolerance) 28
2.6.3.7 Ripple 30
2.6.3.8 Tendermint 31
Ενότητα 3: Έξυπνα Συμβόλαια 32

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.1 Ορισμός Έξυπνου Συμβολαίου 32
3.2 Δομή Έξυπνου Συμβολαίου 33
3.3 Λειτουργία Έξυπνου Συμβολαίου 33
3.4 Βασικά Χαρακτηριστικά και Οφέλη του Έξυπνου Συμβολαίου 34
3.5 Αποκεντρωμένος Αυτόνομος Οργανισμός 34
3.6 Διπλή ολοκλήρωση (dual integration) 35
Ενότητα 4: Αξιοποίηση Αλυσίδας Καταγραφών στο Διαδίκτυο των Πραγμάτων 36
4.1 Οφέλη της ενσωμάτωσης 36
4.1.1 Αποκέντρωση και Αποδιαμεσολάβηση 37
4.1.2 Διαφάνεια και Ελεγξιμότητα 37
4.1.3 Ανθεκτικότητα 37
4.1.4 Ασφάλεια 38
4.1.5 Ταχύτητα 39
4.1.6 Εξοικονόμηση δαπανών 40
4.1.7 Μη μεταβλητότητα 40
4.1.8 Αυτονομία 41
4.1.9 Ταυτοποίηση Συσκευής 41
4.1.10 Ασφαλής ανάπτυξη κώδικα 42
4.2 Εφαρμογές 42
4.2.1 Αυτόνομη Αποκεντρωμένη Διομότιμη Τηλεμετρία 42
4.2.2 Αυτοδιαχειριζόμενα Δίκτυα Μεταφορών 43
4.2.3 Ασφαλής Λειτουργία Έξυπνης Πόλης 44
4.2.4 Ασφαλής Ενημέρωση Υλικολογισμικού Έξυπνων Συσκευών 45
4.2.5 Αποδοτική Διαχείριση Βιομηχανικής Παραγωγής 46
4.2.6 Ασφαλής Λειτουργία Έξυπνου Σπιτιού 47
4.2.7 Αυτόνομη Αγορά Ενέργειας 48
4.2.8 Διαφανής Διαχείριση της Εφοδιαστικής Αλυσίδας 49
4.3 Προκλήσεις της ενσωμάτωσης 50
4.3.1 Απόδοση 51
4.3.1.1 Ενεργειακή κατανάλωση 51
4.3.1.2 Επεξεργαστική Ισχύς και χρόνος επεξεργασίας 52
4.3.1.3 Χαμηλή διεκπεραιωτικότητα συναλλαγών 52
4.3.1.4 Υψηλή χρονική καθυστέρηση 53
4.3.1.5 Χαμηλή χωρητικότητα αποθήκευσης 53
4.3.1.6 Όρια εύρους ζώνης 54
4.3.1.7 Πλεονασμός στην εκτέλεση 54
4.3.1.8 Δυνατότητα κλιμάκωσης / Επεκτασιμότητα 55

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.3.2 Ασφάλεια 56
4.3.3 Ιδιωτικότητα 59
4.3.4 Νομοκανονιστικό Πλαίσιο 60
4.3.4.1 Νομική Επιβολή Ευφυών Συμβολαίων 61
4.3.4.2 Συμμόρφωση με το ΓΚΠΔ 61
4.3.4.3 Απαρχαιωμένη νομοθεσία 61
4.3.4.4 Αδυναμία αναίρεσης συναλλαγής και ανάκτησης χρημάτων 61
4.3.5 Υιοθέτηση της τεχνολογίας 62
4.3.5.1 Ενημέρωση κοινού και έλλειψη δεξιοτήτων 62
4.3.5.2 Ζητήματα διακυβέρνησης 62
4.3.5.3 Αποτίμηση της αξίας των εξομοιωμένων αγαθών 63
4.4 Μέτρα Αντιμετώπισης Προκλήσεων 63
4.5 Η Περίπτωση του Έξυπνου Σπιτιού 67
4.5.1 Αρχιτεκτονική Δομή 67
4.5.1.1 Αποθηκευτικό νέφος 67
4.5.1.2 Δίκτυο επικάλυψης 68
4.5.1.3 Έξυπνο σπίτι (τοπικό δίκτυο) 69
4.5.2 Βασικά συστατικά έξυπνου σπιτιού 69
4.5.2.1 Επιτρεπτές συναλλαγές 69
4.5.2.2 Τοπικό BC 69
4.5.2.3 Εξορύκτης Έξυπνου Σπιτιού (SHM) 70
4.5.2.4 Τοπική αποθήκευση 70
4.5.3 Αρχική διαμόρφωση στο έξυπνο σπίτι 71
4.5.3.1 Διαδικασία ένταξης νέας συσκευής 71
4.5.3.2 Διαμόρφωση κεφαλίδας πολιτικής 71
4.5.4 Διαχείριση των συναλλαγών 71
4.5.5 Κοινή επικάλυψη (shared overlay) 73
4.5.6 Κατανεμημένη εμπιστοσύνη / αξιοπιστία 73
4.5.7 Ανάλυση της ασφάλειας 74
4.5.8 Ανάλυση της απόδοσης 74
4.5.9 Συμπεράσματα 75
4.6 Η Περίπτωση της Αγοράς Ενέργειας 75
4.6.1 Όραμα -Σκοπός 76
4.6.2 Εργαλεία ανάπτυξης λογισμικού 76
4.6.2.1 EW Origin 76
4.6.2.2 EW Link 76
4.6.2.3 EW D3A 76

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.6.3 Διακυβέρνηση 77
4.6.4 Υποστηρικτικές Τεχνολογίες 77
4.6.4.1 Proof-of-Authority 77
4.6.4.2 Light Client 79
4.6.4.3 Εξουσιοδότηση (permissioning) 79
4.6.4.4 Ιδιωτικές συναλλαγές 79
4.6.5 Επόμενα βήματα 80
Ενότητα 5: Τάσεις 81
5.1 Μεγάλα Δεδομένα 81
5.2 Χρήση Υπολογιστικής Ομίχλης 82
5.3 Εξέταση των διαφορετικών Αλυσίδων Καταγραφών 83
5.4 Τεχνητή Νοημοσύνη 83
5.5 Πρωτόκολλο Συναίνεσης προσαρμοσμένο στο Διαδίκτυο των Πραγμάτων 84
5.6 Ανάπτυξη του Διαδικτύου των Στρατιωτικών Αντικειμένων 84
5.7 Ενσωμάτωση πρωτοκόλλων επικοινωνίας με αλυσίδα καταγραφών 84
Ενότητα 6: Υλοποίηση ενός έξυπνου συμβολαίου για την εφοδιαστική αλυσίδα 85
6.1 Κίνητρο και Στόχος Υλοποίησης 85
6.2 Συναφείς έρευνες και εγχειρήματα 86
6.3 Περιγραφή της εφαρμογής 87
6.4 Τεχνολογία Ethereum 89
6.4.1 Βασικές Έννοιες 90
6.4.2 Γλώσσα Solidity 91
6.4.3 Ολοκληρωμένο περιβάλλον ανάπτυξης Remix 91
6.5 Επόμενα Βήματα και Συμπεράσματα Υλοποίησης 92
6.5.1 Βελτίωση απόδοσης 92
6.5.2 Αξιολόγηση διαφορετικών IoT τεχνολογιών και συσκευών 92
6.5.3 Επέκταση λειτουργικότητας 92
6.5.4 Ένταξη εξωτερικών φορέων 93
Ενότητα 7: Συμπεράσματα 94
Ενότητα 8: Λεξικό Όρων 96
Ενότητα 9: Βιβλιογραφία 100
Ενότητα 10: Παράρτημα 105
10.1 Κώδικας υλοποίησης σε γλώσσα solidity 105
10.2 Εγχειρίδιο Χρήσης 113

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Κατάλογος Εικόνων

Εφαρμογές IoT. Αναπαραγωγή από Jesus et al. (2018) 14

Δομή Blockchain. Αναπαραγωγή από Zheng et al. (2018) 18

Δομή μπλοκ. Αναπαραγωγή από Jesus et al. (2018) 20

Σενάριο διακλάδωσης, όπου η μακρύτερη υπολογιστικά αλυσίδα επιλέγεται ως αυθεντική. Αναπαραγωγή από Zheng et al. (2018) 21

Υπολογισμός απόδειξης-του-έργου βάση ορίου. Αναπαραγωγή από Panarello et al. (2018) 24

Μία γενική υλοποίηση της συναίνεσης DPoS 27

Ομαλή λειτουργία PBFT με ελαττωματικό κόμβο. Αναπαραγωγή από Castro και Liskov (1999) 29

Το σύστημα ενός Έξυπνου Συμβολαίου. Αναπαραγωγή από Alharby και Moorsel (2017) 33

Οφέλη ενσωμάτωσης των δύο τεχνολογιών 36

Προκλήσεις της ενσωμάτωσης των δύο τεχνολογιών 50

Επισκόπηση προτεινόμενης αρχιτεκτονικής. Αναπαραγωγή από Dorri et al. (2017) 68

Επισκόπηση Έξυπνου Σπιτιού. Αναπαραγωγή από Dorri et al. (2017) 71

Ο μηχανισμός συναίνεσης του Proof-of-Authority (PoA) που χρησιμοποιείται από το EWF. Αναπαραγωγή από Energy Web Foundation (2019) 78

Ενσωμάτωση Αλυσίδας Καταγραφών και Διαδικτύου των Πραγμάτων με χρήση Υπολογιστικής Νέφους. Αναπαραγωγή από Makhdoom et al. (2019) 82

Διαφάνεια της εφοδιαστικής αλυσίδας με τη χρήση Blockchain, Smart Contracts και IoT 88

Σενάριο ομαλής μεταφοράς προϊόντος από τον παραγωγό στον χονδρέμπορο 88

Κατάλογος Πινάκων

Πίνακας δομής κεφαλίδας πολιτικής. Βασισμένο στο Dorri et al. (2017) 70

Πίνακας δομής συναλλαγών. Βασισμένο στο Dorri et al. (2017) 70

Πίνακας βασικών προσαρμογών Ethereum στο Web Energy Chain 77

Ενότητα 1: Διαδίκτυο των Πραγμάτων

Ο όρος "Internet of Things" (Διαδίκτυο των πραγμάτων) χρησιμοποιήθηκε πρώτη φορά από τον Kevin Ashton ως τίτλος μιας παρουσίασης που έκανε στην Procter & Gamble (P&G) το 1999 (Journal, 2009). Ο Kevin θέλοντας να αντιμετωπίσει το πρόβλημα παρακολούθησης και καταγραφής προϊόντων της εφοδιαστικής αλυσίδας της επιχείρησης, σύνδεσε την τεχνολογία RFID με τα προϊόντα και στη συνέχεια την παρακολούθηση των προϊόντων μέσω του Διαδικτύου. Από τότε μέχρι σήμερα το IoT εξελίχθηκε και επεκτάθηκε σε περισσότερους τομείς με πολύ περισσότερα αντικείμενα να ανήκουν σε αυτό. Τα αντικείμενα αυτά είναι εξοπλισμένα με ενσωματωμένους αισθητήρες, ενεργοποιητές, επεξεργαστές και πομποδέκτες. Μερικές συσκευές που μπορούν να συνδεθούν σε ένα IoT δίκτυο είναι τα "έξυπνα" κινητά, wearables συσκευές όπως ρολόγια, ηλεκτρικές συσκευές όπως ψυγείο, πλυντήριο, ηλεκτρονικές συσκευές όπως συστήματα συναγερμού, κάμερες, ψηφιακές συσκευές υγείας κ.α. (Sethi and Sarangi, 2017).

1.1 Ορισμός του Διαδικτύου των Πραγμάτων

Επί του παρόντος, δεν υπάρχει μόνο ένας ορισμός του IoT. Αρκετοί συγγραφείς και ιδρύματα συνέβαλαν στην οικοδόμηση του οράματός του. Με βάση την I.T.U.[1], (2012) το Διαδίκτυο των Πραγμάτων ορίζεται ως μια παγκόσμια υποδομή για την κοινωνία της πληροφορίας, επιτρέποντας την παροχή προηγμένων υπηρεσιών μέσω της διασύνδεσης (φυσικών και εικονικών) αντικειμένων με βάση τις υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών (ICT). Το IoT μπορεί να εκληφθεί ως ένα εκτεταμένο όραμα με τεχνολογικές και κοινωνικές επιπτώσεις.

1.2 Βασικά χαρακτηριστικά

Τα θεμελιώδη χαρακτηριστικά του IoT είναι τα εξής:

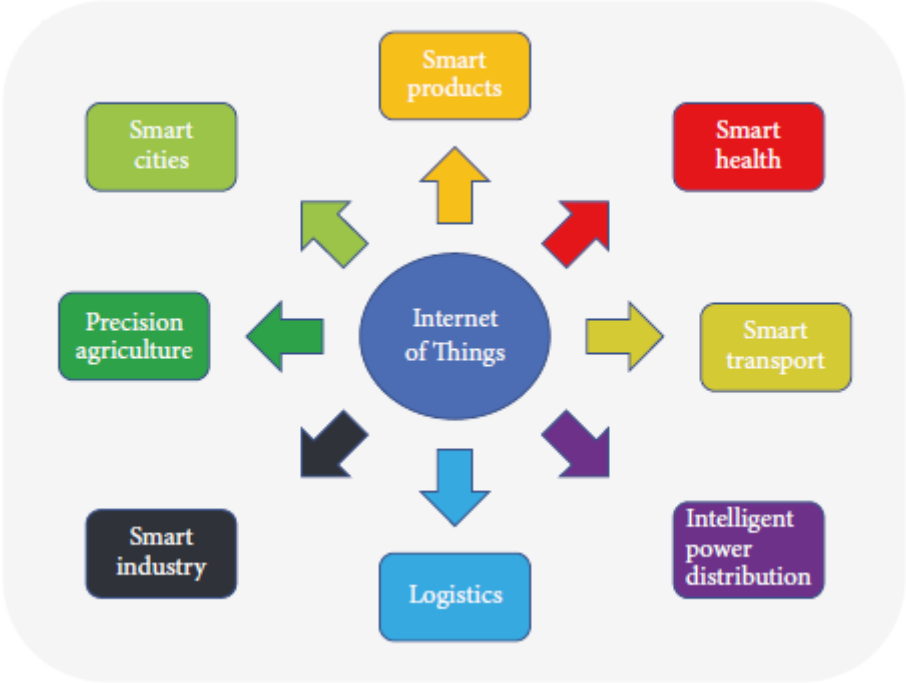
1. *Διασυνδεσιμότητα*: Με βάση το IoT καθετί μπορεί να είναι διασυνδεδεμένο με την υποδομή παγκόσμιας πληροφόρησης και επικοινωνίας.
2. *Υπηρεσίες που σχετίζονται με τα πράγματα*: Το IoT είναι ικανό να παρέχει υπηρεσίες μεταξύ αντικείμενων που έχουν περιορισμένους πόρους και προκειμένου να το πετύχει αυτό τόσο οι τεχνολογίες στον φυσικό όσο και στον κόσμο της πληροφορίας θα αλλάξουν.
3. *Ετερογένεια*: Οι συσκευές στο IoT είναι ανομοιογενείς αφού είναι φτιαγμένες από διαφορετικά υλισμικά και ανήκουν σε διαφορετικές πλατφόρμες και δίκτυα.
4. *Δυναμικές αλλαγές*: Η κατάσταση των συσκευών αλλάζει δυναμικά (από αδρανής σε ενεργή, από συνδεδεμένη σε εκτός σύνδεσης) όπως επίσης και το πλαίσιο των συσκευών, συμπεριλαμβανομένης της θέσης και της ταχύτητας.

[1] Διεθνής Ένωση Τηλεπικοινωνιών.

5. *Τεράστια κλίμακα*: Το IoT καλείται να διαχειριστεί έναν μεγάλο αριθμό συσκευών και επικοινωνιών, σε υψηλή κλίμακα σε σύγκριση με το διαδίκτυο. Ο όγκος της επικοινωνίας μεταξύ συσκευών θα αυξηθεί πολύ σε σύγκριση με αυτό που παράγει ο άνθρωπος. Ακόμη πιο κρίσιμη θα είναι η διαχείριση των παραγόμενων δεδομένων και η αφομοίωσή τους από τις εφαρμογές.

1.3 Εφαρμογές

Το IoT καλύπτει την επεξεργασία των δεδομένων και την επικοινωνία μεταξύ συσκευών διαφορετικών πλατφορμών και δυνατοτήτων χωρίς την ανθρώπινη παρέμβαση. Οι εφαρμογές του IoT διεισδύουν στην καθημερινότητά , στον επιχειρησιακό τομέα και την κοινωνία, μετατρέποντας τον κόσμο πιο "έξυπνο". Για το IoT υπάρχουν πολυάριθμες και ποικίλες εφαρμογές. Στη συνέχεια αναφέρουμε επιγραμματικά τις βασικότερες με κάποια παραδείγματα (Jesus et al., 2018):



Εφαρμογές IoT. Αναπαραγωγή από Jesus et al. (2018)

Α) *Έξυπνα προϊόντα*: smartphones, το έξυπνο σπίτι, το έξυπνο αυτοκίνητο, η έξυπνη τηλεόραση, φορητές συσκευές. Β) *Έξυπνη υγεία*: απομακρυσμένη παρακολούθηση αντικειμένων και ανθρώπων, πρόληψη των προβλημάτων υγείας σε πραγματικό χρόνο. Γ) *Έξυπνες μεταφορές*: κοινοποίηση των συνθηκών κυκλοφορίας, ευφυής έλεγχος των διαδρομών, απομακρυσμένη παρακολούθηση του οχήματος, συντονισμός κίνησης. Δ) *Ευφυής κατανομή* ισχύος: παρακολούθηση των ενεργειακών εγκαταστάσεων, έξυπνοι υποσταθμοί, διανομή ενέργειας και απομακρυσμένες μετρήσεις οικιακών μετρητών ηλεκτρικής ενέργειας. Ε) *Έξυπνη εφοδιαστική αλυσίδα*: ιχνηλασιμότητα, διανομή και διαχείριση αποθεμάτων. ΣΤ) *Έξυπνη βιομηχανία*: εξοικονόμηση ενέργειας, έλεγχος ρύπανσης, ασφάλεια κατασκευής, παρακολούθηση κύκλου ζωής των προϊόντων, παρακολούθηση των αγαθών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

στην αλυσίδα εφοδιασμού. Ζ) *Έξυπνη γεωργία*: διαχείριση ποιότητας, παρακολούθηση του περιβάλλοντος για την παραγωγή αλλά και την καλλιέργεια, διαχείριση της παραγωγικής διαδικασίας. Η) *Έξυπνες πόλεις*: δομική παρακολούθηση, έξυπνος φωτισμός δρόμου, συστήματα παρακολούθησης, πυρασφάλειας, έξυπνοι δρόμοι με προειδοποιήσεις, διαθεσιμότητα χώρων στάθμευσης κα.

1.4 Προκλήσεις και ανοικτά ζητήματα

Το IoT παρουσιάζει μια τεράστια ευκαιρία ανάπτυξης για όλους τους κλάδους. Πολλές επιχειρήσεις εστιάζουν στο IoT και τη συνδεσιμότητα των προϊόντων και υπηρεσιών τους. Για να μπορέσει όμως η βιομηχανία IoT να αναπτυχθεί υπάρχουν τρεις κατηγορίες προκλήσεων που πρέπει να αντιμετωπιστούν: τεχνολογικές, επιχειρησιακές και κοινωνικές (Iot.ieee.org, 2017).

Αρχικά, οι βασικές τεχνολογικές προκλήσεις αναφέρονται σε ζητήματα ασφάλειας συστημάτων, θέμα στο οποίο θα αναφερθούμε αργότερα. Η *συνδεσιμότητα* ενός πολύ μεγάλου αριθμού συσκευών, θα αποτελέσει μία από τις μεγαλύτερες προκλήσεις του μέλλοντος του Ίντερνετ και θα αψηφήσει την ίδια τη δομή των σημερινών μοντέλων επικοινωνίας και τεχνολογιών. Τα κεντρικοποιημένα δίκτυα δεν θα μπορούν να υποστηρίξουν τη συνδεσιμότητα δισεκατομμυρίων συσκευών. Η *έλλειψη κοινών προτύπων* αποτελεί μία ακόμα τροχοπέδη. Υπάρχει μεγάλη ανομοιογένεια στις συσκευές που αλληλοεπιδρούν στο IoT κάτι το οποίο καθιστά επιτακτική την υιοθέτηση νέων πρωτοκόλλων επικοινωνίας, δικτύου κλπ.

Άλλα ανοικτά ζητήματα τα οποία χρήζουν επίλυσης καθώς η τεχνολογία του IoT θα επεκτείνεται είναι: θέματα αρχιτεκτονικής σχεδίασης, ενεργειακά αποδοτική ανίχνευση, υποστήριξη δικτύων με διαφορετικές QoS απαιτήσεις, αποτελεσματική διαχείριση και προγραμματισμός πόρων του Cloud, το πρόβλημα της επαρκούς διευθυνσιοδότησης, η δικτύωση σε επίπεδο μεταφοράς, lightweight λύσεις ασφάλειας και αποτελεσματικές λύσεις για μεγάλα ετερογενή δεδομένα (Atzori, Iera and Morabito, 2010; Gubbi et al., 2013; Jing et al., 2014).

1.5 Ασφάλεια

Το IoT είναι εξαιρετικά ευάλωτο σε επιθέσεις για διάφορους λόγους. Τον περισσότερο χρόνο οι συσκευές λειτουργούν χωρίς επίβλεψη και έτσι είναι εύκολο κανείς να τους επιτεθεί. Έπειτα, οι περισσότερες επικοινωνίες είναι ασύρματες, γεγονός που καθιστά την υποκλοπή εξαιρετικά απλή. Τέλος, οι περισσότερες συσκευές χαρακτηρίζονται από χαμηλές δυνατότητες σε ενέργεια όσο και υπολογιστική ισχύ και άρα δεν μπορούν να εφαρμόσουν πολύπλοκα συστήματα ασφάλειας. Η ασφάλεια θα πρέπει να προστατεύει τις υπηρεσίες, το υλισμικό, το λογισμικό, τις πληροφορίες και τα δεδομένα τόσο στη μετάβαση όσο και στην αποθήκευση. Τα βασικά προβλήματα που σχετίζονται με την ασφάλεια αφορούν την αυθεντικοποίηση, την εμπιστευτικότητα και ακεραιότητα των δεδομένων.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ο *έλεγχος αυθεντικοποίησης* είναι δύσκολος, καθώς απαιτεί κατάλληλες υποδομές και διακομιστές που επιτυγχάνουν το στόχο τους μέσω της ανταλλαγής κατάλληλων μηνυμάτων με άλλους κόμβους. Στο IoT τέτοιες προσεγγίσεις δεν είναι εφικτές δεδομένου ότι τα αντικείμενα που συνδέονται δεν μπορούν να ανταλλάξουν πολλά μηνύματα με τους διακομιστές. Επιπλέον, τα αντικείμενα αυτά έχουν περιορισμένους πόρους σε σύγκριση με τις τρέχουσες συσκευές επικοινωνίας και τους υπολογιστές.

Η *εμπιστευτικότητα* των δεδομένων αποτελεί θεμελιώδες πρόβλημα. Μία συσκευή IoT πρέπει να είναι σε θέση να επαληθεύει ότι μία οντότητα έχει εξουσιοδότηση πρόσβασης στην υπηρεσία. Αυτό απαιτεί μηχανισμό ελέγχου πρόσβασης και εξουσιοδότησης και μηχανισμό ελέγχου αυθεντικοποίησης και διαχείρισης ταυτότητας. Η εξουσιοδότηση βοηθάει να προσδιοριστεί αν κατά την ταυτοποίηση το άτομο ή η συσκευή επιτρέπεται να λάβει μια υπηρεσία. Ο έλεγχος πρόσβασης συνεπάγεται τη διαχείριση πρόσβασης στους πόρους χρησιμοποιώντας ένα ευρύ φάσμα κριτηρίων. Η εξουσιοδότηση και ο έλεγχος πρόσβασης είναι σημαντικοί για τη δημιουργία ασφαλούς σύνδεσης μεταξύ συσκευών και υπηρεσιών. Εξίσου σημαντική είναι η αυθεντικοποίηση και η διαχείριση της ταυτότητας. Πολλοί χρήστες, αντικείμενα και συσκευές πρέπει να πιστοποιούν ο ένας τον άλλο μέσω αξιόπιστων υπηρεσιών (Abomhara and Køien, 2015).

Η *ακεραιότητα* εξασφαλίζεται συνήθως με την προστασία δεδομένων με κωδικούς πρόσβασης. Ωστόσο, τα μήκη του κωδικού πρόσβασης που υποστηρίζονται από τεχνολογίες IoT είναι στις περισσότερες περιπτώσεις πολύ μικρά για να παρέχουν ισχυρά επίπεδα προστασίας. Οι τυπικοί κρυπτογραφικοί αλγόριθμοι δαπανούν μεγάλους πόρους όσον αφορά την ενέργεια και το εύρος ζώνης.

1.6 Ιδιωτικότητα

Η ιδιωτικότητα είναι ένα σημαντικό ζήτημα στο IoT περιβάλλον. Τα αντικείμενα του IoT, όπως τα αυτοκίνητα, τα παιχνίδια και οι οικιακές συσκευές, μπορούν να χρησιμοποιηθούν για *παράνομη παρακολούθηση*. Οι ανησυχίες των πολιτών για την προστασία της ιδιωτικής ζωής τους είναι δικαιολογημένες. Στην πραγματικότητα, ο τρόπος με τον οποίο θα επιτευχθεί η συλλογή, η εξόρυξη, η τροφοδοσία και η διάδοση δεδομένων στο διαδίκτυο θα είναι τελείως διαφορετικός από αυτούς που γνωρίζουμε έως τώρα. Πολλές ιδιωτικές πληροφορίες σχετικά με ένα άτομο μπορούν να συλλεχθούν εν αγνοία του και να διατηρηθούν επ' αόριστον. Κατά συνέπεια, η ιδιωτική ζωή θα πρέπει να προστατεύεται εξασφαλίζοντας ότι τα άτομα μπορούν να *ελέγχουν ποιά από τα προσωπικά τους δεδομένα* συλλέγονται, ποιός τα συλλέγει και πότε συμβαίνει αυτό. Επιπλέον, τα δεδομένα αυτά πρέπει να χρησιμοποιούνται μόνο για την υποστήριξη των εξουσιοδοτημένων υπηρεσιών από εξουσιοδοτημένους φορείς και τέλος, τα παραπάνω δεδομένα θα πρέπει να αποθηκεύονται μόνο για το διάστημα που είναι απολύτως αναγκαία και μετά να διαγράφονται (*digital forgetting*).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

1.7 Εμπιστοσύνη

Η εμπιστοσύνη διαδραματίζει σημαντικό ρόλο στην καθιέρωση ασφαλούς επικοινωνίας, όταν ορισμένα αντικείμενα επικοινωνούν σε ένα αβέβαιο περιβάλλον IoT. Δύο διαστάσεις εμπιστοσύνης θα πρέπει να εξετάζονται στο IoT: η *εμπιστοσύνη στις αλληλεπιδράσεις μεταξύ οντοτήτων* και η *εμπιστοσύνη στο σύστημα* από την οπτική γωνία των χρηστών. Η αξιοπιστία μιας συσκευής IoT εξαρτάται από τα συστατικά της στοιχεία, το υλισμικό, το λογισμικό και την πηγή ενέργειας. Προκειμένου να αποκτηθεί εμπιστοσύνη χρήστη/υπηρεσιών, θα πρέπει να υπάρχει ένας αποτελεσματικός μηχανισμός καθορισμού της σε ένα δυναμικό και συνεργατικό περιβάλλον IoT.

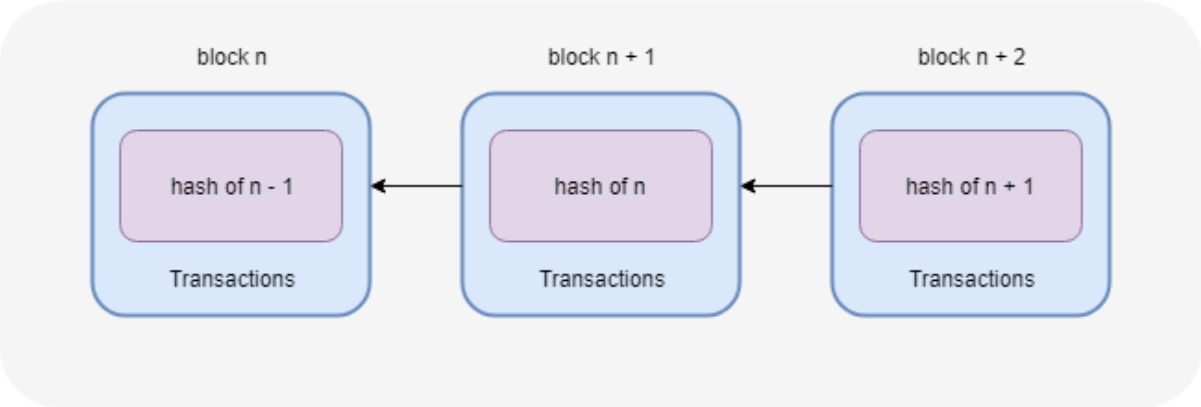
ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 2: Αλυσίδα Καταγραφών

Το ζήτημα της εμπιστοσύνης στα πληροφοριακά συστήματα είναι εξαιρετικά περίπλοκο όταν δεν παρέχονται μηχανισμοί επαλήθευσης ή ελέγχου πολλώ δε μάλλον όταν έχουν να αντιμετωπίσουν ευαίσθητες πληροφορίες. Μέσα σε αυτό το κλίμα, ο Satoshi Nakamoto (2008) έφερε στο προσκήνιο ένα άρθρο όπου παρουσίασε δύο ριζοσπαστικές έννοιες με πολύ μεγάλο αντίκτυπο. Το πρώτο είναι το Bitcoin, ένα εικονικό κρυπτονόμισμα που διατηρεί την αξία του χωρίς τη στήριξη από οποιαδήποτε κεντρική αρχή ή οικονομική οντότητα. Αντίθετα, το νόμισμα κρατείται συλλογικά και με ασφάλεια από ένα αποκεντρωμένο διομότιμο δίκτυο ελεγχόμενο και επαληθεύσιμο. Η δεύτερη έννοια, της οποίας η δημοτικότητα αυξήθηκε ακόμα πιο ραγδαία είναι το Blockchain (Reyna et al., 2018).

Η ιδέα του BC αρχίζει να καθιστά σαφές ότι υπερβαίνει την τεχνολογική καινοτομία., μπορεί να αλλάξει τον τρόπο πραγματοποίησης όλων των τύπων συναλλαγών και να επιτρέψει ένα ευρύ φάσμα δυνατοτήτων σε ποικίλους τομείς. Μπορούμε να διακρίνουμε την εξέλιξή του σε τρία στάδια: Blockchain 1.0, 2.0 και 3.0. Το BC 1.0 είναι η εμπορική χρήση με μεταφορά χρημάτων, εμβάσματα και ψηφιακά συστήματα πληρωμών. Στο BC 2.0 ξεκινά η χρήση του από χρηματοοικονομικές εφαρμογές που το χρησιμοποιούν πολύ πιο εκτεταμένα από τις απλές χρηματικές συναλλαγές, όπως μετοχές, ομόλογα, δάνεια, υποθήκες και έξυπνες συμβάσεις. Το Blockchain 3.0 αναφέρεται στη χρήση του σε εφαρμογές πέρα από το νόμισμα, την οικονομία και τις αγορές, ιδιαίτερα στους τομείς της διακυβέρνησης, της υγείας και της επιστήμης (Jesus et al., 2018).

2.1 Ορισμός Αλυσίδας Καταγραφών



Δομή Blockchain. Αναπαραγωγή από Zheng et al. (2018)

Η αλυσίδα καταγραφών ή αλλιώς blockchain (BC) είναι μία βάση δεδομένων που διαμοιράζεται μεταξύ των συμμετεχόντων μερών στο δίκτυο. Οι συναλλαγές ομαδοποιούνται σχηματίζοντας μπλοκ (*block*) με χρονοσήμανση. Κάθε μπλοκ αναγνωρίζεται από το κρυπτογραφικό του αποτύπωμα[2] (*hash*) και

[2] Μία τιμή κρυπτογραφικού αλγόριθμου κατακερματισμού - *hash*.

παραπέμπει στο αντίστοιχο αποτύπωμα του μπλοκ που προηγούνταν, δημιουργώντας έτσι μια αλυσίδα (*chain*). Το BC περιέχει όλες τις συναλλαγές που έχουν εκτελεστεί σε ένα κατανεμημένο μητρώο καταγραφών (*distributed ledger*) το οποίο διαμοιράζει στους συμμετέχοντες στο δίκτυο. Κάθε συναλλαγή αποθηκεύεται στο κατανεμημένο μητρώο και πρέπει να επαληθεύεται με τη συγκατάθεση της πλειοψηφίας των συμμετεχόντων στο δίκτυο. Όλες οι συναλλαγές που έχουν γίνει ποτέ περιέχονται στο BC και κάθε κόμβος που έχει πρόσβαση σε αυτήν την ταξινομημένη, διασυνδεδεμένη λίστα καταγραφών μπορεί να το διαβάσει και να καταλάβει ποια είναι η κατάσταση των δεδομένων που ανταλλάσσονται στο δίκτυο.

2.2 Δομή Μπλοκ

Τα δομικά συστατικά ενός μπλοκ είναι δύο, η *κεφαλίδα* και οι *συναλλαγές* οι οποίες αποτελούν τα δεδομένα που αποθηκεύονται. Μέσα στην κεφαλίδα υπάρχουν τα κάτωθι πεδία:

(i) *Ύψος*: η διαφορά μεταξύ του αριθμού του τελευταίου και του πρώτου μπλοκ ονομάζεται *ύψος*. Αυξάνεται σειριακά. Δεν χρησιμοποιείται για αναγνώριση ενός μπλοκ, καθώς μπορεί να υπάρχουν στιγμιαία δύο ή περισσότερα μπλοκ με το ίδιο ύψος (περίπτωση μιας *διακλάδωσης* στην αλυσίδα).

(ii) *Hash κεφαλίδας*: Είναι το παραγόμενο μίας κρυπτογραφικής συνάρτησης και είναι το κύριο αναγνωριστικό του μπλοκ. Δεν αποτελεί μέρος της δομής δεδομένων του μπλοκ και επίσης δεν αποστέλλεται μέσω του δικτύου. Κάθε πλήρης κόμβος το υπολογίζει με την παραλαβή ενός νέου μπλοκ. Μετά από αυτό, το αποθηκεύουν σε ξεχωριστή βάση δεδομένων, ως μεταδεδομένο του μπλοκ.

(iii) *Hash του προηγούμενου μπλοκ*: Αυτό το πεδίο περιλαμβάνεται για να επιτρέψει τη σύνδεση ενός μπλοκ με το προηγούμενο.

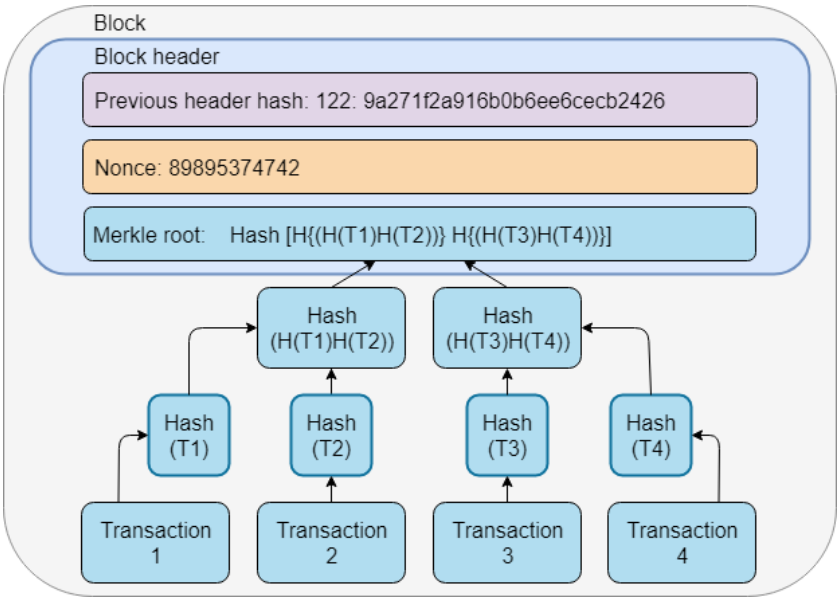
(iv) *Nonce*: ένας αριθμός που χρησιμοποιείται ως μεταβλητή για να τροποποιήσει την έξοδο του *hash* κεφαλίδας. Σε συνδυασμό με το πεδίο *δυσκολίας* χρησιμοποιείται για να αποδείξει ότι ένας εξορύκτης έχει εκτελέσει ένα έργο. Εάν η δυσκολία επιβάλλει ότι η επικεφαλίδα hash ξεκινά με μια ακολουθία τριών μηδενικών, ο εξορύκτης θα επαναλάβει το nonce έως ότου η επικεφαλίδα hash ικανοποιήσει αυτήν την απαίτηση.

(v) *Δυσκολία*: Για να αποφευχθεί η συμπερίληψη νέων μπλοκ σε διαστήματα μικρότερα των 10 λεπτών, η *δυσκολία* ρυθμίζεται αυξάνοντας τον αριθμό των μηδενικών. Επομένως, καθώς θα είναι πιο δύσκολο να βρεθεί το νέο hash, ο χρόνος συμπερίληψης των νέων μπλοκ θα προσαρμοστεί μέχρι να πλησιάσει το 10λεπτο στόχο. Κάθε κόμβος εξόρυξης υπολογίζει ανεξάρτητα τη νέα δυσκολία κάθε 2016 νέων μπλοκ εκτελώντας τον ακόλουθο μαθηματικό υπολογισμό: $\text{New}_{Diff} = \text{Old}_{Diff} \times \frac{Time\ n\ Blocks}{(Time\ Target \times n\ Blocks)}$

(vi) *Δυαδικά δέντρα κατακερματισμού (Merkle trees)*: ένα πλήρες δυαδικό δέντρο με μία k-bit τιμή που σχετίζεται με κάθε κόμβο δέντρου. Η τιμή ενός εσωτερικού κόμβου είναι μια μονόδρομη συνάρτηση

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

των τιμών των παιδιών του. Σχεδιάζονται έτσι ώστε μια τιμή *φύλλου (leaf)* να μπορεί να ελεγχθεί έναντι μιας δημόσια γνωστής τιμής *ρίζας* παρέχοντας τις τιμές των αντίστοιχων ζευγών στην διαδρομή των φύλλων προς τη ρίζα. Στο BC, παρέχει μια αποτελεσματική διαδικασία για τον έλεγχο αν μια συναλλαγή βρίσκεται στο μπλοκ. Για να χτιστεί το δέντρο, πρέπει να ξεκινήσουμε με τα φύλλα, τα οποία περιέχουν το *hash* των συναλλαγών. Δεδομένου ότι πρόκειται για ένα πλήρες δυαδικό δέντρο, στο οποίο όλοι οι εσωτερικοί κόμβοι έχουν δύο παιδιά και όλα τα φύλλα είναι στο ίδιο επίπεδο, εάν υπάρχει ένας μονός αριθμός συναλλαγών για να συνοψίσουμε, η τελευταία συναλλαγή hash θα αναπαραχθεί για να δημιουργηθεί άρτιος αριθμός φύλλων . Στη συνέχεια, τα φύλλα ομαδοποιούνται ανά δύο και το hash τους παράγει έναν *γονικό* κόμβο. Οι γονικοί κόμβοι στη συνέχεια ομαδοποιούνται σε ζεύγη και βιώνουν την ίδια διαδικασία μέχρι να μην υπάρχουν άλλα ζεύγη, δημιουργώντας έτσι έναν κόμβο *ρίζας* που ονομάζεται *ρίζα Merkle* (Makhdoom et al., 2019).



Δομή μπλοκ. Αναπαραγωγή από Jesus et al. (2018)

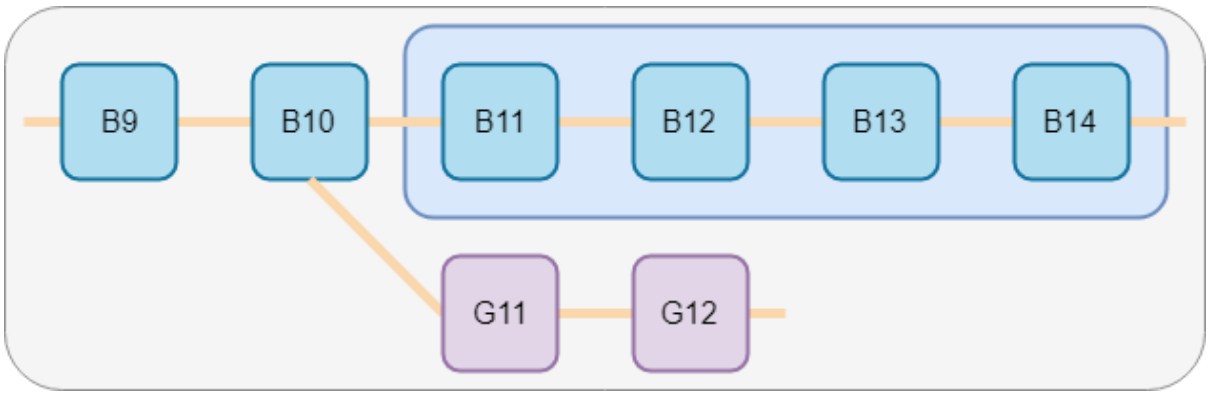
2.3 Λειτουργία Αλυσίδας Καταγραφών

Για να κατανοήσουμε σε βάθος τη φύση του BC πρέπει να μελετήσουμε πώς λειτουργεί. Πρόκειται για ένα διομότιμο δίκτυο (peer-to-peer) κόμβων που ενεργούν πάνω στο ίδιο δίκτυο μέσω του αντιγράφου (του μητρώου καταγραφών) που κατέχει ο καθένας. Οι χρήστες αλληλεπιδρούν μέσω ενός ζεύγους *ιδιωτικών / δημόσιων κλειδιών*. Χρησιμοποιούν το ιδιωτικό τους κλειδί για να υπογράψουν τις δικές τους συναλλαγές ενώ για να τους απευθυνθεί κανείς στο δίκτυο το πράττει μέσω του δημόσιου κλειδιού τους. Η χρήση της ασύμμετρης κρυπτογραφίας φέρνει στο δίκτυο έλεγχο επιβεβαίωση της γνησιότητας, ακεραιότητα και μη αποποίηση της ευθύνης. Κάθε υπογεγραμμένη συναλλαγή εκπέμπεται από τον κόμβο του χρήστη στους εγγύτερους κόμβους τους. Εκείνοι με τη σειρά τους βεβαιώνουν ότι αυτή η εισερχόμενη συναλλαγή είναι έγκυρη πριν την αναμεταδώσουν περαιτέρω. Όσες συναλλαγές είναι μη έγκυρες απορρίπτονται. Τελικά η συναλλαγή αυτή κατανέμεται σε ολόκληρο το δίκτυο. Οι

επικυρωμένες συναλλαγές, συλλέγονται κατά τη διάρκεια ενός συμφωνημένου χρονικού διαστήματος και συσκευάζονται σε ένα υποψήφιο μπλοκ. Αυτή η διαδικασία ονομάζεται *εξόρυξη - mining*. Ο κόμβος εξόρυξης, δηλαδή ο *εξορύκτης* μεταδίδει αυτό το μπλοκ πίσω στο δίκτυο. Η επιλογή του κόμβου εξόρυξης καθώς και του περιεχομένου του μπλοκ σχετίζονται άμεσα με το *μηχανισμό συναίνεσης* που χρησιμοποιεί το δίκτυο και θα αναλυθεί σε επόμενη υποενότητα. Οι κόμβοι με τη σειρά τους επιβεβαιώνουν ότι το προτεινόμενο μπλοκ πρώτον περιέχει έγκυρες συναλλαγές και δεύτερον παραπέμπει μέσω της τιμής *hash* στο προηγούμενου μπλοκ στην αλυσίδα. Αν και οι δύο έλεγχοι στεφθούν με επιτυχία, οι κόμβοι προσθέτουν το μπλοκ στην αλυσίδα τους και εφαρμόζουν τις συναλλαγές που περιέχουν για να ενημερώσουν την εικόνα του BC. Εάν δεν συμβαίνει αυτό, το προτεινόμενο μπλοκ απορρίπτεται και σηματοδοτείται το τέλος ενός γύρου. Η αυτή διαδικασία είναι επαναλαμβανόμενη (Christidis and Devetsikiotis, 2016).

2.4 Διακλαδώσεις στο δίκτυο

Στην σπάνια περίπτωση που δύο κόμβοι βρουν σχεδόν ταυτόχρονα το κατάλληλο nonce δημιουργείται μία *διακλάδωση (fork)*. Το πρωτόκολλο συναίνεσης POW ορίζει ότι η μακρύτερη υπολογιστικά αλυσίδα, κρίνεται η *αυθεντική*. Έστω ότι προκύπτουν δύο *διακλαδώσεις* που δημιουργούνται από τα ταυτόχρονα επικυρωμένα μπλοκ B11 και F11. Οι εξορύκτες εργάζονται και στις δύο για να προσθέσουν το επόμενο μπλοκ. Όταν ένα νέο μπλοκ προστεθεί στο μπλοκ B11, οι εξορύκτες που εργάζονται στη ο διακλάδωση F11-F12 θα μεταβούν στο B12. Το μπλοκ F12 γίνεται ένα *ορφανό*. Αφού προστεθούν μερικά νέα μπλοκ στο BC, είναι σχεδόν αδύνατο να αντιστραφεί το blockchain για να παραβιαστούν οι συναλλαγές. Στο Bitcoin, έπειτα από έξι μπλοκ, η αλυσίδα θεωρείται αυθεντική (Zheng et al., 2018).



Σενάριο διακλάδωσης, όπου η μακρύτερη υπολογιστικά αλυσίδα επιλέγεται ως αυθεντική. Αναπαραγωγή από Zheng et al. (2018)

2.4.1 Ελαστική και σταθερή διακλάδωση

Κάποιες φορές γεννιέται η ανάγκη ενημερώσεων του κώδικα και η βελτιστοποίηση των δικτύων BC και αποσκοπούν στη βελτίωση των υποκείμενων πρωτοκόλλων τους. Αυτές οι βελτιώσεις είναι γνωστές ως ελαστικές και σταθερές διακλαδώσεις στην ορολογία blockchain. Οι μεν *ελαστικές*

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

διακλαδώσεις (hard forks) παρέχουν μια ενημέρωση στο λογισμικό του πρωτοκόλλου που αναγνωρίζει την συμβατότητα με τα προηγούμενα μπλοκ και έχουν ως προαπαιτούμενο τη συναίνεση της πλειοψηφίας των εξορυκτών στο νέο λογισμικό. Παρόλα αυτά, η νέα λειτουργικότητα μπορεί να απορριφθεί από τους περισσότερους κόμβους με το να προσκολλώνται στους παλαιούς κανόνες. Από την άλλη δε, οι *σταθερές διακλαδώσεις (hard forks)* φέρνουν ριζική αλλαγή, χωρίς συμβατότητα με προηγούμενα μπλοκ και συναλλαγές. Συνεπώς, όλοι οι κόμβοι πρέπει να αναβαθμιστούν στην πιο πρόσφατη ενημέρωση και όσοι διατηρούν παλαιότερη έκδοση δεν θα γίνονται πλέον αποδεκτοί. Η κοινότητα μπορεί να διχαστεί. Παραδείγματα αποτελούν τα Ethereum, Ethereum Classic, Bitcoin, Bitcoin Cash και Bitcoin Gold. Αυτές οι διακλαδώσεις έχουν προχωρήσει ταυτόχρονα και σήμερα ανταγωνίζονται μεταξύ τους.

2.5 Ταξινόμηση Αλυσίδων Καταγραφών

Οι Fernández-Caramés και Fraga-Lamas (2018) επισημαίνουν ότι παρόλο που οι περισσότεροι συγγραφείς στην προσπάθειά τους να κατηγοριοποιήσουν τις υλοποιήσεις BC χρησιμοποιούν τους όρους *δημόσιο/χωρίς εξουσιοδότηση και ιδιωτικό/με εξουσιοδότηση* ως συνώνυμους. Σε πολλές περιπτώσεις αυτό δεν επηρεάζει κάτι. Στην περίπτωση του IoT όμως οι ρόλοι οφείλουν να είναι διακριτοί ανάμεσα σε *αυθεντικοποίηση* – ποιός μπορεί να έχει πρόσβαση στο BC, διαφορά μεταξύ *δημόσιου και ιδιωτικού* και σε *εξουσιοδότηση* – τί μπορεί μία συσκευή να κάνει, διαφορά μεταξύ *χωρίς εξουσιοδότηση και με εξουσιοδότηση*. Οι διακρίσεις μεταξύ σωστής ορολογίας είναι ανοιχτές και πιθανώς οι ορισμοί που δίνονται να διαφέρουν από άλλους ερευνητές.

Σε ένα δημόσιο BC ο οποιοσδήποτε μπορεί να συμμετέχει χωρίς έγκριση, με τη δυνατότητα να δρα ως *απλός κόμβος* ή ως *εξορύκτης/επικυρωτής*[3]. Στα ιδιωτικά, ο ιδιοκτήτης θέτει περιορισμούς ως προς την πρόσβαση. Αρκετά από αυτά είναι και με εξουσιοδότηση[4] ώστε να ελέγχεται ποιος συναλλάσσεται, φέρει εις πέρας έξυπνα συμβόλαια ή συμμετέχει ως εξορύκτης.

Μία άλλη κατηγοριοποίηση είναι μεταξύ BC που στοχεύουν αποκλειστικά στη μεταφορά και παρακολούθηση ψηφιακών αγαθών[5] (πχ., Bitcoin) και μοντέλων που λογαριασμού επιτρέπουν την εκτέλεση κάποιας λογικής (δηλ. εκτέλεση έξυπνων συμβολαίων) τη δημιουργία πολύπλοκων επαληθεύσιμων διεργασιών. Το τίμημα των έξυπνων συμβολαίων στο BC είναι υψηλή διεκπεραιωτικότητα συναλλαγών χαμηλός ταυτοχρονισμός.

Επιπλέον, υπάρχουν συστήματα όπως το Ripple που χρησιμοποιούν μάρκες ενώ άλλα σαν το Hyperledger που δεν χρησιμοποιούν. Οι *μάρκες (tokens)* δεν συνδέονται απαραίτητα με την ύπαρξη

[3] Οι τελευταίοι έχουν να λαμβάνουν οικονομικά κίνητρα εν αντιθέσει με τους απλούς κόμβους, πχ. Bitcoin, Ethereum, Litecoin κα.
[4] Χωρίς αυτό να είναι δεσμευτικό.
[5] Ή αλλιώς μοντέλα UTXO (unspent transaction outputs)

κρυπτονομισμάτων, αλλά μπορούν να χρησιμοποιηθούν ως εσωτερικές αποδείξεις που αποδεικνύουν ότι ορισμένα γεγονότα συνέβησαν σε συγκεκριμένες χρονικές στιγμές.

2.6 Συναίνεση στο δίκτυο

2.6.1 Ανάγκη μίας κοινής καθολικής εικόνας

Για την αποφυγή χάους σε αυτό το κατανεμημένο περιβάλλον και με σκοπό τη διατήρηση μιας κοινής καθολικής εικόνας παντού, κάθε δίκτυο BC πρέπει να καθορίσει ορισμένους κανόνες στους οποίους θα πρέπει να συμμορφώνεται κάθε συναλλαγή της βάσης δεδομένων. Αυτοί οι κανόνες καθορίζονται από την εκάστοτε εφαρμογή, ερμηνευμένοι σε κώδικα ο οποίος εφαρμόζεται σε κάθε πελάτη του BC και εν συνεχεία χρησιμοποιείται αρχικά για να αποφασιστεί αν μια εισερχόμενη συναλλαγή είναι έγκυρη και κατά συνέπεια αν πρέπει να μεταφερθεί στο δίκτυο ή όχι. Είναι επιτακτική ανάγκη οι κόμβοι να συμφωνούν σχετικά με τις συναλλαγές και τη σειρά με την οποία είναι καταχωρημένες σε κάθε νεοεισαχθέν μπλοκ. Διαφορετικά, τα μεμονωμένα αντίγραφα του BC θα αποκλίνουν και θα καταλήξουμε σε διακλάδωση - *fork* - δηλαδή οι κόμβοι θα έχουν μια διαφορετική εικόνα της παγκόσμιας κατάστασης και το δίκτυο δεν θα είναι πλέον σε θέση να διατηρήσει μια μοναδική έγκυρη ιστορική αναδρομή (εκτός αν έχει επιλυθεί αυτή η διακλάδωση). Συνεπώς, κρίνεται αναγκαία η ύπαρξη ενός κατανεμημένου μηχανισμού συναίνεσης σε κάθε δίκτυο BC προκειμένου να επιτευχθεί αυτό (Christidis and Devetsikiotis, 2016).

