ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Οι Τεχνολογίες (Blockchain) ως Συστατικό των Σύγχρονων Εφαρμογών Πληροφορικής

ΤΗΛΙΑΚΟΥ ΦΑΝΕΡΩΜΕΝΗ
Α.Μ. 141199

Εισηγητής: Δρ. ΚΑΡΚΑΖΗΣ ΠΑΝΑΓΙΩΤΗΣ, Αν. Καθηγητής

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Οι Τεχνολογίες (Blockchain) ως Συστατικό των Σύγχρονων Εφαρμογών Πληροφορικής

ΤΗΛΙΑΚΟΥ ΦΑΝΕΡΩΜΕΝΗ
Α.Μ. 141199

Εισηγητής:

Δρ. ΚΑΡΚΑΖΗΣ ΠΑΝΑΓΙΩΤΗΣ, Αν. Καθηγητής

Εξεταστική Επιτροπή:

Παναγιώτης Καρκαζής, Αν. Καθηγητής
Νικόλαος Μυριδάκης , Επ. Καθηγητής
Ελένη – Αικατερίνη Λελίγκου, Αν. Καθηγήτρια

Panagiotis Karkazis
Digitally signed by Panagiotis Karkazis
Date: 2023.03.14 16:16:50 +02'00'

Nikolaos Myridakis
Digitally signed by Nikolaos Myridakis
Date: 2023.03.15 10:16:15 +02'00'

Eleni Aikaterini Leligkou
Digitally signed by Eleni Aikaterini Leligkou
Date: 2023.03.15 11:15:53 +02'00'

Ημερομηνία εξέτασης 10/03/2023

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Τηλιακού Φανερωμένη του Μιχαήλ, με αριθμό μητρώου 141199 φοιτήτρια του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Η Δηλούσα

Τηλιακού Φανερωμένη

ΕΥΧΑΡΙΣΤΙΕΣ

Με την εκτέλεση της διπλωματικής μου εργασίας θα ήθελα να ευχαριστήσω τους γονείς μου για την αμέριστη συμπαράσταση και υποστήριξη τους σε όλα τα στάδια της ζωής μου. Ακόμα, θα ήθελα να ευχαριστήσω και τον επιβλέποντα καθηγητή μου, που με καθοδήγησε και μου έδωσε την ευκαιρία να ασχοληθώ με το θέμα των Τεχνολογιών (Blockchain) ως Συστατικό των Σύγχρονων Εφαρμογών Πληροφορικής.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Το Blockchain είναι μια σύγχρονη τεχνολογία που έχει φέρει επανάσταση στον τρόπο με τον οποίο η κοινωνία αλληλεπιδρά και συναλλάσσεται. Θα μπορούσε να οριστεί ως μια αλυσίδα μπλοκ που αποθηκεύει πληροφορίες με ψηφιακές υπογραφές σε ένα κατανεμημένο και αποκεντρωμένο δίκτυο. Αυτή η τεχνική υιοθετήθηκε για πρώτη φορά για τη δημιουργία ψηφιακών κρυπτονομισμάτων, όπως το Bitcoin και το Ethereum. Ωστόσο, η έρευνα και οι βιομηχανικές μελέτες επικεντρώθηκαν πρόσφατα στις ευκαιρίες που παρέχει το blockchain σε διάφορους άλλους τομείς εφαρμογών για να επωφεληθούν από τα κύρια χαρακτηριστικά αυτής της τεχνολογίας, όπως: αποκέντρωση, συνέπεια, ανωνυμία και δυνατότητα ελέγχου. Αυτή η διπλωματική εξετάζει τη χρήση του blockchain σε διάφορους ενδιαφέροντες τομείς, και συγκεκριμένα: οικονομία, υγεία, περίθαλψη, συστήματα πληροφοριών, ασύρματα δίκτυα, Διαδίκτυο των πραγμάτων, έξυπνα δίκτυα, κυβερνητικές υπηρεσίες , στρατός και εθνική άμυνα. Επιπλέον, περιγράφει το Corda και το Ripple και κάνει επίσης σύγκριση μεταξύ των δύο πλατφορμών.

