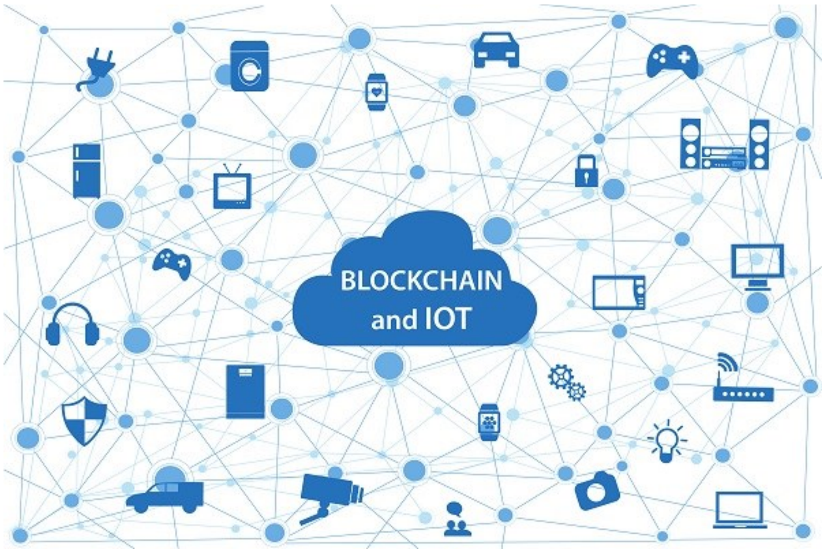
ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΜΕΛΕΤΗ ΤΗΣ ΧΡΗΣΗΣ BLOCKCHAIN ΚΑΙ ΕΞΥΠΝΩΝ ΣΥΜΒΟΛΑΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»



Του φοιτητή
Τζιμτζίμη Ελευθέριου
Αρ. Μητρώου: 20/2016

Επιβλέπων Καθηγητής
Χατζημίσιος Περικλής
Καθηγητής

Θεσσαλονίκη, Σεπτέμβριος 2022

Τίτλος Δ.Ε. Μελέτη της χρήσης Blockchain και Έξυπνων Συμβολαίων στο Διαδίκτυο των Πραγμάτων
Κωδικός Δ.Ε. …
Ονοματεπώνυμο φοιτητή Τζιμτζίμης Ελευθέριος
Ονοματεπώνυμο εισηγητή Περικλής Χατζημίσιος
Ημερομηνία ανάληψης Δ.Ε. …
Ημερομηνία περάτωσης Δ.Ε. …

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Στη μνήμη της γιαγιάς μου

Πρόλογος

Τις τελευταίες δεκαετίες, η ταχεία πρόοδος της τεχνολογίας Blockchain χρησιμοποιείται ολοένα και περισσότερο σε διάφορους τομείς. Η λύσεις που παρέχει η τεχνολογία Blockchain έχει μεγάλη σημασία για πολλούς τομείς και κλάδους της επιχειρηματικότητας και όχι μόνο. Μερικά χαρακτηριστικά που κάνουν αυτή την τεχνολογία τόσο σημαντική είναι η διαφάνεια, η ψηφιακή ελευθερία, η πολυλειτουργικότητα, η προηγμένη ασφάλεια και το χαμηλό της κόστος. Το δημόσιο Blockchain παρέχει διαφάνεια λόγω της φύσης του. Αυτός ο τύπος Blockchain είναι πολύ χρήσιμος για τη βελτίωση πολλών πτυχών της σημερινής μας κοινωνίας, συμπεριλαμβανομένης της διεξαγωγής ηλεκτρονικών εκλογών. Η χρήση της τεχνολογίας Blockchain, παρέχει τον έλεγχο της πραγματικής ψηφιακής ελευθερίας του χρήστη. Η εν λόγω τεχνολογία δεν περιορίζεται μόνο στον χρηματοοικονομικό τομέα, καθώς μπορεί να χρησιμοποιηθεί σχεδόν σε κάθε τομέα και αγορά, συμπεριλαμβανομένων των εμπορικών οικονομικών, των τραπεζών, της κυβέρνησης, της υγειονομικής περίθαλψης, της εκπαίδευσης κ.ο.κ. Επιπλέον, τεχνολογίες όπως το "Διαδίκτυο των Πραγμάτων (Internet of Things – IoT)" υιοθετούνται ολοένα και περισσότερο δείχνοντας μια μελλοντική τάση καθιέρωσής τους. Ως εκ τούτου είναι σημαντικό να μελετηθεί η χρήση του Blockchain και των έξυπνων συμβολαίων σε εφαρμογές IoT και να μελετηθούν τα πλεονεκτήματα του συνδυασμού αυτών των δύο νέων και πολλά υποσχόμενων τεχνολογιών.

Περίληψη

Ένα Blockchain είναι ουσιαστικά μια κατανεμημένη βάση δεδομένων με αρχεία ή ένα δημόσιο βιβλίο όλων των συναλλαγών ή ψηφιακών γεγονότων που έχουν εκτελεστεί και μοιραστεί μεταξύ των συμμετεχόντων μερών. Κάθε συναλλαγή στο δημόσιο βιβλίο επαληθεύεται με τη συναίνεση της πλειοψηφίας των συμμετεχόντων στο σύστημα. Μόλις εισαχθούν, οι πληροφορίες δεν μπορούν ποτέ να διαγραφούν. Το Blockchain περιέχει ένα συγκεκριμένο και επαληθεύσιμο αρχείο κάθε συναλλαγής που έγινε ποτέ. Η συγκεκριμένη εργασία μελετά το πλαίσιο της αλληλεπίδρασης της τεχνολογίας του Blockchain με την τεχνολογία του Ίντερνετ των Πραγμάτων και εστιάζει στο περιβάλλον των έξυπνων πόλεων. Οι σύνθετες αλυσίδες εφοδιασμού είναι απαραίτητες για τις βιομηχανίες και τις επιχειρήσεις. Μια αλυσίδα εφοδιασμού περιγράφεται ως μια συνεργασία περισσότερων από δύο οργανισμών που ελέγχουν τη ροή των εμπορευμάτων, των υπηρεσιών κοινής ωφέλειας, της οικονομίας, της γνώσης από μια πηγή στον αντίστοιχο καταναλωτή. Υπάρχει ζήτηση για έναν διαφανή, ιχνηλάσιμο, μηχανισμό εφοδιαστικής αλυσίδας που να προλαμβάνει όλες τις πληροφορίες, από τις πρώτες ύλες έως τις λεπτομέρειες κατασκευής των αλιευτικών προϊόντων, καθώς και την ιχνηλασιμότητα από το εργοστάσιο στον καταναλωτή. Έτσι, η συγκεκριμένη διπλωματική εργασία αποτελείται από διάφορα περιβάλλοντα, κάτι το οποίο χαρακτηρίζει και την πολυδιάσταση πορεία της τεχνολογίας Blockchain, καθώς περιγράφει και αναλύει την τεχνολογία Blockchain, τις έξυπνες συμβάσεις και τις πλατφόρμες Blockchain για το Ίντερνετ των Πραγμάτων, ενώ μέσω της βιβλιογραφικής ανασκόπησης αναλύει διεξοδικά το πεδίο των τεχνολογιών Blockchain και Έξυπνων Συμβολαίων στο Internet of Things.

« Study of the use of Blockchain and Smart Contracts in the Internet of Things»

«Eleftherios Tzimtzimis»

Abstract

A Blockchain is essentially a distributed database with files or a public book of all transactions or digital events that have been executed and shared between the participating parties. Every transaction in the public book is verified with the consent of the majority of the participants in the system. Once entered, the information cannot be deleted by any chance. The Blockchain contains a specific and verifiable record of every transaction ever made. This dissertation examines the context of the interaction of Blockchain technology with the technology of the Internet of Things and focuses on the environment of smart cities. Complex supply chains are essential for industries and businesses. A supply chain is described as a collaboration of more than two organizations that control the flow of goods, utilities, the economy, knowledge from one source to the respective consumer. There is a demand for a transparent, traceable, supply chain mechanism that prevents all information, from raw materials to manufacturing details of fishery products, as well as traceability from the factory to the consumer. Thus, this dissertation consists of various environments, which characterizes the multidimensional course of Blockchain technology, as it describes and analyzes Blockchain technology, smart contracts and Blockchain platforms for the Internet of Things, while through the literature review analyzes the field of Blockchain and Smart Contracts technologies on the Internet of Things.

.

Ευχαριστίες

Η ολοκλήρωση της παρούσας εργασίας θα ήταν αδύνατη χωρίς την πολύτιμη βοήθεια του καθηγητή μου Περικλή Χατζημίσιου τον οποίο θα ήθελα να ευχαριστήσω θερμά για την εμπιστοσύνη που μου έδειξε, και για την καθοδήγηση που μου έδωσε κατά τη διάρκεια υλοποίησης της. Επίσης, θα ήθελα να ευχαριστήσω την οικογένειά μου η οποία με στήριξε τις σπουδές μου με διάφορους τρόπους, φροντίζοντας για το καλύτερο δυνατό αποτέλεσμα.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

Blockchain	BC
Blockchain for Internet of Thongs	BIoT
Byzantine Fault-Tolerant	BFT
Cyber-Physical Systems	CPS
Directed acyclic graph	DAG
Electronic Health Records	EHR
Industrial IoT	IIoT
Internet of Energy	IoE
Internet of Thongs	IoT
practical Byzantine Fault Tolerance	pBFT
Proof of work	PoW
Proof-of-Capacity	PoC
Proof-of-Stake	PoS
Representative Transport Protocol	REST
Secure Sockets Layer	SSL
Virtual Machine	VM
Ανανεώσιμες Πηγές Ενέργειας	ΑΠΕ

Κεφάλαιο 1ο: Η Τεχνολογία Blockchain

1.1 Εισαγωγή

Η συμμετοχή ενός πιστωτικού τρίτου μέρους όπως είναι για παράδειγμα μία τράπεζα απαιτείται στις συναλλαγές που διεξάγονται σε κεντρική μορφή συνήθως μεταξύ των μερών στα υπάρχοντα συστήματα. Βέβαια μέσα από αυτό θα μπορούσαν να προκύψουν ζητήματα ασφαλείας ή υψηλά τέλη συναλλαγών και για να αντιμετωπιστούν αυτού του είδους τα προβλήματα δημιουργήθηκε η τεχνολογία blockchain η οποία επιτρέπει σε πιστωτικές οντότητες να αλληλοεπιδρούν κατανεμημένα χωρίς να εμπλέκεται κάποιο πιστωτικό τρίτο μέρος. Η τεχνολογία blockchain ορίζεται ως μία βάση δεδομένων στην οποία καταγράφονται όλες οι συναλλαγές που συμβαίνουν σε ένα δίκτυο. Η πρώτη φορά που εισήχθη το blockchain ήταν για το Bitcoin το οποίο αποτελεί σύστημα ψηφιακής πληρωμής, ωστόσο ακολούθως χρησιμοποιήθηκε για να αναπτυχθεί ένα ευρύ φάσμα αποκεντρωμένων εφαρμογών. Τα έξυπνα συμβόλαια αποτελούν ελκυστική εφαρμογή που μπορούν να αναπτυχθούν πάνω από το blockchain.

Η έξυπνη σύμβαση αποτελεί εκτελέσιμο κώδικα που τρέχει στο blockchain με σκοπό να διευκολύνει, να εκτελέσει και να επιβάλει τους όρους μιας συμφωνίας ανάμεσα στα μη πιστωτικά μέρη. Είναι επίσης δυνατόν να θεωρηθεί ως σύστημα που απελευθερώνει ψηφιακά στοιχεία περιουσίας σε όλα ή σε κάποια από τα μέρη που εμπλέκονται αφού ληφθούν υπόψη οι κανόνες που έχουν προκαθοριστεί (Buterin, 2017).

Οι έξυπνες συμβάσεις δεν χρειάζεται να βασιστούν σε κάποιο αξιόπιστο τρίτο μέρος για να λειτουργήσουν έχοντας ως αποτέλεσμα το χαμηλό κόστος συναλλαγής, σε αντίθεση με τα παραδοσιακά συμβόλαια. Για να αναπτυχθούν έξυπνα συμβόλαια έχουν δημιουργηθεί διάφορες πλατφόρμες blockchain που μπορούν να χρησιμοποιηθούν και το Ethereum είναι η πιο συνηθισμένη. Η πλατφόρμα αυτή χρησιμοποιείται συχνότερα καθώς η γλώσσα της υποστηρίζει το γνωστό Tuning - πληρότητας το οποίο επιτρέπει να δημιουργηθούν πιο προηγμένες και προσαρμοσμένες συμβάσεις. Οι έξυπνες συμβάσεις είναι δυνατόν να εφαρμοστούν σε πολλών ειδών εφαρμογές.

1.2 Εισαγωγή στο Blockchain

Ως blockchain ορίζεται μία κατανεμημένη βάση δεδομένων η οποία αποτελείται από αρχεία ή ένα δημόσιο βιβλίο που συμπεριλαμβάνει όλες τις συναλλαγές ή τα ψηφιακά γεγονότα που έχουν λάβει χώρα και έχουν διαμοιραστεί ανάμεσα στα εμπλεκόμενα μέρη. Η τεχνολογία blockchain δεν είναι αμφιλεγόμενη καθώς έχει λειτουργήσει σωστά στη διάρκεια των χρόνων ενώ λαμβάνει χώρα τόσο σε οικονομικές όσο και μη οικονομικές εφαρμογές ανά τον κόσμο. Προσφάτως ο Marc Andreessen έκρινε το blockchain ως τη σημαντικότερη εφεύρεση του διαδικτύου. Ο Johann Palychata της BNP Paribas ανέφερε ότι για να λειτουργήσει το Bitcoin χρειάζεται ένα λογισμικό που να μοιάζει με τον ατμό και να μπορεί να μεταμορφώσει και τον κόσμο (Borenstein, 2016).

Η ψηφιακή οικονομία του σήμερα είναι βασισμένη στην εξάρτηση της αξιοπιστίας μιας συγκεκριμένης αρχής. Όλες οι ηλεκτρονικές συναλλαγές είναι βασισμένες στην εμπιστοσύνη και την αλήθεια κάποιου ο οποίος μπορεί να παρέχει υπηρεσίες ηλεκτρονικού ταχυδρομείου που μπορεί για παράδειγμα να μας πει ότι το e-mail μας παραδόθηκε, ότι κάποιο ψηφιακό πιστοποιητικό είναι άξιο εμπιστοσύνης, ή μπορεί κάποιο μέσο κοινωνικής δικτύωσης όπως είναι το Facebook να μας ενημερώνει ότι οι αναρτήσεις που κάνουμε σχετικά με τη ζωή μας είναι προσβάσιμες μόνο σε φίλους μας ή μπορεί να είναι και μία τράπεζα που μας λέει πως τα χρήματά μας έχουν παραδοθεί στους οικείους μας που μπορεί να βρίσκονται μακριά με αξιόπιστο τρόπο. Πραγματικότητα αποτελεί ότι πλέον η ζωή μας βασίζεται στον ψηφιακό κόσμο και σε μία τρίτη οντότητα στην οποία έχουμε εμπιστευτεί την ασφάλεια και την ιδιωτικότητα των ψηφιακών μας στοιχείων. Γεγονός αποτελεί επίσης ότι οι προσωπικές μας πληροφορίες μπορεί να κλαπούν να χειραγωγηθούν ή να διακυβευθούν.

Αυτό είναι και το κρίσιμο σημείο πού εισέρχεται η τεχνολογία blockchain καθώς αυτή μπορεί να επιτρέψει μία κατανεμημένη συναίνεση στην οποία όλες οι ηλεκτρονικές συναλλαγές που περιλαμβάνουν ψηφιακά περιουσιακά στοιχεία είναι δυνατόν να επαληθευτούν οποιαδήποτε στιγμή στο μέλλον. Αυτό συμβαίνει χωρίς να διακυβεύονται τα ψηφιακά περιουσιακά στοιχεία των εμπλεκομένων ατόμων. Δύο πολύ σημαντικά χαρακτηριστικά της τεχνολογίας blockchain είναι η συναίνεση και ανωνυμία. σύμφωνα με τους Crosby et al. (2016) έμφαση δίνεται στις δυσκολίες που αντιμετωπίζουν όλοι οι κλάδοι στη σημερινή ψηφιακή οικονομία εξαιτίας της εμφάνισης της τεχνολογίας blockchain. Η νέα αυτή τεχνολογία μπορεί να γίνει ο κινητήριος μοχλός ανάπτυξης της ψηφιακής οικονομίας την οποία χρησιμοποιούμε όλο και περισσότερο για να ψωνίσουμε ηλεκτρονικά ή να μοιραστούμε τα προσωπικά μας δεδομένα. Αναμφισβήτητο είναι το γεγονός ότι σε αυτό το χώρο που υπάρχουν σημαντικές ευκαιρίες η επανάσταση μόλις ξεκινάει. Και οι Crosby et al. (2016) δίνουν έμφαση σε ορισμένες εφαρμογές blockchain και πιο συγκεκριμένα ασχολούνται με το τομέα των συμβολαιογράφων των ασφαλίσεων των ιδιωτικών προστασιών κ.λπ.

1.3 Η Έννοια του Blockchain

Το blockchain χαρακτηρίζεται διαφορετικά ως αλυσίδα από μπλοκ και αποτελεί έναν κατάλογο αρχείων που αναπτύσσεται τα οποία ονομάζονται μπλοκ και συνδέονται μέσω της κρυπτογραφίας. Κάθε ένα από τα μπλοκ διαθέτει έναν κρυπτογραφικό κατακερματισμό του προηγούμενου μπλοκ, ένα χρονικό σήμα καθώς και δεδομένα συναλλαγής (Brito & Castillo, 2013; Iansiti & Lakhani, 2017). Το blockchain σχεδιάστηκε για να είναι ανθεκτικό την τροποποίηση δεδομένων και επί της ουσίας αποτελεί ανοιχτό κατανεμημένο λογιστικό βιβλίο στο οποίο καταγράφονται οι συναλλαγές ανάμεσα σε δύο μέρη με τρόπο που επαληθεύεται (Iansiti & Lakhani, 2017). Για να μπορέσει κάποιος να το χρησιμοποιήσει σαν κατανεμημένο λογιστικό βιβλίο το blockchain διαχειρίζεται ένα δίκτυο το λεγόμενο peer to peer το οποίο δίνει τη δυνατότητα στους υπολογιστές που ανήκουν σε αυτόν να μοιράζονται ισόποσα τους πόρους και να ακολουθούν το πρωτόκολλο επικοινωνίας μεταξύ των κόμβων με σκοπό την επικύρωση των νέων μπλοκ. Εάν καταγραφούν δεδομένα σε οποιοδήποτε δεδομένο μπλοκ τότε δεν είναι δυνατόν να υπάρξει τροποποίησή τους χωρίς να αλλοιωθούν τα επόμενα μπλοκ γεγονός που απαιτεί η συναίνεση της πλειοψηφίας του δικτύου. Αν και υπάρχει περίπτωση να συμβούν αλλοιώσεις στα αρχεία μπλοκ τα blockchain θεωρούνται ασφαλή εξαιτίας του σχεδιασμού τους και αποτελούν παράδειγμα ενός κατανεμημένου συστήματος υπολογιστών που έχουν υψηλή ανοχή σε βλάβες (Raval, 2016).

Το blockchain χαρακτηρίζεται διαφορετικά ως αλυσίδα από μπλοκ και αποτελεί έναν κατάλογο αρχείων που αναπτύσσεται τα οποία ονομάζονται μπλοκ και συνδέονται μέσω της κρυπτογραφίας. Κάθε ένα από τα μπλοκ διαθέτει έναν κρυπτογραφικό κατακερματισμό του προηγούμενου μπλοκ, ένα χρονικό σήμα καθώς και δεδομένα συναλλαγής (Brito & Castillo, 2013; Iansiti & Lakhani, 2017). Το blockchain σχεδιάστηκε για να είναι ανθεκτικό την τροποποίηση δεδομένων και επί της ουσίας αποτελεί ανοιχτό κατανεμημένο λογιστικό βιβλίο στο οποίο καταγράφονται οι συναλλαγές ανάμεσα σε δύο μέρη με τρόπο που επαληθεύεται (Iansiti & Lakhani, 2017). Για να μπορέσει κάποιος να το χρησιμοποιήσει σαν κατανεμημένο λογιστικό βιβλίο το blockchain διαχειρίζεται ένα δίκτυο το λεγόμενο peer to peer το οποίο δίνει τη δυνατότητα στους υπολογιστές που ανήκουν σε αυτόν να μοιράζονται ισόποσα τους πόρους και να ακολουθούν το πρωτόκολλο επικοινωνίας μεταξύ των κόμβων με σκοπό την επικύρωση των νέων μπλοκ. Εάν καταγραφούν δεδομένα σε οποιοδήποτε δεδομένο μπλοκ τότε δεν είναι δυνατόν

να υπάρξει τροποποίησή τους χωρίς να αλλοιωθούν τα επόμενα μπλοκ γεγονός που απαιτεί η συναίνεση της πλειοψηφίας του δικτύου. Αν και υπάρχει περίπτωση να συμβούν αλλοιώσεις στα αρχεία μπλοκ τα blockchain θεωρούνται ασφαλή εξαιτίας του σχεδιασμού τους και αποτελούν παράδειγμα ενός κατανεμημένου συστήματος υπολογιστών που έχουν υψηλή ανοχή σε βλάβες (Raval, 2016).

1.3.1. Ιστορία των Blockchain

Το 1991 η Stuart Haber και W. Scott Stornetta περιέγραψαν για πρώτη φορά μία κρυπτογραφικά ασφαλισμένη αλυσίδα μπλοκ (Haber & Stornetta, 1990; Iansiti & Lakhani, 2017). Οι δύο μελετητές είχαν σκοπό να βάλουν σε λειτουργία ένα σύστημα εντός του οποίου δεν θα μπορούσε να συμβεί παραβίαση του χρόνου σημάτων των εγγράφων. Το 1992 η τάδε εισήγαγαν το Merkle Tree στο σχεδιασμό τους το οποίο είναι ένα δέντρο κατακερματισμού όπου κάθε κόμβος φύλλων έχει την ετικέτα του κατακερματισμού ενός μπλοκ δεδομένων και κάθε κόμβος που δεν αποτελεί φύλλο επισημαίνεται με τον κρυπτογραφικό κατακερματισμό των ετικετών των κόμβων που ανήκουν σε αυτόν. Το γεγονός αυτό βοήθησε στη βελτίωση της αποτελεσματικότητας του σχεδιασμού επιτρέποντας έτσι τη συλλογή πολλών πιστοποιητικών εγγράφων σε ένα μπλοκ (Bayer et al., 1993; Iansiti & Lakhani, 2017).

Το 2008 έγινε για πρώτη φορά αντιληπτό το πρώτο blockchain από ένα άτομο ή από μία ομάδα ατόμων γνωστό και ως Satoshi Nakamoto. Ο Nakamoto ή η ομάδα ατόμων με το όνομα Nakamoto βοήθησε στη βελτίωση του σχεδιασμού της προσπάθειάς τους χρησιμοποιώντας μία μέθοδο απόδειξης εργασίας χρονοσήμανσης (Hashcash) χωρίς να είναι απαραίτητη η υπογραφή της από ένα συμβαλλόμενο μέρος ενώ μειώθηκε η ταχύτητα με την οποία τα μπλοκ προστίθενται στην αλυσίδα. Τον επόμενο χρόνο εφαρμόστηκε ο σχεδιασμός από τον Nakamoto ως βασικό συστατικό του Bitcoin κρυπτονομισματος το οποίο μπορεί να χρησιμοποιηθεί ως ένας δημόσιος λογιστικός κατάλογος που αφορά τις συναλλαγές τους στο δίκτυο (Iansiti & Lakhani, 2017).

Τα 20 GB έφτασε το μέγεθος του αρχείου μπλοκ αλυσίδων Bitcoin τον Αύγουστο του 2014 εντός του οποίου περιέχουν τα αρχεία όλων των συναλλαγών που έχουν πραγματοποιηθεί στο δίκτυο (Chuen, 2015). Τον Ιανουάριο του 2015 σημειώθηκε αύξηση με το μέγεθος να φτάνει σχεδόν τα 30 GB ενώ στο διάστημα μεταξύ Ιανουαρίου 2016 έως Ιανουάριο 2017 το blockchain Bitcoin αυξήθηκε από τα 50 και MB στα 100 GB. Σε αρχική έρευνα του Satoshi Nakamoto οι λέξεις μπλοκ και αλυσίδα χρησιμοποιήθηκαν χωριστά όμως στο τέλος έγιναν γνωστά σαν μία λέξη, ως blockchain.

Πολλών ειδών συμβάσεις λειτουργούν σε ένα Blockchain, όπως είναι τα τιμολόγια που εξοφλούνται όταν φτάνει μια αποστολή ή όταν μοιράζονται πιστοποιητικά που αποστέλλονται σε μετόχους εάν τα κέρδη τους φτάσουν σε συγκεκριμένο αριθμό. Όλα αυτά για να λειτουργήσουν απαιτούν την ύπαρξη μιας αφηρημένης μηχανής που χρησιμοποιείται με σκοπό να μελετηθούν προβλήματα λήψης απόφασης εκτός της αλυσίδας με στόχο την πρόσβαση σε εξωτερικά δεδομένα ή γεγονότα που σχετίζονται με συνθήκες χρόνου ή αγοράς όταν χρειάζεται να αλληλεπιδράσουν με το Blockchain (Godfrey-Welch et al., 2018).

Μια πολυεθνική εταιρεία επαγγελματικών υπηρεσιών ονόματι Accenture η οποία προσφέρει υπηρεσίες σε ζητήματα που αφορούν στρατηγική, συμβουλευτική, ψηφιακή τεχνολογία και επιχειρήσεις αναφέρει ότι με βάση την εφαρμογή της θεωρίας διάδοσης των καινοτομιών, τα Blockchains έφθασαν το 2016 σε ποσοστό 13,5% σε χρηματοπιστωτικές υπηρεσίες φθάνοντας με αυτό τον τρόπο στις πρώτες θέσεις των επιχειρήσεων που υιοθέτησαν την εφαρμογή του (Godfrey-Welch et al., 2018). Χάρη στην πρωτοβουλία του Επιμελητηρίου Ψηφιακού Εμπορίου, οι εμπορικές ομάδες του κλάδου δημιούργηαν το Παγκόσμιο Φόρουμ του Blockchain to 2016.

1.3.2. Δομή των Blockchain

Ως Blockchain θεωρείται ο αποκεντρωμένος, κατανεμημένος και δημόσιος λογιστικός κατάλογος ο οποίος χρησιμοποιείται με σκοπό την καταγραφή συναλλαγών μεταξύ υπολογιστών ούτως ώστε κάθε εγγραφή που εμπλέκεται να μην έχει τη δυνατότητα αναδρομικής τροποποίησης χωρίς την αλλαγή και των επόμενων μπλοκ (Armstrong, 2016). Η κατάσταση αυτή επιτρέπει στα εμπλεκόμενα μέλη να επαληθεύουν και να ελέγχουν τις συναλλαγές ελεύθερα και ανέξοδα (Catalini & Gans, 2016).

Μια βάση δεδομένων Blockchain είναι αυτόνομα διαχειρίσιμη κάνοντας χρήση του δικτύου peer to peer και ενός κατανεμημένου διακομιστή χρονοσημάνσεων. Μια μαζική συνεργασία η οποία βασίζεται στο συλλογικό συμφέρον πιστοποιεί τα παραπάνω (Tapscott & Tapscott, 2016). Ο σχεδιασμός αυτός μπορεί να διευκολύνει τη σκληρή ροή εργασιών κατά την οποία η αβεβαιότητα των εμπλεκόμενων ατόμων αναφορικά με την προστασία των δεδομένων τους δεν υπάρχει πλέον.

1.3.3. Η Έννοια των Μπλοκ

Χάρη στα μπλοκ διατηρούνται ομάδες έγκυρων κατακερματισμένων και κωδικοποιημένων σε Merkle tree συναλλαγών (Iansiti & Lakhani, 2017). Σε κάθε μπλοκ περιλαμβάνεται ο κρυπτογραφικός κατακερματισμός του προηγούμενου μπλοκ στο Blockchain και έτσι τα δύο μπλοκ συνδέονται αποτελώντας μια αλυσίδα συνδεδεμένων μπλοκ. Η διαδικασία αυτή που επαναλαμβάνεται επιβεβαιώνει την ακεραιότητα του προηγούμενου μπλοκ διαδοχικά, μέχρι το αρχικό μπλοκ γένεσης (Bhaskar & Chuen, 2015).

Είναι πιθανό χωριστά μπλοκ να μπορούν να παράγονται ταυτόχρονα. Κάθε Blockchain διαθέτει, εκτός από ένα ασφαλές ιστορικό, και έναν συγκεκριμένο αλγόριθμο με τη βοήθεια του οποίου βαθμολογούνται διάφορες εκδόσεις του ιστορικού, ώστε να είναι εφικτό να επιλεχθεί κάποιος που έχει βαθμολογία υψηλότερη από άλλους. Όσα μπλοκ δεν επιλέχθηκαν για να συμπεριληφθούν στην αλυσίδα, λέγονται ορφανά τμήματα (Bhaskar & Chuen, 2015).

Κάθε φορά που ένας ομότιμος χρήστης λαμβάνει μία έκδοση υψηλότερης βαθμολογίας που συχνά είναι η παλιά έκδοση στην οποία έχει προστεθεί ένα καινούργιο μπλοκ επεκτείνεται ή αντικαθίσταται η δική τους βάση δεδομένων ενώ μεταδίδεται η βελτίωση των ομότιμων χρηστών. Σε καμία περίπτωση δεν υπάρχει απόλυτη εγγύηση ότι μία συγκεκριμένη καταχώρηση θα διατηρηθεί στην έκδοση με τη μεγαλύτερη βαθμολογία για πάντα. Τα blockchains είναι έτσι κατασκευασμένα ώστε να μπορούν να προσθέτουν στα παλιά μπλοκ τη βαθμολογία των νέων μπλοκ και να τους παρέχουν το κίνητρο της επέκτασης με νέα μπλοκ και όχι της αντικατάστασης των παλιών μπλοκ (Antonopoulos, 2014). Έτσι η περίπτωση να γίνει αντικατάσταση ενός μπλοκ που ήδη υπάρχει μειώνεται αισθητά διότι πάνω από αυτό χτίζονται περισσότερα μπλοκ που εν τέλει τοποθετούν το παλιό μπλοκ πολύ χαμηλά σε σειρά ταξινόμησης (Antonopoulos, 2014; Nakamoto, 2008).

1.3.4. Χρόνος του Μπλοκ

Ο χρόνος που χρειάζεται το μπλοκ είναι ο μέσος χρόνος που απαιτείται για να φτιάξει το δίκτυο ένα νέο μπλοκ στην αλυσίδα των μπλοκ. Κάποια Blockchain μπορούν να δημιουργήσουν ένα καινούριο μπλοκ ανά 5 δευτερόλεπτα. Από τη στιγμή που ολοκληρώνεται η διαδικασία δημιουργίας ενός νέου μπλοκ, τα δεδομένα μπορούν να επαληθευτούν. Στην κρυπτονομισματική αυτό μπορεί να συμβεί με την πραγματοποίηση μιας συναλλαγής και έτσι ο μικρότερος χρόνος μπλοκ ισούται με γρηγορότερες συναλλαγές. Σχετικά με το Ethereum, ο χρόνος του μπλοκ υπολογίζεται ανάμεσα σε 14 και 15 δευτερόλεπτα ενώ του Bitcoin είναι στα 10 λεπτά.

1.3.5. Σκληρή Διακλάδωση

Ως σκληρή διακλάδωση ορίζεται η αλλαγή ενός κανόνα ώστε το λογισμικό που έχει επικυρωθεί με βάση τους παλιούς κανόνες να αντιμετωπίζει τα μπλοκ που παράγονται με βάση τους νέους κανόνες ως άκυρα. Όταν προκύπτει η σκληρή διακλάδωση, όλοι οι κόμβοι πρόκειται να λειτουργούν με τον τρόπο που ορίζουν οι νέοι κανόνες σε ό,τι αφορά την αναβάθμιση του λογισμικού τους. Υπάρχει η περίπτωση μόνιμης διάσπασης εάν μια ομάδα κόμβων συνεχίζει να χρησιμοποιεί παλιό λογισμικό όταν άλλοι κόμβοι χρησιμοποιούν νέο. Η Ethereum συνάντησε δυσκολίες στο κομμάτι της ανάκτησης δεδομένων των επενδυτών της εταιρείας ‘’The DAO’’ καθώς έπεσε θύμα επίθεσης hacker ο οποίος εντόπισε ένα τρωτό σημείο στον κώδικά της.

Σε τέτοιες περιπτώσεις η διακλάδωση που προκύπτει από έναν διαχωρισμό δημιουργεί αλυσίδες Ethereum και Ethereum Classic. Το 2014 η κοινότητα Nxt κλήθηκε να εξετάσει μια σκληρή διακλάδωση που θα οδηγούσε σε απόσυρση αρχείων Blockchain για την άμβλυνση των επιπτώσεων απώλειας 50 εκατομμυρίων NXT από μια μεγάλη ανταλλαγή κρυπτονομισμάτων. Η πρόταση για τις σκληρές διακλαδώσεις απορρίφθηκε και ορισμένα από τα κεφάλαια ανακτήθηκαν μετά από διαπραγματεύσεις και πληρωμές ρητρών. Άλλος τρόπος για να αποφευχθεί μια μόνιμη διάσπαση, είναι οι κόμβοι που χρησιμοποιούν το νέο λογισμικό να επιστρέψουν στους παλιούς κανόνες (Lee, 2013).

1.4 Τεχνολογία Blockchain

1.4.

1.4.1. Σύντομη ιστορία του Bitcoin

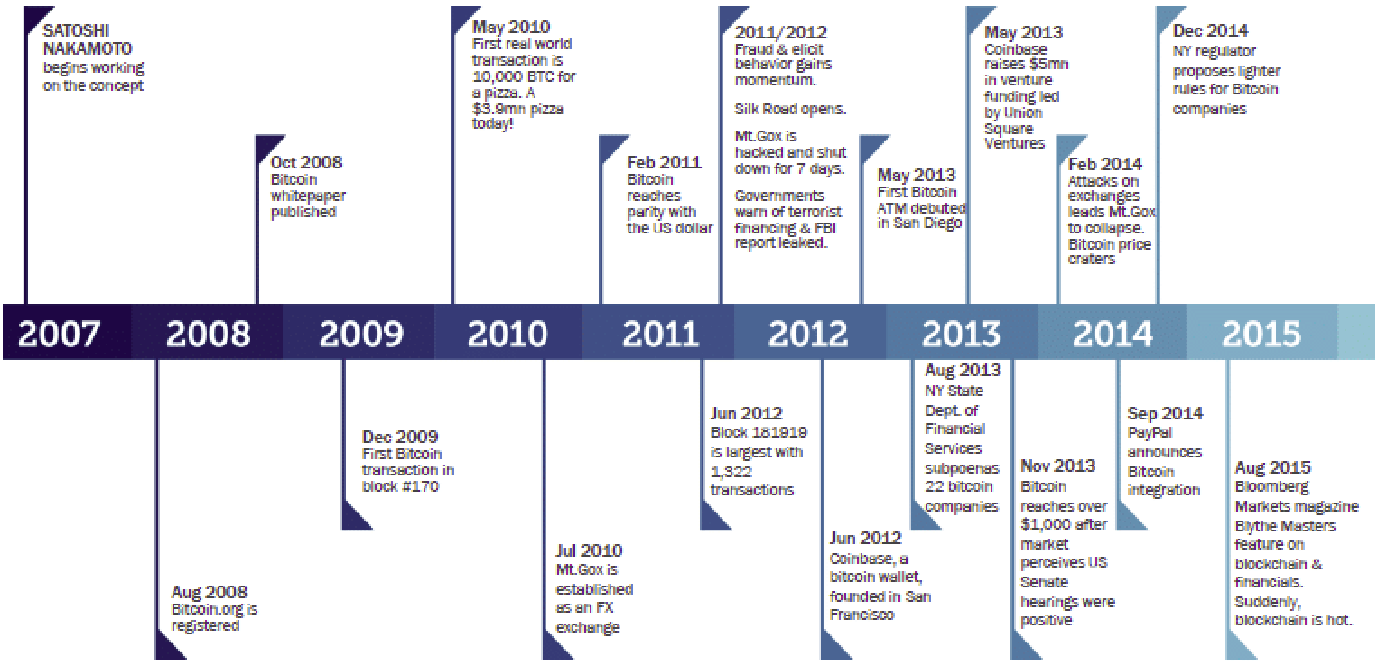
Το 2008 δημοσιεύτηκε από ένα άτομο ή μία ομάδα ατόμων με όνομα Satoshi Nakamoto ένα άρθρο με τίτλο "Bitcoin: Ένα μεταξύ ίσων Ηλεκτρονικό Ταμείο". Στο συγκεκριμένο άρθρο περιγράφθηκε μία έκδοση ανάμεσα σε ομότιμους των ηλεκτρονικών μετρητών που θα επέτρεπε την άμεση αποστολή των διαδικτυακών πληρωμών από το ένα μέρος στο άλλο χωρίς να περνάνε από χρηματοπιστωτικό ίδρυμα. Ο πρώτος τρόπος με τον οποίο υλοποιήθηκε αυτή η ιδέα ήταν το Bitcoin.

όλα τα δίκτυα και τα μέσα ανταλλαγής κατά τα οποία χρησιμοποιείται η κρυπτογράφηση για να εξασφαλιστούν οι συναλλαγές φέρουν την ετικέτα ‘’cryptocurrencies’’ αντίθετα με εκείνα τα συστήματα στα οποία οι συναλλαγές διακινούνται μέσα από μία κεντρική οντότητα που θεωρείται έμπιστη.

Μέχρι σήμερα κανείς δεν γνωρίζει ποιος είναι ο συντάκτης του πρώτου εγγράφου με όνομα Satoshi Nakamoto, καθώς ο ίδιος θέλησε να διατηρήσει την ανωνυμία του. Λίγο αργότερα ο ίδιος κυκλοφόρησε ένα πρόγραμμα ανοιχτού κώδικα μέσα από το οποίο υλοποιήθηκε το νέο πρωτόκολλο ξεκινώντας με το μπλοκ Genesis 50 νομισμάτων όπου μπορεί οποιοσδήποτε να εγκαταστήσει το πρόγραμμα αυτό του ανοιχτού κώδικα και να γίνει μέρος του δικτύου peer-to-peer Bitcoin. Από τότε έχει αυξηθεί κατά πολύ η δημοτικότητα του και συνεχίζει να αυξάνεται διαρκώς.

Πέραν τούτων η τεχνολογία Blockchain ανακαλύπτει νέες εφαρμογές πέραν της χρηματοδότησης

.



Σχήμα 1-1. Η Ιστορία του Bitcoin

1.4.2. Η Λειτουργία του Blockchain

Για να εξηγηθεί η έννοια του blockchain χρειάζεται να εξηγηθεί και πώς λειτουργεί το Bitcoin διότι τα δύο αυτά είναι αλληλένδετα. Η τεχνολογία blockchain ισχύει για οποιαδήποτε ψηφιακή συναλλαγή περιουσιακού στοιχείου συμβαίνει στο διαδίκτυο.

- Επικύρωση των καταχωρήσεων

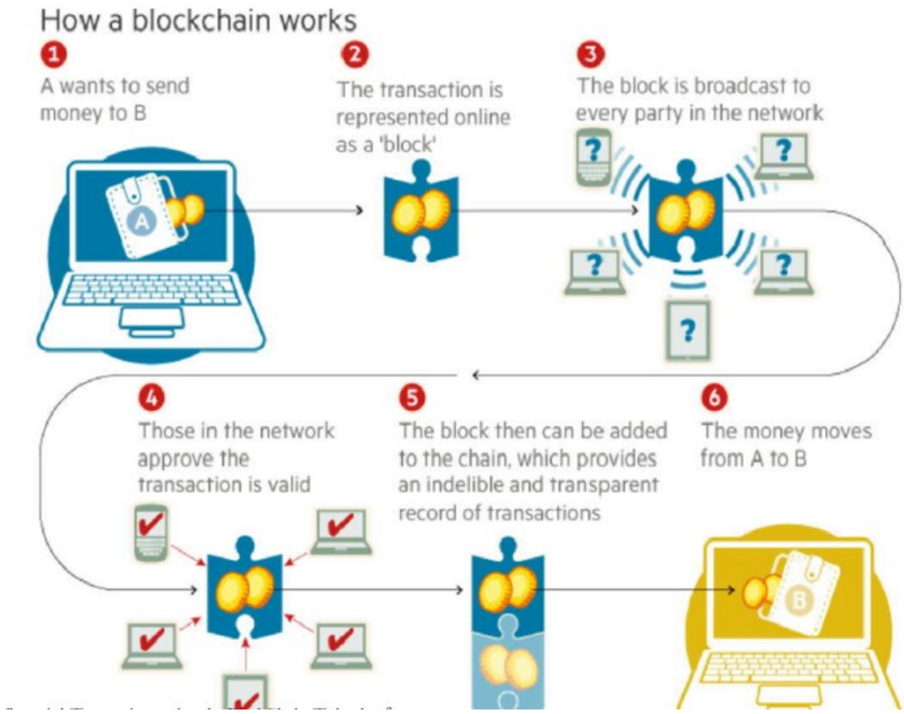
- Εισαγωγές διασφάλισης
- Διατήρηση ιστορικού αρχείου

Το ηλεκτρονικό εμπόριο είναι συνυφασμένο με τα χρηματοπιστωτικά ιδρύματα τα οποία λειτουργούν σαν αξιόπιστοι τρίτοι, επεξεργάζονται και μεσολαβούν στις ηλεκτρονικές συναλλαγές. Ο ρόλος τους είναι η επικύρωση, η διασφάλιση και διατήρηση των συναλλαγών. Το να συμβούν ηλεκτρονικές απάτες στις συναλλαγές είναι αναπόφευκτο και για αυτό απαιτείται μεσολάβηση από χρηματοπιστωτικές συναλλαγές. Το γεγονός αυτό ενέχει υψηλό κόστος συναλλαγής. το Bitcoin δεν χρησιμοποιεί κάποιο μηχανισμό εμπιστοσύνης τρίτου μέρους για δύο ενδιαφερόμενα μέρη που προσπαθούν να ολοκληρώσουν μία διαδικτυακή συναλλαγή, αντίθετα χρησιμοποιεί την κρυπτογραφική απόδειξη όπου κάθε συναλλαγή είναι προστατευμένη μέσα από την ψηφιακή υπογραφή, αποστέλλεται στο "δημόσιο κλειδί" του δέκτη και υπογράφεται ηλεκτρονικά με τη χρήση του ‘’ιδιωτικού κλειδιού’’ του αποστολέα. Για να μπορέσει ο ιδιοκτήτης ενός κρυπτονομισματος να προβεί σε διαδικτυακές συναλλαγές και να πληρώσει χρήματα κάπου, οφείλει πρωτίστως να αποδείξει ότι είναι κάτοχος του ‘’ιδιωτικού κλειδιού’’.

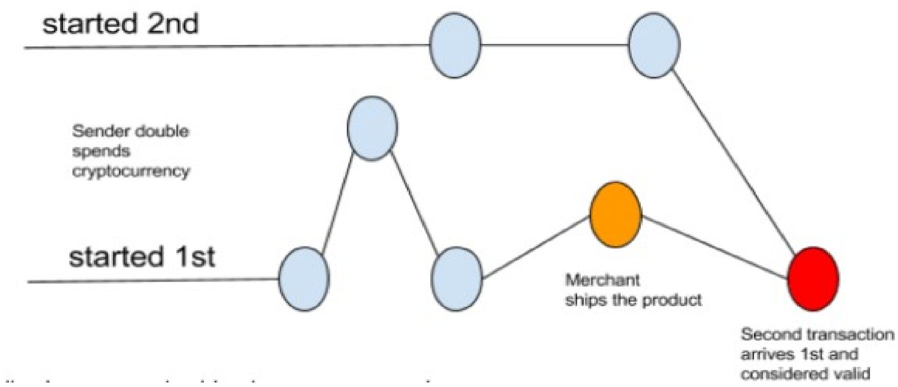
Η οντότητα που θα λάβει κάποιο ψηφιακό νόμισμα χρειάζεται να επαληθευτεί βάζοντας την ψηφιακή του υπογραφή που σημαίνει ταυτόχρονα ότι είναι κάτοχος ιδιωτικού κλειδιού και χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να προβεί στην αντίστοιχη συναλλαγή. Κάθε μία συναλλαγή μεταδίδεται σε κόμβους στο δίκτυο του Bitcoin και στη συνέχεια σημειώνεται σε δημόσιο βιβλίο αφού ολοκληρωθεί η επαλήθευση. Για να καταγραφεί στο δημόσιο βιβλίο η καθεμία από τις συναλλαγές πρέπει να επαληθεύεται για την εγκυρότητα της. Μέσα από αυτό τον κόμβο επαλήθευσης εξασφαλίζονται δύο πράγματα, πρώτον η οντότητα που θα ξοδέψει τα χρήματα διαθέτει την κρυπτογράφηση αφού έχει επαληθευτεί η ψηφιακή υπογραφή της συναλλαγής και, δεύτερον το μέρος που θα ξοδέψει έχει αρκετά κρυπτονομίσματα στη διάθεσή του μπορεί να ελέγξει τις συναλλαγές μέσα από το λογαριασμό του ή μέσα από το δημόσιο κλειδί που είναι σημειωμένο στο βιβλίο. Όλα αυτά διασφαλίζουν την ισορροπία στο λογαριασμό πριν ολοκληρωθεί η χρηματική συναλλαγή

Βέβαια υπάρχει και το ζήτημα διατήρησης της σειράς των συναλλαγών που μεταφέρονται σε κάθε κόμβο στο δίκτυο Bitcoin. Ανάμεσα σε ομότιμα μέρη οι συναλλαγές δεν φτάνουν σύμφωνα με τη χρονική σειρά που δημιουργούνται και έτσι υπάρχει ανάγκη για ένα σύστημα που θα διασφαλίζει ότι δεν θα προκύψει διπλή δαπάνη του κρυπτονομισματος. έχοντας κατά νου ότι οι συναλλαγές μεταφέρονται στον κόμβο μέσα από ένα κόμβο του δικτύου Bitcoin δεν υπάρχει κάποια εγγύηση ότι η σειρά με την οποία θα εισαχθούν στον κόμβο είναι ίδια με αυτή που δημιουργήθηκαν οι συναλλαγές. Όλα αυτά σημαίνουν πως πρέπει να αναπτυχθεί ένας μηχανισμός ώστε το δίκτυο Bitcoin να συμφωνεί με τη σειρά των συναλλαγών.

Το Bitcoin βρήκε λύση σε αυτό το πρόβλημα με τη δημιουργία ενός μηχανισμού που είναι σήμερα γνωστός ως τεχνολογία blockchain και λειτουργεί ως εξής. Το σύστημα Bitcoin αρχικά δίνει εντολή για τις συναλλαγές βάζοντας τις σε ομάδες που τις ονομάζει μπλοκ και στη συνέχεια αυτά τα μπλοκ συνδέονται μέσω του blockchain. Οι συναλλαγές μέσα σε ένα μπλοκ θεωρείται ότι συνέβησαν την ίδια στιγμή και συνδέονται μεταξύ τους με σειρά γραμμική χρονολογική και κάθε μπλοκ διαθέτει το ύφος του προηγούμενου. Βέβαια υπάρχει ένα ακόμη πρόβλημα, ότι οποιοσδήποτε κόμβος του δικτύου δύναται να συλλέξει συναλλαγές που δεν έχουν επιβεβαιωθεί και να προβεί στη δημιουργία μπλοκ μεταδίδοντας στη συνέχεια στο υπόλοιπο δίκτυο την πρόταση του πιο μπλοκ θα πρέπει να είναι το επόμενο στο blockchain.