2.6.2 Το πρόβλημα των βυζαντινών στρατηγών

Ο τρόπος επίτευξης συναίνεσης μεταξύ των αναξιόπιστων κόμβων μπορεί να θεωρηθεί συνώνυμο του *προβλήματος των βυζαντινών στρατηγών* (BGP). Μια ομάδα κόμβων (στρατηγοί) που δεν εμπιστεύονται ο ένας τον άλλον όταν ανταλλάσσουν κρυπτονομίσματα (μηνύματα), επειδή ενδέχεται κακόβουλα τρίτα μέρη (προδότες) να αποπειραθούν να τα παραπλανήσουν, προσπαθούν να καταλήξουν σε συμφωνία για την εγκυρότητα των συναλλαγών (απόφασης ενός πλάνου μάχης). Στην περίπτωση των κρυπτονομισμάτων, αυτό το υπολογιστικό πρόβλημα σχετίζεται αυτό της διπλής δαπάνης, το οποίο εξετάζει πώς μπορεί να διαπιστωθεί ότι κάποιο ποσό ψηφιακού χρήματος δεν είχε δαπανηθεί ξανά χωρίς την επικύρωση ενός αξιόπιστου τρίτου όπως μία τράπεζα που τηρεί αρχείο όλων των συναλλαγών και των υπολοίπων των χρηστών. Η επίτευξη συναίνεσης σε ένα τέτοιο περιβάλλον είναι μια πρόκληση ιδιαιτέρως λόγω της κατανεμημένης φύσης του δικτύου. Στο BC, δεν υπάρχει κεντρικός κόμβος που να εξασφαλίζει ότι τα μητρώα καταγραφών στους κατανεμημένους κόμβους είναι όλα ίδια. Οι κόμβοι δεν χρειάζεται να εμπιστεύονται τους άλλους κόμβους. Επομένως, απαιτούνται ορισμένα πρωτόκολλα για να εξασφαλιστεί ότι τα μητρώα καταγραφών συναλλαγών είναι παντού συνεπή (Zheng et al., 2018).

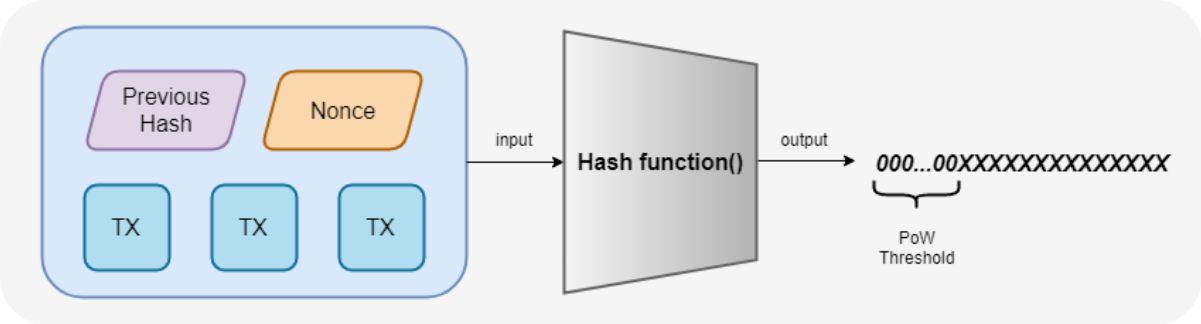
2.6.3 Πρωτόκολλα συναίνεσης

Επομένως, ένα πρωτόκολλο συναίνεσης πρέπει να παρουσιάζει την ιδιότητα της *ανοχής βυζαντινού σφάλματος (Byzantine Fault Tolerant - BFT)*. Με βάση τους Panarello et al. (2018) τα πρωτόκολλα BFT κατηγοριοποιούνται σε:

1) **Proof-of-*:** Η βάση αυτών των αλγορίθμων είναι η εκλογή ενός ηγέτη. Ο ηγέτης είναι τότε υπεύθυνος για την επικύρωση του νέου μπλοκ και την διάδοση μέσω του δικτύου. Σε περίπτωση σύγκρουσης υπάρχουν επίσης μηχανισμοί επίλυσης.
2) **Βυζαντινή Συμφωνία (Byzantine Agreement - BA)**: Η βάση αυτών των αλγορίθμων είναι η εκλογή πλειοψηφίας. Όλοι οι συμμετέχοντες στο δίκτυο λαμβάνουν μέρος στην επικύρωση και όταν ένα ελάχιστο όριο κόμβων συμφωνεί για ένα μπλοκ, το μπλοκ προστίθεται στο δίκτυο υπό την προϋπόθεση ότι η πλειονότητα των κόμβων είναι ειλικρινείς.

Αμέσως μετά παραθέτουμε τις πιο κοινές προσεγγίσεις για την επίτευξη συναίνεσης στο BC.

2.6.3.1 Απόδειξη-του-Έργου (Proof-of-Work)



Υπολογισμός απόδειξης-του-έργου βάση ορίου. Αναπαραγωγή από Panarello et al. (2018)

Πρόκειται για μία στρατηγική συναίνεσης που χρησιμοποιείται στο δίκτυο Bitcoin και είναι ένα υπολογιστικά εντατικό μαθηματικό πρόβλημα. Επιπλέον, η PoW αποτελεί ένα ασύμμετρο έργο, δηλαδή είναι δύσκολο ως προς την επίλυση και πολύ εύκολο στην επαλήθευση. Το κάτωθι σχήμα αποτελεί ένα παράδειγμα. Ένας κόμβος, για να επισυνάψει ένα μπλοκ στην αλυσίδα, πρέπει να βρει έναν αριθμό - *nonce*[6] - στην κεφαλίδα του μπλοκ έτσι ώστε η κρυπτογραφική συνάρτηση κατακερματισμού *SHA-256* αυτού του *nonce* και των δεδομένων του μπλοκ να αποδώσει μια

[6] Το *"nonce"* σε ένα μπλοκ του Bitcoin είναι ένα πεδίο 32-bit (4-byte) του οποίου η τιμή έχει οριστεί έτσι ώστε η κρυπτογραφική συνάρτηση κατακερματισμού όλου του μπλοκ να περιέχει μία σειρά συνεχόμενων μηδενικών. Τα υπόλοιπα πεδία του μπλοκ δεν αλλάζουν, καθώς έχουν καθορισμένο νόημα (συναλλαγές, κρυπτογραφικό αποτύπωμα προηγούμενου μπλοκ κα.).

προκύπτουσα τιμή - *hash* - η οποία ξεκινάει με την απαιτούμενη ποσότητα μηδενικών[7] που αναμένει το δίκτυο. Ο αριθμός των διαδοχικών μηδενικών - "0" ονομάζεται *όριο* - *threshold*. Δεδομένου ότι πρόκειται για κρυπτογραφική λειτουργία κατακερματισμού μονής κατεύθυνσης, οποιοσδήποτε άλλος κόμβος μπορεί εύκολα να επαληθεύσει ότι η δεδομένη λύση ικανοποιεί την απαίτηση και υιοθετεί αυτό το μπλοκ για το BC της αλλά δεν μπορεί να συμβεί το αντίθετο, δηλαδή να εκτιμηθεί από το αποτέλεσμα ποιο είναι το περιεχόμενο του αρχικού μπλοκ.

Ο κάθε κόμβος του δικτύου υπολογίζει συνεχώς ένα *hash* χρησιμοποιώντας διαφορετικά *nonces* μέχρι να επιτευχθεί το *threshold*. Οποιοσδήποτε εξ αυτών μπορεί να λύσει αυτό το "παζλ" και να επιδείξει το έργο που εκπόνησε, τη λεγόμενη "απόδειξη-του-έργου" (proof-of-work, αλλιώς PoW). Όταν ένας κόμβος αποκτά τη σχετική τιμή, όλοι οι άλλοι κόμβοι πρέπει να επιβεβαιώσουν αμοιβαία την ορθότητά της και να προχωρούν στην ενσωμάτωση του μπλοκ στην αλυσίδα τους. Οι κόμβοι που υπολογίζουν τα *hashes* ονομάζονται *εξορύκτες* και η διαδικασία αυτή ονομάζεται *εξόρυξη*. Δεδομένου ότι ο υπολογισμός της πιστοποίησης είναι χρονοβόρος διαδικασία, προτείνεται επίσης ένας μηχανισμός παροχής κινήτρων (π.χ., η χορήγηση μικρής δόσης κρυπτονομισμάτων στον εξορύκτη). Το συγκεκριμένο πρωτόκολλο συναίνεσης έχει επικριθεί έντονα επειδή θεωρείται εξαιρετικά δύσκολο, υπολογιστικά βαρύ και πολύ ακριβό όσον αφορά την κατανάλωση ενέργειας (Christidis and Devetsikiotis, 2016; Zheng et al., 2018; Panarello et al., 2018).

2.6.3.2 Απόδειξη-του-Μεριδίου (Proof-of-Stake[8])

Αποτελεί μια εναλλακτική στην PoW καθώς απαιτεί λιγότερη υπολογιστική ισχύ και εξοικονομεί ενέργεια. Είναι μια κατηγορία αλγορίθμων συναίνεσης για τα δημόσια BC που εξαρτώνται από την οικονομική συμμετοχή στο δίκτυο. Αντί να επιβραβεύεται ο "ταχύτερος" κόμβος, ο δημιουργός του επόμενου μπλοκ επιλέγεται με πιθανοτικό τρόπο και η πιθανότητα επιλογής ενός κόμβου είναι ανάλογη του *"μεριδίου"* που παρουσιάζουν οι συμμετέχοντες, δηλαδή της *κυριότητας* τους. Στην PoS, τα μπλοκ συνήθως επικυρώνονται, δεν εξορύσσονται και λειτουργούν με τον εξής τρόπο: το BC παρακολουθεί ένα σύνολο *επικυρωτών* και όποιος κατέχει κρυπτονομίσματα μπορεί να γίνει *επικυρωτής* στέλνοντας έναν ειδικό τύπο συναλλαγής που κλειδώνει τα κρυπτονομίσματά του σε μία *κατάθεση*. Ο αλγόριθμος επιλέγει τυχαία έναν επικυρωτή κατά τη διάρκεια μίας χρονικής περιόδου (π.χ. κάθε 10 δευτερόλεπτα) και εκχωρεί στον εν λόγω *επικυρωτή* το δικαίωμα δημιουργίας ενός μόνο μπλοκ. Ένας κακόβουλος κινδυνεύει να χάσει το μερίδιό του καθώς και το δικαίωμα συμμετοχής.

Η επιλογή βασίζεται στον *"πλούτο"* των συμμετεχόντων αφού υπάρχει η πεποίθηση ότι τα άτομα με περισσότερα νομίσματα είναι λιγότερο πιθανό να επιτεθούν στο δίκτυο. Όμως, όσο περισσότερα

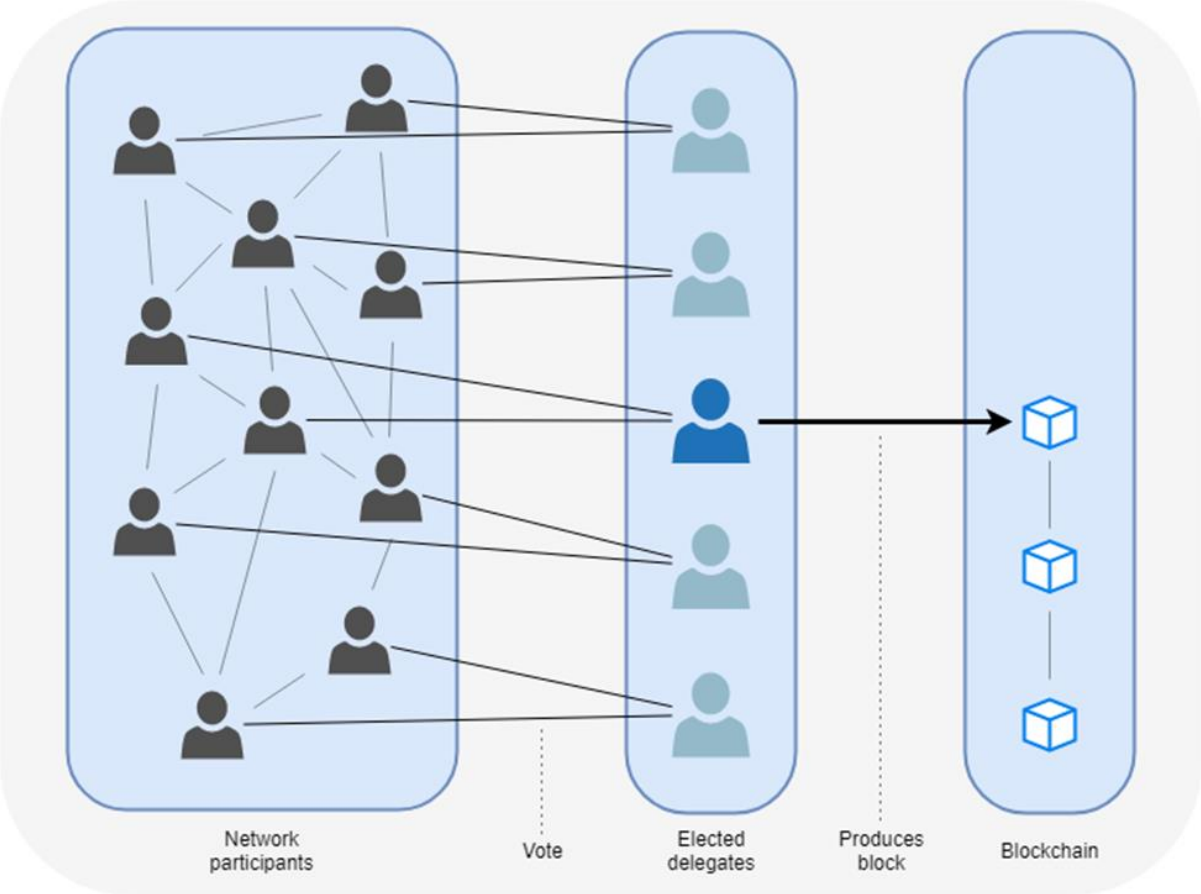
[7] Σημειώστε ότι όσο περισσότερα τα μηδενικά που προηγούνται, τόσο πιο δύσκολη είναι η λύση αυτού του παζλ. Αυτό ονομάζεται αύξηση του στόχου. Το δίκτυο ρυθμίζει το επίπεδο δυσκολίας κάθε 2016 μπλοκ για να προσαρμόζεται στις αλλαγές στην ισχύ CPU του δικτύου και για να βεβαιώνεται ότι τα μπλοκ παράγονται με σταθερό ρυθμό.

[8] Ο όρος *stake* μπορεί να αποδοθεί στα χρηματοοικονομικά ως *μερίδιο* ή *κυριότητα*. Συνάμα, σε άλλες εκφράσεις πχ. *at stake* αποδίδει το *διακύβευμα*.

νομίσματα κατέχει κάποιος, τόσο περισσότερη δύναμη αποκτά. Αυτό είναι άδικο, διότι ο πλουσιότερος είναι βέβαιο ότι θα κυριαρχήσει στο δίκτυο. Ως αποτέλεσμα, προτείνονται πολλές λύσεις συνδυαστικά με το μέγεθος του *διακυβεύματος / μεριδίου* για να αποφασιστεί ποιος θα δημιουργήσει το επόμενο μπλοκ. Συγκεκριμένα, το Blackcoin χρησιμοποιεί *τυχαιοποίηση (randomization)* για να προβλέψει τον επόμενο δημιουργό, με βάση έναν τύπο που αναζητά τη *χαμηλότερη τιμή hash* σε συνδυασμό με το *μέγεθος του μεριδίου*. Δεδομένου ότι οι εγγυήσεις είναι δημόσιες, κάθε κόμβος μπορεί να προβλέψει, με εύλογη ακρίβεια, ποιος λογαριασμός θα αποκτήσει το δικαίωμα επικύρωσης ενός μπλοκ. Το Peercoin τάσσεται υπέρ της επιλογής νομισμάτων με βάση την *ηλικία* τους. Στο Peercoin, τα *παλαιότερα* και *μεγαλύτερα σύνολα νομισμάτων* έχουν μεγαλύτερη πιθανότητα παραγωγής του επόμενου μπλοκ. Πολλά BC υιοθετούν την PoW αρχικά και μεταπηδούν σε PoS σταδιακά, όπως η Ethereum από το Ethash στο Casper. Στο Casper, ένας κόμβος καλείται να καταθέσει ένα εχέγγυο ασφαλείας, που ονομάζεται *εγγύηση - bonding* και έτσι γίνεται ένας *εγγυημένος επικυρωτής*. Έπειτα, ο *επικυρωτής* μπορεί να *ποντάρει* ένα ποσό στο ποιο μπλοκ θα συμπεριληφθεί στη συνέχεια στο BC. Κατά την αποδοχή, θα λάβει μια ανταμοιβή. Τα *ποντάρισματα* ενάντια στη συναίνεση (κακόβουλα) θα προκαλέσουν στον *επικυρωτή* τη διαγραφή της *εγγύησης* (Zheng et al., 2018; Panarello et al., 2018; Jesus et al., 2018).

2.6.3.3 Κατ' Εκπροσώπευση Απόδειξη-του-Μεριδίου (Delegated Proof-of-Stake)

Παρόμοια με την POS, οι εξορύκτες έχουν προτεραιότητά να παράγουν μπλοκ σύμφωνα με το μερίδιό τους. Η μεγάλη διαφορά μεταξύ της POS και της DPOS είναι ότι η POS είναι άμεσα δημοκρατική ενώ το DPOS είναι αντιπροσωπευτικά δημοκρατική. Τα ενδιαφερόμενα μέρη εκλέγουν τους *εκπροσώπους* τους μέσω *ψηφοφορίας* για να δημιουργήσουν και να επικυρώσουν ένα μπλοκ. Η ευθύνη της διαχείρισης του δικτύου παρέχεται σε *εκπροσώπους* που δεν έχουν κίνητρα. Οι *εκπρόσωποι* μπορούν επίσης να προτείνουν αλλαγές που μπορούν να υιοθετηθούν με βάση την ψηφοφορία του δικτύου. Η ευθύνη της επικύρωσης συναλλαγών και της δημιουργίας μπλοκ στηρίζεται σε *μάρτυρες*. Η επιλογή *ηγέτη* είναι *ντετερμινιστική* και βασίζεται στον *αλγόριθμο κυκλικής επαναφοράς (Round Robin)*. Οι *μάρτυρες* πληρώνονται όσον αφορά τη δημιουργία μπλοκ. Επιπλέον, οι χρήστες δεν χρειάζεται να ανησυχούν για τους ανέντιμους αντιπροσώπους επειδή οι αντιπρόσωποι μπορούν να καταψηφιστούν εύκολα. Με σημαντικά λιγότερους κόμβους να εμπλέκονται στη διαδικασία η επικύρωση του μπλοκ και κατά συνέπεια των συναλλαγών, επισπεύδεται. Οι *εκπρόσωποι* είναι υπεύθυνοι για τη ρύθμιση παραμέτρων του δικτύου, όπως το *μέγεθος του μπλοκ* και τα *χρονικά διαστήματα* μεταξύ μπλοκ καθώς και για τα *πλάνα αμοιβών*. Το DPOS έχει ήδη εφαρμοστεί και είναι η ραχοκοκαλιά του Bitshares (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018; Panarello et al., 2018).



Μία γενική υλοποίηση της συναίνεσης DPoS

2.6.3.4 Απόδειξη του Χρόνου που παρήλθε (Proof-of-Elapsed-Time)

Για να αντιμετωπίσει τα προβλήματα της υψηλής κατανάλωσης ρεύματος και της χρονικής καθυστέρησης στα πρωτόκολλα συναίνεσης με βάση την PoW, η Intel ανέπτυξε ένα πρωτόκολλο συναίνεσης βασισμένο σε λοταρίες για την Sawtooth Lake, μια κατανεμημένη πλατφόρμα εφαρμογών που βασίζεται σε BC. Η απόδειξη του χρόνου που παρήλθε (PoET) εκμεταλλεύεται το αξιόπιστο περιβάλλον εκτέλεσης (Trusted Execution Environment - TEE) των επεξεργαστών της Intel και ιδιαίτερα τις επεκτάσεις λογισμικού προστασίας (Software Guard Extensions - SGX) για την επίτευξη συναίνεσης. Οι SGX είναι ένα σύνολο εντολών κώδικα σχετικά με την ασφάλεια ενσωματωμένο σε ορισμένες CPU της Intel. Επιτρέπουν σε επίπεδο κώδικα χρήστη να ορίσει απομονωμένες ιδιωτικές περιοχές μνήμης - *enclaves* - το περιεχόμενο των οποίων είναι προστατευμένο και απροσπέλαστο από κάθε εξωτερική διεργασία. Ο PoET χρησιμοποιεί ένα μοντέλο τυχαίας εκλογής ενός ηγέτη, ο οποίος θα επικυρώσει ή θα εξορύξει τα μπλοκ. Λειτουργεί ουσιαστικά ως εξής: υπάρχει ένα *εξειδικευμένο υλισμικό* για τη δημιουργία μιας τυχαίας τιμής χρόνου. Κάθε επικυρωτής ή εξορύκτης ζητά μία *λήξη χρόνου* για αυτό το υλισμικό. Ο επικυρωτής με τον *συντομότερο χρόνο αναμονής* για ένα δεδομένο μπλοκ εκλέγεται ως *ηγέτης* και περιμένει αυτόν τον δεδομένο χρόνο για να επικυρώσει το μπλοκ. Μετά από αυτό, το μπλοκ θα συμπεριληφθεί στην αλυσίδα και η διαδικασία θα επαναληφθεί. Εκτός από την

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εκλογή ηγέτη με βάση την PoET για τον οποίο απαιτείται ειδικά σχεδιασμένο υλισμικό, το υπόλοιπο πρωτόκολλο λειτουργεί όπως το πρωτόκολλο Bitcoin.

Αυτό το μοντέλο προτείνεται για χρήση σε ιδιωτικές BC καθώς με βάση τη θεωρία, οι επικυρωτές πρέπει να είναι ειλικρινείς. Ο αλγόριθμος εκλογής ηγέτη PoET πληροί τα κριτήρια για έναν καλό αλγόριθμο λοταρίας δηλαδή την αμεροληψία, την επένδυση και την επαλήθευση. Η πιθανότητα εκλογής είναι ανάλογη με τους πόρους που συνεισφέρονται (για παράδειγμα, ισχύς επεξεργασίας). Η τυχαιότητα στη δημιουργία χρόνου αναμονής εξασφαλίζει ότι η λειτουργία του ηγέτη κατανέμεται ομοιόμορφα μεταξύ όλων των επικυρωτών. Το χαμηλό κόστος συμμετοχής καθιστά εφικτή τη συμμετοχή μεγάλου αριθμού επικυρωτών, αυξάνοντας την ευρωστία του αλγόριθμου συναίνεσης. Μια μεγάλη ανησυχία για τον PoET είναι ότι είναι άρρηκτα συνδεδεμένο με το υλισμικό της Intel. Οι ερευνητές επεσήμαναν επίσης ότι το SGX παρουσιάζει ελαττώματα ασφαλείας (Panarello et al., 2018; Jesus et al., 2018; Makhdoom et al., 2019).

2.6.3.5 Απόδειξη-της-Δραστηριότητας (Proof-of-Activity)

Για να συνδυαστούν τα πλεονεκτήματα του POW και του POS, προτείνεται η απόδειξη-της-δραστηριότητας. Η γενική ιδέα πηγάζει από ένα οικονομικό φαινόμενο γνωστό ως *"Τραγωδία των Κοινοτήτων",* το οποίο είναι ένα διαδεδομένο πρόβλημα στη μελέτη των οικονομικών και της θεωρίας των παιχνιδιών. Αναφέρεται σε ένα περιβάλλον όπου οι συμμετέχοντες έχουν την ευκαιρία να ενεργούν εγωιστικά, αναλαμβάνοντας δράση για να ωφεληθούν εις βάρος του κοινού συμφέροντος. Στο PoW, με την πάροδο του χρόνου η εξόρυξη θα καταστεί σημαντικά λιγότερο προσοδοφόρα αφού η ανταμοιβή σε κρυπτονομίσματα για τη δημιουργία κάθε νέου μπλοκ θα υποχωρεί σταδιακά. Όταν η επιβράβευση καταστεί αμελητέα και η οικονομική αμοιβή θα αποτελείται σχεδόν εξ ολοκλήρου από τα τέλη συναλλαγών, οι εξορύκτες θα έχουν μικρότερο ενδιαφέρον για τη διασφάλιση της ασφάλειας του δικτύου, καθιστώντας το έτσι ευάλωτο σε διάφορες επιθέσεις. Ως εκ τούτου, το προτεινόμενο πρωτόκολλο PoA αποσκοπεί στην αύξηση του κόστους μιας επίθεσης από έναν κακόβουλο χρήστη, αναγκάζοντάς τον να επιτύχει *οκτώ φορές ταχύτερο ρυθμό κατακερματισμού* από ό,τι οι έντιμοι εξορύκτες του δικτύου. Στην PoA, ένα εξορυγμένο μπλοκ πρέπει να υπογραφεί από τους *ν* διαφορετικούς εξορύκτες για να θεωρείται έγκυρο. Με αυτόν τον τρόπο, αν κάποιος είναι κάτοχος του 50% όλων των κρυπτονομισμάτων, δεν μπορεί να ελέγξει τη δημιουργία νέων μπλοκ από μόνος του. Επιπλέον, μειώνει την πολυπλοκότητα των υπολογισμών στο *1/10* της Bitcoin PoW, ελαχιστοποιώντας έτσι την κατανάλωση ενέργειας. Ωστόσο, η απόδειξη της δραστηριότητας στοχεύει επίσης στην εξασφάλιση μόνο εφαρμογών κρυπτονομισμάτων (Zheng et al., 2018; Makhdoom et al., 2019).

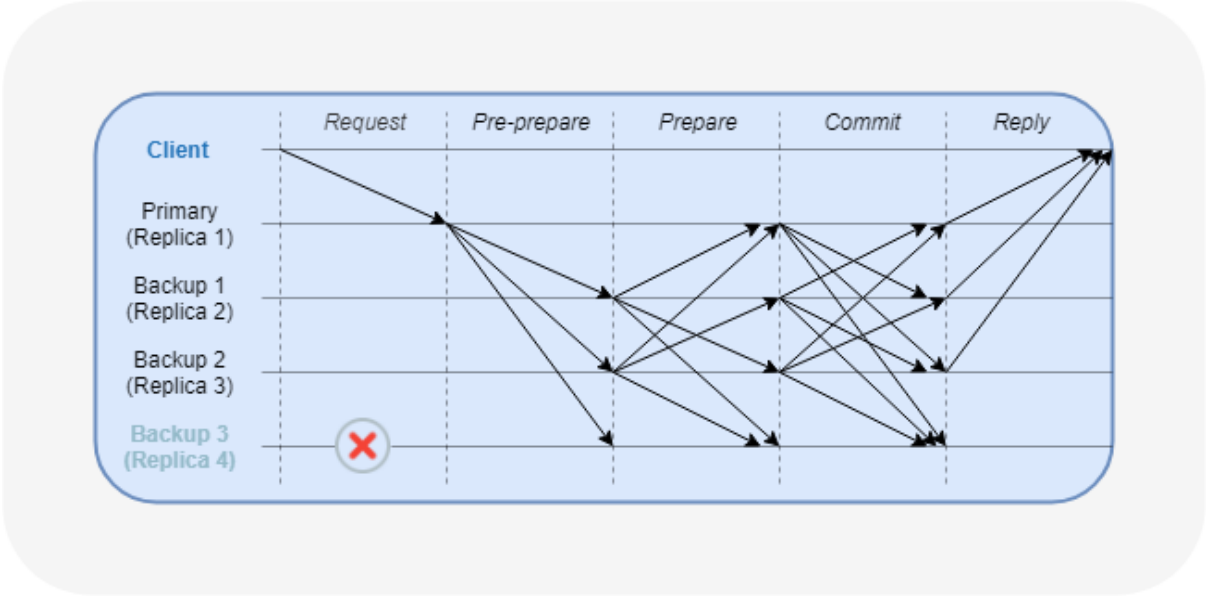
2.6.3.6 Πρακτική Ανοχής Βυζαντινού Σφάλματος (Practical Byzantine Fault Tolerance)

Η λειτουργία ενός πρωτοκόλλου συναίνεσης είναι να διατηρηθεί η σειρά των συναλλαγών σε ένα δίκτυο BC, παρά τις όποιες απειλές. Μία από αυτές είναι και η ταυτόχρονη αποτυχία πολλαπλών

κόμβων δικτύου, ένας από τους τύπους βυζαντινών σφαλμάτων. Η Πρακτική Ανοχή Βυζαντινού Σφάλματος (PBFT) παρέχει μια λύση στο πρόβλημα των βυζαντινών στρατηγών που λειτουργεί σε ασύγχρονα περιβάλλοντα όπως το διαδίκτυο. Περιλαμβάνει ένα πρωτόκολλο τριών φάσεων, όπου σε κάθε φάση ένας κόμβος πρέπει να λάβει ψήφους περισσότερες από τα 2/3 των συνολικών κόμβων για να προχωρήσει και την έννοια ενός «πρωτεύοντος» κόμβου (*ηγέτη*) που ενεργεί ως εξορύκτης μπλοκ. Ο ηγέτης μπορεί να αλλάξει από το υπόλοιπο δίκτυο μέσω ενός μηχανισμού ψηφοφορίας αποκαλούμενου "view-change", εάν καταρρεύσει ή εκδηλώσει αυθαίρετη συμπεριφορά. Το PBFT λειτουργεί με την παραδοχή ότι λιγότερο από το ένα τρίτο των κόμβων είναι ελαττωματικό *(f)*, γι' αυτό λέμε ότι απαιτεί τουλάχιστον *3f + 1* κόμβους.

Συνοπτικά η λειτουργία του αλγορίθμου PBFT εξελίσσεται ως εξής:

a) Ένας πελάτης (*client*) στέλνει αίτημα (*request*) υπηρεσίας στο πρωτεύον μηχάνημα.
b) Το πρωτεύον αποστέλλει ένα μήνυμα προετοιμασίας (*pre-prepare message*) στα μηχανήματα με τα αντίγραφα ασφαλείας (*backup replicas*).
c) Το μηχάνημα επικυρώνει το μήνυμα και εάν ένα μηχάνημα συμφωνεί αποστέλλει ένα μήνυμα ετοιμασίας (*prepare message*) προς όλους τους υπόλοιπους.
d) Όταν ένα μηχάνημα λάβει ένα αριθμό έγκυρων μηνυμάτων μηνύματα που συμφωνούν με την υπηρεσία, αποστέλλει ένα επιβεβαιωτικό μήνυμα (*commit message*)
e) Τα αντίγραφα αφού λάβουν ένα αριθμό επιβεβαιωτικών μηνυμάτων εκτελούν το αίτημα και επιστρέφουν στον πελάτη μία απάντηση (*reply*)



Ομαλή λειτουργία PBFT με ελαττωματικό κόμβο. Αναπαραγωγή από Castro και Liskov (1999)

Οι φάσεις προετοιμασίας και ετοιμασίας χρησιμοποιούνται για μπουν σε σειρά τα αιτήματα που αποστέλλονται στην ίδια *όψη* ακόμα και αν ο πρωτεύων, ο οποίος προτείνει τη σειρά των αιτήσεων,

είναι ελαττωματικός. Οι φάσεις ετοιμασίας και δέσμευσης χρησιμοποιούνται για να εξασφαλίσουν ότι τα αιτήματα που εκτελούνται είναι σε σειρά για όλες τις *όψεις*.

Καθώς ο συνολικός αριθμός κόμβων χρειάζεται να είναι γνωστός, το PBFT δεν είναι κατάλληλο για δημόσια συστήματα και χρησιμοποιείται μόνο σε ιδιωτικά. Το PBFT διασφαλίζει ότι τουλάχιστον τα 2/3 των κόμβων καταλήγουν σε συναίνεση σχετικά με τη σειρά συναλλαγών πριν τις επισυνάψουν στο κοινό κατανεμημένο μητρώο. Τα ασύγχρονα πρωτόκολλα αναμένεται να εξασθενούν σημαντικά όταν το υποκείμενο δίκτυο συμπεριφέρεται με απρόβλεπτο τρόπο (Christidis and Devetsikiotis, 2016; Makhdoom et al., 2019; Castro and Liskov, 1999)

2.6.3.7 Ripple

Ο αλγόριθμος συναίνεσης Ripple προτάθηκε ως λύση για τις υψηλές χρονικές καθυστερήσεις που παρατηρούνται σε αρκετά BC, οι οποίες οφείλονται εν μέρει στις σύγχρονες (synchronous) επικοινωνίες μεταξύ των κόμβων (Fernández-Caramés and Fraga-Lamas, 2018). Χρησιμοποιεί *συλλογικά αξιόπιστα υποδίκτυα* εντός ενός ευρύτερου δικτύου. Μέσα σε αυτό οι κόμβοι κατηγοριοποιούνται σε δύο τύπους:

1) *διακομιστές* επιφορτισμένοι με τη διαδικασία συναίνεσης και
2) *πελάτες* υπεύθυνοι μόνο για μεταφορά κεφαλαίων.

Εν αντιθέσει με το PBFT όπου οι κόμβοι αλληλοεπιδρούν με κάθε άλλο κόμβο στο δίκτυο, κάθε διακομιστής Ripple διατηρεί μια λίστα μοναδικών κόμβων (Unique Node List - UNL). Η *UNL* χρησιμοποιείται από το διακομιστή για να θέσει επερωτήματα στους κόμβους που ανήκουν σε αυτή, κατά τον προσδιορισμό του εάν πρέπει μια συναλλαγή να προστεθεί στο κατανεμημένο μητρώο καταγραφών. Ο τρόπος λειτουργίας είναι ο εξής:

1) Ένας *πελάτης* υποβάλλει τη συναλλαγή στον *διακομιστή*
2) Ο *διακομιστής* μεταδίδει τη συναλλαγή σε άλλους κόμβους
3) Κάθε *διακομιστής* προσαρτάται σε ένα *υποδίκτυο* κόμβων επικύρωσης και αποφασίζει βάσει των συστάσεων (recommendations) των επικυρωτών του.
4) Όταν μια υπερψηφία (ποσοστό 80%) κόμβων εγκρίνει αυτήν την *υποψήφια συναλλαγή*, αυτή η συναλλαγή θα συμπεριληφθεί στο νέο επικυρωμένο μητρώο (*Last-Closed Ledger*).

Για έναν κόμβο, το κατανεμημένο μητρώο καταγραφών διατηρείται ακέραιο εφόσον το ποσοστό των ελαττωματικών κόμβων της UNL του είναι μικρότερο από 20% (Zheng et al., 2018; Jesus et al., 2018). Η αλλιώς, το πρωτόκολλο απαιτεί τουλάχιστον *5f + 1* κόμβους για την ομαλή λειτουργία του. (Christidis and Devetsikiotis, 2016).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

2.6.3.8 Tendermint

Το Tendermint (Kwon, 2014) είναι ένας αλγόριθμος βυζαντινής συναίνεσης. Η διαδικασία είναι αρκετά παρόμοια με την PBFT, αλλά οι κόμβοι στο Tendermint πρέπει να κλειδώσουν τα νομίσματά τους για να γίνουν *επικυρωτές,* να δώσουν *εγγύηση*. Παρέχει μεγαλύτερη ασφάλεια όσον αφορά το επιστρεφόμενο αποτέλεσμα στον πελάτη αφού απαιτεί περισσότεροι από το ένα τρίτο των κόμβων να μην είναι ελαττωματικοί. Επιτρέπει την αλλαγή του συνόλου επικυρωτών και ηγετών δυναμικά. Ένα μπλοκ ξεκινάει από έναν *προτείνοντα*, ο οποίος επιλέγεται από αποκλειστικούς *επικυρωτές* με βάση τον *αλγόριθμο κυκλικής επαναφοράς,* με δικαίωμα ψήφου ανάλογο με την *εγγύησή* τους. Η επικύρωση συναλλαγών γίνεται με βάση την πλειοψηφία, δηλ. οι ειλικρινείς επικυρωτές θα πρέπει να έχουν πλειοψηφία μεγαλύτερη ή ίση με 2/3 των συνολικών ψήφων. Ένας *προτείνων* (proposer) θα επιλέξει να μεταδώσει ένα *ανεπιβεβαίωτο* μπλοκ σε αυτόν τον γύρο. Όλοι οι κόμβοι πρέπει να είναι γνωστοί για την επιλογή του *προτείνοντος*. Χωρίζεται στα κάτωθι τρία βήματα:

- *Βήμα προ-ψήφισης (prevote)*. Οι επικυρωτές επιλέγουν εάν θα αναμεταδώσουν ένα μήνυμα προ-*ψήφισης* για το προτεινόμενο μπλοκ.
- *Βήμα προ-δέσμευσης (precommit)*. Εάν ένας κόμβος έχει λάβει μηνύματα προ-*ψήφισης* περισσότερα από 2/3 των συνολικών για το προτεινόμενο μπλοκ, αναμεταδίδει ένα μήνυμα *δέσμευσης* για αυτό το μπλοκ. Αν όμως έχει λάβει μηνύματα *προ*-δέσμευσης περισσότερα από τα 2/3 των συνολικών, εισέρχεται στο στάδιο δέσμευσης.
- *Βήμα δέσμευσης (commit)*. Ο κόμβος επικυρώνει το μπλοκ και αναμεταδίδει ένα μήνυμα *δέσμευσης* για αυτό το μπλοκ. Αν ο κόμβος έχει λάβει άνω των 2/3 των συνολικών μηνυμάτων *δέσμευσης*, δέχεται το μπλοκ.

Η διαδικασία συναίνεσης για το επόμενο μπλοκ μπορεί να επεκταθεί σε πολλούς γύρους ανάλογα με τις συνθήκες. Πχ. ο υποψήφιος που έχει οριστεί να μην είναι συνδεδεμένος, το μπλοκ που προτείνεται από τον ορισθέντα προτείνοντα να μην διαδόθηκε έγκαιρα ή ακόμα να υπάρχει έγκυρο μπλοκ αλλά λιγότερα από τα 2/3 μηνυμάτων προ-ψήφισης ή προ-δέσμευσης να ληφθούν έγκαιρα από τους επικυρωτές. Ένας κακόβουλος χρήστης (MITM) μπορεί να εκμεταλλευτεί αυτή την εξάρτηση από το χρόνο ώστε να καθυστερήσει σκόπιμα τα μηνύματα από τους προτείνοντες, αναγκάζοντας έτσι το πρωτόκολλο να συνεχίσει για πολλούς γύρους ώστε το σύστημα θα βιώνει καθυστερήσεις στον υπολογισμό των νέων μπλοκ. Για να περιορίσει τη διάδοση των ψευδών μπλοκ από τους προτείνοντες, η Tendermint κατάσχει την εγγύηση των ελαττωματικών – μη έντιμων προτεινόντων. Επίσης, η δαπάνη επικοινωνίας είναι μεγάλη. Ενδεικτικά, για έναν πελάτη και τέσσερις κόμβους επικύρωσης, το πρωτόκολλο συναίνεσης Tendermint χρειάζεται να μοιραστεί 21 μηνύματα για να επεξεργαστεί μία μόνο συναλλαγή.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 3: Έξυπνα Συμβόλαια

Αξιοποιώντας την ικανότητα του Bitcoin να εκτελεί αυτόνομα script, οι προγραμματιστές δημιούργησαν νέες εκδόσεις του BC που μπορούν να εκτελούν αυθαίρετους υπολογισμούς εκτός από τη μεταφορά νομισμάτων. Επί παραδείγματι, το Ethereum υλοποιεί ένα είδος κώδικα που ονομάζεται Έξυπνο Συμβόλαιο με το οποίο δύναται να εκτελέσει οποιονδήποτε αλγόριθμο, ενσωματωμένο στο BC του, ως μέρος των συναλλαγών του.

Η βασική ιδέα πίσω από την χρησιμότητά στο IoT του είναι η ανάπτυξη αυτόνομων αντικειμένων ή συσκευών IoT, τα οποία θα είναι σε θέση να μισθώνουν ή να πουλούν τα δεδομένα τους καθώς και να διατηρήσουν την λειτουργικότητά τους πληρώνοντας υπηρεσίες συντήρησης. Τέτοια αυτόνομα συστήματα πιθανόν να συμβάλλουν στην ανάπτυξη της καθολικής "Οικονομίας των Πάντων" με σκοπό να προσφέρουν αποτελεσματικές και συνεπείς υπηρεσίες χωρίς μεσάζοντες.

3.1 Ορισμός Έξυπνου Συμβολαίου

Η ιδέα των έξυπνων συμβολαίων προήλθε από τον Szabo το 1994 και ορίστηκε ως ένα μηχανογραφημένο πρωτόκολλο συναλλαγών που εκτελεί τους όρους μιας σύμβασης. Ωστόσο, δεν διαδόθηκε ευρέως μέχρι την εμφάνιση της τεχνολογίας BC. Ένα έξυπνο συμβόλαιο είναι ένας κώδικας που τρέχει στο BC για να διευκολύνει, να εκτελέσει και να επιβάλει τους όρους μιας συμφωνίας. Βασικός στόχος ενός έξυπνου συμβολαίου είναι να εκτελεστούν αυτόματα οι όροι μιας συμφωνίας όταν πληρούνται οι καθορισμένοι όροι. Υπόσχονται χαμηλές αμοιβές συναλλαγών σε σύγκριση με τα παραδοσιακά συστήματα που απαιτούν από έναν αξιόπιστο τρίτο να επιβάλει και να εκτελέσει τους όρους μιας συμφωνίας. Ένα έξυπνο συμβόλαιο μπορεί να θεωρηθεί ως ένα σύστημα που απελευθερώνει ψηφιακά αγαθά σε όλα ή σε ορισμένα από τα εμπλεκόμενα μέρη μόλις επιτευχθούν αυθαίρετοι προκαθορισμένοι κανόνες.

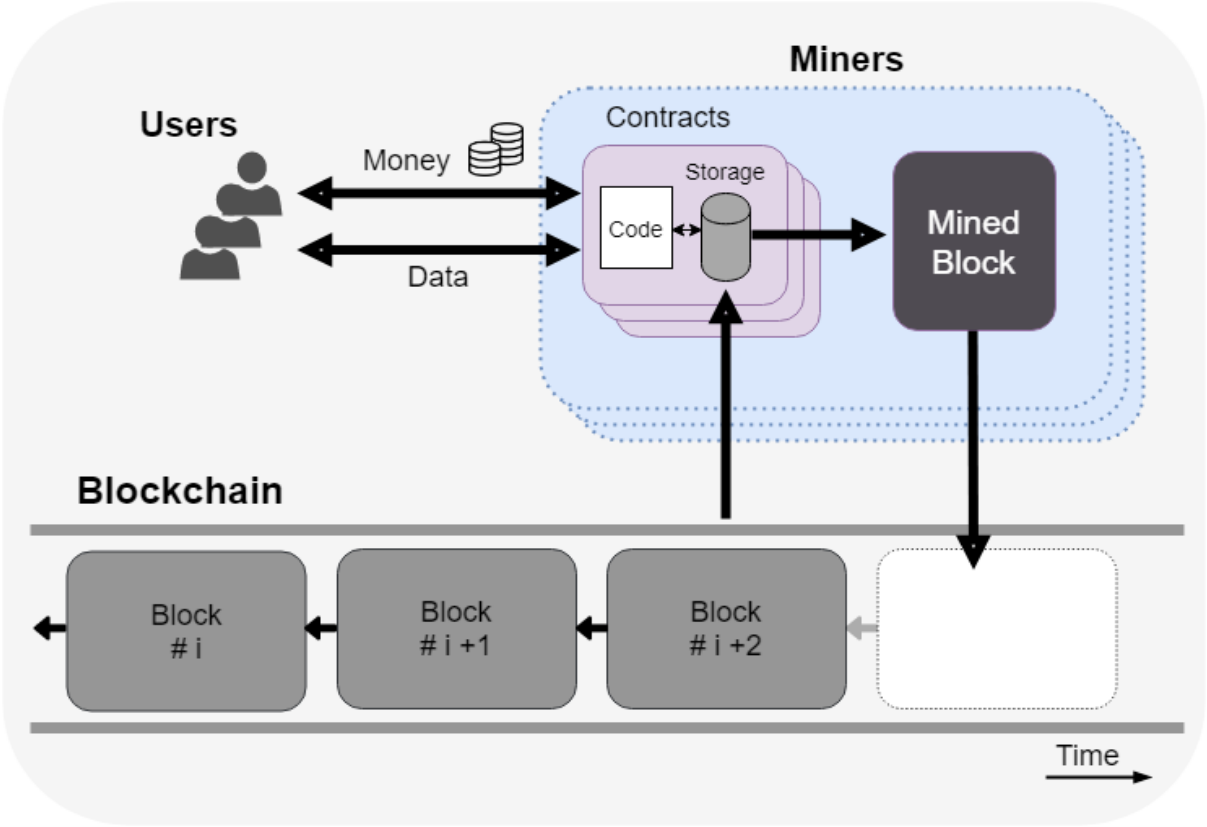
Οι Alharby και Moorsel (2017) επισημαίνουν ότι υπάρχουν πολλοί διαφορετικοί ορισμοί ενός SC στη βιβλιογραφία. Επίσης προχωρούν στον αποσαφηνισμό δύο παραπλανητικών εννοιών του κώδικα έξυπνου συμβολαίου και την έξυπνη νομική σύμβαση:

- Ο *κώδικας έξυπνου συμβολαίου* σημαίνει "κώδικας που αποθηκεύεται, επαληθεύεται και εκτελείται σε ένα BC". Η ικανότητα αυτού του SC εξαρτάται εξ ολοκλήρου από τη γλώσσα προγραμματισμού που χρησιμοποιείται για την έκφραση της σύμβασης και τα χαρακτηριστικά του BC.
- Η *έξυπνη νομική σύμβαση* σημαίνει κώδικα για την ολοκλήρωση ή την αντικατάσταση των νομικών συμβάσεων. Η ικανότητα αυτού του SC δεν εξαρτάται από την τεχνολογία, αλλά από νομικά, πολιτικά και επιχειρηματικά θεσμικά όργανα. Ένα SC αποτελείται από δύο ξεχωριστά συστατικά μέρη. Στην παρούσα μελέτη θα μας απασχολήσει η πρώτη περίπτωση.

3.2 Δομή Έξυπνου Συμβολαίου

Ένα SC αποτελείται από ένα *υπόλοιπο λογαριασμού*, έναν *ιδιωτικό αποθηκευτικό χώρο* και έναν *εκτελέσιμο κώδικα*. Η *κατάσταση* του συμβολαίου περιλαμβάνει την αποθήκευση και το υπόλοιπο του συμβολαίου. Η *κατάσταση* αποθηκεύεται στο BC και ενημερώνεται κάθε φορά που γίνεται κλήση της σύμβασης. Ο κώδικας αποτελείται από συναρτήσεις και μεταβλητές. Οι συναρτήσεις εκτελούνται όποτε γίνονται συναλλαγές. Οι συναλλαγές προς τα SC εμπεριέχουν παραμέτρους εισόδου καθώς απαιτούνται από τις προαναφερθείσες συναρτήσεις. Σε κάθε SC ανατίθεται μια μοναδική διεύθυνση 20 bytes. Ακολουθεί η λειτουργία του SC απεικονίζεται στην εικόνα που.

3.3 Λειτουργία Έξυπνου Συμβολαίου



Το σύστημα ενός Έξυπνου Συμβολαίου. Αναπαραγωγή από Alharby και Moorsel (2017)

Μόλις εφαρμοστεί η σύμβαση στο BC, ο κώδικας δεν μπορεί να αλλάξει. Για να αλληλεπιδράσουν με αυτό οι χρήστες, χρειάζεται απλά να στείλουν μια συναλλαγή στη διεύθυνση του. Αυτή η συναλλαγή θα εκτελεστεί έπειτα από κάθε κόμβο στο δίκτυο για να επιτευχθεί συναίνεση σχετικά με το αποτέλεσμά του. Η κατάσταση του SC θα ενημερωθεί αναλόγως. Το SC μπορεί, με βάση τη συναλλαγή που λαμβάνει, να διαβάζει ή να γράφει στον ιδιωτικό αποθηκευτικό χώρο, να αποθηκεύει χρήματα στο υπόλοιπο του λογαριασμού, να στέλνει ή να λαμβάνει μηνύματα ή χρήματα από χρήστες ή άλλα SC ή ακόμα και να δημιουργεί νέα SC.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3.4 Βασικά Χαρακτηριστικά και Οφέλη του Έξυπνου Συμβολαίου

Διακρίνουμε δύο τύπους: Ένα *ντετερμινιστικό* SC είναι μια έξυπνη σύμβαση που όταν εκτελείται, δεν απαιτεί καμία πληροφορία από εξωτερικό συμβαλλόμενο μέρος. Ένα *μη-ντετερμινιστικό* SC είναι μια σύμβαση που εξαρτάται από πληροφορίες από ένα εξωτερικό μέρος (*χρησμοί - oracles*). Για παράδειγμα, ένα συμβόλαιο που απαιτεί την τρέχουσα πληροφορία καιρού, η οποία δεν είναι διαθέσιμη στο BC.

Τα έξυπνα συμβόλαια, με βάση τους Panarello et al. (2018) χαρακτηρίζονται από τις ακόλουθες ιδιότητες:

1. Αυτονομία: Όσοι συμμετέχουν δίνουν την συγκατάθεσή τους στις αποφάσεις και επομένως απαλείφεται η ανάγκη διαμεσολάβησης και η μεροληψία που σχετίζεται με αυτή.
2. Εμπιστοσύνη: Τα βασικά έγγραφα είναι διαθέσιμα σε ένα δημόσιο μητρώο καταγραφών και επομένως εξαλείφεται ο κίνδυνος να καταστραφούν ή να χαθούν.
3. Αντίγραφα ασφαλείας: Λόγω της αποκεντρωμένης φύσης του BC, η παρουσία των δεδομένων σε πολλούς κόμβους που συμμετέχουν στο δίκτυο καθιστά τα δεδομένα ασφαλή.
4. Εξοικονόμηση: Οι έξυπνες συμβάσεις εξαλείφουν την ανάγκη για τρίτων μερών κάτι που συμβάλει στην μείωση των δαπανών.

Δίχως αμφιβολία οι έξυπνες συμβάσεις εισάγουν μια σειρά πλεονεκτημάτων όπως μας αναφέρουν οι Reyna et al., (2018). Συνοπτικά τα SC προσφέρουν ταχύτητα, ακρίβεια, αποτελεσματικότητα και διαφάνεια και μείωση του κόστους, γεγονός που έχουν ενθαρρύνει την εμφάνιση πολλών νέων εφαρμογών σε μια μεγάλη ποικιλία τομέων. Παρόλο που η Bitcoin προσφέρει μια βασική γλώσσα script, αυτή κρίθηκε ανεπαρκής, γεγονός που οδήγησε στην εμφάνιση νέων πλατφορμών BC με ενσωματωμένη SC λειτουργικότητα.

3.5 Αποκεντρωμένος Αυτόνομος Οργανισμός

Αξίζει ακόμη να σημειωθεί, πως τα έξυπνα συμβόλαια αποτέλεσαν τη γενεσιουργό δύναμη για τους *Αποκεντρωμένους Αυτόνομους Οργανισμούς*[9] *(Distributed Autonomous Organizations - DAO),* οντότητες στο Blockchain των οποίων η συμπεριφορά δύναται να μεταβληθεί εάν ακολουθείται μια συγκεκριμένη διαδικασία που ενσωματωμένη στον κώδικα του συμβολαίου. Ένα χαρακτηριστικό παράδειγμα είναι αυτό ενός έξυπνου συμβολαίου που καλεί με τη σειρά του ένα άλλο συμβόλαιο μέσω της μοναδικής διεύθυνσής του για να εκτελέσει την κύρια λειτουργία του. Αυτή η διεύθυνση εντοπίζεται στο μεταβλητό μέρος της εσωτερικής βάσης δεδομένων του συμβολαίου. Το συμβόλαιο περιέχει επίσης έναν κατάλογο μελών, διευθύνσεις (δημόσια κλειδιά) που ψηφίζουν για τη

[9] Συχνά αναφερόμενων και ως Αποκεντρωμένες Αυτόνομες Εταιρίες/Επιχειρήσεις (Distributed Autonomous Corporations).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συμπεριφορά του. Ένας κανόνας μπορεί να συμπεριληφθεί στο συμβόλαιο, έτσι ώστε εάν η πλειοψηφία αυτών των ψηφοφόρων, ψηφίσουν με κάποιο συγκεκριμένο τρόπο, το συμβόλαιο θα τροποποιήσει τη συμπεριφορά του καλώντας τη διεύθυνση που έλαβε από την πλειονότητα των ψήφων για να εκτελέσει την κύρια λειτουργία της.

3.6 Διπλή ολοκλήρωση (dual integration)

Η διπλή ολοκλήρωση είναι μια διαδικασία που σκοπό έχει τη συσχέτιση μίας πραγματικής – φυσικής σύμβασης και ενός έξυπνου συμβολαίου με τρόπο μοναδικό, επαληθεύσιμο και μη αμφισβητήσιμο. Τα βήματα της είναι τα εξής:

1. Σύνταξη μίας φυσικής σύμβασης
2. Ανάπτυξη ενός έξυπνου συμβολαίου, καταγραφή της διεύθυνσής του στην ΑΚ και συμπερίληψη της διεύθυνσης στην πραγματική σύμβαση
3. Παραγωγή ενός κρυπτογραφικού αποτυπώματος που προκύπτει από την λειτουργία μιας συνάρτησης κατακερματισμού πάνω στη φυσική σύμβαση, καταγραφή του αποτυπώματος και αποθήκευση
4. Αποστολή μιας συναλλαγής στο ΕΣ που περιλαμβάνει το κρυπτογραφικό αποτύπωμα του πραγματικού συμβολαίου στα μεταδεδομένα της, το ΕΣ αποθηκεύει στη συνέχεια αυτή την πληροφορία στη δική του εσωτερική βάση δεδομένων.