ABSTRACT

Blockchain is a modern technology that has revolutionized the way society interacts and transacts. It could be defined as a blockchain that stores information with digital signatures in a distributed and decentralized network. This technique was first adopted to create digital cryptocurrencies such as Bitcoin and Ethereum. However, research and industrial studies have recently focused on the opportunities that blockchain provides to various other application areas to take advantage of the main features of this technology, such as: decentralization, persistence, anonymity and auditability. This paper examines the use of blockchain in several interesting areas, namely: economy, health, healthcare, information systems, wireless networks, Internet of Things, smart grids, government services, military and national defense. In addition, it describes Corda and Ripple and also makes a comparison between the two platforms.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Αρχιτεκτονική Ηλεκτρονικών Υπολογιστών
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: blockchain, εφαρμογές, Corda, Ripple

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

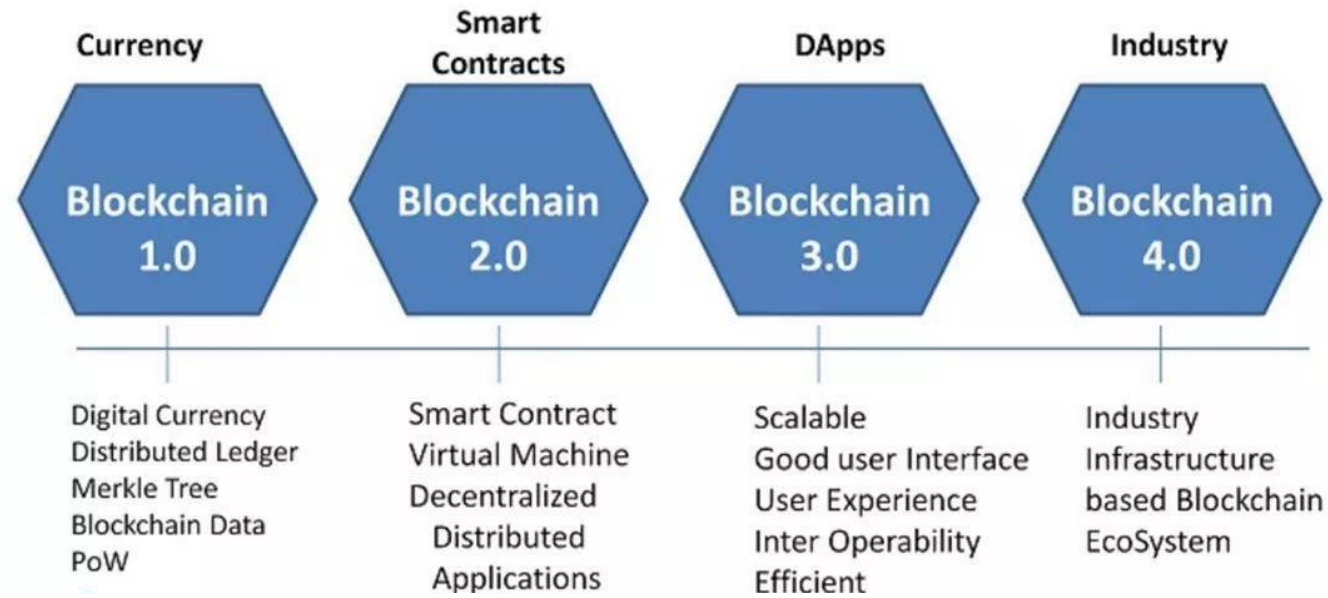
Σε αυτό το κεφάλαιο αναλύεται το αντικείμενο της διπλωματικής εργασίας και γίνεται μια ιστορική αναδρομή γύρω από τις μεθόδους που έχουν παρουσιαστεί σε αυτήν την περιοχή.