Σχήμα 1-2. Οικονομικές συναλλαγές με χρήση του BlockChain, (Barski&Wilmer, 2016)

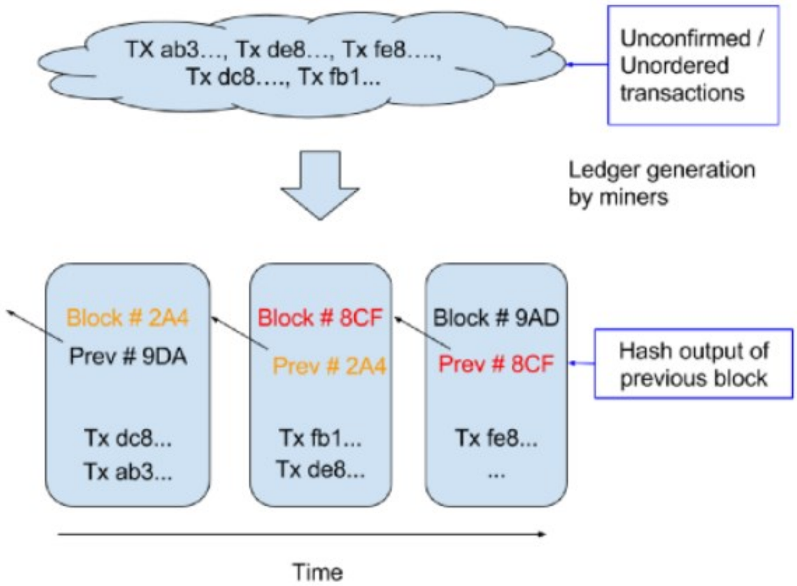


Σχήμα 1-3. Διπλή δαπάνη λόγω καθυστερήσεων διάδοσης στο δίκτυο ομότιμων

Ως προς το πώς αποφασίζει το δίκτυο ποιο μπλοκ θα είναι το επόμενο στο blockchain η απάντηση είναι ότι μπορούν να δημιουργηθούν πολλά μπλοκ από διαφορετικούς κόμβους ταυτόχρονα και κανείς δεν μπορεί να βασιστεί στην εντολή εφόσον τα μπλοκ είναι δυνατόν να φτάσουν σε διαφορετικά σημεία του δικτύου με βάση τις διαφορετικές εντολές που λαμβάνουν.

Το Bitcoin έχει βρει λύση και σε αυτό το πρόβλημα μέσα από την εισαγωγή ενός μαθηματικού παζλ. Κάθε μπλοκ γίνεται αποδεκτό στην αλυσίδα των μπλοκ υπό τον όρο ότι διαθέτει τη λύση σε ένα απαιτητικό μαθηματικό πρόβλημα. Η διαδικασία αυτή λέγεται ‘’απόδειξη εργασίας’’. Όταν δηλαδή ένας κόμβος που δημιουργεί ένα μπλοκ χρειάζεται να αποδείξει ότι μπορεί να λύσει το μαθηματικό παζλ βάζοντας αρκετούς υπολογιστικούς πόρους.

Η μέση απαιτούμενη προσπάθεια είναι εκθετική στον αριθμό των μηδενικών bits που χρειάζονται, αλλά η διαδικασία επαλήθευσης είναι πολύ απλή και μπορεί να γίνει με την εκτέλεση ενός μόνο ίχνους.



Σχήμα 1-4. Δημιουργία Blockchain από μη συμφωνημένες συναλλαγές

Η πολυπλοκότητα του μαθηματικού αυτού προβλήματος, υπάρχει η δυνατότητα, να ρυθμιστεί με τέτοιο τρόπο ώστε να διαρκέσει κατά μέσο όρο 10 λεπτά για έναν κόμβο στο δίκτυο Bitcoin ώστε να μπορέσει να κάνει μία σωστή πρόβλεψη και να δημιουργήσει ένα μπλοκ. Είναι λίγες βέβαια οι πιθανότητες του να δημιουργηθούν περισσότερα του ενός μπλοκ στο σύστημα των Bitcoin σε μία συγκεκριμένη χρονική στιγμή γιατί για να λύσει ο πρώτος κόμβος το πρόβλημα μεταφέρει το μπλοκ στο υπόλοιπο δίκτυο. Ενδεχομένως περισσότερα του ενός μπλοκ να μπορέσουν να λυθούν την ίδια στιγμή οδηγώντας σε διάφορους πιθανούς κλάδους. Βέβαια τα μαθηματικά που απαιτούνται για να λυθεί το πρόβλημα είναι πιο περίπλοκα και έτσι το blockchain σταθεροποιείται με γρήγορους ρυθμούς και μετά από αυτό κάθε κόμβος συμφωνεί για τη σειρά των μπλοκ. Οι υπολογιστικοί πόροι που δίνονται μέσα από τους κόμβους με σκοπό να λυθεί το μαθηματικό παζλ και να δημιουργηθούν νέα μπλοκ λέγονται ‘’κόμβοι εξόρυξης’’ και λαμβάνουν οικονομική επιβράβευση για την προσπάθειά τους. Το δίκτυο είναι δυνατόν να δεχτεί μόνο το μεγαλύτερο μπλοκ την ως έγκυρο και έτσι είναι αδύνατο για έναν εισβολέα να προσπαθήσει να εισάγει η δόλια συναλλαγή καθώς καλείται να αντιμετωπίσει καλούς κόμβους ώστε να δημιουργήσει τα επόμενα μπλοκ και να κάνει άλλους κόμβους του δικτύου Bitcoin να αποδεχτούν τη συναλλαγή χαρακτηρίζοντάς την έγκυρη. Η προσπάθεια αυτή θεωρείται δύσκολη διότι τα μπλοκ στο blockchain συνδέονται μεταξύ τους κρυπτογραφικά.

.

1.4.3. Υπάρχουσα αγορά

Η τεχνολογία blockchain μπορεί να εφαρμοστεί όχι μόνο σε οικονομικούς ή χρηματοοικονομικούς τομείς οι οποίοι βασίζονται σε μία τρίτη εμπιστευτική ηλεκτρονική οντότητα για την επικύρωση και την προστασία των διαδικτυακών συναλλαγών των ψηφιακών περιουσιακών στοιχείων. Υπάρχει μία εφαρμογή που λέγεται Smart contracts η οποία δημιουργήθηκε το 1994 από τον Nick Szabo. Ο συγκεκριμένος είχε την ιδέα του να εκτελούνται αυτόματα οι συμβάσεις μεταξύ των εμπλεκομένων μερών. Βέβαια μέχρι να έρθει η στιγμή να δημιουργηθούν τα κρυπτογραφικά νομίσματα για τις προγραμματισμένες πληρωμές δεν μπόρεσε να βρει τον τρόπο χρήσης. Πλέον τα προγράμματα blockchain και Smart contracts μπορούν να συνδεθούν ώστε να ενεργοποιήσουν τις πληρωμές αφού ενεργοποιηθεί μία συμβατική συμφωνία.

Τα Smart contracts θεωρούνται ως την κορυφαία εφαρμογή των κρυπτονομισμάτων είναι επί της ουσίας συμβόλαια που επιβάλλονται αυτόματα μέσα από πρωτόκολλο υπολογιστών.

Η τεχνολογία blockchain έχει κάνει πιο εύκολη τη διαδικασία της εγγραφής, της επαλήθευσης και της εκτέλεσής τους. Επιπροσθέτως όσες εταιρείες χαρακτηρίζονται ως ανοιχτού κώδικα επιτρέπουν τη χρήση Smart contract με την τεχνολογία blockchain ενώ πολλές εταιρείες που έχουν ως βάση λειτουργίας του στις τεχνολογίες Bitcoin και blockchain τώρα ξεκινούν να στηρίζουν τα Smart contracts. Στην περίπτωση που τα περιουσιακά στοιχεία μεταφέρονται μόνο αφού πληρούνται ορισμένες προϋποθέσεις είναι δυνατόν να αντικατασταθούν από τα Smart contracts.

Η Ethereum επιτρέπει σε όποιον θέλει να δημιουργήσει τα δικά του κρυπτονομίσματα και να τα χρησιμοποιήσει για να πληρώσει τα Smart Contracts, ενώ και η ίδια κατέχει τα δικά της κρυπτονομίσματα (ether) που χρησιμοποιούνται για την πληρωμή των υπηρεσιών.

Η εταιρία Ethereum ήδη ασχολείται με ένα ευρύ φάσμα εφαρμογών σε τομείς που σχετίζονται με τη διακυβέρνηση, τις αυτόνομες τράπεζες, την πρόσβαση χωρίς κλειδί, τη χρηματοδότηση πλήθους, την εμπορία χρηματοπιστωτικών παραγώγων και το διακανονισμό χρησιμοποιώντας τα Smart Contracts.

Υπάρχουν ορισμένα Blockchain για να υποστηρίξουν εφαρμογές εκτός πέραν των κρυπτονομισμάτων. Τη δεδομένη στιγμή υπάρχουν τρεις προσεγγίσεις που υποστηρίζουν άλλες εφαρμογές με σκοπό την καταπολέμηση των περιορισμών του blockchain Bitcoin:

- Εναλλακτικά Blockchains: Αποτελούν έναν τρόπο χρήσης του αλγόριθμου Blockchain που στόχο έχει να επιτεύξει την κατανεμημένη συναίνεση ενός ψηφιακού στοιχείου. Το σύστημα αυτό μοιράζεται όσους τολμούν να εξάγουν κάποιο μητρικό δίκτυο, για παράδειγμα το Bitcoin, με τη διαδικασία αυτή να ονομάζεται συγχωνευμένη εξόρυξη. Αυτού του είδους τα Blockchain δημιουργήθηκαν για να βοηθήσουν εφαρμογές να υλοποιηθούν (πχ DNS, SSL αποθήκευση αρχείων κ.α.).

- ColoredCoins: Πρόκειται για μια μέθοδο των προγραμματιστών με την οποία δημιουργούν ψηφιακά στοιχεία πάνω από το Blockchain των Bitcoin με τη χρήση λειτουργιών πέραν των ψηφιακών νομισμάτων.
- Sidechains: Πρόκειται για εναλλακτική μορφή Blockchains τα οποία υποστηρίζονται από τα Bitcoins μέσα από μια συμφωνία Bitcoin. Υπάρχει η περίπτωση να διαθέτει κάποιος πολλά SideChains τα οποία είναι συνδεδεμένα με τα Bitcoins και να διακρίνονται από διαφορετικά χαρακτηριστικά εκμεταλλευόμενα την ανθεκτικότητα που προέρχεται από την αλυσίδα Bitcoin. Το BlockchainBitcoin ακολούθως μπορεί να υποστηρίξει τα πρόσθετα χαρακτηριστικά επαναλαμβάνοντας ενέργειες.

Υπάρχουν αρκετές εταιρίες οι οποίες διερευνούν εναλλακτικές και νέες χρήσεις των Blockchain προς όφελος των δικών τους εφαρμογών. Μερικές από αυτές είναι η IBM, η Samsung, η Overstock, η Amazon, η UBS, η Citi, η Ebay και η Verizon Wireless. Οι 9 στις 10 μεγαλύτερες τράπεζες παγκοσμίως σύναψαν πρόσφατα (Σεπτέμβριος του 2015) συνεργασία με την εταιρεία χρηματοπιστωτικής τεχνολογίας R3, η οποία βρίσκεται στη Νέα Υόρκη με σκοπό να οικοδομήσουν ένα πλαίσιο χρήσης της τεχνολογίας Blockchain (Kelly, 2016). Ορισμένες τράπεζες που εμπλέκονται σε αυτή την κίνηση είναι η JP Morgan, η State Street, η UBS, η Royal Bank Of Scotland, η CreditSuisse, η BBVA και η Bank of Australia

1.5 Επίλογος

Ως blockchain ορίζεται μία κατανεμημένη βάση δεδομένων η οποία αποτελείται από αρχεία ή ένα δημόσιο βιβλίο που περιλαμβάνει όλες τις συναλλαγές ή ψηφιακά γεγονότα που έχουν λάβει χώρα και έχουν διαμοιραστεί ανάμεσα στα εμπλεκόμενα μέρη. Καθεμία από τις συναλλαγές που έχουν καταγραφεί στο δημόσιο βιβλίο είναι δυνατόν να επαληθευτεί με τη συναίνεση των περισσότερων από τους συμμετέχοντες στο σύστημα. Εάν εισαχθούν πληροφορίες δεν μπορούν να διαγραφούν κατόπιν. Το blockchain διαθέτει ένα συγκεκριμένο αρχείο που επαληθεύει κάθε μία από τις συναλλαγές που έχουν γίνει ποτέ. Το Bitcoin θεωρείται το πιο δημοφιλές παράδειγμα που συνδέεται με την τεχνολογία των blockchain. Έχει υποστεί κριτική καθώς έχει συμβάλλει στην καθιέρωση μιας παγκόσμιας αγοράς πολλών δισεκατομμυρίων ανώνυμων συναλλαγών χωρίς να ελέγχονται κυβερνητικά. Έτσι πρέπει να αντιμετωπίσει κάποια ρυθμιστικά προβλήματα που σχετίζονται με τις εθνικές κυβερνήσεις και τα χρηματοπιστωτικά ιδρύματα. Τα πλεονεκτήματα που διαθέτει η τεχνολογία blockchain αντισταθμίζονται με τα ρυθμιστικά και τα τεχνικά προβλήματα. Οι έξυπνες συμβάσεις αποτελούν μία αναδυόμενη περίπτωση χρήσης στην τεχνολογία blockchain. Ως έξυπνες συμβάσεις θεωρούνται τα βασικά προγράμματα των ηλεκτρονικών υπολογιστών μέσα από τα οποία μπορούν αυτόματα να εκτελεστούν οι όροι μιας σύμβασης. Τα εμπλεκόμενα μέρη μίας συμβατικής συμφωνίας δύνανται να πραγματοποιήσουν αυτόματα πληρωμές όταν πληρούνται οι προκαθορισμένες προϋποθέσεις μιας έξυπνης σύμβασης.

.

Ως έξυπνη ιδιότητα ορίζεται μία ιδέα που έχει να κάνει με τον έλεγχο της ιδιοκτησίας ενός ακινήτου ή ενός άλλου στοιχείο πού χρησιμοποιείται το blockchain ή Smart contracts. Με την λέξη ακίνητο εννοείται ένα αυτοκίνητο ένα σπίτι ή ένα Smartphone ή μπορεί να υπονοούνται οι μετοχές μιας εταιρείας.

Στο συγκεκριμένο σημείο είναι καλό να προστεθεί ότι και το Bitcoin δεν είναι ένα πραγματικό νόμισμα αντίθετα έχει να κάνει με τον έλεγχο της ιδιοκτησίας των χρημάτων. Η τεχνολογία blockchain εφαρμόζεται σε πολλούς τομείς τόσο χρηματικούς όσο και μη χρηματοοικονομικούς. Τα χρηματοπιστωτικά ιδρύματα και οι τράπεζες δεν αντιμετωπίζουν πλέον την τεχνολογία blockchain ως κάτι απειλητικό για τα παραδοσιακά επιχειρηματικά μοντέλα. Οι πιο σημαντικές τράπεζες παγκοσμίως ψάχνουν ευκαιρίες στον τομέα αυτό αναζητώντας καινοτόμες εφαρμογές blockchain.

Πρόσφατα σε μία συνέντευξη της η Rain Lohmus που προέρχεται από την τράπεζα LHV της Εσθονίας αποκάλυψε ότι το blockchain θεωρείται ως το πιο δοκιμασμένο και ασφαλές στοιχείο για τραπεζικές και χρηματοοικονομικές συναλλαγές.

Εξίσου ατελείωτες είναι και οι ευκαιρίες για μη οικονομικές εφαρμογές. Με αυτό τον τρόπο προβλέπονται όλα τα νομικά έγγραφα, τα ιατρικά αρχεία, οι πληρωμές πιστότητας στη μουσική βιομηχανία, οι συμβολαιογράφοι, οι ιδιωτικές ασφάλειες και οι άδειες γάμου στο blockchain. Η αποθήκευση του δακτυλικού αποτυπώματος αντί της αποθήκευσης του ίδιου του ψηφιακού στοιχείου βοηθά στην επίτευξη του στόχου ανωνυμίας ή της προστασίας της ιδιωτικής ζωής.

Γεγονός αποτελεί ότι τα πλεονεκτήματα που παρουσιάζει η τεχνολογία blockchain έρχεται σε αντιστάθμιση με τα ρυθμιστικά ζητήματα και τις προκλήσεις που λαμβάνουν χώρα σε τεχνικό επίπεδο. Οι έξυπνες συμβάσεις αποτελούν βασική περίπτωση της χρήσης της τεχνολογίας του blockchain. Οι τελευταίες συνιστούν βασικά προγράμματα ηλεκτρονικών υπολογιστών Με τη βοήθεια των οποίων μπορούν να εκτελεστούν αυτόματα οι όροι μιας σύμβασης. Τα μέρη που συμμετέχουν σε μία συμβατική συμφωνία είναι δυνατόν να ολοκληρώσουν αυτόματα πληρωμές αφού πληρούνται οι προβλεπόμενες προϋποθέσεις της έξυπνης σύμβασης.

Κεφάλαιο 2ο: Έξυπνες Συμβάσεις

2.1 Εισαγωγή

Τα έξυπνα συμβόλαια είναι ουσιαστικά αυτοματοποιημένες συμφωνίες μεταξύ του δημιουργού της σύμβασης και του παραλήπτη. Αυτή η συμφωνία αποτελεί έναν κώδικα που ενσωματώνεται στο Blockchain, καθιστώντας την αμετάβλητη καθώς και μη αναστρέψιμη. Συνήθως χρησιμοποιούνται για την αυτοματοποίηση της εκτέλεσης μιας συμφωνίας, ώστε όλα τα μέρη να μπορούν να είναι βέβαιοι για τη σύναψη αμέσως, χωρίς να χρειάζονται μεσάζοντες. Μπορούν επίσης να αυτοματοποιήσουν μια ροή εργασίας, ξεκινώντας όταν ικανοποιούνται ορισμένες συνθήκες. Μια υπογεγραμμένη σύμβαση που δημιουργεί μια συμβατική σύνδεση μεταξύ δύο ή περισσότερων μερών είναι γνωστή ως εκτελεσμένη σύμβαση. Κάθε μέρος υπόσχεται να τηρήσει τα νομικά καθήκοντα που συμφώνησε στη γραπτή συμφωνία μόλις υπογραφεί σωστά η σύμβαση. Δημοφιλή από το δεύτερο πιο δημοφιλές Blockchain στον κόσμο, το Ethereum (ETH), τα έξυπνα συμβόλαια έχουν οδηγήσει στη σειρά αποκεντρωμένων εφαρμογών του δικτύου (DApps) και άλλων περιπτώσεων χρήσης.

Ένα βασικό πλεονέκτημα των δικτύων Blockchain είναι η αυτοματοποίηση εργασιών που παραδοσιακά απαιτούν έναν μεσάζοντα τρίτου μέρους. Για παράδειγμα, αντί να χρειάζεται μια τράπεζα να εγκρίνει τη μεταφορά κεφαλαίων από πελάτη σε ελεύθερο επαγγελματία, η διαδικασία μπορεί να συμβεί αυτόματα, χάρη σε ένα έξυπνο συμβόλαιο. Το μόνο που απαιτείται είναι δύο μέρη να συμφωνήσουν σε μια ιδέα. Ένα άλλο παράδειγμα θα μπορούσε να είναι μια ρυθμιστική ομάδα και οι πολίτες που αντιπροσωπεύει να συζητούν έναν νόμο. Εάν αυτά τα δύο μέρη καταλήξουν σε συμφωνία σε ένα σύστημα που βασίζεται σε Blockchain, ο νόμος θα τεθεί σε ισχύ μέσω μιας εκτελεσθείσας συμφωνίας.

Τα έξυπνα συμβόλαια μπορούν να προγραμματιστούν ώστε να λειτουργούν για τις μάζες, αντικαθιστώντας τις κυβερνητικές εντολές και τα συστήματα λιανικής, μεταξύ άλλων πλεονεκτημάτων. Επιπλέον, τα έξυπνα συμβόλαια θα εξαλείφουν ενδεχομένως την ανάγκη προσαγωγής ορισμένων διαφωνιών στα δικαστήρια, εξοικονομώντας χρόνο και χρήμα στα μέρη. Αυτή η ασφάλεια οφείλεται σε μεγάλο βαθμό στον υποκείμενο κώδικα έξυπνης σύμβασης. Στο Ethereum, για παράδειγμα, τα συμβόλαια γράφονται στη γλώσσα προγραμματισμού Solidity, η οποία είναι πλήρης Turing. Αυτό σημαίνει ότι οι κανόνες και οι περιορισμοί των έξυπνων συμβάσεων είναι ενσωματωμένοι στον κώδικα του δικτύου και κανένας κακός παράγοντας δεν μπορεί να χειραγωγήσει τέτοιους κανόνες. Στην ιδανική περίπτωση, αυτοί οι περιορισμοί θα μετριάζανε τις απάτες ή τις κρυφές τροποποιήσεις συμβολαίων. Τα έξυπνα συμβόλαια κρυπτογράφησης μπορούν να τεθούν σε ισχύ μόνο εάν όλοι οι συμμετέχοντες συμφωνήσουν και υπογράψουν για το θέμα. Στη συνέχεια, έχει οριστεί για τη ζωή.

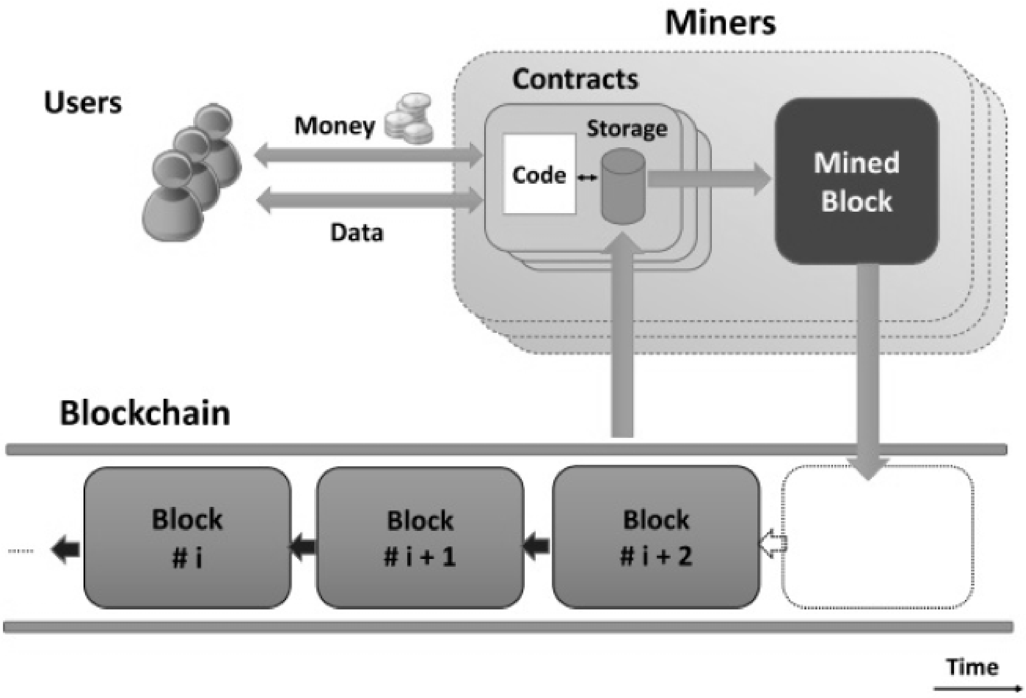
Με πιο τεχνικούς όρους, η ιδέα ενός έξυπνου συμβολαίου μπορεί να αναλυθεί σε μερικά βήματα. Πρώτον, ένα έξυπνο συμβόλαιο χρειάζεται συμφωνία μεταξύ δύο ή περισσότερων μερών. Μόλις καθιερωθούν, οι δύο μπορούν να συμφωνήσουν σε όρους υπό τους οποίους το έξυπνο συμβόλαιο θα θεωρείται ολοκληρωμένο. Η απόφαση θα εγγραφεί στο έξυπνο συμβόλαιο, το οποίο στη συνέχεια κρυπτογραφείται και αποθηκεύεται στο δίκτυο Blockchain. Μόλις ολοκληρωθεί η σύμβαση, η συναλλαγή καταγράφεται στο Blockchain όπως και κάθε άλλη. Στη συνέχεια, όλοι οι κόμβοι θα ενημερώσουν το αντίγραφό τους του Blockchain με αυτήν τη συναλλαγή, ενημερώνοντας τη νέα «κατάσταση» του δικτύου.

2.2 Η Έννοια των Έξυπνων Συμβάσεων

Μια έξυπνη σύμβαση είναι ένας εκτελέσιμος κώδικας που τρέχει στο Blockchain για να διευκολύνει, να εκτελέσει και να επιβάλει τους όρους μιας συμφωνίας. Ο κύριος στόχος μιας έξυπνης σύμβασης είναι να εκτελεστούν αυτομάτως οι όροι μιας συμφωνίας όταν πληρούνται οι καθορισμένοι όροι. Έτσι, οι έξυπνες συμβάσεις 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. Η ιδέα των έξυπνων συμβάσεων προήλθε από τον Szabo το 1994, (Szabo, 2017).

Ωστόσο, η ιδέα δεν εφαρμόστηκε μέχρι την εμφάνιση της τεχνολογίας Blockchain. Μία έξυπνη σύμβαση μπορεί να θεωρηθεί ως ένα σύστημα που απελευθερώνει ψηφιακά περιουσιακά στοιχεία σε όλα ή σε ορισμένα από τα εμπλεκόμενα μέρη μόλις έχουν επιτευχθεί αυθαίρετοι προκαθορισμένοι κανόνες, (Buterin, 2017). Για παράδειγμα, η Alice στέλνει X νομισματικές μονάδες στον Bob, αν λάβει Y νομισματικές μονάδες από τον Carl.

Πολλοί διαφορετικοί ορισμοί μιας έξυπνης σύμβασης έχουν συζητηθεί στη βιβλιογραφία. Στην εργασία του Stark, (2017), ο συντάκτης ταξινόμησε όλους τους ορισμούς σε δύο κατηγορίες, δηλαδή τον έξυπνο κώδικα σύμβασης και την έξυπνη νομική σύμβαση. Ο έξυπνος κώδικας σύμβασης σημαίνει "κώδικας που αποθηκεύεται, επαληθεύεται και εκτελείται σε ένα Blockchain", (Stark, 2017). Η ικανότητα αυτής της έξυπνης σύμβασης εξαρτάται εξ ολοκλήρου από τη γλώσσα προγραμματισμού που χρησιμοποιείται για την έκφραση της σύμβασης και τα χαρακτηριστικά του Blockchain. Έξυπνη νομική σύμβαση σημαίνει κώδικας για την ολοκλήρωση ή την αντικατάσταση των νομικών συμβάσεων. Η ικανότητα αυτής της έξυπνης σύμβασης δεν εξαρτάται από την τεχνολογία, αλλά από τα νομικά, πολιτικά και επιχειρηματικά θεσμικά όργανα. Το επίκεντρο εδώ θα είναι ο πρώτος ορισμός, ο οποίος είναι έξυπνος κώδικας σύμβασης.



Σχήμα 2-1. Σύστημα έξυπνης σύμβασης.

Μια έξυπνη σύμβαση έχει ένα υπόλοιπο λογαριασμού, έναν ιδιωτικό αποθηκευτικό χώρο και έναν εκτελέσιμο κώδικα. Η κατάσταση της σύμβασης περιλαμβάνει την αποθήκευση και το υπόλοιπο της σύμβασης. Η κατάσταση αποθηκεύεται στο Blockchain και ενημερώνεται κάθε φορά που γίνεται επίκληση της σύμβασης. Το σχήμα 2-1 απεικονίζει το έξυπνο σύστημα συμβάσεων.

Σε κάθε σύμβαση θα ανατεθεί μια μοναδική διεύθυνση 20 bytes. Μόλις εφαρμοστεί η σύμβαση στο Blockchain, ο κώδικας της δεν μπορεί να αλλάξει. Για να εκτελεστεί μια σύμβαση, οι χρήστες μπορούν απλά να στείλουν μια συναλλαγή στη διεύθυνση της σύμβασης. Αυτή η συναλλαγή θα εκτελεστεί έπειτα από κάθε κόμβο συναίνεσης (που ονομάζεται miner) στο δίκτυο για να επιτευχθεί συναίνεση σχετικά με το αποτέλεσμα της. Η κατάσταση της σύμβασης θα ενημερωθεί αναλόγως. Η σύμβαση μπορεί, με βάση τη συναλλαγή που λαμβάνει, να διαβάζει / γράφει στον ιδιωτικό χώρο αποθήκευσης, να αποθηκεύει χρήματα στο υπόλοιπο του λογαριασμού, να στέλνει / να λαμβάνει μηνύματα ή χρήματα από χρήστες / άλλες συμβάσεις ή ακόμα και να δημιουργεί νέες συμβάσεις.

Υπάρχουν δύο τύποι έξυπνων συμβάσεων, δηλαδή, ντετερμινιστικές και μη-ντετερμινιστικές έξυπνες συμβάσεις, (Morabito, 2017). Μια ντετερμινιστική έξυπνη σύμβαση είναι μια έξυπνη σύμβαση που όταν εκτελείται, δεν απαιτεί καμία πληροφορία από εξωτερικό συμβαλλόμενο μέρος (εκτός του Blockchain). Μια μη ντετερμινιστική έξυπνη σύμβαση είναι μια σύμβαση που εξαρτάται από πληροφορίες (που ονομάζονται χρησμοί ή τροφοδοσίες δεδομένων) από ένα εξωτερικό μέρος. Τέτοιο παράδειγμα είναι μια σύμβαση που απαιτεί την εκτέλεση των τρεχουσών πληροφοριών καιρού, η οποία δεν είναι διαθέσιμη στο Blockchain.

2.3 Πλατφόρμες για έξυπνες συμβάσεις

Οι έξυπνες συμβάσεις μπορούν να αναπτυχθούν και να τρέξουν σε διαφορετικές πλατφόρμες Blockchain (π.χ. Ethereum, Bitcoin και NXT). Οι διαφορετικές πλατφόρμες προσφέρουν ιδιαίτερα χαρακτηριστικά για την ανάπτυξη έξυπνων συμβάσεων. Ορισμένες πλατφόρμες υποστηρίζουν γλώσσες προγραμματισμού υψηλού επιπέδου για την ανάπτυξη έξυπνων συμβάσεων. Θα αναπτυχθούν τρεις δημόσιες πλατφόρμες εδώ.

Το Bitcoin, (Nkamoto, 2008), είναι μια δημόσια πλατφόρμα Blockchain που μπορεί να χρησιμοποιηθεί για την επεξεργασία κρυπτογραφικών συναλλαγών, αλλά με μια πολύ περιορισμένη ικανότητα υπολογισμού. Το Bitcoin χρησιμοποιεί μια γλώσσα προγραμματισμού που βασίζεται σε δέσμη ενεργειών bytecode. Η δυνατότητα δημιουργίας έξυπνης σύμβασης με πλούσια λογική είναι πολύ περιορισμένη με τη γλώσσα δέσμης ενεργειών Bitcoin, (Lewis, 2017). Στο Bitcoin, είναι δυνατή μια απλή λογική που απαιτεί πολλαπλές υπογραφές για να υπογράψει μια μόνο συναλλαγή πριν επιβεβαιώσει την πληρωμή. Ωστόσο, η συγγραφή συμβάσεων με σύνθετη λογική δεν είναι δυνατή λόγω των περιορισμών της γλώσσας Bitcoin. Η γλώσσα γραφής Bitcoin, για παράδειγμα, δεν υποστηρίζει ούτε βρόχους ούτε όρια απόσυρσης, (Buterin, 2017). Για να εφαρμόσει ένα βρόχο, ο μόνος πιθανός τρόπος είναι η επανάληψη του κώδικα πολλές φορές, η οποία είναι αναποτελεσματική.

Όταν το Bitcoin εισήχθη για πρώτη φορά το 2008, ένα από τα βασικά του σημεία πώλησης ήταν η ανωνυμία - οι χρήστες θα μπορούν να ξοδεύουν τα bitcoins "χωρίς πληροφορίες που να συνδέουν τη συναλλαγή με κανέναν", (Nakamoto, 2008). Τα τελευταία χρόνια, ωστόσο, οι ερευνητές έχουν δείξει ότι το Bitcoin προσφέρει πολύ ασθενέστερη ανωνυμία από ό, τι αρχικά αναμενόταν, (Meiklejohn et al, 2013), αποδεικνύοντας ότι θα μπορούσαν να ακολουθήσουν την κίνηση κεφαλαίων στο blockcain του Bitcoin.

Η κοινότητα αντέδρασε σε αυτό προτείνοντας δύο βασικές προσεγγίσεις για τη βελτίωση της ανωνυμίας του Bitcoin: (1) νέα συστήματα ανωνυμίας συμβατά με Bitcoin, (Sasson et al, 2014), (2) νέα ανώνυμα κρυπτονομίσματα που είναι ανεξάρτητα από το Bitcoin, (Sasson et al, 2014). Στην εργασία των Heilman et al, (2016), λαμβάνεται η προηγούμενη προσέγγιση αναπτύσσοντας νέα σχήματα ανωνυμίας που είναι συμβατά με το Bitcoin μέσω ενός μαλακού εργαλείου. Τα συστήματά αυτά προσφέρουν ένα νέο αντιστάθμισμα μεταξύ της πρακτικότητας (δηλαδή της ταχύτητας συναλλαγής), της ασφάλειας (δηλαδή της αντίστασης στις επιθέσεις διπλής δαπάνης, της άρνησης συναλλαγής DoS και των επιθέσεων Sybil) και της ανωνυμίας (δηλαδή των μη συνδεόμενων συναλλαγών).

Η τεχνική των Heilman et al, (2016), εμπνευσμένη από το eCash, (Chaum, 1983), λειτουργεί ως εξής. Για να πληρώσει ένας χρήστης A ανώνυμα έναν άλλο χρήστη B, θα πρέπει πρώτα να ανταλλάξει ένα bitcoin για ένα ανώνυμο κουπόνι μέσω του διαμεσολαβητή I. Τότε θα μπορούσε ο B να εξαργυρώσει το ανώνυμο κουπόνι με τον I για να λάβει ένα bitcoin πίσω. Το σχήμα των Heilman et al, (2016) ξεπερνά δύο βασικές προκλήσεις: (i) εξασφάλιση της μη σύνδεσης των κουπονιών (δηλαδή, κρύβοντας τη σχέση μεταξύ έκδοσης και εξόφλησης ενός κουπονιού) και (ii) επιβολή δίκαιης ανταλλαγής μεταξύ των συμμετεχόντων (δηλαδή οι χρήστες μπορούν να εξαργυρώσουν εκδοθέντα δελτία ακόμη και ενάντια σε ένα μη συνεργάσιμο ή κακόβουλο I, και κανένα μέρος δεν μπορεί να κλέψει ή να διπλασιάσει τα κουπόνια και τα bitcoins).

Το NXT είναι μια δημόσια πλατφόρμα Blockchain που περιλαμβάνει ενσωματωμένες έξυπνες συμβάσεις ως πρότυπα, (Lewis, 2017). Το NXT επιτρέπει μόνο την ανάπτυξη έξυπνων συμβάσεων χρησιμοποιώντας αυτά τα πρότυπα. Εντούτοις, δεν επιτρέπει εξειδικευμένες έξυπνες συμβάσεις εξαιτίας της έλλειψης της Turing-πληρότητας στη γλώσσα προγραμματισμού του.

Το Ethereum, (Wood, 2014), είναι μια δημόσια πλατφόρμα Blockchain που μπορεί να υποστηρίξει προηγμένες και προσαρμοσμένες έξυπνες συμβάσεις με τη βοήθεια της πλήρους γλώσσας προγραμματισμού Turing. Η πλατφόρμα Ethereum μπορεί να υποστηρίξει όρια απόσυρσης, βρόχους, οικονομικές συμβάσεις και αγορές τυχερών παιχνιδιών. Ο κώδικας των έξυπνων συμβάσεων του Ethereum γράφεται σε μια βασισμένη σε στοίβα γλώσσα bytecode και εκτελείται σε Ethereum Virtual Machine (EVM). Μπορούν να χρησιμοποιηθούν πολλές γλώσσες υψηλού επιπέδου (π.χ. Solidity, Serpent και LLL) για τη σύνταξη έξυπνων συμβάσεων του Ethereum. Ο κώδικας αυτών των γλωσσών μπορεί στη συνέχεια να μεταγλωττιστεί σε byteodes EVM που θα εκτελεστούν. Το Ethereum είναι σήμερα η πιο κοινή πλατφόρμα για την ανάπτυξη έξυπνων συμβάσεων.

2.4 Εφαρμογές έξυπνων συμβάσεων

Υπάρχουν διάφορες πιθανές εφαρμογές στις οποίες μπορούν να εφαρμοστούν έξυπνες συμβάσεις. Ορισμένες από αυτές τις εφαρμογές είναι οι εξής:

- Internet των πραγμάτων και έξυπνη ιδιοκτησία, (Christidis & Devetsikiotis, 2016): υπάρχουν δισεκατομμύρια κόμβοι που μοιράζονται δεδομένα μεταξύ τους μέσω του Διαδικτύου. Μια πιθανή περίπτωση χρήσης έξυπνων συμβάσεων βασισμένων σε Blockchain είναι να επιτρέπεται στους εν λόγω κόμβους να μοιράζονται ή να έχουν πρόσβαση σε διαφορετικές ψηφιακές ιδιότητες χωρίς αξιόπιστο τρίτο μέρος. Υπάρχουν διάφορες εταιρείες που ερευνούν αυτήν την περίπτωση χρήσης. Για παράδειγμα, η Slock.it είναι μια γερμανική εταιρεία που χρησιμοποιεί τις έξυπνες συμβάσεις που βασίζονται στο Ethereum για την ενοικίαση, πώληση ή διανομή οτιδήποτε (π.χ. πώληση ενός αυτοκινήτου) χωρίς τη συμμετοχή ενός αξιόπιστου τρίτου μέρους.
- Διαχείριση δικαιωμάτων μουσικής, (Egbertsen et al, 2016): μια πιθανή περίπτωση χρήσης είναι η καταγραφή των δικαιωμάτων κυριότητας μιας μουσικής στο Blockchain. Μια έξυπνη σύμβαση μπορεί να επιβάλει την πληρωμή για τους ιδιοκτήτες μουσικής για τη χρήση μουσικής για εμπορικούς σκοπούς. Εξασφαλίζει επίσης ότι η πληρωμή διανέμεται μεταξύ των ιδιοκτητών της μουσικής. Η Ujo είναι μια εταιρεία που ερευνά τη χρήση έξυπνων συμβολαίων που βασίζονται σε Blockchain στη μουσική βιομηχανία.
  • Ηλεκτρονικό εμπόριο: μια πιθανή περίπτωση χρήσης είναι να διευκολυνθεί το εμπόριο μεταξύ

μη πιστωτικών μερών (π.χ. πωλητής και αγοραστής) χωρίς πιστωτικό τρίτο μέρος. Αυτό θα είχε ως αποτέλεσμα τη μείωση του κόστους συναλλαγών. Οι έξυπνες συμβάσεις μπορούν να αποδεσμεύσουν την πληρωμή στον πωλητή μόλις ο αγοραστής είναι ικανοποιημένος με το προϊόν ή την υπηρεσία που έλαβε, (Banasik et al, 2016).

Υπάρχουν και άλλες πιθανές εφαρμογές όπως η ηλεκτρονική ψηφοφορία, η πληρωμή υποθηκών, η διαχείριση ψηφιακών δικαιωμάτων, η ασφάλιση αυτοκινήτων, η αποθήκευση κατανεμημένων αρχείων, η διαχείριση ταυτότητας και η αλυσίδα εφοδιασμού. Τα Zerocash, (Sasson et al, 2014), και Zerocoin, (Miers et al, 2013), παρέχουν ανώνυμα πληρωμές μέσω της χρήσης ενός νέου τύπου κρυπτογραφικών αποδείξεων (ZK-SNARK). Σε αντίθεση με τα σχήματα των Heilman et al, (2016), είναι από μόνα τους κρυπτονομίσματα και δεν μπορούν να ενσωματωθούν με το Bitcoin. Εν τω μεταξύ, στην εργασία των Saxena et al, (2014), εμφανίζεται ένα ανώνυμο σχήμα πληρωμής που μπορεί να προσφέρει προστασία της ανωνυμίας στο Bitcoin, το οποίο παρέχει εξαιρετική προστασία προσωπικών δεδομένων και είναι πολύ γρήγορο.

Ωστόσο, τα μέρη που εμπιστεύονται την ανωνυμοποίηση των συναλλαγών σύμφωνα με την εργασία των Saxena et al, (2014), εξακολουθούν να μπορούν να παραβιάζουν την ταυτότητα των χρηστών, ακόμη και αν είναι ειλικρινείς-αλλά-περίεργοι.

Μία υπηρεσία ανάμειξης bitcoin παρέχει ανωνυμία μεταφέροντας τις πληρωμές από ένα σύνολο εισερχομένων διευθύνσεων bitcoin σε ένα σύνολο εξόδων bitcoin διευθύνσεων, έτσι ώστε να είναι δύσκολο να εντοπιστεί ποια διεύθυνση εισόδου πληρώνει ποια διεύθυνση εξόδου. Το Mixcoin, (Bonneau et al, 2014), χρησιμοποιεί ένα αξιόπιστο τρίτο μέρος για να αναμειγνύει διευθύνσεις Bitcoin, αλλά αυτό το τρίτο μέρος μπορεί να παραβιάσει το απόρρητο των χρηστών και να κλέψει τα bitcoins των χρηστών, η κλοπή εντοπίζεται αλλά δεν αποτρέπεται.

Το Blindcoin, (Valenta & Rowan, 2015), είναι βελτίωση του Mixcoin διατηρώντας την ιδιωτικότητα των χρηστών έναντι της υπηρεσίας ανάμιξης, αλλά όπως συμβαίνει και με το Mixcoin, η κλοπή εξακολουθεί να μην εμποδίζεται. Το CoinParty, (Ziegeldorf et al, 2015), είναι ασφαλές αν 2/3 από τα μέρη ανάμιξης είναι ειλικρινά.

Το CoinJoin, (Maxwell, 2013), και το CoinShuffle, (Ruffing et al, 2014), είναι βελτιώσεις ως προς την προηγούμενη εργασία, εμποδίζοντας την κλοπή. Η εργασία των Meiklejohn & Orlandi, (2015), δείχνει μια αυστηρή απόδειξη ανωνυμίας για ένα σχήμα "σχεδόν ταυτόσημο" με το CoinShuffle. Το σύνολο ανωνυμίας του CoinShuffle θεωρείται μικρό λόγω των εξόδων συντονισμού, (Bissias et al, 2014).

Εν τω μεταξύ, τα σχήματα των Heilman et al, (2016), δεν περιορίζονται σε μικρά σύνολα ανωνυμίας. Επιπλέον, τόσο το Coin-Shuffle όσο και το CoinJoin τρέχουν ένα ολόκληρο μείγμα σε μια συναλλαγή bitcoin. Έτσι, ένας και μοναδικός χρήστης που διακόπτει τη λειτουργία του διακόπτει το μείγμα για όλους τους άλλους χρήστες.

Επιπλέον, οι συνδυασμοί χρηστών δεν μπορούν να υποχρεωθούν να πληρώσουν προκαταβολικά τέλη, έτσι ώστε τα συστήματα αυτά είναι ευάλωτα σε επιθέσεις DoS (Bonneau et al, 2015), (όπου οι χρήστες ενώνουν το μίγμα και στη συνέχεια τερματίζουν) και σε επιθέσεις Sybil (όπου ένας αντίπαλος φανερώνει έναν χρήστη, αναγκάζοντας τον να αναμιχθεί με Sybil οντότητες που είναι κρυφά υπό τον έλεγχό της), (Bissias et al, 2014).

Το XIM, (Bissias et al, 2014), είναι ένα αποκεντρωμένο πρωτόκολλο το οποίο βασίζεται στον μίκτη δίκαιης ανταλλαγής, (Barber et al, 2012), και αποτρέπει την κλοπή bitcoin και αντιστέκεται στις επιθέσεις DoS και Sybil μέσω τελών. Επίσης οι Heilman et al, (2016), αποτρέπουν τις κλοπές bitcoin και αντιστέκονται στις επιθέσεις DoS και Sybil με τέλη. Ένα από τα κλειδιά του XIM είναι μια ασφαλής μέθοδος για τη συνένωση των χρηστών της μίξης. Δυστυχώς, αυτή η μέθοδος συνεργασίας προσθέτει αρκετές ώρες στην εκτέλεση του πρωτοκόλλου, επειδή οι χρήστες πρέπει να διαφημίζουν τους εαυτούς τους ως συνεργάτες μίξης στο Blockchain. Τα σχήματα των Heilman et al, (2016) είναι ταχύτερα, επειδή δεν απαιτούν υπηρεσία συνεργατών.

Το CoinSwap, (Maxwell, 2013), είναι ένας μίκτης δίκαιης ανταλλαγής που επιτρέπει σε δύο μέρη να αποστέλλουν ανώνυμα Bitcoins μέσω ενδιάμεσου φορέα. Όπως και στα σχήματα των Heilman et al, (2016), ο διαμεσολαβητής του CoinSwap εμποδίζεται να κλέβει κεφάλαια με τη χρήση δίκαιης ανταλλαγής. Αντίθετα από τα συστήματά των Heilman et al, (2016), ωστόσο, το CoinSwap δεν παρέχει ανωνυμία εναντίον ακόμη και ενός έντιμου αλλά περίεργου μεσάζοντα.

Το σχήμα Blockchain των Heilman et al, (2016), διαρκεί περίπου 30 λεπτά, δηλαδή είναι πιο αργό από τα 10 λεπτά του Coinshuffle. Ωστόσο, το off-Blockchain σχέδιό των Heilman et al, (2016), είναι ταχύτερο από το CoinShuffle, καθώς λειτουργεί μόνο σε δευτερόλεπτα, (Poon & Dryja, 2015). Ωστόσο, το off-Blockchain σχήμα των Heilman et al, (2016), υποστηρίζει μόνο την ανωνυμία ενάντια σε έναν ειλικρινή αλλά περίεργο μεσάζοντα.

Τα κρυπτονομίσματα όπως το Bitcoin, (Nakamoto, 2009), και τα altcoins, (Bonneau et al, 2015), έχουν αποκτήσει γρήγορα δημοτικότητα και συχνά αναφέρονται ως μια ματιά στο μέλλον, (The rise and rise of bitcoin. Documentary). Αυτά τα αναδυόμενα συστήματα κρυπτονομισμάτων οικοδομούνται πάνω από μια νέα τεχνολογία Blockchain όπου οι κόμβοι ελέγχου συναίνεσης (miners) διατρέχουν τη κατανεμημένη συναίνεση της οποίας η ασφάλεια εξασφαλίζεται αν κανένα μέρος δεν ασκεί μεγάλο μέρος των υπολογιστικών (ή άλλων μορφών) πόρων. Συνεπώς, οι όροι "Blockchain" και "miners" χρησιμοποιούνται συχνά εναλλακτικά.

Τα Blockchains όπως το Bitcoin καταλήγουν σε συναίνεση όχι μόνο σε μια ροή δεδομένων αλλά και σε υπολογισμούς που περιλαμβάνουν αυτά τα δεδομένα. Στο Bitcoin, συγκεκριμένα, τα δεδομένα περιλαμβάνουν τη συναλλαγή μεταφοράς χρημάτων που προτείνουν οι χρήστες και ο υπολογισμός περιλαμβάνει την επικύρωση συναλλαγής και την ενημέρωση μιας δομής δεδομένων που ονομάζεται σύνολο μη εξερχόμενων συναλλαγών, το οποίο, παρακολουθεί τα υπόλοιπα των λογαριασμών των χρηστών.