Η τελευταία ενέργεια προϋποθέτει ότι το ΕΣ εμπεριέχει μία κατάλληλα προγραμματισμένη συνάρτηση η οποία επιτρέπει σε ένα αναγνωρίσιμο από την δημόσια διεύθυνση του χρήστη να αποθηκεύσει δεδομένα στο ΕΣ (Christidis and Devetsikiotis, 2016).

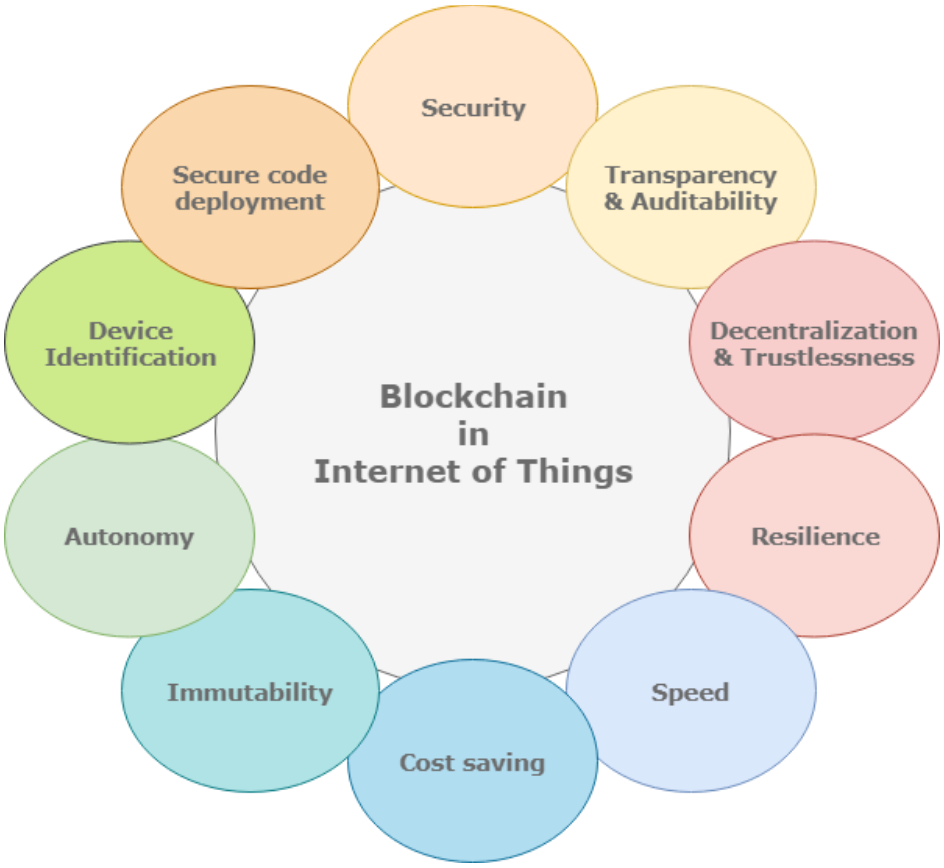
ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 4: Αξιοποίηση Αλυσίδας Καταγραφών στο Διαδίκτυο των Πραγμάτων

Το διαδίκτυο των πραγμάτων και η αλυσίδα καταγραφών θεωρούνται αναδυόμενες έννοιες και τεχνολογίες. Συνάμα μετασχηματίζουν τομείς και δημιουργούν νέες προοπτικές και σενάρια εφαρμογής. Δημιουργείται μία μοναδική ευκαιρία γένεσης νέων εννοιών και τεχνολογιών τα οποία να μοιράζονται τα εγγενή χαρακτηριστικά και των δύο, διερευνώντας τον τρόπο με τον οποίο το IoT μπορεί να επωφεληθεί από τον αποκεντρωμένο χαρακτήρα του Blockchain. Στο παρόν κεφάλαιο μελετούμε τα πλεονεκτήματα που προσφέρει αυτή η συγχώνευση, διακρίνουμε εφαρμογές που ξεχωρίζουν σε διάφορους τομείς, αναλύουμε τις βασικές προκλήσεις και παραθέτουμε μέτρα αντιμετώπισης.

4.1 Οφέλη της ενσωμάτωσης

Αναδύονται πολλά οφέλη από την υιοθέτηση της αλυσίδας καταγραφών από το διαδίκτυο των πραγμάτων. Πολλά από αυτά είναι εμφανή ανά περίπτωση ή εμπίπτουν σε ορισμένα σενάρια. Στην παρούσα υποενότητα γίνεται καταγραφή και συνοπτική ανάλυση των πιο αντιπροσωπευτικών πλεονεκτημάτων που προσφέρει η ενοποίηση των δύο τεχνολογιών.



Οφέλη ενσωμάτωσης των δύο τεχνολογιών

4.1.1 Αποκέντρωση και Αποδιαμεσολάβηση

Ένα βασικό μειονέκτημα, ιδίως σε επίπεδο ασφάλειας των εφαρμογών και πλατφορμών του IoT είναι η εξάρτηση από ένα κεντρικοποιημένο σύννεφο (cloud). Η ενσωμάτωση της τεχνολογίας BC αποτελεί μία πρόταση η οποία θα οδηγήσει στην εξάλειψη πολλών από τα προβλήματα που σχετίζονται με το μοντέλο του κεντρικού cloud (Kshetri, 2017). Μελετώντας τη φύση και τη λειτουργία του BC, παρατηρήσαμε ότι αποτελεί ένα δημόσιο μητρώο καταγραφής όλων των συναλλαγών στο δίκτυο που διατηρείται από διάφορους αποκεντρωμένους κόμβους.

Η τεχνολογία Blockchain επιτρέπει ένα αποκεντρωμένο διομότιμο δίκτυο, όπου οι ομότιμοι κόμβοι δεν χρειάζεται να έχουν έναν αξιόπιστο διαμεσολαβητή για την ομαλή αλληλεπίδραση μεταξύ τους. Στον κόσμο των οικονομικών, όταν οι συναλλασσόμενοι δεν εμπιστεύονται ο ένας τον άλλον, είθισται να υπάρχει μια μοναδική κεντρική αρχή η οποία έχει τη δυνατότητα να εγκρίνει ή να θέτει συγκεκριμένους κανόνες για να γίνει αποδεκτή μία συναλλαγή. Ένα δίκτυο BC δεν ελέγχεται από μία τέτοια αρχή αλλά βασίζεται σε μία κρυπτογραφική απόδειξη και όλες οι συναλλαγές επαληθεύονται και επικυρώνονται με συναίνεση μεταξύ των ομότιμων κόμβων (Pongnumkul, Siripanpornchana and Thajchayapong, 2017). Παρόμοια και στον τομέα IoT, θα βοηθήσει στην πρόληψη σεναρίων όπου μερικές ισχυρές εταιρείες ελέγχουν την επεξεργασία και την αποθήκευση των πληροφοριών ενός τεράστιου αριθμού ανθρώπων (Reyna et al., 2018).

4.1.2 Διαφάνεια και Ελεγξιμότητα

Ένα βασικό χαρακτηριστικό του BC είναι η διαφάνειά του. Όλοι οι συμμετέχοντες έχουν τη δυνατότητα να προσπελάσουν και να δουν όλες τις συναλλαγές καθώς και όλα τα μπλοκ συναλλαγών αφού ο καθένας διατηρεί το δικό του αντίγραφο από το μητρώο καταγραφών (Atlam et al., 2018). Αυτό είναι πράγματι ένα νέο καινοτόμο επίπεδο διαφάνειας που αναμφίβολα συμβάλλει στο χτίσιμο εμπιστοσύνης απέναντι σε ένα IoT σύστημα**.**

Καθώς κάθε μία από τις συναλλαγές στην αλυσίδα καταγραφών επικυρώνεται και καταγράφεται με χρονοσήμανση, είναι δυνατός ο εντοπισμός και η ανίχνευση προηγούμενων καταγράφων μέσω πρόσβασης από οποιοδήποτε κόμβο στο κατανεμημένο δίκτυο. Επιπλέον, ο διαφανής χαρακτήρας του δημόσιου μητρώου καταγραφών που διατηρείται από ένα δίκτυο BC, το καθιστά ασφαλές και ελέγξιμο καθώς όλοι οι χρήστες του δικτύου γνωρίζουν όλες τις συναλλαγές και οι συναλλαγές αυτές δεν μπορούν να αμφισβητηθούν.

4.1.3 Ανθεκτικότητα

Το δίκτυο του BC είναι ανθεκτικό στις βλάβες και τα σφάλματα, καθώς είναι ένα αποκεντρωμένο διομότιμο δίκτυο χωρίς κανένα μοναδικό σημείο αστοχίας. Η ίδια η αλυσίδα είναι ένα μη μεταβλητό και ανθεκτικό μητρώο καταγραφών και οι συναλλαγές που έχουν καταγραφεί στο BC κατόπιν

συναίνεσης μεταξύ των ομότιμων δεν μπορούν πλέον να τροποποιηθούν ή να διαγραφούν. Κάθε κόμβος στο IoT θα έχει το δικό του αντίγραφο από το μητρώο καταγραφών, έτσι, το σύστημα είναι σε θέση να επιβιώσει από δυνητικές επιθέσεις. Ακόμα και αν ένας κόμβος είναι εκτεθειμένος σε κίνδυνο, η αλυσίδα καταγραφών θα διατηρούταν ακέραιη από κάθε άλλο κόμβο. Διατηρώντας μία αναπαραγωγή των δεδομένων σε κάθε κόμβο στο IoT θα βελτιωθούν και οι ανάγκες ανταλλαγής πληροφοριών. Παρ 'όλα αυτά, η υλοποίηση ενός BC εισάγει νέα ζητήματα επεξεργασίας και αποθήκευσης όπως θα δούμε σε επόμενη ενότητα.

4.1.4 Ασφάλεια

Ίσως το πιο προβεβλημένο χαρακτηριστικό από την κείμενη βιβλιογραφία το οποίο προσδίδει σημαντική αξία στην ενσωμάτωση της τεχνολογίας BC στο IoT. Η ασφάλεια δεν αποτελεί ένα ανεξάρτητο χαρακτηριστικό αλλά όπως θα δούμε στην ανάλυση που ακολουθεί μελετάται σε συνάρτηση με άλλα χαρακτηριστικά στα οποία έχουμε ήδη αναφερθεί. Το BC πληροί σε ένα ικανοποιητικό βαθμό την τριάδα ιδιοτήτων CIA (*Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα*)

Η *εμπιστευτικότητα* απαντάται στο γεγονός ότι όλες οι συναλλαγές σε ένα δίκτυο BC ενισχύονται με ισχυρή κρυπτογράφηση. Έτσι, τα δεδομένα πλέον δεν συλλέγονται, αποθηκεύονται και διαχειρίζονται κεντρικά αλλά με τη χρήση αλγορίθμων κρυπτογράφησης, προστατεύονται και μοιράζονται μόνο μεταξύ των συναλλασσόμενων μερών. Σε ένα IoT δίκτυο είναι δύσκολο να εξασφαλισθεί ότι μόνο όσοι έχουν δικαιώματα μπορούν να έχουν πρόσβαση σε συγκεκριμένες πληροφορίες, είτε πρόκειται για απλή ανάγνωση είτε για επεξεργασία. Για να κατοχυρωθεί αυτή η ιδιότητα, η αλυσίδα καταγραφών χρησιμοποιεί ένα μηχανισμό ψευδο-ανωνυμοποίησης (pseudo-anonymization). Ο κίνδυνος είναι ότι εάν αποκαλυφθεί ο κάτοχος ενός κλειδιού, η σύνδεση αυτή θα μπορούσε να αποκαλύψει άλλες συναλλαγές που ανήκουν στην ίδιο κάτοχο. Ως πρόσθετο μέτρο προστασίας, θα πρέπει να χρησιμοποιείται ένα νέο ζεύγος κλειδιών για κάθε συναλλαγή για να μην δύναται να γίνει η σύνδεσή τους με έναν κοινό κάτοχο (Nakamoto, 2008).

Η εγγενής ανωνυμία που προσφέρεται στο BC είναι κατάλληλη για τις περισσότερες περιπτώσεις χρήσης του IoT όπου η ταυτότητα των χρηστών πρέπει να παραμείνει ιδιωτική (Dorri, Kanhere and Jurdak, 2016). Η συγκεκριμένη ιδιότητα έχει επικριθεί στον τομέα των κρυπτονομισμάτων καθώς δίνει πρόσφορο έδαφος στην παράνομη ηλεκτρονική αγορά. Από την άλλη, θα μπορούσε να εκληφθεί ως πλεονέκτημα αν χρησιμοποιηθεί για διαφορετικούς σκοπούς, όπως στα εκλογικά συστήματα ψηφοφορίας.

Όσον αφορά την *ακεραιότητα*, πρέπει να επισημάνουμε ότι η θεμελίωση του BC έχει σχεδιαστεί ώστε να αποθηκεύονται πληροφορίες που δεν μπορούν να τροποποιηθούν ή πιο ορθά ότι είναι πολύ δαπανηρό να συμβεί τροποποίηση μόλις αποθηκευτούν. Η συγκεκριμένη ιδιότητα σχετίζεται άμεσα με τη μη μεταβλητότητα. Ένα δίκτυο BC είναι ζωτικής σημασίας στο περιβάλλον IoT το οποίο

αποτελείται από πολυάριθμες και ετερογενείς συσκευές. Οι πληροφορίες και οι επικοινωνίες μπορούν να εξασφαλιστούν εάν αποθηκεύονται ως συναλλαγές της BC. Η αλυσίδα καταγραφών μπορεί να αντιμετωπίσει τις ανταλλαγές μηνυμάτων των συσκευών ως συναλλαγές, επικυρωμένες μέσω Ευφυών Συμβολαίων, προστατεύοντας έτσι την επικοινωνία μεταξύ των συσκευών (Reyna et al., 2018).

Το κυρίαρχο κεντρικοποιημένο μοντέλο cloud είναι ευάλωτο σε παραποίηση δεδομένων. Η συλλογή δεδομένων σε πραγματικό χρόνο δεν διασφαλίζει ότι οι πληροφορίες θα τύχουν ορθής και αρμόζουσας μεταχείρισης. Ο Kshetri (2017) μας παραθέτουν το παράδειγμα ενός συστήματος ύδρευσης. Στην περίπτωση που διαπιστωθεί ότι υπάρχουν αποδεικτικά στοιχεία μίας παράβασης (δείγματα από αισθητήρες υψηλών επίπεδων συγκέντρωσης μόλυβδου) που μπορεί να οδηγήσουν σε υψηλό κόστος ή αγωγές τότε οι δημόσιοι λειτουργοί ή οι εταιρείες παροχής υπηρεσιών ύδατος μπορεί να λογοκρίνουν, να παραποιήσουν ή και να διαγράψουν δεδομένα και αναλύσεις που αποτελούν ψηφιακά πειστήρια. Και πάλι η χρήση BC μπορεί να αποτρέψει τέτοιες καταστάσεις αφού οι κακόβουλες ενέργειες μπορούν να εντοπιστούν και να προληφθούν.

Η τρίτη ιδιότητα ασφάλειας είναι η διαθεσιμότητα και σχετίζεται άμεσα με την ανθεκτικότητα. Είναι η πιο σαφώς και εύκολα υλοποιήσιμη από τις τρεις, δεδομένου ότι η αλυσίδα καταγραφών είναι εκ σχεδιασμού ένα κατανεμημένο σύστημα, πράγμα που της επιτρέπει να συνεχίζει να λειτουργεί ακόμα και αν κάποιοι κόμβοι δέχονται επίθεση. Μία ωφέλιμη ιδιότητα για το IoT δεδομένου ότι η υπηρεσία πρέπει να είναι πάντα ενεργή όταν ζητηθεί από έναν νόμιμο χρήστη και αυτό απαιτεί την υποδομή επικοινωνίας και τη βάση δεδομένων, δηλαδή του BC. Η διαθεσιμότητα είναι κρίσιμη σε αυτοματοποιημένα συστήματα όπως δίκτυα οχημάτων, μεταποιητικές βιομηχανίες και έξυπνα δίκτυα τα οποία επεξεργάζονται πληροφορίες σε πραγματικό χρόνο. Ο χρόνος εκτός λειτουργίας ενός αισθητήρα μπορεί να οδηγήσει σε απώλειες που κυμαίνονται από απλώς χρηματικές (οικονομικό αντίκτυπο) έως απειλητικές (επικίνδυνες για τη ζωή) καταστάσεις. Ένα μοναδικό σημείο αστοχίας επηρεάζει τη διαθεσιμότητα των υπηρεσιών όταν οι διακομιστές σύννεφων (cloud) είναι εκτός λειτουργίας εξαιτίας σφαλμάτων λογισμικού, επιθέσεων στον κυβερνοχώρο, προβλημάτων τροφοδοσίας, ψύξης και άλλων ζητημάτων. Αντιθέτως, στην περίπτωση του BC, τα δεδομένα αντιγράφονται σε πολλούς υπολογιστές / κόμβους και τα όποια προβλήματα προκύψουν σε μερικούς κόμβους δεν διαταράσσουν τις υπηρεσίες BC. Επομένως, ενδείκνυται για τη διαθεσιμότητα των δεδομένων. Για να πληγεί αυτή η ιδιότητα σε ένα δίκτυο BC, ένα μεγάλο ποσοστό κόμβων πρέπει να είναι κακόβουλοι.

4.1.5 Ταχύτητα

Η αλυσίδα καταγραφών είναι ένα αποκεντρωμένο σύστημα το οποίο εξαλείφει την ανάγκη για μεσάζοντες, εξοικονομώντας έτσι χρόνο και εξαλείφοντας πιθανές συγκρούσεις συμφερόντων. Οι συναλλαγές με μία τράπεζα καθώς και οι διατραπεζικές συναλλαγές μπορεί ενδεχομένως να χρειαστούν μέρες για την επικύρωση και την τελική διευθέτηση. Οι BC συναλλαγές εκτελούνται όλο το

εικοσιτετράωρο – επτά ημέρες την εβδομάδα και μπορούν να μειώσουν το χρόνο ολοκλήρωσης μίας συναλλαγής μέσα σε μερικά λεπτά. Συνδυάζοντας τις τεχνολογίες BC, SC και IoT αυτοματοποιούνται οι χρονοβόρες ροές εργασιών με νέους και μοναδικούς τρόπους, επιτυγχάνοντας κρυπτογραφική επαλήθευση, καθώς και σημαντική εξοικονόμηση κόστους και χρόνου στις διαδικασίες. Έτσι διευκολύνεται αισθητά η υλοποίηση κατανεμημένων εφαρμογές στο IoT όπως για παράδειγμα οι μηχανισμοί αυτόματης πληρωμής (Huckle et al., 2016).

Επίσης, μια συναλλαγή BC διανέμεται σε ολόκληρο το δίκτυο μέσα σε λίγα λεπτά και υποβάλλεται σε επεξεργασία ανά πάσα στιγμή καθ' όλη τη διάρκεια της ημέρας. Άρα σε ένα IoT δίκτυο η προσπέλαση στις πληροφορίες είναι άμεση και δεν χρειάζεται η μεσολάβηση ενός cloud διακομιστή.

4.1.6 Εξοικονόμηση δαπανών

Οι υπάρχουσες υλοποιήσεις IoT είναι ακριβές λόγω του υψηλού κόστους υποδομής και συντήρησης που συνδέεται με την κεντρικοποιημένη αρχιτεκτονική cloud δικτύων, τις μεγάλες μονάδες διακομιστών (large server farms), τα data centers και τον εξοπλισμό δικτύωσης. Ο συνολικός όγκος των παραγόμενων επικοινωνιών που θα πρέπει να διαχειριστούν τα συγκεκριμένα δίκτυα όταν θα υπάρχουν δεκάδες δισεκατομμύρια συσκευές IoT θα αυξήσει σημαντικά αυτό το κόστος. Φαίνεται λοιπόν ότι το IoT αν στραφεί προς την λύση του BC μπορεί να επωφεληθεί σημαντικά από την αρχιτεκτονική του για να μειώσει σε μεγάλο βαθμό τα λειτουργικά κόστη. Αν αξιοποιηθεί κατάλληλα η αλυσίδα καταγραφών μπορεί επιτεύξει επιμερισμό της ισχύς και του αποθηκευτικού χώρου και δεν είναι πολύ ακριβή όσον αφορά τον εξοπλισμό και την υποδομή της.

Ακόμη, η χρήση των κρυπτονομισμάτων που βασίζονται στην τεχνολογία blockchain, θεωρείται ότι φέρνει επανάσταση στις πληρωμές χάρη στα πλεονεκτήματά τους σε σχέση με τα παραδοσιακά νομίσματα. Από την κατάργηση των διαμεσολαβητών, τα τέλη πληρωμής των εμπόρων μπορούν να μειωθούν κάτω από το 1%. Αυτό είναι σημαντικό για τις περιπτώσεις έξυπνων συσκευών που πραγματοποιούν μικρο-πληρωμές.

Και από πλευράς κατασκευαστών έξυπνων συσκευών υπάρχει όφελος από την υιοθέτηση του BC. Με την πάροδο του χρόνο οι συσκευές χρήζουν συντήρησης. Στο παρόν, είναι αρκετά δυσχερές και κοστοβόρο να πραγματοποιηθούν ενημερώσεις λογισμικού σε εκατομμύρια έξυπνες συσκευές.

4.1.7 Μη μεταβλητότητα

Η διατήρηση ενός αμετάβλητου μητρώου καταγραφών είναι ένα από τα κύρια πλεονεκτήματα της τεχνολογίας BC. Όπως είδαμε, η συγκεκριμένη εγγενής ιδιότητα του BC συμβάλει σημαντικά στη διατήρηση της ακεραιότητας των IoT δεδομένων. Οποιεσδήποτε αλλαγές στο κατανεμημένο μητρώο καταγραφών πρέπει να επαληθευτούν από την πλειονότητα των κόμβων του δικτύου. Ως εκ τούτου, τα δεδομένα δεν μπορούν να τροποποιηθούν, αλλοιωθούν ή να διαγραφούν με ευκολία. Η ενσωμάτωση

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ενός μητρώου καταγραφών για τα δεδομένα IoT θα βελτιώσει το επίπεδο της ασφάλειας και της ιδιωτικότητας, χαρακτηριστικά τα οποία αποτελούν μεγάλες προκλήσεις για αυτή την τεχνολογία, καθώς και για όλες σχεδόν τις νέες τεχνολογίες.

Αυτή η ιδιότητα μπορεί να αξιοποιηθεί από διάφορα σενάρια στο διαδίκτυο των πραγμάτων. Όλες οι κεντρικές βάσεις δεδομένων μπορεί να καταστραφούν ή να αλλοιωθούν και συνήθως χρειάζεται η συμβολή ενός τρίτου για να διατηρηθεί η ακεραιότητα των πληροφοριών. Με το BC υπάρχει η δυνατότητα να δημιουργηθεί ένα ιστορικό καταγραφών σχετικά με τη διαμόρφωση και την κατάσταση των έξυπνων συσκευών χωρίς να ανησυχούμε για τα προαναφερθέντα προβλήματα.

4.1.8 Αυτονομία

Η τεχνολογία του BC μπορεί να επιταχύνει τη δημιουργία ενός οικοσυστήματος των υπηρεσιών και της αγοράς δεδομένων στο IoT, όπου οι συναλλαγές μεταξύ ομότιμων είναι δυνατές χωρίς τη διαμεσολάβηση αρχών. Εφαρμογές νέας γενιάς είναι πλέον εφικτές, καθιστώντας δυνατή την ανάπτυξη ευφυών αυτόνομων αγαθών και υλισμικού ως υπηρεσία (HaaS). Το BC μπορεί να επιτρέπει στις συσκευές IoT να επικοινωνούν μεταξύ τους και να πραγματοποιούν συναλλαγές αυτόνομα καθώς κάθε συσκευή έχει δικό της λογαριασμό BC και δεν υπάρχει ανάγκη για αξιόπιστο τρίτο μέρος. Η χρήση έξυπνων συμβολαίων ενδείκνυται για την ανάπτυξη αυτόνομων αντικειμένων ή συσκευών IoT, τα οποία θα μπορούν να εκτελούν οικονομικές συναλλαγές, να πουλούν τα δεδομένα τους ή να διαχειρίζονται τη συντήρησή τους κα.

Μέχρι τώρα υπάρχουν αρκετά παραδείγματα τόσο σε ερευνητικό επίπεδο αλλά και με τη μορφή πιλοτικών εμπορικών υλοποιήσεων όπως το εγχείρημα της IBM, ονόματι ADEPT, ένα κατανεμημένο δίκτυο όπου οι ηλεκτρικές συσκευές σε ένα σπίτι μπορούν να αναγνωρίσουν προβλήματα στην ομαλή λειτουργία τους και να εφαρμόσουν αναβάθμιση του λογισμικού τους. Η πλατφόρμα Filament έχει κατασκευάσει μια υποδομή βασισμένη στην τεχνολογία blockchain που επιτρέπει στις συσκευές να επικοινωνούν μεταξύ τους μεταξύ τους, να παρέχουν μικρο-υπηρεσίες (microservices) να πραγματοποιούν μικρο-πληρωμές (micro-payments) καθώς και να εκτελούν αυτόματα ενέργειες με ασφάλεια. Επίσης, η Slock.it στοχεύει στην οικοδόμηση μιας οικονομίας όπου οντότητες του διαδικτύου των πραγμάτων θα μπορούν να ενοικιαστούν με ασφάλεια και γρήγορα χωρίς την παρουσία οποιασδήποτε αρχής.

4.1.9 Ταυτοποίηση Συσκευής

Χρησιμοποιώντας ένα κοινό σύστημα BC οι συμμετέχοντες είναι σε θέση να ταυτοποιήσουν κάθε συσκευή. Σε προηγούμενη υποενότητα είδαμε ότι άπαξ και οι αρχικές πληροφορίες που εισάγονται σε μία αλυσίδα καταγραφών είναι ακριβείς, μπορεί να επιτευχθεί η μη μεταβλητότητα των δεδομένων. Επομένως, το βασικό ζήτημα είναι η διαβεβαίωση ότι τα προς αποθήκευση δεδομένα ανταποκρίνονται

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

στις ιδιότητες των φυσικών αγαθών, φυσικών προσώπων (διαπιστευτήρια), της χρήσης πόρων (ενέργεια και εύρος ζώνης μέσω συσκευών IoT) και άλλων σχετικών γεγονότων. Αυτή η περίπτωση μπορεί να αντιμετωπιστεί σχετικά εύκολα για τις περισσότερες συσκευές IoT. Παραδείγματος χάριν, ένα ιδιωτικό BC μπορεί να χρησιμοποιηθεί για την αποθήκευση κρυπτογραφικών τιμών κατακερματισμού (cryptographic hashes) από το υλικολογισμικό κάθε συσκευής. Ένα τέτοιο σύστημα δημιουργεί μία μόνιμη εγγραφή της διαμόρφωσης και της κατάστασης της συσκευής. Αυτή η εγγραφή μπορεί να χρησιμοποιηθεί για να επαληθεύσει ότι μια δεδομένη συσκευή είναι γνήσια και ότι το λογισμικό και οι ρυθμίσεις της δεν έχουν αλλοιωθεί ή παραβιαστεί. Μόνο τότε επιτρέπεται στη συσκευή να συνδεθεί με άλλες συσκευές ή υπηρεσίες. Δηλαδή, το BC μπορεί να παρέχει αξιόπιστη κατανεμημένη αυθεντικοποίηση και εξουσιοδότηση συσκευών για τις εφαρμογές IoT.

4.1.10 Ασφαλής ανάπτυξη κώδικα

Εκμεταλλευόμενοι την ασφαλή και αμετάβλητη αποθήκευση (ιδιότητα της μη μεταβλητότητας), το BC μπορεί επίσης να χρησιμοποιηθεί για τη διατήρηση μητρώου ενημερώσεων, patch και την αντικατάσταση εξαρτημάτων που εφαρμόζονται σε οποιοδήποτε προϊόν ή συσκευή καθ' όλη τη διάρκεια ζωής του. Με παρόμοιο τρόπο και ο κώδικας μπορεί να παραμείνει ακέραιος και να προωθείται με ασφάλεια στις συσκευές.

Είναι γνωστό ότι μεμονωμένα κάθε συσκευή IoT παρουσιάζει συγκεκριμένες ευπάθειες σε κυβερνοεπιθέσεις λόγω πολλών παραγόντων, όπως η μακροβιώτητα, η έλλειψη φυσικής προστασίας, οι ελλείψεις υλισμικού ή η υποτυπώδης υλοποίηση Διεπαφών Ανθρώπου – Μηχανής (Boudguiga et al., 2017). Επομένως, ενσωματώνοντας ένα BC, οι κατασκευαστές μπορούν να παρακολουθούν την κατάσταση των συσκευών IoT (έλεγχος ακεραιότητας λογισμικού) και να διανέμουν με ασφάλεια σε αυτές διαθέσιμες ενημερώσεις (είτε συγχρονισμένα είτε κατά το χρόνο εκτέλεσης).

4.2 Εφαρμογές

4.2.1 Αυτόνομη Αποκεντρωμένη Διομότιμη Τηλεμετρία

IBM σε συνεργασία με την Samsung Electronics έκανε από τα πρώτα βήματα για κινηθεί προς την κατεύθυνση των BC λύσεων για το IoT. Το 2015 η εταιρεία πρότεινε ένα έργο με τίτλο ADEPT, δηλαδή Αυτόνομη Αποκεντρωμένη Διομότιμη Τηλεμετρία (Autonomous Decentralized Peer-to-Peer Telemetry). Η ADEPT στοχεύει στην εφαρμογή ενός αποκεντρωμένου, αυτόνομου, εύρωστου, κλιμακούμενου και ασφαλούς πλαισίου για το IoT που δεν έχει κανένα σημείο αποτυχίας. Σύμφωνα με τους συγγραφείς, η ADEPT παρουσιάζεται περισσότερο ως σημείο εκκίνησης για περεταίρω διερεύνηση παρά ως έτοιμη εμπορική υλοποίηση. Περιγράφει διαφορετικές περιπτώσεις πρακτικής χρήσης του συστήματος, όπως ένα πλυντήριο που χρησιμοποιεί SC για να αγοράζει απορρυπαντικό όταν τελειώνουν οι προμήθειες του.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Η αρχιτεκτονική ADEPT βασίζεται στο πρωτόκολλο TeleHash για την ανταλλαγή μηνυμάτων, στο BitTorrent για το διαμοιρασμό αρχείων και στην πλατφόρμα του Ethereum για την εκτέλεση έξυπνων συμβάσεων και τη δημιουργία αποκεντρωμένων αυτόνομων οργανισμών (DAOs). Το προτεινόμενο σύστημα στοχεύει στην επίλυση των προβλημάτων που παρουσιάζουν τα συμβατικά δίκτυα IoT σχετικά με την εμπιστοσύνη σε μια κεντρική οντότητα, ένα μοναδικό σημείο αποτυχίας, ζητήματα ιδιωτικότητας των χρηστών και δεδομένων τους, σφάλματα που προκαλούνται από τις ανθρώπινες αλληλεπιδράσεις κα. Προσπαθεί επίσης να παρέχει διαχείριση ταυτότητας και έλεγχο πρόσβασης καθορισμένο από τον χρήστη και δυνατότητα κλιμάκωσης. Στα θετικά του συγκαταλέγονται ότι είναι framework ανοιχτού κώδικα και άρα η υιοθέτησή του θα επισπευσθεί και ότι χρησιμοποιεί αποδεδειγμένες τεχνολογίες (BitTorrent, TeleHash, Ethereum). Υπάρχουν ορισμένα κενά όσον αφορά την ενοποίησή του με το IoT. Καθότι πρόκειται για μία ερευνητική μελέτη χρήζει περαιτέρω δοκιμών για να εξασφαλίσει η αξιοπιστία του όσον αφορά την ασφάλεια και την αποδοτικότητα (Karst and Brodar, 2017).

4.2.2 Αυτοδιαχειριζόμενα Δίκτυα Μεταφορών

Ένας από τους υποσχόμενους IoT τομείς είναι οι έξυπνες μεταφορές που σχετίζεται με την κοινοποίηση των συνθηκών κυκλοφορίας, τον ευφυή έλεγχο των διαδρομών, την απομακρυσμένη παρακολούθηση του οχήματος και το συντονισμό των αυτοκινητοδρόμων. Τα ad hoc δίκτυα οχημάτων, αναφερόμενα ως VANET (Vehicular-Ad-hoc-NETworks) συχνά επικεντρώνονται σε κεντρικοποιημένες αρχιτεκτονικές δικτύου που ελέγχονται από κυβερνητικούς οργανισμούς. Οι κεντρικές διαχειριστικές αρχές αποτελούν μοναδικά σημεία αποτυχίας, αξιόλογους στόχους για επιτιθέμενους και προσφέρουν χαμηλότερη προστασία της ιδιωτικότητας των χρηστών. Για την αποφυγή τέτοιων ζητημάτων, οι Leiding, Memarmoshrefi και Hogrefe (2016) προτείνουν ένα αποκεντρωμένο, αυτοδιαχειριζόμενο VANET δίκτυο που στηρίζεται στα SC του Ethereum και σε έναν μηχανισμό αυθεντικοποίησης.

Τα δομικά στοιχεία της αρχιτεκτονικής περιλαμβάνουν: α) οχήματα, β) επί του οχήματος μονάδες (on board units - OBUs) για την ανταλλαγή πληροφοριών με τις RSU ή άλλα OBU μέσω ασύρματης επικοινωνίας μικρής εμβέλειας ή άλλων ραδιοφωνικών τεχνολογιών, γ) μονάδες εφαρμογών (application units - AUs) επιμερισμένες με την εκτέλεση εφαρμογών που μπορούν να αξιοποιήσουν τις δυνατότητες επικοινωνίας του OBU και δ) επί του δρόμου μονάδες (road side units - RSUs) τοποθετημένες σε ειδικές θέσεις όπως σταυροδρόμια υπεύθυνες να αλληλεπιδρούν με άλλες συσκευές για την παροχή επικοινωνίας εντός του δικτύου υποδομής.

Υπάρχει επικοινωνία είτε μεταξύ οχημάτων μέσω των RSU είτε απευθείας μέσω της υποδομής του δικτύου. Τα SC χρησιμοποιούνται για την επιβολή συγκεκριμένων κανόνων ή την παροχή διαφόρων υπηρεσιών. Κάθε κόμβος είναι καταχωρημένος και αναγνωρισμένος από τη διεύθυνση του Ethereum, δηλαδή από ένα hash του δημόσιου κλειδιού του. Για την πρόσβαση στις παρεχόμενες υπηρεσίες, κάθε κόμβος πρέπει να πληρώσει με κρυπτονομίσματα Ethers. Έτσι επιλύεται το ζήτημα της

χρηματοδότησης της υποδομής του δικτύου. Επίσης, η πληρωμή που πραγματοποιείται από τους χρήστες χρησιμεύει ως κίνητρο για τους προμηθευτές που παρέχουν εφαρμογές και τις συναφείς με αυτές υπηρεσίες. Σε ένα σενάριο πραγματικού κόσμου, ο λογαριασμός Ethereum ενός χρήστη μπορεί να χρησιμοποιηθεί για την πραγματοποίηση αυτοματοποιημένων πληρωμών ασφάλισης αυτοκινήτου, καταβολή φόρων, εγγραφής σε υπηρεσίες, πρόσθετων υπηρεσιών όπως επικαιροποίηση κυκλοφορίας σε πραγματικό χρόνο και πληρωμής προστίμων για παραβίαση της κυκλοφορίας.

Υπάρχουν αρκετά κενά στο σενάριο των VANET. Δεν αποσαφηνίζεται πώς εκτελείται το πρωτόκολλο συναίνεσης και ποιες πληροφορίες θα περάσουν ως συναλλαγές στο BC και αν σε αυτές θα συγκαταλέγονται και οι επικοινωνίες μεταξύ οχημάτων. Ακόμη δεν αναφέρεται αν τα οχήματα είναι εξορύκτες ή ποια άλλη οντότητα θα αναλάβει την εξόρυξη. Δεν γνωρίζουμε επίσης, τί χρονικές καθυστερήσεις μπορεί να ανεχθεί η υλοποίηση και ποια είναι η επίπτωση σε υπηρεσίες πραγματικού χρόνου.

4.2.3 Ασφαλής Λειτουργία Έξυπνης Πόλης

Οι έξυπνες πόλεις μπορούν να προσφέρουν καινοτόμες λύσεις και πιο άμεση αλληλεπίδραση και συνεργασία μεταξύ των πολιτών και της τοπικής αυτοδιοίκησης. Με τη ραγδαία αύξηση του πληθυσμού δυσχεραίνεται το ζήτημα της επικοινωνίας και για να αντιμετωπιστεί το φαινόμενο αυτό, οι πόλεις επικεντρώνονται στις σύγχρονες τεχνολογίες, στοχεύουν στη μείωση του κόστους, στη βέλτιστη χρήση των πόρων και στη δημιουργία ενός πιο εύχρηστου αστικού περιβάλλοντος.

Η διαχείριση της έξυπνης πόλης βασίζεται στη συνεχή ανταλλαγή δεδομένων μεταξύ έξυπνων συσκευών, οι οποίες συλλέγουν αυτά τα δεδομένα από τους πολίτες και το περιβάλλον. Ο κίνδυνος επίθεσης σε κρίσιμες υπηρεσίες μιας έξυπνης πόλης είναι πολύ υψηλός και, εάν συμβεί, θα μπορούσε να προκαλέσει σοβαρή ζημία στην ιδιωτική ζωή των πολιτών. Μία υποψήφια λύση σε αυτά τα ζητήματα αποτελεί και το BC. Οι Biswas και Muthukkumarasamy (2016) παρουσιάζουν μια επισκόπηση ενός πλαισίου ασφάλειας τεσσάρων επιπέδων:

1. Φυσικό επίπεδο: αποτελείται από τις συσκευές της έξυπνης πόλης οι οποίες φέρουν αισθητήρες και ενεργοποιητές. Λόγω της έλλειψης ενός καθολικού προτύπου για έξυπνες συσκευές εγείρονται ζητήματα δυσκολίας στο διαμοιρασμού δεδομένων που λαμβάνονται από ετερογενείς συσκευές και την ενοποίηση αυτών των συσκευών ώστε να παρέχεται μεταξύ τους διασυνδεσιμότητα.
2. Επίπεδο επικοινωνιών: τα δίκτυα της πόλης χρησιμοποιούν διάφορα πρωτόκολλα επικοινωνίας τα οποία πρέπει να είναι συμβατά με αυτά του BC για να υπάρξει ασφάλεια και ιδιωτικότητα. Προτείνεται η μετατροπή των συναλλαγών σε μπλοκ με τη χρήση του TeleHash, διαμοιρασμός δεδομένων μέσω του BitTorrent και το Ethereum για την υλοποίηση SC.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

3. Επίπεδο βάσης δεδομένων: η αποθήκευση των δεδομένων που θα βασίζεται στην αλυσίδα καταγραφών. Προτείνονται τα ιδιωτικά BC για την εξασφάλιση της επεκτασιμότητας, των επιδόσεων και της ασφάλειας για εφαρμογές σε πραγματικό χρόνο, όπως τα συστήματα κυκλοφορίας.
4. Επίπεδο Διεπαφής: οι έξυπνες εφαρμογές της πόλης που μέσω αλληλεπίδρασης θα λαμβάνουν αποτελεσματικές αποφάσεις.

Οι συγγραφείς ισχυρίζονται ότι η ενσωμάτωση του BC στην έξυπνη πόλη θα προσφέρει μια κοινή πλατφόρμα όπου όλες οι συσκευές θα μπορούν να επικοινωνούν με ασφάλεια. Επιπλέον, η χρήση blockchain θα αποτρέψει τη διαθεσιμότητα δεδομένων και τις επιθέσεις ακεραιότητας δεδομένων. Παρέχει επίσης ένα αξιόπιστο αρχείο καταγραφής των συναλλαγών, το οποίο μπορεί να χρησιμοποιηθεί αργότερα για σκοπούς ελέγχου.

Μειονεκτήματα. Το μειονέκτημα είναι ότι δεν υπάρχει μία πρακτική εφαρμογή της συγκεκριμένης πρότασης, δηλαδή δεν υπάρχει ποιοτική ή ποσοτική ανάλυση των απαιτήσεων σε υπολογιστικούς πόρους, συμφόρηση μετάδοσης δεδομένων. Επιπλέον, δεν καθορίζεται ποια πλατφόρμα blockchain και ποιο πρωτόκολλο συναίνεσης είναι καταλληλότερα στην εφαρμογή της έξυπνη πόλης.

4.2.4 Ασφαλής Ενημέρωση Υλικολογισμικού Έξυπνων Συσκευών

Ο εκρηκτικός αριθμός συσκευών που συμμετέχουν σε δίκτυα IoT δυσκολεύει τη διαχείριση. Οι συσκευές μπορεί να έχουν πλήρη ή περιορισμένη συνδεσιμότητα στο Διαδίκτυο. Ανεξαρτήτως, είναι εκτεθειμένες σε επιτιθέμενους και γενικά δεν έχουν "ασφάλεια από το σχεδιασμό". Έτσι, είναι απαραίτητο να μπορούν να ενημερώνονται, να επιδιορθώνουν τις ευπάθειές τους και να εμποδίζουν τους κακόβουλους χρήστες να τις μετατρέψουν σε botnets. Το BC μπορεί επίσης να χρησιμοποιηθεί για την καταχώρηση ενημερώσεων, επιδιορθώσεων και αντικατάστασης εξαρτημάτων που εφαρμόζονται σε οποιοδήποτε προϊόν ή συσκευή καθ' όλη τη διάρκεια ζωής του. Πιο συγκεκριμένα, οι συσκευές IoT έχουν ενσωματωμένο κάποιο υλικολογισμικό που συνήθως ενημερώνεται για να διορθώνει σφάλματα, να αποτρέπει επιθέσεις ή απλώς να βελτιώνει κάποια λειτουργικότητα. Παραδοσιακά, έπρεπε να ενημερώνονται χειροκίνητα ή με ασύρματες ενημερώσεις. Με το BC οι κατασκευαστές μπορούν να παρακολουθούν την κατάσταση των συσκευών και τις ενημερώσεις με υψηλότερη εμπιστοσύνη.

Υπάρχουν αρκετές προσπάθειες σχεδιασμού και υλοποίησης υποδομών ενημέρωσης συσκευών IoT που βασίζονται στο BC που να επιτρέπουν στις συσκευές να ελέγχουν με ασφάλεια την έκδοση του λογισμικού και την ακεραιότητά τους και στη συνέχεια να κατεβάζουν το πιο πρόσφατο λογισμικό. Σύμφωνα με τους Boudguiga et al., (2017) η υποδομή επικαιροποίησης θα πρέπει να εφαρμόζει τις ιδιότητες της τριάδας της CIA και διερευνούν πώς η χρήση μιας υποδομής BC μπορεί να ικανοποιήσει αυτές τις απαιτήσεις, με έμφαση στη διαθεσιμότητα.

Η αρχιτεκτονική εμπεριέχει ένα σύνολο ελεγκτικών[10] κόμβων που μπορούν να ανήκουν σε εθνικούς οργανισμούς στον τομέα του κυβερνοχώρου ή σε εταιρείες πιστοποίησης, συσκευές IoT με περιορισμένους πόρους και τους κατασκευαστές. Οι τελευταίοι προωθούν μία ενημέρωση στο BC με τη μορφή μίας συναλλαγής αφού ενσωματώσουν κάποια αναγνωριστικά για λόγους ασφάλειας. Μια συσκευή ρωτά περιοδικά το BC επιλέγοντας τυχαία έναν από τους υποστηρικτικούς κόμβους της να ελέγξει εάν έχουν τοποθετηθεί ενημερώσεις για αυτήν. Αυτοί οι κόμβοι λαμβάνουν τον κώδικα μίας νέας ενημέρωσης απευθείας από τον κατασκευαστή. Στη συνέχεια, ελέγχουν την ακεραιότητα της υπογραφής του κατασκευαστή, αλλά και τον κώδικα για σφάλματα και γνωστές επιθέσεις. Μια συσκευή θα κατεβάσει μία νέα ενημέρωση αφού λάβει έγκριση από ένα αριθμό ελεγκτικών κόμβων και άνω.

Η παρούσα λύση δεν περιλαμβάνει εχέγγυα εμπιστευτικότητας όπως μηχανισμούς κρυπτογράφησης κατά τη μετάδοση ή τί συμβαίνει στην περίπτωση που κάποιος αποκτήσει παράνομα πρόσβαση σε μία συσκευή. Επίσης υπάρχει το ενδεχόμενο συμφόρησης λόγω του αυξημένου αριθμού συναλλαγών έγκρισης από τους ελεγκτικούς κόμβους και δεν αναφέρεται εάν καταγράφονται όλα τα μηνύματα που σχετίζονται με την πιστοποίηση του λογισμικού πώς θα διαχειριστεί το σύστημα το συνεχώς αυξανόμενο μέγεθος του BC. Δεν υπάρχει πληροφόρηση σχετικά με πολυπλοκότητα της επικοινωνίας, κατανάλωση ενέργειας, τη χρονική καθυστέρηση μίας και το πρωτόκολλο BC.

4.2.5 Αποδοτική Διαχείριση Βιομηχανικής Παραγωγής

Με βάση τους Panarello et al. (2018), έξυπνη βιομηχανία μπορεί να οριστεί η υιοθέτηση ψηφιακών τεχνολογιών ικανών να βελτιώσουν τη διασύνδεση και τη συνεργασία των πόρων που χρησιμοποιούνται κατά τις επιχειρησιακές διαδικασίες που διανέμονται κατά μήκος της αλυσίδας αξίας. Η Filament, ένας πάροχος BC λύσεων για το IoT, έχει κατασκευάσει ασύρματους αισθητήρες, τα λεγόμενα Taps, που μπορούν να επικοινωνήσουν με συσκευές σε απόσταση 10 μιλίων. Οι εφαρμογές της περιλαμβάνουν αισθητήρες συνδεδεμένους σε ένα αποκεντρωμένο σύστημα και χρήση αυτόνομων έξυπνων συμβολαίων. Σε αυτό το πλαίσιο ο Kshetri (2017) διαβλέπει μία νέα χρήση στην επόμενη γενιά του Βιομηχανικού IoT όπου Taps θα τοποθετούνται σε απομακρυσμένες τοποθεσίες που εκτελούνται γεωτρήσεις. Ένα γεωτρύπανο βάσει προκαθορισμένων συνθηκών θα αναγνωρίζει την ανάγκη αίτησης ενός νέου εξαρτήματος και το παραγγέλνει αυτόματα μέσω ενός drone.

Οι Bahga και Madisetti (2016) πρότειναν ένα καινοφανές σύστημα BC πλατφόρμας για το Βιομηχανικό IoT (BPIIoT) η οποία ήρθε να ενισχύσει τη βιομηχανία με βάση το cloud (CBM), ένα νέο παράδειγμα παραγωγής που στοχεύει στην παροχή παραγωγικών πόρων και δυνατοτήτων ως υπηρεσία. Η αρχιτεκτονική αποτελείται από συσκευές IoT που είναι κόμβοι και έχουν λογαριασμό στο BC, χρήστες

[10] Οι συγγραφείς χρησιμοποιούν τον όρο "innocuousness checking nodes", όπου innocuousness αποδίδεται ως *η ιδιότητα του να είναι εντελώς ακίνδυνο.*

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

– καταναλωτές, το cloud δίκτυο και SC που λειτουργούν ως συμφωνίες μεταξύ των καταναλωτών και των βιομηχανικών πόρων για την παροχή υπηρεσιών κατασκευής κατά παραγγελία. Αυτό που κάνει τη διαφορά για τις βιομηχανικές μηχανές στην προτεινόμενη πλατφόρμα είναι οι συσκευές IoT καθώς επιτρέπουν στις υπάρχουσες μηχανές να επικοινωνούν με το cloud καθώς και το δίκτυο BC. Το BPIIoT μπορεί να αξιοποιηθεί για διάφορες εφαρμογές όπως: α) Βιομηχανική Παραγωγή Κατά Παραγγελία, β) Ευφυείς Διαγνωστική και Συντήρηση Μηχανών, γ) Ιχνηλασιμότητα, δ) Παρακολούθηση Αλυσίδας Εφοδιασμού, ε) Πιστοποίηση Προϊόντων, στ) Συναλλαγές από Καταναλωτή σε Μηχάνημα και Μηχανή σε Μηχανή, ζ) Παρακολούθηση Ταυτότητας και Φήμης του Προμηθευτή, η) Μητρώο Καταγραφής Αγαθών και Εμπορευμάτων.

Επιπλέον, οι συγγραφείς πρότειναν μια περίπτωση χρήσης συντήρησης μηχανήματος και έξυπνη εφαρμογή διάγνωσης. Το σύστημα βασίζεται στο Ethereum και οι συμβάσεις αναπτύσσονται σε γλώσσα Solidity. Τα οφέλη αυτής της επιλογής ενσωματώνονται στην τεχνολογία BC και, ως εκ τούτου, το σύστημα πάσχει από τα ίδια προβλήματα με το Ethereum, και συγκεκριμένα: ευπάθειες των SC, ζητήματα ιδιωτικότητας, αποτελεσματικότητα και έλλειψη κυβερνητικής ρύθμισης. Ακόμη, για τη διασφάλιση των συσκευών, υπάρχουν κενά. Δεν διασαφηνίζεται αν κάποιος χρήστης μπορεί να εκμεταλλευτεί το σύστημα και τί δικλείδες ασφαλείας υπάρχουν. Στην πραγματικότητα, οι συγγραφείς έκαναν επίδειξη μίας περιορισμένη εφαρμογής οπότε υπολείπεται ελέγχου σε πιο αντιπροσωπευτικές συνθήκες παραγωγής.

4.2.6 Ασφαλής Λειτουργία Έξυπνου Σπιτιού

Το έξυπνο σπίτι ενδέχεται να προσφέρει ένα ολοκληρωμένο σύστημα αυτοματισμού, να βελτιώσει την άνεση, την ασφάλεια και την κατανάλωση των ανθρώπων που το χρησιμοποιούν. Επιτρέπει στους ιδιοκτήτες να διαχειρίζονται πολλές λειτουργίες ακόμα από απόσταση. Είναι εφικτός ο προγραμματισμός, η ενεργοποίηση, η απενεργοποίηση και ο έλεγχος των συσκευών εντός του σπιτιού χωρίς να κρίνεται απαραίτητη η φυσική παρουσία όσων διαμένουν εκεί. Οι κάτοικοι έχουν τη δυνατότητα να καθορίζουν τα επίπεδα κατανάλωσης ενέργειας του σπιτιού και να προσαρμόζουν το οίκημα στις προτιμήσεις και τις συνήθειες του ιδιοκτήτη. Στα έξυπνα σπίτια είναι πιθανό να προκύψουν προκλήσεις όσον αφορά την προστασία της ιδιωτικής ζωής και εν γένει θέματα ασφάλειας. Εγείρεται το ζήτημα της επάρκειας σε γνώσεις, ικανότητες και εργαλεία ενός μέσου καταναλωτή για να αμυνθεί αν διαπιστώσει ότι είναι θύμα μίας εξωτερικής επίθεσης ασφαλείας στο IoT περιβάλλον του σπιτιού.

Ένας πεπειραμένος κακόβουλος χρήστης έχει διάφορα είδη επιθέσεων που θα μπορούσε να επιχειρήσει με απώτερο σκοπό να αποκτήσει πρόσβαση σε εμπιστευτικά και ιδιωτικά δεδομένα των χρηστών του σπιτιού. Κάποια από αυτά είναι το κακόβουλο λογισμικό όπως οι ιοί κερκόπορτας, η επίθεση Man-In-The-Middle σε περίπτωση μη κρυπτογραφημένων πρωτοκόλλων επικοινωνίας, και η ηλεκτρονική παρείσφρηση στον κωδικό πρόσβασης της συσκευής δρομολογητή στο σπίτι. Σε πολλές περιπτώσεις, το "χακάρισμα" μιας συσκευής μπορεί να ανοίξει εν αγνοία του χρήστη μία δίοδο να παραβιαστούν και

άλλα άτομα. Βάση ορισμένων μελετών, η κρυπτογράφηση των παραγόμενων δεδομένων από έναν αισθητήρα δεν είναι αρκετή. Μπορεί ο αισθητήρας να αποκαλύψει πολλές πληροφορίες σχετικά με τις δραστηριότητες των κατοίκων αν αναλυθούν τα μεταδεδομένα τους και τα πρότυπα της κίνησης του δικτύου (Panarello et al., 2018). Σε επόμενη υποενότητα αναλύεται ένα σενάριο που ισχυρίζεται ότι επιλύει τα σημαντικότερα από αυτά τα ζητήματα.

4.2.7 Αυτόνομη Αγορά Ενέργειας

Το BC, με βάση το Energy Web Foundation (2018), το BC έχει τη δυνατότητα να διαδραματίσει κρίσιμο ρόλο στο μετασχηματισμό των αγορών ενέργειας. Παρακάτω παρατίθενται τρία χαρακτηριστικά παραδείγματα όπου το BC αξιοποιείται από τον ενεργειακό τομέα.