1.1 Περιγραφή του αντικειμένου της διπλωματικής εργασίας

Διαφορετικά είδη συμφωνιών, συμβάσεων και οικονομικών συναλλαγών διατηρούνται και καταγράφονται σε μια σταθερή δομή στα παραδοσιακά επιχειρηματικά, κοινωνικά και πολιτικά μας συστήματα. Μέρα με τη μέρα, λόγω της ψηφιακής μετάβασης και της ταχείας ανάπτυξης των τεχνολογιών του Διαδικτύου, προχωράμε προς έναν κόσμο όπου η διαφάνεια αποτελεί υποχρεωτική προσδοκία των τελικών χρηστών. Στη σημερινή ψηφιακή εποχή, είτε στην επιχείρηση είτε σε οποιαδήποτε άλλη επικοινωνία, οι συμμετέχοντες ενδιαφερόμενοι θέλουν να συναλλάσσονται χωρίς κανέναν μεσάζοντα και αναμένουν εμπιστοσύνη και αξιοπιστία μέσω του τεχνολογικού σχεδιασμού. Η τεχνολογία Blockchain έχει θεωρηθεί εξαιρετική τεχνολογία για την εκπλήρωση αυτών των στόχων. Αρχικά, χρησιμοποιήθηκε σε κρυπτονομίσματα όπως το Bitcoin και το Ethereum (Wood et al., 2014). Το Bitcoin εισήχθη από τον Satoshi Nakamoto το 2008 και έχει εκτιμηθεί ιδιαίτερα για την αποκεντρωμένη, peer-to-peer επικοινωνία.

1.2 Ιστορική αναδρομή

Η εμφάνιση του Blockchain είχε τεράστιο αντίκτυπο στις επιχειρήσεις και τις βιομηχανίες πληροφορικής. Τα τελευταία χρόνια, μεγάλες εταιρείες όπως η IBM(IBM Home Page, 2016) καταβάλλουν προσπάθειες για να παρέχουν πιο ισχυρές, αξιόπιστες και οικονομικά αποδοτικές πλατφόρμες για αυτήν. Η τεχνική βελτίωση στο Blockchain από το Blockchain 1.0 στο Blockchain 4.0 το έχει κάνει πιο κατάλληλο για βιομηχανικές εφαρμογές. Με το να είναι πιο επεκτάσιμη, προγραμματιζόμενη, με βελτιστοποιημένη δομή δεδομένων για μπλοκ και για συναλλαγές και με νέες μεθόδους συναίνεσης δημιουργεί μια τεράστια ζήτηση για Blockchain σε όλες τις εφαρμογές του πραγματικού κόσμου. Η **εικόνα 1** απεικονίζει την εξέλιξη της τεχνολογίας Blockchain.



Εικόνα 1.Εξέλιξη της τεχνολογίας Blockchain (IBAX Network).

ToBlockchain έχει ξεκινήσει από την 1η γενιά και πλέον βρισκόμαστε στην 4η, όπως φαίνεται και στην παραπάνω εικόνα.

- Η πρώτη γενιά της τεχνολογία **Blockchain 1.0** εστιάζει στα κρυπτονομίσματα και την αποκέντρωση. Η συγκεκριμένη τεχνολογία περιοριζόταν στην αποθήκευση και μεταφορά αξίας (π.χ. Bitcoin, Ripple, Dash). Όλα ξεκίνησαν με το κρυπτονόμισμα του Bitcoin το οποίο είναι και το ποιο διαδεδομένο. Όπως το Bitcoin έτσι και όλα τα υπόλοιπα νομίσματα αντίστοιχης τεχνολογίας χρησιμοποιούν την συγκεκριμένη γενιά . Η πρώτη εφαρμογή του Blockchain ήταν η καταγραφή οικονομικών συναλλαγών με Bitcoin .
- Η δεύτερη γενιά της τεχνολογία **Blockchain 2.0** είναι η εποχή των έξυπνων συμβολαίων που βοήθησαν το Blockchain να ξεπεράσει την αρχική του λειτουργικότητα για την τροφοδοσία κρυπτονομισμάτων. Τα έξυπνα συμβόλαια έδωσαν στους χρήστες μια διέξοδο να αυτοματοποιήσουν τις διοργανωτικές τους συμβάσεις. Καθώς τα αυτόνομα προγράμματα ηλεκτρονικών υπολογιστών ζουν στο Blockchain, τα έξυπνα συμβόλαια μπορούν να εκτελούνται αυτόματα όταν πληρούνται προκαθορισμένες προϋποθέσεις, εξαλείφοντας τον ρόλο των μεσαζόντων. Τα έξυπνα συμβόλαια έχουν αποκτήσει ευρέως διαδεδομένη