Τα νεοεμφανιζόμενα συστήματα κρυπτονομισμάτων, όπως το Ethereum, (Wood, "Ethereum: A secure decentralized transaction ledger"), αγκαλιάζουν την ιδέα της εκτέλεσης αυθαίρετων προγραμμάτων που ορίζονται από το χρήστη στο Blockchain, δημιουργώντας έτσι ένα εκφραστικό αποκεντρωμένο σύστημα έξυπνης σύμβασης.

Η εκφραστική δύναμη του Blockchain ενισχύεται περαιτέρω από το γεγονός ότι τα Blockchain ενσωματώνουν φυσικά μια διακριτή έννοια του χρόνου, δηλαδή ένα ρολόι που αυξάνεται κάθε φορά που εξορύσσετε ένα νέο μπλοκ. Η ύπαρξη ενός τέτοιου αξιόπιστου ρολογιού είναι ζωτικής σημασίας για την επίτευξη οικονομικής δικαιοσύνης στα πρωτόκολλα.

Συγκεκριμένα, τα κακόβουλα συμβαλλόμενα μέρη ενδέχεται να αποποιηθούν πρόωρα από ένα πρωτόκολλο για να αποφύγουν την πληρωμή χρημάτων. Ωστόσο, με ένα αξιόπιστο ρολόι, μπορούν να χρησιμοποιηθούν χρονικά όρια για να καταστούν εμφανείς τέτοιες διακοπές, έτσι ώστε το Blockchain να μπορεί να τιμωρήσει οικονομικά τα μέρη που αποποιούνται, ανακατανέμοντας τις εξασφαλιστικές τους καταθέσεις σε έντιμα μέρη που δεν αποποιούνται από το πρωτόκολλο. Αυτό καθιστά το μοντέλο κρυπτογραφίας του Blockchain πιο ισχυρό από το παραδοσιακό μοντέλο χωρίς Blockchain, όπου η δικαιοσύνη είναι από καιρό γνωστό ότι είναι αδύνατη εν γένει όταν η πλειονότητα των μερών μπορεί να είναι διεφθαρμένη, (Cleve, 1986). Εν ολίγοις, τα Blockchains επιτρέπουν στα μέρη να γνωρίζουν αμοιβαία ότι μπορούν να συναλλάσσονται με ασφάλεια χωρίς έναν κεντρικό αξιόπιστο ενδιάμεσο και να αποφεύγουν υψηλό νομικό και συναλλακτικό κόστος.

Παρά την εκφραστικότητα και τη δύναμη του Blockchain και των έξυπνων συμβάσεων, η σημερινή μορφή αυτών των τεχνολογιών στερείται της ιδιωτικότητας των συναλλαγών. Η όλη αλληλουχία των ενεργειών που λαμβάνονται σε μία έξυπνη σύμβαση διαδίδεται σε όλο το δίκτυο και / ή καταγράφεται στο Blockchain και ως εκ τούτου είναι δημόσια ορατή. Παρόλο που τα μέρη μπορούν να δημιουργήσουν νέα ψευδώνυμα δημόσια κλειδιά για να αυξήσουν την ανωνυμία τους, οι τιμές όλων των συναλλαγών και υπολοίπων για κάθε (ψευδώνυμο) δημόσιο κλειδί είναι δημόσια ορατές. Περαιτέρω, πρόσφατα έργα έχουν επίσης επιδείξει επιθέσεις άρσης ανωνυμίας με την ανάλυση των δομών γραφημάτων των συναλλαγών των κρυπτονομισμάτων, (Meiklejohn et al, 2013).

2.5 Δίκτυα καναλιών μικροπληρωμών

Κανάλια μικροπληρωμών: Για να δημιουργηθεί ένα κανάλι μικροπληρωμών ανά ζεύγος, τα A και B πληρώνουν το καθένα κάποια ποσότητα bitcoins σε μια συναλλαγή μεσεγγύησης Te η οποία είναι καταχωρημένη στο Blockchain. Αυτή η συναλλαγή μεσεγγύησης είναι σε Blockchain και επομένως αργή (≈ 10 λεπτά), αλλά όλες οι επόμενες συναλλαγές είναι off-Blockchain και ως εκ τούτου γρήγορες (≈ δευτερόλεπτα).

Η Te εξασφαλίζει ότι κανένας από τους συμμετέχοντες δεν θα αποκαταστήσει τη συναλλαγή εκτός Blockchain. Ας υποτεθεί ότι x bitcoins πληρώνονται στο Te. Το Te προσφέρει αυτά τα x bitcoins να δαπανηθούν υπό την προϋπόθεση: "Οι δαπάνες της συναλλαγής να υπογράφονται από τον A και τον B ". Στη συνέχεια, η συναλλαγή δαπανών Tr έχει τη μορφή: "a bitcoins πληρώνονται στον A και b bitcoins πληρώνονται στον B" όπου a και b αντικατοπτρίζουν τη συμφωνηθείσα ισορροπία bitcoins μεταξύ των A και B.

Μόλις επιβεβαιωθεί η Te στο Blockchain, τα A και B μπορούν να μεταφέρουν κεφάλαια μεταξύ τους εκτός Blockchain υπογράφοντας μια συναλλαγή δαπανών Tr. Είναι σημαντικό ότι το Tr δεν δημοσιεύτηκε στο Blockchain. Αντ 'αυτού, η ύπαρξη του Tr δημιουργεί μια αξιόπιστη απειλή όπου κάθε συμβαλλόμενο μέρος μπορεί να διεκδικήσει τα κατανεμημένα bitcoins τους δημοσιεύοντας το Tr στο Blockchain. Αυτό εμποδίζει οποιοδήποτε από τα μέρη να αποφύγουν την κατανομή που αντικατοπτρίζεται στο Tr. Για να συνεχίσει να κάνει πληρωμές off-Blockchain, τα A και B πρέπει απλώς να υπογράψουν μια νέα συναλλαγή Tr που αντικατοπτρίζει τη νέα ισορροπία bitcoins a΄ και b΄.

Τα κανάλια μικροπληρωμών διαθέτουν μηχανισμούς που εξασφαλίζουν ότι αυτή η μεταγενέστερη συναλλαγή T΄r αντικαθιστά πάντα μια προηγούμενη συναλλαγή Tr. Το πρωτόκολλό των Heilman et al, (2016), εφαρμόζεται γενικά σε οποιοδήποτε κανάλι μικροπληρωμών με έναν τέτοιο μηχανισμό, π.χ., Lightning Network, (Poon & Dryja, 2015), Duplex Micropayment Channels (DMC), (Decker & Wattenhofer, 2015).

Δίκτυα καναλιών μικροπληρωμών: Τα δίκτυα καναλιών μικροπληρωμών έχουν σχεδιαστεί για να αποφεύγεται η απαίτηση από κάθε ζεύγος μερών να προκαθορίζουν ένα κανάλι μικροπληρωμών ανά ζεύγος μεταξύ τους. Πράγματι, μια τέτοια απαίτηση θα ήταν ανέφικτη, καθόσον απαιτεί το καθένα ζεύγος χρηστών να κλειδώνουν κεφάλαια σε πολλές διαφορετικές συναλλαγές μεσεγγύησης Te στο Blockchain.

Αντ 'αυτού, ας υποτεθεί ότι ένα ζεύγος χρηστών A και B συνδέονται με ένα μονοπάτι των χρηστών με εγκατεστημένα ζευγαρωτά κανάλια μικροπληρωμών (δηλαδή, ο A έχει ένα κανάλι με τον A1, ο A1 έχει ένα κανάλι με τον A2, ..., ο Am-1 έχει ένα κανάλι με τον Am, ο Am έχει κανάλι με τον B). Στη συνέχεια, η διαδρομή των χρηστών μπορεί να εκτελέσει ένα πρωτόκολλο για τη μεταφορά χρημάτων από τον A στον B. Ωστόσο, δεν αρκεί να πρέπει ο κάθε χρήστης Ai να δημιουργήσει μια συναλλαγή πληρώνοντας τον επόμενο χρήστη Ai + 1 στη διαδρομή, αφού ένας κακόβουλος χρήστης Ak θα μπορούσε να κλέβει κεφάλαια παραλείποντας να δημιουργήσει μια συναλλαγή a για τον Ak + 1. Αντίθετα, το Lightning Network και το DMC χρησιμοποιούν ένα πρωτόκολλο που βασίζεται σε συμβόλαια που έχουν χρονομετρηθεί με hash (ίχνος) ή HTLC. Μια συναλλαγή T είναι ένα HTLC αν προσφέρει bitcoins υπό την προϋπόθεση: "Η συναλλαγή δαπανών πρέπει να περιέχει την προϋπόθεση του y και να επιβεβαιωθεί εντός του χρονικού περιγράμματος tw", όπου το y = H (χ) και το x είναι τυχαία τιμή, δηλ.η προϋπόθεση. Λέμε ότι το T είναι κλειδωμένο υπό την προϋπόθεση του y.

Τα κανάλια μικροπληρωμών χρησιμοποιούν τα HTLC ως εξής. Ας υποτεθεί η υπάρχουσα ισορροπία μεταξύ A και B να είναι a bitcoin για τον A και b bitcoin για τον B. Ας υποτεθεί τώρα ότι το A θέλει να μεταφέρει e bitcoin στον B, ενημερώνοντας τα υπόλοιπα σε a-e και b +e. Πρώτον, ο B επιλέγει τυχαία τιμή x, υπολογίζει το y = H (x) και ανακοινώνει y σε όλους στη διαδρομή. Στη συνέχεια, ο A ρωτά κάθε ζεύγος συμβαλλόμενων μερών (Ai, Ai + 1) στο μονοπάτι για να μεταφέρει e bitcoin που είναι κλειδωμένα κάτω από την πρόβλεψη του y χρησιμοποιώντας το κανάλι μικροπληρωμής από τον Ai στον Ai + 1. Ο μηχανισμός της μεταφοράς μεταξύ Ai και Ai + 1 έχει ως εξής. Ας υποτεθεί ότι η υπάρχουσα ισορροπία μεταξύ Ai και Ai + 1 είναι c bitcoin για τον Ai και d bitcoin για τον Ai + 1. Στη συνέχεια, οι Ai και Ai + 1 υπογράφουν από κοινού μια νέα συναλλαγή δαπανών T΄r της φόρμας "c-e bitcoins πληρώνονται στον Ai και d +e _bitcoins πληρώνονται στον Ai + 1" με την προϋπόθεση ότι "η συναλλαγή δαπανών περιέχει την προϋπόθεση y μέσα στο χρονικό παράθυρο tw ".

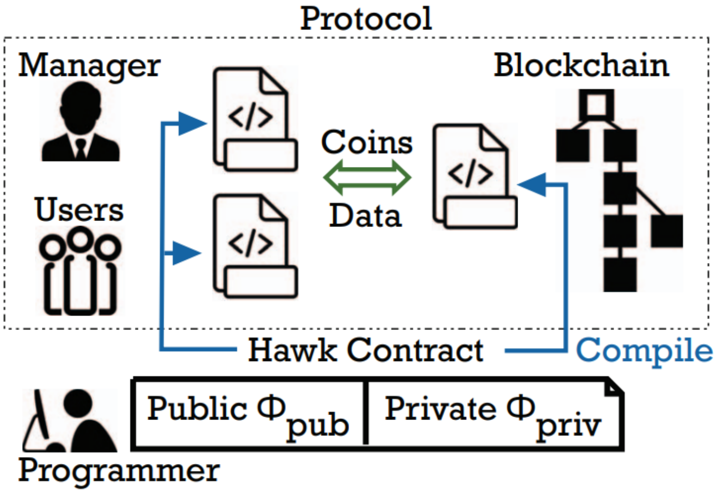
Μόλις ο A βλέπει ότι όλες οι συναλλαγές στο μονοπάτι έχουν υπογραφεί, απελευθερώνει την προϋπόθεση του x στη διαδρομή και τη ροή κεφαλαίων από Ai σε Aj. Εάν οποιοσδήποτε χρήστης αρνείται να υπογράψει μια συναλλαγή, ο χρονοδιακόπτης tw επιτρέπει σε όλους τους υπογράφοντες χρήστες να ανακτήσουν τα χρήματά τους. Ο χρονοδιακόπτης μειώνεται κατά μήκος της διαδρομής για να αποφευχθούν οι συνθήκες της κούρσας. Το όλο πρωτόκολλο παρουσιάζεται εκτός Blockchain, με το x και τα HTLC να δημιουργούν μια αξιόπιστη απειλή ότι οι χρήστες μπορούν να ανακτήσουν τα χρήματά τους αν αναρτηθούν στο Blockchain.

2.6 Πλαίσιο οικοδόμησης έξυπνων συμβάσεων

Το Hawk είναι ένα πλαίσιο για την οικοδόμηση έξυπνων συμβάσεων που διατηρούν την ιδιωτικότητα. Με το Hawk, ένας μη εξειδικευμένος προγραμματιστής μπορεί εύκολα να γράψει ένα πρόγραμμα Hawk χωρίς να χρειάζεται να εφαρμόσει κρυπτογραφία. Ο μεταγλωττιστής του Hawk είναι υπεύθυνος για την κατάρτιση του προγράμματος σε κρυπτογραφικό πρωτόκολλο μεταξύ του Blockchain και των χρηστών. Ένα πρόγραμμα Hawk περιλαμβάνει δύο μέρη:

- Ένα ιδιωτικό τμήμα που δηλώνεται ως φpriv το οποίο λαμβάνει δεδομένα εισόδου των μερών (π.χ. επιλογές σε παιχνίδι πέτρα, χαρτί, ψαλίδι) καθώς και νομισματικές μονάδες (π.χ. προσφορές σε δημοπρασία). Το φpriv εκτελεί υπολογισμό για να καθορίσει την κατανομή των πληρωμών μεταξύ των μερών. Για παράδειγμα, σε μια δημοπρασία, η προσφορά του νικητή μεταβιβάζεται στον πωλητή και επιστρέφονται οι προσφορές των άλλων. Το ιδιωτικό πρόγραμμα φpriv του Hawk αποσκοπεί στην προστασία των δεδομένων των συμμετεχόντων και στην ανταλλαγή χρημάτων.
- Μία δημόσια μερίδα που δηλώνεται ως φpub που δεν αγγίζει ιδιωτικά δεδομένα ή χρήματα. Ο μεταγλωττιστής θα μεταγλωττίσει το πρόγραμμα Hawk στα ακόλουθα κομμάτια τα οποία ορίζουν από κοινού ένα κρυπτογραφικό πρωτόκολλο μεταξύ χρηστών, του διαχειριστή και του Blockchain:

- το πρόγραμμα Blockchain που θα εκτελεστεί από όλους τους κόμβους συναίνεσης.
- ένα πρόγραμμα που πρέπει να εκτελεστεί από τους χρήστες.
- ένα πρόγραμμα που θα εκτελεστεί από ένα ειδικό διευκολυνόμενο μέρος που ονομάζεται διευθυντής-manager.



Σχήμα 2-2. Δομή του συμβολαίου Hawk.

2.7 Επίλογος

Μια έξυπνη σύμβαση αποτελεί έναν εκτελέσιμος κώδικας που τρέχει στο Blockchain για να διευκολύνει, να εκτελέσει και να επιβάλει τους όρους μιας συμφωνίας, με στόχο να εκτελεστούν αυτομάτως οι όροι της συμφωνίας όταν πληρούνται οι καθορισμένοι όροι. Οι έξυπνες συμβάσεις μπορούν να αναπτυχθούν και να τρέξουν σε διαφορετικές πλατφόρμες Blockchain, όπως το Ethereum, το Bitcoin και το NXT. Το Bitcoin είναι μια δημόσια πλατφόρμα Blockchain που μπορεί να χρησιμοποιηθεί για την επεξεργασία κρυπτογραφικών συναλλαγών, αλλά με μια πολύ περιορισμένη ικανότητα υπολογισμού. Το Bitcoin χρησιμοποιεί μια γλώσσα προγραμματισμού που βασίζεται σε δέσμη ενεργειών bytecode. Υπάρχουν διάφορες πιθανές εφαρμογές στις οποίες μπορούν να εφαρμοστούν έξυπνες συμβάσεις, όπως το IoT στο οποίο υπάρχουν δισεκατομμύρια κόμβοι που μοιράζονται δεδομένα μεταξύ τους μέσω του Διαδικτύου και η διαχείριση δικαιωμάτων μουσικής, όπου μια έξυπνη σύμβαση μπορεί να επιβάλει την πληρωμή για τους ιδιοκτήτες μουσικής για τη χρήση μουσικής για εμπορικούς σκοπούς. Επιπλέον, μια άλλη εφαρμογή των έξυπνων συμβάσεων συναντάται στο ηλεκτρονικό εμπόριο, όπου μια πιθανή περίπτωση χρήσης είναι να διευκολυνθεί το εμπόριο μεταξύ μη πιστωτικών μερών χωρίς πιστωτικό τρίτο μέρος. Οι έξυπνες συμβάσεις μπορούν να αποδεσμεύσουν την πληρωμή στον πωλητή μόλις ο αγοραστής είναι ικανοποιημένος με το προϊόν ή την υπηρεσία που έλαβε).

Κεφάλαιο 3ο: Βιβλιογραφική ανασκόπηση τεχνολογιών Blockchain και Έξυπνων Συμβολαίων στα IoT

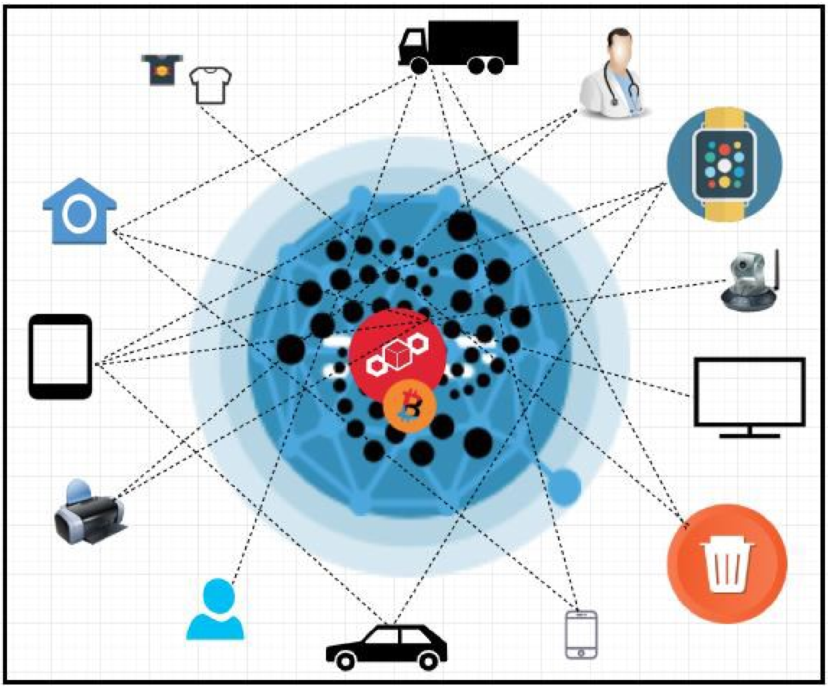
3.1 Εισαγωγή

Το Blockchain (BC) στο Διαδίκτυο των πραγμάτων (Internet of Things -IoT) είναι μια νέα τεχνολογία που λειτουργεί με αποκεντρωμένο, διανεμημένο, δημόσιο και σε πραγματικό χρόνο καθολικό (ledger) για την αποθήκευση συναλλαγών μεταξύ κόμβων IoT. Ένα Blockchain είναι μια σειρά μπλοκ όπου κάθε μπλοκ συνδέεται με τα προηγούμενα. Κάθε ένα έχει τον κρυπτογραφικό κωδικό κατακερματισμού, τον προηγούμενο κατακερματισμό και τα δεδομένα του. Οι συναλλαγές σε BC είναι οι βασικές μονάδες που χρησιμοποιούνται για τη μεταφορά δεδομένων μεταξύ των κόμβων IoT. Οι κόμβοι IoT είναι διαφορετικού είδους φυσικές αλλά έξυπνες συσκευές με ενσωματωμένους αισθητήρες, ενεργοποιητές, προγράμματα και είναι ικανοί να επικοινωνούν με άλλους κόμβους IoT. Ο ρόλος του BC στο IoT είναι να παρέχει μια διαδικασία επεξεργασίας ασφαλών αρχείων δεδομένων μέσω κόμβων IoT. Η BC είναι μια ασφαλής τεχνολογία που μπορεί να χρησιμοποιηθεί δημόσια και ανοιχτά. Το IoT απαιτεί τέτοιου είδους τεχνολογία για να επιτρέπει την ασφαλή επικοινωνία μεταξύ κόμβων IoT σε ετερογενές περιβάλλον. Οι συναλλαγές στο BC θα μπορούσαν να εντοπιστούν και να διερευνηθούν μέσω όσων έχουν πιστοποιηθεί για επικοινωνία εντός του IoT. Το BC στο IoT μπορεί να βοηθήσει στη βελτίωση της ασφάλειας επικοινωνίας.

Τα IoT και τα BC αυξάνουν τις επιχειρηματικές ευκαιρίες και ανοίγματα στις νέες αγορές όπου όλοι και όλα μπορούν να επικοινωνήσουν σε πραγματικό χρόνο με γνησιότητα, απόρρητο και ασφάλεια με μία αποκεντροποιημένη προσέγγιση. Η ενσωμάτωση αυτής της νέας τεχνολογίας πρόκειται να αλλάξει τον σημερινό κόσμο αφού οι συσκευές θα μπορούν να επικοινωνούν χωρίς την ανθρώπινη μεσολάβηση, σε διάφορα επίπεδα. Ο σκοπός του πλαισίου είναι να λάβει τα ασφαλή δεδομένα στη σωστή τοποθεσία, με τη σωστή μορφή, σε πραγματικό χρόνο. Το BC θα μπορούσε να χρησιμοποιηθεί στο να ανιχνεύει δισεκατομμύρια συνδεδεμένων IoT, να τα συντονίζει, να επιτρέπει τη διαδικασία των συναλλαγών, να επιλύει ή να περιορίζει τα σφάλματα και να φτιάχνει το ευέλικτο οικοσύστημα όπου θα τρέχουν τα φυσικά πράγματα. Οι τεχνικές κατακερματισμού χρησιμοποιούνται σε ομάδες δεδομένων από τα BC για τη δημιουργία απορρήτου πληροφοριών για τους χρήστες

3.2 Blockchain και IoT

Το IoT αναπτύσσεται εκθετικά χρόνο με το χρόνο με στόχο τις τεχνολογίες 5G, όπως Smart Homes and Cities, e-Health, κατανεμημένη νοημοσύνη κ.λπ., αλλά έχει προκλήσεις στον τομέα της ασφάλειας και της ιδιωτικής ζωής. Οι συσκευές IoT συνδέονται με αποκεντρωμένη προσέγγιση. Έτσι, καθίσταται πολύπλοκη η χρήση των τυπικών υπαρχουσών τεχνικών ασφαλείας στην επικοινωνία μεταξύ των κόμβων IoT. Το BC είναι μια τεχνολογία που παρέχει την ασφάλεια στις συναλλαγές μεταξύ των συσκευών IoT. Παρέχει ένα αποκεντρωμένο, διανεμημένο και κοινόχρηστο καθολικό για την αποθήκευση των δεδομένων των μπλοκ που υποβάλλονται σε επεξεργασία και επαληθεύονται σε ένα δίκτυο IoT. Η διαχείριση των δεδομένων που αποθηκεύονται στο δημόσιο καθολικό γίνεται αυτόματα χρησιμοποιώντας την τοπολογία Peer-to-peer. Το BC είναι μια τεχνολογία όπου οι συναλλαγές ενεργοποιούνται με τη μορφή μπλοκ στο BC μεταξύ κόμβων IoT. Τα μπλοκ συνδέονται μεταξύ τους και κάθε συσκευή κρατά την προηγούμενη διεύθυνση της συσκευής. Το Blockchain και το IoT λειτουργούν μαζί στο πλαίσιο ολοκλήρωσης IoT και Cloud. Στο μέλλον, το BC θα φέρει επανάσταση στην επικοινωνία IoT (Reyna et al., 2018). Οι στόχοι της ενσωμάτωσης BC και IoT θα μπορούσαν να συνοψιστούν ως εξής.

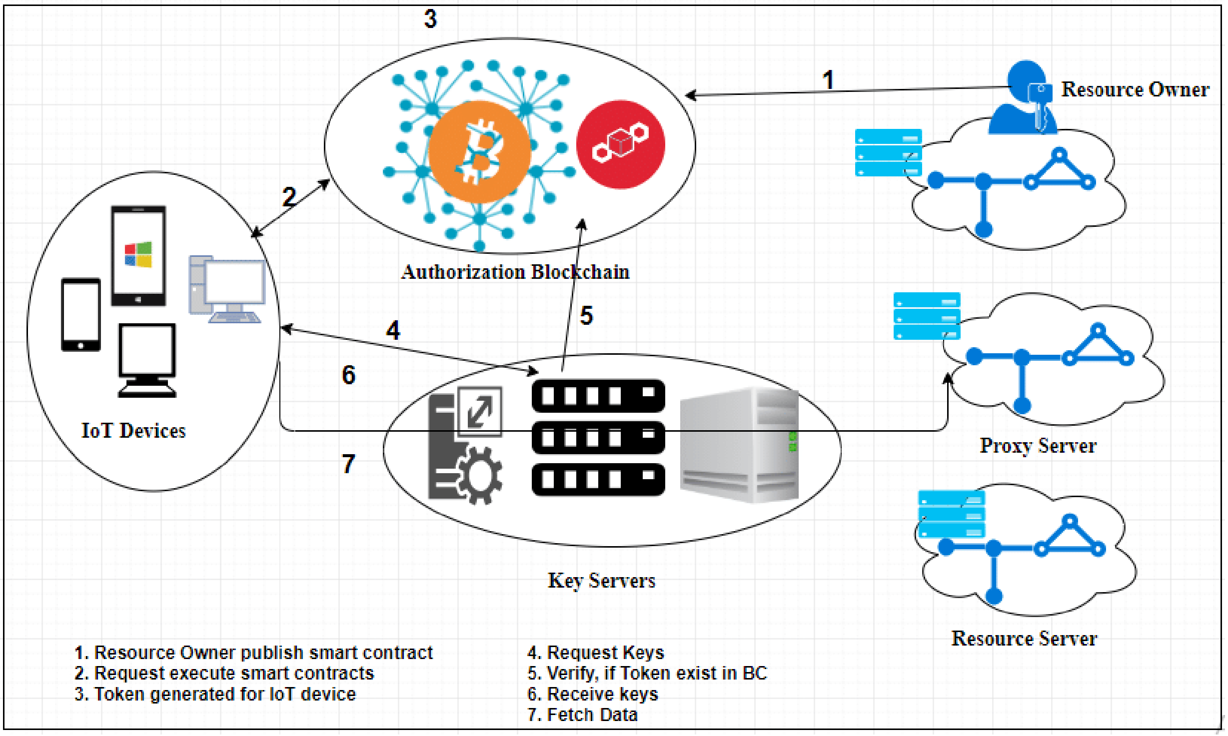


Σχήμα 3-1. Blockchain και IoT

- Αποκεντρωμένο πλαίσιο: Αυτή η προσέγγιση είναι παρόμοια σε IoT και BC. Αφαιρείται το κεντρικό σύστημα και παρέχει τη δυνατότητα αποκεντρωμένου συστήματος. Βελτιώνει την πιθανότητα αστοχίας και την απόδοση του συνολικού συστήματος
- Ασφάλεια: Στο BC, οι συναλλαγές μεταξύ κόμβων είναι ασφαλείς. Πρόκειται για μια πολύ νέα προσέγγιση για ασφαλή επικοινωνία. Το BC επιτρέπει στις συσκευές IoT να επικοινωνούν μεταξύ τους με ασφαλή τρόπο.
- Αναγνώριση: Στο IoT, όλες οι συνδεδεμένες συσκευές ταυτοποιούνται μοναδικά με μία μοναδική ταυτότητα (ID) . Κάθε μπλοκ στο BC ταυτοποιείται επίσης μοναδικά. Έτσι, το BC είναι μια αξιόπιστη τεχνολογία που παρέχει μοναδικά ταυτοποιημένα δεδομένα αποθηκευμένα σε δημόσιο καθολικό.
- Αξιοπιστία: Οι κόμβοι IoT στο BC έχουν τη δυνατότητα πιστοποίησης των πληροφοριών που διαβιβάζονται στο δίκτυο. Τα δεδομένα είναι αξιόπιστα επειδή επαληθεύονται από τους χρήστες πριν εισέλθουν στο BC. Μόνο επαληθευμένα μπλοκ μπορούν να εισέλθουν στο BC.

- Αυτονομία : Στο BC, όλοι οι κόμβοι IoT είναι ελεύθεροι να επικοινωνούν με οποιονδήποτε κόμβο στο δίκτυο χωρίς το κεντρικό σύστημα.
- Επεκτασιμότητα: Στο BC, οι συσκευές IoT θα επικοινωνούν σε υψηλά διαθέσιμα, κατανεμημένα δίκτυα πληροφοριών που συνδέονται με τη συσκευή προορισμού σε πραγματικό χρόνο και ανταλλάσσουν πληροφορίες.

Η ασφάλεια και το απόρρητο στην επικοινωνία μεταξύ συσκευών IoT ήταν οι μεγάλες προτεραιότητες κατά τα έτη 2017 και 2018. Πολλές μελέτες δημοσιεύτηκαν αυτά τα χρόνια. Το 1990, οι Stuart Haber και W. Scott Stornetta έγραψαν ένα άρθρο (Haber & Stornetta,1990), σχετικά με την ανταλλαγή εγγράφου με απόρρητο χωρίς να αποθηκεύονται πληροφορίες στην υπηρεσία χρονικής σήμανσης. Η ιδέα των BC πρωτοεμφανίστηκε στη μελέτη των (Haber & Stornetta, 1990) αλλά τα πρώτα BC παρουσιάστηκαν από τον Satoshi Nakamoto το 2008. Στην εργασία του (Nakamoto, 2008) παρουσίασε μία μελέτη όπου τα μπλοκς προστέθηκαν σε μία αλυσίδα και σχημάτισαν μία αλυσίδα με μπλοκ. Στο άρθρο των (Alphand et al., 2018), οι συγγραφείς παρουσίασαν το διαδίκτυο των πραγμάτων αλυσίδας (IoTChain) για ταυτοποίηση της προς ανταλλαγή πληροφορίας μεταξύ δύο κόμβων στο διαδίκτυο IoT. Παρουσίασαν έναν αλγόριθμο για να ανταλλάξουν την πληροφορία στο IoT και στα BC (ακόλουθο σχήμα) (Alphand et al., 2018). Στη μελέτη του ο (Tanweer Alam, 2019) ήταν επικεντρωμένος στο κομμάτι της εξουσιοδότησης της ασφάλειας στο πλαίσιο IoTChain



Σχήμα 3-2. Πλαίσιο IoTChain

Στην εργασία των (Alam & Benaida, 2019), ερευνήθηκε το πλαίσιο cloud και MANET για τη σύνδεση των έξυπνων συσκευών στο διαδίκτυο των πραγμάτων (IoT) και την παροχή ασφάλειας στην επικοινωνίας. Στο άρθρο τους οι (Alam & Benaida, 2018) παρουσίασαν ένα πολύ ωραίο πλαίσιο που ονομάζεται internet-cloud framework, πρόκειται για μια καλή ιδέα για παροχή ασφαλούς επικοινωνίας στις συσκευές IoT. Στο άρθρο του ο (Alam 2017), παρείχε ένα πλαίσιο ενδιάμεσου λογισμικού στην αρχιτεκτονική cloud-MANET για πρόσβαση σε δεδομένα μεταξύ των συσκευών IoT. Η μελέτη των (Alam, 2018),(Alam & Benaida, (2018) αντιπροσώπευσε την αξιοπιστία στην επικοινωνία μεταξύ των κόμβων IoT. Στα άρθρα (Alam et al., 2010), (Alam et al., 2014) (Alam &Sharma, 2010), (Singh et al., 2014), (Sharma et al.,2008) παρουσιάζονται τα μοντέλα κινητικότητας για επικοινωνία σε δίκτυα 5G. Στην εργασία του ο (Alam, 2017), ανέλυσε το πλαίσιο κινητικότητας που βασίζεται σε ασαφή λογική για την ασφάλεια στην επικοινωνία. Στο άρθρο τους οι (Conoscenti et al., 2016), παρουσίασαν μια καλή έρευνα για τις BC και το IoT. Ανέλυσαν την ιδέα της ασφάλειας στο BC-IoT για την ανάπτυξη των εφαρμογών IoT με τη δύναμη των BC.

Ο ρόλος του BC στο IoT

Το IoT επιτρέπει στα συνδεδεμένα φυσικά αντικείμενα να ανταλλάξουν τις πληροφορίες τους στο ετερογενές δίκτυο (Gubbi et al., 2013). Το IoT θα μπορούσε να διαιρεθεί στους ακόλουθους τομείς:

- Φυσικά πράγματα: Το IoT παρέχει μία μοναδική ID για κάθε συνδεδεμένο πράγμα στο δίκτυο. Τα φυσικά πράγματα μπορούν να ανταλλάσσουν δεδομένα με άλλους IoT κόμβους.
- Gateways: Οι πύλες είναι οι συσκευές που λειτουργούν μεταξύ φυσικών πραγμάτων και του νέφους (cloud) για να διασφαλιστεί ότι η σύνδεση έχει δημιουργηθεί και ότι παρέχεται ασφάλεια στο δίκτυο.
- Δικτύωση: χρησιμοποιείται για τον έλεγχο της ροής δεδομένων και για τη δημιουργία της συντομότερης διαδρομής μεταξύ των κόμβων IoT.
- Cloud: Χρησιμοποιείται για την αποθήκευση και τον υπολογισμό των δεδομένων.

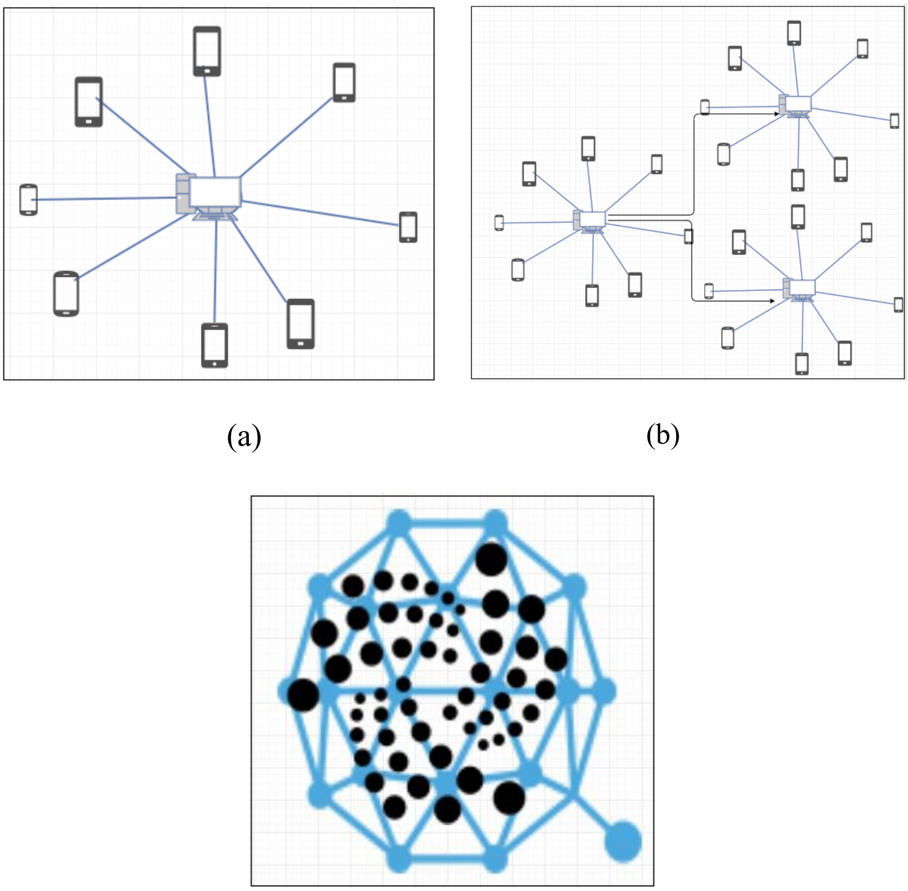
Το BC είναι μια αλυσίδα επαληθευμένων και κρυπτογραφικών μπλοκ συναλλαγών που κατέχονται από τη συσκευή που είναι συνδεδεμένη σε ένα δίκτυο. Τα δεδομένα μπλοκ αποθηκεύονται στο ψηφιακό καθολικό που κοινοποιείται και διανέμεται δημόσια. Το BC παρέχει ασφαλή επικοινωνία στο δίκτυο IoT. Το Blockchain μπορεί να είναι ιδιωτικό, δημόσιο ή Κοινοπραξία BC με διαφορετικές ιδιότητες. Ο ακόλουθος πίνακας αντιπροσωπεύει τη διαφοροποίηση μεταξύ όλων των ειδών των Blockchain.

Πίνακας 3.1. Είδη BC και οι ιδιότητές τους

BC/ Ιδιότητες	**Αποδοτι-Κότητα**	**Αποκε-ντρωμένο**	**Ανάπτυξη Συμφωνιών**	**Ακίνητο**	**Διάβασμα**	**Καθορισμός**
Ιδιωτικό BC	Καλή	Όχι	Ναι	Είναι πιθανό	Μπορεί να είναι δημόσια	Μόνο μία βιομηχανία

Δημόσιο BC	Χειρότερη	Ναι	Όχι	Όχι	Δημόσια	All miners
Κοινοπραξία BC	Καλή	Μερικές φορές	Ναι	Είναι πιθανό	Μπορεί να είναι δημόσια	IoT συσκευές

Η βάση δεδομένων σε Blockchains έχει ιδιότητες όπως το αποκεντρωμένο μοντέλο εμπιστοσύνης, υψηλή ασφάλεια, υψηλή πρόσβαση στο κοινό, το απόρρητο είναι από χαμηλό σε υψηλό και οι ταυτότητες είναι μεταβιβάσιμες ενώ σε μια κεντρική βάση δεδομένων, οι ιδιότητες που τις χαρακτηρίζουν είναι το κεντρικό μοντέλο εμπιστοσύνης, η χαμηλή ασφάλεια, η χαμηλή πρόσβαση στο κοινό, ενώ το απόρρητο είναι υψηλού βαθμού και οι ταυτότητες μη μεταβιβάσιμες. Από τις παραπάνω ιδιότητες, το Blockchain είναι πιο προηγμένο από τον κεντρικό χώρο αποθήκευσης.



(a) (b) (c)

Σχήμα 3-3. (a) Κεντρικό (b) Αποκεντροποιημένο (c) Κατανεμημένο

Οι παραπάνω πλατφόρμες χρησιμοποιούνται για την ανάπτυξη εφαρμογών IoT με τη χρήση τεχνολογίας BC.

- IOTA: Το IOTA είναι η νέα πλατφόρμα για το Blockchain και το IoT και ονομάζεται Blockchain επόμενης γενιάς. Αυτή η πλατφόρμα διευκολύνει την υψηλή ακεραιότητα δεδομένων, την υψηλή απόδοση των συναλλαγών και την υψηλή εγκυρότητα των μπλοκ με τη χρήση λιγότερων πόρων. Επιλύει τους περιορισμούς των μπλοκ αλυσίδων (www.iota.org).
- IOTIFY: Παρέχει διαδικτυακή λύση IoT για την ελαχιστοποίηση των περιορισμών της τεχνολογίας Blockchains με τη μορφή προσαρμοσμένων εφαρμογών (iotify.org)
- iExec: Είναι ένα εργαλείο ανοιχτού BC κώδικα. Διευκολύνει τις εφαρμογές με αποκεντρωμένα πλεονεκτήματα cloud (iex.ec/overview).
- Xage: Είναι η ασφαλής πλατφόρμα Blockchain για το IoT που αυξάνει τον αυτοματισμό και τις ασφαλείς πληροφορίες (xage.com).
- SONM: Είναι μια αποκεντρωμένη BC πλατφόρμα υπολογιστών ομίχλης και παρέχει ασφαλείς υπηρεσίες cloud.

Η εργασία των Alamri et al., 2019 διαχωρίζει τη σχετική με την εφαρμογή της Τεχνολογίας Blockchain σε IoT βιβλιογραφία σε τρεις ενότητες, την αρχιτεκτονική, τις τρέχουσες προκλήσεις και τα προβλήματα των εφαρμογών Blockchain Internet of Things (BIoT). Η κριτική περιελάμβανε διάφορα βιβλία, περιοδικά, επιστολές, αναφορές και άλλα σχετικά έγγραφα, καθώς και ακαδημαϊκές βάσεις δεδομένων όπως το Science Direct, το EBSCO, το Emerald και το SAGE. Για την αναζήτηση σχετικής βιβλιογραφίας, χρησιμοποιήθηκε ένα ευρύ φάσμα σχετικών όρων, όπως IOT, BIot, Block chain, Message Time και Algorithms. Όσον αφορά τις ημερομηνίες αναθεώρησης των πηγών της λογοτεχνίας, ο ερευνητής εξέτασε ένα μείγμα παλαιών και σύγχρονων μελετών για να παρέχει μια ολοκληρωμένη περιγραφή των αποτελεσμάτων σε αυτόν τον τομέα.

Η τεχνολογία Blockchain χρησιμοποιείται σε περισσότερους από έναν τομείς και καταστάσεις. Σε διαφορετικές πηγές όπως στην εργασία των (Swan, 2015) προτάθηκε ότι η πρόοδος στην εφαρμογή του Blockchain ξεκίνησε δίπλα στο Bitcoin ως Blockchain v1.0 εν συνεχεία άλλαξε σε σχέση με έξυπνες συμβάσεις όπως το Blockchain v2.0 και έπειτα προχώρησε στη δικαιοσύνη, σε εφαρμογές παραγωγής, αποδοτικότητας και Blockchain v3.0.

Οι συγγραφείς του "Blockchain παντού" δήλωσαν ότι η κύρια βοήθεια της χρήσης Blockchain με έξυπνα συμβόλαια είναι η αυτόματη αξιολόγηση αυτών των συμβολαίων. Υιοθετώντας έξυπνα συμβόλαια, οι θερμοκρασίες μπορούν να αξιολογηθούν αυτόματα και να ειδοποιηθεί ο αποστολέας και ο παραλήπτης. Εκτός αυτού, τα αποθηκευμένα δεδομένα ήταν διαχειρίσιμα από τον μετρητή και θα μπορούσαν να χρησιμοποιηθούν για τη διεξαγωγή ελέγχου από εξωτερικά μέρη για να διασφαλιστεί η πρακτική της καλής διανομής ιατρικών προϊόντων.Με το Ethereum, ένα τέτοιο αποκεντρωμένο σύστημα μπορεί να χρησιμοποιηθεί πλήρως για να μην υπόκειται σε παραβιάσεις με χαμηλό κόστος, σε κάθε σύμβαση και σε byte. Με τη συμμετοχή πολλών ενδιαφερομένων στην αλυσίδα εφοδιασμού, η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για να αυτοματοποιήσει τις διαδικασίες και τελικά να εξοικονομήσει κόστος διασφαλίζοντας την εμπιστοσύνη μεταξύ των ενδιαφερομένων (Bocek, 2017).

Το Blockchain είναι ένα πολύπλοκο είδος τεχολογίας μορφής Block και πρέπει να προσαρμοστεί σε συγκεκριμένες επιχειρηματικές απαιτήσεις. Λόγω των διαφόρων μορφών χρήσης είναι δύσκολο να υπάρχει μία απλή δομή, οπότε πρέπει να δημιουργηθούν διαφορετικές εκδόσεις εφαρμογών Blockchain και αρχιτεκτονικές εφαρμογές που ταιριάζουν στις ανάγκες κάθε επιχείρησης/βιομηχανίας. Η προσέγγιση που παρουσιάστηκε ήταν ένα μόνο υβρίδιο. Το Blockchain χρησιμοποιείται μαζί με έναν κεντρικό διακομιστή και μια προσέγγιση που στηρίζεται σε βάση δεδομένων.

Οι κύριες συνιστώσες του εν λόγω συστήματος είναι το Ethereum Blockchain δίκτυο, οι έξυπνοι κόμβοι, ο διακομιστής, οι κινητές συσκευές και οι αισθητήρες. Η θερμοκρασία διαφυλάσσεται με έξυπνα συμβόλαια. Για κάθε νέα ομάδα φαρμακευτικών προϊόντων ή φορτία που περιλαμβάνουν εξαιρετικές απαιτήσεις θερμοκρασίας, τα έξυπνα συμβόλαια διαμορφώνονται και αναπτύσσονται από τον διακομιστή για να διασφαλίζουν τις απαιτήσεις συμμόρφωσης για ορθές πρακτικές διανομής (good distribution practice-GDP) (Orenge, 2018). Επομένως, ο χάρτης αντλήθηκε από την αποστολή στον τίτλο της σύμβασης μέσω συνδεδεμένης βάσης δεδομένων με χαμηλό κόστος. Ο διακομιστής φιλοξενεί τον κόμβο modum.io AG Ethereum που εμπλέκεται στο δίκτυο Ethereum και μπορεί να παρακολουθήσει τροποποιήσεις στους έξυπνους κόμβους ή να δημιουργήσει ένα νέο συμβόλαιο ή έξυπνα συμβόλαια (Taylor & Liddle, 2019). Ο κόμβος Ethereum συνδέεται με διακομιστή υπέρ πρωτοκόλλου μεταφοράς κειμένου (Hyper Text Transfer Protocol- HTTP) μέσω JSON. Τα δεδομένα που αποθηκεύονται και είναι είτε πολύ μεγάλα, είτε πολύ ευαίσθητα για να αποθηκεύονται στο Blockchain, αποθηκεύονται στη βάση δεδομένων PostgreSQL και αυτό συμπεριλαμβάνει ακατέργαστα δεδομένα θερμοκρασίας, γιατί τα μεγάλα δεν είναι δυνατό να αποθηκευτούν σε έξυπνους κόμβους. Οι έξυπνοι κόμβοι επαληθεύουν το εύρος της θερμοκρασίας και αποθηκεύουν το αποτέλεσμα της επαλήθευσης στους έξυπνους κόμβους με παγκόσμιο ενιαίο εντοπιστή πόρων (Uniform Resource Location -URL), οι οποίοι με τη σειρά τους αναφέρονται στα ακατέργαστα δεδομένα θερμοκρασίας και τα δεδομένα λιανικής.

Οι πελάτες Android επικοινωνούν στο μπροστινό άκρο του διακομιστή μέσω μιας διεπαφής αντιπροσωπευτικού πρωτοκόλλου μεταφοράς (Representative Transport Protocol-REST) που έχει σχεδιαστεί με το JSON για κρυπτογράφηση και αποκρυπτογράφηση αιτημάτων / απαντήσεων. Μέσω του κινητού τηλεφώνου, οι χρήστες μπορούν να εγγράψουν νέες αποστολές, συμπεριλαμβανομένων των διοικητικών στοιχείων εντός του συστήματος και να δημιουργήσουν ένα έξυπνο συμβόλαιο για κάθε αποστολή. Η διασύνδεση προγραμματισμού εφαρμογών (Application Programming Interface-API) θα πρέπει επίσης να επιτρέπει στον παραλήπτη της αποστολής να λαμβάνει τις μετρήσεις θερμοκρασίας που αναφέρονται από τον αισθητήρα στον διακομιστή. Τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να ενημερώνονται για το αποτέλεσμα της σύμβασης και να έχουν πρόσβαση στις μετρήσεις θερμοκρασίας, χρησιμοποιώντας κατά προτίμηση τη γραφική παράσταση (Bocek, 2017). Μια διαδικτυακή πύλη και μια υποδομή αποτελούσαν τα βασικά στοιχεία των συσκευών Multichain και IoT.