Κοινοτική ηλιακή ενέργεια: Εφευρέθηκε για να παρέχει σε μία κοινότητα ανθρώπων έναν τρόπο να αξιοποιήσουν τα οφέλη της ηλιακής ενέργειας μέσω μίας επίγειας εγκατάστασης η οποία τείνει να είναι φθηνότερη από μία αντίστοιχη στον τελευταίο όροφο μίας πολυκατοικίας και η ιδιοκτησία και τα οφέλη της οποίας μοιράζονται στην κοινότητα. Από την ενσωμάτωση του BC προκύπτουν οι ακόλουθες βελτιώσεις: α) μείωση συμπληρωματικών χρεώσεων[11] με τη χρήση SC για την αυτόματη διαχείριση κυριότητας αγαθών, πληρωμών και διακυβέρνησης, β) γεωγραφική διεύρυνση / επέκταση της αγοράς πέρα των κοινοτήτων, γ) εύκολη ρευστοποίηση της παραγόμενης ενέργειας αλλά και των μετοχών στο έργο (χωρίς γραφειοκρατία), δ) λόγω των παραπάνω, καλύτερη αξιοποίηση και ανάπτυξη των ανανεώσιμων πηγών ενέργειας.

Αποκέντρωση κι επανασχεδιασμός ηλεκτρικού δικτύου: Η χρήση έξυπνων συσκευών για τη διαχείριση του ηλεκτρικού δικτύου, στο παρόν είναι μία διαδικασία ακριβή, μη ασφαλής και ενέχει δύσκολη ενσωμάτωση των συσκευών σε αυτό. Με το BC θα μπορούσε να επιτευχθεί α) αυτόματη σύνδεση μιας νέας συσκευής ή ενός ηλεκτρικού υποδικτύου σε μια ασφαλή, αποκεντρωμένη πλατφόρμα που προτρέπει τους χρήστες μέσω των συσκευών τους να χρησιμοποιούν ή όχι ηλεκτρική ενέργεια σε συγκεκριμένες χρονικές στιγμές μέσω κοστολόγησης σε πραγματικό χρόνο καθώς και β) συμμετοχή σε νέες αγορές ηλεκτρικής ενέργειας. Έτσι, κάθε συσκευή δύναται να έχει ξεχωριστή ταυτότητα, συνδεδεμένη με τις προτιμήσεις του χρήστη, οι ενέργειές της να ιχνηλατούνται διαφανώς και μέσω των SC τα έσοδα μπορούν να διαιρεθούν και να διανεμηθούν αυτόματα.

Παρακολούθηση πιστοποιητικών ανανεώσιμης ενέργειας: Τα πιστοποιητικά ανανεώσιμης ενέργειας ήρθαν στο φως σε διάφορες χώρες ώστε να ανταποκριθούν στα εμπορικά συμφέροντα και στις κυβερνητικές ρυθμίσεις. Όμως παρουσιάζουν χειροκίνητη και δαπανηρή διαχείριση, καθιστώντας τις αγορές αδιαφανείς, υψηλού κόστους και απρόσιτες για τους περισσότερους "μικρότερους" συμμετέχοντες. Η αξιοποίηση του BC θα επιφέρει α) τη συσχέτιση κάθε αγαθού με μία μοναδική

[11] Επιπλέον χρεώσεις πέραν του εξοπλισμού και της εγκατάστασής του όπως νομικές αμοιβές, έξοδα αδειοδότησης, έξοδα διασύνδεση, κόστη διαχείρισης, κόστος απόκτησης από τον πελάτη.

ψηφιακή ταυτότητα, β) την παρακολούθηση της διαδικασίας παραγωγής του και σύνδεσή του με τον κάτοχό του, γ) τη χρήση ΕΣ για υπολογισμό οφέλους από τις παραγόμενες kWh σε σύγκριση με την εξοικονόμηση άνθρακα ή για αυτοματοποιημένη αγορά πιστώσεων βάσει του προφίλ κατανάλωσης και δ) τη διατήρηση της ιδιωτικότητας μέσω προαιρετικής χρήσης κρυπτογραφίας. Εντέλει η ψηφιοποίηση των οντοτήτων προσφέρει διαφάνεια και εξοικονόμηση δαπανών.

Στα προαναφερθέντα σενάρια η χρήση IoT προσθέτει διευκόλυνση και αυτονομία ιδιαιτέρως στη δεύτερη περίπτωση με τη χρήση έξυπνων συσκευών. Οι έξυπνες συσκευές θα μπορούσαν να ενεργήσουν ως αυτόνομοι πράκτορες και να ρυθμιστούν ώστε να συμμετέχουν αυτόνομα σε αγορές ενέργειας. Επιπρόσθετα, σε σύμπραξη με άλλες συσκευές από γειτονικά σπίτια μπορούν να αγοράζουν μαζικά ηλεκτρική ενέργεια για την επίτευξη χαμηλότερου κόστος. Ακόμη το IoT θα συμβάλει καθοριστικά Σε επόμενη υποενότητα αναλύεται ένα σενάριο αγοράς ενέργειας.

4.2.8 Διαφανής Διαχείριση της Εφοδιαστικής Αλυσίδας

Το BC είναι μία πολλά υποσχόμενη τεχνολογία για τη SCM. Έρευνα των Chang, Iakovou και Shi, (2019) έδειξε πως μπορεί να επιλύσει βασικά ζητήματα που ταλανίζουν τον κλάδο. Πιο συγκεκριμένα:

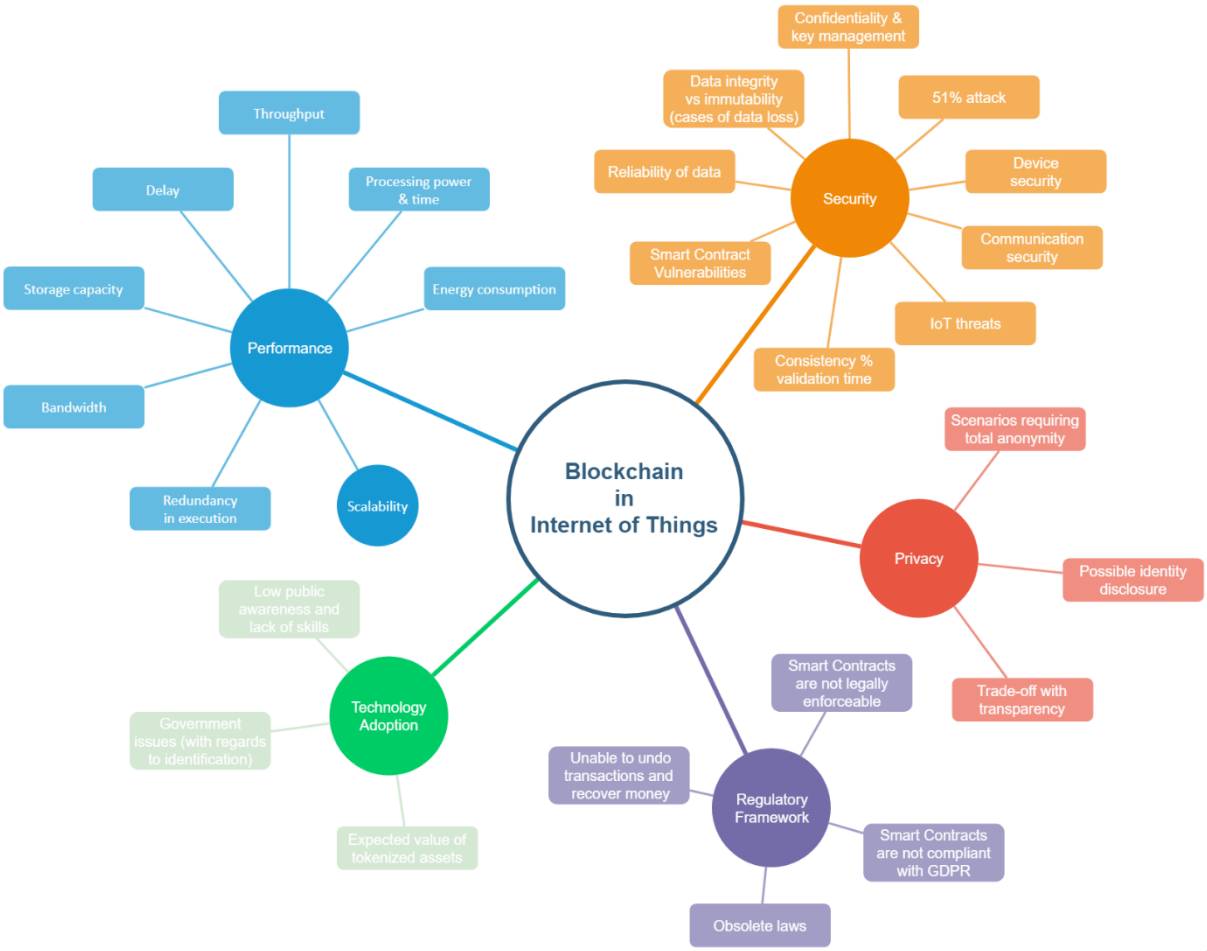
1. Εκμετάλλευση της ιδιότητας της ελεγξιμότητας που παρέχει το BC για ιχνηλασιμότητα και διασφάλιση προέλευσης προϊόντων.
2. Επίλυση διενέξεων με τη χρήση SC για αυτόματη ενεργοποίηση αποζημιώσεων ή προστίμων σε περίπτωση παράβασης όρων μίας συμφωνίας.
3. Βοηθά στην επαληθευσιμότητα της ακεραιότητας των φορτίων.
4. Αυτόματη διαχείριση ψηφιακών εγγράφων που παράγονται κατά μήκος της εφοδιαστικής αλυσίδας.
5. Η διαφάνεια και η μη μεταβλητότητα βοηθούν να επιβληθεί η συμμόρφωση σε υγειονομικούς, εμπορικούς και νομικούς κανονισμούς.
6. Διαχείριση της εμπιστοσύνης μεταξύ των ενδιαφερόμενων μερών μέσω της αποδιαμεσολάβησης.

Το κατανεμημένο μητρώο καταγραφών αν συνδυαστεί με ένα δίκτυο αισθητήρων που συνδέει τα φορτηγά φορτίου, τους ψύκτες αποθήκευσης προϊόντων κλπ., θα ενισχύσει σημαντικά τη λειτουργικότητα του BC αφού θα δύναται να παρακολουθήσει τη θέση του προϊόντος και τις περιβαλλοντικές παραμέτρους όπως θερμοκρασία και υγρασία. Σε επόμενη υποενότητα παραθέτουμε σενάρια ενσωμάτωσης IoT και BC στην SCM και σε άλλη υποενότητα παρατίθεται μία εφαρμογή ενός SC για τη διαφάνεια στην εφοδιαστική αλυσίδα.

4.3 Προκλήσεις της ενσωμάτωσης

Οι Al-Fuqaha et al. (2015) πραγματοποιώντας μια ενδελεχή επισκόπηση ορισμένων από τις βασικές προκλήσεις του IoT μεταξύ άλλων θίγουν τα καίρια ζητήματα της διαθεσιμότητας, ασφάλειας, αξιοπιστίας, εμπιστοσύνης, επεκτασιμότητας, διαχείρισης και απόδοσης τα οποία αποτελούν τροχοπέδη για την υλοποίηση αποτελεσματικών υπηρεσιών. Επί παραδείγματι, η ασφάλεια και η προστασία της ιδιωτικότητας διαδραματίζουν σημαντικό ρόλο σε όλες τις αγορές παγκοσμίως λόγω της ευαισθησίας της ιδιωτικής ζωής των καταναλωτών. Επίσης, η αξιολόγηση της απόδοσης των υπηρεσιών IoT αποτελεί σημαντική πρόκληση. Από την άλλη, ως μία αναπτυσσόμενη τεχνολογία, το BC είναι φυσικό να αντιμετωπίζει πολλαπλά προβλήματα. Από αυτές, οι Zheng et al. (2018) σε σχετική τους μελέτη, ξεχωρίζουν τα θέματα της επεκτασιμότητας, της διαρροή της ιδιωτικότητας, αποδοτικότητας μηχανισμών συναίνεσης και την επιρρέπεια σε επιθέσεις όπως η «εγωιστική εξόρυξη».

Στις επόμενες παραγράφους παρέχεται μία σύνοψη των βασικών ζητημάτων που εντοπίζονται κατά την ενοποίηση των δύο τεχνολογιών με βάση τις πρόσφατες δημοσιεύσεις της ερευνητικής κοινότητας. Τα ζητήματα που εντοπίστηκαν ταξινομήθηκαν στις εξής βασικές κατηγορίες: απόδοση, ασφάλεια, ιδιωτικότητα, υποδομή, υιοθέτηση της τεχνολογίας. Ακολουθεί η ανάλυσή τους.



Προκλήσεις της ενσωμάτωσης των δύο τεχνολογιών

4.3.1 Απόδοση

Η αξιολόγηση της απόδοσης των υπηρεσιών IoT είναι μια μεγάλη πρόκληση επειδή εξαρτάται από πολλές συνιστώσες καθώς και από τις επιδόσεις των υποκείμενων τεχνολογιών. Το IoT, όπως και άλλα συστήματα, πρέπει να αναπτύσσει και να βελτιώνει συνεχώς τις υπηρεσίες του ώστε να ανταποκρίνεται στις απαιτήσεις των πελατών. Οι συσκευές IoT πρέπει να παρακολουθούνται και να αξιολογούνται για να παρέχουν την καλύτερη δυνατή απόδοση σε προσιτή τιμή για τους πελάτες. Πολλές μετρικές μπορούν να χρησιμοποιηθούν για την αξιολόγηση της απόδοσης του IoT, συμπεριλαμβανομένης του χρόνου επεξεργασίας, της ταχύτητας επικοινωνίας και του κόστους (Al-Fuqaha et al., 2015).

Η απόδοση είναι μία από τις μεγαλύτερες ανησυχίες όσον αφορά και την υιοθέτηση του BC καθώς με βάση τους Pongnumkul, Siripanpornchana και Thajchayapong (2017) η ανάλυσης της μπορεί να παράσχει χρήσιμη πληροφόρηση στους επαγγελματίες για τη λήψη αποφάσεων σχετικά με την υιοθέτηση τεχνολογίας στα συστήματα πληροφορικής τους. Σε αυτή την κατεύθυνση, για την σύγκριση μεταξύ BC βασισμένων στην PoW και στη PBFT, ο Vukolić (2015) χρησιμοποίησε μετρικές όπως διεκπεραιωτικότητα , χρονική καθυστέρηση και ενεργειακή κατανάλωση.

Εκτός από τις μετρήσεις που σχετίζονται άμεσα με την απόδοση, πολλές επιπλέον μετρήσεις είναι συχνά χρήσιμες για να εξηγήσουν τις αιτίες της υποβάθμισης της απόδοσης. Με βάση όλα αυτά καθώς και την μελέτη της πρόσφατης βιβλιογραφίας ακολουθεί η ανάλυση της απόδοσης.

4.3.1.1 Ενεργειακή κατανάλωση

Ένας από τους πιο καίριους περιορισμούς που επιβραδύνουν την ομαλή ενοποίηση των δύο τεχνολογιών είναι η διαχείριση της ενεργειακής κατανάλωσης. Τα άκρα των IoT δικτύων απαρτίζονται κυρίως από τελικούς κόμβους οι οποίοι χρησιμοποιούν υλισμικό με περιορισμένους πόρους και τροφοδοτούνται με μπαταρίες. Ως εκ τούτου, η ενεργειακή απόδοση είναι το κλειδί για την μακροβιότητα ενός κόμβου και κατ' επέκταση για την ομαλή λειτουργία ενός IoT δικτύου. Η ενσωμάτωση ενός BC επηρεάζει το προαναφερθέν ζήτημα καθώς πολλά BC χαρακτηρίζονται ως ενεργειακά αδηφάγα.

Πολλά BC, όπως αυτό που υλοποιείται στο Bitcoin, κάνουν χρήση τεράστιων ποσοτήτων ηλεκτρικού ρεύματος λόγω της διαδικασίας εξόρυξης, η οποία όπως έχουμε παρατηρήσει σε προηγούμενη ενότητα, περιλαμβάνει έναν αλγόριθμο συναίνεσης που βασίζεται στην «απόδειξη της εργασίας» (PoW), η οποία αναγκάζει τους εξορύκτες να επιλύσουν ένα υπολογιστικά εντατικό αλλά εύκολα επαληθεύσιμο έργο – την ανεύρεση μίας τιμής κατακερματισμού υπό ορισμένες προϋποθέσεις – για να δημιουργήσουν ένα νέο μπλοκ. Εκτός αυτού, το BC αυξάνεται καθώς οι χρήστες αποθηκεύουν τις συναλλαγές τους και αυτό συνεπάγεται ότι απαιτούνται πιο ισχυροί εξορύκτες για να διαχειριστούν τα πρωτόκολλα συναίνεσης στο BC.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ένας άλλος συντελεστής που επιβαρύνει την ενεργειακή κατανάλωση είναι οι επικοινωνίες. Οι επικοινωνίες στα διομότιμα δίκτυα απαιτούν συσκευές στα άκρα του δικτύου, οι οποίες θα τροφοδοτούνται συνεχώς, πράγμα που θα μπορούσε να οδηγήσει σε μεγάλη ενεργειακή απώλεια. Οι συγκεκριμένες επικοινωνίες, είναι απαραίτητες για ένα BC ώστε να επικοινωνούν οι ομότιμοι και να διανείμουν τις συναλλαγές και τα μπλοκ. Όσο περισσότερες ανανεώσεις λαμβάνει ένα BC τόσο περισσότερη κατανάλωση ενέργειας αφιερώνεται στις επικοινωνίες.

4.3.1.2 Επεξεργαστική Ισχύς και χρόνος επεξεργασίας

Σε μια τυπική υλοποίηση IoT, συσκευές περιορισμένων πόρων χρησιμοποιούνται ως τελικοί κόμβοι που επικοινωνούν με μια πύλη δικτύου (gateway) η οποία είναι υπεύθυνη για την προώθηση δεδομένων αισθητήρων σε ανώτερα στρώματα (υπολογιστικό νέφος ή διακομιστής). Κατά την ενσωμάτωση του BC, εάν οι τελικοί κόμβοι πρέπει να αλληλεπιδρούν με αυτή, θα μπορούσε να παρέχεται κρυπτογραφική λειτουργικότητα στις συσκευές IoT. Αυτό είναι κομβικό για την πραγματοποίηση της αυτονομίας του IoT, η οποία επιτυγχάνεται με το τίμημα ενός πιο εξελιγμένου υλισμικού και υψηλότερων υπολογιστικών εξόδων (Reyna et al., 2018).

Η επίλυση της απόδειξης του έργου (PoW) απαιτεί επίσης πολύ εξελιγμένο υλισμικό και δεν μπορεί να επιτευχθεί ακόμη και με τη χρήση ηλεκτρονικών υπολογιστών από το ράφι[12] (Dorri, Kanhere and Jurdak, 2017). Επιπλέον, όπως οι Atlam et al. (2018) τονίζουν, τα συστήματα IoT έχουν διάφορους τύπους συσκευών, με πολύ διαφορετικές υπολογιστικές δυνατότητες και δεν μπορούν όλες να τρέξουν τους ίδιους αλγορίθμους κρυπτογράφησης με την απαιτούμενη ταχύτητα.

Εν κατακλείδι, οι IoT συσκευές διακρίνονται στην πλειοψηφία τους από χαμηλές υπολογιστικές δυνατότητες λόγω υλισμικού. Η εκτέλεση έργων με υπερβολικό φόρτο (επεξεργαστική ισχύς) και σε σύντομο διάστημα (χρόνο επεξεργασίας), όπως οι συναρτήσεις κατακερματισμού και κρυπτογράφησης, μπορεί να μην είναι εφικτή.

4.3.1.3 Χαμηλή διεκπεραιωτικότητα συναλλαγών

Οι υλοποιήσεις στο IoT ενδέχεται να απαιτούν από ένα δίκτυο BC να είναι ικανό να διαχειρίζεται μεγάλα ποσά συναλλαγών ανά μονάδα χρόνου. Από την άλλη, είναι γνωστό ότι μερικές από τις τρέχουσες υλοποιήσεις BC μπορούν να επεξεργαστούν μόνο λίγες συναλλαγές ανά δευτερόλεπτο, επομένως αυτό θα μπορούσε να αποτελέσει πιθανή συμφόρηση (bottleneck) για το IoT.

Ενδεικτικά, αναφέρουμε ότι το BC του Bitcoin υποστηρίζει (θεωρητικά) κατά μέγιστο 7 συναλλαγές ανά δευτερόλεπτο, παρόλο που ο αριθμός μπορεί να αυξηθεί με την επεξεργασία μεγαλύτερων μπλοκ ή με την τροποποίηση ορισμένων παραμέτρων της συμπεριφοράς των κόμβων κατά την αποδοχή των

[12] Ο όρος από το ράφι (off-the-shelf) χρησιμοποιείται για να περιγράψει ένα προϊόν που είναι άμεσα διαθέσιμο και δεν χρειάζεται να είναι ειδικά κατασκευασμένο για να ταιριάζει σε συγκεκριμένο σκοπό.

συναλλαγών. Ακόμα και τότε όμως, άλλα δίκτυα είναι εξαιρετικά ταχύτερα όπως για παράδειγμα, το δίκτυο VISA (VisaNet) το οποίο είναι σε θέση να χειριστεί έως και 24.000 συναλλαγές ανά δευτερόλεπτο.

Επί του ζητήματος, οι Christidis και Devetsikiotis (2016) ισχυρίζονται πως συγκριτικά με μια σωστά ρυθμισμένη κεντρική βάση δεδομένων, μια λύση BC γενικά θα υποαποδίδει οδηγώντας σε χαμηλότερη διεκπαιρεωτική ικανότητα επεξεργασίας συναλλαγών και μεγαλύτερες καθυστερήσεις και πως το πρόβλημα αυτό είναι ιδιαίτερα έντονο στα δημόσια δίκτυα, όπου αναπτύσσονται μηχανισμοί απόδειξης του έργου.

4.3.1.4 Υψηλή χρονική καθυστέρηση

Όσον αφορά την καθυστέρηση, είναι σημαντικό να σημειωθεί ότι οι συναλλαγές ΑΚ χρειάζονται κάποιο χρόνο για να υποστούν επεξεργασία. Για παράδειγμα, στην περίπτωση του Bitcoin, ο χρόνος δημιουργίας ενός νέου μπλοκ ακολουθεί μια κατανομή Poisson με μέσο όρο 10 λεπτών. Για να αποφευχθεί το φαινόμενο της διπλής δαπάνης, συνήθως χρειάζεται να προστεθούν πέντε ή έξι μπλοκ στην αλυσίδα πριν επαληθευθεί η οριστικότητα μίας συναλλαγής. Αυτό αυτομάτως σε όρους αγοράς ερμηνεύεται ως προσμονή μίας ώρας για έναν έμπορο μέχρι να είναι σίγουρος ότι μία οικονομική δοσοληψία έχει επιβεβαιωθεί. Κάτι πραγματικά δυσχαιρές σε σύγκριση με την περίπτωση της VISA όπου μόνο μερικά δευτερόλεπτα είναι αρκετά.

Αναφορικά με το μηχανισμό συναίνεσης, πρέπει να αναφερθεί ότι η πολυπλοκότητα της διαδικασίας συναίνεσης είναι πιο σημαντική σε όρους καθυστέρησης από την εξατομικευμένη διαδικασία του κατακερματισμού.

Το συνεχώς αυξανόμενο μέγεθος της ΑΚ καθιστά επίσης αυξητικό το χρόνο που απαιτείται για να συγχρονιστεί[13] ένας νέος χρήστης ή συσκευή μόλις συνδεθούν στο δίκτυο. Ως εκ τούτου, αποτελεί πρόκληση ο σχεδιασμός μιας ασφαλούς λύσης IoT βασισμένης σε BC, η οποία από τη μία πλευρά να καλύπτει τους περιορισμένους πόρους των συσκευών IoT και από την άλλη να κληροδοτήσει τα μέγιστα οφέλη του BC.

Επίσης οι Panarello et al. (2018) επισημαίνουν ότι σε ένα κατανεμημένο σύστημα, υπάρχουν καθυστερήσεις δικτύου και δεν είναι εφικτό όλοι οι κόμβοι να λαμβάνουν ταυτόχρονα όλα τα μπλοκ των συναλλαγών.

4.3.1.5 Χαμηλή χωρητικότητα αποθήκευσης

Στο πλαίσιο των εφαρμογών IoT, διακρίνουμε εγγενείς περιορισμούς χωρητικότητας. Οι συσκευές δύνανται να παράγουν gigabyte δεδομένων σε πραγματικό χρόνο. Το γεγονός αυτό αποτελεί ένα

[13] Αναφερόμαστε κυρίως στη λήψη (download) και αποθήκευση του συνολικού όγκου μίας αλυσίδας καταγραφών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μεγάλο εμπόδιο στην ολοκλήρωσή του με το BC καθότι η τελευταία δεν έχει σχεδιαστεί για να αποθηκεύει μεγάλες ποσότητες δεδομένων.

Το κατανεμημένο μητρώο καταγραφών συναλλαγών θα αυξηθεί σε μέγεθος με την πάροδο του χρόνου και με την προσθήκη νέων κόμβων στο δίκτυο. Επίσης, τα BC αυξάνονται περιοδικά καθώς οι χρήστες αποθηκεύουν τις συναλλαγές τους, οδηγώντας σε μεγαλύτερους αρχικούς χρόνους λήψης και στην ανάγκη χρήσης πιο ισχυρών εξορυκτών[14] που θα διαθέτουν μεγαλύτερες μόνιμες[15] μνήμες. Οι περισσότεροι κόμβοι IoT δεν θα είναι σε θέση να διαχειριστούν ακόμη και ένα μικρό μέρος ενός παραδοσιακού blockchain. Αυτό συνεπάγεται ότι θα αδυνατούν να λειτουργήσουν ως πλήρεις κόμβοι ή κόμβοι επικύρωσης. Επιπρόσθετα, πολλοί κόμβοι αναγκάζονται να αποθηκεύουν μεγάλες ποσότητες δεδομένων που δεν τους ενδιαφέρουν / αφορούν, κάτι που μπορεί να θεωρηθεί ως σπατάλη υπολογιστικών πόρων.

4.3.1.6 Όρια εύρους ζώνης

Οι Fernández-Caramés και Fraga-Lamas (2018) σε σχετική τους ανάλυση, εντοπίζουν τους βασικούς παράγοντες που διαμορφώνουν τις παρούσες προκλήσεις ενσωμάτωσης των δύο προς μελέτη τεχνολογιών. Μεταξύ άλλων αναφέρονται και στο μέγεθος μίας συναλλαγής σε σχέση με το μέγεθος του μπλοκ και τις επιπτώσεις τους με βάση τα όρια του εύρος ζώνης του δικτύου και την κατανάλωση ενέργειας.

Πιο συγκεκριμένα, υποστηρίζουν ότι ο αριθμός των συναλλαγών και το μέγεθος του μπλοκ πρέπει να κλιμακωθούν σύμφωνα με τους περιορισμούς του εύρους ζώνης των δικτύων IoT. Δηλαδή, πολλές μικρές συναλλαγές θα αυξήσουν τις επικοινωνίες και άρα ενδέχεται να μεγεθύνουν την κατανάλωση ενέργειας, ενώ μερικές μεγάλες μπορεί να περιλαμβάνουν μεγάλα ωφέλιμα φορτία που δεν μπορούν να τα διαχειριστούν κάποιες IoT συσκευές.

4.3.1.7 Πλεονασμός στην εκτέλεση

Δεδομένου ότι όλοι οι κόμβοι σε ένα δίκτυο BC εκτελούν τους ίδιους υπολογισμούς σε μια προσπάθεια εξόρυξης του επόμενου μπλοκ, αυτή δεν είναι μια αποτελεσματική προσέγγιση. Λόγω αυτού τού πλεονασμού εκτέλεσης, η συμβολή ενός μεμονωμένου κόμβου στο συνολικό δίκτυο είναι πολύ μικρή, παρόλο που ο κόμβος μπορεί να εκτελεί πολύ σκληρούς υπολογισμούς. Επιπλέον, με λιγότερους χρόνους μπλοκ, θα υπάρξουν περισσότερα ορφανά μπλοκ, και συνεπώς μία αύξηση της σπατάλης υπολογιστικών και ενεργειακών πόρων.

[14] Με την έννοια των μηχανημάτων – ηλεκτρονικών υπολογιστών αφοσιωμένων στη διαδικασία εξόρυξη.

[15] Ο όρος μόνιμη μνήμη (persistent memory) αναφέρεται σε οποιαδήποτε μέθοδο ή/και εξοπλισμό για την αποτελεσματική αποθήκευση των δομών δεδομένων έτσι ώστε να μπορούν να συνεχίσουν να παρέχουν πρόσβαση και μετά το τέλος της διαδικασίας που τις δημιούργησε ή τροποποίησε τελευταία.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Η πρόσβαση σε πολλές πηγές δεδομένων, όπως είναι οι «χρησμοί» (oracles) θα μπορούσε να επιβαρύνει τα έξυπνα συμβόλαια και να δημιουργήσει συμφόρηση. Σήμερα, τα ΕΣ είναι διανεμημένα και αποκεντρωμένα στη φύση τους, αλλά δεν μοιράζονται πόρους για τη κατανομή έργων και την αντιμετώπιση μεγάλων φόρτων υπολογιστικής. Με άλλα λόγια, η εκτέλεση ΕΣ γίνεται σε έναν μόνο κόμβο ενώ ταυτόχρονα η εκτέλεση του κώδικα γίνεται από πολλούς κόμβους. Αυτή η διανομή γίνεται μόνο στα πλαίσια της διαδικασία επικύρωσης αντί να χρησιμεύει στη διανομή εργασιών.

4.3.1.8 Δυνατότητα κλιμάκωσης / Επεκτασιμότητα

Σχετικά τη δυνατότητα επέκτασης, οι Dorri, Kanhere και Jurdak (2016) τοποθετούνται άμεσα: *"Το blockchain κλιμακώνεται πτωχά καθώς ο αριθμός των κόμβων στο δίκτυο αυξάνεται. Τα δίκτυα IoT αναμένεται να περιέχουν μεγάλο αριθμό κόμβων."*

Η κλιμακωσιμότητα μίας IoT εφαρμογής με αξιοποίηση του BC επηρεάζεται άμεσα από άλλους παράγοντες απόδοσης. Αρχικά, το συγκεκριμένο ζήτημα συναντά το εμπόδιο του μεγέθους του BC σε συνδυασμό με τη χαμηλή χωρητικότητα αποθήκευσης και τη υψηλή καθυστέρηση συγχρονισμού. Η επέκταση στον αριθμό των χρηστών θα επιφέρει πλήθυνση των συναλλαγών και μοιραία μεγέθυνση του όγκου του BC. Αυτό όμως ενέχει δύο κινδύνους. Πρώτον, το BC δεν έχει σχεδιαστεί για να αποθηκεύει τόσο μεγάλο όγκο δεδομένων. Κατά δεύτερον, η απαίτηση αποθήκευσης ολόκληρου του BC από τους πλήρεις κόμβους εμποδίζει την ενσωμάτωση των συσκευών IoT απευθείας με το BC, αφού όπως έχουμε αναφέρει και πάλι, χαρακτηρίζονται από περιορισμένες δυνατότητες επεξεργασίας και αποθήκευσης. Ακόμη, υπάρχει μη αμελητέα καθυστέρηση κατά την εισαγωγή ενός πλήρους κόμβου στο δίκτυο ως προς το συγχρονισμό του, αφού το αυξανόμενο μέγεθος της ΑΚ απαιτεί μεγάλο το χρονικό διάστημα για να το λάβει και να το αποθηκεύσει τοπικά.

Το ζήτημα της δυνατότητας επέκτασης δυσχεραίνεται σημαντικά από τις υψηλές χρονικές καθυστερήσεις και το μέγεθος του μπλοκ σε συσχέτιση με την επεξεργαστική ισχύ, την ενεργειακή κατανάλωση και το εύρος ζώνης. Οι απαιτήσεις για την ανταλλαγή δεδομένων σε πραγματικό χρόνο των περισσότερων συστημάτων IoT όπως το WSN, τα έξυπνα οχήματα, το έξυπνο σύστημα μεταφορών και άλλα, απαιτούν βελτίωση στον χρόνο επιβεβαίωσης των συναλλαγών, χωρίς να διακυβεύεται η ασφάλεια και η απόδοση του συστήματος. Σε ένα BC βασισμένο στην PoW, η μείωση του χρόνου δημιουργίας νέου μπλοκ μειώνει τον χρόνο επιβεβαίωσης των συναλλαγών, όμως για να διατηρηθεί το ίδιο επίπεδο ασφάλειας[16], μία συναλλαγή πρέπει να περιμένει περισσότερες επιβεβαιώσεις εξαιτίας του μικρότερου βαθμού δυσκολίας εξόρυξης. Επιπλέον, η «συντόμευση» της διαδικασίας εξόρυξης θα επιφέρει περισσότερα ορφανά μπλοκ και συνεπώς σπατάλη υπολογιστικών και ενεργειακών πόρων. Ένας άλλος παράγοντας που σχετίζεται με την καθυστέρηση των συναλλαγών είναι το μέγεθος του

[16] Σε σύγκριση με τον προεπιλεγμένο χρόνο εξόρυξης των 10 λεπτών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

μπλοκ. Υπάρχει η πεποίθηση ότι αυξάνοντας το μέγεθος του μπλοκ η απόδοση μπορεί να αυξηθεί ενώ στην πραγματικότητα, ένα μεγαλύτερο μπλοκ θα χρειαστεί περισσότερο χρόνο για να διαδοθεί στο δίκτυο. Ως εκ τούτου, οι κόμβοι με συνδέσεις χαμηλού εύρους ζώνης στο διαδίκτυο θα υποφέρουν ενώ οι εύποροι εξορύκτες με περισσότερο εύρος ζώνης θα υπερέχουν. Επιπλέον, ένα αυξημένο μέγεθος μπλοκ θα έχει επίσης ως αποτέλεσμα την ταχύτερη ανάπτυξη του μεγέθους blockchain, που θα επηρεάσει τον αριθμό των πλήρων κόμβων στο δίκτυο, καθώς απαιτούνται περισσότεροι πόροι για την αποθήκευση του πλήρους BC (Makhdoom et al., 2019).

Η συμβολή της επικύρωσης των συναλλαγών, των χρόνων εξόρυξης και του μεγέθους του μπλοκ υποδεικνύουν ότι τα πρωτόκολλα συναίνεσης έχουν άμεση επίδραση στην κλιμακωσιμότητα ενός BC δικτύου. Ακόμη, τα ζητήματα επεκτασιμότητας στο BC ενδέχεται να οδηγήσουν σε κεντρικοποίηση ρίχνοντας μια σκιά στο μέλλον των κρυπτονομισμάτων και των εφαρμογών BC. Το BC κλιμακώνεται ανεπαρκώς καθώς αυξάνεται ο αριθμός των κόμβων στο δίκτυο. Ο φόβος κεντρικοποίησης απορρέει από το γεγονός ότι μόνο λίγοι κόμβοι θα πληρούν τις προϋποθέσεις[17] να παράξουν ένα νέο μπλοκ. Με τον τρόπο αυτό εγκυμονεί ο κίνδυνος να συγκεντρωθεί εξουσία σε ένα γκρουπ εξορυκτών που θα ελέγχουν το δίκτυο.

4.3.2 Ασφάλεια

Η ασφάλεια μαζί με την ιδιωτικότητα αποτελούν δύο από τους κρισιμότερους τομείς για την επιτυχή ολοκλήρωση των δύο τεχνολογιών. Θεωρείται ένας από τους βασικούς παράγοντες που εισήλθε το BC στις υλοποιήσεις του IoT, αφού η τεχνική της υλοποίηση υπόσχεται να καταστείλει αρκετές από τις μέχρι τώρα υπάρχουσες ευπάθειες και αδυναμίες στα έξυπνα συστήματα. Μολονότι αυτό ισχύει έως ένα βαθμό, δεν έχουν διευθετηθεί επαρκώς όλα τα ζητήματα.

Το θεώρημα CAP (Consistency – Availability - Partitioning) ισχυρίζεται ότι σε ένα κατανεμημένο στο δίκτυο σύστημα μπορούν να επιτευχθούν μόνο δύο από τις τρεις επιθυμητές ιδιότητες (Brewer, 2012):

- C: Συνέπεια (consistency), δηλαδή να διατηρεί άμεσα την τελευταία και συνεπή εικόνα του συστήματος
- A: Υψηλή διαθεσιμότητα (availability) του συστήματος για ανάγνωση δεδομένων ή εγγραφή
- P: Ανοχή στον διαχωρισμό (partitioning) του δικτύου σε τμήματα

Το BC αν μη τι άλλο είναι ένα κατανεμημένο σύστημα. Με βάση αυτό οι Bahga και Madisetti (2016) αναδεικνύουν τη σχέση μεταξύ του θεωρήματος CAP και του BC. Για συστήματα κατανεμημένων δεδομένων, υπάρχει συμβιβασμός μεταξύ συνέπειας και διαθεσιμότητας. Με άλλα λόγια κατά τον κατακερματισμό μίας βάσης, ένα κατανεμημένο σύστημα δεδομένων μπορεί είτε να παρέχει συνέπεια είτε διαθεσιμότητα αλλά όχι και τα δύο ταυτόχρονα. Το BC ως φαίνεται θυσιάζει τη συνέπεια ώστε να

[17] Στην παρούσα ανάλυση, αυτό ερμηνεύεται ως να είναι πλήρεις κόμβοι, με επαρκείς υπολογιστικούς πόρους.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

διασφαλίσει διαθεσιμότητα. Το BC είναι ένα κατανεμημένο μητρώο καταγραφής συναλλαγών το οποίο στο τέλος επιτυγχάνει συνέπεια, δηλαδή όλοι οι κόμβοι βλέπουν το ίδιο μητρώο καταγραφών. Στο Ethereum, ο χρόνος επικύρωσης (χρόνος μετά τον οποίο ένα νέο μπλοκ παράγεται) είναι περίπου μερικά δευτερόλεπτα, κατά πολύ ταχύτερος από αυτόν του Bitcoin - περίπου 10 λεπτά. Φυσικό επακόλουθο του γρήγορου χρόνου επικύρωσης είναι η μειωμένη ασφάλεια, επομένως, πολλές εφαρμογές BC απαιτούν πολλαπλές επιβεβαιώσεις για πρόσφατα παραγμένα μπλοκ ώστε να εξασφαλιστούν από τη «διπλή δαπάνη». Ο ταχύτερος χρόνος επικύρωσης οδηγεί επίσης σε υψηλό αριθμό παραγόμενων ορφανών μπλοκ, δηλαδή μπλοκ που πράχθηκαν και τα οποία δεν συνεισφέρουν στην κύρια αλυσίδα. Συνεπαγόμενα, ο υψηλός ρυθμός αύξησης αυτών των μπλοκ μειώνει την ασφάλεια της κύριας αλυσίδας.

Ευπάθειες Έξυπνων Συμβολαίων: Τα έξυπνα συμβόλαια ανοίγουν νέες φουτουριστικές προοπτικές: στο μέλλον, ένα άτομο μπορεί να αποφασίσει να νοικιάσει ένα αυτοκίνητο ή ένα σπίτι χρησιμοποιώντας κρυπτονομίσματα όπως το Bitcoin ή το Litecoin και το Ethereum. Υποθέτοντας ότι ο μισθωτής και το άτομο που επιθυμεί να νοικιάσει το περιουσιακό στοιχείο (για παράδειγμα ένα σπίτι) όριζαν προηγουμένως ένα Ευφυές Συμβόλαιο, τότε το άτομο θα μπορούσε να πληρώσει "νομίσματα" στο SC που με τη σειρά του θα επέτρεπε στο ιδιωτικό του κρυπτο-κλειδί να ανοίξει την πόρτα για μία χρονική προθεσμία που καθορίζεται στη σύμβαση. Τα SC όμως μπορούν να έχουν ευπάθειες στο λογισμικό τους τις οποίες μπορούν δυνητικά να τις εκμεταλλευτούν χάκερ. Χαρακτηριστικά, τον Ιούνιο του 2016, ένας επιτιθέμενος κατόρθωσε να αδειάσει περισσότερα από 3,6 εκατομμύρια Ether από τον Αποκεντρωμένο Αυτόνομο Οργανισμό (DAO) της Slock.it. Ο επιτιθέμενος το κατάφερε, εκμεταλλευόμενος μια ευπάθεια του ΕΣ με ονομασία «recursive call bug»[18]. Δεδομένου ότι τα SC αποτελούν συμφωνίες μεταξύ συναλλασσόμενων μερών μέσα σε ένα BC και δεν επιβάλλονται νομικά εκτός του δικτύου, τέτοιες επιθέσεις μπορούν να θέσουν σε κίνδυνο τους οργανισμούς, τους εξορύκτες μέχρι και το ίδιο το δίκτυο BC. Επίσης, η λειτουργία SC πολλές φορές απαιτεί τη χρήση «χρησμών» (oracles), ειδικές οντότητες που παρέχουν δεδομένα από τον πραγματικό κόσμο στον ψηφιακό με αξιόπιστο τρόπο. Η επαλήθευση αυτών των δεδομένων δεν είναι εύκολη. Οι Gatteschi et al. (2018) τονίζουν ότι ακόμα και αν υποτεθεί ότι τα SC είναι απαλλαγμένα από σφάλματα, οι συνέπειες της χορήγησης λανθασμένων πληροφοριών μπορεί να είναι καταστρεπτικές.

Αξιοπιστία των δεδομένων που παράγονται από το IoT. Το BC μπορεί να διασφαλίσει ότι τα δεδομένα στην αλυσίδα παραμένουν αμετάβλητα, ωστόσο, αν τα δεδομένα φθάνουν ήδη αλλοιωμένα στο BC, τότε θα αποθηκευτούν και θα παραμείνουν αλλοιωμένα. Μεταβολή των δεδομένων στο IoT μπορεί να προκύψει από πολλές καταστάσεις εκτός από κακόβουλες. Η ευημερία της αρχιτεκτονικής του IoT επηρεάζεται από πολλούς παράγοντες όπως το περιβάλλον του, οι συμμετέχοντες, ο βανδαλισμός και η βλάβη των συσκευών. Μερικές φορές οι ίδιες οι συσκευές καθώς και οι αισθητήρες και οι

[18] Ο επιτιθέμενος ήταν σε θέση να «ζητά» από το έξυπνο συμβόλαιο (DAO) να του δώσει πίσω κρυπτονομίσματα Ether, αρκετές φορές πριν το έξυπνο συμβόλαιο καταφέρει να ενημερώσει το υπόλοιπό του.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ενεργοποιητές τους αποτυγχάνουν να λειτουργούν σωστά από την αρχή. Κάτι τέτοιο δεν μπορεί να εντοπιστεί μέχρι να πραγματοποιηθεί έλεγχος στη συγκεκριμένη συσκευή ή ορισμένες φορές να παρατηρηθεί ότι έπειτα από την ομαλή της λειτουργία διακρίνεται αλλαγή στη συμπεριφορά της για κάποιο αδιευκρίνιστο λόγο, λόγου χάριν ένα βραχυκύκλωμα, αποσύνδεση από το δίκτυο, προγραμματισμένη απαξίωση[19] κ.ο.κ.

Ακεραιότητα των δεδομένων: Τα θεμέλια ενός BC έχουν σχεδιαστεί για να αποθηκεύουν πληροφορίες που δεν μπορούν να τροποποιηθούν ή είναι πολύ δαπανηρό να το κάνουν μόλις αποθηκευτούν (χαρακτηριστικό της μη μεταβλητότητας). Ωστόσο, στο παρελθόν υπήρχαν ορισμένες καταστάσεις όπου η αρχή αυτή αγνοήθηκε. Για παράδειγμα, το 2014, κάτω από αδιευκρίνιστες συνθήκες, η πλατφόρμα ανταλλαγής νομισμάτων MintPal ενημέρωσε τους χρήστες της ότι ένας χάκερ είχε κλέψει σχεδόν 8 εκατομμύρια Vericoins, δηλαδή περίπου το 30% του συνόλου των εν κυκλοφορία κρυπτονομισμάτων της. Για να αποφευχθεί η απώλεια επενδυτικών κεφαλαίων και η δυσχερής κατάσταση όπου ένα υποκείμενο θα ελέγχει μία μεγάλη ποσότητα των συνολικών κρυπτονομισμάτων, οι προγραμματιστές της Vericoin αποφάσισαν να εκτελέσουν μία σταθερή διακλάδωση[20] (hard fork) του BC, με σκοπό να αντιστρέψουν τη ζημιά . Παρατηρούμε ότι παρά τον ισχυρισμό ότι οι BC αποτελούν μόνιμη αποθήκευση για δεδομένα που δεν μπορούν να τροποποιηθούν, στην πράξη σε εξαιρετικές περιπτώσεις[21] δεν ισχύει.

Όσον αφορά την εμπιστευτικότητα, ένα κομμάτι που σχετίζεται με τα δεδομένα των συναλλαγών και άρα αγγίζουν θέματα ιδιωτικότητας, έχουν αναλύονται σε επόμενη υποενότητα. Για έναν μεμονωμένο χρήστη, το βασικό σημείο για τη διατήρηση της εμπιστευτικότητας των δεδομένων του είναι η καλή διαχείριση των ιδιωτικών κλειδιών του. Ο λόγος είναι ότι ένας επιτιθέμενος έχει πρόσβαση στο δημόσιο κλειδί του και άρα αυτό που υπολείπεται είναι το ιδιωτικό ώστε συνδυάζοντας και τα δύο να είναι σε θέση να μιμηθεί κάποιον πραγματοποιώντας συναλλαγές ή να τον κλέψει απευθείας, αφαιρώντας του κρυπτονομίσματα.

Επιθέσεις διαθεσιμότητας: Στην πραγματικότητα η πιο σαφής ιδιότητα της ασφάλειας για τα BC, δεδομένου ότι οι τελευταίες σχεδιάζονται για να είναι κατανεμημένα συστήματα, πράγμα που τους επιτρέπει να συνεχίσουν το έργο τους ακόμα και αν κάποιοι κόμβοι δέχονται επίθεση. Παρ 'όλα αυτά, η διαθεσιμότητα μπορεί να διακυβευτεί μέσω άλλων τύπων επιθέσεων. Η πιο επίφοβη εξ αυτών είναι μια «επίθεση του 51 τοις εκατό», αλλιώς γνωστή και ως επίθεση της πλειοψηφίας, όπου ένας μόνο εξορύκτης μπορεί να ελέγξει ολόκληρο την αλυσίδα καταγραφών και να πραγματοποιήσει συναλλαγές κατά βούληση. Σε αυτήν την περίπτωση, τα δεδομένα είναι διαθέσιμα, αλλά η διαθεσιμότητα για την

[19] Οικονομικός όρος που συναντάτε στα οικονομικά και τη βιομηχανία κα αναφέρεται είναι στην πολιτική σχεδιασμού και παραγωγής ενός προϊόντος με σκόπιμα περιορισμένη ωφέλιμη ζωή, ώστε να καταστεί απηρχαιωμένο ή μη λειτουργικό μετά από μια ορισμένη χρονική περίοδο. Σκοπός είναι η επανάληψη της αγοράς και συνεπαγόμενα η μεγιστοποίηση των κερδών (Bulow, 1986).

[20] Μια σταθερή διακλάδωση είναι μόνιμη απόκλιση από την προηγούμενη έκδοση της αλυσίδας καταγραφής.

[21] Τέτοιες ενέργειες δικαιολογούνται για σοβαρές αιτίες όπως η απώλεια των δεδομένων μεγάλου αριθμού χρηστών.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

εκτέλεση συναλλαγών μπορεί να αποκλειστεί από τον εισβολέα που ελέγχει το δίκτυο. Προφανώς, αυτό το είδος επίθεσης επηρεάζει επίσης την ακεραιότητα των δεδομένων.

Ασφάλεια συσκευών: Αυτό το ζήτημα έχει δύο πτυχές, πρώτα αφορά τις επιθέσεις λυτρισμικού (ransomware), οι οποίες έχουν ασήμαντη επίπτωση στην περίπτωση ενός κατανεμημένου μητρώου καταγραφών. Όσο έστω και λίγοι κόμβοι δεν επηρεάζονται, το δίκτυο εξακολουθεί να διατηρεί ακέραιο το ακριβές αντίγραφο του κατανεμημένου μητρώου. Ωστόσο, η δεύτερη πτυχή είναι ότι ένας κόμβος που έχει εκτεθεί σε κακόβουλο λογισμικό μπορεί να εισάγει πλαστά / κακόβουλα δεδομένα στο δίκτυο.

Εκτός από αυτές τις προκλήσεις, υπάρχουν πολλές απειλές που μπορούν να επηρεάσουν το IoT, μεταξύ άλλων η υποκλοπή (eavesdropping), η άρνηση υπηρεσίας (denial of service) ή η απόκτηση του ελέγχου μίας IoT οντότητας (controlling). Αυτές οι συσκευές είναι πιο πιθανό να υποστούν ηλεκτρονική παρείσφρηση, αφού οι μειωμένες δυνατότητές τους τούς περιορίζουν ως προς τις ενημερώσεις υλικολογισμικού, εμποδίζοντας τους να προστατευθούν από πιθανά σφάλματα ή παραβιάσεις ασφαλείας. Επιπλέον, είναι μερικές φορές δύσκολο να ενημερωθούν οι συσκευές μία προς μία, σε σενάρια αναπτύξεις IoT που εκτείνονται σε παγκόσμια κλίμακα.

Ασφάλεια κατά την επικοινωνία: Η ολοκλήρωση του IoT και του BC μπορεί επίσης να έχει επιπτώσεις στις επικοινωνίες. Επί του παρόντος, τα πρωτόκολλα εφαρμογής IoT, όπως το CoAP και το MQTT, χρησιμοποιούν άλλα πρωτόκολλα ασφάλειας όπως το TLS ή το DTLS για την παροχή ασφαλών επικοινωνιών. Αυτά τα πρωτόκολλα ασφαλείας είναι πολυσύνθετα και βαριά και εκτός αυτού χαρακτηρίζονται από την ανάγκη κεντρικής διαχείρισης και διακυβέρνησης βασικών υποδομών, συνήθως με PKI.

4.3.3 Ιδιωτικότητα

Το BC προσφέρει πράγματι ένα ανυπέρβλητο νέο επίπεδο διαφάνειας που αναμφίβολα συμβάλλει στην οικοδόμηση εμπιστοσύνης. Ωστόσο, αυτή η διαφάνεια έχει αντίκτυπο στην ιδιωτική ζωή. Δεδομένου ότι το BC αποτελεί ένα δημόσιο μητρώο καταγραφών και ο καθένας μπορεί να δει όλες τις συναλλαγές σε ένα δίκτυο. Έτσι, παραμένουν ανησυχίες για την προστασία της ιδιωτικής ζωής των συναλλασσόμενων μερών.

Πολλές εφαρμογές IoT, όπως τα σενάρια που αφορούν το τομέα της υγείας λειτουργούν με ευαίσθητα δεδομένα (π.χ. μία συσκευή παρακολούθησης ζωτικών ενδείξεων είναι διασυνδεδεμένη με ένα άτομο). Σε τέτοιες περιπτώσεις καθίσταται απαραίτητο να αντιμετωπιστεί το πρόβλημα της ανωνυμίας τόσο σε επίπεδο ταυτότητας όσο και σε επίπεδο δεδομένων. Το πρόβλημα της προστασίας του ιδιωτικού απορρήτου των δεδομένων στις συσκευές του IoT ενέχει μεγάλο βαθμό δυσκολίας, δεδομένου ότι περιλαμβάνει πολλά στάδια: από τη συλλογή δεδομένων και επεκτείνεται μέχρι τα επίπεδα της επικοινωνίας και των εφαρμογών. Η εξασφάλιση της συσκευής ώστε τα δεδομένα να αποθηκεύονται με ασφάλεια και να μην έχουν πρόσβαση άτομα χωρίς άδεια είναι μια πρόκληση, καθώς απαιτεί την

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ενσωμάτωση κρυπτογραφικού λογισμικού ασφαλείας πάνω στη συσκευή. Τέτοιες λύσεις για είναι εφικτές και βιώσιμες, θα πρέπει να λαμβάνουν υπόψη την έλλειψη επαρκών υπολογιστικών πόρων των ίδιων των συσκευών καθώς και τους περιορισμούς που σχετίζονται με το οικονομικό κόστος.

Το BC παρουσιάζεται ως η ιδανική λύση για την αντιμετώπιση της διαχείρισης ταυτότητας στο IoT, ωστόσο όπως είδαμε και προηγουμένως, ενδέχεται να υπάρχουν εφαρμογές όπου πρέπει να διασφαλίζεται η πλήρης ανωνυμία. Η διατήρηση της ιδιωτικότητας στο BC είναι ένα πολύπλοκο ζήτημα. Κάθε συμμετέχουσα συσκευή αναγνωρίζεται από το δημόσιο κλειδί της (ή το hash του). Κατά τη συναλλαγή, οι συμμετέχοντες δεν χρειάζεται να γνωρίζουν το κλειδί όλων των άλλων κόμβων του δικτύου. Απλώς χρειάζονται το κλειδί του αντισυμβαλλομένου της συναλλαγής τους. Ωστόσο, όλες οι συναλλαγές σε ένα BC συμβαίνουν δημόσια και διαμοιράζονται στο δίκτυο. Αναλύοντας αυτά τα δεδομένα, ένα ενδιαφερόμενο μέρος μπορεί να εντοπίσει μοτίβα και να κάνει συνδέσεις μεταξύ διευθύνσεων και τελικά να οδηγηθεί σε εμπεριστατωμένα συμπεράσματα σχετικά με τις πραγματικές ταυτότητες των χρηστών.