απήχηση επειδή είναι αδιαπραγμάτευτα και μειώνουν το κόστος επαλήθευσης, εξαίρεσης, διαιτησίας και προστασίας από απάτη, επιπλέον του ότι επιτρέπουν την αυτοματοποιημένη εκτέλεση χωρίς άδεια. Επίσης, τα έξυπνα συμβόλαια επιτρέπουν την διαφανή καταγραφή δεδομένων, η οποία είναι εύκολα επαληθεύσιμη και παρέχει στα εμπλεκόμενα μέρη ίση κυριαρχία στις συμφωνίες τους. Το πολύ δημοφιλές Ethereum και Cardano είναι ένα blockchain 2ης γενιάς. Για να τροφοδοτήσει τη λειτουργικότητα των έξυπνων συμβολαίων, το Ethereum είναι το βασικό εργαλείο Blockchain για εφαρμογές , ειδικά την αλυσίδα εφοδιασμού. Όπως και το Bitcoin, το Ethereum προσαρμόζει επίσης τη συναινετική μέθοδο Proof-of-Work, η οποία απαιτεί τη χρήση βαρέως εξοπλισμού εξόρυξης και τη δαπάνη σημαντικών πόρων.

- Η τρίτη γενιά της τεχνολογία **Blockchain 3.0** είναι οι εφαρμογές blockchain (DApps). Το blockchain τρίτης γενιάς επικεντρώνεται στην βελτίωση και διόρθωση των προηγούμενων γενιών. Έχει να κάνει με την άνοδο των αποκεντρωμένων εφαρμογών (DApps). Διευκολύνοντας διάφορους κλάδους όπως η υγειονομική περίθαλψη, η εκπαίδευση, η γεωργία, το ηλεκτρονικό εμπόριο και πολλοί άλλοι. Επικεντρώνεται σε τομείς όπως είναι η ταχύτητα, η ασφάλεια, η επεκτασιμότητα. Παραδείγματα αυτών των Blockchain είναι τα Hyperledger, R3 Corda και Ethereum , Quorum. (Androulaki et al., 2018 . Wood et al., 2014)
- Η τέταρτη γενιά της τεχνολογία **Blockchain 4.0** καταργεί σχεδόν όλους τους περιορισμούς που είχε το παλαιότερο τύπου Blockchain και υπόσχεται να αναβαθμίσει το Blockchain ως ένα επιχειρηματικό περιβάλλον. Οι προγραμματιστές και οι μηχανικοί αναζητούν τρόπους για να ενσωματώσουν τις δυνατότητες της σε διαφορετικούς κλάδους για να βελτιστοποιήσουν την απόδοσή τους. Η τεχνολογία αυτή έχει τη δυνατότητα να αλλάξει πλήρως τον τρόπο με τον οποίο οι εταιρείες χειρίζονται δεδομένα και άλλες ευαίσθητες πληροφορίες. Οι εφαρμογές των κατανεμημένων λογιστικών βιβλίων και των blockchain είναι ουσιαστικά απεριόριστες. Θα επιτρέψει στις επιχειρήσεις να μεταφέρουν ορισμένες ή όλες τις τρέχουσες δραστηριότητές τους σε ασφαλείς, αυτοκαταγραφόμενες εφαρμογές που βασίζονται σε αποκεντρωμένα, αξιόπιστα και κρυπτογραφημένα λογιστικά βιβλία. Πλέον το Blockchain πέρα από τα νομίσματα, τη χρηματοδότηση και τις χρηματοοικονομικές αγορές, εισέρχεται

και παρέχει λύσεις σε ένα μεγάλο μέρος του επιχειρηματικού κλάδου όπως είναι ο τομέας της υγείας, της κυβέρνησης, ο νομικός κλάδος, ο κλάδος της επιστήμης, του προγραμματισμού, το πολιτισμού, της τέχνης. κλπ. Κυρίως καταφέρνει για πρώτη φορά, να κάνει τα βασικά, εγγενή πλεονεκτήματα του blockchain πιο προσιτά.