Η διαδικτυακή πύλη παρέχει στους προγραμματιστές ασφαλή και ακριβή έλεγχο των ενημερώσεων λογισμικού. Χαρακτηρίζεται από την είσοδο στην δομή Blockchain, την οποία μοιράζονται οι κατασκευαστές. Κάθε κατασκευαστής θα πρέπει να παρέχει τουλάχιστον ένα επιχειρηματικό κόμβο για την ανάπτυξη υπολογιστικής ισχύος και διαθεσιμότητας υποδομής. Για το πρωτότυπο, ένα συμβόλαιο Blockchain φιλοξενήθηκε στον διακομιστή XenServer και εφαρμόστηκε ως εικονική μηχανή (Virtual Machine -VM). Η διαδικτυακή πύλη και οι διαδικτυακές συσκευές μπορούν να μοιράζονται πράγματα με αναβαθμίσεις λογισμικού και επιβεβαιώσεις μέσω της δομής Blockchain. Το σύστημα βασίζεται σε ασύμμετρη κρυπτογράφηση για να διασφαλίσει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Οι συσκευές διαδικτύου είτε είχαν φυσική παρουσία (i) από πάνελ εξέλιξης, όπως το Raspberry Pi, που ήταν πιο κοντά σε μηχανές πραγματικού πεδίου, ή (ii) από εικονικές συσκευές Qemu, για να εκτιμηθεί η τυπική επεκτασιμότητα (S. Brady, et al., 2017).

Για να προωθηθεί η ενημέρωση λογισμικού:

- Το εργοστάσιο συνδέεται στην πύλη
- Επιλέγει τη συσκευή που θα αναβαθμίσει
- «Κατεβάζει» το λογισμικό αναβάθμισης με μεταδεδομένα (metadata)
- Επιλέγεται μία από τις επιλογές
- Υπογραφή και αναβάθμιση
- Υπογραφή και κρυπτογράφηση

Η πρώτη μέθοδος είναι καλή για την προώθηση ενός μη κρυπτογραφημένου αρχείου στο Blockchain, ενώ η δεύτερη μέθοδος παρέχει εμπιστευτικότητα. Πολλά αρχεία απαιτούνται εξαιτίας του υλισμικού (hardware). Ωστόσο, το κλειδί αποκρυπτογράφησης υποτίθεται ότι έχει οριστεί για κάθε υπάρχουσα συσκευή. Η δομή Blockchain διασφαλίζει ότι οι συναλλαγές είναι σωστές σε λιγότερο από ένα δευτερόλεπτο. Κάθε συσκευή IoT επικοινωνεί τακτικά με το Blockchain και στη συνέχεια διασφαλίζει ότι μια νέα ενημέρωση είναι διαθέσιμη για λήψη. Επομένως, η συσκευή IoT εγκαθιστά και κατεβάζει την ενημέρωση. Στη συνέχεια, εκδίδεται μια απόκριση Blockchain στη σύγχρονη ανίχνευση υλικού (Boudguiga, 2017).

Σε γενικές γραμμές, ένα Blockchain μπορεί να θεωρηθεί ως μόνιμη εγγραφή της οποίας οι εγγραφές αποθηκεύονται σε συγκεκριμένα χρονικά μπλοκ. Το κάθε μπλόκ περιέχει συναλλαγές. Το σύμπλεγμα ορίζεται από το κατακερματισμό του και αναφέρεται στον προηγούμενο κατακερματισμό συμπλέγματος. Όλα αποθηκεύονται στο δημόσιο Blockchain. Προκαθορισμένα κλειδιά κρυπτογράφησης ήταν διαδεδομένα στο διαδίκτυο τα οποία εκτελούνται σε λογισμικό υλικό πριν από την αποστολή. Σκοπός τους είναι να χρησιμεύσουν ως βάση σε άλλους αλγόριθμους κρυπτογράφησης.

Ωστόσο, υπάρχει ένας αριθμός πανομοιότυπων ή μη τυχαίων κλειδιών. Αυτά τα αποτελέσματα επιτρέπουν σε έναν εισβολέα να μαντέψει ή να γνωρίζει το κλειδί κρυπτογράφησης που χρησιμοποιεί η συσκευή (Consult, 2015).

Τα δεδομένα που δημιουργούνται από συσκευές IoT είναι εκτεταμένα, συνδυάζοντας απλά δεδομένα όπως ιστότοπους και πιο περίπλοκα δεδομένα, όπως παρακολούθηση βίντεο. Για ανάλυση δεδομένων, τα ιστορικά δεδομένα πρέπει να αντιστραφούν και τα δεδομένα πρέπει να αποθηκευτούν κάπου. Αυτό σημαίνει ότι τα δεδομένα από συσκευές Διαδικτύου θα είναι υψηλών προτύπων. Σημαίνει επίσης ότι δεδομένης της ποικιλίας των συσκευών απόκτησης δεδομένων, τα δεδομένα θα είναι επίσης ετερογενή. Μια άλλη πτυχή των πραγμάτων δεδομένων διαδικτύου είναι η σχέση μεταξύ χώρου και χρόνου. Το διαδίκτυο θα τοποθετήσει τα πράγματα σε μια συγκεκριμένη τοποθεσία και θα τοποθετήσει μια διάσταση χρόνου σε σημαντικά δεδομένα στη στατιστική ανάλυση. Μόνο μία μικρή ποσότητα δεδομένων που θα κρατηθεί από συσκευές διαδικτύου θα είναι χρήσιμη. Τα video είναι ένα παράδειγμα όπου τα καρέ του video που λαμβάνονται όταν κάποιος κάνει κάτι παράνομο είναι χρήσιμα, ενώ αυτά που λαμβάνονται κατά τη διάρκεια της εργασίας δεν είναι χρήσιμα (Chen, 2014).

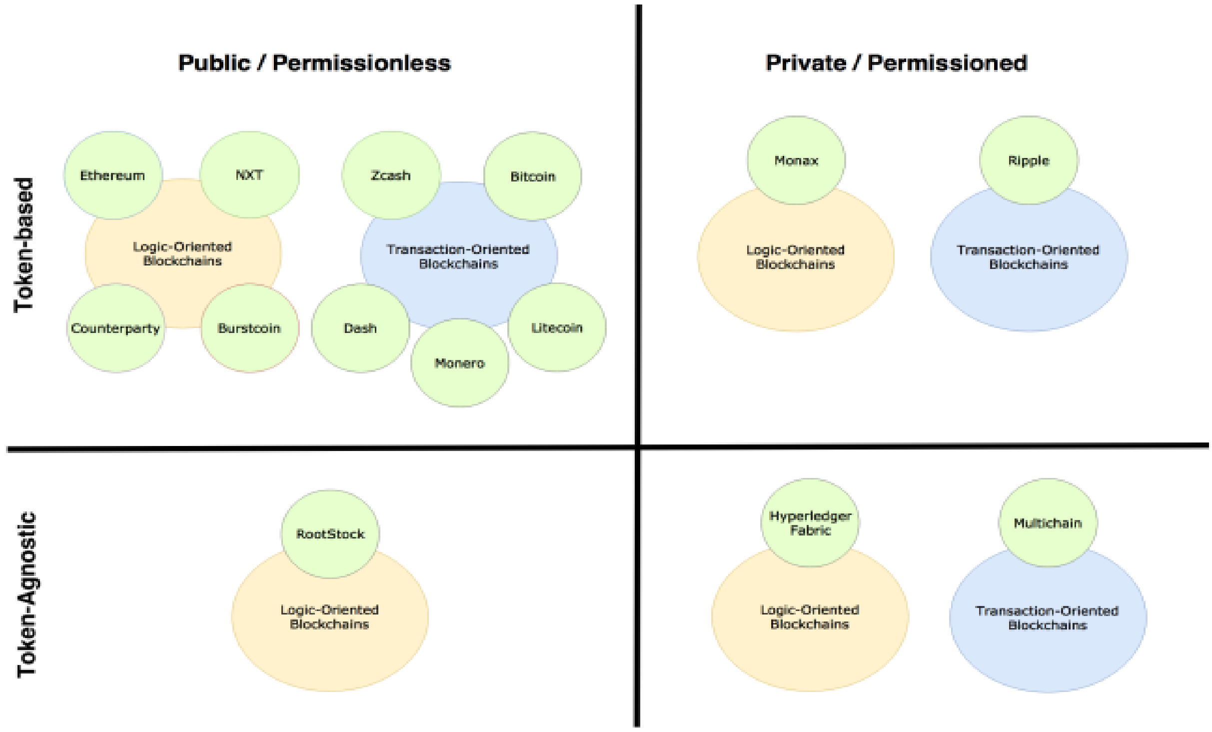
Λέγεται ότι το πρωτόκολλο ενημέρωσης Blockchain επιτυγχάνει συναίνεση σε ένα βυζαντινό περιβάλλον εάν επιτευχθούν τα παρακάτω χαρακτηριστικά (S.Bano, 2017):

- **Υγεία:** Αυτό συμβαίνει όταν όλοι οι έγκυροι κόμβοι που έχουν ενεργοποιηθεί σε μία κοινόχρηστη κατάσταση, απαιτούν την προσθήκη Blockchain από το ίδιο μπλοκ, κάθε τεκμηριωμένος κόμβος μετακινείται σε μια νέα κατάσταση τοπικής αντιγραφής, η οποία είναι το Blockchain που οδηγείται από αυτό το μπλοκ.
- **Συμφωνία - συνέπεια:** Εάν ο αξιόπιστος κόμβος επιβεβαιώσει ότι υπάρχει μια νέα κεφαλή συμπλέγματος, οποιοσδήποτε αξιόπιστος κόμβος που ενημερώνει την τοπική οθόνη Blockchain θα ενημερωθεί χρησιμοποιώντας αυτήν την κεφαλή συμπλέγματος.
- **Ζωτικότητα – τερματισμός:** Τελικώς θα διασφαλιστούν όλες οι συναλλαγές οι οποίες προέρχονται από τους πιο ευφυείς κόμβους
- **Συνολική παραγγελία:** Όλοι οι έγκυροι κόμβοι αποδέχονται την ίδια εντολή συναλλαγής εφόσον είναι βέβαιοι για τις απόψεις τους για το τοπικό Blockchain. Πρωτόκολλα που είναι σύμφωνα διαφέρουν σε διαφορετικά δίκτυα Blockchain. Επειδή επετράπη στα δίκτυα Blockchain να αναγνωρίσουν πιο αυστηρό έλεγχο στον συγχρονισμό των κόμβων συναίνεσης, ενδέχεται αυτά να προσφέρουν πρωτόκολλα Βυζαντινού Σφάλματος-Ανοχής (Byzantine Fault-Tolerant BFT) για να παρουσιάσουν τα απαιτούμενα χαρακτηριστικά συμβατότητας. Μια τυπική εφαρμογή τέτοιων πρωτοκόλλων μπορεί να υπάρχει σε κυματοειδές δίκτυο, όπου μια ομάδα ταυτόχρονων διακομιστών Ripple επεκτείνει το Blockchain μέσω του μηχανισμού ψηφοφορίας. Επιπλέον, εάν παρουσιαστεί ένα εξωτερικό Oracle για να ρυθμίσει τον αρχικό κόμβο για τη δημιουργία του μπλοκ, το πρακτικό BFT (PBFT) μπορεί να ληφθεί για την

εφαρμογή ενός σχήματος δέσμευσης τριών σταδίων για την επέκταση του Blockchain (Cachin, 2016).

Στην περίπτωση των εφαρμογών του Διαδικτύου των πραγμάτων (Internet of things - IoT), είναι σημαντικό να γίνεται μία διάκριση μεταξύ του ελέγχου ταυτότητας (δηλαδή ποιος μπορεί να έχει πρόσβαση στην αλυσίδα συστοιχιών (Blockchain - BC), ιδιωτική έναντι δημόσιας) και της εξουσιοδότησης (δηλαδή τι μπορεί να κάνει μια συσκευή IoT χωρίς άδεια, έναντι μίας με άδεια). Ωστόσο, πρέπει να σημειωθεί ότι τέτοιες διακρίσεις είναι ακόμα υπό συζήτηση και οι ορισμοί που δίνονται στη συνέχεια ενδέχεται να διαφέρουν συγκριτικά με ορισμούς που προκύπτουν από άλλες μελέτες. Στις δημόσιες αλυσίδες συστοιχιών μπορεί να εγγραφεί ο οποιοσδήποτε χωρίς να απαιτείται η έγκριση τρίτων. Έτσι, είναι σε θέση να λειτουργεί ως απλός κόμβος ή ως εξορύκτης(miner)/ελεγκτής. Οι εξορύκτες/ελεγκτές λαμβάνουν συνήθως οικονομικά κίνητρα σε δημόσιες αλυσίδες συστοιχιών όπως το Bitcoin, το Ethereum ή το Litecoin. Στην περίπτωση των ιδιωτικών αλυσίδων συστοιχιών, ο ιδιοκτήτης περιορίζει την πρόσβαση στο δίκτυο. Επίσης, πολλές ιδιωτικές αλυσίδες συστοιχιών αδειοδοτούνται ούτως ώστε να γίνεται ένας έλεγχος μεταξύ χρηστών, με σκοπό τον εντοπισμό αυτών που μπορούν να εκτελούν συναλλαγές, να πραγματοποιούν έξυπνες συμβάσεις ή να ενεργούν ως εξορύκτες στο δίκτυο. Πρέπει όμως να ληφθεί υπόψη ότι δεν έχουν λάβει άδεια όλες οι ιδιωτικές αλυσίδες συστοιχιών. Για παράδειγμα, ένας οργανισμός μπορεί να αναπτύξει μία ιδιωτική αλυσίδα συστοιχιών βασιζόμενη στην πλατφόρμα Ethereum, η οποία όμως είναι δημόσια. Παραδείγματα επιτρεπόμενων αλυσίδων συστοιχιών είναι αυτές που χρησιμοποιούνται από την Hyperledger-Fabric ή την Ripple. Μπορεί επίσης να γίνει διάκριση μεταξύ αλυσίδων συστοιχιών που στοχεύουν αποκλειστικά στην παρακολούθηση ψηφιακών περιουσιακών στοιχείων (π.χ. Bitcoin) και αλυσίδων συστοιχιών που επιτρέπουν την εκτέλεση μίας συγκεκριμένης λογικής (δηλαδή, έξυπνων συμβάσεων). Επιπλέον, υπάρχουν συστήματα που χρησιμοποιούν μάρκες/κρυπτονομίσματα (π.χ. Ripple), ενώ άλλα όχι (π.χ. Hyperledger). Ωστόσο πρέπει να ληφθεί υπόψη ότι τέτοιες μάρκες/κρυπτονομίσματα (tokens) δεν σχετίζονται απαραίτητα με την ύπαρξη κρυπτονομίσματος, αλλά μπορούν να χρησιμοποιηθούν ως εσωτερικές αποδείξεις που να υποδεικνύουν ότι ορισμένα γεγονότα συνέβησαν σε συγκεκριμένες χρονικές στιγμές.

Συνοπτικά, οι διαφορετικοί τύποι αλυσίδων συστοιχιών απεικονίζονται στην Εικόνα 1 παρακάτω, μαζί με πολλά παραδείγματα υλοποιήσεων.



Σχήμα 3-4. Ταξινόμηση αλυσίδων συστοιχιών και πρακτικά παραδείγματα.
Πηγή: (Fernández-Caramés & Fraga-Lamas, 2018).

3.3 Αναγκαιότητα χρήσης Blockchain στο IoT

Προτού γίνει μία πιο λεπτομερείς ανάλυση σχετικά με τον τρόπο χρήσης μιας αλυσίδας συστοιχιών για εφαρμογές IoT, πρέπει πρώτα να τονιστεί ότι η αλυσίδα συστοιχιών δεν αποτελεί πάντα τη καλύτερη λύση για κάθε σενάριο IoT. Οι παραδοσιακές βάσεις δεδομένων ή τα βιβλία καταχώρησης που βασίζονται σε ένα κατευθυνόμενο άκυκλο γράφημα (Directed acyclic graph - DAG) ενδέχεται να ταιριάζουν καλύτερα σε ορισμένες εφαρμογές IoT. Συγκεκριμένα, προκειμένου να καθοριστεί εάν η χρήση μιας αλυσίδας συστοιχιών είναι κατάλληλη, ένας προγραμματιστής θα πρέπει να αποφασίσει εάν τα ακόλουθα χαρακτηριστικά είναι απαραίτητα για μια εφαρμογή IoT:

- Αποκέντρωση. Οι εφαρμογές IoT απαιτούν αποκέντρωση όταν δεν υπάρχει ένα αξιόπιστο κεντρικό σύστημα. Ωστόσο, πολλοί χρήστες εξακολουθούν να εμπιστεύονται τυφλά ορισμένες εταιρείες, κυβερνητικές υπηρεσίες ή τράπεζες. Σε τέτοιες περιπτώσεις αμοιβαίας εμπιστοσύνης, δεν απαιτείται αλυσίδα συστοιχιών.
- Ανταλλαγές P2P (Peer-to-peer). Στο IoT, οι περισσότερες επικοινωνίες μεταδίδονται από κόμβους σε πύλες που δρομολογούν δεδομένα σε έναν απομακρυσμένο διακομιστή ή νέφος (cloud). Οι επικοινωνίες μεταξύ ομοτίμων (peers) σε επίπεδο κόμβου δεν είναι στην πραγματικότητα πολύ συχνές, εκτός από συγκεκριμένες εφαρμογές, όπως στη νοημοσύνη σμήνους (Swarm intelligence - SI) ή σε συστήματα υπολογιστών ομίχλης (Preden et al., 2015).

Υπάρχουν επίσης άλλα παραδείγματα που ενισχύουν τις επικοινωνίες μεταξύ κόμβων στο ίδιο επίπεδο, όπως συμβαίνει στην ομίχλη υπολογιστών (Fog computing) με τοπικές πύλες (Bonomi et al., 2012).

- Σύστημα πληρωμής. Ορισμένες εφαρμογές IoT μπορεί να απαιτούν την εκτέλεση οικονομικών συναλλαγών με τρίτους, ενώ άλλες όχι. Επιπλέον, οι οικονομικές συναλλαγές μπορούν ακόμη να πραγματοποιούνται μέσω παραδοσιακών συστημάτων πληρωμών, αν και συνήθως συνεπάγονται με την πληρωμή προμηθειών συναλλαγών (οι οποίες προϋποθέτουν την εμπιστοσύνη σε τράπεζες ή μεσάζοντες).
- Δημόσια διαδοχική καταγραφή συναλλαγών. Πολλά δίκτυα IoT συλλέγουν δεδομένα που πρέπει να σφραγιστούν και να αποθηκευτούν διαδοχικά. Ωστόσο, τέτοιες ανάγκες μπορούν εύκολα να καλυφθούν με τις παραδοσιακές βάσεις δεδομένων, ειδικά σε περιπτώσεις όπου η ασφάλεια είναι εγγυημένη ή οι κυβερνοεπιθέσεις αποτελούν σπάνιο φαινόμενο.
- Στιβαρό κατανεμημένο σύστημα. Τα κατανεμημένα συστήματα μπορούν επίσης να χτιστούν πάνω από νέφη (clouds), συμπλέγματα διακομιστών ή οποιαδήποτε μορφή παραδοσιακών κατανεμημένων υπολογιστικών συστημάτων. Όμως, η ανάγκη αυτού του χαρακτηριστικού δεν αρκεί για να δικαιολογήσει τη χρήση μιας αλυσίδας συστοιχιών καθώς πρέπει επίσης να υπάρχει τουλάχιστον, έλλειψη εμπιστοσύνης στην οντότητα που διαχειρίζεται το αντίστοιχο κατανεμημένο υπολογιστικό σύστημα.
- Συλλογή μικροσυναλλαγών. Ορισμένες εφαρμογές IoT μπορεί να χρειαστεί να τηρούν αρχείο κάθε συναλλαγής, ούτως ώστε να μπορούν να διατηρούν την ιχνηλασιμότητα είτε για λόγους ελέγχου είτε επειδή οι τεχνικές των μεγάλων δεδομένων (Big Data) εφαρμόζονται σε μεταγενέστερη φάση. Σε αυτές τις περιπτώσεις, μπορεί να φανεί χρήσιμη μια πλευρική αλυσίδα (Back et al., 2014). Ωστόσο, υπάρχουν και άλλες εφαρμογές οι οποίες δεν χρειάζεται να αποθηκεύουν κάθε συλλεγόμενη τιμή. Για παράδειγμα, στην απομακρυσμένη αγροτική παρακολούθηση, όπου οι επικοινωνίες είναι δαπανηρές, είναι συνηθισμένο να χρησιμοποιούνται κόμβοι IoT που κάνουν επαναφορά ανά ώρα για τη λήψη περιβαλλοντικών δεδομένων από αισθητήρες. Σε τέτοιες περιπτώσεις, ένα τοπικό σύστημα μπορεί να συλλέγει και να αποθηκεύει τα δεδομένα, αλλά και να μεταδίδει συνολικά (μία φορά την ημέρα), τις επεξεργασμένες πληροφορίες σε μία συναλλαγή (Pérez-Expósito et al., 2017).

3.4 Δυνατότητες και Προοπτικές Εφαρμογής Blockcain σε IoT

Η προσέγγιση ενσωμάτωσης BC-IoT έχει πολλές αξιοσημείωτες δυνατότητες. Ανοίγει και για τους δύο τομείς νέους ορίζοντες. Μερικές από τις δυνατότητες είναι οι εξής:

- **Οικοδόμηση εμπιστοσύνης μεταξύ των μερών:** Η προσέγγιση BC-IoT θα δημιουργήσει εμπιστοσύνη μεταξύ των διαφόρων συνδεδεμένων συσκευών χάρη στα χαρακτηριστικά ασφαλείας της. Μόνο επαληθευμένες συσκευές μπορούν να επικοινωνούν στο δίκτυο και κάθε μπλοκ της συναλλαγής θα επαληθεύεται πρώτα από τους χρήστες και στη συνέχεια θα μπορούν να εισέλθουν στο BC.

- **Μείωση του κόστους:** Αυτή η προσέγγιση θα μειώσει το κόστος, επειδή επικοινωνεί απευθείας χωρίς την παρέμβαση τρίτου. Εξαλείφει όλους τους κόμβους τρίτων μεταξύ του αποστολέα και του παραλήπτη. Παρέχει άμεση επικοινωνία.
- **Ελάττωση χρόνου:** Αυτή η προσέγγιση ελαττώνει πολύ το χρόνο. Ελαττώνει το χρόνο που απαιτείται στις συναλλαγές από ημέρες σε δευτερόλεπτο.
- **Ασφάλεια και απόρρητο:** Παρέχει ασφάλεια και απόρρητο σε συσκευές και πληροφορίες.
- **Κοινωνικές υπηρεσίες:** Αυτή η προσέγγιση παρέχει δημόσιες και κοινωνικές υπηρεσίες στις συνδεδεμένες συσκευές. Όλες οι συνδεδεμένες συσκευές μπορούν να επικοινωνούν και να ανταλλάσσουν πληροφορίες μεταξύ τους
- **Χρηματοοικονομικές υπηρεσίες:** Αυτή η προσέγγιση μεταφέρει χρήματα με ασφαλή τρόπο χωρίς μεσολάβηση τρίτου. Παρέχει γρήγορη, ασφαλή και απόρρητη χρηματοοικονομική υπηρεσία. Ελάττωσε το κόστος μεταφοράς και τον απαιτούμενο χρόνο.
- **Διαχείριση κινδύνων:** Αυτή η προσέγγιση διαδραματίζει σημαντικό ρόλο για την ανάλυση και τη μείωση του κινδύνου αποτυχίας των πόρων και των συναλλαγών.

Το IoT και το BC θα μπορούσαν να αντιμετωπίσουν πολλές προκλήσεις όπως κλίμακα, αποθήκευση, δεξιότητες, ανακαλύψεις κ.λπ. Τα παρακάτω είναι οι προκλήσεις που αντιμετωπίζει η προσέγγιση ολοκλήρωσης:

- Επεκτασιμότητα: Το BC μπορεί να «κολλήσει» λόγω του μεγάλου φορτίου της συναλλαγής. Ο χώρος αποθήκευσης Bitcoin γίνεται όλο και μεγαλύτερος από τα 197 GB το 2019 (https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size). Μια πιθανή ενσωμάτωση των IoT και BC, θα έχει σαν αποτέλεσμα ένα πολύ βαρύτερο φορτίο από την τρέχουσα κατάσταση.
- Αποθήκευση: Το ψηφιακό καθολικό θα αποθηκεύεται σε κάθε κόμβο IoT. Με την πάροδο του χρόνου, θα αυξηθεί το μέγεθος αποθήκευσης τόσο ώστε να είναι ένα βαρύ φορτίο για κάθε συνδεδεμένη συσκευή
- Έλλειψη δεξιοτήτων: Το BC είναι μια νέα τεχνολογία. Είναι γνωστό από πολύ λίγους στον κόσμο. Αυτό από μόνο του αποτελεί μία πρόκληση για την εκπαίδευση του κόσμου σε μια τέτοια τεχνολογία
- Ανακάλυψη και ολοκλήρωση: Στην πραγματικότητα, το BC δεν έχει σχεδιαστεί για IoT. Είναι πολύ δύσκολο για τις συνδεδεμένες συσκευές να ανακαλύψουν μια άλλη συσκευή στο BC και το IoT. Έτσι, οι κόμβοι IoT μπορούν να ανακαλύψουν ο ένας τον άλλον, αλλά δεν μπορούν να ανακαλύψουν και να ενσωματώσουν το BC με μια άλλη συσκευή.

- Απόρρητο: Το καθολικό διανέμεται δημόσια σε κάθε συνδεδεμένο κόμβο. Οι κόμβοι μπορούν να δουν τις συναλλαγές του καθολικού. Έτσι, το απόρρητο είναι επίσης μια πρόκληση στην ολοκληρωμένη προσέγγιση
- Διαλειτουργικότητα: Το BC μπορεί να είναι δημόσιο ή ιδιωτικό. Έτσι, η διαλειτουργικότητα μεταξύ δημόσιων και ιδιωτικών Blockchain είναι επίσης μια πρόκληση στην προσέγγιση BC-IoT.
- Κανονισμοί: Το IoT-BC θα ενεργήσει παγκοσμίως, έτσι αντιμετωπίζει πολλούς κανονισμούς για την εφαρμογή αυτής της προσέγγισης παγκοσμίως.

Το BC και το IoT είναι μια νέα προσέγγιση που διερευνήθηκε στη μέλετη του (Tanweer, 2019) όπου περιγράφονται πολλές ευκαιρίες και προκλήσεις. Επίσης, υπάρχουν διαθέσιμες πλατφόρμες. Αυτή η προσέγγιση μπορεί να είναι το μέλλον του διαδικτύου επειδή μπορεί να αναθεωρήσει το τρέχον σύστημα διαδικτύου και να το αλλάξει σε ένα νέο όπου κάθε έξυπνη συσκευή θα συνδεθεί με άλλες συσκευές χρησιμοποιώντας το δίκτυο peer-to-peer σε πραγματικό χρόνο. Μπορεί να μειώσει το τρέχον κόστος και το χρόνο και να παρέχει τις σωστές πληροφορίες στη σωστή συσκευή σε πραγματικό χρόνο. Έτσι, μπορεί να είναι πολύ χρήσιμο στο μέλλον

Σήμερα, η ανάπτυξη των τεχνολογιών σε περιβάλλον BIoT ως Cyber-Physical Systems (CPS) (Fraga-Lamas, 2016) ή RFID (Barro-Torres, 2014) και συστήματα τηλεμετρίας (Hernández-Rojas, 2017) ή 4G / 5G ευρυζωνικές επικοινωνίες (Fraga-Lamas et al., 2016) βρισκόταν σε πολλές προκλήσεις.

Συγκεκριμένα, η κατάσταση της αποστολής και κρίσιμες καταστάσεις (Fraga-Lamas, 2017) αύξησαν τις ανησυχίες. Επιπλέον, το μείγμα προτείνει επιπλέον μελλοντικές λειτουργικές ανάγκες, και ότι η ανάπτυξη εφαρμογών BIoTs είναι μια σύνθετη διαδικασία, η οποία επηρεάστηκε από πολλά χαρακτηριστικά, τα οποία ήταν διασυνδεδεμένα.

3.5 Ενοποίηση Blockchain και IoT

Οι (Brody & Pureswaran, 2014) στη μελέτη τους θεώρησαν ότι το διαρκώς διευρυμένο οικοσύστημα συσκευών IoT πρέπει να στραφεί προς μια αποκεντρωμένη αρχιτεκτονική προκειμένου να διατηρήσει τη βιωσιμότητά του. Από την πλευρά του καταναλωτή αφενός, υπάρχει έλλειψη εμπιστοσύνης καθώς και ανάγκη για προσέγγιση «ασφάλειας μέσω διαφάνειας», ενώ αφετέρου, από την πλευρά του κατασκευαστή, υπάρχει τεράστιο κόστος συντήρησης που σχετίζεται με το τρέχον συγκεντρωτικό μοντέλο. Τέτοια ζητήματα δύνανται να αντιμετωπιστούν αποτελεσματικά με το Blockchain το οποίο αποτελεί από μόνο του ένα μοντέλο δικτύου peer-to-peer λιγότερο αξιόπιστο, επεκτάσιμο, ικανό να διανέμει δεδομένα με ασφάλεια και να λειτουργεί με διαφάνεια.

Προκειμένου να καταστεί κατανοητή η πλήρης λειτουργία του εν λόγω μοντέλου, γίνεται η παραδοχή ότι θεωρείται μία ρύθμιση όπου όλες οι συσκευές IoT λειτουργούν σε ένα ενιαίο δίκτυο Blockchain. Το έξυπνο συμβόλαιο που αναπτύχθηκε από τον κατασκευαστή διευκολύνει την αποθήκευση του κατακερματισμού της τελευταίας ενημέρωσης υλικολογισμικού δικτύου (Benet, 2015). Οι συσκευές χρησιμοποιούν τη διεύθυνση του έξυπνου συμβολαίου ή κάποια άλλη υπηρεσία εντοπισμού προκειμένου να υποβάλουν ερωτήματα στη σύμβαση, να λάβουν νέες ενημερώσεις υλικολογισμικού και να τις ζητήσουν με το κατακερματισμό του. Ο κόμβος του ίδιου του κατασκευαστή εξυπηρετεί τα αρχικά αιτήματα αρχείων, μπορεί ωστόσο να διακόψει την προβολή μόλις αυτό το δυαδικό αρχείο διαδοθεί σε έναν ικανό αριθμό κόμβων. Οι διαμορφωμένες συσκευές υποτίθεται ότι μοιράζονται το δυαδικό αρχείο που έχουν λάβει, επιτρέποντας έτσι την ανάκτηση των ενημερώσεων υλικολογισμικού. Αυτό ισχύει ακόμη και για εκείνες τις συσκευές που συνδέονται στο δίκτυο αφού ο κατασκευαστής σταματήσει να συμμετέχει. Για τα παραπάνω δεν απαιτείται καμία αλληλεπίδραση χρήστη γιατί στην ουσία συμβαίνουν αυτόματα. Επιπλέον, ένα δίκτυο Blockchain ανταλλαγής κρυπτονομισμάτων ανοίγει τον δρόμο για εύκολη ανταλλαγή υπηρεσιών μεταξύ συσκευών και παρέχει επίσης ένα λογικό επίπεδο χρέωσης. Προκειμένου να αποκομίσουν κάποιο κέρδος ή να διατηρήσουν το κόστος υποδομής τους, αυτές οι συσκευές που αποθηκεύουν το δυαδικό αντίγραφο ενδέχεται να χρεώνουν για την εξυπηρέτησή που παρέχουν. Άλλα παραδείγματα περιλαμβάνουν τα EtherAPI που βοηθούν στη δημιουργία εσόδων από κλήσεις API και το Filecoin που διευκολύνει τις συσκευές να δανείζουν χώρο στο δίσκο τους με ενοικίαση. Με ένα κρυπτονόμισμα όπως το Ethereum ή το Bitcoin, κάθε συσκευή λαμβάνει κατάλληλη αποζημίωση με τη βοήθεια μικροσυναλλαγών για τη χρήση της. Κάτι τέτοιο είναι δυνατό επειδή κάθε συσκευή μπορεί να έχει τον δικό της προσωπικό τραπεζικό λογαριασμό και να εκθέτει τους πόρους της σε άλλες συσκευές (Yassami et al., 2016).

Η ενσωμάτωση του IoT και του Blockchain διευκολύνει επίσης την κοινή χρήση ιδιοκτησίας και υπηρεσιών. Το Slock.it εισήγαγε την έννοια των "Slocks" ή έξυπνων ηλεκτρονικών κλειδαριών που μπορούν να ξεκλειδωθούν μόνο από τη συσκευή που φέρει την κατάλληλη λεκτική μονάδα (token). Κατ' επέκταση, η ενσωμάτωση του IoT και του Blockchain στον ενεργειακό τομέα διευκολύνει την αγορά peer-to-peer όπου τα μηχανήματα είναι σε θέση να αγοράζουν και να πωλούν ενέργεια αυτόματα με βάση ορισμένα κριτήρια που καθορίζονται από τον χρήστη. Για παράδειγμα, το TransActive Grid αναδεικνύει την έννοια της αγοράς peer-to-peer για τον εφοδιασμό ανανεώσιμων πηγών ενέργειας στη Νέα Υόρκη. Τα εγκατεστημένα ηλιακά πάνελ καταγράφουν την πλεονάζουσα παραγωγή σε ένα Blockchain και την πωλούν μέσω έξυπνων συμβολαίων (Rutkin, 2016).

Η χρησιμότητα της ενσωμάτωσης Blockchain και IoT μπορεί να φανεί σε ένα τυπικό παράδειγμα εφοδιαστικής αλυσίδας στο οποίο ένα κοντέινερ που απελευθερώνεται από την τοποθεσία κατασκευής (περιοχή A), αποστέλλεται στο γειτονικό λιμάνι (περιοχή B) μέσω σιδηροδρόμου, από εκεί αποστέλλεται στη θύρα προορισμού (περιοχή C), αποστέλλεται ξανά στη διεύθυνση του διανομέα (περιοχή D) και τελικά παραλαμβάνεται στην περιοχή των λιανοπωλητών (περιοχή E). Ως εκ τούτου, η διαδικασία που συζητήθηκε περιλαμβάνει πολλούς ελέγχους και ενδιαφερόμενους κατά τη διάρκεια της πορείας αυτής. Προκειμένου να παρακολουθείται το περιουσιακό στοιχείο, κάθε ενδιαφερόμενος διατηρεί τη δική του βάση δεδομένων, την οποία ενημερώνει με βάση τα στοιχεία που λαμβάνονται από άλλα μέρη που βρίσκονται κατά μήκος της αλυσίδας. Ένα δίκτυο Blockchain που εισήχθη για την παρακολούθηση αυτού του στοιχείου είναι ουσιαστικά μια κοινόχρηστη βάση δεδομένων που αποτελείται από κρυπτογραφικά επαληθευμένες ενημερώσεις οι οποίες διαδίδονται αυτόματα προκειμένου να δημιουργηθεί μια ελεγχόμενη δοκιμή πληροφοριών. Μόλις φτάσει στη θύρα προορισμού, ο μεταφορέας στέλνει ένα υπογεγραμμένο μήνυμα σε ένα συμφωνημένο, προκαθορισμένο έξυπνο συμβόλαιο έτσι ώστε όλοι στην αλυσίδα να γνωρίζουν την τρέχουσα θέση του κοντέινερ. Η υπογεγραμμένη συναλλαγή λειτουργεί ως κρυπτογραφικά επαληθεύσιμη απόδειξη για την επιτυχή παραλαβή του κοντέινερ στη θύρα προορισμού. Ο παραλήπτης δημοσιεύει επίσης στο ίδιο έξυπνο συμβόλαιο για να επιβεβαιώσει την κατοχή του όσον αφορά το κοντέινερ (Chang & Chen, 2020).

3.6 Ταξινόμηση του Blockchain

Ανάλογα με τα δεδομένα, τη διαθεσιμότητά τους και τη διαφορετική δράση που σχετίζεται με αυτά, τα Blockchains ταξινομούνται σε τρεις διαφορετικούς τύπους: τα ομοσπονδιακά/μεικτά/κοινοπραξίας (federated), τα ιδιωτικά και τα δημόσια. Σύμφωνα με ορισμένους συγγραφείς, τα ιδιωτικά/με άδεια και τα δημόσια/χωρίς άδεια θεωρούνται συνώνυμα μεταξύ τους. Ωστόσο, υπάρχει κάποια διαφορά όσον αφορά την εξουσιοδότηση (αυτά με άδεια έναντι αυτών χωρίς άδεια) και τον έλεγχο ταυτότητας (ιδιωτική έναντι δημόσιας). Στα ιδιωτικά Blockchain, η πρόσβαση στο δίκτυο περιορίζεται από τον ιδιοκτήτη. Όσον αφορά τα δημόσια Blockchain, δεν απαιτείται έγκριση τρίτου μέρους για την ένταξη στο Blockchain. Μπορούν να λειτουργήσουν ως κόμβοι ή ως miner (εξορύκτης). Ένα σύστημα που βασίζεται στην απόκριση πρόκλησης χρησιμοποιείται για την επιλογή του κόμβου που θα προστεθεί στο Blockchain όπου κάθε κόμβος θα επιχειρούσε να λύσει την πρόκληση. Τίθεται λοιπόν στο σημείο αυτό το ερώτημα για το ποια θα είναι τα κίνητρα για άλλους κόμβους που συμμετέχουν σε αυτήν την πρόκληση. Έτσι, στους εξορύκτες (miner) δίνονται οικονομικά κίνητρα όπως το Bitcoin, το Litecoin ή το Ethereum προκειμένου να καταστούν τμήματα της πρόκλησης (Liu et al., 2018). Το ομοσπονδιακό Blockchain ή το Blockchain κοινοπραξίας είναι ένας άλλος τύπος Blockchain με άδεια, παρόμοιο με το ιδιωτικό. Τα δίκτυα κοινοπραξιών ενισχύουν τη διαφάνεια μεταξύ των διαφόρων εμπλεκομένων μερών και μπορούν να εκτείνονται σε πολλούς οργανισμούς. Το Blockchain κοινοπραξίας χρησιμοποιείται ως μια αξιόπιστα συγχρονισμένη και ελεγχόμενη βάση δεδομένων που παρακολουθεί την ανταλλαγή δεδομένων μεταξύ των μελών της κοινοπραξίας. Το μοντέλο χωρίς άδεια είναι ένα ανοιχτό περιβάλλον που ταιριάζει καλύτερα για κρυπτονομίσματα. Πρόκειται ουσιαστικά για μία δωρεάν οικονομική εφαρμογή ανοικτού ελέγχου, ενώ το μοντέλο με άδεια είναι ένα στενό περιβάλλον πραγματικά κατάλληλο για επιχειρηματικές εφαρμογές όπως το Hyperledger Fabric (Wang et al., 2018), το Smart Contract ή το Ripple. Μπορούν ακόμη να ταξινομηθούν σε δύο κατηγορίες: α) ως Blockchain όπου χρησιμοποιείται συγκεκριμένη λογική όπως Smart Contracts και β) ως Blockchain όπου μπορούν να παρακολουθούνται ψηφιακά στοιχεία όπως το Bitcoin. Επίσης, υπάρχουν ορισμένα συστήματα που χρησιμοποιούν token (Ripple) και μερικά που δεν χρησιμοποιούν token (Hyperledger). Στην περίπτωση αυτή τα tokens μπορούν να αναφέρονται ως απόδειξη, για να δικαιολογήσουν την εμφάνιση συγκεκριμένων γεγονότων σε συγκεκριμένη χρονική στιγμή.

3.7 Πλατφόρμες Blockchain για IoT

Ακολουθεί ανάλυση προκειμένου να εκτιμηθεί η πιο κατάλληλη πλατφόρμα Blockchain για εφαρμογές IoT, σύγκριση των πιο ευρέως αποδεκτών και εξέχουσες πλατφόρμες Blockchain συμπεριλαμβανομένων των IOTA, Hyperledger-Fabric, Ethereum και Bitcoin. Ένα μπλοκ λιγότερο κατανεμημένο καθολικό και διάδοχος του Blockchain που ονομάζεται IOTA έχει σχεδιαστεί ειδικά για την ενεργοποίηση μικροπληρωμών στο βιομηχανικό IoT. Η IOTA αντιμετωπίζει ζητήματα όπως αυτά των υψηλών προμηθειών συναλλαγών και της επεκτασιμότητας. Πριν ξεκινήσει τη δική του συναλλαγή, κάθε κόμβος στο IOTA επικυρώνει οποιεσδήποτε δύο προηγούμενες συναλλαγές χωρίς να χρειάζεται οι εξορύκτες να εξορύσσουν ένα έγκυρο μπλοκ συναλλαγών. Το IOTA δεν διαθέτει συναινετικό τελικό αποτέλεσμα, επομένως είναι επιρρεπές σε καθυστέρηση που προκαλεί διακλάδωση στην επιβεβαίωση συναλλαγής. Το Hyperledger και το Ethereum έχουν διαφορετική αρχιτεκτονική από το Blockchain, καθώς έχουν σχεδιαστεί για αλληλεπιδράσεις M2M και προσφέρουν συναλλαγές χωρίς χρέωση. Τα ζητήματα επεκτασιμότητας του Blockchain μπορούν επίσης να λυθούν σε κάποιο βαθμό χρησιμοποιώντας αυτές τις πλατφόρμες. Τα συστήματα IoT έχουν σχεδιαστεί για πολλές εφαρμογές που κυμαίνονται από τα συστήματα βιομηχανικού ελέγχου έως τα έξυπνα ρολόγια. Το Hyperledger και το Ethereum μπορούν να χρησιμοποιηθούν σε αυτά τα συστήματα λόγω της δυνατότητας εφαρμογής τους σε πολλαπλές εφαρμογές Blockchain.

3.7.1 Ασφάλεια IoT που Βασίζεται σε Blockchain

Με την πάροδο του χρόνου έχει πια αναφερθεί εκθετική αύξηση των επιθέσεων λόγω της συγχώνευσης του φυσικού κόσμου και του Διαδικτύου που οδηγεί σε περίπλοκες επιπτώσεις στην ασφάλεια (Correia et al. 2011). Παρακάτω παρουσιάζονται τα ζητήματα ασφάλειας που αντιμετωπίζουν οι συγκεντρωμένες αρχιτεκτονικές του IoT και τα πιθανά οφέλη της ενοποίησης του Blockchain με το IoT. Το υπερ-επεκτεινόμενο άκρο φέρνει στο προσκήνιο τη μεγάλη πρόκληση ασφαλείας στο IoT, καθώς οι κόμβοι στο άκρο του δικτύου είναι τα πιο ευάλωτα σημεία εναντίον των οποίων μπορεί να εξαπολυθεί τεράστιο εύρος επιθέσεων. Ένα σύνολο κακόβουλων κόμβων και άλλων συσκευών στο άκρο του IoT μπορεί να εξαπολύσει επιθέσεις botnet οι οποίες είναι σε θέση να οδηγήσουν σε ολική κατάρρευση την παροχή υπηρεσιών IoT (Kolias et al., 2017). Οι πολύ συγκεντρωτικές διαμορφώσεις στο IoT είναι μια άλλη αιτία απειλής της διαθεσιμότητας παροχής υπηρεσιών IoT. Τόσο η διαθεσιμότητα, όσο ακόμη κι ένα κεντρικό σημείο αστοχίας αποτελεί επίσης απειλή για την εξουσιοδότηση και την εμπιστευτικότητα, καθώς ο πάροχος υπηρεσιών είναι σε θέση να παραβιάσει ή να κάνει κακή χρήση των δεδομένων του χρήστη. Επιπλέον, η πλαστογράφηση ταυτότητας καθώς και η ανάλυση πληροφοριών κυκλοφορίας ενδέχεται να οδηγήσουν σε επίθεση που διακυβεύει το απόρρητο. Το IoT αντιμετωπίζει επιθέσεις ακεραιότητας, όπως βυζαντινές επιθέσεις (επιθέσεις όπου οι αντίπαλοι έχουν τον πλήρη έλεγχο ενός αριθμού συσκευών που έχουν πιστοποιηθεί και συμπεριφέρονται αυθαίρετα ΄ώστε να διακόψουν το δίκτυο) και επιθέσεις τροποποίησης (Wu et al., 2018). Οι επιθέσεις έγχυσης σε συγκεντρωτικές διαμορφώσεις IoT αμφισβητούν την ακεραιότητα των δεδομένων καθώς η πολιτική λήψης αποφάσεων σε αυτές τις διαμορφώσεις βασίζεται στις εισερχόμενες ροές δεδομένων. Ο χρόνος διακοπής λειτουργίας του IoT, η κλοπή και η αλλαγή δεδομένων μπορεί να οδηγήσουν σε απώλειες διαφορετικής έντασης. Η διασφάλιση της ασφάλειας είναι υψίστης σημασίας για ένα σύστημα όπου απαιτείται αυτόνομη αλληλεπίδραση μεταξύ έξυπνων συσκευών. Οι τρέχουσες λύσεις ασφάλειας IoT περιλαμβάνουν λύσεις ασφαλείας που βασίζονται σε τρίτους και είναι συγκεντρωτικές .

Η χρήση του Blockchain για την επιβολή της ασφάλειας χωρίς να εξαρτάται από τρίτο μέρος έχει αποδειχθεί σημαντικά επωφελής για τα συστήματα IoT. Με τα πλεονεκτήματα της ενσωματωμένης προστασίας, της δυνατότητας ελέγχου, του σχεδιασμού με ανοχή σε σφάλματα και της αποκεντρωμένης υποδομής δημόσιου κλειδιού έναντι πολυάριθμων επιθέσεων, το Blockchain είναι σε θέση να παρέχει ασφάλεια σε συναλλακτικά δίκτυα όπως το Bitcoin. Δεδομένου ότι όλες οι συσκευές που εμπλέκονται σε μια συναλλαγή διαθέτουν μια αποκλειστική διεύθυνση Blockchain, η λύση που βασίζεται σε Blockchain είναι ανθεκτική στον ψευδή έλεγχο ταυτότητας. Τα πρωτόκολλα συναίνεσης του Blockchain είναι ικανά να αποτρέπουν κακόβουλους χρήστες από επιθέσεις DoS καθώς απαιτούνται τέλη συναλλαγών κάθε φορά ακόμη και για την πραγματοποίηση κενών συναλλαγών (Wan et al., 2019). Συνεπώς, το Blockchain αποδεικνύεται να είναι περισσότερο από ικανό να παρέχει βελτιωμένη ασφάλεια στη στοίβα IoT.

3.7.2 Blockchain και Παροχή Ελέγχου Πρόσβασης

Στο πρόσφατο παρελθόν, πολλοί ερευνητές πρότειναν την επιβολή πολιτικών ελέγχου πρόσβασης σε ένα σύστημα IoT χωρίς την ανάγκη ανάμειξης τρίτων. Οι (Axon & Goldsmith, 2017) παρουσίασαν μια ανεκτική σε σφάλματα και ασφαλή υποδομή δημόσιου κλειδιού. Οι (Hashemi et al. 2016) παρουσίασαν μια πολυεπίπεδη αρχιτεκτονική Blockchain που εκτελεί έλεγχο πρόσβασης και αποθήκευση δεδομένων σε διαφορετικά επίπεδα. Το προτεινόμενο πλαίσιο αποτελείται από τρία επίπεδα:

- αποκεντρωμένη αποθήκευση που βασίζεται σε Blockchain για την αποθήκευση των δεδομένων του χρήστη.
- μηχανισμό ελέγχου πρόσβασης
- ροή μηνυμάτων για διαπραγματευτική πρόσβαση μεταξύ των δύο μερών.