Η ανωνυμία δεν είναι απαραίτητη σε όλες τις περιπτώσεις. Σε ορισμένα σενάρια όπου υπάρχει συλλογή δεδομένων, απαιτείται η διασφάλιση της ιδιωτικότητας των συναλλαγών καθώς ενδέχεται να επιτρέψουν την παρακολούθηση και την πρόβλεψη της συμπεριφοράς ή των συνηθειών των ανθρώπων. Αυτό έχει ήδη συμβεί σε τομείς όπως τα συστήματα μεταφοράς με χρήση καρτών RFID, όπου οι αποθηκευμένες πληροφορίες (δηλαδή δεδομένα σχετικά με ταξίδια που εκτελέστηκαν, χρηματικό υπόλοιπο, προσωπικά δεδομένα κλπ.) υποτίθεται ότι είναι ανώνυμες, αλλά στην πράξη μπορούν να συλλέγονται από τρίτους. Το ζήτημα γίνεται ακόμα πιο περίπλοκο όταν προστεθεί ένα BC, καθώς το περιεχόμενο κάθε συναλλαγής (ουσιαστικά τα δεδομένα που παράγει το ενοποιημένο σύστημα) εκτίθεται σε κάθε κόμβο του δικτύου, ώστε να μπορεί να επικυρωθεί. Αυτό σε ορισμένους κλάδους, όπως τη βιομηχανία ή το χρηματοπιστωτικό τομέα, δεν είναι θεμιτό αφού επιτρέπει την παρακολούθηση της δραστηριότητας των ανταγωνιστών (Christidis and Devetsikiotis, 2016; Bahga and Madisetti, 2016; Reyna et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018).

4.3.4 Νομοκανονιστικό Πλαίσιο

Το όραμα ενός συστήματος που λειτουργεί χωρίς να περιορίζεται από κανονισμούς είναι κατά πολύ υπεύθυνο για τη διάδοση και την επιτυχία του Bitcoin. Όπως φαίνεται, το BC, ειδικά στο πλαίσιο των ψηφιακών κρυπτονομισμάτων, έχει φέρει μαζί του πολλές αντιπαραθέσεις σχετικά με τη νομιμότητα. Δεδομένου ότι το BC καταργεί την ανάγκη για μια κεντρική αρχή ή έναν αξιόπιστο διαμεσολαβητή για την επικύρωση των συναλλαγών, παραμένουν κανονιστικά εμπόδια στην ευρεία αξιοποίηση της τεχνολογίας. Για τα αποκεντρωμένα συστήματα απαιτούνται νέοι κανονισμοί της εκάστοτε κυβέρνησης και κλάδου. Επιπλέον, υπάρχει ανάγκη να διασφαλιστεί η νομική ισχύς των έξυπνων συμβάσεων, προκειμένου να αποφευχθούν οι διενέξεις μεταξύ των συναλλασσόμενων μερών (Bahga and Madisetti, 2016; Reyna et al., 2018).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.3.4.1 Νομική Επιβολή Ευφυών Συμβολαίων

Μέχρι τώρα δεν έχουν θεσπιστεί κανόνες για την επιβολή ευφυών συμβολαίων και την εύρυθμη επίλυση τυχόν αντιπαραθέσεων. Καταβάλλονται προσπάθειες ώστε οι τεχνικοί κανόνες των SC να είναι νομικά εκτελεστοί και δεσμευτικοί για όλα τα μέρη. Μέχρι τότε εγείρονται ανησυχίες τί θα συμβεί εάν, παρά την επαληθευσιμότητα της συνολικής διαδικασίας, μια συναλλασσόμενη οντότητα αμφισβητήσει το αποτέλεσμα μιας ΕΣ. Λίγες κινήσεις έχουν πραγματοποιηθεί για τη δέσμευση συμβάσεων πραγματικού κόσμου με τις έξυπνες συμβάσεις και εξακολουθεί να αποτελεί ζήτημα που χρήζει περαιτέρω μελέτης (Christidis and Devetsikiotis, 2016; Fernández-Caramés and Fraga-Lamas, 2018).

4.3.4.2 Συμμόρφωση με το ΓΚΠΔ[22]

Ο νέος κανονισμός που τέθηκε σε ισχύ από τις 25 Μαΐου του 2018 παρέχει στους τελικούς χρήστες περισσότερα δικαιώματα για τα προσωπικά δεδομένα και θέτει νέες υποχρεώσεις στους υπεύθυνους επεξεργασίας δεδομένων. Σε ένα καθαρά αποκεντρωμένο BC σύστημα δεν υπάρχουν υπεύθυνοι επεξεργασίας των δεδομένων κάτι που καθιστά δύσκολη την εφαρμογή του κανονισμού. Επίσης, από την άλλη πλευρά, το δικαίωμα της λήθης[23], μία από τις βασικές κατευθυντήριες γραμμές του ΓΚΠΔ, είναι αντικρουόμενο με την κεντρική ιδέα της τεχνολογίας BC. Στα δημόσια BC, όλα τα δεδομένα αναπαράγονται και διαμοιράζονται σε όλες τις μηχανές του δικτύου.

4.3.4.3 Απαρχαιωμένη νομοθεσία

Ο τομέας IoT επηρεάζεται επίσης από τους νόμους ή τους κανονισμούς μίας χώρας σχετικά με την ιδιωτικότητα των δεδομένων. Οι περισσότεροι από αυτούς τους νόμους καθίστανται ξεπερασμένοι και πρέπει να αναθεωρηθούν, ειδικά έπειτα από την εμφάνιση νέων διεισδυτικών τεχνολογιών, όπως το BC. Η ανάπτυξη νέων νόμων και προτύπων μπορεί να διευκολύνει την πιστοποίηση των χαρακτηριστικών ασφαλείας των συσκευών και με αυτόν τον τρόπο να βοηθήσει στην κατασκευή του πιο ασφαλούς και αξιόπιστου δικτύου IoT. Υπό αυτή την έννοια, οι νόμοι που αφορούν την προστασία της ιδιωτικότητας και τη διαχείριση των πληροφοριών εξακολουθούν να αποτελούν μια μεγάλη πρόκληση που πρέπει να αντιμετωπιστεί στο IoT και, ως εκ τούτου, θα είναι ακόμη μεγαλύτερη πρόκληση εάν χρησιμοποιηθούν σε συνδυασμό με BC.

4.3.4.4 Αδυναμία αναίρεσης συναλλαγής και ανάκτησης χρημάτων

Όπως αναφέρθηκε, η έλλειψη κανονισμών λειτουργίας δημιουργεί μειονεκτήματα, επειδή δεν είναι δυνατοί οι μηχανισμοί για την ανάκτηση ή την επαναφορά του ιδιωτικού κλειδιού ή την αναίρεση μίας συναλλαγής. Νομοθετικές ρυθμίσεις για διεθνείς συναλλαγές: Η ΑΚ είναι μια νέα τεχνολογία που θα έχει τη δυνατότητα να συνδέει διαφορετικούς ανθρώπους από διαφορετικές χώρες χωρίς να ακολουθεί

[22] Γενικός Κανονισμός για την Προστασία των Δεδομένων.
[23] Άρθρο 17, § 1 του ΚΑΝΟΝΙΣΜΟΥ (ΕΕ) 2016/679.

κανένα νόμο ή κώδικα συμμόρφωσης, κάτι που αποτελεί σοβαρό ζήτημα τόσο για τους κατασκευαστές όσο και για τους παρόχους υπηρεσιών. Αυτή η πρόκληση θα αποτελέσει το κύριο εμπόδιο για την υιοθέτηση του blockchain σε πολλές επιχειρήσεις και εφαρμογές. Προστασία από παραπλάνηση: Ακόμη οι Fernández-Caramés and Fraga-Lamas, (2018) θίγουν το ζήτημα της προστασίας του κοινού και των επενδυτών παραθέτοντας την περίπτωση όπου ορισμένοι προγραμματιστές μπορούν να πλαστογραφήσουν τις επιδόσεις των BC τους, προκειμένου να προσελκύσουν επενδυτές με γνώμονα τα αναμενόμενα κέρδη.

4.3.5 Υιοθέτηση της τεχνολογίας

Για να διανθίσει μία τεχνολογία και να ενσωματωθεί στην καθημερινή μας ζωή και την κοινωνία, πρέπει να είναι αποδεκτή από την πλειοψηφία των κόσμου, να υπάρχει επαρκώς εκπαιδευμένο ανθρώπινο δυναμικό και να είναι σύμφωνη με τις πρακτικές της εκάστοτε κυβερνητικής αρχής. Παρακάτω αναλύουμε τέτοια ζητήματα που αποτελούν τροχοπέδη στην ομαλή ενσωμάτωση των τεχνολογιών του BC και IoT.

4.3.5.1 Ενημέρωση κοινού και έλλειψη δεξιοτήτων

Το BC είναι μια εκκολαπτόμενη τεχνολογία και απαντάται κυρίως στον χρηματοπιστωτικό τομέα με το Bitcoin να αποτελεί τη δημοφιλέστερη εφαρμογή. Η έλλειψη ενημέρωσης σχετικά με την εφαρμογή της τεχνολογίας BC σε άλλους τομείς επηρεάζει την ευρεία υιοθέτησή της. Ως εκ τούτου, λίγοι άνθρωποι έχουν βαθιά γνώση και δεξιότητες επί του θέματος, και αυτοί ασχολούνται κυρίως με τα οικονομικά. Σε άλλους τομείς, διακρίνεται μια ευρέως διαδεδομένη έλλειψη κατανόησης του τρόπου με τον οποίο λειτουργεί το BC. Υπάρχουν παντού έξυπνες συσκευές, και έτσι η υιοθέτηση του BC στο IoT θα είναι πολύ δύσκολη χωρίς την ευαισθητοποίηση του κοινού και εκπαίδευση όσων ασχολούνται με την τεχνολογία.

4.3.5.2 Ζητήματα διακυβέρνησης

Ένας από τους παράγοντες που μπορεί να εμποδίσουν την ευρεία υιοθέτηση μιας εφαρμογής BIoT είναι το γεγονός ότι το BC επιτρέπει την ψευδο-ανωνυμία (δηλ. οι χρήστες ή οι συσκευές αναγνωρίζονται από τις διευθύνσεις τους, αλλά δεν συνδέονται σαφώς με αυτές). Ορισμένες κυβερνήσεις κρατών πιθανόν να απαιτήσουν μια ισχυρή σχέση μεταξύ της πραγματικής – φυσικής και της διαδικτυακής ταυτότητας. Επιβαρυντικό στοιχείο στην όλη υπόθεση αποτελεί το γεγονός ότι επειδή οι συναλλαγές στο IoT δύναται να διεξαχθούν σε παγκόσμιο επίπεδο, ενδέχεται να μην είναι σαφές ποιά αρχή οφείλει να εκτελέσει αυτή την ταυτοποίηση.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.3.5.3 Αποτίμηση της αξίας των εξομοιωμένων αγαθών[24]

Μη αμελητέο είναι και το ζήτημα της αναμενόμενης αξίας των εξομοιωμένων αγαθών. Τα BC μεταξύ άλλων χρησιμοποιούνται και για την ανταλλαγή μαρκών (tokens), επειδή συνδέονται με κάποια αξία. Υπάρχουν ερωτήματα τα οποία προβληματίζουν και μπορούν δυνητικά να αποτρέψουν ένα άτομο από να χρησιμοποιήσει τη νέα αυτή τεχνολογία. Για παράδειγμα, στην περίπτωση που η συσκευή ενός χρήστη προσλαμβάνει και διατηρεί στην κατοχή της μάρκες ενός BC, πώς μπορεί ο χρήστης να εξαργυρώσει αυτές τις μάρκες στον πραγματικό κόσμο (να κάνει μία ανάληψη μετρητών όπως θα λέγαμε στον τραπεζικό τομέα), ποιά είναι τα εχέγγυα ως προς το χρήστη ότι αυτό θα συμβεί όταν το θελήσει; Σε ένα BC που δεν υποστηρίζει SC, η διπλή ολοκλήρωση δεν είναι επιλογή. Αν οι απαντήσεις δεν είναι προφανείς και ικανοποιητικά πειστικές ενδέχεται η τεχνολογία να μην αξιοποιηθεί από το ευρύ κοινό και αντίθετα να προτιμηθούν παραδοσιακές μορφές συναλλαγής.

4.4 Μέτρα Αντιμετώπισης Προκλήσεων

Για την αποκάλυψη ταυτότητας. Προσπαθώντας να περιοριστεί το ζήτημα της ιδιωτικότητας σε εφαρμογές που είναι κρίσιμης σημασίας μπορούμε α) Να γίνεται χρήση νέου κλειδιού για κάθε συναλλαγή ή διαφορετικό κλειδί ανά αντισυμβαλλόμενο, για να δυσχεράνει τον εντοπισμό προτύπων. Υπάρχουν ιεραρχικά ντετερμινιστικά πορτοφόλια που υποστηρίζουν την παραγωγή πλήθους κλειδιών και υποστηρίζονται από τα περισσότερα μεγάλα κρυπτονομίσματα. Το πρόβλημα είναι με κάθε συναλλαγή το νέο κλειδί πρέπει να γνωστοποιείται στον αντισυμβαλλόμενο το οποίο είναι πολύπλοκο και χρονοβόρο. β) Η διατήρηση διαφορετικών BC ανάλογα με το είδος της συναλλαγής που πραγματοποιούμε στην περίπτωση ιδιωτικών BC για να αποφευχθεί το φαινόμενο κάποιος στο δίκτυο να αποκτήσει ανταγωνιστικό πλεονέκτημα παρακολουθώντας τη δραστηριότητα της συσκευής. Συστήνεται παραμετροποίηση της αλυσίδας καταγραφών ώστε να επιτρέπεται μόνο αλληλεπίδραση με συγκεκριμένες οντότητες με τις οποίες είναι απαραίτητη η συνεργασία και μόνο για τις επιθυμητές ενέργειες. Η λύση αυτή αυξάνει το κόστος συντονισμού μεταξύ BC αλλά αποτελεί απαραίτητο συμβιβασμό για την ενίσχυση της ιδιωτικότητας.

Για τη διασφάλιση προσωπικών δεδομένων. Το περιεχόμενο κάθε συναλλαγής εκτίθεται σε κάθε κόμβο του δικτύου, ώστε να μπορεί να επικυρωθεί. Επομένως, για τη διατήρηση του απορρήτου των συναλλαγών μέσα σε ένα δίκτυο blockchain (αφορά και την εμπιστευτικότητα) προτείνεται η εφαρμογή ομομορφικής κρυπτογράφησης. Ένα τέτοιο είδος κρυπτογράφησης επιτρέπει στις IoT υπηρεσίες τρίτων μερών να επεξεργάζονται μια συναλλαγή χωρίς να αποκαλύπτει τα μη κρυπτογραφημένα δεδομένα σε αυτές τις υπηρεσίες. Προτάσεις παραλλαγών στο πρωτόκολλο του Bitcoin έχουν γίνει για τη χρήση ομοιομορφικών δεσμεύσεων χωρίς να αποκαλύπτουν τα μη κρυπτογραφημένα δεδομένα στις υπηρεσίες αυτές. Ένας άλλος τρόπος αντιμετώπισης του θέματος είναι μέσω των αποδείξεων μηδενικής

[24] Απόδοση του όρου “tokenized assets”.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

γνώσης (zero-knowledge proofs) που επιτρέπουν σε μία πλευρά να μπορεί να αποδείξει σε μία άλλη την εγκυρότητα μιας δήλωσης χωρίς να αποκαλύψει το περιεχόμενό της. Στην περίπτωση εφαρμογών IoT, μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας ή κατά τη διάρκεια τακτικών συναλλαγών, προκειμένου να αποφευχθεί η αποκάλυψη της ταυτότητας ενός χρήστη ή μιας συσκευής. Και οι δύο μέθοδοι είναι έχουν υψηλή κατανάλωση πόρων, οπότε η εφαρμογή του στις συσκευές IoT με περιορισμένες πηγές είναι επί του παρόντος περιορισμένη. Όπως στην περίπτωση της διατήρησης της ιδιωτικότητας, ένα BC που έχει συσταθεί για να εξυπηρετεί μια πολύ συγκεκριμένη διαδικασία και έπειτα από τη χρήση της απορρίπτεται, μπορεί να είναι μια αποδεκτή λύση (Christidis and Devetsikiotis, 2016; Fernández-Caramés and Fraga-Lamas, 2018).

Η προστασίας του ιδιωτικού απορρήτου των δεδομένων σε συσκευές IoT συνεπάγεται μεγαλύτερη δυσκολία. Η εξασφάλιση της συσκευής ώστε τα δεδομένα να αποθηκεύονται με ασφάλεια και να μην έχουν πρόσβαση σε άτομα χωρίς άδεια είναι μια πρόκληση, καθώς απαιτεί την ενσωμάτωση κρυπτογραφικού λογισμικού ασφαλείας στη συσκευή. Εγείρονται όμως ζητήματα διαθεσιμότητας πόρων και οικονομικής βιωσιμότητας. Πολλές τεχνολογίες έχουν χρησιμοποιηθεί για την εξασφάλιση επικοινωνιών με χρήση κρυπτογράφησης (IPsec, SSL / TLS, DTLS). Οι περιορισμοί της συσκευής IoT καθιστούν συχνά απαραίτητη τη χρήση λιγότερο περιορισμένων συσκευών, όπως πύλες για την ενσωμάτωση αυτών των πρωτοκόλλων ασφαλείας. Η χρήση κρυπτογραφικού υλισμικού θα μπορούσε να επιταχύνει τις κρυπτογραφικές διαδικασίες και να αποφευχθεί η υπερφόρτωση σύνθετων ασφαλών πρωτοκόλλων λογισμικού. Η προστασία των δεδομένων και της ιδιωτικής ζωής αποτελούν βασικές προκλήσεις. Άλλες τεχνικές είναι μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης σε ιδιωτικά BC, η χρήση SC για τη διαχείριση της ιδιωτικότητας των δεδομένων και η αποθήκευση εκτός αλυσίδας.

Για επεκτασιμότητα. Δεδομένου ότι το BC δεν μπορεί να επεξεργαστεί περισσότερα συναλλαγές από ότι ένας μόνο κόμβος, μία από τις μεθόδους που ερευνάται για να μειωθεί ο χρόνος επιβεβαίωσης συναλλαγών είναι το "Sharding". Αυτό σημαίνει ότι ένα υποσύνολο κόμβων επεξεργάζεται ένα υποσύνολο συναλλαγών. Το υποσύνολο των εξορυκτών θα πρέπει να συμπληρωθεί κατά τρόπο ώστε το σύστημα να είναι ακόμα ασφαλές και να μπορούν να υποβάλλονται σε επεξεργασία πολλές συναλλαγές ταυτόχρονα. Στην καθαρότερη μορφή του, κάθε τμήμα έχει το δικό της ιστορικό συναλλαγών και επηρεάζεται μόνο από τις συναλλαγές που περιέχει. Παραδείγματος χάριν, σε ένα BC πολλαπλών περιουσιακών στοιχείων, υπάρχουν n τμήματα (shards), και κάθε ένα συνδέεται με ένα συγκεκριμένο περιουσιακό στοιχείο. Σε πιο προχωρημένες μορφές, οι συναλλαγές σε ένα τμήμα μπορούν επίσης να προκαλέσουν γεγονότα σε κάποια άλλο τμήμα. Αυτό συνήθως ονομάζεται επικοινωνία μεταξύ τμημάτων. Ωστόσο, αυτή τη στιγμή βρίσκεται σε μια πρώιμη κατάσταση, υπάρχουν πολλές προκλήσεις που θα πρέπει να επιλυθούν πριν από την ευρεία υιοθέτηση του sharding. Ορισμένες από αυτές τις προκλήσεις περιλαμβάνουν: επικοινωνία μεταξύ των τμημάτων, ανίχνευση απάτης, χειραγώγηση μεμονωμένων τμημάτων και επιθέσεις διαθεσιμότητας δεδομένων.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μια άλλη προσέγγιση για τη μείωση του χρόνου επεξεργασίας συναλλαγών είναι η "Raiden". Προτείνει τη χρήση τεχνολογίας καναλιών κατάστασης (state channel) για την εκτός αλυσίδας (off-chain) επεκτασιμότητα του δικτύου Ethereum και τη διευκόλυνση των μικροσυναλλαγών μεταξύ συσκευών IoT. Οι συναλλαγές εκτός αλυσίδας θα επιτρέψουν σε ένα σύνολο κόμβων να δημιουργήσουν κανάλια πληρωμής μεταξύ τους, χωρίς να πραγματοποιούν απευθείας συναλλαγές με το BC του Ethereum. Ως εκ τούτου, οι συναλλαγές εκτός αλυσίδας θα είναι ταχύτερες και φθηνότερες από εκείνες επί της αλυσίδας, επειδή μπορούν να καταγραφούν αμέσως και δεν υπάρχει λόγος να περιμένουν επιβεβαίωση από μπλοκ. Ωστόσο, πιστεύεται ότι οι στρατηγικές βασισμένες σε κανάλια μπορούν να αυξήσουν την κλιμάκωση των συναλλαγών μόνο αλλά δεν μπορούν να κλιμακώσουν την αποθηκευτική δυνατότητα. Επιπλέον, είναι ευάλωτες σε επιθέσεις DoS.

Γενικά, αναμένουμε ότι τα συστήματα BC θα ωριμάσουν και θα βελτιωθούν περαιτέρω όσον αφορά την ικανότητα κλιμάκωσης και την ιδιωτικότητα στο μέλλον, συνδυάζοντας και εφαρμόζοντας ιδέες όπως, για παράδειγμα, νέους αλγόριθμους συναίνεσης, το "sharing" ή η ομομορφική κρυπτογράφηση. (Eberhardt and Tai, 2017).

Για Χρονική Καθυστέρηση**.** Σε ένα BC που βασίζεται στην PoW, η μείωση του χρόνου δημιουργίας νέου μπλοκ μειώνει τον χρόνο επιβεβαίωσης των συναλλαγών αλλά για να επιτευχθεί το ίδιο επίπεδο ασφάλειας με τον χρόνο εξόρυξης των 10 λεπτών, μία συναλλαγή πρέπει να περιμένει περισσότερες επιβεβαιώσεις εξαιτίας της μικρότερης δυσκολίας εξόρυξης ενός μπλοκ. Επιπλέον, με μικρότερους χρόνους εξόρυξης, θα υπάρξουν περισσότερα stale μπλοκ, συνεπώς, αύξηση της σπατάλης υπολογιστικών και ενεργειακών πόρων. Ένας άλλος παράγοντας που σχετίζεται με την καθυστέρηση των συναλλαγών είναι το μέγεθος του μπλοκ. Υπάρχει η πεποίθηση ότι αυξάνοντας το μέγεθος του μπλοκ, για παράδειγμα από 1MB έως 2MB σε blockchain Bitcoin, η απόδοση μπορεί να αυξηθεί. Αλλά στην πραγματικότητα, ένα μεγαλύτερο μπλοκ θα διαρκέσει περισσότερο για να διαδοθεί στο δίκτυο. Ως εκ τούτου, οι κόμβοι με συνδέσεις χαμηλού εύρους ζώνης στο διαδίκτυο θα υποφέρουν ενώ εύποροι εξορύκτες με περισσότερο εύρος ζώνης θα υπερέχουν. Επιπλέον, ένα αυξημένο μέγεθος μπλοκ θα έχει επίσης ως αποτέλεσμα την ταχύτερη ανάπτυξη του μεγέθους blockchain, που θα επηρεάσει τον αριθμό των πλήρων κόμβων στο δίκτυο, καθώς απαιτούνται περισσότεροι πόροι για την αποθήκευση του πλήρους BC.

Για την αξιοπιστία χρησμών. Οι επιπτώσεις θα μπορούσαν να μετριαστούν μερικώς, βασιζόμενοι σε περισσότερα από ένα χρησμούς, που έλαβαν πληροφορίες από διαφορετικές πηγές (Gatteschi et al., 2018).

Για την ασφάλεια συσκευών. Για το λόγο αυτό, οι συσκευές IoT θα πρέπει να ελέγχονται διεξοδικά πριν από την ενσωμάτωσή τους στο BC, θα πρέπει να τοποθετούνται και να εγκαθίστανται σε κατάλληλο μέρος προς αποφυγή φυσικών ζημιών και υλοποίηση τεχνικών ανίχνευσης βλαβών μόλις συμβούν.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Για τη νομική επιβολή SC. Ένας τρόπος για να αυξηθούν οι πιθανότητες νομικής επιβολής είναι να συμπεριληφθεί αναφορά μέσα στην φυσική σύμβαση στον πραγματικό κόσμο του έξυπνου συμβολαίου και αντίστροφα – περίπτωση της διπλής ολοκλήρωσης. Αν προκύψει οποιαδήποτε νομική διένεξη, με την επίδειξη του κρυπτογραφικού αποτυπώματος που έχει αποθηκευτεί στο ΕΣ και έπειτα παρουσιάζοντας τη φυσική σύμβαση στον πραγματικό κόσμο (που προσδιορίζεται με μοναδικό τρόπο από αυτό το προαναφερθέν αποτύπωμα) μπορεί να αποδειχθεί ο συσχετισμός μεταξύ των ενεργειών στο BC και του προσδοκώμενου αποτελέσματος τον φυσικό κόσμο (Christidis and Devetsikiotis, 2016).

Για συμμόρφωση με ΓΚΠΔ. Οι Ferrag et al. (2018) ισχυρίζονται στα δημόσια BC όλα τα δεδομένα αντιγράφονται και διανέμονται στο δίκτυο και πως μόνο ο συνδυασμός ΑΚ με αξιόπιστες λύσεις υλισμικού μπορεί να λύσει αυτό το ζήτημα και ότι κάποιες αρχικές προσπάθειες έχουν ήδη αναληφθεί αλλά αυτός είναι ένας ελπιδοφόρος τομέας έρευνας για το εγγύς μέλλον.

Για την λύση της αποτίμησης της αξίας των εξομοιωμένων αγαθών, Και εδώ μπορεί να βοηθήσει η διπλή ολοκλήρωση. Παράγωγή ενός κρυπτογραφικού αποτυπώματος που προκύπτει από την λειτουργία μιας συνάρτησης κατακερματισμού πάνω σε μια φυσική σύμβαση στον πραγματικό κόσμο και ενσωμάτωση αυτού του αποτυπώματος ως μεταδεδομένο στις μάρκες που ανταλλάσσονται (δηλαδή, συμβολαιογραφική πράξη με κρυπτογραφικό αποτύπωμα). Σε όλες τις περιπτώσεις, οι συμμετέχοντες δόκιμο είναι να εξετάζουν εκ των προτέρων ποιος είναι πίσω από τα ανταλλασσόμενα αγαθά και να αξιολογεί τις διαβεβαιώσεις που έχει σχετικά με την αξία τους (Christidis and Devetsikiotis, 2016).

Για την ενεργειακή αποδοτικότητα. Στα δίκτυα P2P, είναι απαραίτητο να επικοινωνούν οι διομότιμο για να διανέμουν τα μπλοκ. όσο περισσότερες ενημερώσεις λαμβάνει ένα BC τόσο περισσότερη κατανάλωση ενέργειας αφιερώνεται στις επικοινωνίες. Για να μειωθεί ο αριθμός των ενημερώσεων, τα mini-BC επιτρέπουν στους κόμβους IoT να αλληλεπιδρούν άμεσα με μία αλυσίδα καταγραφών, καθώς διατηρούν μόνο τις πιο πρόσφατες συναλλαγές και μειώνουν τις υπολογιστικές απαιτήσεις ενός πλήρους κόμβου (Fernández-Caramés and Fraga-Lamas, 2018).

Για τη χαμηλή χωρητικότητα αποθήκευσης και τον περιορισμό κλιμακωσιμότητας εξαιτίας του μεγέθους του BC. Και εδώ μπορεί να συνεισφέρει η ενσωμάτωση του mini-BC. Ένα τέτοιο BC εισάγει την έννοια του δέντρου λογαριασμών, το οποίο αποθηκεύει την τρέχουσα κατάσταση κάθε χρήστη (κάθε διεύθυνσης για την ακρίβεια). Επομένως, μόνο η πιο πρόσφατη συναλλαγή πρέπει να αποθηκευτεί στο BC μαζί με το δέντρο λογαριασμού. Επομένως, το μέγεθος αυξάνεται μόνο όταν οι νέοι χρήστες προστίθενται στο blockchain (Fernández-Caramés and Fraga-Lamas, 2018).

Για τον περιορισμό του εύρους ζώνης**.** Ο καθορισμός του μεγέθους της συναλλαγής και του μπλοκ πρέπει να λάβουν υπόψιν τους περιορισμούς του εύρους ζώνης των δικτύων IoT κατά την κλιμάκωσή τους. Πολλές μικρές συναλλαγές θα αυξήσουν την κατανάλωση ενέργειας (από την αύξηση

επικοινωνίας) αντιθέτως μερικές μεγάλες μπορεί να περιλαμβάνουν μεγάλα ωφέλιμα φορτία που δεν μπορούν να αντιμετωπιστούν από ορισμένες IoT συσκευές (Fernández-Caramés and Fraga-Lamas, 2018).

4.5 Η Περίπτωση του Έξυπνου Σπιτιού

Όπως είδαμε σε προηγούμενη υποενότητα, το έξυπνο σπίτι είναι μία από τις γνωστές εφαρμογές BC σε IoT περιβάλλοντα. Μεταξύ άλλων είδαμε ότι έχουν ζητήματα ασφάλειας και ιδιωτικότητας, ετερογένειας των πόρων στις συσκευές και πολλά σημεία επιθέσεων. Έτσι, αναδύεται η λύση του BC λόγω της κατανεμημένης, ασφαλούς και ιδιωτικής φύσης του. Το PoW όμως απαιτεί υψηλούς πόρους και επειδή δεν μπορεί να επιτευχθεί με συμβατούς υπολογιστές σε ορισμένες περιπτώσεις γίνεται χρήση εξελιγμένου υλισμικού. Ακόμη ενέχει μεγάλες χρονικές καθυστερήσεις και χαμηλή κλιμακωσιμότητα εξαιτίας της κατανομής των μπλοκ στο δίκτυο. Για αυτούς τους λόγους προτείνεται η εξάλειψή του και η εφαρμογή μιας ιεραρχικής δομής με κατανεμημένη εμπιστοσύνη με βάση πρόσφατες έρευνες (Dorri et al., 2017; Dorri, Kanhere and Jurdak, 2016; Dorri, Kanhere and Jurdak, 2017).

Στόχος της προτεινόμενης λύσης είναι η εισαγωγή ενός νέου τύπου BC που έχει βελτιστοποιηθεί για το IoT. Για τον έλεγχο της λύσης, χρησιμοποιείται το σενάριο ενός έξυπνου σπιτιού ως αντιπροσωπευτικό για ποικίλες περιπτώσεις χρήσης IoT που η αρχιτεκτονική αυτή είναι εφαρμόσιμη. Γίνεται χρήση διαφορετικών BC αναλόγως με το σε ποιο επίπεδο λαμβάνει χώρα μία συναλλαγή. Μέσα στο έξυπνο σπίτι χρησιμοποιείται μία ελαφριά υλοποίηση του BC που διατηρεί τα βασικά πλεονεκτήματα της προστασίας της ιδιωτικότητας και ασφάλειας, εξαλείφοντας γνωστά IoT ζητήματα. Υιοθετείται μια ιεραρχική δομή για τη βελτιστοποίηση της κατανάλωσης πόρων και την αύξηση της επεκτασιμότητας του δικτύου. Το πλαίσιο αποτελείται από τρία επίπεδα: το έξυπνο σπίτι, το δίκτυο επικάλυψης και το αποθηκευτικό νέφος.

4.5.1 Αρχιτεκτονική Δομή

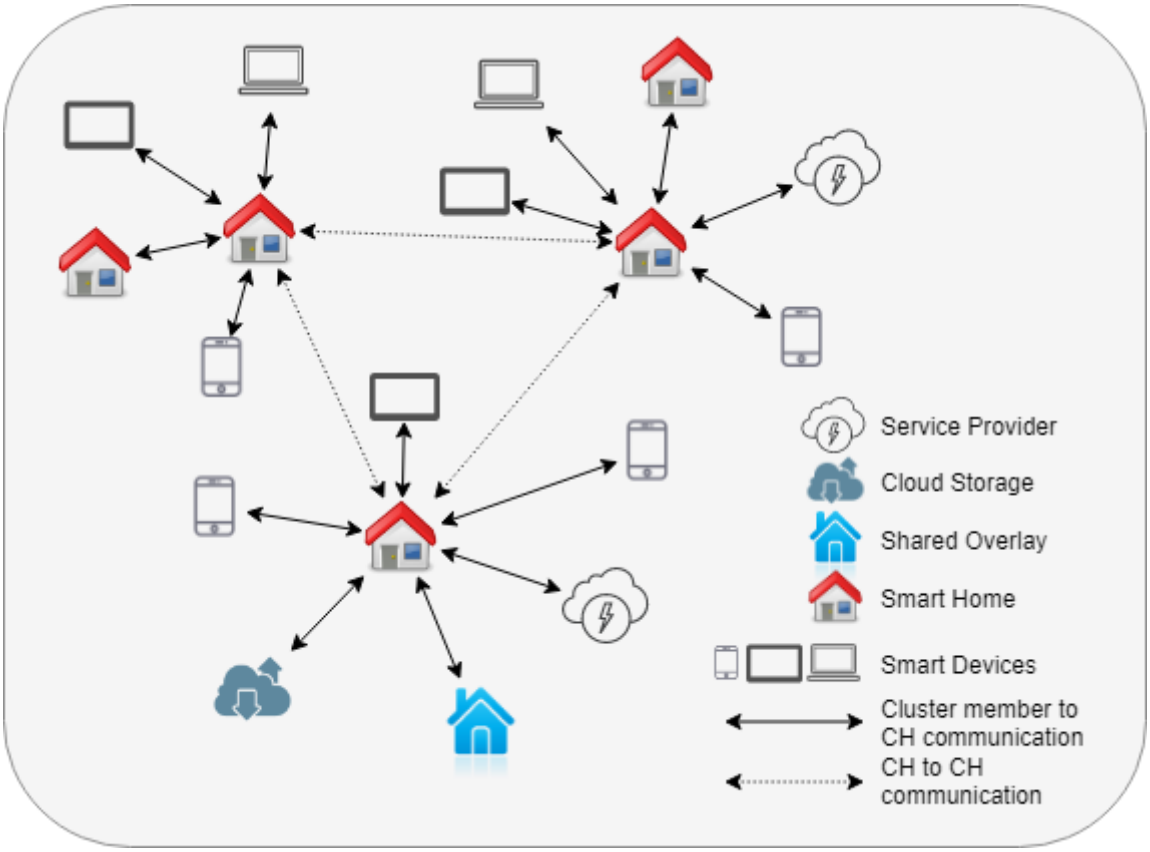
Η αρχιτεκτονική του δομή αποτελείται από τρία συστατικά μέρη που αναλύονται εν συνεχεία:

4.5.1.1 Αποθηκευτικό νέφος

Το αποθηκευτικό νέφος (cloud storage – CS) χρησιμοποιείται για το διαμοιρασμό και την αποθήκευση των δεδομένων. Σε μερικές περιπτώσεις ο χρήστης επιθυμεί να αποθηκεύει εκεί τα δεδομένα του ώστε ένα τρίτο μέρος, δηλαδή ένας πάροχος υπηρεσιών (SP), να έχει πρόσβαση στα δεδομένα συσκευών του έξυπνου σπιτιού για να παρέχει έξυπνες και εξατομικευμένες υπηρεσίες. Τα δεδομένα των χρήστη αποθηκεύονται σε μπλοκ με ένα *μοναδικό αριθμό μπλοκ* και *hash* τα οποία χρησιμοποιούνται για αυθεντικοποίηση. Δηλαδή αν ο χρήστης δώσει έναν έγκυρο αριθμό μπλοκ και hash το οποίο εντοπίσει το CS, τότε ο χρήστης αυτομάτως έχει αυθεντικοποιηθεί. Αφού ολοκληρωθεί η αποθήκευση, ο αριθμός μπλοκ κρυπτογραφείται με βάση ένα κοινό κλειδί που παράγεται με τη μέθοδο ανταλλαγής κλειδιών

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Diffie-Hellman. Έτσι εξασφαλίζεται ότι μόνο όποιος έχει στην κατοχή του το κοινό κλειδί είναι σε θέση να γνωρίζει τον αριθμό μπλοκ και κανένας άλλος. Επίσης, ένας χρήστης δύναται να δημιουργήσει ένα κοινό μητρώο για όλες τις συσκευές του είτε διαφορετικά μητρώα καταγραφών για κάθε συσκευή αν θέλει ο SP να έχει πρόσβαση σε όλο το ιστορικό της συσκευής.



Επισκόπηση προτεινόμενης αρχιτεκτονικής. Αναπαραγωγή από Dorri et al. (2017)

4.5.1.2 Δίκτυο επικάλυψης

Συσκευές με επάρκεια πόρων δημιουργούν ένα δίκτυο επικάλυψης για την υλοποίηση ενός κατανεμημένου δημόσιου BC που προσφέρει ασφάλεια και ιδιωτικότητα από άκρο σε άκρο. Το δίκτυο επικάλυψης αποτελείται από έξυπνα σπίτια (SH), παρόχους υπηρεσιών (SP), αποθηκευτικό νέφος (CS), έξυπνα κινητά ή/και ηλεκτρονικούς υπολογιστές. Η δομή του είναι παρόμοια με αυτή των διομότιμων δικτύων. Πιο συγκεκριμένα οι κόμβοι είναι χωρισμένοι σε *συστάδες* (clusters) οι οποίες διατηρούν εκλεγμένους *επικεφαλής συστάδων* (cluster heads - CH) μεταξύ των οποίων σχηματίζεται ένα δίκτυο BC. Κάθε κόμβος μπορεί να αλλάξει *συστάδα* κατά το δοκούν αν βιώνει μεγάλες καθυστερήσεις ενώ και οι κόμβοι έχουν το δικαίωμα να εκλέξουν νέο CH. Ένας CH διατηρεί τρεις λίστες: μία λίστα με τα δημόσια κλειδιά των *αιτούντων* που έχουν πρόσβαση στα δεδομένα των έξυπνων σπιτιών, άλλη μία λίστα με τα δημόσια κλειδιά των *αιτούμενων* έξυπνων σπιτιών (για την ακρίβεια των υπολογιστών που τα διαχειρίζονται) που συνδέονται σε αυτό και μία τρίτη λίστα με τις συναλλαγές που απεστάλησαν σε άλλους CH στο δίκτυο. Κάθε κόμβος χρησιμοποιεί το Tor για να συνδεθεί με το δίκτυο επικάλυψης

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

για επιπλέον ανωνυμία στο επίπεδο IP. Κάθε χρήστης μπορεί να έχει περισσότερους από έναν κόμβους στο δίκτυο επικάλυψης. Το κοινόχρηστο BC διατηρείται από τους CH και εμπεριέχει διάφορες συναλλαγές πολλαπλής υπογραφής για παρακολούθηση και πρόσβαση. Οι συναλλαγές πολλαπλής υπογραφής είναι συναλλαγές που πρέπει να υπογραφούν από δύο - έναν *αιτών* κι έναν *αιτούντα*. Σε αντίθεση με το κλασικό BC, εδώ κάθε CH αποφασίζει ανεξάρτητα αν θα διατηρήσει ή θα απορρίψει ένα μπλοκ ανάλογα με το ποιοι είναι οι συμμετέχοντες σε μία συναλλαγή. Έτσι, δεν υπάρχει ανάγκη συγχρονισμού των CH και άρα μειώνονται οι επιβαρύνσεις συγχρονισμού.

4.5.1.3 Έξυπνο σπίτι (τοπικό δίκτυο)

Το έξυπνο σπίτι εν συντομία αποτελείται από:

- Μία συσκευή με επαρκείς πόρους (π.χ. ένας H/Y) και σταθερή σύνδεση στο διαδίκτυο, επιφορτισμένη με το ρόλο του εξορύκτη, υπεύθυνη για το χειρισμό των επικοινωνιών μέσα και έξω από το σπίτι. Θα αναφερόμαστε σε αυτή ως *εξορύκτης έξυπνου σπιτιού* (SHM).
- Συσκευές IoT (π.χ. έξυπνος θερμοστάτης, έξυπνοι λαμπτήρες, κάμερες IP) και αισθητήρες.
- Ένα ιδιωτικό και ασφαλές BC για τη ρύθμιση και τον έλεγχο των επικοινωνιών.
- Τοπικό αποθηκευτικό χώρο (π.χ. ένας backup σκληρός).

4.5.2 Βασικά συστατικά έξυπνου σπιτιού

4.5.2.1 Επιτρεπτές συναλλαγές

Οι επιτρεπτές συναλλαγές σε ένα έξυπνο σπίτι συνοπτικά είναι οι κάτωθι:

- Αποθήκευσης δεδομένων από συσκευές (*store*)
- Πρόσβασης από SP στις συσκευές ή από τον ιδιοκτήτη προς το CS (*access*)
- Παρακολούθησης από τον ιδιοκτήτη προς τις συσκευές (*monitor*)
- Προσθήκης συσκευής στο έξυπνο σπίτι (*genesis*)
- Αφαίρεση συσκευής από το έξυπνο σπίτι (*remove*)

Κάθε είδος συναλλαγής έχει ένα κοινό κλειδί για διασφάλιση της επικοινωνίας και γίνεται χρήση ελαφριάς μορφής κρυπτογράφησης όπως θα αναλύσουμε παρακάτω.

4.5.2.2 Τοπικό BC

Το τοπικό BC σε ένα SH χρησιμοποιείται για α) την καταγραφή και παρακολούθηση του ιστορικού των συσκευών και β) την πολιτική εξουσιοδότησης συσκευών και την επιβολή της πολιτικής ελέγχου πρόσβασης του ιδιοκτήτη στο σπίτι του, σχετικά με τις εισερχόμενες κι εξερχόμενες συναλλαγές. Σε αντίθεση με το αποκεντρωμένο BC, αυτό το διαχειρίζεται κεντρικά ο ιδιοκτήτης του σπιτιού μέσω του τοπικού SHM. Κανένα εκ των δύο δεν εκτελεί την PoW.

Στη συνέχεια θα δούμε τη δομή μπλοκ, της κεφαλίδας πολιτικής και των συναλλαγών. Κάθε μπλοκ περιέχει τρία μέρη: την κεφαλίδα του η οποία εμπεριέχει το hash προηγούμενου μπλοκ ώστε να διατηρείται αμετάβλητο το BC, την κεφαλίδα πολιτικής που χρησιμεύει στην εξουσιοδότηση συσκευών και την εφαρμογή της πολιτικής του ιδιοκτήτη για το σπίτι του και ένα αριθμό από συναλλαγές. Η δομή των δύο τελευταίων παρατίθεται σε επόμενους πίνακες.

4.5.2.3 Εξορύκτης Έξυπνου Σπιτιού (SHM)

Συσκευή που διαχειρίζεται τις εντός και εκτός συναλλαγές του έξυπνου σπιτιού. Συνδέεται άμεσα ή έμμεσα με μία συσκευή πύλης δικτύου. Είναι υπεύθυνη για αυθεντικοποίηση, εξουσιοδότηση, έλεγχο συναλλαγών, παραγωγή συναλλαγών genesis, διανομή και ανανέωση κλειδιών, αλλαγή δομής συναλλαγών, δημιουργία και διαχείριση συστάδων.

4.5.2.4 Τοπική αποθήκευση

Μία αποθηκευτική συσκευή για την τοπική αποθήκευση των δεδομένων είτε ενσωματωμένη στον SHM είτε χωριστή. Διατηρεί ξεχωριστά μητρώα καταγραφών για κάθε συσκευή.

Παράμετρος Μπλοκ	**Περιεχόμενο**
Requester	Δημόσιο κλειδί αιτούντα (για τοπικές συσκευές είναι ίδιο με το *Device ID*).
Requested for	Ενέργεια προς αίτηση (μία από τις επιτρεπτές συναλλαγές).
Device ID	Το αναγνωριστικό μίας συσκευής μέσα στο έξυπνο σπίτι.
Action	Ενέργεια με βάση τις προηγούμενες παραμέτρους (πχ να επιτραπεί, να αρνηθεί).

Πίνακας δομής κεφαλίδας πολιτικής. Βασισμένο στο Dorri et al. (2017)

Παράμετρος Συναλλαγής	**Περιεχόμενο**
Previous Transaction Transaction Number	Αριθμοί για ιχνηλασία συναλλαγών ίδιας συσκευής και χρήση ως μοναδικό αναγνωριστικό.
Device ID	Το αναγνωριστικό μίας συσκευής μέσα στο έξυπνο σπίτι.
Transaction Type	Είδος συναλλαγής. Μπορεί να είναι *store, access, monitor, genesis,*
Corresponding Multisig Transaction	Χρησιμοποιείται μόνο για συναλλαγές από το δίκτυο επικάλυψης.

Πίνακας δομής συναλλαγών. Βασισμένο στο Dorri et al. (2017)

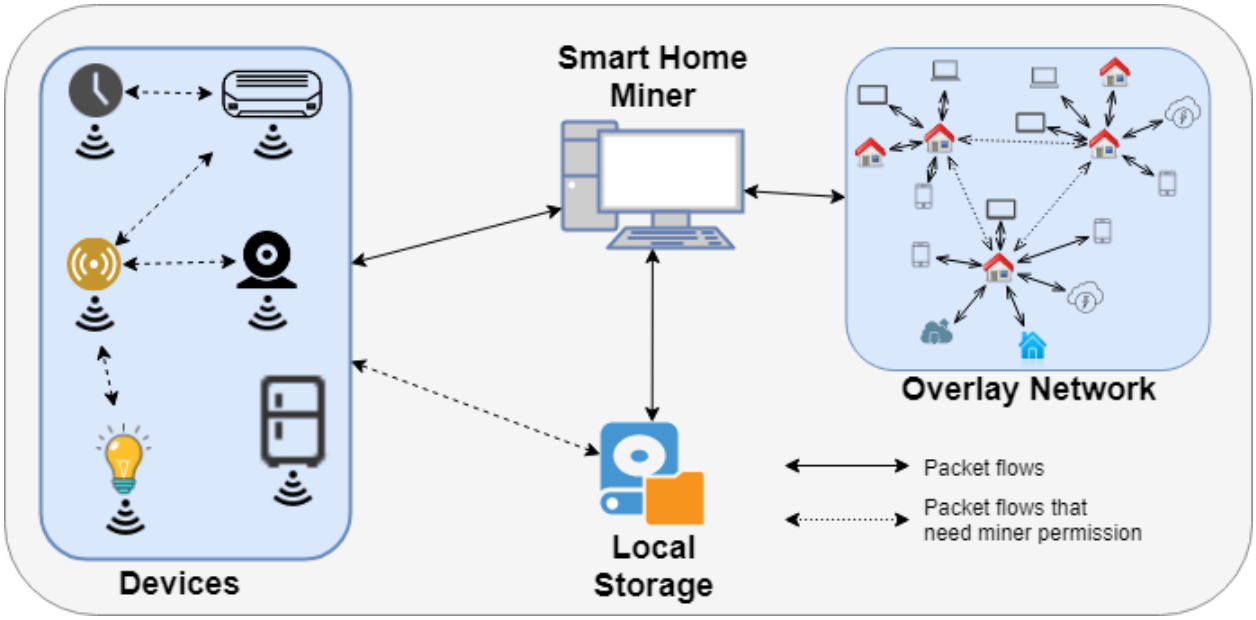
4.5.3 Αρχική διαμόρφωση στο έξυπνο σπίτι

4.5.3.1 Διαδικασία ένταξης νέας συσκευής

Αρχικά γίνεται δημιουργία ενός κοινού κλειδιού μεταξύ του SHM και της συσκευής με βάση την ανταλλαγή κλειδιών Diffie-Hellman. Ο SHM εκτελεί μία συναλλαγή *genesis* ώστε να αποθηκευτεί το κοινό κλειδί και έτσι ουσιαστικά επιτελείται η προσθήκη μίας νέας συσκευής.

4.5.3.2 Διαμόρφωση κεφαλίδας πολιτικής

Ο εκάστοτε ιδιοκτήτης του σπιτιού ορίζει την δική του πολιτική εξουσιοδότησης συσκευών και ελέγχου πρόσβασης προς αυτές σύμφωνα με την προαναφερθείσα δομή και την προσθέτει στην κεφαλίδα πολιτικής στο πρώτο μπλοκ. Κατά τη λειτουργία, λαμβάνεται υπόψιν η κεφαλίδα πολιτικής του τελευταίου μπλοκ, οπότε η όποια ενημέρωση πολιτικής πραγματοποιείται από τον κάτοχο, αλλάζοντας την κεφαλίδα πολιτικής του τελευταίου μπλοκ.



Επισκόπηση Έξυπνου Σπιτιού. Αναπαραγωγή από Dorri et al. (2017)

4.5.4 Διαχείριση των συναλλαγών

Η μέθοδος αλληλεπίδρασης μεταξύ συσκευών έχει δύο οφέλη, την παρακολούθηση των συσκευών που ανταλλάσσουν δεδομένα μεταξύ τους από τον SHM και ότι η επικοινωνία μεταξύ τους διασφαλίζεται με ένα κοινό κλειδί.

Μεταξύ συσκευών επικοινωνία. Για την εντός έξυπνου σπιτιού επικοινωνία (π.χ. ένας έξυπνος λαμπτήρας ζητά δεδομένα από ένα αισθητήρα κίνησης για να ανάψει το φως), ο SHM ελέγχει την πολιτική του ιδιοκτήτη αναφορικά με τις συσκευές και αν το επιτρέπει εκδίδει και διαμοιράζει ένα κοινό κλειδί μεταξύ τους. Πλέον οι συσκευές επικοινωνούν απευθείας με τη χρήση του κοινού τους

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κλειδιού. Στην περίπτωση που ο ιδιοκτήτης αλλάξει την πολιτική που αφορά τις συσκευές, γίνεται ανάκληση αδείας αποστέλλοντας στις αντίστοιχες συσκευές ότι το κλειδί τους δεν είναι πλέον έγκυρο.

Συναλλαγές αποθήκευσης τοπικά. Οι συσκευές μέσα στο έξυπνο σπίτι έχουν απαιτήσεις διατήρησης των δεδομένων τους τοπικά ή στο νέφος. Η τοπική αποθήκευση γίνεται μέσω μίας συναλλαγής store από τη συσκευή στον SHM, ελέγχου της πολιτικής για τα δικαιώματα της συσκευής και έκδοση και διαμοιρασμό κοινού κλειδιού στη συσκευή και την μονάδα αποθήκευσης. Μέσω του κοινού κλειδιού η αποθηκευτική μονάδα πραγματοποιεί έλεγχο αυθεντικοποίησης. Με τη λήψη του κλειδιού από τον SHM δημιουργεί ένα αρχικό σημείο για τα δεδομένα της συσκευής και η τελευταία μπορεί πλέον να επικοινωνεί απευθείας και να στέλνει τα δεδομένα της για αποθήκευση.

Συναλλαγές αποθήκευσης στο νέφος. Αρχικά ο SHM στέλνει στο νέφος μία αίτηση, δημιουργείται ένα αρχικό σημείο για τα δεδομένα της συσκευής και το επιστρέφει στον SHM. Όταν μία συσκευή στείλει μία αίτηση μαζί με τα δεδομένα της προς αποθήκευση στον SHM, τότε αυτός εξουσιοδοτεί τη συσκευή, ελέγχει τον αριθμό του τελευταίου μπλοκ και hash που έχει διατηρήσει στο τοπικό BC για αυτή και δημιουργεί ένα τυχαίο αριθμό ID. Έπειτα δημιουργεί μία συναλλαγή *store* με τα προαναφερθέντα δεδομένα και υπολογίζει το hash της και τα αποστέλλει μαζί στον απομακρυσμένο αποθηκευτικό χώρο. Εκεί, πρώτα εκτελείται έλεγχος αν η συναλλαγή είναι έγκυρη και αν υπάρχει διαθέσιμος χώρος. Μετά γίνεται υπολογισμός του hash των πακέτων που παρελήφθησαν και αν ταιριάζει με το hash που έλαβε επιτρέπει την αποθήκευση. Αν όλα είναι θετικά, εκτελείται η αποθήκευση και επιστρέφεται ο νέος αριθμός μπλοκ μαζί με το hash του ώστε να χρησιμοποιηθεί σε επόμενες συναλλαγές *store*.

Οι δύο τελευταίες συναλλαγές, της πρόσβασης και της παρακολούθησης αφορούν τον ιδιοκτήτη του σπιτιού που μπορεί να βρίσκεται κάπου απομακρυσμένα αλλά και τους SP στην προσπάθειά τους να παράσχουν προσωποποιημένες υπηρεσίες.

Συναλλαγές πρόσβασης. Ο SP μπορεί να χρειάζεται πρόσβαση σε πρόσφατα δεδομένα της συσκευής ή και σε ολόκληρο το ιστορικό της για να παρέχει ορισμένες υπηρεσίες. Για το σκοπό αυτό, δημιουργεί και υπογράφει μία *συναλλαγή πολλαπλών υπογραφών πρόσβασης (access)* και την προωθεί στον CH του. Εκείνος με βάση τη λίστες των *αιτούντων* και των *αιτούμενων* ελέγχει αν εμπεριέχεται σε κάποια από αυτές και αν ισχύει διαμοιράζει τη συναλλαγής στη συστάδα του. Ειδάλλως, την προωθεί σε άλλους CH και εγγράφει το δημόσιο κλειδί του αιτούμενου στην τρίτη λίστα. Όταν φτάσει η συναλλαγή στον SHM, εκείνος ελέγχει αν με βάση την πολιτική του ιδιοκτήτη επιτρέπεται πρόσβαση στον SP για τη συγκεκριμένη *access* συναλλαγή και έπειτα αν τα δεδομένα είναι αποθηκευμένα τοπικά ή στο νέφος. Για την πρώτη περίπτωση τα ανακτά από την αποθηκευτική συσκευή, τα κρυπτογραφεί και τα αποστέλλει στον αιτούντα ενώ για τη δεύτερη υπάρχουν δύο προσεγγίσεις. Η απλή είναι να ζητήσει ο SHM τα δεδομένα από το νέφος και να τα στείλει. Αλλιώς, παραδίδει στον αιτούντα τον αριθμό του τελευταίου μπλοκ και το hash του ώστε να δει ολόκληρο το ιστορικό της συσκευής. Αυτό προτιμάται όταν τα αποθηκευμένα δεδομένα σχετίζονται μόνο με μία συσκευή. Κατόπιν υπογράφει και ο SHM τη

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

συναλλαγή και την αποστέλλει σε διάφορους CH ώστε να αποθηκευτεί και στο δίκτυο επικάλυψης. Μπορεί να επιλέξει να μην το κάνει αν θέλει να διατηρήσει μεγαλύτερο επίπεδο ιδιωτικότητας. Όλοι οι CH που προώθησαν τη συναλλαγή καθώς και οι CH του *αιτούντα* και του *αιτούμενου* αποφασίζουν να αποθηκεύσουν τη συναλλαγή στο BC τους.

Συναλλαγές παρακολούθησης. Ο ιδιοκτήτης μπορεί να επιθυμεί πρόσβαση στα δεδομένα μίας συσκευής σε πραγματικό χρόνο. Όταν ο SHM λάβει μία συναλλαγή *monitor*, ελέγχει αν ο αιτών έχει δικαίωμα λήψης δεδομένων από τη συγκεκριμένη συσκευή που ζητά. Στην περίπτωση που έχει, ο SHM του αποστέλλει περιοδικά δεδομένα μέχρι να λάβει μία ειδοποίηση να σταματήσει ή έως ότου λήξει το διάστημα ασφαλείας (*threshold*) που έχει ορίσει ο ιδιοκτήτης. Αυτό το χρονικό διάστημα ορίζεται για να μειωθεί η επιβάρυνση στο δίκτυο και να αποφευχθούν πιθανές επιθέσεις.

4.5.5 Κοινή επικάλυψη (shared overlay)

Αν ένας χρήστης διατηρεί περισσότερα από ένα σπίτια ορίζεται ένα επίπεδο κοινόχρηστης επικάλυψης (*shared overlay*). Δηλαδή, τα έξυπνα σπίτια διαχειρίζονται κεντρικά σαν ένα ενιαίο, με έναν κοινόχρηστο εξορύκτη (*shared overlay miner*). Στο *κοινόχρηστο BC* κάθε σπίτι έχει μία συναλλαγή *genesis* πάνω στην οποία συνδέονται όλες οι συναλλαγές *genesis* των συσκευών της από τον κοινόχρηστο εξορύκτη και με αυτές συνδέονται τα υπόλοιπα μπλοκ. Αυτή η υλοποίηση οδηγεί σε *διακλάδωση* στο κοινόχρηστο BC κάτι το οποίο αποκλίνει από την τυπική υλοποίηση του BC όπου κάτι τέτοιο απαγορεύεται. Ακόμη, για την επικοινωνία συσκευών μεταξύ των έξυπνων σπιτιών δημιουργείται μια σύνδεση Εικονικού Ιδιωτικού Δικτύου (VPN) μεταξύ της διαδικτυακής πύλης σε κάθε σπίτι και του κοινόχρηστου εξορύκτη για τη δρομολόγηση των πακέτων σε αυτόν.

4.5.6 Κατανεμημένη εμπιστοσύνη / αξιοπιστία

Στο δίκτυο επικάλυψης, κάθε CH διατηρεί μία *αξιολόγηση αξιοπιστίας* για τους άλλους CH βάσει *άμεσων* και *έμμεσων αποδείξεων*. Ο CH A έχει άμεσες αποδείξεις για τον CH B αν ελέγξει ένα μπλοκ που εξορύσσεται από το B. Εάν ο A λάβει το μπλοκ του B από τον C, τότε έχει έμμεσες ενδείξεις για τον B. Όταν ένα CH δημιουργεί ένα νέο μπλοκ πρέπει να δημιουργήσει μια *συναλλαγή πολλαπλών συναλλαγών* που χρησιμοποιείται για την αξιολόγηση της αξιοπιστίας και να αποστείλει και τα δύο στους γειτονικούς CH. Εάν ένας CH έχει άμεσες αποδείξεις με τον εξορύκτη ή άλλους CH που έχουν υπογράψει τη συναλλαγή, τότε ελέγχει τυχαία ένα μέρος των συναλλαγών στο μπλοκ ελέγχοντας τις υπογραφές τους. Το ποσοστό των συναλλαγών που θα ελέγξει είναι ανάλογο του αριθμού των επιτυχώς επαληθευμένων μπλοκ του συγκεκριμένου CH. Εάν όμως δεν έχει άμεσες αποδείξεις με τον εξορύκτη ή αυτούς που την υπέγραψαν, τότε ελέγχει όλες τις συναλλαγές.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.5.7 Ανάλυση της ασφάλειας

Οι συγγραφείς ισχυρίζονται ότι η υλοποίηση καλύπτει τις απαιτήσεις ασφαλείας. Πιο συγκεκριμένα αναφέρονται ότι σε επίπεδο *εμπιστευτικότητας* παρέχεται διασφάλιση ότι μόνο ο εξουσιοδοτημένος χρήστης / συσκευή μπορεί να διαβάσει τα δεδομένα χάρη στη συμμετρική κρυπτογράφηση (ο μηχανισμός παραγωγής και χρήσης κοινών κλειδιών που αναλύσαμε προηγουμένως), σε επίπεδο *ακεραιότητας* ότι τα δεδομένα μεταφέρονται στον προορισμό τους αναλλοίωτα (με τη χρήση κρυπτογραφικών αποτυπωμάτων - hash) ενώ για τη *διαθεσιμότητα* των συσκευών και των υπηρεσιών τους ότι περιορίζονται από τον SHM οι επιτρεπτές συναλλαγές από και προς τις συσκευές. Ακόμη, ότι το έξυπνο σπίτι διασφαλίζεται από τις δύο πιο κοινές επιθέσεις.

Επίθεση DDoS: Αρχικά, επειδή όλες οι επικοινωνίες ελέγχονται από τον SHM, δεν θα ήταν εφικτό να εγκατασταθεί απευθείας κακόβουλο λογισμικό στις έξυπνες συσκευές. Επιπλέον, επειδή υπάρχει έλεγχος εξουσιοδότησης δεν θα μπορούσαν οι συσκευές να περάσουν μεγάλο αριθμό αιτημάτων από τον SHM, αφού αυτή θα απορρίπτονταν. Στο επίπεδο του δικτύου επικάλυψης η διατήρηση *λίστας αιτούντων* και *αιτούμενων* αποκλείει αυτή την επίθεση από τους CH. Σε περίπτωση που υπάρξουν πολλές μη επιτυχημένες συναλλαγές *access* από ένα συγκεκριμένο δημόσιο κλειδί τότε ο CH το μπλοκάρει και απορρίπτει όλες τις εισερχόμενές από αυτό συναλλαγές. Οπότε μπορεί να επιτύχει μόνο αν στείλει μαζικά πολλές συναλλαγές με διαφορετικό δημόσιο κλειδί.

Απειλή συσχετισμού: Για την προστασία από αυτή την επίθεση, τα δεδομένα κάθε συσκευής μοιράζονται και αποθηκεύονται με ένα μοναδικό κλειδί. Ο SHM δημιουργεί ένα μοναδικό μητρώο καταγραφών στο αποθηκευτικό νέφος για κάθε συσκευή χρησιμοποιώντας διαφορετικό δημόσιο κλειδί.

Επίθεση Dropping: Ένας κακόβουλος έχει τον έλεγχο ενός CH ή μιας ομάδας CH. Αυτοί υπό τον έλεγχο του στη συνέχεια απορρίπτουν όλες τις ληφθείσες συναλλαγές και μπλοκ. Ωστόσο, μια τέτοια επίθεση θα ανιχνευθεί, δεδομένου ότι οι κόμβοι των συστάδων δεν θα δέχονταν καμία συναλλαγή ή υπηρεσία από το δίκτυο. Εάν εντοπιστεί μια τέτοια κατάσταση, τότε όλοι οι κόμβοι μέσα στο ίδιο σύμπλεγμα ενημερώνονται γι' αυτό και εκλέγεται ένας νέος CH.

Επίθεση εξόρυξης: Ένας κακόβουλος να ελέγχει πολλά CH που συνεργάζονται και υπογράφουν μία συναλλαγή πολλαπλών υπογραφών μαζί με ένα ψευδές μπλοκ που εξορύσσεται από αυτούς. Στην προτεινόμενη αρχιτεκτονική όλες οι συναλλαγές ή ένα τμήμα τους πρέπει να επαληθεύονται από άλλους CH. Ακόμα και αν ένας CH δεν μπορεί να ανιχνεύσει ένα ψευδές μπλοκ, άλλοι CH μπορεί να είναι σε θέση να το ανιχνεύσουν και να μεταδώσει έναν συναγερμό στους υπόλοιπους CH.

4.5.8 Ανάλυση της απόδοσης

Επιβάρυνση στο μέγεθος των πακέτων: Σχετίζεται με το μήκος των μεταδιδόμενων πακέτων. Η χρήση κρυπτογράφησης και hashing αυξάνει το μέγεθος των πακέτων, όμως η επίδρασή τους είναι μικρή.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Χρονική επιβάρυνση: Αναφέρεται στον χρόνο επεξεργασίας κάθε συναλλαγής από τον εξορύκτη, δηλαδή το διάστημα από τη λήψη ενός αιτήματος μέχρι την απάντηση του. Η χρήση της προτεινόμενης αρχιτεκτονικής προσθέτει μικρή καθυστέρηση στο χρόνο επεξεργασίας των πακέτων (της τάξεως των 20ms) για τους προαναφερθέντες λόγους.

Επιβάρυνση στην ενεργειακή κατανάλωση: Ουσιαστικά είναι η ενέργεια που καταναλώνεται από τον εξορύκτη για τη διεκπεραίωση συναλλαγών και την εκτέλεση hashing και κρυπτογράφησης. Η κατανάλωση της CPU είναι μικρή (0.002mj) όμως η κατανάλωση της μετάδοσης των πακέτων διπλασιάστηκε. Επιπλέον υπάρχει μία αύξηση 60% στην ενέργεια κατά τη διαρκή ασύρματη λειτουργία.

4.5.9 Συμπεράσματα

Οι μέχρι τώρα διαθέσιμες λύσεις ασφάλειας για IoT δεν είναι κατάλληλες εξαιτίας της υψηλής ενεργειακής κατανάλωσης και των επιβαρύνσεων επεξεργασίας. Η προτεινόμενη μέθοδος αντιμετωπίζει τα βασικά ζητήματα με την εισαγωγή του BC. Από την ανάλυση της προτεινόμενης λύσης σε ένα έξυπνο σπίτι προκύπτει ότι τα παραγόμενα οφέλη σε επίπεδο ασφάλειας και ιδιωτικότητας που προσφέρονται υπερτερούν των επιβαρύνσεων που εισήχθησαν με την ενσωμάτωση του BC και είναι διαχειρίσιμες από τις περιορισμένες σε πόρους IoT συσκευές. Ακόμη εφαρμόζεται μία μέθοδος κατανεμημένης αξιοπιστίας ώστε να μειωθεί ο χρόνος επεξεργασίας των νέων μπλοκ.

4.6 Η Περίπτωση της Αγοράς Ενέργειας

Όπως είδαμε το Ίδρυμα Διαδικτυακής Ενέργειας (Energy Web Foundation - EWF) κινείται προς τη μετατροπή της αγοράς ενέργειας ενσωματώνοντας το BC και IoT συσκευές. Είναι ένας παγκόσμιος μη κερδοσκοπικός οργανισμός που αποτελείται από τρεις βασικούς πυλώνες: α) μία *κοινότητα* άνω των 100 συνεργαζόμενων εταιριών διάσπαρτων ανά τον κόσμο (κοινής ωφέλειας, εκμετάλλευσης δικτύων, προγραμματιστές ανανεώσιμων πηγών ενέργειας, αγοραστές ενέργειας κα.), β) της *τεχνολογίας* που χρησιμοποιεί, δηλαδή μίας ειδικά διαμορφωμένης για τον τομέα της ενέργειας υποδομής BC η οποία αποτελείται από ένα δημόσιο δίκτυο εξουσιοδοτημένων επικυρωτών (που απαρτίζονται από τις συνεργαζόμενες εταιρίες) και το πρωτόκολλο συναίνεσης Proof-of-Authority και γ) της *διανομής* έτοιμων λύσεων λογισμικού και υλισμικού για να επισπευθεί η ανάπτυξη του κλάδου. Στα μέσα του 2019, το EWF εγκαινίασε την ενεργειακή αλυσίδα ενέργειας (Energy Web Chain), την πρώτη επιχειρηματική πλατφόρμα ανοικτού κώδικα, προσαρμοσμένη στις κανονιστικές, επιχειρησιακές και εμπορικές ανάγκες του κλάδου (Energy Web Foundation, 2018; Energy Web Foundation, 2019).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

4.6.1 Όραμα -Σκοπός

Σκοπός του εγχειρήματος του EWF είναι η απελευθέρωση των δυνατοτήτων αποκεντρωμένων δυνατοτήτων του BC για να επιτύχει μία παγκόσμια μετάβαση σε ένα δημοκρατικό, ψηφιακό ενεργειακό τομέα, χωρίς περιττές εκπομπές άνθρακα.

4.6.2 Εργαλεία ανάπτυξης λογισμικού

Το EWF αναπτύσσει εργαλεία ανάπτυξης λογισμικού (*SDK*) για να μειωθούν τα κόστη και ο χρόνος ανάπτυξης. Τα *SDK* αποτελούν πλήρως ανεπτυγμένες εφαρμογές ανοιχτού κώδικα που μπορούν να αναπαραχθούν, να τροποποιηθούν και να χρησιμοποιηθούν ως αναφορά για ανάπτυξη άλλων εμπορικών εφαρμογών.

4.6.2.1 EW Origin

Ένα χαρτοφυλάκιο από εργαλεία (toolkit) απευθυνόμενο σε εταιρίες και ρυθμιστικές αρχές με σκοπό τη εφαρμογή εμπορικών συναλλαγών ενέργειας και την παρακολούθηση ενεργειακών πιστοποιητικών (*EAC*)[25]. Καταγράφει την προέλευση και παρακολουθεί αυτόματα την κυριότητα της ανανεώσιμης ηλεκτρικής ενέργειας με ακεραιότητα και λεπτομέρεια συμπεριλαμβανομένης της θέσης, του χρόνου, του είδους και των εκπομπών CO^2. Το αποτέλεσμα είναι χαμηλότερο κόστος και μεγαλύτερη διαφάνεια στις συναλλαγές πιστοποιητικών προέλευσης, μεγαλύτερη πρόσβαση στην αγορά για αγοραστές και παραγωγούς όλων των μεγεθών και νέες αποκεντρωμένες εφαρμογές.

4.6.2.2 EW Link

Γεφύρωση φυσικού και ψηφιακού κόσμου. Αποτελεί σύνολο από αρχιτεκτονικές και πρότυπα σύνδεσης φυσικών αγαθών (όπως έξυπνες συσκευές, θερμοστάτες, ηλεκτρικά αυτοκίνητα κα.) μέσω υλοποιημένων *full client, light client*, και *API* στο BC με χαμηλό κόστος, ασφαλή και αξιόπιστο τρόπο ώστε να μπορούν να επικοινωνούν και να πραγματοποιούν συναλλαγές ανεξάρτητα. Ένα υλοποιημένο παράδειγμα είναι η εφαρμογή ενός *EW light client* σε μια απλή συσκευή IoT για να διευκολύνει την επικοινωνία με τους μετρητές παραγωγής ηλεκτρικής ενέργειας.

4.6.2.3 EW D3A

Μία δομή για επαναλαμβανόμενες, αποκεντρωμένες τοπικές αγορές ηλεκτρικής ενέργειας. Είναι ένα μοντέλο (*Decentralized Autonomous Area Agent - D3A*) όπου κάθε συσκευή που καταναλώνει ή παράγει ενέργεια μπορεί να συνεργάζεται με άλλες συσκευές στην τοπική της περιοχή, προκειμένου να βελτιστοποιήσει τις λειτουργικές αποφάσεις με βάση τις προτιμήσεις των χρηστών και τις συνθήκες του συστήματος, χρησιμοποιώντας δεδομένα και επικοινωνίες κατά μήκος της αλυσίδας αξίας.

[25] Έγγραφο που πιστοποιεί ότι η ενέργεια που καταναλώνεται προέρχεται από ανανεώσιμες πηγές. Μπορούν να αγορασθούν, να πωληθούν, να μεταφερθούν και να αποσυρθούν.

Πρόκειται ουσιαστικά για αυτόνομη διαχείριση προσφοράς και ζήτησης μέσω συσκευών σε επίπεδο ενός σπιτιού, ενός οικοδομικού συγκροτήματος κα. Δεν είναι ακόμη έτοιμη σε παραγωγικό περιβάλλον.

4.6.3 Διακυβέρνηση

Η διαχείριση του συστήματος προβλέπει την εφαρμογή κανόνων και επιτήρησης για τη διατήρηση της σταθερότητας και ασφάλειας της EWC και την προάσπιση των καταναλωτικών συμφερόντων. Επίσης στοχεύει στην εξισορρόπηση των παραγόμενων οφελών έναντι της κανονιστικής συμμόρφωσης. Απώτερος σκοπός είναι η αλυσίδα να χρησιμοποιείται από πολλούς αλλά να μην ανήκει σε κανέναν.

4.6.4 Υποστηρικτικές Τεχνολογίες

Σχετικά με την ανάπτυξη της απαραίτητης τεχνολογίας αρχικά υπήρξε ένα δίλημμα επιλογής μεταξύ δημιουργίας ενός νέου BC και χρήσης ενός υπάρχοντος. Προτιμήθηκε το δεύτερο ώστε να αξιοποιηθούν οι διαθέσιμοι πόροι στην επίλυση ζητημάτων που αντιμετωπίζουν οι εφαρμογές ειδικά στον ενεργειακό τομέα. Προτιμήθηκε το Ethereum σαν πρώτη ύλη κυρίως λόγω του ότι είναι ανοιχτού κώδικα, αποτελεί δημόσιο BC και άρα ανθεκτικό σε επιθέσεις, παραμετροποιήσιμο και επειδή είναι ευρέως γνωστό μπορεί να αξιοποιηθεί πλούτος υπάρχουσας γνώσης και δεξιοτήτων. Η νέα πλατφόρμα προσαρμόστηκε και αναπτύχθηκε επεκτείνοντας λειτουργικότητα και χαρακτηριστικά. Το βασικότερο ήταν να καλυφθούν οι κύριες απαιτήσεις του τομέα. Αυτές συνοψίζονται στον κάτωθι πίνακα μαζί με τις προσαρμογές για την αντιμετώπισή τους και ακολουθεί η ανάλυσή τους.

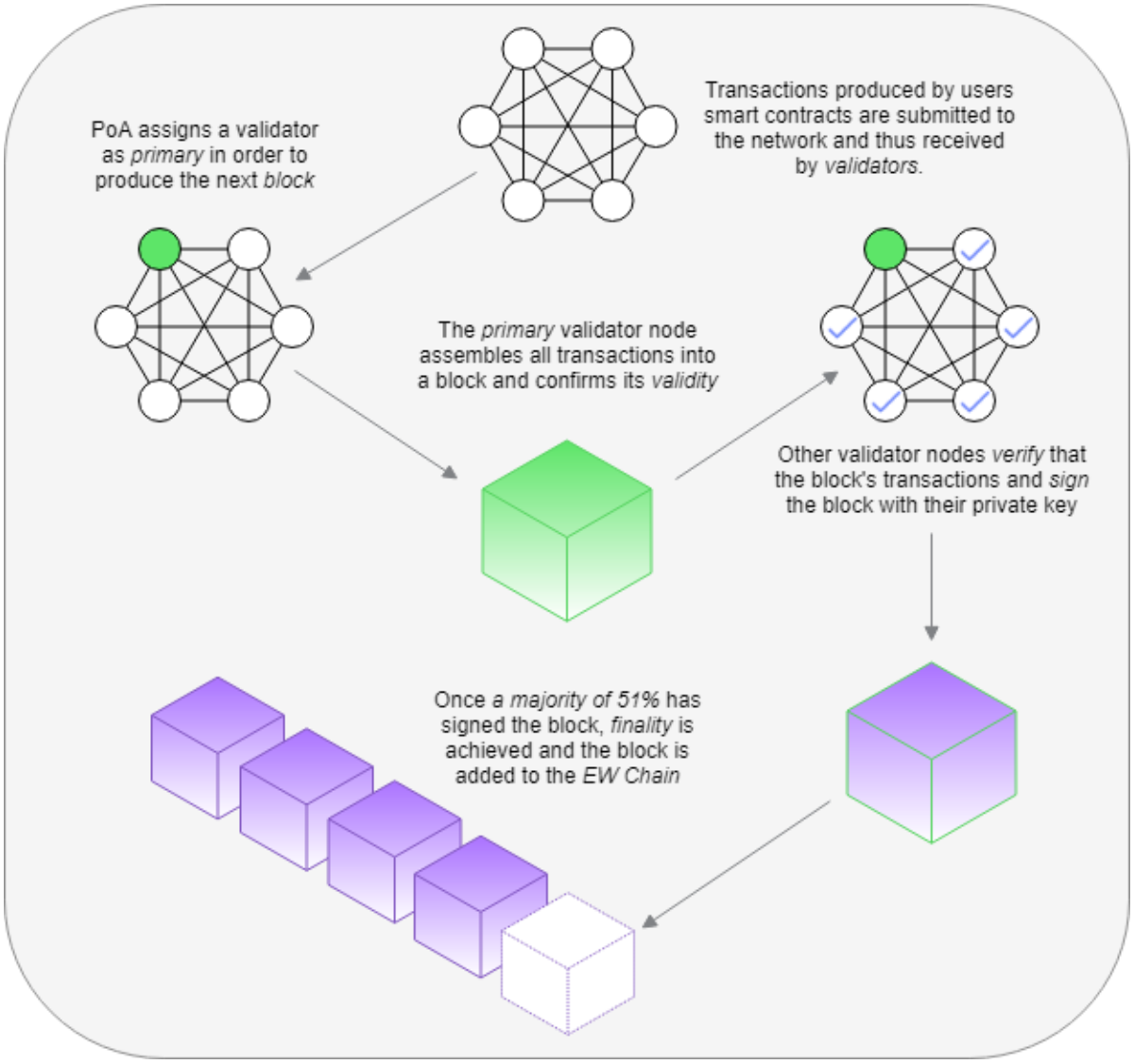
Ζητήματα	Προσαρμογές της πλατφόρμας
Χαμηλή διεκπεραιωτικότητα συναλλαγών	Αντικατάσταση συναίνεσης PoW από την PoAuth
Δυσχερής ενσωμάτωση IoT τεχνολογίας	Δημιουργία ελαφριάς έκδοσης client εφαρμογής
Αδυναμία διαφοροποίησης δικαιωμάτων	Εφαρμογή μηχανισμών εξουσιοδότησης
Χαμηλή ιδιωτικότητα	Εφαρμογή μηχανισμών ιδιωτικών συναλλαγών

Πίνακας βασικών προσαρμογών Ethereum στο Web Energy Chain

4.6.4.1 Proof-of-Authority

Παρέχει βελτιωμένη λειτουργικότητα και τεχνική ικανότητα για κανονιστική εποπτεία, διατηρώντας ταυτόχρονα την ασφάλεια και την αξιοπιστία σε επίπεδο δικτύου. Ο μηχανισμός PoAuth επιλέχθηκε για τρεις λόγους: α) *επιτρέπει την επεξεργασία πολλών συναλλαγών*, της τάξεως των χιλιάδων ανά δευτερόλεπτο (υποστηρίζεται ότι επιτυγχάνει τριάντα φορές μεγαλύτερη *διεκπεραιωτικότητα* από το Ethereum, β) *ελαχιστοποιεί την κατανάλωση πόρων και συνεπαγόμενα το κόστος συναλλαγής*. Η εξάλειψη του PoW οδηγεί σε 54.000 φορές λιγότερη κατανάλωση ενέργειας και 350 φορές χαμηλότερο κόστος δικτύου (δηλαδή δαπάνες που πραγματοποιούνται από οργανισμούς που φιλοξενούν κόμβους

επικύρωσης) το οποίο ερμηνεύεται σε χαμηλότερο κόστος συναλλαγής, γ) *βελτιώνει τη συμμόρφωση* σε κανονισμούς και επιχειρηματικές απαιτήσεις στον ενεργειακό τομέα αντικαθιστώντας τους ανώνυμους εξορύκτες με επιλεγμένους επικυρωτές. Έτσι ενισχύει την ικανότητα των αποκεντρωμένων εφαρμογών να συμμορφώνονται με διάφορους κανονισμούς, όπως το GDPR και αυξάνει την υιοθέτηση της τεχνολογίας. Σε αυτό το μοντέλο συναίνεσης PoAuth, μόνο μια καθορισμένη ομάδα κόμβων, που ονομάζεται *validators - επικυρωτές*, έχουν την άδεια να επαληθεύσουν τις συναλλαγές και να δημιουργήσουν νέα μπλοκ. Αυτή η προσέγγιση προσφέρει διάφορα οφέλη αν και θυσιάζει ένα μικρό αλλά όχι ασήμαντο επίπεδο αποκέντρωσης.



Ο μηχανισμός συναίνεσης του Proof-of-Authority (PoA) που χρησιμοποιείται από το EWF. Αναπαραγωγή από Energy Web Foundation (2019)

Η λειτουργία του μηχανισμού συναίνεσης PoAuth συνοψίζεται ως εξής: Κάθε κόμβος επικύρωσης διατηρεί μία λίστα με τα δημόσια κλειδιά από όλους τους επικυρωτές και αλλάζει καθώς προστίθενται ή καταργούνται επικυρωτές. Ο αλγόριθμος PoAuth ορίζει ένα *πρωτεύων επικυρωτή* ο οποίος είναι

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

υπεύθυνος για τη συλλογή των συναλλαγών και τη σύσταση του νέου μπλοκ, μέσα σε *ένα καθορισμένο χρονικό περιθώριο*. Υπάρχουν *συγχρονισμένα ρολόγια* μεταξύ των κόμβων επικύρωσης στο δίκτυο για να αποφευχθεί η δημιουργία μπλοκ σε αυθαίρετο χρόνο και από αυθαίρετο επικυρωτή. Αν λόγω προβλημάτων υλισμικού ο επικυρωτής δεν παράξει νέο μπλοκ ή λόγω συνδεσιμότητας δικτύου δεν επαληθευτεί από επαρκές αριθμό επικυρωτών ο επόμενος επικυρωτής προχωρά στη δημιουργία του μπλοκ με τις συναλλαγές που έχουν μείνει εκκρεμείς. Κατόπιν της παραγωγής νέου μπλοκ, οι υπόλοιποι κόμβοι επικύρωσης επαληθεύουν τις συναλλαγές, *υπογράφουν το μπλοκ με τα ιδιωτικά κλειδιά* τους και το προωθούν στο δίκτυο. Άπαξ και υπογραφεί - επαληθευθεί το μπλοκ από μία πλειοψηφία 51% θεωρείται έγκυρο και οι συναλλαγές οριστικές και προστίθεται στην EW Chain.

4.6.4.2 Light Client

Προσφέρει συρρίκνωση του μεγέθους του πελάτη για τη διευκόλυνση της σύνδεσης των συσκευών IoT και των κατανεμημένων ενεργειακών πόρων στην EW Chain. Είναι ουσιώδες οι συσκευές περιορισμένων πόρων να έχουν πλήρη πρόσβαση στο δίκτυο χωρίς να χρειάζεται να αποθηκεύουν και να διατηρούν ολόκληρο το αντίγραφο του BC ενώ παράλληλα, η αλληλεπίδραση με αυτό δεν θα πρέπει να θέτει σε κίνδυνο την ασφάλεια των συσκευών. Ο *EW light client* αποθηκεύει μια "ελαφριά" έκδοση του BC στις συσκευές και παρέχει ένα πρωτόκολλο όπου αναζητά πρόσθετα δεδομένα στο δίκτυο όταν αυτά απαιτούνται, παρέχοντας ένα επίπεδο ασφάλειας ισοδύναμο με εκείνο των κόμβων επικύρωσης. Η ελαφριά έκδοση περιλαμβάνει κεφαλίδες μπλοκ και μεταβλητές κατάστασης, επιτρέποντας ένα παρόμοιο επίπεδο αξιοπιστίας και χρηστικότητας όπως στους πλήρεις κόμβους, ενώ αποθηκεύει μόνο ένα μικρό ποσοστό των δεδομένων BC. Μπορεί να υποστηρίξει το μηχανισμό συναίνεσης του PoAuth.

4.6.4.3 Εξουσιοδότηση (permissioning)

Τεχνική δυνατότητα διαφοροποίησης κόμβων και λογαριασμών βάσει διακυβέρνησης, εφαρμογών και κανονιστικών απαιτήσεων. Η ιδιότητα της εξουσιοδότησης ουσιαστικά παρέχει διαφορετικά προνόμια σε διαφορετικούς φορείς. *Σε επίπεδο συναίνεσης*, επιτρέπει σε ορισμένους κόμβους με συγκεκριμένα κριτήρια να έχουν τη δυνατότητα δημιουργίας μπλοκ. *Σε επίπεδο εφαρμογής*, καθιστά εφικτό για συγκεκριμένους χρήστες ή έξυπνα συμβόλαια να διεξάγουν συγκεκριμένες συναλλαγές. Κάτι το οποίο εκμεταλλεύονται προγραμματιστές SC, εταιρίες κοινής ωφελείας και ρυθμιστικές αρχές ώστε να ελέγχουν ποιος μπορεί να συναλλάσσεται με ποιόν και ποιος έχει δικαίωμα να δημιουργεί νέα SC.

4.6.4.4 Ιδιωτικές συναλλαγές

Χρησιμεύουν στη διατήρηση της ιδιωτικότητας των χρηστών και τη συμμόρφωση σε κανονισμούς εμπιστευτικότητας των δεδομένων. Γίνεται χρήση SC με κρυπτογραφημένο κώδικα και μεταβλητές καταστάσεων για τον έλεγχο του ποιος μπορεί να έχει πρόσβαση, να αλλάξει και να επικυρώσει τα δεδομένα που περιέχονται στο SC. Λειτουργούν ως εξής. Ένα δημόσιο SC περιέχει ένα εμφωλευμένο

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

κρυπτογραφημένο ιδιωτικό SC και μια ξεχωριστή λίστα επικυρωτών για ιδιωτικές συναλλαγές. Η πρόσβαση στα κρυπτογραφημένα δεδομένα γίνεται μέσω *ενός μοναδικού κλειδιού* το οποίο δημιουργείται και κατανέμεται μεταξύ ενός υποσυνόλου κόμβων εν ονόματι *Secret Store*. Ένα ξεχωριστό SC επιτρέπει σε συγκεκριμένες διευθύνσεις να έχουν πρόσβαση στο κρυπτογραφημένο ιδιωτικό SC ζητώντας από το *Secret Store* να αποκρυπτογραφήσει τα δεδομένα. Έπειτα ο παραλήπτης στέλνει ένα ιδιωτικό μήνυμα συναλλαγής στους ιδιωτικούς επικυρωτές. Εκείνοι παράγουν μία νέα κρυπτογραφημένη κατάσταση, την υπογράφουν και την προωθούν μέσω του δημόσιου SC στο δίκτυο του BC. Οι *ιδιωτικές συναλλαγές* δεν ενδείκνυνται για όλες τις περιπτώσεις καθώς είναι πολύπλοκες διαδικασίες και δεν επιτρέπουν την ανταλλαγή μαρκών. Προτείνονται για την ανταλλαγή ορισμένων δεδομένων που προτιμάται να μην είναι δημόσια διαθέσιμες όπως τιμές και ποσότητες συναλλαγών.

4.6.5 Επόμενα βήματα

Το EWF επικεντρώνει τις προσπάθειες του σε τέσσερις τομείς:

1. Μεγέθυνση του οικοσυστήματος, δηλαδή αύξηση των συνεργαζόμενων εταιριών, περισσότερη τεκμηρίωση υλοποιήσεων, διενέργεια εργαστήριων και ημερίδων και εκπαίδευση των ρυθμιστικών αρχών.
2. Βελτίωση των ήδη υπαρχόντων SDK και ανάπτυξη νέων.
3. Περαιτέρω έλεγχος λειτουργικότητας σε τεστ περιβάλλον για τον εντοπισμό όλων των πιθανών φορέων επίθεσης και δημιουργία μηχανισμών άμυνας.
4. Προσθήκη νέων τεχνικών χαρακτηριστικών για τη διευκόλυνση όσων αναπτύσσουν εφαρμογές.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 5: Τάσεις

Αναφορικά με το φλέγον ζήτημα αν τελικά είναι σε θέση το BC να ενισχύσει το IoT ο Kshetri (2017) απαντά «ίσως». Η ενοποίησή τους έχει μεγάλη δυναμική και έχει ως στόχο να μετασχηματίσει πολλές βιομηχανίες. Οι συσκευές IoT μπορούν να πραγματοποιούν αυτόνομες συναλλαγές μέσω έξυπνων συμβολαίων. Επίσης ο συνδυασμός με τεχνητή νοημοσύνη (AI) είναι πολλά υποσχόμενος για το μέλλον. Ο συνδυασμός των δύο τεχνολογιών έχει δείξει τις δυνατότητές του τόσο στη βιομηχανία όσο και στον ακαδημαϊκό κόσμο. Στην παρούσα ενότητα συζητάμε πιθανές μελλοντικές κατευθύνσεις και τάσεις στον υπό εξέταση κλάδο.

5.1 Μεγάλα Δεδομένα

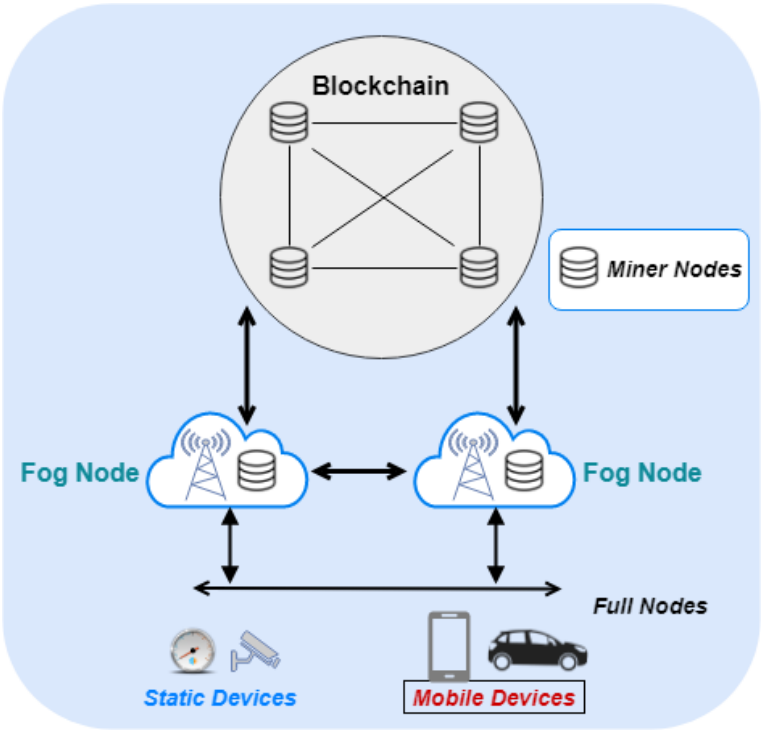
Οι Karafiloski και Mishev (2017) θίγουν το πρόβλημα διαχείρισης των ευαίσθητων και προσωπικών δεδομένων στο πλαίσιο των μεγάλων δεδομένων σε διάφορους τομείς, ένας εξ ’αυτών και το IoT. Εκεί ο όγκος παραγόμενης πληροφορίας αυξάνεται εκθετικά και καθώς οι χρήστες δημιουργούν και δημοσιεύουν δεδομένα θα πρέπει να παραμείνουν και οι κάτοχοι τους. Στις περιπτώσεις παρακολούθησης των ενεργειών και των ενδιαφερόντων τους, οι χρήστες πρέπει τουλάχιστον να έχουν επίγνωση γι’ αυτό και να αποκομίζουν ορισμένα οφέλη. Η αλυσίδα καταγραφών είναι πολλά υποσχόμενη για την εξέλιξη των big data. Το BC μπορεί να λειτουργήσει για τον κόσμο ως ένα φίλτρο ελέγχου των δεδομένων και των συναλλαγών του μέσω μηχανισμών αυθεντικοποίησης, περιορισμού της πρόσβασης ανάλογα με τις ανάγκες του χρήστη και κρυπτογράφησης των δεδομένων. Η ύπαρξη ενός πρωτοκόλλου που εκτελεί εντολές ανεπηρέαστο από τρίτους αποτελεί ελκυστική ιδιότητα για τα μεγάλα δεδομένα και δεν είναι απίθανο στο μέλλον να συμπεριλάβουν στις υποστηρικτικές τεχνολογίες τους ένα κατανεμημένο διομότιμο δίκτυο BC για την αποθήκευση και διαχείριση των δεδομένων.

Ο μεγάλος όγκος πληροφορίας αποτελεί δοκιμασία για το IoT αφού για να ανταπεξέλθει στις υψηλές απαιτήσεις επεξεργαστικής ισχύς και αποθήκευσης έχει αξιοποιήσει τις κατανεμημένες δυνατότητες της υπολογιστικής νέφους και των μεγάλων δεδομένων. Εξαιτίας αυτού, οι τεχνικές εξόρυξης δεδομένων (data mining) είναι σε θέση να αντιμετωπίσουν τα δεδομένα IoT σαν ένα σύνολο, λόγω της αύξησης της δυνατότητας επεξεργασίας από την cloud τεχνολογία. Από τη μεριά τους τα μεγάλα δεδομένα επέτρεψαν την ταυτόχρονη επεξεργασία μεγάλων ποσοτήτων δεδομένων, επιτρέποντας την εξαγωγή γνώσης, κάτι το οποίο ήταν δύσκολα επιτεύξιμο προηγουμένως. Στο μέλλον, με την ενσωμάτωση του IoT με το BC, τα SC θα πρέπει να αξιοποιούν τον κατανεμημένο χαρακτήρα τους ώστε να επιτρέπουν δυνατότητα επεξεργασίας στο βαθμό που απαιτείται από το IoT και καλύπτεται προσωρινά από τις δύο προαναφερθείσες τεχνολογίες (Reyna et al., 2018).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5.2 Χρήση Υπολογιστικής Ομίχλης

Με βάση τα τωρινά δεδομένα, τα περισσότερα συστήματα IoT λόγω υπολογιστής και αποθηκευτικής έλλειψης εξαρτώνται από μια cloud πλατφόρμα. Λόγω των περιορισμένων πόρων οι συσκευές IoT δεν μπορούν να χρησιμοποιηθούν ως εξορύκτες σε ένα δίκτυο BC. Για να γίνει ομαλότερη η μετάβαση από μία υλοποίηση cloud σε μία εφαρμογή BC οι Makhdoom et al. (2019) προτείνουν την αξιοποίηση της τεχνολογίας Υπολογιστικής Ομίχλης (Fog Computing).



Ενσωμάτωση Αλυσίδας Καταγραφών και Διαδικτύου των Πραγμάτων με χρήση Υπολογιστικής Νέφους. Αναπαραγωγή από Makhdoom et al. (2019)

Οι κόμβοι ομίχλης εφοδιασμένοι με περισσότερους πόρους έχουν τη δυνατότητα να ενσωματώνουν εξορύκτες για τη συλλογή και εξόρυξη συναλλαγών που λαμβάνουν από τις συσκευές IoT και άρα να διευκολύνουν την άμεση αλληλεπίδραση μεταξύ των συσκευών IoT και του BC. Επιπρόσθετα, οι συσκευές IoT διαθέτουν πόρους για να είναι οι πλήρεις κόμβοι, δηλαδή να αποθηκεύουν το BC, να αναδιανέμουν και να επικυρώσουν συναλλαγές. Έτσι, οι συναλλαγές από τις συσκευές IoT θα διαδοθούν στους κόμβους ομίχλης και ως εκ τούτου, το IoT μπορεί να εκμεταλλευτεί την υπάρχουσα υποδομή υπολογιστών ομίχλης για να υιοθετήσει την τεχνολογία BC. Μία εφικτή λύση μέχρις ότου οι συσκευές IoT να κατασκευάζονται με ενσωματωμένη λειτουργικότητα εξόρυξης για να καρπωθούν από τα μέγιστα οφέλη της κατανεμημένης BC αρχιτεκτονικής.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

5.3 Εξέταση των διαφορετικών Αλυσίδων Καταγραφών

Στο εγγύς μέλλον, θα υπάρξει ανάγκη βελτιστοποίησης των διάφορων τύπων BC για να καλύψουν διαφορετικές εφαρμογές. Επιπρόσθετα οι χρήστες για να καλύψουν τις απαιτήσεις των συστημάτων τους πιθανόν να χρειαστεί να συνδυάσουν IoT και BC. Πώς όμως θα επιλέξουν τον τύπο BC που ταιριάζει καλύτερα στην περίπτωσή τους;

Γεννάται η ανάγκη ενός μηχανισμού εξέτασης των BC εφαρμογών που να χωρίζεται σε δύο στάδια:

1. Προτυποποίηση. Η φάση αυτή περιέχει μία ευρεία κατανόηση των αλυσίδων εφοδιασμού, των αγορών, των προϊόντων και των υπηρεσιών, εντοπισμού και καταγραφής των διαφορετικών απαιτήσεων και καθορισμό των κριτηρίων ελέγχου.
2. Εκτέλεση του ελέγχου. Όταν ένα BC γεννιέται, θα μπορούσε να δοκιμαστεί με τα προσυμφωνημένα κριτήρια ώστε να επαληθευτεί αν πληρούν τις απαιτήσεις που ισχυρίζονται οι δημιουργοί τους.

Να τονίσουμε ότι είναι ουσιώδες να υπάρχει πληθώρα διαφορετικών κριτηρίων για την έγκυρη αξιολόγηση, όπως ιδιωτικότητα, ασφάλεια, ενεργειακή απόδοση, διεκπεραιωτικότητα, χρονική καθυστέρηση, αποθηκευτική ικανότητα, κλπ. Πρέπει να ληφθεί υπόψη ότι ο έλεγχος πρέπει να γίνει με διαφορετική βαρύτητα ανά περίπτωση, πχ. για μία ηλεκτρονική επιχείρηση η διεκπεραιωτικότητα έχει αξία, οπότε πρέπει να εξεταστεί ο μέσος χρόνος από τη στιγμή που στέλνει μια συναλλαγή ένας χρήστης μέχρι αυτή να ενταχθεί στο BC (Zheng et al., 2018; Fernández-Caramés and Fraga-Lamas, 2018).

5.4 Τεχνητή Νοημοσύνη

Νέες ευκαιρίες για εφαρμογές τεχνητής νοημοσύνης (AI) ξεπροβάλλουν λόγω των πρόσφατων εξελίξεων στην τεχνολογία. Οι τεχνολογίες AI αναπτύσσονται ταχύτατα και κρίνεται ότι έχουν τη δυνατότητα να επιλύσουν αρκετά προβλήματα. Μία περίπτωση που η συμβολή της θα ήταν καίρια είναι αναφορικά με τη χρήση χρησμών (oracles). Σε μία υποθετική εφαρμογή IoT, μπορεί να υπάρχει η ανάγκη ένα oracle που είναι υπεύθυνο για να καθορίσει εάν πληρείται η προϋπόθεση ενός SC. Τις περισσότερες φορές το ρόλο αυτό αναλαμβάνει ένα αξιόπιστο τρίτο μέρος. Οι τεχνικές της AI μπορούν να συμβάλλουν στην ανάπτυξη ενός ευφυούς χρησμού ο οποίος δεν θα ελέγχεται από κανένα, απλά θα μαθαίνει με βάση τη πληροφόρηση που λαμβάνει απέξω από το σύστημα και θα εκπαιδεύεται μόνος του.

Μία τέτοια υλοποίηση θα εξάλειφε οποιεσδήποτε αντιπαραθέσεις και το έξυπνο συμβόλαιο μπορεί να γίνει ακόμα πιο έξυπνο. Σημαντικό είναι να μην παραβλέπουμε ότι, η AI είναι μία τεχνολογία ιδιαιτέρως διεισδυτική στη ζωή μας. Το BC και το SC θα μπορούσαν να συμβάλουν στον περιορισμό συμπεριφορών που αποκλίνουν από την ομαλή λειτουργία σχετικά με τα προϊόντα της AI. Επί

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

παραδείγματι, νόμοι που ενσωματώνονται μέσα σε έξυπνο συμβόλαιο θα μπορούσαν να συμβάλουν στην αποτροπή παραβιάσεων που προκαλούνται από αυτο-οδηγούμενα, έξυπνα αυτοκίνητα.

5.5 Πρωτόκολλο Συναίνεσης προσαρμοσμένο στο Διαδίκτυο των Πραγμάτων

Στα μελλοντικά σχέδια των Makhdoom et al. (2019) είναι ο σχεδιασμός μίας αρχιτεκτονικής IoT βασισμένης σε blockchain η οποία να στηρίζεται σε ένα πρωτόκολλο συναίνεσης ειδικά μελετημένο για IoT με απώτερο στόχο την επίτευξη ασφάλειας καθώς και την αποδοτικότητα και ακεραιότητα της διαδικασίας επικύρωσης συναλλαγών. Σε αυτή την προσπάθεια, συγκαταλέγεται και η απόπειρα διασφάλισης της επαλήθευσης των συσκευών κατά τη διαδικασία επικύρωσης συναλλαγών.

5.6 Ανάπτυξη του Διαδικτύου των Στρατιωτικών Αντικειμένων

Η τεχνολογία θα διαδραματίσει έναν ολοένα και πιο σημαντικό ρόλο στην κοινωνία μας στο προσεχές μέλλον, τόσο σε πολιτικό όσο και σε στρατιωτικό επίπεδο, με την ανάπτυξη του Διαδικτύου των Drones του Διαδικτύου των Στρατιωτικών Αντικειμένων και του Διαδικτύου των Αντικειμένων Μάχης. Λόγω του χρονικά ευαίσθητου χαρακτήρα ορισμένων εφαρμογών ιδίως σε στρατιωτικά περιβάλλοντα, ο προσδιορισμός των πιθανών φορέων απειλής και η χάραξη πορείας δράσης επιβάλλεται να εκτελούνται αυτόματα με ελάχιστη ανθρώπινη παρέμβαση.

5.7 Ενσωμάτωση πρωτοκόλλων επικοινωνίας με αλυσίδα καταγραφών

Από την πρότερη ανάλυση των σεναρίων ADEPT και VANET είδαμε ότι οι συγγραφείς συνιστούν τη χρήση του TeleHash για την ανταλλαγή μηνυμάτων με σκοπό την ενσωμάτωση των πρωτόκολλων του BC με το επίπεδο επικοινωνίας του IoT. Πρόκειται για ένα ελαφρύ και ασφαλές πρωτόκολλο διομότιμου δικτύου που χρησιμοποιεί κρυπτογράφηση για την ασφαλή επικοινωνία πλέγματος μεταξύ διαφορετικών πλατφορμών. Οι συναλλαγές μπορούν να μετατραπούν σε μπλοκ και να μεταδοθούν περαιτέρω στο BC δίκτυο.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 6: Υλοποίηση ενός έξυπνου συμβολαίου για την εφοδιαστική αλυσίδα

6.1 Κίνητρο και Στόχος Υλοποίησης

Η εφοδιαστική αλυσίδα έχει ανάγκη το IoT ώστε να καταστούν έξυπνες οι διαδικασίες που σχετίζονται με αυτή. Παράλληλα όμως εξελίσσεται και έρευνα για την ενσωμάτωση του BC ώστε να αναπτυχθούν νέα μοντέλα λειτουργίας και να προαχθεί η διαφάνεια και η εμπιστοσύνη. Όπως είδαμε σε προηγούμενη ανάλυση υπάρχουν αρκετές εφαρμογές που μπορούν ενοποιήσουν τις δύο τεχνολογίες. Δεν λείπουν όμως και από τον επιχειρηματικό κόσμο οι πρακτικές εφαρμογές.

Ενδεικτικά, η Accenture κατόπιν μελέτης έχει συμπεράνει ότι το BC σε συνδυασμό με το IoT και την τεχνολογία RFID μπορούν να αντιμετωπίσουν αποτελεσματικά τα ζητήματα διαχείρισης προέλευσης, χειραγώγησης εγγράφων και της παρουσίας αγαθών που είναι απομίμηση. Η ικανότητα του BC να καταγράφει με μοναδικά κρυπτογραφικά αποτυπώματα τόσο υλικά στοιχεία (π.χ. ανταλλακτικά αεροσκαφών) όσο και άυλα αγαθά (π.χ. πιστοποιητικά αξιοπλοΐας) αναδεικνύει τις δυνατότητές του ως μία λύση σε διεταιρικό επίπεδο για *παρακολούθηση και ανίχνευση των ανταλλακτικών*. Η καινοτομία του υπόκειται όχι στον τρόπο τεχνικής παρακολούθησης ή εντοπισμού των πραγματικών στοιχείων αλλά στον τρόπο καταγραφής και ανταλλαγής αυτών των πληροφοριών. Σε σύγκριση με την εναλλακτική που προσφέρει η αποθήκευση σε cloud, το BC ξεχωρίζει λόγω της δυνατότητας των προγραμματισμένων SC που χρησιμοποιούν δεδομένα ιχνηλασιμότητας για την αυτόματη δημιουργία πιστοποιητικών αξιοπλοΐας (Roussakis and Rajkov, 2018).

Μία άλλη μεγάλη πολυεθνική στα ίδια χνάρια, η IBM υπόσχεται στους υποψήφιους πελάτες της να μετασχηματίσει την επιχείρησή τους, καταγράφοντας τα IoT δεδομένα σε ένα άφθαρτο ψηφιακό μητρώο, ιδανικό για ασφάλεια και την ανάληψη ευθυνών. Το IoT επιτρέπει στις συσκευές να στέλνουν δεδομένα σε ιδιωτικά BC για να συμπεριληφθούν σε συναλλαγές, δημιουργώντας αρχεία ανθεκτικά στις παραβιάσεις. Το IBM BC επιτρέπει στους επιχειρηματικούς συνεργάτες να έχουν πρόσβαση και να παρέχουν δεδομένα IoT χωρίς την ανάγκη κεντρικού ελέγχου και διαχείρισης. Κάθε συναλλαγή μπορεί να επαληθευτεί για να αποφευχθούν οι διαφορές και να διασφαλιστεί ότι κάθε εταίρος είναι υπόλογος για τους σαφώς καθορισμένους ρόλους του. Η εταιρία εκμεταλλεύεται τις δύο τεχνολογίες για να παρέχει υπηρεσίες μεταφοράς εμπορευμάτων, παρακολούθηση εξαρτημάτων και συμμόρφωση αεροσκαφών, αυτοκίνητων ή άλλων οχημάτων, καταγραφή δεδομένων επιχειρησιακής συντήρησης μηχανών αεροσκαφών, ανελκυστήρων κα (Ibm.com, 2019).

Το κίνητρο πίσω από αυτή την υλοποίηση είναι η πρακτική εφαρμογή των εννοιών που μελετήθηκαν με σκοπό τη βαθύτερη κατανόηση ενός μέρους του υπό μελέτη αντικειμένου, το οποίο έχει ραγδαία εξέλιξη και απήχηση στον εργασιακό τομέα. Παρότι υπάρχουν πλούτος ιδεών και σεναρίων

εφαρμογής, δυστυχώς δεν είναι εύκολη η εύρεση παραδειγμάτων κώδικα έξυπνων συμβολαίων ή ευρύτερων εφαρμογών ανοιχτού κώδικα. Όποτε θα γίνει μία ανάπτυξη ενός SC για το Ethereum σε γλώσσα Solidity, επηρεασμένο από το σενάριο παρακολούθησης μεταφοράς φορτίου. Θα ακολουθήσει σύντομη περιγραφή των λειτουργιών που θέλουμε να πετύχουμε, την περιγραφή των τεχνολογιών που χρησιμοποιήθηκαν, ανάλυση του script και σύντομα συμπεράσματα.