Τα δεδομένα του Blockchain αποθηκεύονται σε κρυπτογραφημένη μορφή που μπορεί να αποκρυπτογραφηθεί μόνο από τους συμμετέχοντες που διαθέτουν δικαιώματα πρόσβασης. Οι (Zhang & Wen, 2017) εισήγαγαν μια προσέγγιση ελέγχου πρόσβασης που βασίζεται σε διακριτικά στο IoT. Οι (Quaddah et al., 2016) παρουσίασαν μια προσέγγιση ελέγχου πρόσβασης με token που εκχωρεί διαφορετικούς ρόλους πρόσβασης σε διαφορετικούς χρήστες ενώ τα δικαιώματα πρόσβασης μπορούν να ανακληθούν χρησιμοποιώντας έξυπνες συμβάσεις. Ο (Novo, 2018) πρότεινε την αποθήκευση κρυπτογραφημένων κομματιών δεδομένων σε Blockchain και χρησιμοποίησε πολιτικές έξυπνων συμβολαίων και μια προσέγγιση με token για την ανάκληση και την παροχή πρόσβασης σε δεδομένα IoT.

Το Blockchain μπορεί να χρησιμοποιηθεί για τον εντοπισμό κακόβουλης δραστηριότητας και τη διαχείριση των προνομίων πρόσβασης σε προσεγγίσεις που επικεντρώνονται στη σχεδίαση εφαρμογών χωρίς την ανάπτυξη token ή μείωση των τελών συναλλαγών. Οι (Dorri et al. 2017) πρότειναν τη χρήση τοπικών Blockchain συνδεδεμένων με δημόσια Blockchain επικάλυψης. Οι αποφάσεις σχετικά με τα δικαιώματα πρόσβασης των καταστημάτων Blockchain με δυνατότητα επαλήθευσης δημοσίως είναι ικανές να ανιχνεύουν προσπάθειες μη εξουσιοδοτημένης πρόσβασης. Οι (Ali et al. 2017) ενίσχυσαν την ιδέα μη λαμβάνοντας υπόψη τις συναλλαγές από μη εξουσιοδοτημένους χρήστες. Οι (Shafagh et al., 2017) παρουσίασαν ένα σύστημα ελέγχου πρόσβασης που βασίζεται σε Blockchain και το οποίο αποθηκεύει δεδομένα σε αποκεντρωμένους πίνακες κατακερματισμού εκτός αλυσίδας. Σε αυτό το σενάριο, το Blockchain αποθηκεύει δικαιώματα πρόσβασης για διάφορους χρήστες και οι κόμβοι έχουν πρόσβαση στα αρχεία Blockchain για τη λήψη αποφάσεων ελέγχου πρόσβασης.

3.7.3 Blockchain και Διατήρηση Ακεραιότητας των Δεδομένων

Σε ένα σύστημα IoT που βασίζεται σε Blockchain, ένας αντίπαλος επιχειρεί να δημιουργήσει ψευδή μπλοκ. Ωστόσο, στη δημόσια εφαρμογή Blockchain, αυτό δεν είναι καθόλου δυνατό λόγω της χρήσης κατανεμημένης συναίνεσης για τη διατήρηση των κανονικών αρχείων Blockchain. Οι (Biswas & Muthukkumarasamy, 2016) πρότειναν την εγγύηση της ακεραιότητας των δεδομένων σε συστήματα έξυπνων πόλεων που βασίζονται σε Blockchain. Η δυνατότητα προγραμματισμού ορίστηκε πάνω από τις αποκεντρωμένες εγγραφές Blockchain χρησιμοποιώντας έξυπνα συμβόλαια και Blockchain Ethereum. Οι (Dorri et al., 2017) στην μελέτη τους, πρότειναν τη διατήρηση των εγγραφών τμημάτων δεδομένων IoT στο νέφος χρησιμοποιώντας ένα πολυεπίπεδο πλαίσιο Blockchain. Το χρησιμοποιούμενο δημόσιο Blockchain επικάλυψης διατηρεί αμετάβλητα αρχεία τμημάτων δεδομένων χρησιμοποιώντας κατακερματισμό. Οι (Shafagh et al., 2017) παρουσίασαν ένα σχήμα αποθήκευσης δεδομένων που βασίζεται σε αμετάβλητα αρχεία Blockchain και αποκεντρωμένους πίνακες κατακερματισμού. Το Blockchain διατηρεί τις πολιτικές ακεραιότητας δεδομένων και ελέγχου πρόσβασης, ενώ τα αιτήματα δεδομένων υποβάλλονται στους κόμβους DHT. Οι (Kang et al., 2017) ανέλυσαν ένα σχήμα ακεραιότητας δεδομένων που χρησιμοποιεί Blockchain και εκτελεί ελέγχους ακεραιότητας βάσει ερωτημάτων χωρίς την ανάγκη επαλήθευσης τρίτου μέρους. Η απώλεια ακεραιότητας δεδομένων εντοπίζεται από τη διαδικασία επαλήθευσης αρχείων Blockchain. Οι (Yang et al., 2017) παρουσίασαν ένα σχέδιο αξιολόγησης αξιοπιστίας που βασίζεται σε Blockchain για το Διαδίκτυο των Οχημάτων. Το σύστημα φήμης που βασίζεται σε Blockchain λαμβάνει αποφάσεις σχετικά με την αξιοπιστία του μηνύματος με βάση τη φήμη του αποστολέα.

Η εφαρμογή Blockchain στο IoT για τη λήψη ασφαλών ενημερώσεων λογισμικού είναι ένα πολύ σημαντικό θέμα που συγκεντρώνει το ενδιαφέρον των μελετητών. Οι (Lee & Lee, 2016) πρότειναν σχήματα peer to peer στα οποία οι ενσωματωμένες συσκευές IoT λαμβάνουν ασφαλείς ενημερώσεις και διασφαλίζουν την ακεραιότητα υλικολογισμικού σε ένα δίκτυο Blockchain. Οι (Steger et al., 2018) πρότειναν στη μελέτη τους επεκτασιμότητα η οποία διασφαλίζει κλιμακωτή αρχιτεκτονική Blockchain και ασφαλή συστήματα ενημέρωσης λογισμικού για έξυπνα οχήματα. Αυτό επιτρέπει στις ενημερώσεις λογισμικού να διαδίδονται στα οχήματα με ασφαλή τρόπο χωρίς να διακυβεύεται η ακεραιότητα των δεδομένων. Περαιτέρω, οι (Boudguiga et al., 2017) πρότειναν τη χρήση αδειοδοτημένων Blockchain για την αποθήκευση των ενημερώσεων λογισμικού με ασφαλή τρόπο peer to peer για συσκευές IoT.

3.7.4 Blockchain και Βελτίωση Διαθεσιμότητας

Οι λύσεις που παρέχουν αποθήκευση δεδομένων σε αλυσίδα δεν έχουν κεντρικά ευάλωτα σημεία και επομένως διαθέτουν ενσωματωμένες δυνατότητες διαθεσιμότητας. Αυτή η διαθεσιμότητα των αρχείων αλληλεπίδρασης βελτιώνεται περαιτέρω με μηχανισμούς αποθήκευσης εκτός αλυσίδας. Στο σημείο αυτό αναλύονται οι μοναδικές σχεδιαστικές λύσεις που προτείνονται για τη βελτίωση της διαθεσιμότητας του IoT. Οι (Alphand et al., 2018) πρότειναν στην εργασία τους ένα σχέδιο εξουσιοδότησης για το IoT που χρησιμοποιεί Blockchain. Οι (Chakraborty et al., 2018) ανέπτυξαν λύση για το χειρισμό προβλημάτων περιορισμένων πόρων των συσκευών IoT χρησιμοποιώντας πολυεπίπεδες λύσεις Blockchain. Οι κόμβοι που βρίσκονται στο υψηλότερο επίπεδο διαθέτουν υψηλότερες δυνατότητες αποθήκευσης και υπολογισμού, ενώ οι κόμβοι με περιορισμένους πόρους που βρίσκονται στα χαμηλότερα επίπεδα δεν είναι ικανοί να επιβάλλουν πολιτικές ασφαλείας. Οι κόμβοι υψηλότερου επιπέδου διευκολύνουν τις επικοινωνίες μεταξύ των κόμβων χαμηλότερου επιπέδου με περιορισμένους πόρους. Οι (Ali et al., 2017) πρότειναν ένα έξυπνο συμβόλαιο και πολυεπίπεδο σύστημα Blockchain για να εγγυηθεί τον έλεγχο πρόσβασης. Η δημόσια αλυσίδα μπλοκ Ethereum χρησιμοποιείται στο υψηλότερο επίπεδο ώστε να διασφαλίζεται η διαθεσιμότητα. Οι (Bahga & Madisetti, 2016) ανέλυσαν ένα σύστημα παραγωγής βασισμένο σε Blockchain στο οποίο οι χρήστες έχουν την ευελιξία να εκδίδουν απευθείας εντολές κατασκευής κατά τη διάρκεια των συναλλαγών το οποίο είναι επωφελές για πολλές συναλλαγές, όπως είναι η παρακολούθηση της εφοδιαστικής αλυσίδας, η διάγνωση μηχανημάτων και η κατασκευή κατ' απαίτηση. Οι συγγραφείς παρουσίασαν επίσης περιπτώσεις χρήσης διαγνωστικών και συντήρησης μηχανήματος. Αυτή η αποκεντρωμένη συνδεδεμένη συσκευή επιτρέπει στο δίκτυο να παραμένει ζωντανό ακόμα και σε περίπτωση πολλαπλών σφαλμάτων του μηχανήματος.

3.7.5 Blockchain και Διασφάλιση Εμπιστευτικότητας των Δεδομένων

Οι αρχιτεκτονικές που βασίζονται σε Blockchain διαθέτουν ενσωματωμένα χαρακτηριστικά εμπιστευτικότητας και εξουσιοδότησης, καθώς περιλαμβάνουν κάθε συναλλαγή που πρέπει να υπογράφεται χρησιμοποιώντας το ιδιωτικό κλειδί του εκδότη. Οι (Axon & Goldsmith, 2017) πρότειναν ένα PKI που βασίζεται σε Blockchain για την αποτελεσματική διαχείριση των συστημάτων IoT. Χρησιμοποίησαν έξυπνες συμβάσεις για την έκδοση εντολών, όπως η καταγραφή πληροφοριών χρήσης ενέργειας και η αλλαγή πολιτικών εργασίας στο Blockchain. Οι (Ouaddah et al., 2016) πρότειναν μια προσέγγιση με token με το όνομα «Fair Access» που επιτρέπει δικαιώματα πρόσβασης με την έκδοση προσαρμοσμένου κρυπτονομίσματος στις συναλλαγές. Το ιδιωτικό κλειδί του αιτούντος χρησιμοποιείται για την υπογραφή των συναλλαγών παραχώρησης πρόσβασης που επιτρέπουν εμπιστευτικά ανακληθέντα δικαιώματα πρόσβασης. Οι (Alphand et al., 2018) ανέπτυξαν μια πλατφόρμα διαχείρισης ασφάλειας IoT που διατηρεί αρχεία αλληλεπίδρασης και επιβάλλει πολιτικές εξουσιοδότησης. Οι ερευνητές χρησιμοποίησαν Blockchain για την επιβολή ευελιξίας στον καθορισμό των πολιτικών εξουσιοδότησης μαζί με τη διατήρηση αρχείου συμβάντων πρόσβασης. Οι (Aitzhan & Svetinovic, 2016) πρότειναν συστήματα ασφαλείας για την επιβολή του απορρήτου στα έξυπνα δίκτυα συναλλαγών ενέργειας κάτι που ουσιαστικά στοχεύει στην απόκρυψη της ταυτότητας του παραγωγού ενέργειας διατηρώντας τις κοινοποιημένες πληροφορίες εμπιστευτικές. Οι μελετητές πρότειναν να δημιουργήσουν και να αλλάξουν τη διεύθυνση των παραγωγών ενέργειας προκειμένου να κρύψουν την ταυτότητα του παραγωγού. Οι (Cha et al., 2018) παρουσίασαν ένα Blockchain που βασίζεται στην υπογραφή που χρησιμοποιεί το Blockchain Ethereum για τη διατήρηση της εμπιστευτικότητας μεταξύ των πυλών IoT και των wearables. Αυτές οι πύλες χρησιμοποιούν έξυπνες συμβάσεις για την αλληλεπίδραση με αυτές τις συσκευές, καθιστώντας έτσι εμπιστευτικές τις αλληλεπιδράσεις IoT.

3.7.6 Εφαρμογές BIoT

Η τεχνολογία αλυσίδας συστοιχιών (Blockchain - BC) μπορεί να εφαρμοστεί σε πολλούς τομείς και για διάφορες περιπτώσεις. Μερικοί συγγραφείς, όπως ο (Swan, 2015), ανέφεραν ότι η εξέλιξη της δυνατότητας της εφαρμογής Blockchain ξεκίνησε με το Bitcoin (Blockchain 1.0), στη συνέχεια εξελίχθηκε προς τα έξυπνα συμβόλαια (Blockchain 2.0) και αργότερα μεταφέρθηκε στις εφαρμογές δικαιοσύνης, αποτελεσματικότητας και συντονισμού (Blockchain 3.0). Όσον αφορά τα έξυπνα συμβόλαια, ορίζονται ως κομμάτια αυτοδύναμου αποκεντρωμένου κώδικα που εκτελούνται αυτόνομα όταν πληρούνται ορισμένες προϋποθέσεις. Τα έξυπνα συμβόλαια μπορούν να εφαρμοστούν σε πολλές πρακτικές περιπτώσεις, συμπεριλαμβανομένων διεθνών μεταφορών, στεγαστικών δανείων ή χρηματοδότησης από κοινού.

Η Ethereum είναι αναμφισβήτητα η πιο δημοφιλής πλατφόρμα που βασίζεται σε αλυσίδα συστοιχιών για την εκτέλεση έξυπνων συμβάσεων, αν και στην πραγματικότητα μπορεί να ‘τρέξει’ και άλλες κατανεμημένες εφαρμογές και να αλληλοεπιδράσει με περισσότερες από μία αλυσίδες συστοιχιών. Στην πραγματικότητα, η Ethereum χαρακτηρίζεται ως πληρότητα Turing (Turing-complete), δηλαδή ως μια μαθηματική έννοια που δείχνει ότι η γλώσσα προγραμματισμού της Ethereum μπορεί να χρησιμοποιηθεί για την προσομοίωση οποιασδήποτε άλλης γλώσσας.

Πέρα από τα κρυπτονομίσματα και τα έξυπνα συμβόλαια, οι τεχνολογίες της αλυσίδας συστοιχιών μπορούν να εφαρμοστούν σε διαφορετικούς τομείς όπου εμπλέκονται εφαρμογές IoT, όπως ανίχνευση, αποθήκευση δεδομένων, διαχείριση ταυτότητας, υπηρεσίες χρονοσήμανσης, εφαρμογές έξυπνης διαβίωσης, έξυπνα συστήματα μεταφοράς, φορέσιμη τεχνολογία (wearables), διαχείριση εφοδιαστικής αλυσίδας, ανίχνευση πλήθους μέσω κινητού, καθώς επίσης και στον νόμο και την ασφάλεια του κυβερνοχώρου σε κρίσιμα σενάρια. Η αλυσίδα συστοιχιών μπορεί επίσης να χρησιμοποιηθεί σε γεωργικές εφαρμογές IoT. Για παράδειγμα, στη μελέτη του συγγραφέα (Tian, 2016) παρουσιάζεται ένα σύστημα ιχνηλασιμότητας για την παρακολούθηση των κινεζικών προμηθειών αγροδιατροφής. Το σύστημα βασίζεται στη χρήση της αναγνώρισης ραδιοσυχνοτήτων (Radio Frequency Identification - RFID) και μιας αλυσίδας συστοιχιών, με στόχο να βελτιώσει την ασφάλεια και την ποιότητα των τροφίμων και να μειώσει τις απώλειες στη διαχειριστική υποστήριξη.

Άλλοι συγγραφείς όπως οι (Huh et al., 2017) επικεντρώθηκαν στη διαχείριση συσκευών IoT μέσω μιας αλυσίδας συστοιχιών. Πρότειναν ένα σύστημα ικανό να ελέγχει και να ρυθμίζει τις συσκευές IoT εξ αποστάσεως. Το σύστημα αυτό αποθηκεύει δημόσια κλειδιά στην Ethereum, ενώ τα ιδιωτικά κλειδιά αποθηκεύονται σε κάθε συσκευή IoT. Οι συγγραφείς υποδεικνύουν ότι η χρήση της πλατφόρμας Ethereum είναι απαραίτητη, καθώς τους επιτρέπει να γράφουν τον δικό τους κώδικα για εκτέλεση εντολών στο δίκτυο. Επιπλέον, η ενημέρωση του κώδικα στην Ethereum τροποποιεί τη συμπεριφορά των συσκευών IoT, κάτι που απλοποιεί τη συντήρηση και τις διορθώσεις σφαλμάτων.

Ο ενεργειακός τομέας μπορεί επίσης να επωφεληθεί από την εφαρμογή μιας αλυσίδας συστοιχιών στο IoT ή στο Διαδίκτυο της ενέργειας (Internet of Energy - IoE). Ένα παράδειγμα περιγράφεται λεπτομερώς στη μελέτη των (Lundqvist et al., 2017) όπου οι συγγραφείς προτείνουν ένα σύστημα που βασίζεται σε αλυσίδα συστοιχιών, το οποίο επιτρέπει στις συσκευές IoT/IoE να πληρώνουν η μία την άλλη για υπηρεσίες χωρίς να απαιτείται ανθρώπινη παρέμβαση. Στη μελέτη αυτή περιγράφεται επίσης μια υλοποίηση η οποία απεικονίζει τις δυνατότητες του συστήματος και πιο συγκεκριμένα, τη σύνδεση ενός έξυπνου καλωδίου με μια έξυπνη πρίζα, καθιστώντας δυνατή την πληρωμή της καταναλώσιμης ηλεκτρικής ενέργειας μέσω του συστήματος. Επιπλέον, για να μειώσουν τα τέλη συναλλαγών κρυπτονομισμάτων όπως το Bitcoin, οι συγγραφείς παρουσιάζουν ένα πρωτόκολλο μικροπληρωμών ενιαίας χρέωσης που συγκεντρώνει πολλές μικρές πληρωμές σε μια μεγαλύτερη συναλλαγή.

Αρκετές εφαρμογές της BIoT (BC & IoT) που αφορούν τον τομέα της υγείας, εντοπίζονται επίσης σε διάφορες μελέτες. Για παράδειγμα, στη μελέτη των (Bocek et al., 2017) παρουσιάζεται μια εφαρμογή ιχνηλασιμότητας που χρησιμοποιεί αισθητήρες IoT και τεχνολογία BC τόσο για την επαλήθευση της ακεραιότητας των δεδομένων, όσο και για τη δημόσια πρόσβαση σε αρχεία θερμοκρασίας στην αλυσίδα εφοδιασμού φαρμακευτικών προϊόντων. Αυτή η επαλήθευση είναι κρίσιμης σημασίας για τη μεταφορά ιατρικών προϊόντων προκειμένου να διασφαλιστεί η ποιότητά τους και οι περιβαλλοντικές συνθήκες (δηλαδή η θερμοκρασία και η σχετική υγρασία τους). Έτσι, κάθε δέμα που αποστέλλεται περιέχει έναν αισθητήρα που μεταφέρει τα συλλεγμένα δεδομένα στην αλυσίδα συστοιχιών, όπου ένα έξυπνο συμβόλαιο καθορίζει εάν οι λαμβανόμενες τιμές παραμένουν εντός του επιτρεπόμενου εύρους. Μια άλλη εφαρμογή BIoT για την υγεία περιγράφεται λεπτομερώς στη μελέτη των (Shae & Tsai, 2017), όπου παρουσιάζεται η αρχιτεκτονική μιας πλατφόρμας βασισμένης σε αλυσίδα συστοιχιών για κλινικές δοκιμές και για το ιατρικό μοντέλο του ακριβές φαρμάκου (Precision medicine). Αξίζει επίσης να αναφερθεί η εργασία που περιγράφεται στη μελέτη των (Salahuddin et al., 2017), η οποία παρουσιάζει ένα γενικό έξυπνο σύστημα υγειονομικής περίθαλψης που χρησιμοποιεί συσκευές IoT, υπολογιστικό νέφος και ομίχλη (cloud and fog computing), μία αλυσίδα συστοιχιών τύπου Tor και μεσίτες μηνυμάτων (Message brokers).

Επιπρόσθετα, η τεχνολογίας της αλυσίδας συστοιχιών μπορεί επίσης να βελτιώσει την ασφάλεια χαμηλού επιπέδου του IoT. Ειδικότερα, μπορεί να βελτιωθεί η απομακρυσμένη πιστοποίηση, η οποία είναι η διαδικασία που επαληθεύει εάν η υποκείμενη βάση αξιόπιστων υπολογιστών (Trusted Computer Base - TCB) μιας συσκευής, είναι αξιόπιστη. Αυτή η επαλήθευση μπορεί να πραγματοποιηθεί με τη διαχείριση των μετρήσεων TCB, οι οποίες λαμβάνονται χρησιμοποιώντας συνδυαστικά την τεχνολογία ARM TrustZone και μίας αλυσίδας συστοιχιών, όπου αποθηκεύονται με ασφάλεια. Άλλες, ήδη προτεινόμενες εφαρμογές BIoT, σχετίζονται με έξυπνες πόλεις (Biswas & Muthukkumarasamy, 2016) και βιομηχανικές διαδικασίες (Ahram et al., 2017). Στην περίπτωση των έξυπνων πόλεων προτείνεται ένα πλαίσιο που ενσωματώνει έξυπνες συσκευές με ασφαλή τρόπο για την παροχή εφαρμογών έξυπνων πόλεων. Ενώ, στις βιομηχανικές διαδικασίες εξετάζονται διάφορες βιομηχανικές εφαρμογές που βασίζονται σε αλυσίδα συστοιχιών, συμπεριλαμβανομένης της σύνδεσής τους με βιομηχανικά δίκτυα IoT (Industrial IoT - IIoT).

Τέλος, πρέπει να αναφερθεί ότι τα μεγάλα δεδομένα (Big Data) μπορούν να αξιοποιηθούν από την τεχνολογία της αλυσίδας συστοιχιών ούτως ώστε να διασφαλιστεί η αξιοπιστία τους. Έτσι, ορισμένοι ερευνητές όπως οι (Karafiloski & Mishev, 2017) εξέτασαν τις κύριες λύσεις που βασίζονται σε αλυσίδα συστοιχιών για τη συλλογή και τον έλεγχο τεράστιων ποσοτήτων δεδομένων που μπορεί να συλλέγονται από Δίκτυα IoT.

3.8 Τρέχουσες προκλήσεις για εφαρμογές BIoT

Σήμερα, οι αναδυόμενες τεχνολογίες στο οικοσύστημα του IoT όπως τα κυβερνο-φυσικά συστήματα (Cyber-Physical Systems - CPS), τα συστήματα RFID, τα συστήματα τηλεμετρίας ή οι ευρυζωνικές επικοινωνίες 4G/5G, αντιμετωπίζουν αρκετές προκλήσεις. Συγκεκριμένα, η περίπτωση των σεναρίων που αφορούν τον κρίσιμο παράγοντα αποστολής ενός συστήματος (Mission critical) εγείρουν πρόσθετες ανησυχίες. Η προσθήκη της αλυσίδας συστοιχιών στο ήδη υπάρχον ζήτημα, συνεπάγεται με περαιτέρω λειτουργικές και τεχνικές απαιτήσεις, καθώς η ανάπτυξη εφαρμογών BIoT είναι μια πολύπλοκη διαδικασία που επηρεάζεται από πολλές πτυχές που συνδέονται μεταξύ τους. Οι κύριοι παράγοντες περιγράφονται στις επόμενες υπό-ενότητες και απεικονίζονται στην Εικόνα 2 παρακάτω.

Σχήμα 3-5. Οι περισσότεροι σχετικοί παράγοντες που καθορίζουν την ανάπτυξη μιας εφαρμογής BIoT και οι κύριες σχέσεις τους. Πηγή: (Fernández-Caramés & Fraga-Lamas, 2018).

3.8.1 Απόρρητο

Στην εργασία των (Kravitz & Cooper, 2017) έχει προταθεί η χρήση επιτρεπόμενων αλυσίδων μπλοκ, για ευαίσθητες εφαρμογές κάτι που παρέχει μια αρχή πιστοποίησης ταυτότητας η οποία επιτρέπει στους χρήστες και τους κόμβους να συμμετέχουν στο Blockchain. Το γεγονός αυτό έχει υπέρ και κατά. Στα πλεονεκτήματα θα πρέπει να συμπεριληφθεί το ότι ένα επιτρεπόμενο Blockchain με μια αρχή θα παρείχε κάποια προστασία στους κόμβους, κάτι όμως που μπορεί να αποβεί πολύ επικίνδυνο, επειδή όταν ένας εισβολέας καταλάβει τον κόμβο που ενεργεί ως αρχή πιστοποιητικού, ολόκληρο το σύστημα μπορεί να τεθεί σε κίνδυνο. Η μόνη λύση σε αυτό το πρόβλημα είναι να υπάρχει μια ιδιωτική αλυσίδα μπλοκ που θα εφαρμόζεται σωστά, έτσι ώστε η αρχή έκδοσης πιστοποιητικών να χρειάζεται να εκτελέσει ένα έξυπνο συμβόλαιο για να προσθέσει έναν νέο κόμβο, ο οποίος πρέπει να ακολουθείται από συναίνεση από όλους τους κόμβους ώστε να πραγματοποιηθούν όλες οι αλλαγές.

Τα συστήματα αυτόματης επαλήθευσης ταυτότητας για εφαρμογές IoT αναφέρονται επίσης στην εργασία των (Shi et al., 2020), όπου οι ερευνητές παρουσίασαν ένα σύστημα βασισμένο σε Blockchain για εφαρμογές IoT το οποίο θα ήταν σε θέση να αποκτήσει αυτόματα τις υπογραφές συσκευών IoT, προσδιορίζοντας έτσι συσκευές και χρήστες. Έχουν αναλυθεί ορισμένες λύσεις μηχανικής εκμάθησης που βασίζονται σε Blockchain για λύσεις IoT.

Η λύση που δόθηκε από τους (Mendis et al., 2020) χρησιμοποιεί προσέγγιση βαθιάς μάθησης, η οποία λειτουργεί με κατανεμημένο τρόπο ώστε όλη η εκπαίδευση να μην γίνεται σε μία συσκευή (Raspberry Pi). Δεν υπάρχει καμία εφαρμογή που να χρησιμοποιεί ενισχυτική μάθηση για τέτοια διατήρηση του απορρήτου. Αυτό οφείλεται στο γεγονός ότι από τη στιγμή που η εκπαίδευση μπορεί να γίνει με κατανεμημένο τρόπο, τότε θα έπρεπε να υπάρχει αποτελεσματική εφαρμογή που να επανεκπαιδεύει το παραγόμενο μοντέλο με παρόμοιο τρόπο.

Όλοι οι χρήστες μιας αλυσίδας συστοιχιών προσδιορίζονται από το δημόσιο κλειδί (public key) ή το κατακερματισμό του. Αυτό σημαίνει ότι η ανωνυμία δεν είναι εγγυημένη και δεδομένου ότι όλες οι συναλλαγές είναι κοινές, είναι δυνατό για τρίτους να αναλύσουν τέτοιες συναλλαγές και να συναγάγουν την πραγματική ταυτότητα των συμμετεχόντων. Το απόρρητο είναι ακόμη πιο περίπλοκο σε περιβάλλοντα IoT, καθώς οι συσκευές IoT μπορούν να αποκαλύψουν ιδιωτικά δεδομένα του εκάστοτε χρήστη, τα οποία θα μπορούσαν να αποθηκευτούν σε μια αλυσίδα συστοιχιών. Οι απαιτήσεις απορρήτου της αλυσίδας συστοιχιών διαφέρουν από χώρα σε χώρα. Επομένως, σε αντίθεση με τις παραδοσιακές διαδικτυακές πληρωμές, οι οποίες είναι συνήθως ορατές μόνο σε συναλλασσόμενους και σε μεσάζοντες (π.χ. χρηματοπιστωτικά ιδρύματα, κυβέρνηση), οι διαφανείς συναλλαγές που ενθαρρύνονται από την αλυσίδα συστοιχιών αποτελούν πρόκληση όσον αφορά το απόρρητο.

Η πιστοποίηση ταυτότητας μπορεί επίσης να αποτελεί ένα σημαντικό πρόβλημα στο IoT καθώς εάν ένας πάροχος ταυτότητας είναι υπεύθυνος για την εξουσιοδότηση οντοτήτων, μπορεί επίσης να τους αποκλείσει. Για την αντιμετώπιση μιας τέτοιας πρόκλησης προτείνεται, σύμφωνα με τη μελέτη των (Kravitz & Cooper, 2017), η χρήση μιας επιτρεπόμενης αλυσίδας συστοιχιών για την ασφάλεια και τη διαχείριση πολλαπλών κόμβων IoT. Το προτεινόμενο σύστημα παρέχει μια κατανεμημένη λύση διαχείρισης ταυτότητας που αυξάνει την ασφάλεια και την προστασία από επιθέσεις με περιστρεφόμενα ασύμμετρα κλειδιά. Τέτοια κλειδιά δημιουργούνται τοπικά στη συσκευή και δεν μετακινούνται ποτέ από αυτήν. Για την επαλήθευση της ταυτότητας ενός χρήστη κατά την περιστροφή των κλειδιών, το σύστημα χρησιμοποιεί έναν μηχανισμό που ονομάζεται μέλος ομάδας συσκευών (Device Group Membership - DGM). Αυτό περιλαμβάνει σε μια ομάδα, όλες τις συσκευές που ανήκουν σε έναν χρήστη. Έπειτα, όταν ένας χρήστης πραγματοποιεί μια συναλλαγή, αυτή αντανακλάται στην αλυσίδα συστοιχιών καθώς εκτελέστηκε από μια συσκευή που ανήκε στην ομάδα των χρηστών. Η προτεινόμενη λύση ενισχύει επίσης την ασφάλεια χρησιμοποιώντας ένα σύστημα πιστοποιητικών για έλεγχο ταυτότητας και επιτρέποντας την αντικατάσταση της συνάρτησης κατακερματισμού (εφόσον παραβιαστεί). Αξίζει επίσης να αναφερθεί ότι το σύστημα μπορεί να τροποποιηθεί για να περιορίσει την ποσότητα των προσωρινών δεδομένων που αποθηκεύονται, κάτι που είναι χρήσιμο για συσκευές IoT με μικρό χώρο αποθήκευσης (για παράδειγμα, θα μπορούσαν να αποθηκευτούν μόνο τα δεδομένα από τις προηγούμενες 24 ώρες). Μια άλλη προσέγγιση που επικεντρώνεται στην επίλυση των προβλημάτων ιδιωτικότητας και ευρωστίας που προκύπτουν από τη χρήση κεντρικών συστημάτων διαχείρισης ταυτότητας περιγράφεται στη μελέτη των (Dorri et al., 2017). Σε αυτήν οι συγγραφείς τονίζουν την ανάγκη παροχής συστημάτων αυτόματης επαλήθευσης ταυτότητας για εφαρμογές IoT, όπου απαιτείται επεκτασιμότητα και όπου η ετερογένεια και η κινητικότητα της συσκευής είναι κοινές. Για την αντιμετώπιση τέτοιων προκλήσεων, οι συγγραφείς παρουσιάζουν ένα σύστημα βασισμένο σε αλυσίδα συστοιχιών για έξυπνα σπίτια IoT, το οποίο εξάγει αυτόματα τις υπογραφές της συσκευής προκειμένου να αναγνωρίζει τόσο τις συσκευές όσο και τους χρήστες τους.

Μία ακόμη πρόκληση είναι η διαχείριση πρόσβασης στα δίκτυα IoT. Μερικοί ερευνητές όπως οι (Hashemi et al., 2016), πρότειναν τη βελτίωσή της, ορίζοντας έναν μηχανισμό πολλαπλών επιπέδων βασισμένο σε αλυσίδα συστοιχιών, ο οποίος θα καθόριζε τις δυνατότητες, τις λίστες πρόσβασης και τα δικαιώματα πρόσβασης. Ωστόσο, πρέπει να σημειωθεί ότι σε πολλές εφαρμογές IoT η ανωνυμία δεν είναι απαραίτητη. Το απόρρητο των συναλλαγών απαιτείται σε ορισμένα σενάρια όταν τα συλλεγόμενα δεδομένα ενδέχεται να επιτρέπουν την παρακολούθηση και την πρόβλεψη της συμπεριφοράς ή των συνηθειών των ανθρώπων. Αυτό είναι ήδη ένα ζήτημα σε τομείς όπως τα συστήματα καρτών μεταφοράς που βασίζονται σε RFID, όπου οι αποθηκευμένες πληροφορίες (δηλαδή, ταξίδια, υπόλοιπο, προσωπικά δεδομένα) είναι υποτίθεται ανώνυμες, αλλά στην πράξη μπορεί να συλλέγονται από τρίτους. Το ζήτημα είναι ακόμη πιο προβληματικό κατά την προσθήκη μίας αλυσίδας συστοιχιών, καθώς οι συναλλαγές μοιράζονται μεταξύ ομοτίμων, κάτι που σε ορισμένους τομείς όπως η βιομηχανία ή τα χρηματοοικονομικά συστήματα, επιτρέπει την παρακολούθηση της δραστηριότητας των ανταγωνιστών. Ως εκ τούτου, πρέπει να προταθούν λύσεις για τον μετριασμό αυτών των ζητημάτων απορρήτου. Για παράδειγμα, στην περίπτωση των δημόσιων αλυσίδων συστοιχιών, ο χρήστης δεν χρειάζεται να γνωρίζει τη διεύθυνση κάθε χρήστη, παρά μόνο του αντισυμβαλλομένου με τον οποίο συναλλάσσεται. Εάν ένας συμμετέχων σε αλυσίδα συστοιχιών χρησιμοποιεί μια νέα διεύθυνση για κάθε συναλλαγή, η ανάλυση δεδομένων θα γίνει σαφώς πιο δύσκολη. Αυτό είναι παρόμοιο με αυτό που έχουν εφαρμόσει οι κατασκευαστές smartphone για να αποφύγουν την παρακολούθηση Wi-Fi. Μια πιο πρακτική αλλά λιγότερο ανώνυμη λύση θα συνίστατο στη χρήση μιας μοναδικής διεύθυνσης για κάθε αντισυμβαλλόμενο. Από την άλλη πλευρά, σε μία ιδιωτική αλυσίδα συστοιχιών και εφόσον εκτελούνται έλεγχοι πρόσβασης, υπάρχει τουλάχιστον ένας κόμβος που γνωρίζει ποιος έχει πρόσβαση στο σύστημα. Υποθέτοντας την ουδετερότητα του ελεγκτή πρόσβασης, είναι δυνατό να μειωθεί η έκθεση δημιουργώντας μια ανεξάρτητη αλυσίδα συστοιχιών με κάθε οντότητα με την οποία συνεργάζεται ένας χρήστης. Αυτή η ρύθμιση αυξάνει την πολυπλοκότητα των επικοινωνιών, αλλά απομονώνει τον χρήστη από τη μη επιθυμητή παρακολούθηση. Για παράδειγμα, η πολυαλυσίδα (Multichain) παρέχει μια λύση για την ανάπτυξη ιδιωτικών αλυσίδων συστοιχιών (μπορεί να λειτουργήσει με διαφορετικές αλυσίδες συστοιχιών ταυτοχρόνως) που διασφαλίζει ότι οι δραστηριότητες στην αλυσίδα συστοιχιών μπορούν να παρακολουθούνται από επιλεγμένους συμμετέχοντες.

Οι τεχνικές ανάμειξης μπορούν επίσης να βοηθήσουν στη βελτίωση του απορρήτου. Τέτοιες τεχνικές είναι ικανές να συλλέγουν συναλλαγές από διάφορες συσκευές IoT και να εξάγουν συμβάντα ή άλλες συναλλαγές σε διαφορετικές διευθύνσεις που δεν συνδέονται με τις αρχικές συσκευές. Αυτές οι τεχνικές αυξάνουν το απόρρητο, αλλά δεν είναι τέλειες, καθώς ενδέχεται να απο-ανωνυμοποιηθούν μέσω επιθέσεων αποκάλυψης των στατιστικών στοιχείων. Για την αντιμετώπιση αυτών των ζητημάτων, προτάθηκαν διάφορες λύσεις κυρίως όσον αφορά την αποκάλυψη της κλοπής μέσω ενός μηχανισμού λογοδοσίας ή την απόκρυψη της αντιστοίχισης διεύθυνσης εισόδου/εξόδου από τον διακομιστή μίξης. Το απόρρητο μπορεί επίσης να αυξηθεί μέσω τεχνικών απόδειξης μηδενικής γνώσης, όπως αυτές που χρησιμοποιούνται από το Zerocoin, το Zerocash ή το Zcash. Η απόδειξη μηδενικής γνώσης είναι μια μέθοδος που αποδεικνύει σε έναν αντισυμβαλλόμενο ότι ένας χρήστης γνωρίζει ορισμένες πληροφορίες χωρίς να αποκαλύψει μια τέτοια πληροφορία. Στην περίπτωση εφαρμογών IoT, αποδείξεις μηδενικής γνώσης μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας ή κατά τη διάρκεια τακτικών συναλλαγών, προκειμένου να αποφευχθεί η αποκάλυψη της ταυτότητας ενός χρήστη ή μιας συσκευής. Ωστόσο, αυτές οι αποδείξεις δεν είναι απρόσβλητες από επιθέσεις. Στην πραγματικότητα, όπως στην περίπτωση των τεχνικών μίξης, είναι επιρρεπείς σε απο-ανωνυμοποίηση μέσω επιθέσεων στατιστικής αποκάλυψης, αλλά βελτιώνουν τις τεχνικές μίξης αποφεύγοντας την ανάγκη για έναν διακομιστή μίξης (ο οποίος μπορεί να δημιουργήσει συμφόρηση ασφάλειας ή απόδοσης).

Πρέπει επίσης να επισημανθούν οι προσπάθειες που επικεντρώνονται στο απόρρητο και πραγματοποιούνται μέσω διαφόρων υπηρεσιών όπως το Bytecoin ή το Monero, τα οποία βασίζονται στο CryptoNote. Το CryptoNote είναι ένα πρωτόκολλο που χρησιμοποιεί υπογραφές δακτυλίου και του οποίου οι συναλλαγές δεν μπορούν να παρακολουθηθούν μέσω της αλυσίδας συστοιχιών. Με αυτόν τον τρόπο δεν μπορεί να προσδιοριστεί ποιος εκτέλεσε την κάθε συναλλαγή, αυξάνοντας την ικανότητα του απορρήτου. Τα μόνα άτομα που μπορούν να έχουν πρόσβαση στις πληροφορίες συναλλαγής είναι οι ομάδες ατόμων που τις πραγματοποιούν ή όποιος έχει γνώση για ένα από τα δύο ιδιωτικά κλειδιά. Ένα από τα κλειδιά του CryptoNote είναι η εφαρμογή της έννοιας της υπογραφής δακτυλίου (ring signature), η οποία καθιστά δυνατό τον καθορισμό ενός συνόλου πιθανών υπογραφόντων χωρίς να αποκαλύπτεται ποιος από αυτούς δημιούργησε πραγματικά την υπογραφή. Μια άλλη πιθανή λύση για τη διατήρηση της ιδιωτικότητας είναι η χρήση ομομορφικής κρυπτογράφησης (Homomorphic encryption). Ένα τέτοιο είδος κρυπτογράφησης επιτρέπει σε υπηρεσίες IoT τρίτων, να επεξεργάζονται μια συναλλαγή χωρίς να αποκαλύπτουν τα μη κρυπτογραφημένα δεδομένα σε αυτές τις υπηρεσίες. Αρκετοί ερευνητές όπως οι (França, 2015) και (Lukianov, 2015) έχουν προτείνει παραλλαγές στο πρωτόκολλο του Bitcoin για να αυξηθεί η χρήση των ομομορφικών δεσμεύσεων.

Τέλος, αξίζει να σημειωθεί ότι μέρος των μηχανισμών που αναφέρθηκαν προηγουμένως απαιτούν έναν σχετικό αριθμό υπολογιστικών πόρων. Επομένως η δυνατότητα εφαρμογής τους σε συσκευές IoT με περιορισμένους πόρους, είναι επί του παρόντος περιορισμένη.

3.8.2 Ασφάλεια

Παραδοσιακά, πρέπει να πληρούνται τρεις απαιτήσεις από ένα πληροφοριακό σύστημα προκειμένου να διασφαλιστεί η ασφάλειά του:

1. **Εμπιστευτικότητα**. Οι πιο ευαίσθητες πληροφορίες θα πρέπει να προστατεύονται από μη εξουσιοδοτημένες προσβάσεις. Για τις εφαρμογές IoT, είναι απαραίτητο τα δεδομένα να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση από εξωτερικές υπηρεσίες και χρήστες λόγω του ότι τα δεδομένα που παράγονται από συσκευές IoT, όπως φορητές συσκευές και έξυπνες οικιακές συσκευές, είναι πολύ ευαίσθητα και απόρρητα για τους κατόχους τους. Όσον αφορά τα δεδομένα που παράγονται και αποθηκεύονται σε εφαρμογές IoT, έχει παρατηρηθεί όλα αυτά τα χρόνια ότι οι αρχιτεκτονικές και οι λύσεις του συστήματος έχουν χτιστεί γύρω από κεντρικές επικοινωνίες και λύσεις, όπως φυσικούς διακομιστές, φάρμες διακομιστών ή κεντρικές λύσεις cloud. Αυτές οι υποδομές και οι αρχιτεκτονικές είναι καλές, αν μπορούν όμως να είναι αξιόπιστες και να αντέχουν τις επιθέσεις (Atya et al., 2017). Εάν τα κεντρικά συστήματα δεν είναι αξιόπιστα, τότε οι Blockchain προσφέρουν ένα αποκεντρωμένο σύστημα ή προσέγγιση που ενσωματώνει πολλούς κόμβους. Αυτό σημαίνει ότι δεν υπάρχουν χρόνοι διακοπής λειτουργίας, και ότι εάν ένας κόμβος δεν περιλαμβάνεται, οι άλλοι είναι σε θέση να διατηρήσουν το σύστημα σε αποτελεσματική λειτουργία.
2. **Ακεραιότητα**. Εγγυάται ότι τα δεδομένα δεν αλλοιώνονται ή διαγράφονται από μη εξουσιοδοτημένα άτομα. Συνήθως προστίθεται επίσης ότι, εάν ένα εξουσιοδοτημένο άτομο καταστρέψει τις πληροφορίες, θα πρέπει να είναι δυνατή η αναίρεση των αλλαγών. Αυτή είναι η ιδιότητα του συστήματος που εγγυάται ότι μόλις ένας εισβολέας ή μη εξουσιοδοτημένο μέλος αποκτήσει πρόσβαση στο σύστημα και αλλάξει ή διαγράψει δεδομένα, τότε θα είναι δυνατή η αναίρεση αυτών των αλλαγών και η επιστροφή στην προηγούμενη κατάσταση του συστήματος. Αυτός είναι ουσιαστικά ένας από τους τομείς που οι πρώιμες έννοιες του Blockchain αποδοκιμάζονταν επειδή ένα από τα κύρια στοιχεία των Blockchain είναι ότι είναι αμετάβλητα κάτι που φυσικά δεν είναι απαραίτητο σε ορισμένες περιπτώσεις και για συγκεκριμένες υλοποιήσεις BIoT. Το 2014, αναφέρθηκε ένα γεγονός όταν κλάπηκαν 8 εκατομμύρια Vericoins από την πλατφόρμα MintPal. Το γεγονός αυτό, ώθησε τους δημιουργούς του Vericoin να εκτελέσουν ένα hard fork για να βοηθήσουν στην ανάκτηση των κλεμμένων νομισμάτων. Έτσι, είναι γνωστό ότι οι Blockchain είναι μια πηγή μόνιμης αποθήκευσης, ωστόσο αυτό μπορεί να τροποποιηθεί σε πολύ εξαιρετικές περιπτώσεις. Στις εφαρμογές IoT, η ακεραιότητα των δεδομένων είναι μια ουσιαστική πτυχή που πρέπει να ληφθεί υπόψη εάν παρέχεται από

εξωτερικούς φορείς. Στην εργασία των (Dong & Wang, 2020), οι συγγραφείς πρότειναν μια λύση που θα βοηθήσει στην εξάλειψη των εξωτερικών παρόχων ακεραιότητας δεδομένων, χρησιμοποιώντας την τεχνολογία Blockchain για μια εφαρμογή που βασίζεται σε νέφος IoT. Για μια ισχυρή εφαρμογή BIoT, η ακεραιότητα των δεδομένων πρέπει να ληφθεί υπόψη.

3. **Διαθεσιμότητα**. Τα δεδομένα είναι προσβάσιμα όταν αυτό απαιτείται. Πρόκειται για μία πτυχή των πληροφοριακών συστημάτων που εξετάζει τα δεδομένα στο σύστημα που είναι διαθέσιμα όποτε χρειάζεται. Τα Blockchain έχουν σχεδιαστεί για να διανέμονται και να αποκεντρώνονται. Έτσι, τα δεδομένα μπορούν να διατεθούν ακόμη και αν ένας κόμβος είναι εκτός λειτουργίας ή υπό επίθεση. Όπως σημειώθηκε στην εργασία των (Li et al., 2020), η επίθεση 51% είναι ένα από τα πολλά μέσα με τα οποία μπορεί να τεθεί υπό επίθεση ένα πλήρως αναπαραγώμενο Blockchain. Αυτή η επίθεση υποδηλώνει ότι ένας miner (επιτιθέμενος) έχει τον έλεγχο του 51% των κόμβων στην αλυσίδα και έτσι μπορεί να εμποδίσει τη διαθεσιμότητα της αλυσίδας για την επεξεργασία νέων συναλλαγών.

Για έναν μεμονωμένο χρήστη, το βασικό κριτήριο για τη διατήρηση του απορρήτου είναι η καλή διαχείριση των ιδιωτικών κλειδιών του, καθώς αυτά σε συνδυασμό με ένα δημόσιο κλειδί είναι τα στοιχεία που χρειάζεται ένας εισβολέας για να υποδυθεί κάποιον άλλο χρήστη και να του υποκλέψει κωδικούς και κατ' επέκταση χρήματα/κρυπτονομίσματα. Μια ενδιαφέρουσα πρωτοβουλία που σχετίζεται με αυτό το θέμα, είναι το CONIKS. Αυτό είναι ένα σύστημα διαχείρισης κλειδιών που δημιουργήθηκε για να απαλλάξει τους χρήστες από τη διαχείριση κλειδιών κρυπτογράφησης. Σε ένα τέτοιο σύστημα, ο χρήστης πρέπει πρώτα να ζητήσει ένα δημόσιο κλειδί από έναν πάροχο, ο οποίος απαιτεί μόνο ένα όνομα χρήστη για να πραγματοποιήσει την εγγραφή στο σύστημα CONIKS. Όταν ένας χρήστης θέλει να στείλει ένα μήνυμα σε άλλο χρήστη, το πρόγραμμα-πελάτης του CONIKS αναζητά το κλειδί του αντισυμβαλλομένου στον κατάλογο κλειδιών. Προκειμένου να αποφευχθεί η παραβίαση του κλειδιού από τον πάροχο υπηρεσιών (η οποία μπορεί να διακυβευτεί), πριν από την αποστολή οποιουδήποτε μηνύματος πραγματοποιούνται δύο επαληθεύσεις. Αρχικά ελέγχεται ότι το δημόσιο κλειδί του δέκτη είναι αυτό που χρησιμοποιείται από άλλους πελάτες κατά την επικοινωνία με τον ίδιο χρήστη και στη συνέχεια, ότι ένα τέτοιο κλειδί δεν έχει αλλάξει απροσδόκητα με την πάροδο του χρόνου. Παρόμοιες λύσεις έχουν προταθεί για συσκευές IoT, χρησιμοποιώντας τεχνολογία αλυσίδας συστοιχιών για την ενίσχυση της ταυτότητάς τους και τη διαχείριση της πρόσβασής τους, καθώς οι αλυσίδες συστοιχιών παρέχουν αξιόλογη άμυνα έναντι της πλαστογράφησης των Πρωτοκόλλων Διαδικτύου (Internet Protocol – IP) και των επιθέσεων πλαστογραφίας.

Τα πιστοποιητικά είναι επίσης απαραίτητα για την εγγύηση της ασφάλειας στο Διαδίκτυο. Επομένως, οι αρχές έκδοσης πιστοποιητικών που χρησιμοποιούν μία υποδομή δημόσιου κλειδιού, πρέπει να παρέχουν εμπιστοσύνη σε τρίτους. Ωστόσο, τέτοιες αρχές έχουν αποδειχθεί ότι αποτυγχάνουν σε ορισμένες περιπτώσεις, ακυρώνοντας τα πιστοποιητικά που είχαν εκδοθεί προηγουμένως. Ορισμένες πρόσφατες υπηρεσίες στοχεύουν στη διόρθωση δομικών ελαττωμάτων που εντοπίζονται στο σύστημα πιστοποιητικών SSL (Secure Sockets Layer). Πιο συγκεκριμένα, η Διαφάνεια Πιστοποιητικού της Google (Google's Certificate Transparency) παρέχει ένα πλαίσιο για την παρακολούθηση και τον έλεγχο πιστοποιητικών SSL σε σχεδόν πραγματικό χρόνο. Η λύση αυτή χρησιμοποιεί ένα κατανεμημένο σύστημα που βασίζεται σε δέντρα κατακερματισμού Merkle και επιτρέπει σε τρίτους να ελέγχουν και να επαληθεύουν την εγκυρότητα ενός πιστοποιητικού.

Όσον αφορά την ακεραιότητα, υποδεικνύεται ότι τα θεμέλια μιας αλυσίδας συστοιχιών έχουν σχεδιαστεί για να αποθηκεύουν πληροφορίες που δεν μπορούν να τροποποιηθούν (ή είναι πολύ δαπανηρή η τροποποίησή τους) αφού αποθηκευτούν. Ωστόσο, στο παρελθόν υπήρξαν ορισμένες περιπτώσεις όπου η αρχή αυτή αγνοήθηκε. Για παράδειγμα, το 2014, σε ένα γεγονός που δεν έχει ακόμη διευκρινιστεί, η πλατφόρμα ανταλλαγής νομισμάτων MintPal ενημέρωσε τους χρήστες της ότι ένας χάκερ είχε κλέψει σχεδόν 8 εκατομμύρια Vericoins, ποσό που αντιστοιχούσε σε περίπου 30% των συνολικών νομισμάτων μιας τέτοιας πλατφόρμας. Για να αποφευχθεί η απώλεια κεφαλαίων των επενδυτών, οι προγραμματιστές της Vericoin αποφάσισαν να διαχωρίσουν την αλυσίδα συστοιχιών χρησιμοποιώντας την μέθοδο αλλαγής κανόνων hard fork, αντιστρέφοντας έτσι τη ζημιά (ο όρος hard fork υποδηλώνει την μόνιμη απόκλιση από την προηγούμενη έκδοση της αλυσίδας συστοιχιών). Επομένως, αν και πολλές πηγές πληροφοριών υποδεικνύουν ότι οι αλυσίδες συστοιχιών αποτελούν μια μόνιμη αποθήκευση δεδομένων που δεν είναι δυνατό να τροποποιηθεί, στην πράξη αυτό δεν ισχύει. Εκτός, από ορισμένες πολύ εξαιρετικές περιπτώσεις που αφορούν τη διατήρηση της ακεραιότητας. Στις εφαρμογές IoT, η ακεραιότητα των δεδομένων είναι επίσης απαραίτητη και συνήθως παρέχεται από τρίτους. Για να αποφευχθεί μια τέτοια εξάρτηση, στη μελέτη των (Liu et al., 2017) προτείνεται ένα πλαίσιο υπηρεσίας ακεραιότητας δεδομένων για εφαρμογές IoT που βασίζονται σε cloud, το οποίο χρησιμοποιεί την τεχνολογία της αλυσίδας συστοιχιών εξαλείφοντας έτσι την ανάγκη εμπιστοσύνης τρίτων προσώπων.

Τέλος, ένα άλλο χαρακτηριστικό της ασφάλειας είναι η διαθεσιμότητα, η οποία αποτελεί το πιο απλό χαρακτηριστικό των αλυσίδων συστοιχιών. Ο σχεδιασμός τους ως κατανεμημένα συστήματα τους επιτρέπει να συνεχίσουν να εργάζονται ακόμη και όταν κάποιοι κόμβοι δέχονται επίθεση. Ωστόσο, η διαθεσιμότητα μπορεί να τεθεί σε κίνδυνο μέσω άλλων τύπων επιθέσεων. Η πιο επίφοβη επίθεση είναι μια επίθεση 51 τοις εκατό (ονομάζεται επίσης επίθεση κατά πλειοψηφία), όπου ένας μεμονωμένος εξορύκτης (miner) μπορεί να ελέγξει ολόκληρη την αλυσίδα συστοιχιών και να πραγματοποιήσει συναλλαγές κατά βούληση. Σε αυτήν την περίπτωση, τα δεδομένα είναι διαθέσιμα, αλλά η διαθεσιμότητα για την εκτέλεση συναλλαγών μπορεί να αποκλειστεί από τον εισβολέα που ελέγχει την αλυσίδα συστοιχιών. Προφανώς, αυτού του είδους η επίθεση επηρεάζει επίσης την ακεραιότητα των δεδομένων.

3.8.3 Επεκτασιμότητα, Διακίνηση και Καθυστέρηση

Παρά τα βελτιωμένα χαρακτηριστικά ασφαλείας τους, ο αριθμός των συναλλαγών που μπορούν να πραγματοποιηθούν σε ένα Blockchain είναι ένα θέμα ανησυχίας για τους χρήστες που θέλουν να χρησιμοποιήσουν Blockchain για εφαρμογές και εφαρμογές κύριας ροής. Οι λύσεις IoT απαιτούν να εκτελείται μεγάλος αριθμός συναλλαγών κάθε δεδομένη στιγμή, αλλά ορισμένα δίκτυα Blockchain όπως το Bitcoin είναι ικανά να εκτελούν μόνο 7 συναλλαγές ανά δευτερόλεπτο (Nakamoto & Bitcoin, 2008). Βελτιώσεις έχουν παρουσιαστεί από ερευνητές στο (Li et al., 2020), όπου η απόδοση λέγεται ότι αυξήθηκε όταν τα υπό επεξεργασία μπλοκ ήταν μεγαλύτερα. Εξαίρεση αποτελούν τα μπλοκ μεγέθους 1 MB, μέγεθος που συνήθως δίνεται σε μπλοκ kchains όπως το Bitcoin ή με διαφοροποίηση του τρόπου με τον οποίο αποδέχονται οι κόμβοι και τη διεκπεραίωση συναλλαγών.

Τα Blockchain διαπιστώθηκε ότι παρουσιάζουν υψηλή καθυστέρηση. Για παράδειγμα, το Bitcoin χρειάζεται σχεδόν 10 λεπτά για να ολοκληρώσει μια συναλλαγή. Το ζήτημα του λανθάνοντος χρόνου προκαλείται από τον τύπο του αλγορίθμου συναίνεσης που επιλέγεται για ένα συγκεκριμένο Blockchain. Όσο πιο περίπλοκη είναι η διαδικασία συναίνεσης, τόσο περισσότερος χρόνος απαιτείται για την επεξεργασία της συναλλαγής. Ο αλγόριθμος κατακερματισμού που χρησιμοποιείται σε Blockchains προσθέτει επίσης περισσότερο χρόνο στον χρόνο που απαιτείται για συναλλαγές. Το Litecoin (Queiroz et al., 2019) χρησιμοποιεί ένα Blockchain το οποίο με τη σειρά του χρησιμοποιεί Scrypt αντί για SHA-256 (το οποίο είναι σχετικά πιο γρήγορο).

3.8.4 Ενεργειακή απόδοση

Οι τερματικοί κόμβοι IoT χρησιμοποιούν συνήθως υλικό με περιορισμένους πόρους που τροφοδοτείται από μπαταρίες. Επομένως, η ενεργειακή απόδοση είναι το κλειδί για να καταστεί δυνατή μια μακροχρόνια ανάπτυξη κόμβου. Ωστόσο, πολλές αλυσίδες συστοιχιών διακρίνονται για τη μεγάλη τους ανάγκη για υψηλή ενεργειακή κατανάλωση. Σε τέτοιες περιπτώσεις το μεγαλύτερο μέρος της κατανάλωσης οφείλεται σε δύο παράγοντες:

- Εξόρυξη (mining). Οι αλυσίδες συστοιχιών όπως το Bitcoin κάνουν χρήση τεράστιων ποσοτήτων ηλεκτρικής ενέργειας λόγω της διαδικασίας εξόρυξης, η οποία περιλαμβάνει έναν αλγόριθμο συναίνεσης (PoW) που συνίσταται σε ένα είδος βίαιης αναζήτησης για έναν κατακερματισμό.
- Επικοινωνίες P2P. Οι επικοινωνίες P2P απαιτούν συσκευές αιχμής που πρέπει να ενεργοποιούνται συνεχώς, πράγμα το οποίο θα μπορούσε να οδηγήσει σε σπατάλη ενέργειας. Ορισμένοι ερευνητές όπως οι (Zhang & Helvik, 2012) και (Miyake & Bandai, 2013) πρότειναν ενεργειακά αποδοτικά πρωτόκολλα για δίκτυα P2P αλλά το ζήτημα αυτό πρέπει να μελετηθεί περαιτέρω για τη συγκεκριμένη περίπτωση των δικτύων IoT.

Όσον αφορά την εξόρυξη, ορισμένοι συγγραφείς πρότειναν ότι η ισχύς που καταναλώνεται από τις αποδείξεις εργασίας θα μπορούσε να χρησιμοποιηθεί για κάτι χρήσιμο, παρέχοντας ταυτόχρονα τον αλγόριθμο απαιτούμενης απόδειξης εργασίας (Proof of work – PoW). Η απόκτηση τέτοιων αποδείξεων θα πρέπει να έχει κάποιο βαθμό δυσκολίας, ενώ η επαλήθευση θα πρέπει να είναι πολύ γρήγορη. Ορισμένες υπηρεσίες που βασίζονται σε αλυσίδες συστοιχιών, όπως το Gridcoin, ανταμείβουν την εθελοντική επιστημονική έρευνα υπολογιστών με κρυπτονομίσματα. Ένα άλλο ενδιαφέρον παράδειγμα είναι το Primecoin, του οποίου ο μηχανισμός PoW αναζητά αλυσίδες πρώτων αριθμών. Έτσι, μια τεράστια υποδομή όπως αυτή που εμπλέκεται στο IoT, θα μπορούσε επίσης να αξιοποιηθεί για την επίλυση προβλημάτων χρησιμοποιώντας παράλληλα μια αλυσίδα συστοιχιών. Η απόδειξη χώρου (Proof-of-Space - PoS), γνωστή επίσης ως (Proof-of-Capacity -PoC), έχει προταθεί ως μία πιο οικολογική εναλλακτική του PoW. Τα συστήματα PoS απαιτούν από τους χρήστες να επιδεικνύουν έννομο ενδιαφέρον για μια συγκεκριμένη υπηρεσία εκχωρώντας μια συγκεκριμένη ποσότητα μνήμης ή δίσκου. Αυτός ο μηχανισμός έχει ήδη εφαρμοστεί από κρυπτονομίσματα όπως το Burst-coin. Άλλες συναινετικές μέθοδοι που έχουν προταθεί για τη μείωση της κατανάλωσης ενέργειας σε σχέση με το PoW, είναι τα πρωτόκολλα απόδειξης στοιχήματος (Proof-of-Stake - PoS) ή η πρακτική βυζαντινή ανοχή σφαλμάτων (practical Byzantine Fault Tolerance – pBFT).

Από την άλλη πλευρά, οι επικοινωνίες P2P είναι απαραίτητες για μία αλυσίδα συστοιχιών τόσο για την επικοινωνία ομοτίμων, όσο και για τη διανομή συστοιχιών. Επομένως, όσο περισσότερες ενημερώσεις λαμβάνει μία αλυσίδα συστοιχιών τόσο περισσότερη κατανάλωση ενέργειας αφιερώνεται στις επικοινωνίες. Για να μειωθεί ο αριθμός των ενημερώσεων, οι μίνι αλυσίδες συστοιχιών (mini-blockchains) ενδέχεται να επιτρέπουν στους κόμβους IoT να αλληλεπιδρούν απευθείας με μία αλυσίδα συστοιχιών. Με αυτόν τον τρόπο μπορούν να διατηρούν μόνο τις πιο πρόσφατες συναλλαγές, μειώνοντας παράλληλα τις υπολογιστικές απαιτήσεις ενός πλήρους κόμβου.

Τέλος, όσον αφορά τους αλγόριθμους κατακερματισμού, ο SHA-256 είναι αρκετά διαδεδομένος λόγω του ότι χρησιμοποιείται από το Bitcoin, αλλά οι νέοι αλγόριθμοι όπως ο Scrypt ή ο X11 είναι ταχύτεροι και μπορούν να μειώσουν την κατανάλωση ενέργειας εξόρυξης. Έχουν προταθεί και άλλοι αλγόριθμοι κατακερματισμού, όπως για παράδειγμα ο Blake-256 (Aumasson et al., 2008), ενώ ορισμένες αλυσίδες συστοιχιών μπορούν να κάνουν χρήση διαφορετικών αλγορίθμων κατακερματισμού (π.χ. Myriad). Ωστόσο, για αυτές τις περιπτώσεις απαιτούνται περαιτέρω αναλύσεις σχετικά με την απόδοση και τη βελτιστοποίηση των σύγχρονων συναρτήσεων κατακερματισμού που μπορούν να χρησιμοποιηθούν σε συσκευές IoT.

3.8.5 Διεκπεραιωτική ικανότητα και καθυστέρηση

Οι αναπτύξεις του IoT ενδέχεται να απαιτούν ένα δίκτυο αλυσίδας συστοιχιών, ικανό να διαχειρίζεται μεγάλα ποσά συναλλαγών ανά μονάδα χρόνου. Αυτό όμως προκαλεί έναν σημαντικό περιορισμό σε ορισμένα δίκτυα. Για παράδειγμα, η αλυσίδα συστοιχιών του Bitcoin έχει θεωρητικά ένα μέγιστο όριο επτά συναλλαγών ανά δευτερόλεπτο, αν και μπορεί να αυξηθεί με την επεξεργασία μεγαλύτερων συστοιχιών ή με την τροποποίηση ορισμένων πτυχών της συμπεριφοράς του κόμβου κατά την αποδοχή συναλλαγών. Άλλα δίκτυα όμως, όπως το VISA (VisaNet), είναι ταχύτερα σε εντυπωσιακό βαθμό. Το εν λόγω δίκτυο μπορεί να χειριστεί έως και 24.000 συναλλαγές ανά δευτερόλεπτο. Όσον αφορά την καθυστέρηση (latency), είναι σημαντικό να σημειωθεί ότι οι συναλλαγές μιας αλυσίδας συστοιχιών χρειάζονται κάποιο χρόνο για να διεκπεραιωθούν. Για παράδειγμα, στην περίπτωση του Bitcoin, οι χρόνοι δημιουργίας συστοιχιών ακολουθούν μια κατανομή Πουασσόν (Poisson distribution) με μέσο όρο 10 λεπτών. Για να αποφευχθεί όμως η διπλή δαπάνη, συνιστάται στους εμπόρους να περιμένουν για περίπου μία ώρα, καθώς συνήθως απαιτείται η προσθήκη πέντε ή έξι συστοιχιών στην αλυσίδα πριν επιβεβαιωθεί η αντίστοιχη συναλλαγή. Στη περίπτωση του δικτύου VISA αυτή η καθυστέρηση απαιτεί μόνο λίγα δευτερόλεπτα.

Όσον αφορά την γενική συναίνεση της καθυστέρησης, μπορεί να ειπωθεί ότι η πολυπλοκότητα της διαδικασίας της γενικής συναίνεσης είναι πιο σημαντική ως προς την καθυστέρηση συγκριτικά με τον μεμονωμένο κατακερματισμό. Παρ' όλα αυτά, διαφορετικές αλυσίδες συστοιχιών (όπως π.χ. αυτή που υποστηρίζει το Litecoin), χρησιμοποιούν τον αλγόριθμο scrypt. Δηλαδή έναν αλγόριθμο κατακερματισμού ο οποίος είναι ελαφρώς ταχύτερος σε σχέση με τον SHA-256.

3.8.6 Μέγεθος, εύρος ζώνης και υποδομή της αλυσίδας συστοιχιών

Οι αλυσίδες συστοιχιών αυξάνονται περιοδικά όσο οι χρήστες αποθηκεύουν τις συναλλαγές τους. Αυτό οδηγεί σε μεγαλύτερους αρχικούς χρόνους λήψης και στην ανάγκη χρησιμοποίησης ισχυρότερων εξορυκτών με μεγαλύτερες επίμονες μνήμες. Οι τεχνικές συμπίεσης της αλυσίδας συστοιχιών θα πρέπει να μελετηθούν περαιτέρω, αλλά η αλήθεια είναι ότι οι περισσότεροι κόμβοι IoT δεν θα μπορούσαν να χειριστούν ούτε ένα μικρό κλάσμα μιας παραδοσιακής αλυσίδας συστοιχιών. Επιπλέον, πολλοί κόμβοι θα πρέπει να αποθηκεύουν μεγάλες ποσότητες δεδομένων (τα οποία δεν τους είναι απαραίτητα), κάτι που μπορεί να θεωρηθεί ως σπατάλη υπολογιστικών πόρων. Αυτό το ζήτημα θα μπορούσε να αποφευχθεί με τη χρήση ελαφρών κόμβων, οι οποίοι είναι σε θέση να εκτελούν συναλλαγές στην αλυσίδα συστοιχιών χωρίς να χρειάζεται να τις αποθηκεύσουν. Ωστόσο, αυτή η προσέγγιση απαιτεί στην ιεραρχία του IoT, την ύπαρξη ορισμένων ισχυρών κόμβων που θα διατηρούσαν την αλυσίδα συστοιχιών για τους κόμβους περιορισμένων πόρων. Αυτό συνεπάγεται έναν ορισμένο βαθμό συγκέντρωσης δεδομένων.

Μια άλλη εναλλακτική θα συνίστατο στη χρήση μιας μίνι αλυσίδας συστοιχιών. Μία αλυσίδα τέτοιου είδους εισάγει τη χρήση ενός δέντρου λογαριασμού (account tree), το οποίο αποθηκεύει την τρέχουσα κατάσταση κάθε χρήστη της αλυσίδας συστοιχιών. Με αυτόν τον τρόπο αποθηκεύεται στην αλυσίδα συστοιχιών μαζί με το δέντρο λογαριασμού, μόνο η πιο πρόσφατη συναλλαγή. Αυτό έχει ως αποτέλεσμα να αναπτύσσεται η αλυσίδα συστοιχιών μόνο σε περιπτώσεις που προστίθενται (σε αυτήν) νέοι χρήστες. Επιπλέον, το μέγεθος της συναλλαγής και των συστοιχιών πρέπει να κλιμακώνεται σύμφωνα με τους περιορισμούς του εύρους ζώνης των δικτύων IoT. Με βάση αυτό, πολλές μικρές συναλλαγές θα προκαλούσαν αύξηση στην κατανάλωση ενέργειας που σχετίζεται με τις επικοινωνίες, ενώ μερικές μεγάλες συναλλαγές μπορεί να περιλάμβαναν μεγάλα ωφέλιμα φορτία, τα οποία δεν μπορούν να χειριστούν ορισμένες συσκευές IoT.

Τέλος, όσον αφορά την υποδομή, απαιτούνται ορισμένα στοιχεία για να λειτουργήσει σωστά η αλυσίδα συστοιχιών, όπως η αποκεντρωμένη αποθήκευση, τα πρωτόκολλα επικοινωνίας, το υλικό εξόρυξης, η διαχείριση διευθύνσεων ή η διαχείριση δικτύου. Μέρος αυτών των αναγκών εκπληρώνεται σταδιακά από τη βιομηχανία, δημιουργώντας ειδικό εξοπλισμό για εφαρμογές αλυσίδας συστοιχιών. Για παράδειγμα, οι εξορύκτες (miners) έχουν εξελιχθεί από απλά συστήματα που βασίζονται σε CPU, σε έναν πιο εξελιγμένο εξοπλισμό που αξιοποιεί τη δύναμη των Μονάδων Επεξεργασίας Γραφικών (Graphics Processing Units - GPUs), των Προγραμματιζόμενων Συστοιχιών Πυλών Πεδίου (Field-Programmable Gate Arrays - FPGAs) ή των Ενσωματωμένων Κυκλωμάτων Ειδικής Εφαρμογής (Application-Specific Integrated Circuits - ASICs).

Υπάρχει αρκετά υψηλό κόστος για τη διατήρηση δικτύων Blockchain σε έναν τεράστιο αριθμό κόμβων (peers). Αυτά τα κόστη προέρχονται από την υπολογιστική ισχύ, την ενέργεια, την αποθήκευση και τη μνήμη που απαιτούνται για τη συμμετοχή σε ένα δίκτυο Blockchain. Στην εργασία των (Song et al., 2018), το καθολικό Blockchain ήταν σχεδόν 196 GB το 2018 και αυξήθηκε στα 306,86 GB τον Μάιο του 2020 κάτι που αποτελεί σοβαρή ανησυχία για τις λύσεις IoT. Αυτός ο περιορισμός οφείλεται στον λόγο για τον οποίο οι περισσότερες συσκευές IoT θα είχαν κακούς χρόνους συναλλαγών και κακή επεκτασιμότητα. Έχουν προταθεί λύσεις από ερευνητές για τη μεταφόρτωση των υπολογιστικών εργασιών για αυτές τις συσκευές IoT σε κεντρικούς διακομιστές (ή διακομιστές cloud) ή σε fog server, αλλά αυτές φάνηκε ότι προκαλούν καθυστερήσεις δικτύου (Reyna et al., 2018).

3.8.7 Άλλα σχετικά θέματα

1) Ποσοστό υιοθέτησης

Ένας από τους παράγοντες που μπορεί να εμποδίσει την ευρεία υιοθέτηση μιας εφαρμογής BIoT είναι το γεγονός ότι μία αλυσίδα συστοιχιών επιτρέπει την ψευδοανωνυμία (δηλαδή, οι χρήστες ή οι συσκευές προσδιορίζονται από τις διευθύνσεις, αλλά δεν συνδέονται σαφώς με αυτές). Οι κυβερνήσεις μπορεί να απαιτήσουν μια ισχυρή σύνδεση μεταξύ της ταυτότητας του πραγματικού κόσμου και της διαδικτυακής ταυτότητας. Επιπλέον, δεδομένου ότι οι συναλλαγές IoT μπορούν να πραγματοποιηθούν διεθνώς, ενδέχεται να μην είναι σαφές ποιος πρέπει να πραγματοποιήσει την ταυτοποίηση. Επιπλέον, πρέπει να σημειωθεί ότι η αξία και η ασφάλεια μιας αλυσίδας συστοιχιών αυξάνει με τον αριθμό των χρηστών, καθιστώντας έτσι πιο δύσκολη την πραγματοποίηση επιθέσεων του 51 τοις εκατό που αναφέρθηκαν προηγουμένως. Τέλος, το ποσοστό υιοθέτησης του εξορύκτη επηρεάζει επίσης την ικανότητα ενός δικτύου να επεξεργάζεται συναλλαγές. Επομένως, σε μια ανάπτυξη BIoT, η υπολογιστική ισχύς που προσφέρουν οι εξορύκτες θα πρέπει να κυμαίνεται σε αρκετά υψηλά επίπεδα ούτως ώστε να χειρίζεται τις συναλλαγές που λαμβάνονται από τις συσκευές IoT.

2) Ευχρηστία

Προκειμένου να διευκολυνθεί η εργασία των προγραμματιστών, η πρόσβαση της αλυσίδας συστοιχιών στη διεπαφή προγραμματισμού εφαρμογών (Application Programming Interface - API), θα πρέπει να είναι όσο το δυνατόν πιο φιλική προς το χρήστη. Το ίδιο θα πρέπει να ισχύει και για την API ως προς τη διαχείριση των λογαριασμών των χρηστών.

3) Διαχείριση πολλαπλών αλυσίδων

Σε ορισμένες περιπτώσεις, ο πολλαπλασιασμός των αλυσίδων συστοιχιών έχει οδηγήσει στην ανάγκη για ταυτόχρονη αντιμετώπιση πολλών από αυτών. Αυτό μπορεί επίσης να συμβεί σε ένα σενάριο IoT, όπου για παράδειγμα, οι τιμές των αισθητήρων μπορεί να αποθηκευτούν σε μια ιδιωτική αλυσίδα συστοιχιών, ενώ οι οικονομικές συναλλαγές μεταξύ κόμβων που παρέχουν υπηρεσίες μπορεί να υποστηρίζονται από την αλυσίδα συστοιχιών του Ethereum ή του Bitcoin.

4) Διαχείριση εκδόσεων και διαχωρισμοί (forks)

Οι αλυσίδες συστοιχιών μπορούν να διαχωρίζονται για διαχειριστικούς σκοπούς ή για σκοπούς διαχείρισης εκδόσεων. Από τη στιγμή που μία αλυσίδα συστοιχιών διαχωρίζεται, δεν είναι εύκολο να πραγματοποιηθούν συναλλαγές μεταξύ δύο αλυσίδων.

5) Μποϋκοτάζ εξόρυξης

Οι εξορύκτες είναι αυτοί που αποφασίζουν ποιες συναλλαγές αποθηκεύονται ή όχι στην αλυσίδα συστοιχιών, ώστε να μπορούν να λογοκρίνουν ορισμένες συναλλαγές για οικονομικούς ή ιδεολογικούς λόγους. Αυτό το ζήτημα μπορεί να συμβεί όταν ο αριθμός των συνωμοτών εξορυκτών είναι πάνω από το 51 τοις εκατό του συνόλου, επομένως οι μικρές αλυσίδες και οι αλυσίδες συστοιχιών που αναθέτουν τις αποφάσεις τους σε ένα υποσύνολο εξορυκτών, είναι επιρρεπείς σε αυτού του είδους τα μποϊκοτάζ. Άρα, οι εξορύκτες πρέπει να επιλέγονται με σύνεση ενώ στις περιπτώσεις που έχουν υπογραφεί έξυπνες συμβάσεις, θα πρέπει να επιβάλλονται οι ανάλογες κυρώσεις για κακές συμπεριφορές.

6) Έξυπνη επιβολή συμβολαίων και αυτονομία

Πρέπει επίσης να αναπτυχθούν νομικοί κανόνες για την επιβολή των έξυπνων συμβάσεων και την ορθή επίλυση των διαφορών. Αν και τη σημερινή εποχή εκτελούνται ορισμένες εργασίες για τη δέσμευση πραγματικών συμβάσεων με έξυπνα συμβόλαια, αυτό εξακολουθεί να είναι ένα θέμα που πρέπει να μελετηθεί περισσότερο.

3.9 Blockchain για IoT εστιασμένα στις έξυπνες πόλεις

Η συνεχής ανάπτυξη εφαρμογών που βασίζονται στο Διαδίκτυο των Πραγμάτων (IoT), ανοίγει το δρόμο προς την ανάπτυξη έξυπνων πόλεων (Khan et al., 2020a, 2020b). Οι έξυπνες πόλεις προσφέρουν μεταξύ άλλων έξυπνες μεταφορές, βιομηχανία 4.0, έξυπνη υγειονομική περίθαλψη, έξυπνα σπίτια, έξυπνες τραπεζικές συναλλαγές. Αυτές οι εφαρμογές απαιτούν τεράστια ασφάλεια για το χειρισμό δεδομένων βελτιώνοντας παράλληλα το επίπεδο ζωής των πολιτών. Προκειμένου να ενεργοποιηθούν οι έξυπνες πόλεις με βελτιωμένη ασφάλεια και απόρρητο, χρησιμοποιείται το Blockchain. Πρόκειται για ένα αποκεντρωμένο, ανιχνεύσιμο, διαφανές και αμετάβλητο βιβλίο διακρατικών αρχείων σε δίκτυα Peer-to-Peer (P2P) (Yaqoob et al., 2020). Το Blockchain εισήχθη για πρώτη φορά ως bitcoin που αποτελεί μια λύση για τη μεταφορά ψηφιακών πληρωμών μεταξύ διαφορετικών μερών χωρίς την ανάγκη μιας κεντρικής αρχής (Nakamoto, 2008). Το Bitcoin παρουσίασε τεράστια επιτυχία με κεφαλαιοποίηση αγοράς άνω των 230 δισεκατομμυρίων δολαρίων ΗΠΑ το 2017. Εκτός από τη βελτίωση του χρηματοοικονομικού κλάδου, το Blockchain βρίσκει πιθανές εφαρμογές σε πολλούς άλλους τομείς όπως το IoT, το ηλεκτρονικό εμπόριο, τη λογιστική και τον έλεγχο, το e-Voting, τη διαχείριση περιουσιακών στοιχείων, τη διαχείριση ταυτότητας, την εφοδιαστική αλυσίδα, τη φορολογία, τις τηλεπικοινωνίες, την υγειονομική περίθαλψη (Yaqoob et al., 2021) και τις κρατικές δημόσιες υπηρεσίες.

Η έξυπνη πόλη περιλαμβάνει το οικοσύστημα των έξυπνων περιβαλλόντων που παρέχονται στην πόλη και τα οποία μπορούν να σχεδιάσουν τον τρόπο ζωής των κατοίκων της. Ενδιαφέρεται για την υιοθέτηση τεχνολογιών πληροφοριών και επικοινωνιών για βελτίωση της δημόσιας ευημερίας, της οικονομίας, των κυβερνητικών υπηρεσιών, του περιβάλλοντος, της διαχείρισης πόρων και του αστικού σχεδιασμού. Οι έξυπνες πόλεις οραματίζονται τη χρήση της υπάρχουσας και αναπτυσσόμενης ψηφιακής τεχνολογίας για να βελτιώσουν κάθε πτυχή της ζωής εντός αυτών. Ένας από τους πρωταρχικούς στόχους των έξυπνων πόλεων είναι η μεταρρυθμισμένη παροχή θεμελιωδών υπηρεσιών όπως η στέγαση, η εκπαίδευση, η υγειονομική περίθαλψη, οι μεταφορές, η ενέργεια, το νερό, οι υπηρεσίες κοινής ωφέλειας, η επιτήρηση και η επιβολή του νόμου. Οι έξυπνες πόλεις μπορούν να μετριάζουν προβλήματα της πληθυσμιακής αύξησης και της ταχείας αστικοποίησης ενσωματώνοντας την κοινωνική, επιχειρηματική και φυσική υποδομή τους μέσω της τεχνολογίας. Οι πρόσφατες εξελίξεις τεχνολογιών όπως οι Τεχνολογίες Πληροφορικής και Επικοινωνίας (ICT), τα Blockchain, τα Big Data, η μηχανική μάθηση, ο αυτοματισμός, η Τεχνητή Νοημοσύνη (AI) και το IoT θα κάνουν τις έξυπνες πόλεις πιο διασυνδεδεμένες, οργανωμένες, έξυπνες, βιώσιμες, ασφαλείς και ανθεκτικές. Τα μέτρα απόδοσης για την επιτυχία μιας έξυπνης πόλης συνιστούν την ενσωμάτωση βασικών υπηρεσιών με απρόσκοπτη αφομοίωση στην καθημερινή ζωή των κατοίκων της, διασφαλίζοντας έτσι την αποτελεσματική χρήση των πόρων και τη βελτίωση της ποιότητας ζωής (Tu, 2018). Ωστόσο, κάτι τέτοιο συνεπάγεται τεράστιο όγκο διακίνησης δεδομένων που παράγεται από συστήματα πληροφοριών που ρέουν μέσω δικτύων επικοινωνίας της τεχνολογικής υποδομής της πόλης. Το Blockchain αποτελεί μια λύση στη βασική πρόκληση της ασφάλειας, του απορρήτου και της διαφάνειας αυτών των προσωπικών, οργανωτικών και επιχειρησιακών δεδομένων (Ma et al., 2020). Διάφοροι τύποι συναλλαγών έξυπνων πόλεων μπορούν να καταγραφούν σε ένα Blockchain. Με τη χρήση έξυπνων συμβολαίων, είναι δυνατή η εκτέλεση πολύπλοκων νομικών διαδικασιών ενώ η ανταλλαγή δεδομένων μπορεί να γίνει αυτόματα. Με έξυπνα συμβόλαια και αποκεντρωμένες εφαρμογές, το Blockchain δίνει υψηλό επίπεδο αυτονομίας για την εκτέλεση έξυπνων συναλλαγών κατά τη διάρκεια της επιχειρησιακής διαδικασίας της έξυπνης πόλης. Το Blockchain μπορεί να προσφέρει χαρακτηριστικά όπως ο απρόσκοπτος έλεγχος ταυτότητας, το απόρρητο, η ασφάλεια, η αβίαστη ανάπτυξη και η συντήρηση. Έχουν γίνει τεράστιες προσπάθειες για την εξερεύνηση εφαρμογών Blockchain σε έξυπνες πόλεις. Στην εργασία τους οι (Mohanty et al., 2020), ανέλυσαν το ρόλο του Blockchain για την ασφάλεια του IoT. Οι συγγραφείς (Sharma & Park, 2018) στην μελέτη τους πρότειναν υβριδική αρχιτεκτονική δικτύου για μια έξυπνη πόλη που βασίζεται σε Blockchain με σκοπό την αντιμετώπιση ζητημάτων επικοινωνίας όπως η καθυστέρηση, το εύρος ζώνης, η επεκτασιμότητα, η ασφάλεια και το απόρρητο των δικτύων επικοινωνίας που λειτουργούν στην καρδιά της έξυπνης πόλης.

3.9.1 Αγορά Blockchain για Έξυπνες Πόλεις

Η International Data Corporation (IDC) προέβλεψε την ευρεία υιοθέτηση του Blockchain στον κλάδο. Σύμφωνα με την IDC, τουλάχιστον το 25% των Μεγαλύτερων Δημόσιων Εταιρειών του Κόσμου (G2000) του 2000 θα χρησιμοποιήσει το Blockchain για τη δημιουργία των θεμελίων της ψηφιακής εμπιστοσύνης έως το 2021. Επιπλέον, το ένα τέταρτο των κορυφαίων παγκόσμιων τραπεζών, σχεδόν το ένα πέμπτο των οργανισμών υγειονομικής περίθαλψης, το 50 % των κατασκευαστών και των εμπόρων λιανικής χρησιμοποίησαν Blockchain στο περιβάλλον παραγωγής τους το 2021. Το μέγεθος της αγοράς Blockchain εκτιμάται ότι θα επεκταθεί από 3,0 δισεκατομμύρια USD σε 39,7 δισεκατομμύρια USD έως το 2025 με σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) 67,3% για το 2020-2025.

Η παγκόσμια αγορά έξυπνων πόλεων είχε αξία 624,81 δισεκατομμυρίων USD το 2019 και εκτιμάται ότι θα αυξηθεί με CAGR 18,30%–1712,83 δισεκατομμύρια δολάρια μέχρι το 2025[1]. Επιπλέον, όπως προέβλεψε η IDC, η διεθνής εκταμίευση για τις αναπτυξιακές πρωτοβουλίες των έξυπνων πόλεων ήταν περίπου 124 δισεκατομμύρια δολάρια ΗΠΑ μόνο το 2020, με επέκταση έως και 189,5 δισεκατομμύρια δολάρια ΗΠΑ έως το 2023. Το επίκεντρο σε παγκόσμιο επίπεδο αποτελούν τα έξυπνα περιβάλλοντα που βασίζονται σε δεδομένα ασφάλεια, έξυπνες μεταφορές, ανθεκτική ενέργεια και ανάπτυξη υποδομών[2].

Αρκετές μελέτες εξέτασαν έξυπνες πόλεις, IoT, Blockchain και έξυπνες συμβάσεις. Η μελέτη των (Wu et al., 2019) ασχολήθηκε διεξοδικά με Blockchain από το forking, την κρυπτογραφία, τη δικτύωση, την πολυεπίπεδη αρχιτεκτονική, τη συναίνεση και την προοπτική ασφάλειας. Οι συγγραφείς διερεύνησαν διαφορετικές εφαρμογές του Blockchain καθώς και τις προκλήσεις και τις ευκαιρίες που υπάρχουν στις

[1] Smart Cities Market, 2020. Growth, trends, and forecast (2020 - 2025). https://www. mordorintelligence.com/industry-reports/smart-cities-market. (Accessed 10 July 2020).

[2] IDC Trackers, 2020. Worldwide Smart Cities Spending Guide. https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1843. (Accessed 10 July 2020).

σύγχρονες τεχνολογίες Blockchain, εξέτασαν τους κινδύνους ασφαλείας, τις πραγματικές επιθέσεις και την πρακτική λύση για την ασφάλεια στο Blockchain. Ο μηχανισμός λειτουργίας των έξυπνων συμβολαίων σε δημοφιλείς πλατφόρμες Blockchain αναλύθηκε διεξοδικά στη μελέτη των (Wang et al., 2019α). Επιπλέον, παρουσιάστηκε ένα πλαίσιο έξι επιπέδων για τον κύκλο ζωής των έξυπνων συμβολαίων, τις προκλήσεις, τις εφαρμογές και τις μελλοντικές τάσεις ανάπτυξης και εξέτασαν τις σύγχρονες ευπάθειες ασφαλείας στα έξυπνα συμβόλαια και τις αντίστοιχες πιθανές λύσεις.

Η εξέλιξη, η λειτουργική πολυεπίπεδη αρχιτεκτονική και οι εφαρμογές των έξυπνων πόλεων παρουσιάστηκαν στη μελέτη των (Sookhak et al., 2019) σύμφωνα με τους οποίους η έξυπνη πόλη χωρίζεται σε τέσσερις πυλώνες υποδομής και πιο συγκεκριμένα τη θεσμική, φυσική, κοινωνική και οικονομική υποδομή. Επιπλέον συζητήθηκαν τα ζητήματα απορρήτου, οι απαιτήσεις ασφάλειας καθώς και οι λύσεις και οι προκλήσεις ασφαλείας. Η επικεντρωμένη στα δεδομένα προοπτική στις έξυπνες πόλεις παρέχεται στη μελέτη των (Gharaibeh et al., 2017), όπου αναλύθηκαν τα βασικά σενάρια ανάπτυξης εφαρμογών έξυπνης πόλης, συζητήθηκε ο κύκλος ζωής των δεδομένων σε μια έξυπνη πόλη με την προοπτική της απόκτησης, επεξεργασίας, διάδοσης, παρουσίασης, ασφάλειας και απορρήτου δεδομένων καθώς και η ενεργοποίηση τεχνολογιών δικτύωσης και υπολογιστών. Η σημασία της ιδιωτικής ζωής στις έξυπνες πόλεις τονίστηκε στην εργασία των (Eckhoff & Wagner, 2018). Συζητήθηκαν οι βασικές εφαρμογές της ιδιωτικής ζωής εντός της έξυπνης πόλης, παράλληλα με τις τεχνολογίες ευνοϊκής εφαρμογής, τις σχετικές προκλήσεις και τις σύγχρονες λύσεις για την ενεργοποίηση έξυπνων πόλεων με σκοπό την προστασία της ιδιωτικής ζωής. Οι (Cui et al., 2018) στην εργασία τους ανέλυσαν ανησυχίες για την ασφάλεια και το απόρρητο εντός των έξυπνων πόλεων από το σημείο της ασφάλειας στον κυβερνοχώρο και συζητήθηκαν τα προστατευτικά μέτρα για την ασφάλεια των έξυπνων πόλεων από διάφορες τεχνολογίες όπως κρυπτογραφία, βιομετρία, Blockchain.

Στη μελέτη τους οι (Khan & Salah, 2018) συζήτησαν την αρχιτεκτονική σε επίπεδα IoT και το πρωτόκολλο δικτύου IoT. Κατηγοριοποίησαν τις κρίσιμες ανησυχίες για την ασφάλεια στο IoT και ερεύνησαν αντίστοιχες λύσεις που βασίζονται σε Blockchain. Οι (Reyna et al., 2018) ασχολήθηκαν με τα πιθανά οφέλη και τους τρόπους ενσωμάτωσης του Blockchain με το IoT. Οι συγγραφείς συζήτησαν τις πιθανές εφαρμογές, τις σχετικές προκλήσεις και τις πλατφόρμες Blockchain που καθορίζονται για το IoT. Στην μελέτη τους οι (Ali et al., 2019) συζήτησαν διεξοδικά το απόρρητο που βασίζεται σε Blockchain, την αρχιτεκτονική χωρίς εμπιστοσύνη, την ασφάλεια, τη διαχείριση ταυτότητας, τη διαχείριση δεδομένων, τη δημιουργία εσόδων, τις προκλήσεις και τις κατευθύνσεις έρευνας ειδικά για το αποκεντρωμένο IoT. Στη μελέτη τους οι (Fernández-Caramés & Fraga-Lamas, 2018) παρουσίασαν ένα βελτιστοποιημένο Blockchain για εφαρμογές IoT (BIoT) βασισμένες σε Blockchain σε μια έξυπνη πόλη και αντίστοιχες προκλήσεις ανοιχτής έρευνας. Οι (Ferrag et al., 2019) εξέτασαν τα πρωτόκολλα Blockchain για το IoT και παρουσίασαν διάφορα μοντέλα απειλών και προκλήσεων στα δίκτυα BIoT. Στην εργασία τους οι (Alladi et al., 2019) συζήτησαν τους τομείς εφαρμογής του Blockchain στο Industrial Internet of Things (IIoT), τις αντίστοιχες προκλήσεις του κλάδου και τα ανοιχτά ζητήματα.

Στη μελέτη των (Wang et al., 2020), παρουσιάστηκαν οι απαιτήσεις ασφάλειας για το IoT και το IIoT και συζητήθηκε το αν το Blockchain μπορεί να παίξει το ρόλο του ενεργοποιητή ασφάλειας στο IIoT. Η μελέτη που διεξήχθη από τους (Chen et al., 2020) ασχολήθηκε με τον ρόλο του Blockchain ως αξιόπιστου τρίτου μέρους, με την πλατφόρμα ασφάλειας δεδομένων, με την πλατφόρμα ελέγχου πρόσβασης και την πλατφόρμα αυτόματης πληρωμής στο IoT. Επίσης διερευνήθηκαν οι σχετικές ερευνητικές προκλήσεις. Οι (Xie et al., 2019) στη μελέτη τους συζήτησαν την εφαρμογή της τεχνολογίας Blockchain σε διάφορες έξυπνες περιοχές σε έξυπνες πόλεις και τις σχετικές ερευνητικές προκλήσεις.

Το ακόλουθο σχήμα απεικονίζει την έξυπνη πόλη, όπου διάφορα έξυπνα περιβάλλοντα λειτουργούν παράλληλα. Μέσα σε ένα έξυπνο περιβάλλον, πολλές οντότητες διατηρούν το κατανεμημένο καθολικό σε ένα δίκτυο Blockchain ενώ τα έξυπνα συμβόλαια εκτελούν την επιχειρηματική λογική.

Σχήμα 3-6. Ο ρόλος του Blockchain σε διάφορα έξυπνα περιβάλλοντα εντός της έξυπνης πόλης.

3.9.2 Έξυπνο Ηλεκτρονικό Εμπόριο

Το ηλεκτρονικό εμπόριο ή e-Commerce περιλαμβάνει πωλητές και αγοραστές για την ανταλλαγή περιουσιακών στοιχείων σε πλατφόρμες όπως το Amazon.com. Επιπλέον, τα τρέχοντα συστήματα ηλεκτρονικού εμπορίου βασίζονται σε αξιόπιστα τρίτα μέρη (TTP) για την παράδοση των διαπραγματεύσιμων αντικειμένων. Το Blockchain επιτρέπει τη διενέργεια συναλλαγών μεταξύ των μερών σε ένα περιβάλλον χωρίς εμπιστοσύνη χωρίς μεσάζοντες. Χρησιμοποιώντας Blockchain και έξυπνα συμβόλαια, οι κεντρικοί διαδικτυακοί λιανοπωλητές μπορούν να εξαλειφθούν από ένα τέτοιο οικοσύστημα ηλεκτρονικού εμπορίου. Επιπλέον, τα παραγγελμένα αρχεία καταγραφής μπορούν να χρησιμοποιηθούν για την ιχνηλασιμότητα και τον έλεγχο των ενδιάμεσων φορέων εφοδιαστικής. Οι (Asgaonkar & Krishnamachari, 2018)) πρότειναν ένα πρωτόκολλο μεσεγγύησης διπλής κατάθεσης για να λύσει το δίλημμα του αγοραστή και του πωλητή κατά την πώληση ενός ψηφιακού αγαθού. Το δίλημμα αφορά το θέμα της εμπιστοσύνης για την πληρωμή και την παράδοση γνήσιων ψηφιακών αγαθών. Επινοείται ένα παιχνίδι εκτεταμένης μορφής όπου ο πωλητής είναι ο ηγέτης ενώ ο αγοραστής παίρνει το ρόλο του ακόλουθου. Η χρησιμότητα των παικτών καθορίζεται με βάση μια επιστρεφόμενη κατάθεση, την πραγματική αξία του ψηφιακού αγαθού και την τιμή του αγαθού. Το πρωτόκολλο που βασίζεται σε έξυπνα συμβόλαια απαιτεί από τον πωλητή να κάνει μια επιστρεπτέα κατάθεση ενώ ο αγοραστής πρέπει να κάνει μια επιστρεπτέα κατάθεση καθώς και την πληρωμή του προϊόντος. Εάν κάποιος ανάμεσα στον αγοραστή ή τον πωλητή απατά, η κατάθεση κινδυνεύει να χαθεί. Αυτό δημιουργεί μια κατάσταση όπου η τέλεια στρατηγική βασισμένη στην ισορροπία Nash του υποπαιγνίου για τον αγοραστή και τον πωλητή είναι: «να είμαστε ειλικρινείς μεταξύ μας». Οι ερευνητές υπέθεσαν ότι ο αγοραστής μπορεί να επαληθεύσει τη γνησιότητα των ψηφιακών αγαθών μόλις παραδοθούν και πρότειναν έναν μηχανισμό για την πώληση φυσικών αγαθών χωρίς έναν αξιόπιστο μεσάζοντα χρησιμοποιώντας ένα ηλεκτρονικό ντουλάπι.

Οι (Hasan & Salah, 2018) πρότειναν ένα πλαίσιο απόδειξης παράδοσης (PoD) με δυνατότητα Blockchain για υλικά περιουσιακά στοιχεία. Η διαδικασία περιλαμβάνει μια ασφαλή, διαφανή λύση διαχείρισης logistics για την παράδοση φυσικών αγαθών μέσω του μοναδικού μεταφορέα και συζητήθηκε η ανάλυση κόστους και ασφάλειας για τη λειτουργία του επινοημένου πλαισίου.