6.2 Συναφείς έρευνες και εγχειρήματα

Η εφαρμογή εξετάζει την περίπτωση της παρακολούθησης αγαθών στην εφοδιαστική αλυσίδα χρησιμοποιώντας έξυπνα συμβόλαια και IoT. Από τους πρώτους που μελέτησαν το αντικείμενο είναι οι Christidis και Devetsikiotis (2016). Στην μεταφορά αγαθών κατά μήκος της εφοδιαστικής αλυσίδας υπάρχουν αρκετά ξεχωριστά ενδιαφερόμενα μέρη, πχ παραγωγός, εταιρία εκφόρτωσης, μεταφορείς, χονδρέμποροι κα. Για να έχουν μία εικόνα των αγαθών διατηρούν βάσεις δεδομένων τοπικά και βασίζονται σε πληροφόρηση που λαμβάνουν από τους συνεργάτες τους. Η χρήση συσκευών RFID πάνω στα κοντέινερ και η υλοποίηση BC προσφέρει μία ενιαία βάση όπου οι καταγραφές σε αυτήν παρέχουν κρυπτογραφική επαλήθευση, επιτρέπουν την άμεση πρόσβαση και διάδοση δεδομένων κατά μήκος του δικτύου και συμβάλουν στην ιχνηλασιμότητα των πληροφοριών. Υπάρχουν δύο σενάρια για τη μεταβίβαση εμπορευμάτων. Στο πρώτο γίνεται χρήση ενός SC το οποίο επιβεβαιώνει τη μετάβαση των αγαθών μεταξύ των συμβαλλόμενων. Κατά την μεταβίβαση των αγαθών γίνεται μία "χειραψία", έπειτα ο παραδίδων εκτελεί μία συναλλαγή στο SC για να υπογράψει την παράδοση. Ακολουθεί ο παραλήπτης με μία συναλλαγή από μέρους του για να επιβεβαιώσει την παράδοση. Στο δεύτερο, γίνεται χρήση μαρκών (tokens) για την αποφυγή διενέξεων και αμφισβητήσεων μεταξύ των συμβαλλόμενων κατά τη μεταφορά. Για να τελεσφορήσει μία παράδοση ανταλλάσσονται τα tokens. Ο παραδίδων δημιουργεί μία συναλλαγή όπου παραδίδει το token "έχω το κοντέινερ" στον παραλήπτη. Εκείνος με τη σειρά του παραδίδει το token "έχω παραλάβει το κοντέινερ" στον παραδίδων και προωθεί τη συναλλαγή στο BC. Η ανταλλαγή των token συνεχίζεται μεταξύ των ενδιαφερόμενων μερών μέχρι το token "έχω το κοντέινερ" να φτάσει στο τέλος της εφοδιαστικής αλυσίδας. Επιπρόσθετα μπορεί να επιτευχθεί πλήρης αυτοματοποίηση της διαδικασίας χάρη στο IoT. Κάθε ενδιαφερόμενος μεταφέρει έναν έξυπνο ιχνηλάτη με δυνατότητα σύνδεσης στο διαδίκτυο και εγκατεστημένο ένα client του BC. Όταν οι δύο ενδιαφερόμενοι συναντηθούν, οι συσκευές των ενδιαφερομένων μπορούν να στέλνουν υπογεγραμμένες συναλλαγές μεταβίβασης στο BC αυτόματα χωρίς ανθρώπινη μεσολάβηση.

Τα πολλαπλά οφέλη του BC οδηγούν ερευνητές και προγραμματιστές να αναζητούν τρόπους για να το εντάξουν στο IoT. Από την πλευρά τους οι Casado-Vara et al. (2018) προτείνουν ένα μοντέλο που βασίζεται στο BC και τα πολυπρακτορικά συστήματα (multiple-agent systems) για να εξαλείψουν τα εμπόδια των καθυστερήσεων, της μεγάλης ζήτησης σε εργατικά χέρια, της απώλειας παραγγελιών και των ζητημάτων ασφάλειας με έμφαση στον τομέα της γεωργίας. Χρησιμοποιείται από ένας αυτόνομος

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

πράκτορας σε κάθε επίπεδο της SCM (παραγωγός, επεξεργαστής[26], μεταφορέας, έμπορος λιανικής και αλυσίδα καταγραφών) για να επιλύει τις εκάστοτε αρμοδιότητες. Ο πράκτορας του BC συγχρονίζεται με τους υπόλοιπους έτσι ώστε όλα τα δεδομένα όλων των συναλλαγών να αποθηκεύονται σωστά. Τα SC χρησιμοποιούνται για την αγοραπωλησία αγαθών και υπηρεσιών και την επικοινωνία μεταξύ των πρακτόρων. Έτσι δημιουργείται μία κυκλική οικονομία. Μία καινοτομία είναι η δικλίδα ασφαλείας στις συναλλαγές. Οι πράκτορες αν εντοπίσουν ότι κάποιο συμβαλλόμενο μέρος δεν πληροί τις προκαθορισμένες προϋποθέσεις δεν ολοκληρώνουν τις αγοραπωλησίες.

Το λιμάνι της πόλης του Antwerp στο Βέλγιο είναι από τα μεγαλύτερα σε κίνηση στην Ευρώπη και έχει ήδη ξεκινήσει το εγχείρημα της μετάβασης προς ένα Έξυπνο Λιμάνι χρησιμοποιώντας την τεχνολογία του BC. Με το BC όλες οι πληροφορίες για την απελευθέρωση ενός κοντέινερ συλλέγονται σε μια βάση δεδομένων και περιορίζονται στα εμπλεκόμενα μέρη. Δημιουργούνται ψηφιακά δικαιώματα που μεταφέρονται μεταξύ των μερών και έτσι ο αποστολέας δεν έχει κανένα πλέον δικαίωμα πάνω στο εμπόρευμα μετά την παραλαβή του αποδέκτη. Έτσι, αποκλείεται η διεκδίκηση εμπορευματοκιβωτίων από μη εξουσιοδοτημένα μέρη. Μία ακόμα σπουδαία συμβολή αποτελεί η αυτοματοποίηση και διασφάλιση της ροή των νομικών εγγράφων και πιστοποιητικών υγειονομικής φύσεως, μέσω των έξυπνων συμβολαίων. Εξασφαλίζεται η γνησιότητα, η απώλεια εγγράφων και η ανάγκη διπλοτύπων. Το επόμενα βήμα είναι η ανταλλαγή δεδομένων μεταξύ των εμπλεκομένων στη SCM, η σύνδεση των μεγάλων βάσεων δεδομένων[27] και η αυτοματοποίηση κοινών επιχειρηματικών διαδικασιών με σκοπό την αύξηση της αποτελεσματικότητας (Chang, Iakovou and Shi, 2019).

Προς την κατεύθυνση της εφαρμογής προτύπων και τεχνικών για την απλούστευση και τη διευκόλυνση της ροής και της ανταλλαγής των πληροφοριών μεταξύ εμπορικών επιχειρήσεων και κυβερνήσεων κινείται το "Single Window", μία πλατφόρμα μέσω της οποίας εισάγονται και διαχειρίζονται όλα τα δεδομένα αποστολής και αποδείξεων. Το εγχείρημα αυτό εμποδίζεται εξαιτίας της έλλειψης κατάλληλης τεχνολογίας πληροφοριών και επικοινωνιών για την υλοποίησή του και της απροθυμίας συνεργασίας μεταξύ κυβερνητικών αρχών. Το BC μαζί με το IoT και την υπολογιστική νέφους διαφαίνεται να μπορούν να ξεπεράσουν συλλογικά αυτές τις προκλήσεις.

6.3 Περιγραφή της εφαρμογής

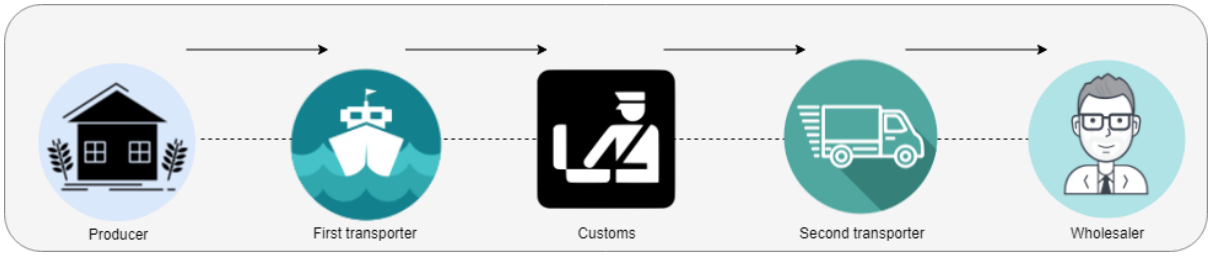
Η εφαρμογή ουσιαστικά αποτελεί μία προσομοίωση της περίπτωσης ενσωμάτωσης BC, IoT και SC για την επίτευξη διαφάνειας στην εφοδιαστική αλυσίδα. Μελετά την περίπτωση όπου ένας χονδρέμπορος παραγγέλνει μία ποσότητα ευπαθών προϊόντων όπως τα οπωροκηπευτικά σε έναν παραγωγό και εκείνος επιλέγει τους μεταφορείς. Στο σενάριό μας εμπλέκεται και το τελωνείο ως σταθμός κατά τη μεταφορά στον τελικό αποδέκτη.

[26] Με την έννοια του διαχειριστή.
[27] Απόδοση του όρου "data silos".



Διαφάνεια της εφοδιαστικής αλυσίδας με τη χρήση Blockchain, Smart Contracts και IoT

Η περίπτωση χρήσης που προσπαθούμε να προσομοιάσουμε ακολουθεί. Ο παραγωγός είναι ο ιδιοκτήτης του SC. Κάθε φορά που γίνεται μία παραγγελία δημιουργεί ένα SC και ορίζει ποιοι είναι οι συμμετέχοντες και ποια είναι τα ποσά που θα λάβει ο καθένας από την πληρωμή που καταθέτει ο τελικός αποδέκτης. Αφού το δίκτυο είναι ιδιωτικό και οι διευθύνσεις που συμμετέχουν στο SC καθορισμένες, παρέχεται έλεγχος πρόσβασης και ταυτοποίηση χρήστη. Ο χονδρέμπορος με μία συναλλαγή ορίζει τα όρια θερμοκρασίας που θεωρεί επιτρεπτά ώστε τα προϊόντα του να διατηρηθούν φρέσκα και καταβάλει με μία άλλη συναλλαγή το συνολικό ποσό πληρωμής, το οποίο εξασφαλίζει το κέρδος του παραγωγού, την πληρωμή του τελωνείου και τις αμοιβές των μεταφορέων. Τα συμβαλλόμενα μέρη καταθέτουν ποσά ως εχέγγυα για να συμμετάσχουν στη διαδικασία. Έτσι ώστε αν το προϊόν πάθει βλάβη, να αποζημιώσουν αυτόματα τους υπόλοιπους. Επίσης, με τη συναλλαγή της κατάθεσης αποδέχονται το SC και όταν ολοκληρωθεί η επιβεβαίωση από όλα τα μέρη θεωρείται ενεργή η παραγγελία και μπορεί να φύγει από τον παραγωγό. Μία συσκευή IoT είναι συνδεδεμένη μέσα στο κοντέινερ του προϊόντος ώστε να προστατεύεται από φθορά και φυσικές επιθέσεις και είναι επιφορτισμένη να αποστέλλει δεδομένα θερμοκρασίας ανά τακτά χρονικά διαστήματα με τη μορφή συναλλαγών που αποθηκεύονται στο BC.



Σενάριο ομαλής μεταφοράς προϊόντος από τον παραγωγό στον χονδρέμπορο

Το SC κρατά στοιχεία για την κατάσταση του εμπορεύματος και τα ανανεώνει αν η θερμοκρασία υπερβεί το προκαθορισμένο όριο. Αν συμβεί αυτό αλλάζει την κατάσταση του εμπορεύματος σε "μη υγιές" και της παραγγελίας σε "ανενεργή". Στο παράδειγμά μας, αν συμβεί κατά τη μεταφορά από τον παραγωγό στο τελωνείο, ο πρώτος μεταφορέας θα αποζημιώσει τον δεύτερο, θα πληρώσει τον παραγωγό ενώ θα επιστραφούν τα χρήματα στον χονδρέμπορο. Αν συμβεί κατά τη μεταφορά από το τελωνείο στο χονδρέμπορο, τότε πάλι θα επιστραφούν τα χρήματα στον χονδρέμπορο και θα αποζημιωθεί ο παραγωγός και ο πρώτος μεταφορέας. Η διαφορά στη δεύτερη περίπτωση είναι ότι ο μεταφορέας θα καλύψει και την πληρωμή των φόρων του τελωνείου. Στο σενάριο που όλα πάνε καλά με το που φθάσει το εμπόρευμα στον τελικό προορισμό, με τη μεταβίβαση γίνεται αυτόματα ο διαμοιρασμός των χρημάτων στα ενδιαφερόμενα μέρη, αλλάζει η κατάσταση της παραγγελίας σε "ανενεργή" και σταματά η IoT συσκευή να μεταδίδει δεδομένα.

Η διαδικασία της μεταφοράς αυτοματοποιείται και μέσω των προαναφερθέντων τεχνολογιών εξασφαλίζονται τα κάτωθι:

- Διαφάνεια και εμπιστοσύνη στον τρόπο που εκτελείται η διαδικασία.
- Παρακολούθηση κατάστασης του προϊόντος.
- Μη μεταβλητή διατήρηση ιστορικού κατά τη μεταφορά του εμπορεύματος.
- Εξασφάλιση των συμφερόντων όλων των μερών.

6.4 Τεχνολογία Ethereum

Το Ethereum ενσωματώνει πολλά χαρακτηριστικά και τεχνολογίες που είναι γνωστά στους χρήστες του Bitcoin, ενώ εισάγει επίσης πολλές τροποποιήσεις και καινοτομίες. Είναι ένα προγραμματιζόμενο BC που επιτρέπει στους χρήστες να δημιουργήσουν τις δικές τους εφαρμογές. Το Ethereum σχεδιάστηκε το 2013 από τον Vitalik Buterin ο οποίος εμπνεύστηκε να δημιουργήσει μια πλατφόρμα η οποία θα διευκολύνει την ανάπτυξη αποκεντρωμένων εφαρμογών (DAO) με βάση το BC. Διαθέτει δύο νομίσματα: ένα δικό του κρυπτονόμισμα που ονομάζεται *Ether* και ένα εσωτερικό νόμισμα για να πληρώνει για υπολογισμούς και τέλη συναλλαγών που ονομάζεται *Gas*. Οι αποκεντρωμένες εφαρμογές μπορούν να προγραμματιστούν με μια ενσωματωμένη ολοκληρωμένη Turing[28] γλώσσα που ονομάζεται *Solidity*. Το Ethereum χρησιμοποιεί το PoW για να επιτύχει συναίνεση μέσα στο δίκτυο, αλλά σύντομα σκοπεύει να κάνει τη μετάβαση σε PoS. Η βασική έκδοση των αλγορίθμων απόδειξης εργασίας που χρησιμοποιεί σήμερα το Ethereum είναι ένας αλγόριθμος κατακερματισμού που ονομάζεται *Dagger-Hashimoto*. Ο χρόνος δημιουργίας μπλοκ είναι σημαντικά χαμηλότερος από ό, τι σε πολλά άλλα συστήματα και πλατφόρμες και ανέρχεται σε περίπου 12 δευτερόλεπτα. Δεδομένου ότι ο χαμηλότερος χρόνος δημιουργίας μπλοκ οδηγεί σε υψηλότερο ρυθμό ορφανών μπλοκ, το σύστημα

[28] Αναφέρεται σε μια γλώσσα προγραμματισμού που μπορεί να λύσει οποιοδήποτε υπολογιστικό πρόβλημα αν παρέχεται αρκετός χρόνος και χώρος

χρησιμοποιεί το πρωτόκολλο *GHOST* για να θεωρήσει την μακρύτερη υπολογιστικά αλυσίδα ως το αυθεντικό BC (Novo, 2018). Ακολουθούν βασικές έννοιες του Ethereum.

6.4.1 Βασικές Έννοιες

Λογαριασμοί Ethereum: Οι *λογαριασμοί* έχουν μία *διεύθυνση* 20-byte και χρησιμοποιούνται για άμεση μεταφορά αξίας και πληροφοριών μεταξύ λογαριασμών. Διακρίνονται σε δύο είδη:

1. εξωτερικοί λογαριασμοί που ελέγχονται με ιδιωτικά κλειδιά και
2. λογαριασμούς συμβολαίων, οι οποίοι ελέγχονται βάσει του συμβατικού τους κώδικα.

Ένας εξωτερικός λογαριασμός δεν έχει κώδικα και χρησιμοποιείται για να στείλει κανείς μηνύματα δημιουργώντας και υπογράφοντας μια συναλλαγή. Από την άλλη σε έναν λογαριασμό συμβολαίου, κάθε φορά που ο λογαριασμός του δέχεται ένα μήνυμα ενεργοποιείται ο κώδικας του, επιτρέποντάς του να διαβάζει και να γράφει στον εσωτερικό αποθηκευτικό χώρο και να στέλνει άλλα μηνύματα ή να δημιουργεί συμβάσεις με τη σειρά του. Τα συμβόλαια είναι αυτόνομοι πράκτορες που ζουν μέσα στο περιβάλλον εκτέλεσης του Ethereum, εκτελώντας πάντοτε ένα συγκεκριμένο κομμάτι κώδικα όταν λάβουν ένα μήνυμα ή μία συναλλαγή. Επίσης έχουν άμεσο έλεγχο πάνω στο υπόλοιπο τους σε Ether.

Μηνύματα: Τα μηνύματα είναι εικονικά αντικείμενα που υπάρχουν μόνο στο περιβάλλον εκτέλεσης του Ethereum. Τα συμβόλαια και έχουν τη δυνατότητα να αποστέλλουν μηνύματα σε άλλα συμβόλαια. Αποτελούνται από τον αποστολέα, τον παραλήπτη, την ποσότητα Ether που μεταφέρεται μαζί με το μήνυμα, ένα προαιρετικό πεδίο και μία τιμή *STARTGAS* (μέγιστος αριθμός υπολογιστικών βημάτων που επιτρέπεται να εκτελέσει η συναλλαγή). Ουσιαστικά, είναι ένα μήνυμα που παράγεται από ένα συμβόλαιο. Η χορήγηση Gas που αντιστοιχεί σε μία συναλλαγή ή συμβόλαιο ισχύει για το συνολικό Gas που καταναλώνεται από τη συγκεκριμένη συναλλαγή και για όλες τις υποεκτελέσεις της.

Συναλλαγές: Μία συναλλαγή είναι ένα μήνυμα που αποστέλλεται από ένα λογαριασμό σε ένα άλλο. Δύναται να περιέχει δυαδικά δεδομένα και Ether. Αν ο παραλήπτης είναι ένα SC, ο κώδικας του εκτελείται και αναλόγως του κόστους εκτέλεσης των υπολογισμών του, αποζημιώνεται σε Gas.

Gas: Κατά τη δημιουργία, κάθε συναλλαγή χρεώνεται με μια ορισμένη ποσότητα Gas. Σκοπός ύπαρξης του είναι να περιορίσει το φόρτο εργασίας που απαιτείται για την εκτέλεση μίας συναλλαγής και να πληρώσει για αυτή την εκτέλεση. Το Gas εξαντλείται προοδευτικά σύμφωνα με συγκεκριμένους κανόνες. Η τιμή καθορίζεται από τον δημιουργό της συναλλαγής, ο οποίος πρέπει να πληρώσει την τιμή του Gas επί την ποσότητά του. Εάν απομείνει κάποια ποσότητα μετά την εκτέλεση, επιστρέφεται στον δημιουργό της. Στην περίπτωση που εξαντληθεί κατά την εκτέλεση ενεργοποιείται εξαίρεση (exception) η οποία επαναφέρει όλες τις τροποποιήσεις που έλαβαν χώρα.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Εκτέλεση κώδικα: Ο κώδικας των συμβολαίων υποστηρίζεται από γλώσσα χαμηλού επιπέδου γνωστή ως *κώδικας εικονικής μηχανής Ethereum* ή *κώδικας EVM* και αποτελείται από μια σειρά από bytes, όπου κάθε byte αντιπροσωπεύει μια λειτουργία.

Νόμισμα και Έκδοση: Το δίκτυο Ethereum περιλαμβάνει το δικό του ενσωματωμένο νόμισμα, *Ether*. Αυτό παρέχει ένα βασικό επίπεδο ρευστότητας για την ανταλλαγή διαφόρων τύπων ψηφιακών αγαθών και, το σημαντικότερο, ένα μηχανισμό πληρωμής των τελών συναλλαγής. Οι ονομαστικές αξίες τους είναι οι εξής: *Wei* = 1^{-18} Ether, *Szabo* = 1^{-12} Ether, *Finney* = 1^{-15} Ether. Στο εγγύς μέλλον, αναμένουμε ότι το Ether θα χρησιμοποιηθεί για συναλλαγές, το Finney για μικροσυναλλαγές και το Szabo και το Wei για τεχνικές συζητήσεις γύρω από τις αμοιβές και την εφαρμογή του πρωτοκόλλου.

Απενεργοποίηση και αυτοκαταστροφή: Αν παραστεί η ανάγκη κατάργησης του κώδικα από το BC, αυτό μπορεί να συμβεί μόνο όταν ένα συμβόλαιο σε αυτή τη διεύθυνση εκτελεί τη λειτουργία *αυτοκαταστροφής (self-destruct)*. Το υπολειπόμενο Ether που είναι αποθηκευμένο στην υπό απενεργοποίηση διεύθυνση, αποστέλλεται σε έναν καθορισμένο παραλήπτη και στη συνέχεια αποδεσμεύεται ο αποθηκευτικός χώρος και ο κώδικας. Η κατάργηση ενός συμβολαίου σύμβασης μπορεί να αποβεί δυνητικά επικίνδυνη αφού αν κάποιος στέλνει Ether σε καταργημένα συμβόλαια, το Ether χάνεται για πάντα (Chinchilla, 2017).

6.4.2 Γλώσσα Solidity

Πρόκειται για μία αντικειμενοστραφή γλώσσα υψηλού επιπέδου για την εφαρμογή SC. Έχει επιρροές από τις γλώσσες C ++, Python και JavaScript και έχει σχεδιαστεί για την EVM αν και μπορεί να τρέξει και σε άλλες πλατφόρμες όπως το Visual Studio 2017. Χρησιμοποιεί στατικούς τύπους[29], υποστηρίζει κληρονομικότητα, βιβλιοθήκες και σύνθετους τύπους που ορίζονται από τον χρήστη, μεταξύ άλλων χαρακτηριστικών. Δίνει τη δυνατότητα δημιουργίας SC για χρήσεις όπως ψηφοφορία, συλλογική χρηματοδότηση, τυφλές δημοπρασίες και πορτοφόλια πολλαπλών υπογραφών. Ο κώδικας υπόκεινται συχνά σε αλλαγές για να προστεθούν νέα χαρακτηριστικά και διορθώσεις σφαλμάτων, οπότε κατά την ανάπτυξη συμβολαίων, θα πρέπει να χρησιμοποιείται η πιο πρόσφατη έκδοση της Solidity. Επί του παρόντος βρίσκεται στην *v0.5.11* έκδοσή της (Solidity.readthedocs.io, 2019).

6.4.3 Ολοκληρωμένο περιβάλλον ανάπτυξης Remix

Η υλοποίησή μας θα γίνει με βάση το Remix. Το Remix είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης που βασίζεται σε πρόγραμμα περιήγησης στο διαδίκτυο, το οποίο μέσω του μεταγλωττιστή του επιτρέπει τη συγγραφή έξυπνων συμβολαίων σε γλώσσα Solidity και στη συνέχεια την ανάπτυξη και εκτέλεση τους. Υπάρχει και η δυνατότητα χρήσης του χωρίς σύνδεση στο διαδίκτυο όμως πρέπει

[29] Μια γλώσσα προγραμματισμού λέγεται ότι χρησιμοποιεί στατικούς τύπους όταν ο έλεγχος τύπων γίνεται κατά τη διάρκεια του χρόνου μεταγλώττισης αντί του χρόνου εκτέλεσης.

να εγκατασταθούν κάποιες τεχνολογίες και ο χρήστης καλό θα είναι να ελέγχει ανά τακτά διαστήματα αν έχει την πιο επικαιροποιημένη έκδοση. Το αρχείο καθώς και οι οδηγίες εγκατάστασης υπάρχουν στη διεύθυνση *https://github.com/ethereum/remix-live/tree/gh-pages*. Για τη χρήση του σε απευθείας σύνδεση ανατρέχουμε στη διεύθυνση *https://remix.ethereum.org* όπου δεν χρειάζεται να εγκαταστήσουμε κανένα λογισμικό ενώ είμαστε βέβαιοι ότι είναι πάντα διαθέσιμη η τελευταία έκδοση, όμως μπορεί να παρατηρηθεί μία μικρή καθυστέρηση που οφείλεται στη φόρτωση.

6.5 Επόμενα Βήματα και Συμπεράσματα Υλοποίησης

Από τη βιβλιογραφική μελέτη του κλάδου, των τεχνολογιών που συμμετέχουν αλλά και την πραγματοποίηση ενός έξυπνου συμβολαίου εντοπίστηκαν βελτιώσεις που θα μπορούσαν να επιτευχθούν.

6.5.1 Βελτίωση απόδοσης

Η παρούσα υλοποίηση έχει σκοπό την βαθύτερη κατανόηση του πώς μπορεί να επιτευχθεί η ενοποίηση BC και IoT στην SCM. Για το λόγο αυτό δόθηκε προτεραιότητα στη συγγραφή κώδικα που να καλύπτει τη βασική λειτουργικότητα και να αναδείξει δυνατότητες και αδυναμίες στο όλο εγχείρημα. Οπότε το ζήτημα της απόδοσης σε οικονομικούς όρους δεν ήταν προτεραιότητα. Δηλαδή κατά την ανάπτυξη της εφαρμογής δεν λήφθηκε υπόψιν η ποσότητα *Gas* που καταναλώνει το SC κατά την εκτέλεση των διαφορετικών συναρτήσεων του. Αξιόλογες υλοποιήσεις που μελετούν την ενοποίηση των δύο τεχνολογιών αλλά και την αξιοποίηση των SC, εντοπίζουν την ανάγκη αξιολόγησης της ποσότητας *Gas* για τη σύγκριση μεταξύ εναλλακτικών μοντέλων αφού είναι ενδεικτική της κατανάλωσης πόρων του EVM (Siris et al. 2019a; Siris et al., 2019b). Σαν επόμενο βήμα λοιπόν θα μπορούσε να θεωρηθεί η μελέτη μίας εναλλακτικής με καλύτερη απόδοση.

6.5.2 Αξιολόγηση διαφορετικών IoT τεχνολογιών και συσκευών

Στο πλαίσιο της παρούσας μελέτης, η συμβολή μίας έξυπνης συσκευής προσομοιάστηκε με κώδικα. Σίγουρα μία πιο εκτενής υλοποίηση με πραγματικές συσκευές με αισθητήρες είναι απαραίτητη ώστε να εξεταστεί η απόδοση του συστήματος και να εντοπιστούν ζητήματα που δεν έχουν προβλεφθεί. Ένας ενδιαφερόμενος θα μπορούσε να επεκτείνει τη λειτουργικότητα για να γίνει μία σύγκριση μεταξύ IoT συσκευών ή/και μεταξύ IoT τεχνολογιών (RFID, WSN).

6.5.3 Επέκταση λειτουργικότητας

Στη συγκεκριμένη εφαρμογή, ανάλογα με τις απαιτήσεις των ενδιαφερόμενων μερών και τη φύση των αγαθών θα μπορούσαν να προστεθούν αισθητήρες μέτρησης υγρασίας και η καταγραφή θέσης με σκοπό την πιο αυστηρή παρακολούθηση των συνθηκών μεταφοράς βρώσιμων και ευπαθών προϊόντων.

6.5.4 Ένταξη εξωτερικών φορέων

Στην SCM δεν αλληλεπιδρούν μόνο οι άμεσα συμβαλλόμενοι. Στην εφαρμογή μας υπάρχει και η οντότητα του Τελωνείου, το οποίο αν και δεν συμμετέχει άμεσα, παρόλα αυτά χρησιμεύει στην αυτοματοποίηση του συστήματος. Η ένταξη και άλλων τέτοιων φορέων μπορεί να ενισχύσει την λειτουργικότητα του συστήματος. Από μελέτη των Chang, Iakovou και Shi (2019) παρατηρούμε ότι κρατικές υπηρεσίες και ρυθμιστικές αρχές θα είχαν άμεσα οφέλη από το BC. Θα μπορούσαν εύκολα να ελέγχουν τυχόν παραβάσεις εμπορικού δικαίου ακόμα και σε διεθνείς συναλλαγές, θα αυτοματοποιούσαν τη συλλογή φόρων από αγοραπωλησίες και θα συνέβαλαν στην υλοποίηση του εγχειρήματος του "Single Window".

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 7: Συμπεράσματα

Η αλυσίδα καταγραφών και τα έξυπνα συμβόλαια είναι εκκολαπτόμενες τεχνολογίες και η ενοποίηση τους με το διαδίκτυο των πραγμάτων αποκαλύπτει ότι υπάρχει πρόσφορο έδαφος για περαιτέρω εξέλιξη. Απέχουμε πολύ από το σημείο πλήρους ωρίμανσης όπου εφαρμογές που αξιοποιούν τις προαναφερθείσες τεχνολογίες θα φτάσουν να γίνουν χρήσιμα εργαλεία στην καθημερινή ζωή μας. Οι μέχρι τώρα αναδυόμενες προκλήσεις αντιμετωπίζονται κατά περίπτωση και υπάρχει έλλειψη προτυποποίησης σε πλατφόρμες BC. Ακόμα όμως και αν βρεθούν καθολικές λύσεις για τα ζητήματα ασφάλειας, ιδιωτικότητας και απόδοσης, παραμένει σημαντική τροχοπέδη η εφαρμογή κατάλληλου νομοκανονιστικού πλαισίου που να ρυθμίζει τέτοιες εφαρμογές.

Δεδομένου ότι οι έξυπνες συσκευές έχουν διεισδύσει στη ζωή μας, η υιοθέτηση του BC στο IoT καθίσταται πολύ δύσκολη χωρίς την ευαισθητοποίηση του κοινού και την εκπαίδευση όσων ασχολούνται με την τεχνολογία. Η έλλειψη ενημέρωσης σχετικά με την εφαρμογή της τεχνολογίας BC σε τομείς εκτός των κρυπτονομισμάτων καταστέλλει την ευρεία αποδοχή της. Καίριας σημασίας είναι και η απουσία εξειδικευμένου ανθρώπινου δυναμικού με βαθιά γνώση και δεξιότητες επί του θέματος ώστε να αντιμετωπιστούν τα όποια τεχνολογικά εμπόδια και να αναζητηθούν νέες εφαρμογές.

Η εφαρμογή απέδειξε ότι όντως η χρήση ενός SC μπορεί να χρησιμοποιηθεί στην εφοδιαστική αλυσίδα για να αντιμετωπιστεί το ζήτημα διαφάνειας και εμπιστοσύνης κατά τη μεταφορά ευπαθών προϊόντων. Συμπεραίνουμε ότι ο αρχικός καθορισμός των συμμετεχόντων από τον κάτοχο του SC χρησιμεύει σε μετέπειτα στάδιο στον έλεγχο αυθεντικοποίησης και εξουσιοδότησης. Υπάρχουν διακριτοί ρόλοι και δικαιώματα που υποχρεώνουν τους συμμετέχοντες σε συμμόρφωση με τους κανόνες του συμβολαίου. Η ενσωμάτωση διαδικασίας αποδοχής του SC και κατά συνέπεια των όρων του, σε συνάρτηση με την επιβολή κατάθεσης ενός χρηματικού ποσού ως εχέγγυου από τα ενδιαφερόμενα μέρη εξασφαλίζουν τα οικονομικά τους συμφέροντα και την μετέπειτα αποφυγή διενέξεων. Η μεταφορά αυτοματοποιείται και προσφέρεται παρακολούθηση κατάστασης του προϊόντος που οδηγεί με τη σειρά του σε αυξημένη ελεγξιμότητα.

Ο τρόπος υλοποίησης της προτεινόμενης εφαρμογής έγινε με γνώμονα την επεκτασιμότητα της λειτουργικότητας του. Έτσι, είναι εύκολο να προστεθεί διαδικασία μέτρησης υγρασίας, να λαμβάνεται υπόψιν ο χρόνος παράδοσης και να γίνεται καταγραφή της θέσης των προϊόντων. Ακόμη, είναι δυνατή η ένταξη κρατικών φορέων για την αποφυγή παραβάσεων εμπορικού δικαίου και την αυτόματη συλλογή φόρων από αγοραπωλησίες.

Κατά τη μελέτη και συγγραφή του κώδικα διαπιστώθηκε ότι υπάρχουν ελάχιστες αναφορές σε έτοιμες, ολοκληρωμένες λύσεις πέρα των κρυπτονομισμάτων για όσους ενδιαφέρονται να αξιοποιήσουν τα SC για την επίλυση γνωστών ζητημάτων σε διάφορους κλάδους. Για το λόγο αυτό στο παράρτημα της παρούσας εργασίας υπάρχει το σύνολο του κώδικα που αναπτύχθηκε (σε γλώσσα solidity) πλήρως

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

τεκμηριωμένο με σχόλια καθώς και ένα εγχειρίδιο χρήσης με αναλυτικά βήματα για την επιτυχή εκτέλεση του SC (στο περιβάλλον του remix IDE).

Εκτός των άλλων παρουσιάσαμε πιθανές μελλοντικές κατευθύνσεις και τάσεις στον υπό εξέταση κλάδο. Ο τομέας των Big Data επηρεάζει ήδη το IoT και αναμένεται να περάσει στη σφαίρα επιρροής και του BC μέσω των ζητημάτων της αποθήκευσης και της αναλυτικής των δεδομένων. Το Fog Computing διαφαίνεται σαν μία ενδιάμεση λύση όπου οι κόμβοι ομίχλης μπορούν να ενσωματώνουν εξορύκτες και να διευκολύνουν τη διασύνδεση IoT συσκευών με το BC. Εντοπίζεται η ανάγκη ύπαρξης ενός μηχανισμού εξέτασης BC με σκοπό την επιλογή του καταλληλότερου ανά εφαρμογή. Η AI υπόσχεται να αντικαταστήσει τη χρήση oracles με SC που θα μαθαίνουν μόνα τους για να λαμβάνουν ευφυείς αποφάσεις. Κάτι το οποίο λείπει και είναι επιτακτικό είναι ο σχεδιασμός ενός πρωτοκόλλου συναίνεσης ειδικά για IoT ώστε να καλύπτονται οι απαιτήσεων ασφάλειας και απόδοσης κατά την επικύρωση. Στο εγγύς μέλλον θα δούμε νέες εφαρμογές όπως το Internet-of-Battlefield-Things όπου το BC θα συμβάλει στην αυτοματοποίηση λήψης αποφάσεων στο πεδίο της μάχης. Τέλος αναμένουμε την ενσωμάτωση των πρωτοκόλλων επικοινωνίας με το BC. Παράδειγμα αποτελεί το TeleHash, ένα ελαφρύ και ασφαλές πρωτόκολλο διομότιμου δικτύου που χρησιμοποιεί κρυπτογράφηση για την ασφαλή επικοινωνία.

Εν κατακλείδι, ο συνδυασμός αλυσίδας καταγραφών, έξυπνων συμβολαίων και διαδικτύου των πραγμάτων δύναται να αναδείξει πολλές νέες και καινοτόμες εφαρμογές όμως απομένει να φανεί ποιές θα υιοθετηθούν από τον επιχειρηματικό κόσμο και τους τελικούς χρήστες.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 8: Λεξικό Όρων

Ασφάλεια (Security)

Ασφάλεια ονομάζεται η προστασία της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας.

Αμφίδρομη πρόσδεση (Two-way peg)

Η αμφίδρομη πρόσδεση αναφέρεται στον μηχανισμό με τον οποίο νομίσματα μεταφέρονται μεταξύ των πλευρικών αλυσίδων και πίσω με ένα πάγια ή με άλλη ντετερμινιστική συναλλαγματική ισοτιμία (Back et al., 2014).

Ακεραιότητα (Integrity)

Ακεραιότητα ονομάζεται η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας (Κάτσικας and Γκρίτζαλης, 2004).

Αντικείμενο (Thing)

Όσον αφορά το Διαδίκτυο των Πραγμάτων, είναι ένα αντικείμενο του φυσικού κόσμου (φυσικά πράγματα) ή του κόσμου των πληροφοριών (εικονικά πράγματα), το οποίο είναι ικανό να αναγνωριστεί και να ενσωματωθεί στα δίκτυα επικοινωνίας.

Αυθεντικοποίηση χρήστη (user authentication)

Αυθεντικοποίηση χρήστη ονομάζεται η διαδικασία που αποσκοπεί στην επιβεβαίωση της ταυτότητας ενός χρήστη (Κάτσικας and Γκρίτζαλης, 2004).

Διεκπεραιωτικότητα / ρυθμαπόδοση (Throughput)

α) Δίκτυα υπολογιστών: το ποσό δεδομένων ανά δευτερόλεπτο που μπορεί να μεταφερθεί (Kurose and Ross, 2012).

β) Αλυσίδα Καταγραφών: Η διεκπεραιωτικότητα ορίζεται ως ο αριθμός επιτυχημένων συναλλαγών ανά δευτερόλεπτο, αρχής γενομένης από τον πρώτο χρόνο ανάπτυξης της συναλλαγής. Η μέση διεκπεραιωτικότητα είναι ο μέσος όρος της διεκπεραιωτικότητας σε σχέση με τον χρόνο εκτέλεσης (Pongnumkul, Siripanpornchana and Thajchayapong, 2017).

Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η αποφυγή της αδικαιολόγητης καθυστέρησης ενός εξουσιοδοτημένου χρήστη να αποκτήσει προσπέλαση σε πληροφορίες ή υπολογιστικούς πόρους (Κάτσικας and Γκρίτζαλης, 2004).

Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Το δικαίωμα διαγραφής είναι το δικαίωμα να ζητεί το υποκείμενο των δεδομένων τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον δεν επιθυμεί πια αυτά τα δεδομένα να αποτελούν αντικείμενο επεξεργασίας, και εφόσον δεν υφίσταται νόμιμος λόγος να τα κατέχει ο υπεύθυνος επεξεργασίας (European Parliament 2016/679/EU).

Δυνατότητα κλιμάκωσης / Επεκτασιμότητα (Scalability)

Η έννοια υποδηλώνει την δυνατότητα ενός συστήματος να ικανοποιεί έναν αυξανόμενο αριθμό στοιχείων ή αντικειμένων, να επεξεργάζεται με άνεση τους αυξανόμενους όγκους εργασίας ή / και να είναι επιδεκτικό στη διεύρυνση (Bondi, 2000).

Εξουσιοδότηση (Authorisation)

Εξουσιοδότηση ονομάζεται η διαδικασία κατά την οποία ο ιδιοκτήτης ενός αγαθού παρέχει κάποιο είδος δικαιώματος σε ένα πρόσωπο ή σε μια διαδικασία (Κάτσικας and Γκρίτζαλης, 2004).

Ελαφρύς εξυπηρετούμενος (Light client)

Ένας τρόπος αλληλεπίδρασης με ένα BC που απαιτεί μόνο ένα πολύ μικρό ποσό υπολογιστικών πόρων, παρακολουθώντας από προεπιλογή μόνο τις κεφαλίδες των μπλοκ της αλυσίδας και την απόκτηση των απαραίτητων πληροφοριών σχετικά με τις συναλλαγές, την κατάσταση ή τις αποδείξεις ζητώντας και επαληθεύοντας τα αποδεικτικά στοιχεία των Merkle δέντρων των σχετικών δεδομένων με βάση τις ανάγκες (James, 2019).

Εμπιστευτικότητα (Confidentiality)

Εμπιστευτικότητα ονομάζεται η αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους (Κάτσικας and Γκρίτζαλης, 2004).

Επιβεβαίωση / Μη αποποίηση ευθύνης (Non Repudiation)

Μη αποποίηση ευθύνης ονομάζεται η αμοιβαία αυθεντικοποίηση αποστολής και παραλαβής δεδομένων από ένα υπολογιστικό συγκρότημα (Κάτσικας and Γκρίτζαλης, 2004).

Ευαίσθητη Πληροφορία (Sensitive Information)

Πληροφορία της οποίας η αποκάλυψη, τροποποίηση ή παρακράτηση χωρίς εξουσιοδότηση μπορεί να προκαλέσει απώλεια ή ζημιά (Κάτσικας and Γκρίτζαλης, 2004).

Ιδιωτικότητα (Privacy)

Αφορά στον έλεγχο του αν και πώς τα προσωπικά δεδομένα ενός προσώπου μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά (Rosenberg, 1992).

Κατάσταση (State)

Ως κατάσταση ορίζεται ένα σύνολο πληροφοριών που αντιπροσωπεύει την "τρέχουσα κατάσταση" ενός συστήματος, ο προσδιορισμός εάν μια συναλλαγή είναι έγκυρη ή όχι καθώς και το αποτέλεσμα μιας συναλλαγής θα πρέπει στο απλούστερο μοντέλο να εξαρτάται μόνο από την κατάσταση. Παραδείγματα δεδομένων κατάστασης περιλαμβάνουν το σύνολο UTXO σε bitcoin, υπόλοιπα, nonces, κώδικα και αποθήκευση στο Ethereum και καταχωρήσεις ονόματος τομέα στο Namecoin (James, 2019).

Μονόδρομη πρόσδεση (one-way peg)

Μια πρώιμη λύση ήταν για τη «μεταφορά» κρυπτονομισμάτων ήταν η καταστροφή bitcoin με έναν αναγνωρίσιμο τρόπο, ο οποίος σε δεύτερο χρόνο θα ανιχνευόταν από μία νέα αλυσίδα καταγραφών για να επιτρέψει τη δημιουργία νέων κρυπτονομισμάτων. Η διαδικασία αυτή είναι επίσης γνωστή ως μονόδρομη πρόσδεση (Back et al., 2014).

Πολυπρακτορικό Σύστημα (multi-agent system)

Είναι ένα ψηφιοποιημένο σύστημα που αποτελείται από πολλούς έξυπνους παράγοντες που αλληλεπιδρούν μεταξύ τους. Χρησιμοποιούνται για την επίλυση σύνθετων προβλημάτων με πολύ καλά αποτελέσματα από σε ένα ευρύ φάσμα εφαρμογών Casado-Vara et al. (2018.

Συνέπεια (Consistency)

Εάν οι μεμονωμένες συναλλαγές αφήνουν τη βάση δεδομένων σε μια "συνεπή" κατάσταση, τότε μια σειριοποιήσιμη εκτέλεση (ισοδύναμη με αποτύπωση σε σειριακή μορφή και εκτέλεση των συναλλαγών) θα εγγυάται ότι όλες οι συναλλαγές τηρούν μια "συνεπή" κατάσταση της βάσης δεδομένων (Bailis, Hellerstein and Stonebraker, 2019).

Συσκευή (device)

Όσον αφορά το Διαδίκτυο των Πραγμάτων, πρόκειται για εξοπλισμό με τις υποχρεωτικές δυνατότητες επικοινωνίας και τις προαιρετικές δυνατότητες ανίχνευσης, ενεργοποίησης, συλλογής δεδομένων, αποθήκευσης δεδομένων και επεξεργασίας δεδομένων.

Χρησμοί (oracles)

Τα έξυπνα συμβόλαια βασίζονται σε δεδομένα που είναι αποθηκευμένα στο blockchain, έτσι για λάβουν δεδομένα από τον "πραγματικό" κόσμο και να τα προωθήσουν στην αλυσίδα καταγραφών (ή και το αντίστροφο) βασίζονται σε εξωτερικές υπηρεσίες, οι οποίες αποδίδονται ως "χρησμοί" (Gatteschi et al., 2018)

Χρονική καθυστέρηση ή λανθάνων χρόνος (Latency / Delay)

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

α) Δίκτυα υπολογιστών: Καθώς ένα πακέτο ταξιδεύει από έναν κόμβο (κεντρικό υπολογιστή ή δρομολογητή) στον επόμενο κόμβο κατά μήκος αυτής της διαδρομής, το πακέτο υποφέρει από διάφορους τύπους χρονικών καθυστερήσεων σε κάθε κόμβο κατά μήκος της διαδρομής (Kurose and Ross, 2012).

β) Αλυσίδα Καταγραφών: Για κάθε συναλλαγή, ως χρονική καθυστέρηση ορίζεται η διαφορά μεταξύ του χρόνου ολοκλήρωσης και του χρόνου ανάπτυξης. Για ένα σύνολο συναλλαγών, η μέση λανθάνουσα καθυστέρηση είναι ο μέσος όρος λανθάνοντος χρόνου όλων των συναλλαγών στο σύνολο δεδομένων (Pongnumkul, Siripanpornchana and Thajchayapong, 2017).

Χρόνος εκτέλεσης (Execution Time)

Αλυσίδα Καταγραφών: Για κάθε σύνολο συναλλαγών, ο χρόνος εκτέλεσης είναι το συνολικό χρονικό διάστημα (αριθμός δευτερολέπτων) κατά τη διάρκεια του οποίου το BC αναλαμβάνει να εκτελέσει και να επιβεβαιώσει όλες τις συναλλαγές στο σύνολο δεδομένων (Pongnumkul, Siripanpornchana and Thajchayapong, 2017).

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 9: Βιβλιογραφία

(Abomhara and Køien, 2015) Abomhara M. and Køien, G. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*, 4(1), pp.65-88. Available at: https://doi.org/10.13052/jcsm2245-1439.414 [Accessed 15 Sep. 2019]

(Al-Fuqaha et al., 2015) Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), pp.2347-2376. Available at: https://doi.org/10.1109/COMST.2015.2444095 [Accessed 3 Sep. 2019]

(Alharby and Moorsel, 2017) Alharby, M. and Moorsel, A. (2017). Blockchain Based Smart Contracts: A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*. Available at: https://doi.org/10.5121/csit.2017.71011 [Accessed 12 Sep. 2019]

(Atlam et al., 2018) Atlam, H.F, Alenezi, A., Alassafi, M.O. and Wills, G. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *International Journal of Intelligent Systems and Applications*, 10(6), pp.40-48. Available at: https://eprints.soton.ac.uk/id/eprint/421529 [Accessed 19 Aug. 2019]

(Atzori, Iera and Morabito, 2010) Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, [online] 54(15), pp.2787-2805. Available at: https://doi.org/10.1016/j.comnet.2010.05.010 [Accessed 15 Sep. 2019].

(Back et al., 2014) Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P., (2014). Enabling blockchain innovations with pegged sidechains. Available at: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains [Accessed 5 Sep. 2019]

(Bahga and Madisetti, 2016) Bahga, A. and Madisetti, V.K. (2016). Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, 09(10), pp.533-546. Available at: http://dx.doi.org/10.4236/jsea.2016.910036 [Accessed 19 Aug. 2019]

(Bailis, Hellerstein and Stonebraker, 2019) Bailis, P., Hellerstein, J. and Stonebraker, M. (2019). *Readings in Database Systems*. 5th ed. p.10.

(Biswas and Muthukkumarasamy, 2016) Biswas, K. and Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. Available at: https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198 [Accessed 13 Sep. 2019]

(Bulow, 1986) Bulow, J. (1986). An Economic Theory of Planned Obsolescence. *The Quarterly Journal of Economics*, 101(4), pp. 729–749. Available at: https://doi.org/10.2307/1884176 [Accessed 4 Sep. 2019]

(Bondi, 2000) Bondi, A. (2000). Characteristics of Scalability and Their Impact on Performance. *Proceedings of the 2nd international workshop on Software and performance*, pp.195-203.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

(Boudguiga et al., 2017) Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A. and Sirdey, R. (2017). Towards better availability and accountability for iot updates by means of a blockchain. *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 50-58. Available at: https://doi.org/10.1109/EuroSPW.2017.50 [Accessed 19 Aug. 2019]

(Casado-Vara et al., 2018) Casado-Vara, R., Prieto, J., la Prieta, F. and Corchado, J. (2018). How blockchain improves the supply chain: case study alimentary supply chain. *Procedia Computer Science*, [online] 134, pp.393-398. Available at: https://doi.org/10.1016/j.procs.2018.07.193 [Accessed 15 Sep. 2019].

(Castro and Liskov, 1999) Castro, M., Liskov, B., (1999). Practical byzantine fault tolerance. In: OSDI, vol. 99, pp.173–186. Available at: https://doi.org/10.1145/571637.571640 [Accessed 11 Sep. 2019]

(Chang, Iakovou and Shi, 2019) Chang, Y., Iakovou, E. and Shi, W. (2019). Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities. *arXiv preprint arXiv:1901.02715*. Available at: https://arxiv.org/abs/1901.02715 [Accessed 20 Aug. 2019]

(Chinchilla, 2017) Chinchilla, C. (2017). *ethereum/wiki*. [online] GitHub. Available at: https://github.com/ethereum/wiki/wiki/White-Paper#ethereum-accounts [Accessed 15 Sep. 2019].

(Christidis and Devetsikiotis, 2016) Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, pp.2292-2303. Available at: https://doi.org/10.1109/ACCESS.2016.2566339 [Accessed 19 Aug. 2019]

(Decker and Wattenhofer, 2015) Decker, C. and Wattenhofer, R. (2015). A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. *Symposium on Self-Stabilizing Systems*, pp.3-18. Available at: https://doi.org/10.1007/978-3-319-21741-3_1 [Accessed 6 Sep. 2019].

(Dorri, Kanhere and Jurdak, 2016) Dorri, A., Kanhere, S.S. and Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*. Available at: http://arxiv.org/abs/1608.05187 [Accessed 19 Aug. 2019]

(Dorri, Kanhere and Jurdak, 2017) Dorri, A., Kanhere, S.S. and Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 173-178. Available at: http://dx.doi.org/10.1145/3054977.3055003 [Accessed 19 Aug. 2019]

(Dorri et al., 2017) Dorri, A., Kanhere, S., Jurdak, R. and Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Available at: https://doi.org/10.1109/PERCOMW.2017.7917634 [Accessed 22 Sep. 2019].

(Dye et al., 2008) Dye, M., Dye, M., McDonald, R. and Rufi, A. (2008). *Network fundamentals*. Indianapolis, Ind.: Cisco Press, pp.496-508.

(Eberhardt and Tai, 2017) Medium. (2019). *Sharding, Raiden, Plasma: The Scaling Solutions that Will Unchain Ethereum*. [online] Available at: https://medium.com/imbrexblog/sharding-raiden-plasma-the-scaling-solutions-that-will-unchain-ethereum-c590e994523b [Accessed 6 Sep. 2019]

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

(Energy Web Foundation, 2018) Energy Web Foundation (2018). The Energy Web Chain: Accelerating the Energy Transition with an Open-source, Decentralized Blockchain Platform.

(Energy Web Foundation, 2019) Energy Web Foundation (2019). The Energy Web Chain: Accelerating the Energy Transition with an Open-source, Decentralized Blockchain Platform (version 2.0). Available at: https://www.energyweb.org/reports/the-energy-web-chain/ [Accessed 20 Aug. 2019]

(Fernández-Caramés and Fraga-Lamas, 2018) Fernández-Caramés, T.M. and Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6, pp.32979 - 33001. Available at: https://doi.org/10.1109/ACCESS.2018.2842685 [Accessed 19 Aug. 2019]

(Ferrag et al., 2018) Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L. and Janicke, H. (2018). Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet of Things Journal*, 6(2), pp.2188-2204. Available at: https://arxiv.org/pdf/1806.09099.pdf [Accessed 19 Aug. 2019]

(Gatteschi et al., 2018) Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet*, 10(2). Available at: https://doi.org/10.3390/fi10020020 [Accessed 4 Sep. 2019]

(Gubbi et al., 2013) Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), pp.1645-1660. Available at: https://doi.org/10.1016/j.future.2013.01.010 [Accessed 15 Sep. 2019]

(European Parliament 2016/679/EU) European Parliament Regulation (EU) 2016/679 of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 5 Sep. 2019]

(Huckle et al., 2016) Huckle, S., Bhattacharya, R., White, M. and Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, 98, pp.461-466. Available at: https://doi.org/10.1016/j.procs.2016.09.074 [Accessed 19 Aug. 2019]

(Ibm.com, 2019) Ibm.com. (2019). *IoT for Blockchain*. [online] Available at: https://www.ibm.com/internet-of-things/trending/blockchain [Accessed 14 Sep. 2019]

(Iot.ieee.org, 2019) Iot.ieee.org. (2019). *Three Major Challenges Facing IoT - IEEE Internet of Things*. [online] Available at: https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot [Accessed 15 Sep. 2019]

(I.T.U., 2012) I.T.U., (2012). Overview of the Internet of things, SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, Next Generation Networks – Frameworks and functional

(James, 2019) James, R. (2019). *On sharding blockchains*. [online] GitHub. Available at: https://github.com/ethereum/wiki/wiki/Sharding-FAQ [Accessed 6 Sep. 2019]

(Jesus et al., 2018) Jesus, E.F., Chicarino, V.R., de Albuquerque, C.V. and Rocha, A.A.d.A. (2018). A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Security and Communication Networks*, 2018, pp.1-27. Available at: https://doi.org/10.1155/2018/9675050 [Accessed 19 Aug. 2019]

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

(Jing et al., 2014) Jing, Q., Vasilakos, A., Wan, J., Lu, J. and Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, [online] 20(8), pp.2481-2501. Available at: https://doi.org/10.1007/s11276-014-0761-7 [Accessed 15 Sep. 2019].