Οι (Liu et al., 2019) σχεδίασαν ένα αυτόνομο σύστημα διαχείρισης συναλλαγών που βασίζεται σε Blockchain με τίτλο «NormaChain» για το ηλεκτρονικό εμπόριο που βασίζεται στο IoT. Προκειμένου να βελτιωθεί η επεκτασιμότητα του δικτύου Blockchain, των υψηλών υπολογιστικών επιβαρύνσεων και της απόδοσης συναλλαγών, χρησιμοποιείται κατακερματισμός τριών επιπέδων. Ο PBFT χρησιμοποιήθηκε ως υποκείμενος αλγόριθμος συναίνεσης. Το επίπεδο συναλλαγής ασχολείται με συναλλαγές που ξεκινούν από χρήστες, οι οποίες αποστέλλονται στο επίπεδο έγκρισης για επεξεργασία. Μόλις εγκριθούν, οι συναλλαγές προωθούνται στην αλυσίδα συναλλαγών. Οι ρυθμιστικές αρχές έχουν μερική πρόσβαση στις πληροφορίες συναλλαγών των χρηστών για νομική εποπτεία, διατηρώντας έτσι μια σωστή ισορροπία μεταξύ του απορρήτου και της νομιμότητας των συναλλαγών. Επινοήθηκε ένα νέο αποκεντρωμένο σύστημα κρυπτογράφησης με δυνατότητα αναζήτησης δημόσιου κλειδιού (DPEKS) για αποκεντρωμένη εποπτεία, το οποίο επιτρέπει την αναζήτηση σε κρυπτογραφημένα δεδομένα με ανέπαφο το απόρρητο. Το επίπεδο εποπτείας διατηρεί αρχείο σάρωσης της αλυσίδας συναλλαγών για μια στοχευμένη παράνομη λίστα λέξεων-κλειδιών στην εποπτική αλυσίδα. Το NormaChain είναι ανθεκτικό σε επιθέσεις ασφαλείας, όπως επιθέσεις κρυπτογραφημένου κειμένου (CCA) και δόλια πρόσβαση στο μυστικό κλειδί. Η Normachain παρέχει κλιμακούμενες, ασφαλείς, ανιχνεύσιμες, νόμιμες και αυτόνομες υπηρεσίες πληρωμών, με χαρακτηριστικά όπως η ακεραιότητα των δεδομένων και η μη άρνηση.

3.9.3 Έξυπνη Ηλεκτρονική Ψηφοφορία

Σε μια έξυπνη πόλη, η ηλεκτρονική διακυβέρνηση στοχεύει στην αυτοματοποίηση της διαδικασίας διακυβέρνησης χρησιμοποιώντας τις ΤΠΕ. Η ψηφοφορία αποτελεί μια διαδικασία διακυβέρνησης για την εκλογή εκπροσώπων των μαζών δημοκρατικά σε εθνικό, πολιτειακό ή επίπεδο πόλης. Η ψηφοφορία σε χαρτί βασίζεται εξ ολοκλήρου στην εντιμότητα των κυβερνητικών στελεχών που διενεργούν την ψηφοφορία, ενώ υπάρχει πλήθος ακόμη μειονεκτημάτων που σχετίζονται με την ψηφοφορία βάσει ψηφοδελτίων, όπως είναι το υψηλό κόστος, η χρονοβόρα, η ασυνέπεια, η νοθεία πριν από τις εκλογές, η ψευδής καταμέτρηση ψήφων, η εύκολη εισαγωγή πλαστών ψηφοδελτίων και η χαμηλή προσέλευση ψηφοφόρων. Η ηλεκτρονική ψηφοφορία είναι ψηφοφορία που βασίζεται στη χρήση ψηφιακής τεχνολογίας. Αντί να χρησιμοποιούν ψηφοδέλτια, οι ψηφοφόροι επαληθεύονται για ψηφοφορία χρησιμοποιώντας βιομετρικά στοιχεία μέσω πλατφορμών λογισμικού. Ωστόσο, μια τέτοια ηλεκτρονική ψηφοφορία είναι ευάλωτη σε επιθέσεις στον κυβερνοχώρο και παραποίηση σε επίπεδο χρήστη και συστήματος. Το Blockchain παρέχει ένα δίκτυο, το οποίο δεν έχει ούτε ένα σημείο αστοχίας, ούτε ελέγχεται από κάποια κεντρική αρχή. Το Blockchain παρέχει ένα ιδιωτικό κλειδί για κάθε χρήστη για την ψηφιακή υπογραφή της συναλλαγής του, το οποίο στη συνέχεια προστίθεται στο ψηφιακό καθολικό μόνο με προσάρτημα. Αυτά τα χαρακτηριστικά του Blockchain μπορούν να αξιοποιηθούν σε κλιμακούμενη ηλεκτρονική ψηφοφορία που βασίζεται σε Blockchain. Στην ηλεκτρονική ψηφοφορία η οποία είναι προσανατολισμένη στο Blockchain, σε κάθε ψηφοφόρο μπορεί να εκχωρηθεί ένα πορτοφόλι με ένα ιδιωτικό κλειδί για έλεγχο ταυτότητας κατά τη διάρκεια της ψηφοφορίας. Κατά τη διάρκεια κάθε ψηφοφορίας, το πορτοφόλι πιστώνεται με ένα νόμισμα που μπορεί να χρησιμοποιηθεί μόνο μία φορά για την ψήφο ενός ευνοϊκού υποψηφίου (Kshetri & Voas, 2018). Το πρωτόκολλο συστήματος μπορεί να σχεδιαστεί έτσι ώστε οι ψηφοφόροι να μπορούν να επικυρωθούν, αλλά να παραμένουν ανώνυμοι κατά την τελική καταμέτρηση.

Ο (Osgood, 2016) στην εργασία του παρουσίασε τις προκλήσεις που συνεπάγεται η ολοκλήρωση της ηλεκτρονικής ψηφοφορίας που βασίζεται σε Blockchain. Η εξ αποστάσεως ψηφοφορία θεωρείται μη πρακτική λόγω θεμάτων κυβερνο-ασφάλειας. Οι συγγραφείς πρότειναν ένα σύστημα ψηφοφορίας που είναι υβρίδιο της ψηφοφορίας που βασίζεται σε ψηφοδέλτιο και της ψηφιακής ψηφοφορίας. Οι ψηφοφόροι ψηφίζουν σε χάρτινα ψηφοδέλτια με κωδικούς QR. Τα σαρωμένα χάρτινα ψηφοδέλτια αποθηκεύονται στο τοπικό Blockchain σε ένα ασφαλές μηχάνημα. Οι σαρωμένες εικόνες των χάρτινων ψηφοδελτίων διατηρούνται επίσης ψηφιακά. Αφού τελειώσει ο χρόνος ψηφοφορίας, όλες οι ψηφιακές πληροφορίες μαζί με το offline Blockchain αποθηκεύονται σε DVD. Στη συνέχεια, οι μηχανές ψηφοφορίας συνδέονται ως κόμβος σε ένα «επιτρεπόμενο Blockchain» για τη συσσώρευση μεμονωμένων μετρήσεων στην τελική καταμέτρηση. Αργότερα, το τελικό Blockchain δημοσιοποιείται σε όλες τις αρμόδιες αρχές για επαλήθευση και επικύρωση. Το προτεινόμενο σύστημα θα αυτοσχεδιάσει την ηλεκτρονική ψηφοφορία. Ωστόσο, δεν είναι ακόμα άψογο.

Οι (Shahzad & Crowcroft, 2019) πρότειναν ένα σύστημα ηλεκτρονικής ψηφοφορίας που βασίζεται σε Blockchain, στο Πακιστάν ως μελέτη περίπτωσης. Οι εργασίες επικεντρώθηκαν κυρίως στις διαδικασίες που ακολουθήθηκαν κατά τη διάρκεια της ψηφοφορίας, την ασφάλεια των δεδομένων των ψηφοφόρων και τις συναλλαγές που αντιστοιχούν στη ψηφοφορία. Το έργο καθιερώνει το Blockchain της κοινοπραξίας, το οποίο διαχειρίζεται μια εθνική αρχή, όπως η εκλογική επιτροπή μιας χώρας. Μετά τη φυσική και βιομετρική ταυτοποίηση των ψηφοφόρων, επιτρέπεται σε αυτούς να ψηφίσουν. Μετά την ολοκλήρωση της ψηφοφορίας σε ένα εκλογικό τμήμα, το αποτέλεσμα επιβεβαιώνεται για αυτό το εκλογικό τμήμα. Η διαδικασία επαναλαμβάνεται για κάθε εκλογικό τμήμα εντός της εκλογικής περιφέρειας για το συλλογικό αποτέλεσμα μιας συγκεκριμένης εκλογικής περιφέρειας και εν συνεχεία ανακοινώνεται το αποτέλεσμα των εθνικών εκλογών. Ο αλγόριθμος απόδειξης πληρότητας BSJC προτείνεται στη μελέτη για την προσαρμογή του Blockchain για ηλεκτρονική ψηφοφορία. Η διαδικασία δημιουργίας μπλοκ ξεκινά ταυτόχρονα με την έναρξη του χρόνου ψηφοφορίας και τερματίζεται μετά τη διακοπή του χρόνου ψηφοφορίας. Η μοναδική ταυτότητα του προεδρεύοντος (PO) προστίθεται χρησιμοποιώντας ένα αποτελεσματικό σύστημα κατακερματισμού κατά τη δημιουργία και τη σφράγιση μπλοκ για βελτιωμένη ασφάλεια. Η εργασία προϋποθέτει απρόσκοπτη συνδεσιμότητα δικτύου χωρίς σημαντική καθυστέρηση.

Στην εργασία του ο (Ayed, (2017) εξέτασε κριτικά διαφορετικά συστήματα ηλεκτρονικής ψηφοφορίας που έχουν σχεδιαστεί από κυβερνήσεις σε πολλές χώρες. Προτάθηκε αρχιτεκτονική Blockchain για ψηφοφορία στο Διαδίκτυο (i-voting) που παρέχει έλεγχο ταυτότητας, ανωνυμία, ακρίβεια και επαληθευσιμότητα. Το Blockchain θα έχει πολλαπλούς κλάδους. Στο πρώτο μπλοκ κάθε κλάδου που είναι γνωστό ως το ιδρυτικό block (foundation block), θα προστεθεί μια ειδική συναλλαγή που αντιπροσωπεύει το όνομα του υποψηφίου. Η ψήφος που δίνεται για έναν υποψήφιο θα προστεθεί με τη μορφή των μπλοκ στον κλάδο που έχει ξεκινήσει από το ιδρυτικό μπλοκ του σχετικού υποψηφίου. Η τελική καταμέτρηση γίνεται με την καταμέτρηση των ψήφων σε κάθε κλάδο, συμπεριλαμβανομένων των ορφανών μπλοκ του κλάδου. Η ψηφοφορία εξασφαλίζεται μόλις δοθεί και εγγραφεί ως συναλλαγή στο δίκτυο Blockchain. Ωστόσο, ο πρωταρχικός περιορισμός του προτεινόμενου συστήματος είναι η κακόβουλη συμπεριφορά στο άκρο του χρήστη κατά την ψηφοφορία.

Με βάση τα χαρακτηριστικά της διαφάνειας και της μη μεταβλητότητας, το πρωτόκολλο ηλεκτρονικής ψηφοφορίας που βασίζεται σε Blockchain μπορεί να θεωρηθεί ως απόδειξη νοθείας, αν και γενικά το Blockchain παρέχει ένα ασφαλές, γρήγορο, διαφανές σύστημα καταμέτρησης και λογοδοσίας για την ψηφοφορία. Οι βασικές προκλήσεις για την επικρατούσα υιοθέτησή του είναι η χαμηλή δημόσια αποδοχή, τεχνολογικά ζητήματα όπως η επεκτασιμότητα και τα προβλήματα αποθήκευσης του χρησιμοποιούμενου συστήματος Blockchain, οι ανησυχίες για το απόρρητο και την ανωνυμία του τελικού χρήστη, η αντίσταση από δικαιούχους του αναποτελεσματικού συστήματος ψηφοφορίας.

3.9.4 Έξυπνες Μεταφορές

Το Έξυπνο Σύστημα Μεταφορών (ITS) ενσωματώνει τη χρήση προηγμένων τεχνολογιών όπως υπολογιστικές συσκευές, δίκτυα αισθητήρων, ασύρματες επικοινωνίες, ηλεκτρονικά μαζί με σύγχρονες στρατηγικές διαχείρισης και τεχνικές διαχείρισης της κυκλοφορίας για να κάνει τα συστήματα μεταφορών αποτελεσματικά, ασφαλή, γρήγορα, άνετα, οικονομικά, κερδοφόρα και συνδεδεμένα. Το έξυπνο σύστημα μεταφοράς περιλαμβάνει συστήματα ελέγχου σημάτων κυκλοφορίας, ενσωμάτωση συστήματος κάμερας ανίχνευσης ταχύτητας (SDCS), αυτόματη αναγνώριση πινακίδων κυκλοφορίας, συστήματα CCTV για παρακολούθηση σε πραγματικό χρόνο και συστήματα διαχείρισης εισιτηρίων κυκλοφορίας.

Η δυνατότητα BFT του Blockchain μπορεί να λύσει το πρόβλημα της επικοινωνίας και της συνεργασίας σε αυτοκίνητα, συσκευές και υποδομές συνδεδεμένες στο δρόμο, smartphone (που ανήκουν σε πεζούς) με πλήρως κατανεμημένο τρόπο για έξυπνα συστήματα μεταφορών. Η αντίσταση «διπλής δαπάνης» του Blockchain θα βοηθήσει σε μια νομισματική συναλλαγή χωρίς κεντρικούς μεσάζοντες, καθιερώνοντας έτσι ένα in-build οικονομικό σύστημα για τα ITS.

Το Blockchain μπορεί να χρησιμοποιηθεί στο οικοσύστημα μεταφορών κοινής χρήσης, δημιουργώντας ένα οικοσύστημα που θα είναι P2P και διαταράσσοντας με τον τρόπο αυτό, το μονοπώλιο των εμπορευματοποιημένων εταιρικών υπηρεσιών μεταφορών όπως το uber, το careem και το lyft. Αυτό θα οδηγήσει σε μια πιο κατανεμημένη οικονομία.

Οι (Yuan & Wang, 2016) πρότειναν το πλαίσιο ITS (B-ITS) επτά επιπέδων βασισμένο σε Blockchain. Στο φυσικό επίπεδο, τα οχήματα μπορούν να εγγραφούν στο Blockchain χρησιμοποιώντας το IoT ως συσκευές επικοινωνίας και υπολογισμού. Το επίπεδο δεδομένων αφορά την ασφαλή προσθήκη δεδομένων με τη μορφή μπλοκ χρησιμοποιώντας SHA256, δέντρα Merkle και χρονική σήμανση στην αλυσίδα μπλοκ. Το επίπεδο δικτύου ασχολείται με τη μετάδοση μπλοκ σε δίκτυα P2P. Το επίπεδο συναίνεσης ασχολείται με την επικύρωση και την επαλήθευση μπλοκ χρησιμοποιώντας διαφορετικούς αλγόριθμους συναίνεσης ώστε να προκύπτει μια παγκόσμια κατάσταση της αλυσίδας μπλοκ. Το επίπεδο κινήτρου ασχολείται με τη διανομή ανταμοιβής σε συνομηλίκους που έχουν προσθέσει ένα έγκυρο μπλοκ στην αλυσίδα μπλοκ. Στο επίπεδο συμβολαίου, αυτόνομα έξυπνα συμβόλαια θα εκτελούνται με την ενεργοποίηση προκαθορισμένων συνθηκών. Το επίπεδο εφαρμογής εξετάζει τις πιθανές περιπτώσεις χρήσης και τα σενάρια εφαρμογής του B-ITS. Οι συγγραφείς συζήτησαν το BITS ως ένα βήμα προς τα εμπρός για το Σύστημα Διαχείρισης Παράλληλων Μεταφορών (PTMS). Ωστόσο, οι ερευνητές δεν ανέφεραν τις τεχνικές λεπτομέρειες για την εφαρμογή του πλαισίου για πρακτικές εφαρμογές στον πραγματικό κόσμο.

3.9.5 Έξυπνη Υγειονομική Περίθαλψη

Ένας από τους πρωταρχικούς στόχους της έξυπνης πόλης είναι να παρέχει υγειονομική περίθαλψη αιχμής στις μάζες. Η ποιότητα της περίθαλψης είναι το μέτρο της ικανότητας των υπηρεσιών υγειονομικής περίθαλψης σε μια έξυπνη πόλη να επιτύχουν τα επιθυμητά αποτελέσματα υγείας σε ατομικό και μαζικό επίπεδο (Glover et al., 2017). Το Blockchain είναι σε θέση να ενισχύσει τον κλάδο της υγειονομικής περίθαλψης. Ολόκληρα ηλεκτρονικά αρχεία υγείας (EHR) μπορούν να αποθηκευτούν σε Blockchain με ταυτοποίηση που βασίζεται σε Blockchain που έχει εκχωρηθεί σε κάθε ασθενή. Η πρόσβαση στις πληροφορίες, η επικύρωση ταυτότητας και τα ζητήματα απορρήτου μπορούν να αντιμετωπιστούν χρησιμοποιώντας έξυπνα συμβόλαια και τεχνολογία ελέγχου πρόσβασης προσανατολισμένη σε Blockchain. Η υγειονομική περίθαλψη είναι ένας κλάδος όπου διαφορετικά μέρη χρειάζονται πρόσβαση στις ίδιες πληροφορίες οι οποίες σχετίζονται με το ιατρικό ιστορικό ενός ασθενούς με διάγνωση και θεραπείες. Η κατανεμημένη αρχιτεκτονική του Blockchain μπορεί να διαχειριστεί την κοινή χρήση δεδομένων, την άδεια πρόσβασης μεταξύ συστημάτων Medicare για κλινική χρήση. Επιπλέον, το Blockchain μπορεί να χρησιμοποιηθεί για τη διαχείριση της εφοδιαστικής αλυσίδας ιατρικών προϊόντων από την κατασκευή έως τη διανομή σε φαρμακευτικά καταστήματα (Angraal et al., 2017), γεγονός που οδηγεί στον εντοπισμό και την πρόληψη της παραχάραξης φαρμάκων με την εξέταση της προέλευσης των ιατρικών προϊόντων.

Οι (Azaria et al., (2016) πρότειναν ένα πρωτότυπο "MedRec" για την αποθήκευση ηλεκτρονικών αρχείων υγείας για ιατρική έρευνα με χρήση Blockchain. Το MedRec παρέχει μια πλατφόρμα για αποθήκευση δεδομένων σε πραγματικό χρόνο, διαλειτουργικά με το σύστημα, των αρχείων υγειονομικής περίθαλψης, ενώ παράλληλα αντιμετωπίζει το απόρρητο των ασθενών και την καλύτερη ποιότητα και ποσότητα δεδομένων για ιατρική έρευνα. Το πρωτόκολλο κατανεμημένου καθολικού είναι παγιωμένο όπως το bitcoin POW. Ο ιατρικός φάκελος αποθηκεύεται χρησιμοποιώντας τον κρυπτογραφικό κατακερματισμό του για την αποφυγή παραβίασης.

Οι συγγραφείς στο (Linn & Koo, 2016) εξέτασαν τα βασικά ζητήματα για τη χρήση της δημόσιας αλυσίδας μπλοκ με στυλ bitcoin για δεδομένα υγειονομικής περίθαλψης. Το κύριο μέλημα είναι η επεκτατική αποθήκευση των αρχείων υγειονομικής περίθαλψης που εμποδίζει την επεκτασιμότητα. Ο ηλεκτρονικός φάκελος υγείας υπογράφεται ψηφιακά από τον πάροχο ή τον ασθενή κατόπιν δημιουργίας για πρόταση προέλευσης. Ο συγγραφέας προτείνει την αποθήκευση μόνο ευρετηρίασης, μεταδεδομένων, δεικτών κατακερματισμού και κρυπτογράφησης που συνδέονται με τον ιατρικό φάκελο στο Blockchain, ενώ το πλήρες αρχείο υγείας αποθηκεύεται εκτός αλυσίδας μπλοκ.

3.9.6 Έξυπνο Δίκτυο – Smart Grid

Το Smart Gird είναι ένα σύγχρονο αυτοσχέδιο ηλεκτρικό δίκτυο για βελτιστοποιημένη απόδοση και αξιοπιστία. Αποτελείται από έξυπνες συσκευές, συσκευές ανίχνευσης, έξυπνους μετρητές, γεννήτριες ηλεκτρικής ενέργειας, ανανεώσιμες πηγές ενέργειας, γραμμές μεταφοράς που είναι υπεύθυνες για την παραγωγή και τη διανομή ηλεκτρικής ενέργειας με αυτοματοποιημένο έλεγχο (Emmanuel & Rayudu, 2016). Το έξυπνο δίκτυο ασχολείται με την προσθήκη δυνατοτήτων ανίχνευσης, παρακολούθησης, επικοινωνίας, ανάλυσης, οπτικοποίησης, υπολογισμού, ελέγχου, αυτοματισμού, διάγνωσης και συντήρησης στο παραδοσιακό σύστημα παροχής ηλεκτρικής ενέργειας. Ο πρωταρχικός στόχος του έξυπνου δικτύου είναι να καλύψει τη ζήτηση με αρκετή προσφορά, να αποτρέψει την απώλεια ενέργειας, να ενισχύσει την αξιοπιστία του δικτύου, την οικονομική προσιτότητα, τη βιωσιμότητα και τη λειτουργική απόδοση.

Οι ανανεώσιμες πηγές ενέργειας (ΑΠΕ) όπως η παραγωγή αιολικής και ηλιακής ενέργειας έχουν εισαγάγει τους λεγόμενους παραγωγούς στις αγορές ενέργειας. Η τοπική παραγωγή ενέργειας για τοπική κατανάλωση έχει χαμηλές απώλειες μετάδοσης εντός του έξυπνου δικτύου. Το Blockchain παρέχει υποδομή συναλλαγών ενέργειας εντός του έξυπνου δικτύου με τρόπο peer to peer χωρίς κεντρική αρχή. Οι (Musleh et al., 2019) συζήτησαν εφαρμογές Blockchain στο έξυπνο δίκτυο, όπως η λειτουργική παρακολούθηση σε πραγματικό χρόνο του δικτύου ηλεκτρικής ενέργειας, η αυτοματοποιημένη αποκεντρωμένη μετάδοση και διανομή ισχύος, η εύρεση της βέλτιστης τοποθεσίας για οικονομική φόρτιση για ένα ηλεκτρικό όχημα, η εξατομικευμένη και αποτελεσματική διαπραγμάτευση ενέργειας μεταξύ προμηθευτών, η φυσική ασφάλεια στον κυβερνοχώρο του έξυπνου δικτύου και οι αποτελεσματικές αναλύσεις κατανάλωσης. Οι συγγραφείς παρουσίασαν ένα πλαίσιο Blockchain ως επίπεδο κυβερνοχώρου για το έξυπνο δίκτυο. Τα Blockchain για συγκεκριμένες εφαρμογές, καθώς και ένα Blockchain που βασίζεται σε συσσωρευτή, αναπτύσσονται με σκοπό την ισχυρή και αξιόπιστη διαχείριση λειτουργίας.

Οι (Dang et al., 2019) συζήτησαν τη χρήση του Blockchain στη διαχείριση από την πλευρά της ζήτησης του έξυπνου δικτύου. Η μελέτη στοχεύει μεγάλους βιομηχανικούς χρήστες ενέργειας και παρουσιάζει μια νέα δομή εμπορίου ηλεκτρικής ενέργειας που βασίζεται στο δίκτυο Blockchain P2P για τη σύμβαση, την επόμενη μέρα, την προσαρμογή και τις αγορές εξισορρόπησης. Επινόησαν ένα βέλτιστο πρόβλημα διαχείρισης φορτίου για έναν συγκεκριμένο βιομηχανικό χρήστη για να ελαχιστοποιήσουν το λειτουργικό κόστος.

Οι (Li et al., 2018) χρησιμοποίησαν την τεχνολογία Blockchain κοινοπραξίας με σκοπό την ασφαλή εμπορία ενέργειας στους κόμβους IIoT που βρίσκονται σε κοντινή γεωγραφική εγγύτητα χωρίς αξιόπιστο μεσάζοντα. Εισάγεται ένα σύστημα πληρωμών με βάση την πίστωση για την αποτελεσματική και ταχεία διαδικασία συναλλαγών, το οποίο παρέχει μια βέλτιστη στρατηγική τιμολόγησης δανείων ακόμη και για καταναλωτές που δεν έχουν πρόβλημα. Το παιχνίδι Stackelberg εφαρμόζεται για την επιλογή της βέλτιστης στρατηγικής τιμολόγησης για τη μεγιστοποίηση της χρησιμότητας της πιστωτικής τράπεζας μέσω κατάλληλου επιτοκίου και επιτόκιο ποινής. Τα έξυπνα συμβόλαια χρησιμοποιούνται για αυτοματοποιημένες συναλλαγές για το εμπόριο ενέργειας μεταξύ προμηθευτών βάσει προκαθορισμένων προτιμήσεων. Οι συσσωρευτές ενέργειας (EAGs) είναι υπεύθυνοι για τη σύζευξη κατάλληλων πωλητών και αγοραστών βάσει των αντίστοιχων ενεργειακών αιτημάτων. Οι συναλλαγές καταγράφονται και ελέγχονται από αυτούς τους προεπιλεγμένους συσσωρευτές ενέργειας με μέτριο λειτουργικό κόστος. Η συναίνεση μεταξύ των συσσωρευτών ενέργειας επιτυγχάνεται χρησιμοποιώντας το PoW. Το προτεινόμενο σχήμα είναι επεκτάσιμο όσον αφορά τον αριθμό των κόμβων που συμμετέχουν IIoT και τον χρόνο επιβεβαίωσης της συναλλαγής. Το κύριο μειονέκτημα του προτεινόμενου συστήματος είναι η σχετικά μικρότερη προστασία του απορρήτου.

3.9.7 Διαχείριση Εφοδιαστικής Αλυσίδας

Οι σύνθετες αλυσίδες εφοδιασμού είναι απαραίτητες για τις βιομηχανίες και τις επιχειρήσεις. Μια αλυσίδα εφοδιασμού περιγράφεται ως μια συνεργασία περισσότερων από δύο οργανισμών που ελέγχουν τη ροή των εμπορευμάτων, των υπηρεσιών κοινής ωφέλειας, της οικονομίας, της γνώσης από μια πηγή στον αντίστοιχο καταναλωτή. Υπάρχει ζήτηση για έναν διαφανή, ιχνηλάσιμο, μηχανισμό εφοδιαστικής αλυσίδας που να προλαμβάνει όλες τις πληροφορίες, από τις πρώτες ύλες έως τις λεπτομέρειες κατασκευής των αλιευτικών προϊόντων, καθώς και την ιχνηλασιμότητα από το εργοστάσιο στον καταναλωτή. Το σύστημα αλυσίδας εφοδιασμού που βασίζεται σε Blockchain μπορεί να καταγράφει όλες τις συγκεκριμένες πληροφορίες κάθε προϊόντος κατά τη διάρκεια του κύκλου ζωής του σε ένα κοινό κατανεμημένο καθολικό με ασφαλή τρόπο. Οι σχετικές πληροφορίες μπορούν να είναι προσβάσιμες σε αντίστοιχες οντότητες.

Οι (Abeyratne & Monfared, 2016) σχεδίασαν ένα σύστημα παραγωγής-προμήθειας-αλυσίδας έτοιμου Blockchain. Με το σύστημα αυτό εκχωρούν σε κάθε προϊόν μια μοναδική ετικέτα ψηφιακής αναγνώρισης. Όλοι οι εμπλεκόμενοι φορείς έχουν πιστοποιημένη πρόσβαση στο καθολικό Blockchain. Επιπλέον αναπτύχθηκε η πλατφόρμα λογισμικού για την εισαγωγή δεδομένων καθώς και για την πρόσβαση στο προφίλ του προϊόντος. Ένα έξυπνο συμβόλαιο αναπτύσσεται για κάθε προϊόν που διέπει τους κανόνες καθώς το προϊόν διέρχεται από την αλυσίδα εφοδιασμού. Το καθολικό θα παρέχει αδιαμφισβήτητα στοιχεία ιδιοκτησίας ενός περιουσιακού στοιχείου μαζί με πληροφορίες θέσης και χρονικής σφράγισης μέσω μιας ασφαλούς διεπαφής χρήστη. Ωστόσο, οι συγγραφείς δεν συζήτησαν τις τεχνικές προκλήσεις που συνεπάγεται η υιοθέτηση του Blockchain στη διαχείριση της εφοδιαστικής αλυσίδας.

Οι (Alahmadi & Lin, 2019) πρότειναν ένα πρωτόκολλο δικαιοσύνης με εξουσιοδότηση Blockchain για τη διαχείριση της εφοδιαστικής αλυσίδας που βασίζεται σε IIoT. Το πρωτόκολλο διασφαλίζει αξιόπιστο κατ' απαίτηση εμπόριο φυσικών αγαθών μεταξύ εμπόρων και προμηθευτών μεταδίδοντας αμετάβλητες εμπορικές πληροφορίες μέσω Blockchain και επιβάλλοντας κυρώσεις μέσω ενός έξυπνου συμβολαίου. Ένα νέο έξυπνο συμβόλαιο αναπτύσσεται για κάθε εμπορική σύμβαση, ενώ η ιδιότητα μη απόρριψης επιβάλλεται με την ψηφιακή υπογραφή της συναλλαγής μέσω ιδιωτικού κλειδιού. Η διαδικασία συναλλαγών περιλαμβάνει την προετοιμασία, την τοποθέτηση παραγγελίας, την τοποθέτηση παραγγελίας, την παράδοση και τη φάση κρίσης με ένα έξυπνο συμβόλαιο. Το προτεινόμενο σχήμα εφαρμόστηκε χρησιμοποιώντας το EVM και πραγματοποιήθηκε αξιολόγηση απόδοσης για χρόνο επιβεβαίωσης συναλλαγής εντός του δικτύου Blockchain.

Οι (Salah et al., 2019) πρότειναν μια προσέγγιση βασισμένη σε Blockchain για αποτελεσματική ιχνηλασιμότητα εντός των αλυσίδων εφοδιασμού γεωργικών προϊόντων και τροφίμων. Η μελέτη επικεντρώθηκε στις καλλιέργειες σόγιας, αλλά το προτεινόμενο σχέδιο είναι γενικό για να εφαρμοστεί στη γεωργική αλυσίδα εφοδιασμού (ASC) οποιουδήποτε καλλιεργητικού προϊόντος. Η τεκμηρίωση βασικών κριτηρίων όπως η χώρα προέλευσης, η σύγχρονη φάση επεξεργασίας των καλλιεργειών, η παρακολούθηση της απόδοσης, η συμμόρφωση με τα κριτήρια αναφοράς ποιότητας και η συμμόρφωση με τις ρυθμιστικές πολιτικές για κάθε χώρα πραγματοποιήθηκε από όλους τους εμπλεκόμενους φορείς μέσω μιας πλατφόρμας Blockchain. Τα έξυπνα συμβόλαια με βάση το Ethereum ρύθμιζαν την αλληλεπίδραση μεταξύ όλων των ενδιαφερομένων, όπως εταιρείες σπόρων, αγρότες, ανελκυστήρες σιτηρών, μεταποιητές σιτηρών, διανομείς, λιανοπωλητές και πελάτες για την αλυσίδα εφοδιασμού της γεωργίας σόγιας με αποκεντρωμένο τρόπο. Ωστόσο, οι συγγραφείς δεν εξήγησαν τις βασικές προκλήσεις που εμπλέκονται, όπως ο χειρισμός των διαφορών, η αυτοματοποιημένη πληρωμή και η πρόληψη της απάτης στην αλυσίδα εφοδιασμού της γεωργίας.

3.10 Περαιτέρω προκλήσεις και συστάσεις

Παρά τα πολλά υποσχόμενα οφέλη και το λαμπρό προβλεπόμενο μέλλον της BIoT, υπάρχουν σημαντικές προκλήσεις στην εξέλιξη και στην ανάπτυξη υφιστάμενων και προγραμματισμένων συστημάτων που θα χρειαστούν περαιτέρω διερεύνηση:

- Πολύπλοκες και τεχνικές προκλήσεις: υπάρχουν ακόμη ζητήματα που πρέπει να αντιμετωπιστούν σχετικά με την επεκτασιμότητα, την ασφάλεια, την κρυπτογραφική ανάπτυξη και τις απαιτήσεις σταθερότητας των νέων εφαρμογών BIoT. Επιπλέον, οι τεχνολογίες αλυσίδας συστοιχιών αντιμετωπίζουν σχεδιαστικούς περιορισμούς στη χωρητικότητα συναλλαγών, στα πρωτόκολλα επικύρωσης ή στην υλοποίηση έξυπνων συμβολαίων. Ακόμα, θα πρέπει να εισαχθούν μέθοδοι για την επίλυση της τάσης ως προς τις συγκεντρωτικές προσεγγίσεις.
- Διαλειτουργικότητα και τυποποίηση: η υιοθέτηση της BIoT θα απαιτήσει τον συμβιβασμό όλων των ενδιαφερομένων για την επίτευξη πλήρους διαλειτουργικότητας (δηλαδή, από τα δεδομένα στη διαλειτουργικότητα πολιτικής) και την ενοποίηση με συστήματα παλαιού τύπου. Θα χρειαστεί επίσης η υιοθέτηση συνεργατικών υλοποιήσεων και η χρήση διεθνών προτύπων για συνεργατική εμπιστοσύνη και προστασία πληροφοριών (δηλαδή, έλεγχος πρόσβασης, έλεγχος ταυτότητας και εξουσιοδότηση). Για παράδειγμα, ο έλεγχος ταυτότητας σε πολλές αρχές ή οργανισμούς απαιτεί Ομοσπονδιακή Διαχείριση Ταυτότητας (Federated Identity Management - FIM). Σε διεθνή κλίμακα, μία FIM υπάρχει επί του παρόντος μόνο σε χαμηλό Επίπεδο Διασφάλισης (low Level of Assurance - LoA). Το απαιτούμενο LoA (από LoA 1 έως LoA 4), όπως ορίζεται από το πρότυπο ISO/IEC 29115:2013, βασίζεται κυρίως στους κινδύνους, στις συνέπειες ενός σφάλματος ελέγχου ταυτότητας ή/και στην κακή χρήση των διαπιστευτηρίων, στον αντίκτυπο που προκύπτει, και σχετικά με την πιθανότητα εμφάνισής τους. Επομένως και μέσω των παραπάνω, προκύπτει ότι θα χρειαστούν μελλοντικά υψηλότερα LoAs.

- Υποδομή αλυσίδας συστοιχιών: θα χρειαστεί να δημιουργηθεί ένα ολοκληρωμένο πλαίσιο εμπιστοσύνης ή υποδομής που να μπορεί να πληροί όλες τις απαιτήσεις για τη χρήση της αλυσίδας συστοιχιών σε συστήματα IoT. Πολλές προσεγγίσεις τελευταίας τεχνολογίας που αντιμετωπίζουν ζητήματα όπως η εμπιστοσύνη, εξαρτώνται από τις πολιτικές και τον έλεγχο μεταξύ τομέων. Για παράδειγμα, οι κυβερνήσεις θα πρέπει να δημιουργήσουν μια υποδομή αλυσίδας συστοιχιών για την υποστήριξη περιπτώσεων χρήσης δημόσιου ενδιαφέροντος.
- Οργανωτικές, διακυβέρνησης, κανονιστικές και νομικές πτυχές: εκτός από τις τεχνολογικές προκλήσεις, η διαμόρφωση του ρυθμιστικού περιβάλλοντος (δηλαδή, η αποκεντρωμένη ιδιοκτησία και η διεθνής δικαιοδοσία) είναι ένα από τα μεγαλύτερα ζητήματα που ξεκλειδώνουν τη δυνητική αξία της BIoT. Για παράδειγμα, είναι πιθανό ορισμένοι προγραμματιστές να παραποιούν την απόδοσή τους στην αλυσίδα συστοιχιών προκειμένου να προσελκύσουν επενδυτές με γνώμονα τα αναμενόμενα κέρδη.
- Γρήγορες δοκιμές πεδίου: στο εγγύς μέλλον, θα πρέπει να βελτιστοποιηθούν διαφορετικοί τύποι αλυσίδων συστοιχιών για διαφορετικές εφαρμογές. Επιπλέον, όταν οι χρήστες θέλουν να συνδυάσουν την αλυσίδα συστοιχιών με τα συστήματα IoT, το πρώτο βήμα είναι να καταλάβουν ποια αλυσίδα συστοιχιών ταιριάζει στις απαιτήσεις τους. Ως εκ τούτου, είναι απαραίτητο να δημιουργηθεί ένας μηχανισμός για τη δοκιμή διαφορετικών αλυσίδων συστοιχιών. Αυτή η προσέγγιση θα πρέπει να χωριστεί σε δύο κύριες φάσεις: τυποποίηση και δοκιμή. Στη φάση της τυποποίησης, μετά από ευρεία κατανόηση των αλυσίδων εφοδιασμού, των αγορών, των προϊόντων και των υπηρεσιών, όλες οι απαιτήσεις πρέπει να αναλυθούν και να συμφωνηθούν. Όταν δημιουργείται μία αλυσίδα συστοιχιών, θα πρέπει να ελέγχεται με βάση τα συμφωνημένα κριτήρια για να επαληθευτεί η απαιτούμενη λειτουργία της. Στην περίπτωση της φάσης δοκιμής, θα πρέπει να αξιολογηθούν διαφορετικά κριτήρια όσον αφορά το απόρρητο, την ασφάλεια, την ενεργειακή απόδοση, την διεκπεραιωτική ικανότητα, την καθυστέρηση, τη χωρητικότητα της αλυσίδας συστοιχιών ή τη χρηστικότητα, μεταξύ άλλων.

Υπό το πρίσμα της προόδου που έχει σημειωθεί τα τελευταία χρόνια στην εφαρμογή και τις λύσεις BIoT, εξακολουθούν να υπάρχουν ορισμένοι τομείς που χρειάζονται περαιτέρω εξέταση. Για την περαιτέρω βελτίωση των εφαρμογών και λύσεων BIoT, απαιτείται περαιτέρω έρευνα καθώς και εξειδικευμένη έρευνα σε ορισμένους τομείς για να καταστεί η ανάπτυξη ασφαλής, και επεκτάσιμη. Οι περιοχές αυτές περιλαμβάνουν τα ακόλουθα:

- Λύσεις βασισμένες στη μηχανική μάθηση για το απόρρητο και την ασφάλεια των εφαρμογών BIoT. Ορισμένες εφαρμογές μηχανικής εκμάθησης για το απόρρητο και την ασφάλεια του BIoT έχουν ήδη συζητηθεί στην εργασία των (Nartey et al., 2021), ωστόσο καλό θα ήταν να εφαρμοστούν άλλοι αλγόριθμοι μηχανικής μάθησης όπως το K-NN και άλλες τεχνικές βαθιάς μάθησης και ομαδοποίησης για την καλύτερη ανίχνευση εισβολής και διατήρηση του απορρήτου

- Τεχνικές Προκλήσεις με την Αποκέντρωση. Λόγω προβλημάτων επεκτασιμότητας, ασφάλειας και απορρήτου, οι περισσότερες από τις εφαρμογές BIoT που έχουν προταθεί μέχρι στιγμής έπρεπε να προσθέσουν κάποια μορφή συγκέντρωσης στο Blockchain. Ωστόσο καθίσταται απαραίτητη η διεξαγωγή έρευνας που θα συμβάλει στη μείωση της τάσης για συγκεντροποίηση και θα κινηθεί προς την κατεύθυνση των πραγματικά αποκεντρωμένων αρχιτεκτονικών που μπορούν να κλιμακωθούν για εφαρμογές BIoT
- Υποδομή Blockchain. Η εμπιστοσύνη είναι ουσιαστικό μέρος της χρήσης IoT σε Blockchains. Ως εκ τούτου, είναι απαραίτητο να υπάρχει ένα σύστημα Blockchain που λύνει πραγματικά το ζήτημα της εμπιστοσύνης στις υλοποιήσεις BIoT, καθώς οι συσκευές IoT παράγουν πολύ ευαίσθητα δεδομένα. Πλήθος προσεγγίσεων έχουν αναπτυχθεί για το λόγο αυτό, οι οποίες όμως εξαρτώνται κυρίως από πολιτικές και συστήματα ελέγχου μεταξύ τομέων. Απαιτείται λοιπόν περισσότερη έρευνα σε αυτόν τον τομέα.
- Διακυβέρνηση, κανονισμοί και νομικές πτυχές. Ο κόσμος του Blockchain, λόγω του υψηλού επιπέδου αποκεντροποίησης του, θεωρείται από πολλούς ως «η γη του κανενός». Δεν υπάρχουν σημαντικοί κανονισμοί και νομικές πτυχές που να δεσμεύουν τη χρήση των Blockchain και την εφαρμογή τους. Η προσθήκη του IoT σε ένα σύστημα που στερείται αυτής της μορφής διακυβέρνησης μπορεί να είναι πολύ επικίνδυνο. Αυτό δεν σημαίνει ότι τα Blockchain θα πρέπει να έχουν εξ ολοκλήρου κεντρικές αρχές, αλλά θα πρέπει να υπάρχουν τουλάχιστον οδηγίες οι οποίες να ακολουθούνται για την εφαρμογή λύσεων και εφαρμογών που θα περιλαμβάνουν IoT.

3.11 Επίλογος

Υπάρχουν πολλά πλεονεκτήματα από τη χρήση Blockchains σε εφαρμογές IoT. Τα IoT, τα τελευταία χρόνια, παρουσιάζουν αναδυόμενες εξελίξεις στις τεχνολογίες που τα τροφοδοτούν. Αυτές οι εξελίξεις σημειώθηκαν στον τομέα των τεχνολογιών επικοινωνίας όπως οι επικοινωνίες 4G/5G, τα συστήματα ελέγχου ταυτότητας και ασφάλειας όπως το RFID και το NFC και τα Cyber-Physical Systems (CPS). Η προσθήκη Blockchain στο IoT εισάγει ζητήματα που επηρεάζουν την επεκτασιμότητα, την επεξεργαστική ισχύ και τον χρόνο, την αποθήκευση, το απόρρητο και τη συνολική απόδοση τέτοιων υλοποιήσεων. Η ανωνυμία του Blockchain είναι κάτι που υπονοείται αλλά δεν εξασφαλίζεται. Αυτό συμβαίνει επειδή οι συσκευές και οι χρήστες των Blockchain προσδιορίζονται από το δημόσιο κλειδί τους ή από το κατακερματισμό τους. Έτσι, οι εισβολείς και οι τρίτοι μπορούν να μελετήσουν τα δημόσια κλειδιά και τους κατακερματισμούς τους και να συναγάγουν την ταυτότητα των κόμβων ή των συμμετεχόντων. Το παραπάνω αποτελεί σοβαρή ανησυχία όταν πρόκειται για συσκευές IoT, επειδή αυτές οι συσκευές συνήθως αποθηκεύουν ή μεταδίδουν ευαίσθητες και προσωπικές πληροφορίες και μόλις επιτευχθεί ένα τέτοιο ίχνος, τότε τίθενται σε κίνδυνο οι συσκευές και οι κάτοχοί τους. Όσον αφορά την εμπιστευτικότητα, το τμήμα που σχετίζεται με τα δεδομένα συναλλαγής σχετίζεται και με το απόρρητό τους, το οποίο αναλύθηκε προηγουμένως. Ενώ, όσον αφορά την υποδομή που υποστηρίζει τα αποθηκευμένα δεδομένα, μπορεί να δηλωθεί ότι οι τρέχουσες εφαρμογές IoT τείνουν να συγκεντρώνουν τις επικοινωνίες σε έναν διακομιστή, σε ένα σύμπλεγμα διακομιστών ή σε ένα νέφος (cloud). Μια τέτοια προσέγγιση ισχύει εφόσον οι διαχειριστές της κεντρικής υποδομής είναι αξιόπιστοι και το σύστημα παραμένει ανθεκτικό έναντι επιθέσεων και εσωτερικών διαρροών. Αντίθετα, οι τεχνολογίες της αλυσίδας συστοιχιών χαρακτηρίζονται ως αποκεντρωμένες. Επομένως, ακόμα και στη περίπτωση που ένας κόμβος βρίσκεται σε κίνδυνο, το παγκόσμιο σύστημα θα πρέπει να συνεχίσει να λειτουργεί. Έχουν εξεταστεί πολλές προσεγγίσεις για τη διασφάλιση της ασφάλειας όσον αφορά τις εφαρμογές BIoT. Ορισμένες χρησιμοποιούν προσεγγίσεις μηχανικής μάθησης και άλλες έχουν ακολουθήσει πιο συμβατικές προσεγγίσεις. Οι διάφορες μελέτες παρουσίασαν διαφορετικούς τρόπους με τους οποίους έχει διασφαλιστεί η ασφάλεια σε ορισμένες εφαρμογές BIoT. Ορισμένες από αυτές τις προσεγγίσεις χρησιμοποίησαν σχήματα όπως ο έλεγχος πρόσβασης, η διασφάλιση εμπιστοσύνης και ακόμη και ο έλεγχος ταυτότητας. Διαπιστώθηκε ότι υπάρχει διαθέσιμη πολύ ενδιαφέρουσα βιβλιογραφία σχετικά με τη διατήρηση της ασφάλειας με παράλληλη βελτίωση της επεκτασιμότητας του Blockchain και αποτελεί έναν τομέα που απαιτεί ακόμα περισσότερη έρευνα. Τα έγγραφα που περιγράφονται εξετάζουν τις συνέπειες του να γίνουν οι λύσεις BIoT πιο επεκτάσιμες, διατηρώντας παράλληλα ένα υψηλό επίπεδο ασφάλειας. Μόλις μια εφαρμογή BIoT γίνει πιο επεκτάσιμη, συνήθως γίνεται εις βάρος μιας πτυχής του Blockchain, η οποία με τη σειρά της μπορεί να προκαλέσει ευπάθειες ασφαλείας. Η επεκτασιμότητα είναι ένα σημαντικό ζήτημα που έχει ταλαιπωρήσει τα Blockchain όλα αυτά τα χρόνια ύπαρξης της τεχνολογίας. Πρόκειται για ένα πρόβλημα που προκαλείται από πολλούς παράγοντες όπως το υψηλό επίπεδο της χρησιμοποιούμενης κρυπτογραφίας και οι αλγόριθμοι συναίνεσης (οι οποίοι συνήθως απαιτούν υψηλή υπολογιστική ισχύ). Πρόκειται για μία πτυχή που προκαλεί ανησυχία όταν εξετάζεται η εφαρμογή του BIoT λόγω των περιορισμένων πόρων που υπάρχουν σε αυτές τις συσκευές IoT. Όλα τα παραπάνω επηρεάζουν την απόδοση των δικτύων Blockchain.

Κεφάλαιο 4ο: Πρακτικό Μέρος

4.1 Στόχος εφαρμογής

Για την ανάπτυξη συμβολαίων για την χρήση σε οποιοδήποτε κλάδο και ακόμα περισσότερο στο Internet Of Things που απαιτούνται συνδέσεις με αισθητήρες απαιτούνται διαδικασίες που είναι ιδιαίτερα πολύπλοκες και ένας χρήστης θα δυσκολευτεί πάρα πολύ να προχωρήσει σε αυτές.

Για το λόγο αυτό απαιτούνται εφαρμογές που να απλοποιούν την διαδικασία των έξυπνων συμβολαίων και από απλούς χρήστες. Με βάση την απαίτηση αυτή είναι η δημιουργία μιας εφαρμογή όπου κάθε χρήστης θα μπορεί με εύκολο τρόπο μέσα από ένα γραφικό περιβάλλον WEB να δημιουργήσει τα δικά του συμβόλαια τόσο για Internet of Things όσο και για οτιδήποτε άλλο. Πιο συγκριμένα οι χρήστες θα κάνουν εγγραφή και θα δημιουργούν και θα αποθηκεύουν εκεί τα συμβόλαια τους παράγοντας τον κατάλληλο κώδικα solidity που χρειάζεται ώστε τελικά να δημιουργήσουν στο Ethereum το συμβόλαιο τους, ενώ ταυτόχρονα θα έχει δημιουργηθεί το κατάλληλο περιβάλλον web για τις συναλλαγές τους.

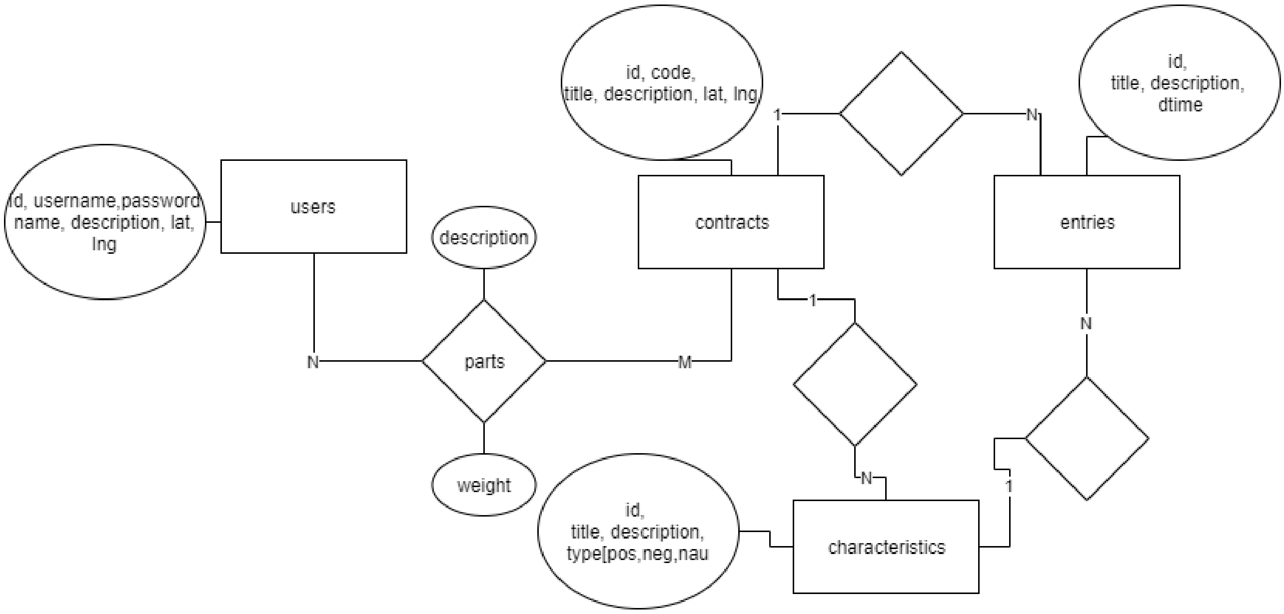
Για το λόγο αυτό δημιουργήθηκε κατάλληλο περιβάλλον σε διαδικτυακό τόπο με τεχνολογίες WEB όπου ένας χρήστης μπορεί να κάνει μια εγγραφή και εκεί να δημιουργήσει τα συμβόλαια του.

Έτσι έχουμε την δυνατότητα να ορίσουμε ένα σύστημα συμβάσεων με συμβαλλόμενους που λειτουργούν μέσα σε ένα Blockchain ορίζοντας τι θα καταγράφεται και τις συνθήκες ελέγχου της σύμβασης . Κάθε αλλαγή μπορεί να εφαρμόζεται κατόπιν συμφωνίας και με τους δύο συμβαλλόμενους κρατώντας και τη χρονική σειρά.

4.2 Η βάση δεδομένων Database

Για να εκτελεστεί το παραπάνω δημιουργήθηκε κατάλληλη βάση με οντότητες τους χρήστες , τα συμβόλαια τους και τελικά τα στοιχεία στο Ethereum.

Το αντίστοιχο διάγραμμα με τις σχέσεις των οντοτήτων φαίνεται παρακάτω:



Σχήμα 4-1. Διάγραμμα εφαρμογής με τις σχέσεις των οντοτήτων.

4.3 Τεχνολογίες που χρησιμοποιούνται

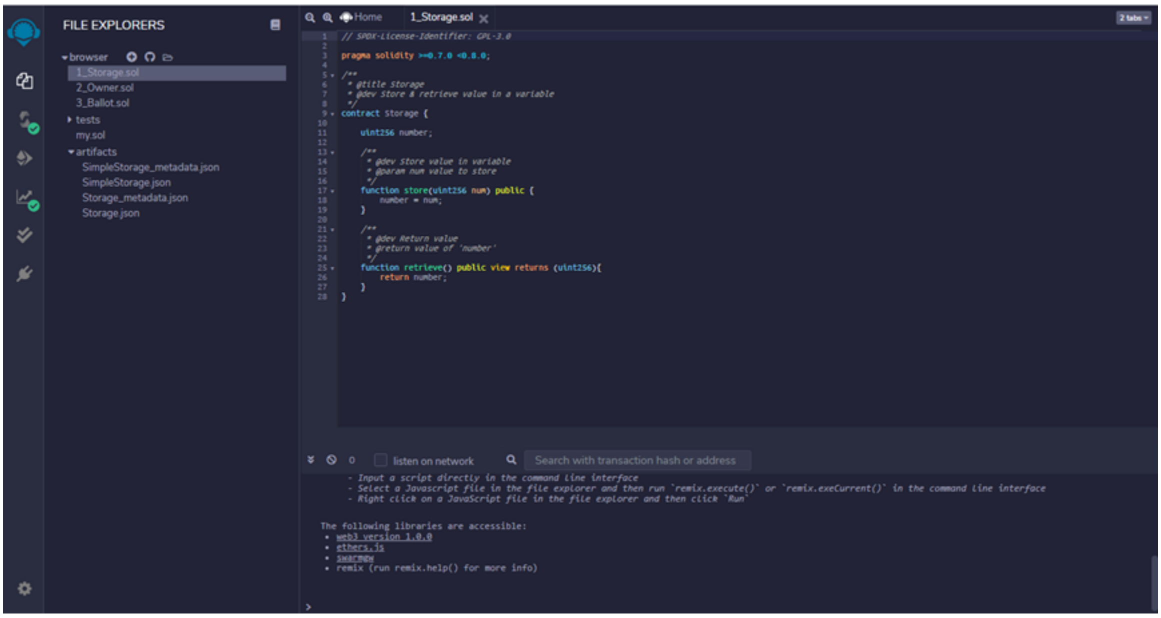
Για εφαρμογή μας θα γίνει χρήση των παρακάτω τεχνολογιών που είναι απαραίτητες για την εφαρμογή μας:

4.3.1 Remix IDE

Το Remix είναι ένα κατάλληλο περιβάλλον για τον προγραμματισμό συμβολαίων Ethereum με χρήση της γλώσσα προγραμματισμού για smart contracts που ονομάζεται Solidity. Το Remix IDE διαθέτει ενσωματωμένο περιβάλλον εντοπισμού σφαλμάτων και δοκιμών. Η διαδικτυακή έκδοση είναι διαθέσιμη στο http://remix.ethereum.org.

Το Remix είναι μια καλή λύση γιατί διαθέτει τα παρακάτω:

- Δημιουργία συμβολαίων με την γλώσσα solidity
- Εντοπισμός σφαλμάτων εκτέλεσης έξυπνου συμβολαίου
- Πρόσβαση στην κατάσταση και ιδιότητες ενός εκτελεσθέντος συμβολαίου
- Ανάλυση κώδικα σταθερότητας ώστε να έχουμε ελαχιστοποίηση των λαθών κωδικοποίησης
- Μαζί με το Mist ή το Metamask (που αναφερόμαστε παρακάτω), το Remix μπορεί να χρησιμοποιηθεί για τον έλεγχο και τον εντοπισμό σφαλμάτων μίας εφαρμογής συμβολαίων.



Σχήμα 4-2. Το περιβάλλον του Remix.

4.3.2 MetaMask

Το Metamask είναι ουσιαστικά ένα πρόσθετο στο αντίστοιχο φυλλομετρητή που επιλέγουμε (δοκιμάστηκε στη περίπτωση μας στο Chrome) και λειτουργεί σαν γέφυρα που επιτρέπει να επισκεφθείτε τον κατανεμημένο ιστό. Δίνει την δυνατότητα εκτέλεσης Ethereum dApps απευθείας σε ένα πρόγραμμα περιήγησής χωρίς να εκτελείτε έναν πλήρη κόμβο Ethereum. Το MetaMask περιλαμβάνει ένα ασφαλές «θησαυροφυλάκιο» ταυτότητας, που παρέχει μια διεπαφή χρήστη για τη διαχείριση των ταυτοτήτων του σε διαφορετικούς ιστότοπους και υπογράφει συναλλαγές Blockchain.

Το πρόσθετο Metamask μπορεί να εγκατασταθεί ακολουθώντας στον παρακάτω σύνδεσμο https://www.metamask.io/

Για τις δοκιμές μας μπορούμε να χρησιμοποιήσουμε ένα πάροχο για Etherium που μπορούμε να αγοράσουμε Ethers (για δοκιμές) όπως ο Ropsten Test Network . Διαφορετικά θα πρέπει να αγοράσουμε πραγματικά Ethers.

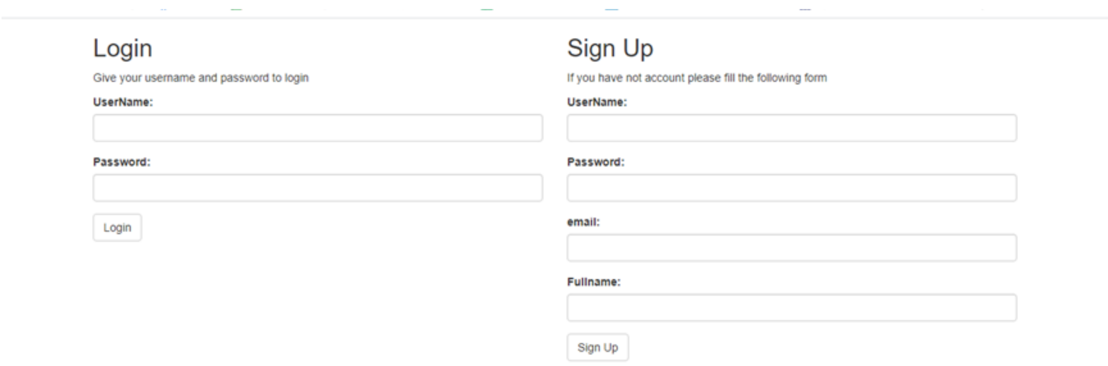
4.3.3 MySQL

Το σύστημα βάσεων δεδομένων MySQL και πρόσβαση σε αυτό μέσω ενός server APACHE απαιτείται για την προσομοίωση της βάσης δεδομένων

4.3.4 Η εφαρμογή

Δημιουργήθηκε κατάλληλο περιβάλλον σε διαδικτυακό τόπο με τεχνολογίες WEB όπου ένας χρήστης μπορεί να κάνει μια εγγραφή και εκεί να δημιουργήσει τα συμβόλαια του.

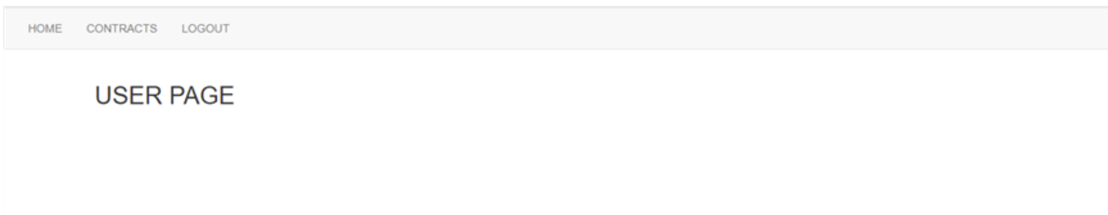
Πιο συγκεκριμένα αρχικά ο χρήστης εισέρχεται στο σύστημα κάνοντας μια εγγραφή



Σχήμα 4-3. Αρχική οθόνη της εφαρμογής, για την εγγραφή νέου χρήση ή για τη σύνδεση των υπαρχόντων χρηστών.

Αφού ο χρήστης κάνει την εγγραφή του τότε μπορεί να κάνει login με το username και password που έδωσε στην εγγραφή του

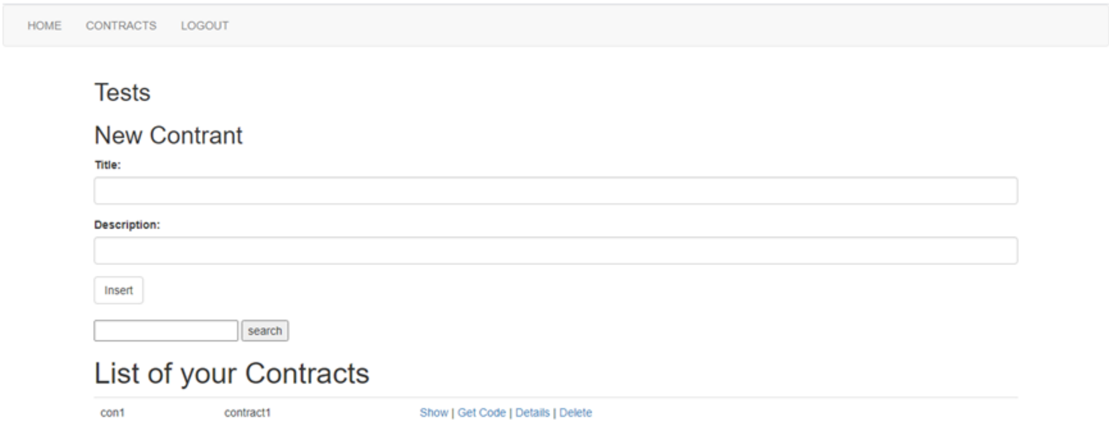
Ο χρήστης αν δώσει σωστά τα στοιχεία του εισέρχεται στην παρακάτω σελίδα



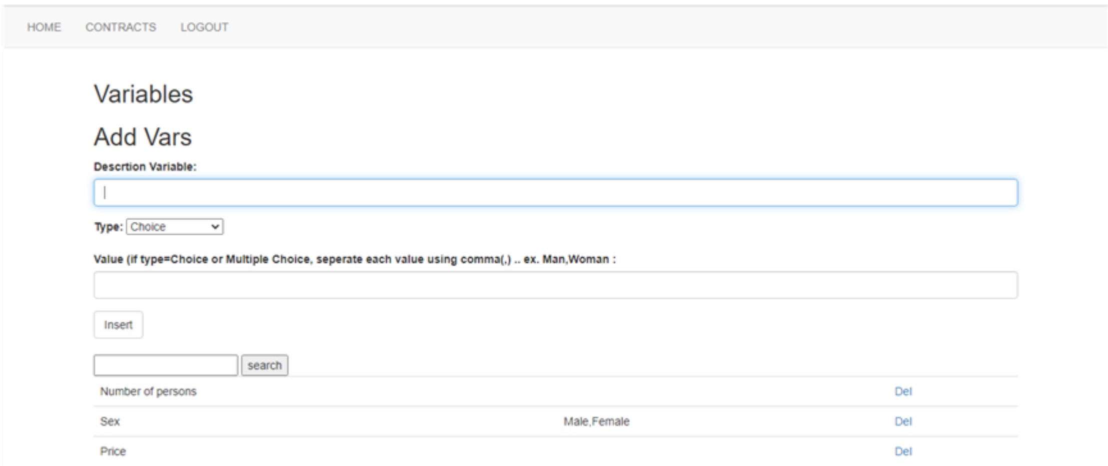
Σχήμα 4-4. Επιτυχής είσοδος του χρήστη στην εφαρμογή.

Στην σελίδα αυτή μπορεί να διαχειριστεί τα συμβόλαια του ή να δημιουργήσει ένα καινούριο όπως φαίνεται στην παρακάτω εικόνα:

Για να εισάγει τις μεταβλητές ενός νέου συμβολαίου αρκεί να πατήσει details όπου εκεί εισάγεται σε μια σελίδα που δημιουργεί τις μεταβλητές του συμβολαίου.



Σχήμα 4-5. Δημιουργία νέο συμβολαίου από τον χρήστη.



Σχήμα 4-6. Καταχώρηση μεταβλητών κατά τη δημιουργία ενός νέου συμβολαίου.

Παρακάτω φαίνεται ένα συμβόλαιο που απαιτεί 3 μεταβλητές που είναι ο αριθμός ατόμων που αφορούν μια αγορά, το φύλο του αγοραστεί , η τιμή τελικά της αγοράς.

Επιλέγοντας σε ένα συμβόλαιο η επιλογή Get Code μας δίνεται ο κώδικας solidity που χρειάζεται για τη δήλωση του συμβολαίου στο Ethereum. Για να το περάσουμε αυτό αρκεί να πάμε στο Remix IDE και να κάνουμε μια απλή αντιγραφή το κώδικα μας και Deploy και πλέον έχουμε δηλώσει στο Ethereum το συμβόλαιο μας

Ο κώδικας μας στο παραπάνω συμβόλαιο είναι:

```
pragma solidity ^0.4.0;


contract contr9 {
```

```
        string public title="con1";
        string public descr="contract1";
        string  public  var0="Number of persons";
        string  public  val0="";
        string  public  var1="Sex";
        string  public  val1="";
        string  public  var2="Price";
        string  public  val2="";
        uint ne=3;

function getQNum() public view returns(uint){
            return ne;
         }

function getQ0() public view returns(string){
            return var0;
         }

function getA0() public view returns(string){
            return val0;
         }

function setA0(string x) public returns(string){
             val0 = x;
             return val0;
         }

function getQ1() public view returns(string){
            return var1;
         }

function getA1() public view returns(string){
            return val1;
```

```
        }

function setA1(string x) public returns(string){
             val1 = x;
             return val1;
        }

function getQ2() public view returns(string){
            return var2;
        }

function getA2() public view returns(string){
            return val2;
        }

function setA2(string x) public returns(string){
             val2 = x;
             return val2;
        }
}
```

Τελικά θα έχουμε δηλώσει το συμβόλαιο μας.

Με την επιλογή Show έχουμε πλεόν το περιβάλλον συναλλαγών του συγκεκριμένου συμβολαίου όπου οι χρήστες μπορούν να περνούν τις συναλλαγές τους, δίνοντας τους απλά το link που παράγεται .

Στην περίπτωση μας είναι το παρακάτω:

Σχήμα 4-7. Προβολή ενός συμβολαίου από την εφαρμογή.

Για να λειτουργήσει αυτό φυσικά πρέπει ο κάθε χρήστης να διαθέτει ένα λογαριασμό στο ethereum δηλαδή να έχει νομίσματα για να κάνει την συναλλαγή του.

Κεφάλαιο 5ο: Συμπεράσματα

Οι τρεις θεμελιώδεις ιδιότητες της τεχνολογίας Blockchain ως δομή δεδομένων, δηλαδή η διανομή, η αμεταβλητότητα και η αποκέντρωση, μπορούν να ωφελήσουν ιδιαίτερα το Διαδίκτυο των Πραγμάτων (IoT) και τις συσκευές που το απαρτίζουν. Η κατανεμημένη πτυχή του Blockchain σημαίνει ότι τα δεδομένα αναπαράγονται σε πολλούς υπολογιστές. Αυτό το γεγονός καθιστά τις κακόβουλες επιθέσεις αναποτελεσματικές αφού πλέον υπάρχουν αρκετές συσκευές-στόχοι. Ο πλεονασμός στον χώρο αποθήκευσης που προκαλείται από την τεχνολογία Blockchain φέρνει επιπλέον ασφάλεια και ενισχύει την πρόσβαση στα δεδομένα, καθώς οι χρήστες στα οικοσυστήματα IoT μπορούν να υποβάλλουν και να ανακτούν τα δεδομένα τους από διαφορετικές συσκευές. Η αμετάβλητη φύση της τεχνολογίας Blockchain σημαίνει ότι οποιαδήποτε αλλαγή στα αποθηκευμένα δεδομένα μπορεί εύκολα να εντοπιστεί. Ωστόσο, η πτυχή της αποκέντρωσης της τεχνολογίας Blockchain μπορεί να είναι ένα σημαντικό ζήτημα κατά την αποθήκευση δεδομένων από συσκευές IoT. Η αποκέντρωση σημαίνει ότι οι υπολογιστές που χρησιμοποιούνται για την αποθήκευση δεδομένων με κατανεμημένο τρόπο μπορεί να ανήκουν σε διαφορετικές οντότητες. Με άλλα λόγια, εάν δεν εφαρμοστεί σωστά, υπάρχει ο κίνδυνος τα ευαίσθητα δεδομένα των χρηστών να μπορούν πλέον να αποθηκευτούν από προεπιλογή και να είναι διαθέσιμα σε τρίτους.

Μια διαφορετική δυνατότητα κατά τη χρήση του Blockchain στο πλαίσιο του IoT είναι η αποθήκευση αρχείων καταγραφής πρόσβασης και αδειών. Συγκεκριμένα, η κατανεμημένη και η αποκέντρωση πτυχή του Blockchain καθιστούν εξαιρετικά δαπανηρή την αποθήκευση μεγάλων δεδομένων. Μια εναλλακτική είναι η διατήρηση των δεδομένων σε ένα κεντρικό αποθετήριο ενώ αποθηκεύονται αρχεία καταγραφής σχετικά με την πρόσβαση στα δεδομένα χρησιμοποιώντας τεχνολογία Blockchain. Στη συνέχεια, οι χρήστες έχουν μια αμετάβλητη δομή δεδομένων η οποία μπορεί να δείξει ποιος είχε πρόσβαση στα δεδομένα τους καθώς και τη χρονική στιγμή που υπήρξε η πρόσβαση.

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για την αποθήκευση αδειών πρόσβασης σε δεδομένα που εκδίδονται από χρήστες. Οποιοδήποτε τρίτο μέρος που απαιτεί πρόσβαση στα δεδομένα ενός χρήστη θα πρέπει πρώτα να το ζητήσει με ένα αίτημα. Αυτά τα αιτήματα καθώς και οι απαντήσεις τους μπορούν να αποθηκευτούν στην αλυσίδα των δεδομένων του Blockchain. Με τη χρήση Blockchain sta IoT, οι χρήστες και οι αιτούντες δεδομένα έχουν μια αμετάβλητη βάση δεδομένων που μπορεί να προσδιορίσει αναμφίβολα ποιος έχει πρόσβαση σε συγκεκριμένα δεδομένα. Αυτή η εφαρμογή έχει μεγάλες δυνατότητες να βελτιώσει το απόρρητο και να αποτελέσει τη ραχοκοκαλιά μιας αγοράς δεδομένων όπου οι χρήστες μπορούν να επωφεληθούν από την πώληση των δικών τους δεδομένων.

Το κατανεμημένο καθολικό ενός blockchain είναι αδιάψευστο, εξαλείφοντας την ανάγκη των εμπλεκόμενων μερών να εμπιστεύονται ο ένας τον άλλον. Ως εκ τούτου, κανένα μέρος δεν έχει τον έλεγχο του τεράστιου όγκου δεδομένων που παράγουν οι συσκευές IoT. Η κρυπτογράφηση Blockchain καθιστά ουσιαστικά αδύνατο για οποιονδήποτε να αντικαταστήσει τα υπάρχοντα αρχεία δεδομένων. Ως εκ τούτου, η χρήση του blockchain για την αποθήκευση δεδομένων IoT προσθέτει ένα άλλο επίπεδο ασφάλειας για να αποτρέψει τους κακόβουλους εισβολείς από το να αποκτήσουν πρόσβαση στο δίκτυο.

Μια κύρια πρόκληση για τους χρήστες του IoT είναι να προστατεύσουν τις πληροφορίες σε ολόκληρο το οικοσύστημα IoT. Τα τρωτά σημεία ασφαλείας καθιστούν τις συσκευές IoT εύκολο στόχο για επιθέσεις κατανεμημένης άρνησης υπηρεσίας, κακόβουλους εισβολείς και παραβιάσεις δεδομένων.

Η ενσωμάτωση του Blockchain στα συστήματα IoT ανοίγει την πόρτα για νέες δυνατότητες που μειώνουν εγγενώς την αναποτελεσματικότητα των κακόβουλων επιθέσεων, ενισχύουν την ασφάλεια και βελτιώνουν τη διαφάνεια για όλα τα εμπλεκόμενα μέρη, ενώ παράλληλα επιτρέπουν ασφαλείς συναλλαγές μεταξύ των χρηστών και των συσκευών IoT. Η σύζευξη αυτών των τεχνολογιών επιτρέπει την παρακολούθηση ενός φυσικού περιουσιακού στοιχείου σε κάθε βήμα της αλυσίδας.

Στα οφέλη από την ενσωμάτωση του Blockchain στα συστήματα IoT συγκαταλέγεται η ενισχυμένη ασφάλεια, το μειωμένο κόστος και οι ταχύτητα των συναλλαγών. Η τεχνολογία Blockchain ενσωματώνει ασφάλεια με τη δυνατότητα επαλήθευσης και επιτρέποντας συναλλαγές που προέρχονται από ένα αξιόπιστο μέρος, καθώς και κρυπτογράφηση κατά τη μετάδοση και αποθήκευση των δεδομένων. Επιπλέον, παρέχει διαφάνεια σχετικά με το ποιος έχει πρόσβαση και ποιος συναλλάσσεται, διατηρώντας όλες αυτές τις πληροφορίες σε ένα αρχείο αλληλεπιδράσεων. Ακόμη, το Blockchain προσθέτει ένα επίπεδο ασφαλείας όσον αφορά την κρυπτογράφηση, την αφαίρεση ενός μόνο σημείου αστοχίας και τη δυνατότητα γρήγορης αναγνώρισης του αδύναμου κρίκου σε ολόκληρο το δίκτυο.

Στην παρούσα μελέτη δημιουργήθηκε ένα κατάλληλο περιβάλλον σε έναν διαδικτυακό τόπο με τεχνολογίες WEB όπου ένας χρήστης μπορεί να κάνει μια εγγραφή και εκεί να δημιουργήσει τα συμβόλαια του. Με αυτό τον τρόπο, υπάρχει η δυνατότητα να ορίσουμε ένα σύστημα συμβάσεων με συμβαλλόμενους που λειτουργούν μέσα σε ένα Blockchain, ορίζοντας τι θα καταγράφεται καθώς και τις συνθήκες ελέγχου της σύμβασης. Κάθε αλλαγή μπορεί να εφαρμόζεται κατόπιν συμφωνίας και με τους δύο συμβαλλόμενους κρατώντας και τη χρονική σειρά. Για την ανάπτυξη της εφαρμογής έγινε χρήση των τεχνολογιών Remix IDE, που αποτελεί ένα κατάλληλο περιβάλλον για τον προγραμματισμό συμβολαίων Ethereum με χρήση της γλώσσα προγραμματισμού για Smart Contracts που ονομάζεται Solidity, του Metamask που στην ουσία αποτελεί ένα πρόσθετο στον φυλλομετρητή που επιλέγουμε και λειτουργεί σαν γέφυρα που επιτρέπει την πρόσβαση στον κατανεμημένο ιστό. Δίνει την δυνατότητα εκτέλεσης Ethereum dApps απευθείας σε ένα πρόγραμμα περιήγησής χωρίς να εκτελείτε έναν πλήρη κόμβο Ethereum. Τέλος, έγινε χρήση μιας βάσης της MySQL με τη χρήση ενός APACHE server.

Στον διαδικτυακό τόπο, ο χρήστης μπορεί να κάνει μια εγγραφή και εκεί να δημιουργήσει τα συμβόλαια του. Για να εισάγει τις μεταβλητές ενός νέου συμβολαίου αρκεί να πατήσει details όπου εκεί εισάγεται σε μια σελίδα που δημιουργεί τις μεταβλητές του συμβολαίου. Με την επιλογή Show, στον χρήστη εμφανίζεται το περιβάλλον συναλλαγών του συγκεκριμένου συμβολαίου όπου οι χρήστες μπορούν να περνούν τις συναλλαγές τους, δίνοντας τους απλά το link που παράγεται . Για να λειτουργήσει αυτό φυσικά πρέπει ο κάθε χρήστης να διαθέτει ένα λογαριασμό στο ethereum δηλαδή να έχει νομίσματα για να κάνει την συναλλαγή του.

Η εφαρμογή μπορεί να λειτουργήσει σε οποιοδήποτε περιβάλλον που περιλαμβάνει αισθητήρες οι οποίοι επικοινωνούν με το διαδίκτυο ή το κεντρικό μηχάνημα και μπορεί να παραμετροποιηθεί . Μελλοντικά η εφαρμογή θα μπορούσε να βελτιωθεί με τη δημιουργία ενός περισσότερο εύκολου περιβάλλοντος προς τον χρήστη που θα μπορεί να το χρησιμοποιήσει σε οποιαδήποτε περίπτωση συστημάτων με αισθητήρες και όπου απαιτεί μεγάλη ασφάλεια.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, *5*(9), 1-10.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.

Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchainBlockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 840-852.

Alahmadi, A., & Lin, X. (2019, May). Towards secure and fair IIoT-enabled supply chain management via blockchainBlockchain-based smart contracts. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

Alam, T. (2018). A reliable communication framework and its use in internet of things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, *3*(5), 450-456.

Alam, T. (2019). Middleware implementation in cloud-MANET mobility model for internet of smart devices. *arXiv preprint arXiv:1902.09744*.

Alam, T., & Benaida, M. (2018). CICS: Cloud–internet communication security framework for the internet of smart devices. *International Journal of Interactive Mobile Technologies (iJIM)*, *12*(6), 74-84.

Alam, T., & Benaida, M. (2019). The role of cloud-MANET framework in the internet of things (IoT). *arXiv preprint arXiv:1902.09436*.

Alam, T., Kumar, P., & Singh, P. (2014). Searching mobile nodes using modified column mobility model. *International Journal of Computer Science and Mobile Computing*, *3*(1), 513-518.

Alam, T., Srivastava, A. P., Gupta, S., & Tiwari, R. G. (2010). Scanning the node using modified column mobility model. *Computer Vision and Information Technology: Advances and Applications*, *455*.

Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur*, *19*, 244-258.

Ali, M. S., Dolui, K., & Antonelli, F. (2017, October). IoT data privacy via blockchainBlockchains and IPFS. In *Proceedings of the seventh international conference on the internet of things* (pp. 1-7).

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchainBlockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1676-1717.

Alladi, T., Chamola, V., Parizi, R. M., & Choo, K. K. R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access*, *7*, 176935-176951.

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... & Zanichelli, F. (2018, April). IoTChain: A blockchainBlockchain security architecture for the Internet of Things. In *2018 IEEE wireless communications and networking conference (WCNC)* (pp. 1-6). IEEE.

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., ... & Zanichelli, F. (2018, April). IoTChain: A blockchainBlockchain security architecture for the Internet of Things. In *2018 IEEE wireless communications and networking conference (WCNC)* (pp. 1-6). IEEE.

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. *Circulation: Cardiovascular quality and outcomes*, *10*(9), e003800.

Asgaonkar, A., & Krishnamachari, B. (2019, May). Solving the buyer and seller’s dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 262-267). IEEE.

Aslam, J., Khan, S. H., Siddiqui, Z. H., Fatima, Z., Maqsood, M., Bhat, M. A., ... & Mujib, A. (2010). Catharanthus roseus (L.) G. Don. An important drug: it’s applications and production. *Pharmacie Globale (IJCP)*, *4*(12), 1-16.

Atya, A. O. F., Qian, Z., Krishnamurthy, S. V., La Porta, T., McDaniel, P., & Marvel, L. (2017, May). Malicious co-residency on the cloud: Attacks and defense. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications* (pp. 1-9). IEEE.

Aumasson, J. P., Henzen, L., Meier, W., & Phan, R. C. W. (2008). Sha-3 proposal blake. *Submission to NIST*, *92*.

Axon, L., & Goldsmith, M. (2017, July). PB-PKI: A Privacy-aware Blockchain-based PKI. In *SECRYPT* (pp. 311-318).

Ayed, A. B. (2017). A conceptual secure blockchainBlockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), 01-09.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchainBlockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchainBlockchain innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblockchainBlockchain-innovations-with-pegged-sidechains*, *72*.

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *9*(10), 533-546.

Banasik, W., Dziembowski, S., & Malinowski, D. (2016, September). Efficient zero-knowledge contingent payments in cryptocurrencies without scripts. In *European Symposium on Research in Computer Security* (pp. 261-280). Springer, Cham.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the age of blockchainBlockchains. *arXiv preprint arXiv:1711.03936*.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012, February). Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security* (pp. 399-414). Springer, Berlin, Heidelberg.

Benet, J. (2015). Replication on IPFS—or, the backing-up content model.

Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2014, November). Sybil-resistant mixing for bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 149-158). ACM.

Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchainBlockchain technology. In *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)* (pp. 1392-1393). IEEE.

Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchainBlockchain technology. In *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)* (pp. 1392-1393). IEEE.

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchainBlockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)* (pp. 772-777). IEEE.

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchainBlockchains in the pharma supply-chain. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 772-777). IEEE.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy* (pp. 104-121). IEEE.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. Anonymity for Bitcoin with accountable mixes.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16).

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, April). Towards better availability and accountability for iot updates by means of a blockchainBlockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 50-58). IEEE.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017, April). Towards better availability and accountability for iot updates by means of a blockchainBlockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 50-58). IEEE.

Brady, S., Hava, A., Perry, P., Murphy, J., Magoni, D., & Portillo-Dominguez, A. O. (2017, June). Towards an emulated IoT test environment for anomaly detection using NEMU. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM, September*, *1*(1), 15.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*, 37.

Buterin, V. (2015). On public and private blockchainBlockchains. *Ethereum blog*, *7*.

Cachin, C. (2016, July). Architecture of the hyperledger blockchainBlockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310, No. 4).

Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A blockchainBlockchain connected gateway for BLE-based devices in the internet of things. *ieee access*, *6*, 24639-24649.

Chakraborty, R. B., Pandey, M., & Rautaray, S. S. (2018). Managing computation load on a blockchainBlockchain–based multi–layered internet–of–things network. *Procedia computer science*, *132*, 469-476.

Chang, S. E., & Chen, Y. (2020). When blockchainBlockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access*, *8*, 62478-62494.

Chaum, D. (1984). Blind signature system. In *Advances in cryptology* (pp. 153-153). Springer, Boston, MA.

Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., & Yu, S. (2020). Blockchain for Internet of things applications: A review and open issues. *Journal of Network and Computer Applications*, *172*, 102839.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile networks and applications*, *19*(2), 171-209.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292-2303.

Cleve, R. (1986, November). Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing* (pp. 364-369). ACM.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-6). IEEE.

Consult, S. E. C. (2015). House of keys: Industry-wide HTTPS certificate and SSH key reuse endangers millions of devices worldwide. In *International Symposium on Consumer Electronics* (pp. 23-30).

Correia, M., Veronese, G. S., Neves, N. F., & Verissimo, P. (2011). Byzantine consensus in asynchronous message-passing systems: a survey. *International Journal of Critical Computer-Based Systems*, *2*(2), 141-161.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE access*, *6*, 46134-46145.

Dang, C., Zhang, J., Kwong, C. P., & Li, L. (2019). Demand side load management for big industrial energy users under blockchainBlockchain-based peer-to-peer electricity market. *IEEE Transactions on Smart Grid*, *10*(6), 6426-6435.

Decker, C., & Wattenhofer, R. (2015, August). A fast and scalable payment network with bitcoin duplex micropayment channels. In *Symposium on Self-Stabilizing Systems* (pp. 3-18). Springer, Cham.

Dong, G., & Wang, X. (2020, May). A secure IoT data integrity auditing scheme based on consortium blockchainBlockchain. In *2020 5th IEEE International Conference on Big Data Analytics (ICBDA)* (pp. 246-250). IEEE.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchainBlockchain for IoT. In *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 173-178). IEEE.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchainBlockchain. *IEEE security & privacy*, *16*(4), 20-29.

Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 489-516.

Egbertsen, W., Hardeman, G., van den Hoven, M., van der Kolk, G., & van Rijsewijk, A. (2016). Replacing paper contracts with Ethereum smart contracts.

Emmanuel, M., & Rayudu, R. (2016). Communication technologies for smart grid applications: A survey. *Journal of Network and Computer Applications*, *74*, 133-148.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, 32979-33001.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188-2204.

Fraga-Lamas, P. (2017). Enabling technologies and cyber-physical systems for mission-critical scenarios.

Fraga-Lamas, P., Castedo-Ribas, L., Morales-Méndez, A., & Camas-Albar, J. M. (2016, May). Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN. In *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (pp. 1-8). IEEE.

Fraga-Lamas, P., Fernández-Caramés, T. M., Noceda-Davila, D., & Vilar-Montesinos, M. (2017, May). RSS stabilization techniques for a real-time passive UHF RFID pipe monitoring system for smart shipyards. In *2017 IEEE International Conference on RFID (RFID)* (pp. 161-166). IEEE.

Fraga-Lamas, P., Noceda-Davila, D., Fernández-Caramés, T. M., Díaz-Bouza, M. A., & Vilar-Montesinos, M. (2016). Smart pipe system for a shipyard 4.0. *Sensors*, *16*(12), 2186.

França, B. F. (2015). Homomorphic mini-blockchainBlockchain scheme.

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. *IEEE Communications Surveys & Tutorials*, *19*(4), 2456-2501.

Glover, W., Li, Q., Naveh, E., & Gross, M. (2017). Improving quality of care through integration in a hospital setting: A human systems integration approach. *IEEE Transactions on Engineering Management*, *64*(3), 365-376.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

Hasan, H. R., & Salah, K. (2018). Proof of delivery of digital assets using blockchainBlockchain and smart contracts. *IEEE Access*, *6*, 65439-65448.

Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016, April). World of empowered IoT users. In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 13-24). IEEE.

Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016, April). World of empowered IoT users. In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 13-24). IEEE.

Heilman, E., Baldimtsi, F., & Goldberg, S. (2016, February). Blindly signed contracts: Anonymous on-blockchainBlockchain and off-blockchainBlockchain bitcoin transactions. In *International conference on financial cryptography and data security* (pp. 43-60). Springer, Berlin, Heidelberg.

Hernández-Rojas, D. L., Fernández-Caramés, T. M., Fraga-Lamas, P., & Escudero, C. J. (2018). Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications. *Sensors*, *18*(1), 57.

Huh, S., Cho, S., Kim, S., "Managing IoT devices using blockchainBlockchain platform", in Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, South Korea, 19-22 Feb. 2017

Kang, J., Yu, R., Huang, X., & Zhang, Y. (2017). Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2627-2637.

Karafiloski, E., & Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017-17th International Conference on Smart Technologies* (pp. 763-768). IEEE.

Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). 6G wireless systems: A vision, architectural elements, and future directions. *IEEE access*, *8*, 147029-147044.

Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. A., Dang, T. N., & Hong, C. S. (2020). Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet of Things Journal*, *7*(10), 10200-10232.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchainBlockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84.

Kravitz, D. W., & Cooper, J. (2017, June). Securing user identity and transactions symbiotically: IoT meets blockchainBlockchain. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Kravitz, D. W., & Cooper, J. (2017, June). Securing user identity and transactions symbiotically: IoT meets blockchainBlockchain. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *Ieee Software*, *35*(4), 95-99.

Kumar, N., & Khanna, R. (2020). A compact multi-band multi-input multi-output antenna for 4G/5G and IoT devices using theory of characteristic modes. *International Journal of RF and Microwave Computer-Aided Engineering*, *30*(1), e22012.

Lee, B., & Lee, J. H. (2017). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *The Journal of Supercomputing*, *73*(3), 1152-1167.

Lewis, A. (2016). A gentle introduction to smart contracts. *Retrievd from https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts*.

Li, S., Yu, M., Yang, C. S., Avestimehr, A. S., Kannan, S., & Viswanath, P. (2020). Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously. *IEEE Transactions on Information Forensics and Security*, *16*, 249-261.

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2017). Consortium blockchainBlockchain for secure energy trading in industrial internet of things. *IEEE transactions on industrial informatics*, *14*(8), 3690-3700.

Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST* (pp. 1-10). Gaithersburg, MD, USA: NIST.

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain based data integrity service framework for IoT data. In *2017 IEEE International Conference on Web Services (ICWS)* (pp. 468-475). IEEE.

Liu, C., Xiao, Y., Javangula, V., Hu, Q., Wang, S., & Cheng, X. (2018). Normachain: A blockchainBlockchain-based normalized autonomous transaction settlement system for iot-based e-commerce. *IEEE Internet of Things Journal*, *6*(3), 4680-4693.

Liu, J., Li, W., Karame, G. O., & Asokan, N. (2018). Toward fairness of cryptocurrency payments. *IEEE Security & Privacy*, *16*(3), 81-89.

Lukianov, D. (2015). Compact confidential transactions for Bitcoin.

Lundqvist, T., De Blanche, A., & Andersson, H. R. H. (2017, June). Thing-to-thing electricity micro payments using blockchainBlockchain technology. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Ma, H., Huang, E. X., & Lam, K. Y. (2020). Blockchain-based mechanism for fine-grained authorization in data crowdsourcing. *Future Generation Computer Systems*, *106*, 121-134.

Maxwell, G. (2013). CoinSwap: Transaction graph disjoint trustless trading. *CoinSwap: Transactiongraphdisjointtrustlesstrading (October 2013)*.

Maxwell, G. (2013, August). CoinJoin: Bitcoin privacy for the real world. In *Post on Bitcoin forum*.

Meiklejohn, S., & Orlandi, C. (2015, January). Privacy-enhancing overlays in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 127-141). Springer, Berlin, Heidelberg.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140). ACM.

Mendis, G. J., Wu, Y., Wei, J., Sabounchi, M., & Roche, R. (2020). A blockchainBlockchain-powered decentralized and secure computing paradigm. *IEEE Transactions on Emerging Topics in Computing*.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy* (pp. 397-411). IEEE.

Miyake, S., & Bandai, M. (2013, March). Energy-efficient mobile p2p communications based on context awareness. In *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 918-923). IEEE.

Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, *102*, 1027-1037.

Morabito, V. (2017). Smart contracts and licensing. In *Business Innovation Through Blockchain* (pp. 101-124). Springer, Cham.

Musleh, A. S., Yao, G., & Muyeen, S. M. (2019). Blockchain applications in smart grid–review and frameworks. *Ieee Access*, *7*, 86746-86757.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.

Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*.

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184-1195.

Orenge, A. O. (2018). Blockchain-based Provenance Solution for Handcrafted Jewellery.

Osgood, R. (2016). The future of democracy: Blockchain voting. *COMP116: Information security*, 1-21.

Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. FairAcces: a new blockchainBlockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. 9 (18), 5943–5964 (2016).

Pérez-Expósito, J. P., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2017). VineSens: An eco-smart decision-support viticulture system. *Sensors*, *17*(3), 465.

Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

Preden, J. S., Tammemäe, K., Jantsch, A., Leier, M., Riid, A., & Calis, E. (2015). The benefits of self-awareness and attention in fog and mist computing. *Computer*, *48*(7), 37-45.

Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management: An International Journal*.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchainBlockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchainBlockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchainBlockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014, September). Coinshuffle: Practical decentralized coin mixing for bitcoin. In *European Symposium on Research in Computer Security* (pp. 345-364). Springer, Cham.

Rutkin, A. (2016). Blockchain-based microgrid gives power to consumers in New York. *New Scientist*, *2*.

Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access*, *7*, 73295-73305.

Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., Sallabi, F. “Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare” in Computer, vol. 50, no. 7, July 2017, pp. 74-79

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE.

Saxena, A., Misra, J., & Dhar, A. (2014, March). Increasing anonymity in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 122-139). Springer, Berlin, Heidelberg.

Shae, Z., & Tsai, J. J. (2017, June). On the design of a blockchainBlockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 1972-1980). IEEE.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). Towards blockchainBlockchain-based auditable storage and sharing of iot data. In *Proceedings of the 2017 on cloud computing security workshop* (pp. 45-50).

Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchainBlockchain technology. *IEEE Access*, *7*, 24477-24488.

Sharma, A., Alam, T., & Srivastava, D. (2008). Ad hoc network architecture based on mobile Ipv6 development. *Advances in Computer Vision and Information Technology*, *224*.

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650-655.

Shi, N., Tan, L., Yang, C., He, C., Xu, J., Lu, Y., & Xu, H. (2021). BacS: A blockchainBlockchain-based access control scheme in distributed internet of things. *Peer-to-peer networking and applications*, *14*(5), 2585-2599.

Singh, P., Kumar, P., & Alam, T. (2014). Generating different mobility scenarios in ad hoc networks. *International Journal of Electronics Communication and Computer Technology*, *4*(2), 582-591.

Song, J. C., Demir, M. A., Prevost, J. J., & Rad, P. (2018, June). Blockchain design for trusted decentralized IoT networks. In *2018 13th Annual Conference on System of Systems Engineering (SoSE)* (pp. 169-174). IEEE.

Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2018). Security and privacy of smart cities: a survey, research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(2), 1718-1743.

Stark, J. (2017). Making sense of blockchainBlockchain smart contracts, 2016. *Acesso em*, *13*.

Steger, M., Dorri, A., Kanhere, S. S., Römer, K., Jurdak, R., & Karner, M. (2018). Secure wireless automotive software updates using blockchainBlockchains: A proof of concept. In *Advanced Microsystems for Automotive Applications 2017* (pp. 137-149). Springer, Cham.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9).

Tian, F. (2016, June). An agri-food supply chain traceability system for China based on RFID & blockchainBlockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)* (pp. 1-6). IEEE.

Tu, W. (2018). Data-driven QoS and QoE management in smart cities: A tutorial study. *IEEE Communications Magazine*, *56*(12), 126-133.

Valenta, L., & Rowan, B. (2015, January). Blindcoin: Blinded, accountable mixes for bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 112-126). Springer, Berlin, Heidelberg.

Wan, S., Li, M., Liu, G., & Wang, C. (2020). Recent advances in consensus protocols for blockchainBlockchain: a survey. *Wireless networks*, *26*(8), 5579-5593.

Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. *Internet of Things*, *10*, 100081.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.

Wang, X., Xu, X., Feagan, L., Huang, S., Jiao, L., & Zhao, W. (2018, July). Inter-bank payment system on enterprise blockchainBlockchain platform. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 614-621). IEEE.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

Wu, J., Song, T., Yu, Y., Wang, C., & Hu, J. (2018). Generalized byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks. *IEEE Access*, *6*, 53272-53286.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019). A comprehensive survey of blockchainBlockchain: From theory to IoT applications and beyond. *IEEE Internet of Things Journal*, *6*(5), 8114-8154.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchainBlockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794-2830.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016, April). The blockchainBlockchain as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182-191). IEEE.

Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). A blockchainBlockchain-based reputation system for data credibility assessment in vehicular networks. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1-16.

Yassami, S., Drego, N., Sergeev, I., Julian, T., Harding, D., & Srinivasan, B. S. (2016). True micropayments with bitcoin.

Yuan, Y., & Wang, F. Y. (2016, November). Towards blockchainBlockchain-based intelligent transportation systems. In *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)* (pp. 2663-2668). IEEE.

Zhang, P., & Helvik, B. E. (2012, July). Towards green P2P: Analysis of energy consumption in P2P and approaches to control. In *2012 International Conference on High Performance Computing & Simulation (HPCS)* (pp. 336-342). IEEE.

Zhang, Y., & Wen, J. (2017). Peer-to-Peer Netw. In *Appl* (Vol. 10, p. 983).

Ziegeldorf, J. H., Grossmann, F., Henze, M., Inden, N., & Wehrle, K. (2015, March). Coinparty: Secure multi-party mixing of bitcoins. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (pp. 75-86). ACM.