(Journal, 2009) Journal, R. (2009). *That 'Internet of Things' Thing*. [online] Available at: http://www.rfidjournal.com/articles/view?4986

(Karafiloski and Mishev, 2017) Karafiloski, E. and Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*. Available at: https://doi.org/10.1109/EUROCON.2017.8011213 [Accessed 14 Sep. 2019]

(Karst and Brodar, 2017) Karst, J. and Brodar, G. (2017). CONNECTING MULTIPLE DEVICES WITH BLOCKCHAIN IN THE INTERNET OF THINGS. Available at: https://courses.cs.ut.ee/MTAT.03.323/2016_fall/uploads/Main/002.pdf [Accessed 12 Sep. 2019].

(Κάτσικας and Γκρίτζαλης, 2004) Κάτσικας Σ., Γκρίτζαλης Δ., (2004). *Ασφάλεια πληροφοριακών συστημάτων*. Εκδόσεις Νέων Τεχνολογιών, pp.25-28.

(Kshetri, 2017) Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional*, 19(4), pp.68-72. Available at: http://dx.doi.org/10.1109/MITP.2017.3051335 [Accessed 19 Aug. 2019]

(Kurose and Ross, 2012) Kurose, J. and Ross, K. (2012). *Computer Networking*. Pearson Education Limited, pp.35-36.

(Leiding, Memarmoshrefi and Hogrefe, 2016) Leiding, B., Memarmoshrefi, P. and Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp '16*. Available at: https://doi.org/10.1145/2968219.2971409 [Accessed 14 Sep. 2019]

(Makhdoom et al., 2019) Makhdoom, I., Abolhasan, M., Abbas, H. and Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 125, pp.251-279. Available at: https://doi.org/10.1016/j.jnca.2018.10.019 [Accessed 19 Aug. 2019]

(Nakamoto, 2008) Nakamoto, S. (2008). Bitcoin: a Peer-to-peer Electronic Cash System. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.9986&rep=rep1&type=pdf [Accessed 12 Sep. 2019]

(Novo, 2018) Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), pp.1184-1195. Available at: https://doi.org/10.1109/JIOT.2018.2812239 [Accessed 19 Aug. 2019]

(Panarello et al., 2018) Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors*, 18(8), p.2575. Available at: https://doi.org/10.3390/s18082575 [Accessed 19 Aug. 2019]

(Pongnumkul, Siripanpornchana and Thajchayapong, 2017) Pongnumkul, S., Siripanpornchana, C. and Thajchayapong, S. (2017). Performance Analysis of Private Blockchain Platforms in Varying Workloads. *26th International Conference on Computer Communication and Networks, ICCCN 2017*, pp.1-6. Available at: https://doi.org/10.1109/ICCCN.2017.8038517 [Accessed 3 Sep. 2019]

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

(Reyna et al., 2018) Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, 88, pp.173-190. Available at: https://doi.org/10.1016/j.future.2018.05.046 [Accessed 19 Aug. 2019]

(Rosenberg, 1992) Rosenberg, R. (1992). *The social impact of computers*. San Diego, Calif.: Academic Press

(Roussakis and Rajkov, 2018) Roussakis, Y. and Rajkov, D. (2018). *Using blockchain for aircraft spare parts tracking: impact on MROs | Accenture Insights*. [online] Accenture-insights.nl. Available at: https://www.accenture-insights.nl/en-us/articles/blockchain-aircraft-spare-part-tracking-impact-mros [Accessed 14 Sep. 2019]

(Sethi and Sarangi, 2017) Sethi, P. and Sarangi, S. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, [online] 2017, pp.1-25. Available at: https://doi.org/10.1155/2017/9324035 [Accessed 15 Sep. 2019].

(Siris et al., 2019a) Siris, V., Nikander, P., Voulgaris, S., Fotiou, N., Lagutin, D. and Polyzos, G. (2019). Interledger Approaches. *IEEE Access*, 7, pp.89948-89966. Available at: https://doi.org/10.1109/ACCESS.2019.2926880 [Accessed 15 Sep. 2019]

(Siris et al., 2019b) Siris, V., Dimopoulos, D., Fotiou, N., Voulgaris, S. and Polyzos, G. (2019). OAuth 2.0 meets Blockchain for Authorization in Constrained IoT Environments. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. Available at: https://doi.org/10.1109/WF-IoT.2019.8767223 [Accessed 15 Sep. 2019]

(Solidity.readthedocs.io, 2019) Solidity.readthedocs.io. (2019). *Solidity - Solidity 0.5.12 documentation*. [online] Available at: https://solidity.readthedocs.io/en/latest/ [Accessed 15 Sep. 2019]

(Vukolić, 2015) Vukolić, M. (2015). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *International Workshop on Open Problems in Network Security (iNetSec)*, pp.112-125. Available at: https://doi.org/10.1007/978-3-319-39028-4_9 [Accessed 3 Sep. 2019]

(Zheng et al., 2018) Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), pp.352-375. Available at: https://www.researchgate.net/publication/328271018 [Accessed 19 Aug. 2019]

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Ενότητα 10: Παράρτημα

10.1 Κώδικας υλοποίησης σε γλώσσα solidity

```
pragma solidity ^0.4.17;

//---------------------------------------------------------------------------//
//>Contract that creates a new order (an order contract)
// At first, we deploy the Smart Contract of OrderCreator
// which can create new instances of Smart Contracts (Order).
// Every new contract (Order) has an address (like an account).
//---------------------------------------------------------------------------//
contract OrderCreator {
   address[] public createdOrders;
   function createNewOrder(uint quantity, string product) public {
      address newOrder = new Order(quantity, product, msg.sender);
      createdOrders.push(newOrder);
   }
}

contract Order {

   //---------------------------//
   // DECLARE VARIABLES
   //---------------------------//

   //---------------------------------------------------------------------------// start of struct
   // Stores details of order cost
   // This structure retains money that each party has to be paid
   // and the total value of the purchase.
   //---------------------------------------------------------------------------//
   struct OrderCostDetails {
      string product;
      uint quantity;
      uint total_price; // total_price = transport_1_cost + transport_2_cost + customs_cost + producers share
      uint transport_1_cost;
      uint transport_2_cost;
      uint customs_cost;
      uint reqApprovalNum;
   }
   mapping(address => OrderCostDetails) ordercostdetails;
   //---------------------------------------------------------------------------// end of struct

   //---------------------------------------------------------------------------// start of struct
   // Stores details of participating parties
   // This structure retains the address for each party involved.
   // It is used for access control and identification of each party.
   //---------------------------------------------------------------------------//
   struct OrderPartyDetails {
      address transport_1;
      address transport_2;
      address wholesaler;
      address customs;
      address dataLogger;
   }
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
mapping(address => OrderPartyDetails) orderpartydetails;
//-------------------------------------------------------------------------// end of struct

//-------------------------------------------------------------------------// start of struct
// Stores details regarding the transfer specifications
// This structure is used for checking of the product status
//-------------------------------------------------------------------------//
struct OrderTransferDetails {
   uint8 minAllowedTemp;
   uint8 maxAllowedTemp;
   string cargoStatus;
   address currentResponsibleParty;
}
mapping(address => OrderTransferDetails) ordertransferdetails;
//-------------------------------------------------------------------------// end of struct

//---------------------------------//
// Address of the producer
//---------------------------------//
address public producer;

//-------------------------------------------------------------------------------------------------------------------//
// Mappings for valid approvers - approvers that confirmed the order
// They are similar to java hash maps and they are used to perform checks:
// 1. approvers: if an address belongs to someone that has to approve the order
// 2. confApprovers: if the approver with this address has already approved the order
//-------------------------------------------------------------------------------------------------------------------//
mapping(address => bool) approvers;
mapping(address => bool) confApprovers;

//-------------------------------------------------------------------------------------------//
// Mapping of transporters
// transporters is used to check if an address belongs to a transporter party
//-------------------------------------------------------------------------------------------//
mapping(address => bool) public transporters;

//-----------------------------------------------------//
// Array that holds the product temperature
//-----------------------------------------------------//
uint[] temp_logs;

//-------------------------------------------------------------------------------------------------------------------//
// numOfApprovers: number of the parties that have confirmed the order
// confirmedOrder: a bool var that is used to check if an order is confirmed and it can proceed
//-------------------------------------------------------------------------------------------------------------------//
uint8 numOfApprovers;
bool confirmedOrder;

//-------------------------------------------------------------------------------------------------------------------//
// Modification functions that are used in other functions in order to avoid repeating code
// producerRestricted: in order to enforce that a function can be executed only from the producer
// wholeRestricted:    in order to enforce that a function can be executed only from the wholesaler
//-------------------------------------------------------------------------------------------------------------------//
modifier producerRestricted() {
   require(msg.sender == producer);
   _;
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
  }
  modifier wholeRestricted() {
    require(msg.sender == orderpartydetails[this].wholesaler);
    _;
  }

  //-------------------------------------------------------------------------------------------//
  // Constructor function of the Order called from an OrderCreator contract
  //-------------------------------------------------------------------------------------------//
  function Order(uint quantity, string product, address creator) public {
    //Initialize producer - vars
    producer = creator;
    numOfApprovers = 0;
    confirmedOrder = false;

    //Initialize instance of OrderCostDetails struct
    ordercostdetails[this] = OrderCostDetails({
    product: product
    , quantity: quantity
    , total_price: 0
    , transport_1_cost: 0
    , transport_2_cost: 0
    , customs_cost: 0
    , reqApprovalNum: 3 // fixed value for the current scenario (wholesaler, transport_1 & transport_2)
    });
  }

  //-------------------------//
  // SETUP FUNCTIONS
  //-------------------------//

  // step 1
  //-------------------------------------------------------------------------------------------//
  // The Producer (the account address of creator of the Order)
  // has to set the amount of money that each party has to be paid
  // and the total_cost that is used as security deposit from each transporter
  //-------------------------------------------------------------------------------------------//
  function setOrderCosts(uint total_price, uint transport_1_cost, uint transport_2_cost, uint customs_cost)
public  producerRestricted {
      //Update instance of OrderCostDetails struct
      ordercostdetails[this].total_price = total_price;
      ordercostdetails[this].transport_1_cost = transport_1_cost;
      ordercostdetails[this].transport_2_cost = transport_2_cost;
      ordercostdetails[this].customs_cost = customs_cost;
  }

  // step 2
  //-----------------------------------------------------------------------//
  // The Producer sets the addresses of each involved party
  //-----------------------------------------------------------------------//
  function setOrderParties(address transport_1, address transport_2, address wholesaler, address customs,
address dataLogger) public producerRestricted {

    // Initialize instance of OrderPartyDetails struct
    orderpartydetails[this] = OrderPartyDetails({
      transport_1: transport_1
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
      , transport_2: transport_2
      , wholesaler: wholesaler
      , customs: customs
      , dataLogger: dataLogger
    });

    // Update mapping of valid approvers ('true' means valid)
    approvers[transport_1] = true;
    approvers[transport_2] = true;
    approvers[wholesaler] = true;

    // Update mapping of confirmed approvers ('false' means they have not confirmed)
    confApprovers[transport_1] = false;
    confApprovers[transport_2] = false;
    confApprovers[wholesaler] = false;

    // Update mapping of transporters ('true' means the address belongs to a valid transporter)
    transporters[transport_1] = true;
    transporters[transport_2] = true;
}

// step 3
//-------------------------------------------------------------------------//
// The Wholesaler sets the temperature limits of the product
//-------------------------------------------------------------------------//
function setTransferDetails(uint8 minAllowedTemp, uint8 maxAllowedTemp) public wholeRestricted {
    ordertransferdetails[this] = OrderTransferDetails({
        minAllowedTemp: minAllowedTemp
      , maxAllowedTemp: maxAllowedTemp
      , cargoStatus: "HEALTHY"
      , currentResponsibleParty: producer
    });
}

// step 4
//-------------------------------------------------------------------------//
// Wholesaler, transport_1 and transport_2 must approve
// the order by paying the amount of total_price + 1 wei
// (extra money to cover the transactions' cost is required)
//-------------------------------------------------------------------------//
function approveOrder() public payable {
    // Check if the address belongs to a valid approver
    require(approvers[msg.sender]);

    // Check if this party has not already approved the ordercostdetails
    require(!confApprovers[msg.sender]);

    // Check if the amount of wei is more than the total_price
    require(msg.value > ordercostdetails[this].total_price);
    confApprovers[msg.sender] = true;
    numOfApprovers++;

    // Check if the required approvals have been made so that the order is confirmed
    if (numOfApprovers == ordercostdetails[this].reqApprovalNum) {
        confirmedOrder = true;
    }
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
  }

  //------------------------//
  // FLOW FUNCTIONS
  //------------------------//

  //-------------------------------------------------------------------------------------------//
  // This function is used by the logger account set in step 2.
  // This is the account of the IoT device that would record the temperature
  // of the product during the stages that the responsible party is a
  // transporter (in our case when transport_1 or transport_2 is the carrier)
  //-------------------------------------------------------------------------------------------//
  function updateProductStatus(uint currentTemp) public {
    // Require that the order is confirmed
    require(confirmedOrder);

    // Require that the sender's account matches the logger account
    require(orderpartydetails[this].dataLogger == msg.sender);

    // Require that the current responsible party is a transporter; to permit temperature logging
    require(transporters[ordertransferdetails[this].currentResponsibleParty]);

    // Compare the current temperature with the predefined limits and update the product status accordingly
    if (currentTemp> ordertransferdetails[this].maxAllowedTemp || currentTemp<
ordertransferdetails[this].minAllowedTemp) {
      ordertransferdetails[this].cargoStatus = "UNHEALTHY";
      temp_logs.push(currentTemp);
    } else {
      // keep temperature logs
      temp_logs.push(currentTemp);
    }
  }

  //-------------------------------------------------------------------------------------------//
  // This function is used during the transport process in order to check the
  // transition of the current responsible party to the next
  //-------------------------------------------------------------------------------------------//
  function handShake(address next) public {

    // Only the current responsible party can call this function for an active order
    require(ordertransferdetails[this].currentResponsibleParty == msg.sender);

    // Check that the next party is different from the current one
    require(ordertransferdetails[this].currentResponsibleParty != next);

    // Require that the order is confirmed
    require(confirmedOrder);

    // In order to perform a comparison between string values, convert them to hashes
    if (keccak256(ordertransferdetails[this].cargoStatus) == keccak256("HEALTHY")) {

      //-----------------------------------------------------//
      // If the status of the product is HEALTHY
      //-----------------------------------------------------//

      //-----------------------------------------------------//
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
        // Case 1: If the next party is the wholesaler
        //       the order is completed and everyone
        //       gets to be paid.
        //---------------------------------------------------------//
        if (next == orderpartydetails[this].wholesaler) {
          // The customs has already been paid

          // Pay each transporter and return their security deposits
          orderpartydetails[this].transport_1.transfer(ordercostdetails[this].transport_1_cost +
ordercostdetails[this].total_price);
          orderpartydetails[this].transport_2.transfer(ordercostdetails[this].transport_2_cost +
ordercostdetails[this].total_price);

          // The remaining amount goes to the producer
          producer.transfer(this.balance);
          confirmedOrder = false;
        }

        //---------------------------------------------------------//
        // Case 2: If the next party is the Customs
        //       the amount set in step 1 should
        //       be paid to the relevant account
        //---------------------------------------------------------//
        else if (next == orderpartydetails[this].customs) {
          // If it goes through customs pay the respective amount
          orderpartydetails[this].customs.transfer(ordercostdetails[this].customs_cost);
          ordertransferdetails[this].currentResponsibleParty = next;
        }

        //---------------------------------------------------------//
        // Case 3: Else; only pass responsibility at
        //       the next party
        //---------------------------------------------------------//
        else {
          ordertransferdetails[this].currentResponsibleParty = next;
        }

        //---------------------------------------------------------//
        // If the status of the product is HEALTHY
        //---------------------------------------------------------//

      } else {

        //-------------------------------------------------------------------------//
        // Case 1: Party transport_1 is responsible
        //       1. return money to wholesaler
        //       2. compensate the producer and the transport_2
        //-------------------------------------------------------------------------//
        if (ordertransferdetails[this].currentResponsibleParty == orderpartydetails[this].transport_1) {
          // Return the security deposit of the wholesaler
          orderpartydetails[this].wholesaler.transfer(ordercostdetails[this].total_price);

          // Compensate the transport_2 and return their security deposits
          orderpartydetails[this].transport_2.transfer(ordercostdetails[this].transport_2_cost +
ordercostdetails[this].total_price);
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
            // Transport_1 gets back the amount he would be paid from his security deposit and the money from
the unpaid customs' fee
            orderpartydetails[this].transport_1.transfer(ordercostdetails[this].transport_1_cost                +
ordercostdetails[this].customs_cost);

            // The remaining amount goes to the producer
            producer.transfer(this.balance);

            // Change order's status
            confirmedOrder = false;
        }

        //-------------------------------------------------------------------------//
        // Case 2: Party transport_2 is responsible
        //       1. return money to wholesaler
        //       2. compensate the producer and the transport_1
        //-------------------------------------------------------------------------//
        else if (ordertransferdetails[this].currentResponsibleParty == orderpartydetails[this].transport_2) {
            // Return the security deposit of the wholesaler
            orderpartydetails[this].wholesaler.transfer(ordercostdetails[this].total_price);

            // Compensate the transport_1 and return their security deposits
            orderpartydetails[this].transport_1.transfer(ordercostdetails[this].transport_1_cost                +
ordercostdetails[this].total_price);

            // Transport_2 gets back the amount he would be paid from his security deposit, Customs fee has been
paid
            orderpartydetails[this].transport_2.transfer(ordercostdetails[this].transport_2_cost);

            // The remaining amount goes to the producer
            producer.transfer(this.balance);

            // Change order's status
            confirmedOrder = false;
        }
    }
  }

  //--------------------------------//
  // AUXILIARY FUNCTIONS
  //--------------------------------//

  // Retrieve the amount of money (wei) retained by Order contract instance
  function getBalance() public view returns (uint) {
    return this.balance;
  }

  // Retrieve the address of the current responsible party
  function getCurrentResponsibleParty() public view returns (address) {
    return ordertransferdetails[this].currentResponsibleParty;
  }

  // Retrieve the number of remaining approvals required to confirm the order and activate it
  function getPendingApprvals() public view returns (uint) {
    return numOfApprovers - ordercostdetails[this].reqApprovalNum;
  }
```


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

```
    // Retrieve the current status of the product
    function getProductStatus() public view returns (string) {
        return ordertransferdetails[this].cargoStatus;
    }

    // Retrieve the order status
    function getOrderStatus() public view returns (string) {
        if (confirmedOrder) {
            return "ACTIVE";
        } else {
            return "INACTIVE";
        }
    }
}
```

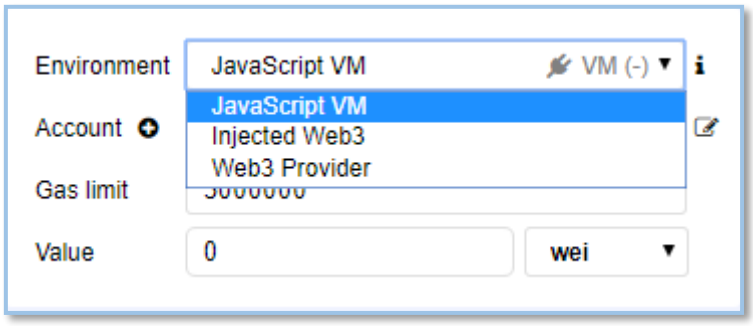

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

10.2 Εγχειρίδιο Χρήσης

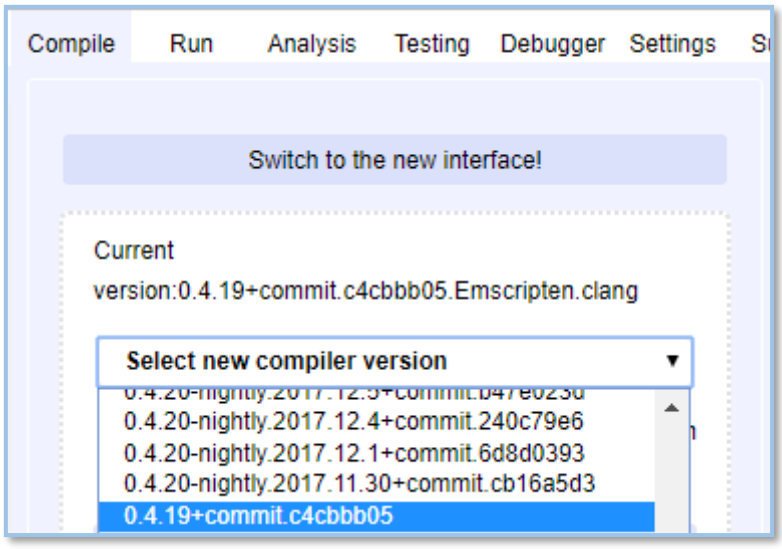
Βήμα 1: Ρυθμίσεις και δημιουργία λογαριασμών

Προσθέτουμε τον κώδικά της προηγούμενης ενότητας σε ένα αρχείο notepad και το αποθηκεύουμε με κατάληξη ".sol". Κατόπιν ανοίγουμε το αρχείο μας στον online IDE του remix.

Επιλέγουμε ως περιβάλλον εκτέλεσης το *JavaScript VM*.

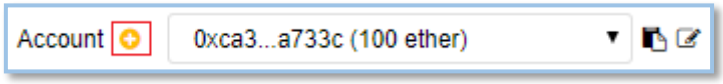


Στο tab του *Compiler* επιλέγουμε τον *"0.4.19+commit.c4cbbb05"* μεταγλωττιστή όπως φαίνεται στην εικόνα.



Επιλέγουμε *Auto compile*.

Επιστρέφουμε στο tab του *Run* και δημιουργούμε στο σύνολο έξι λογαριασμούς.



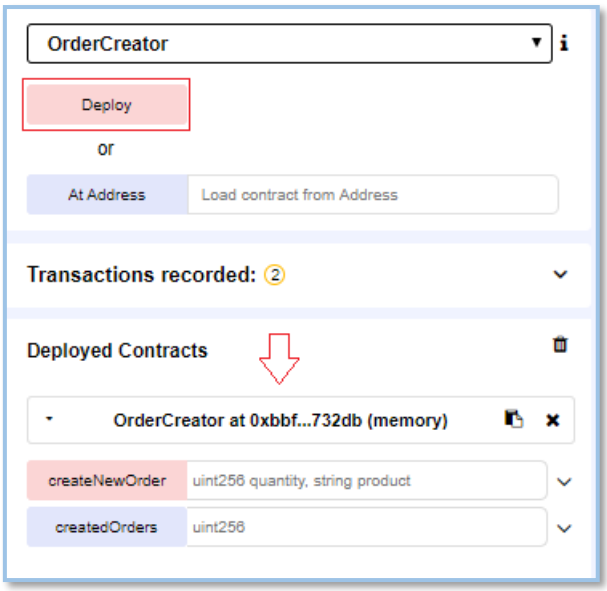
Στο κάτωθι πινακάκι υπάρχουν οι ρόλοι στην υλοποίηση μας και οι αντίστοιχες διευθύνσεις τους

Συμμετέχοντας	Διεύθυνση λογαριασμού
Παραγωγός	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
Πρώτος Μεταφορέας	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
Δεύτερος Μεταφορέας	0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db
Τελωνείο	0x583031d1113ad414f02576bd6afabfb302140225
Χονδρέμπορος	0xdd870fa1b7c4700f2bd7f44238821c26f7392148
IoT Συσκευή	0x8ae6a682b7c4700f2bd7f44238821c26fd10493c

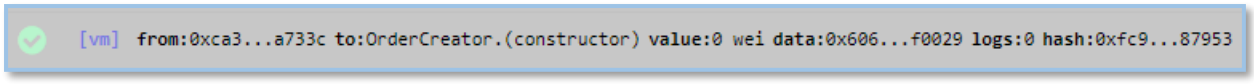
Πίνακας διευθύνσεων λογαριασμών συμμετεχόντων

Βήμα 2: Δημιουργία νέας παραγγελίας

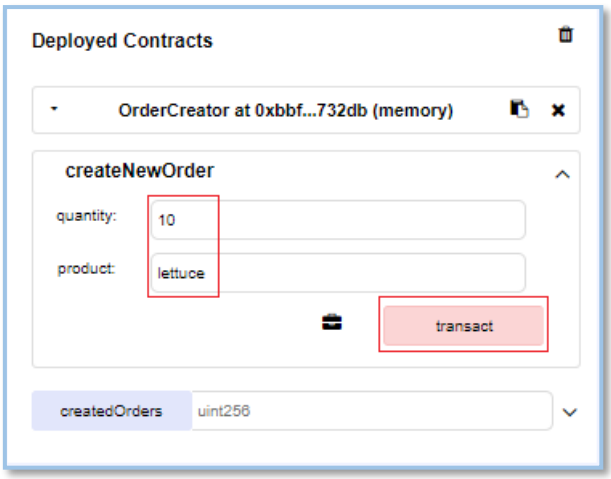
Επιλέγουμε το Smart Contract "OrderCreator" και πατάμε "Deploy".



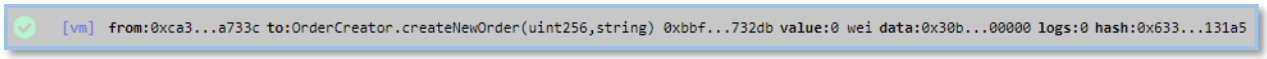
Παρατηρούμε ότι ένα νέο Smart Contract με όνομα "Order" δημιουργήθηκε επιτυχώς.



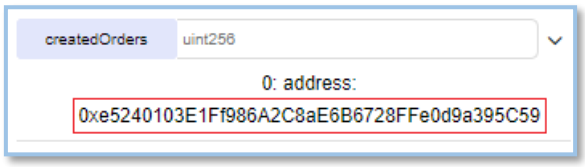
Αφού είμαστε ακόμα με το ρόλο του παραγωγού, μπορούμε να δημιουργήσουμε μία νέα παραγγελία, ανοίγουμε το tab "createNewOrder" συμπληρώνοντας το είδος του προϊόντος και την ποσότητα (πχ 10 τόνους μαρούλι) και πατούμε transact.



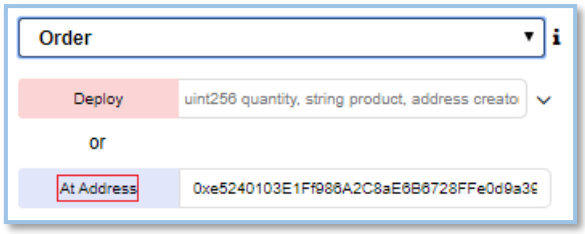
Ομοίως ελέγχουμε ότι η παραγγελία δημιουργήθηκε επιτυχώς.



Στην συνέχεια για να βρούμε τη μοναδική διεύθυνση της παραγγελίας που δημιουργήσαμε πατάμε "createdOrders".



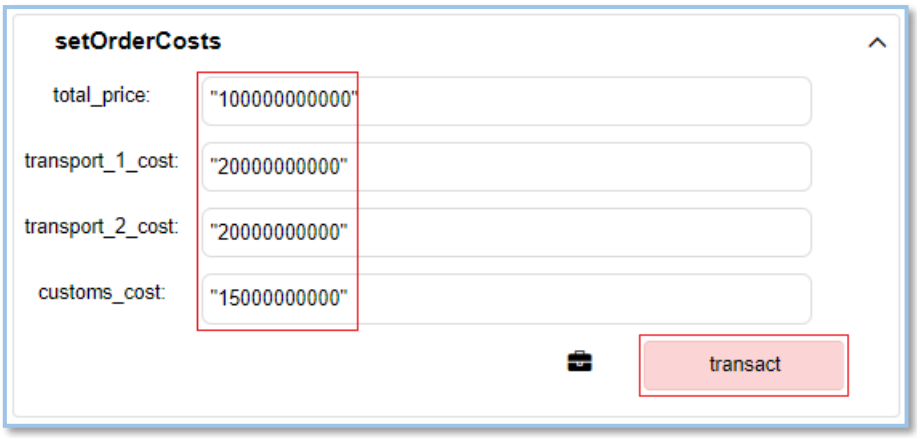
Με βάση αυτή τη διεύθυνση φορτώνουμε το Smart Contract της παραγγελίας.



Βήμα 3: Ορισμός κόστους παραγγελίας

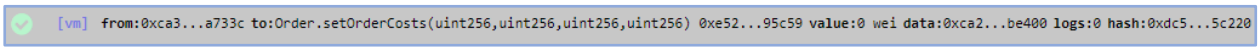
Με το λογαριασμό του παραγωγού πάντα, αφού αυτός είναι ο owner του συμβολαίου, ορίζουμε το συνολικό κόστος της παραγγελίας καθώς επίσης και τις προμήθειες των μεταφορέων και του τελωνείου. Το εναπομείναν ποσό αποτελεί την πληρωμή του παραγωγού, δηλαδή:

$$Producer_profit = total_price - (transport_1_cost + transport_2_cost + customs_cost)$$



Για το παράδειγμά μας βάζουμε το συνολικό κόστος ίσο με εκατό δισεκατομμύρια *wei*, αλλιώς 0.1 *szabo* ή 0.0001 *finney* ή 0.0000001 *ether*. Αντίστοιχα για τους άλλους τρεις συμμετέχοντες τα ποσά 20, 20 και 15 δισεκατομμύρια.

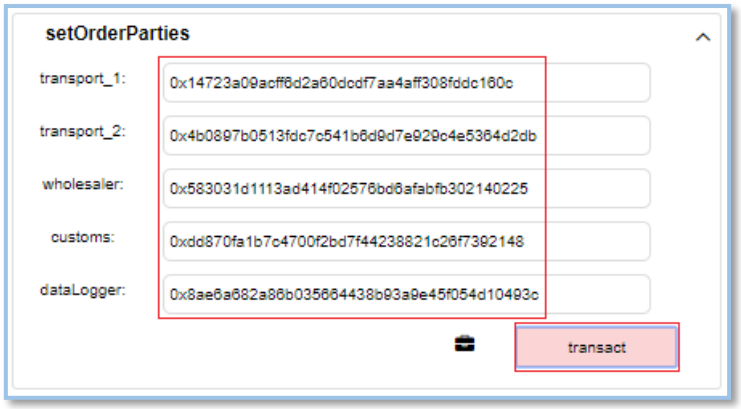
Επιβεβαίωση.



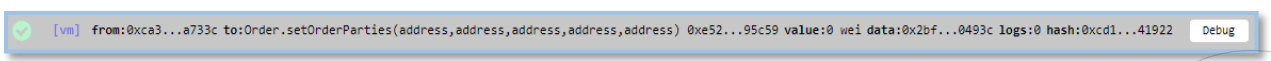
Βήμα 4: Καθορισμός ρόλων – συμμετεχόντων στην παραγγελία

Ο παραγωγός πριν ολοκληρώσει τη παραγγελίας πρέπει να συμπληρώσει την μοναδικές διευθύνσεις των συμμετεχόντων. Αυτό συμβαίνει για να περιορίσουμε την λειτουργία της εφαρμογής μόνο σε όσους είναι επιθυμητό και για να εξασφαλίσουμε την ομαλή μετάβαση των προϊόντων από τον ένα συμμετέχοντα στον άλλο.

Ανοίγουμε το tab "setOrderParties" και συμπληρώνουμε τις διευθύνσεις των δύο μεταφορέων, του τελωνίου και της συσκευής IoT που θα είναι υπεύθυνη να στέλνει συναλλαγές με θερμοκρασίες στο Smart Contract.



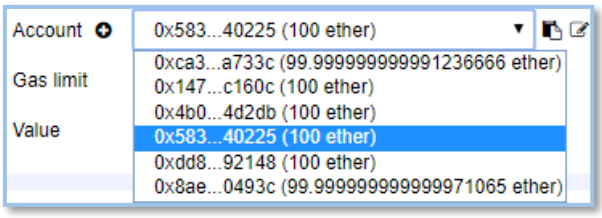
Πατάμε transact και επιβεβαιώνουμε.



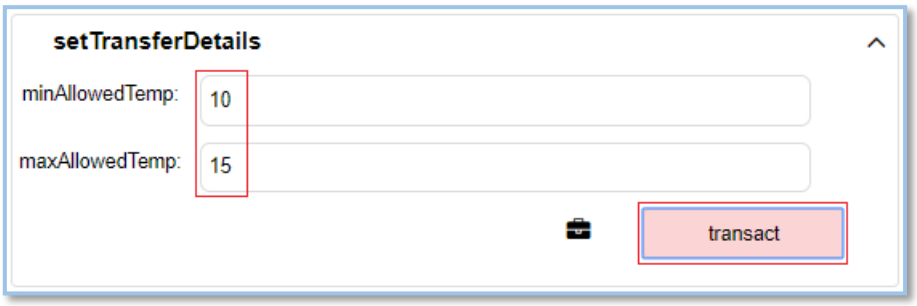
Βήμα 5: Καθορισμός ορίων θερμοκρασίας

Ο χονδρέμπορος, δηλαδή ο πελάτης όσον αφορά τον παραγωγό, θέτει τα όρια της θερμοκρασίας ώστε να διατηρηθεί το προϊόν φρέσκο και να μην αλλοιωθεί. Το όριο αυτό σε πραγματικό περιβάλλον θα μπορούσε να καθορίζεται με βάση υγειονομικές διατάξεις. Στο παράδειγμά μας, μόνο ο χονδρέμπορος έχει το δικαίωμα να θέσει τα όρια για να εξασφαλίσει τα συμφέροντά του.

Επιλέγουμε το λογαριασμό του χονδρεμπόρου



και εν συνεχεία ανοίγουμε το tab "setTransferDetails" θέτουμε τα επιτρεπτά όρια πχ. 10 - 15 βαθμούς κελσίου.

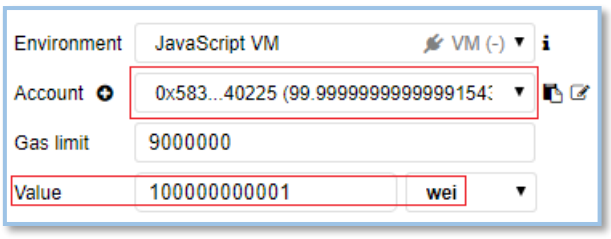


Πατάμε transact και επιβεβαιώνουμε.

Βήμα 6: Κατάθεση πληρωμής και εγγυήσεων και αποδοχή Έξυπνου Συμβολαίου

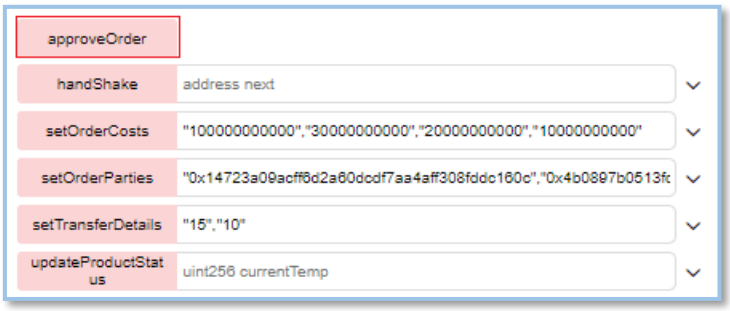
Ο χονδρέμπορος πρέπει να καταθέσει το σύνολο του κόστους (*total_price*) ώστε να καλυφθούν τα έξοδα μεταφοράς (*Producer_profit* + *transport_1_cost* + *transport_2_cost* + *customs_cost*) που είναι το οικονομικό όφελος των μεταφορέων, το κέρδος του παραγωγού και η πληρωμή των φόρων του εκτελωνισμού.

Από το λογαριασμό του χονδρεμπόρου, θέτουμε την τιμή *"100000000001"*. Καλύπτουμε το συνολικό ποσό συν ένα *wei*.

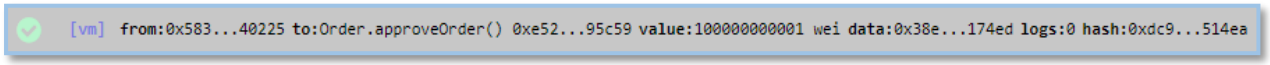


ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Πατάμε

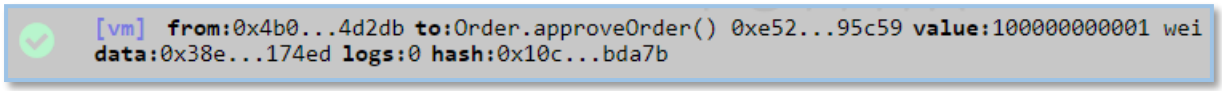


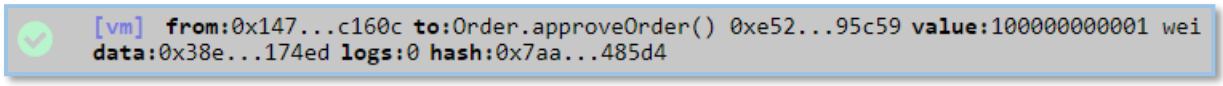
και επιβεβαιώνουμε



Ομοίως, θα επιβεβαιώσουν την παραγγελία (και κατ' επέκταση το Smart Contract) και οι δύο μεταφορείς με το ίδιο ποσό. Ο κώδικας υποχρεώνει να είναι το ποσό κατά την αποδοχή μεγαλύτερο από το *total_price* για να εξασφαλιστούν τα κόστη των συναλλαγών στο Ethereum.

Επιβεβαιώσεις



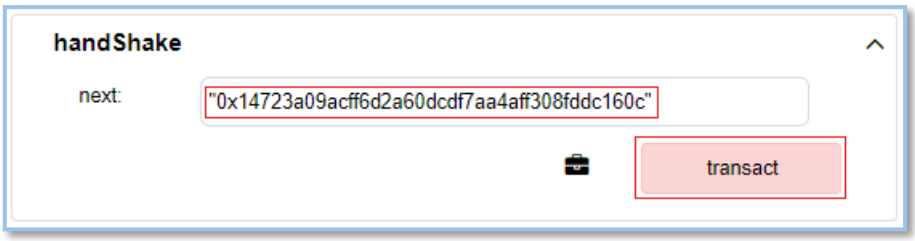


Αφού ολοκληρωθούν όλες οι επιβεβαιώσεις τότε το συμβόλαιο γίνεται ενεργό.

Βήμα 7: Παραλαβή από τον πρώτο μεταφορέα

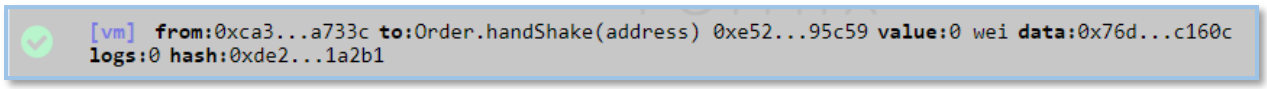
Ο παραγωγός μόλις ενεργοποιηθεί το συμβόλαιο, ειδοποιεί τον μεταφορέα να το παραλάβει. Κατά την παράδοση του εμπορεύματος ο παραγωγός περνά την κυριότητα στον μεταφορέα.

Με το λογαριασμό του παραγωγού, συμπληρώνουμε τη μοναδική διεύθυνση του πρώτου μεταφορέα και πατάμε "handshake"



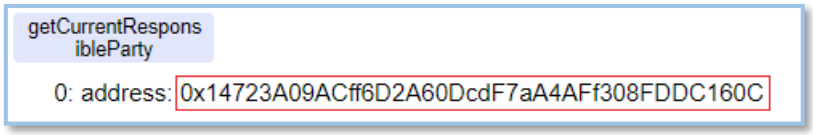
Επιβεβαιώνουμε.

ATHENS UNIVERSITY OF ECONOMICS & BUSINESS
ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



Σημειώνουμε ότι γίνεται έλεγχος κατά την μεταβίβαση της κυριότητας. Μόνο ο φορέας που έχει οριστεί εξαρχής ως επόμενος μπορεί κάθε φορά να παραλάβει το εμπόρευμα.

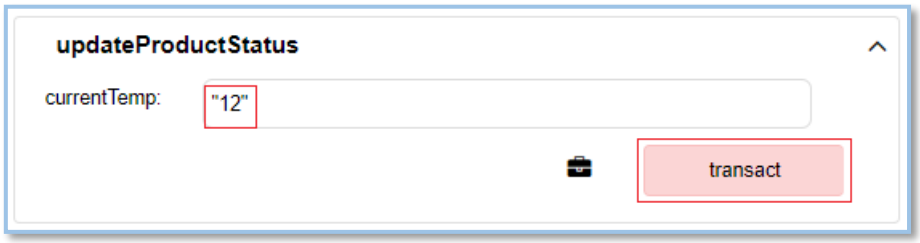
Μπορούμε να ελέγξουμε ότι είναι πλέον υπό την ευθύνη του πρώτου μεταφορέα.



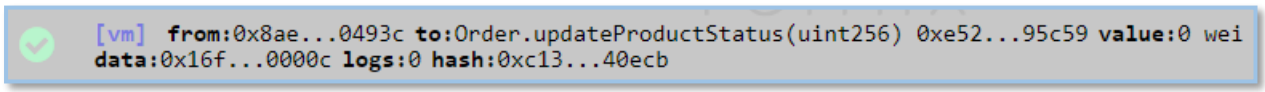
Βήμα 8: Καταγραφή θερμοκρασιών

Αφού γίνει το συμβόλαιο ενεργό και μόνο όταν το εμπόρευμα είναι υπό την ευθύνη μεταφορέα μπορεί η IoT συσκευή να στέλνει συναλλαγές στο Smart Contract με τιμές θερμοκρασίας. Όσο είναι στον παραγωγό και για το διάστημα που είναι στο τελωνείο δεν αποστέλλει τιμές.

Η IoT συσκευή έχει μοναδική διεύθυνση από την οποία αποστέλλονται οι συναλλαγές. Την επιλέγουμε και στο tab *"updateProductStatus"* θέτουμε μία τιμή, πχ 12 και πατάμε transact.



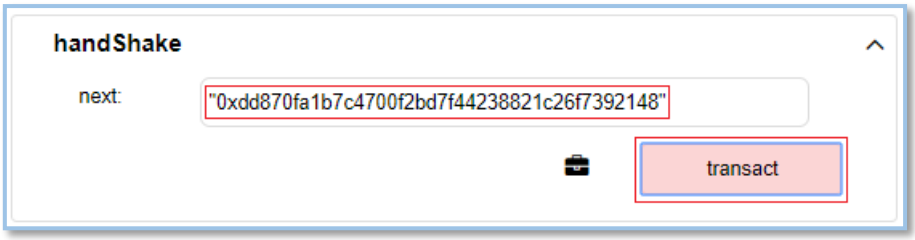
Επιβεβαιώνουμε ότι έγινε η καταγραφή.



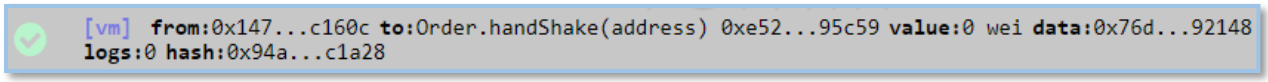
Βήμα 9: Άφιξη στο τελωνείο

Με το πέρασμα στο τελωνείο, αφενός μεταβιβάζεται το προϊόν και αφετέρου πληρώνεται αυτόματα ο φόρος για το εμπόρευμα.

Μεταβιβάζεται η κυριότητα από τον μεταφορέα στο τελωνείο.

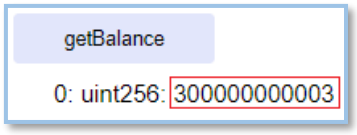


Επιβεβαιώνουμε.

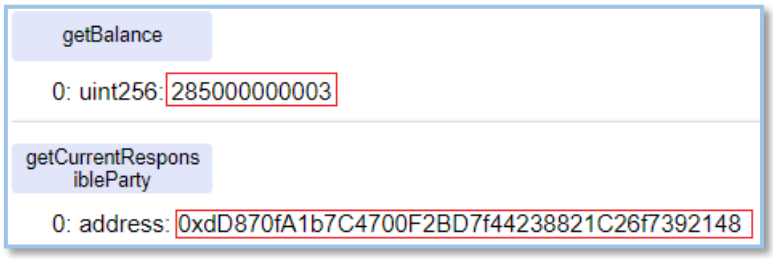


Παρατηρούμε από τη διαφορά του υπόλοιπου στα *wei* του Smart Contract ότι έχει πληρωθεί το τελωνείο.

Υπόλοιπο πριν

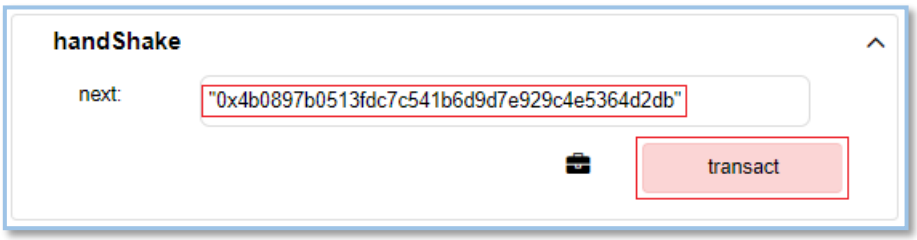


Και υπόλοιπο μετά.

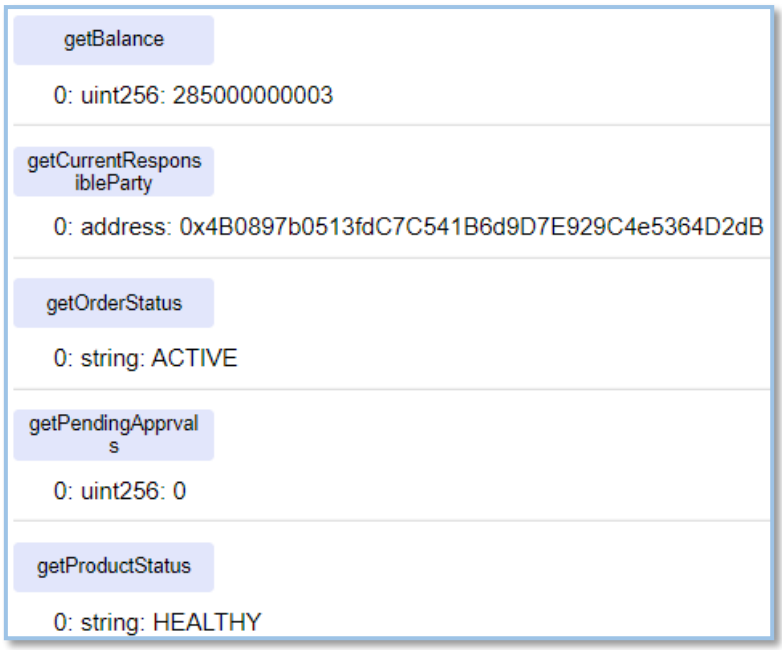


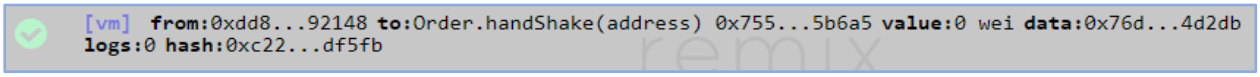
Βήμα 10: Μεταβίβαση στον δεύτερο μεταφορέα και παράδοση

Ομοίως πραγματοποιούμε τη μεταφορά από το τελωνείο στον μεταφορέα

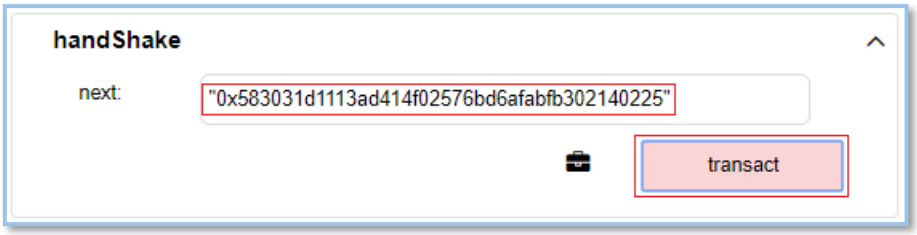


Επιβεβαίωση.

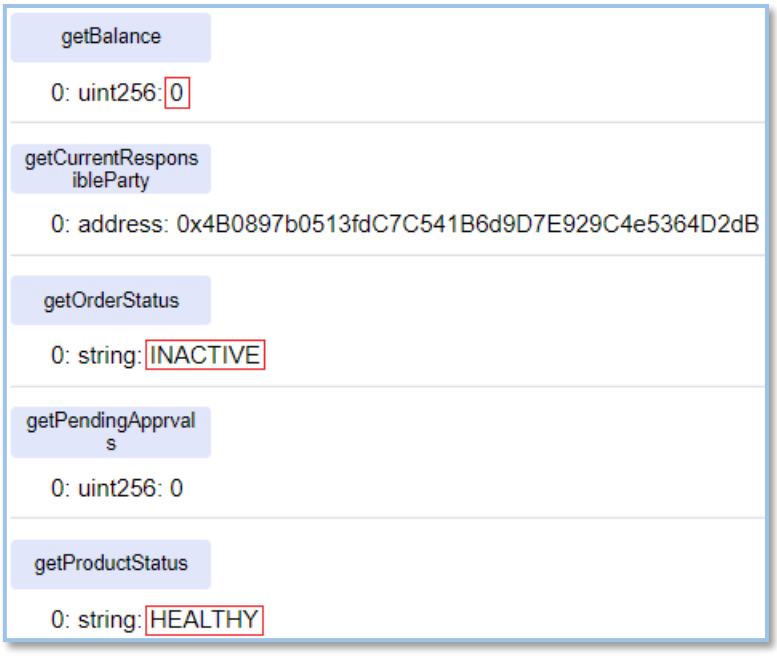


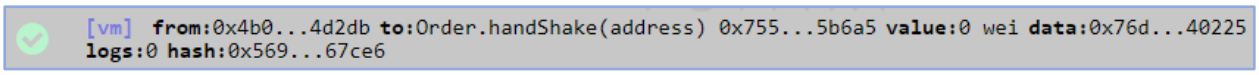


Τελευταία μεταβίβαση.



Επιβεβαίωση.

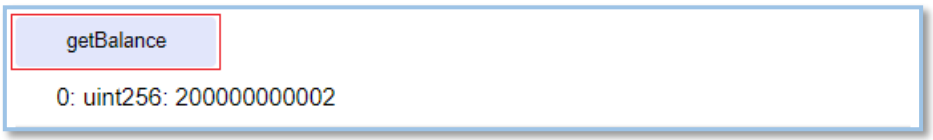




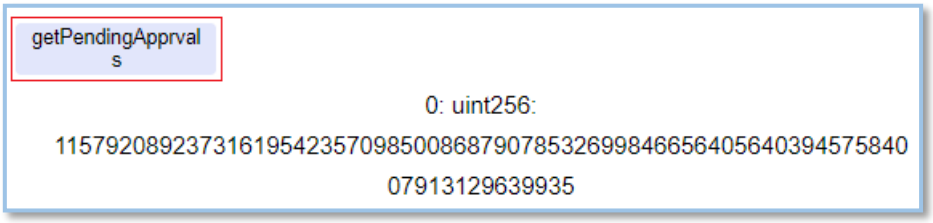
Παρατηρούμε ότι ο λογαριασμός άδειασε, αφού το Smart Contract ολοκληρώθηκε επιτυχώς. Τα χρήματα μοιράστηκαν ως προς τα ποσά που όρισε στην αρχή ο παραγωγός. Ο ίδιος έλαβε το κέρδος του συν τα υπόλοιπα *wei* που απέμειναν από τα επιπρόσθετα για την πραγματοποίηση συναλλαγών.

Βοηθητικές Συναρτήσεις

- Αν στο ενδιάμεσο θελήσουμε να ελέγξουμε το συνολικό ποσό που έχει κατατεθεί στο Smart Contract, μπορούμε να χρησιμοποιήσουμε το *"getBalance"*.



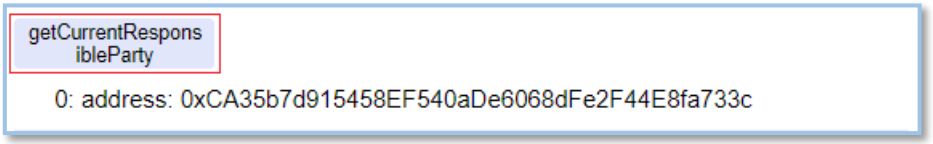
- Αν από την άλλη θελήσουμε να ελέγξουμε τον αριθμό επιβεβαιώσεων που υπολείπονται για την έγκριση του συμβολαίου, πατάμε το *"getPendingApprovals"*.



- Για να ελέγξουμε αν η κατάσταση της παραγγελίας είναι ενεργή, ανατρέχουμε στο *"getOrderStatus"*.



- Για να υπό ποιου την υπευθυνότητα βρίσκονται τα προϊόντα, μπορούμε να το δούμε με την *" getCurrentResponsibleParty"*.



- Η *"getProductStatus"* χρησιμεύει στην παρακολούθηση της κατάστασης των προϊόντων.