Πολλές επιχειρήσεις άρχισαν να προσπαθούν να αναδιαμορφώσουν τα επιχειρηματικά τους μοντέλα για να επωφεληθούν από αυτή τη νέα τεχνολογία. Το Blockchain μπορεί να χρησιμοποιηθεί από τους τρεις τύπους περιβάλλοντος υλοποίησης (Michael et al., 2018):

1. Permissioned Blockchain (Vukolic´, 2017): Αυτό το περιβάλλον παρέχει ιδιόκτητα (γνωστά και ως ιδιωτικά ή κλειστά) δίκτυα που ορίζουν και αποφασίζουν τους συμμετέχοντες και τους ρόλους τους. Αυτό αναπτύσσεται ιδιαίτερα από τις βιομηχανίες για την ιδιωτική εμπορική τους χρήση.

2. Χωρίς άδεια ή δημόσιο Blockchain (Bozic et al., 2016): Πρόκειται για ένα περιβάλλον ανοιχτού κώδικα στο οποίο ο καθένας μπορεί να έχει πρόσβαση, να χρησιμοποιήσει και να συμμετέχει σε αυτό. Για παράδειγμα. Bitcoin blockchain.

3. Hybrid or Consortium Blockchain (Li et al., 2017): Προέρχεται από τους δύο κύριους τύπους blockchain που αναφέρθηκαν παραπάνω. Στο Consortium Blockchain ο έλεγχος των δεδομένων ανάγνωσης και εγγραφής εξαρτάται από τον αριθμό των συμμετεχόντων. Χρησιμοποιείται από ομάδες οργανισμών/εταιρειών, που συνεργάζονται μεταξύ τους σε ορισμένα έργα. Ως εκ τούτου, εργάζονται σε περιβάλλον περιορισμένης πρόσβασης για να αποκομίσουν τα οφέλη της τεχνολογίας.

Η σύγκριση αυτών των περιβαλλόντων Blockchain φαίνεται στον **Πίνακα 1**. Η σύγκριση δείχνει ότι ένα περιβάλλον χωρίς άδεια είναι εξαιρετικά επεκτάσιμο σε σύγκριση με το περιβάλλον με άδεια και το υβριδικό περιβάλλον. Στον τομέα της ασφάλειας προτείνεται ένα πιο ασφαλές επιτρεπόμενο περιβάλλον, που είναι λιγότερο ευάλωτο σε κάθε είδους επίθεση. Και τα τρία περιβάλλοντα είναι διαφανή. Ωστόσο, τα υβριδικά περιβάλλοντα είναι ταχύτερα σε απόδοση σε σύγκριση με αυτά που δεν έχουν άδεια. Σε αντίθεση με τα άλλα δύο, η ανωνυμία διατηρείται εξ ολοκλήρου από ένα περιβάλλον χωρίς άδεια. Σε ένα λιγότερο επιτρεπόμενο περιβάλλον, οποιοσδήποτε συμμετέχων κόμβος μπορεί να συμμετάσχει στη διαδικασία εξόρυξης (mining) και μπορεί να είναι miner, ενώ σε ένα επιτρεπόμενο και υβριδικό περιβάλλον, μόνο επιλεγμένοι κόμβοι μπορούν να συμμετέχουν στην εξόρυξη, που ονομάζονται επικυρωτές (Validators).

	Δημόσιο / Χωρίς άδεια	**Ιδιωτικό/Επιτρεπόμενο**	**Υβριδικό**
Διαχείριση	Δημόσιο	Ενιαίος Κόμβος	Σύνολο Κόμβων
Διακίνηση	Αργή	Γρήγορη	Γρήγορη
Αποκάλυψη ταυτότητας κόμβου	Όχι	Ναι	Ναι
Ενεργειακής απόδοσης	Όχι	Ναί	Ναί
Πρωτόκολλο	PoW, PoS, PoET		PBFT, PoA
Άδεια	Χωρίς άδεια		Με Άδεια
Παράδειγμα	Bitcoin, Ethereum, Ripple		Multichain, Hyperledger, Tendermint, Quorum
Δυνατότητα Επίθεσης	Πιο πιθανό	Λιγότερο Πιθανό	Πιθανό
Επικύρωση συναλλαγής	Οποιοσδήποτε κόμβος μπορεί να είναι Miner		Λίστα Εξουσιοδοτημένων Κόμβων (Validators)
Επεκτασιμότητα	Υψηλός	Χαμηλό/Μεσαίο	Χαμηλό/Μεσαίο
Υποδομή	Αποκεντρωμένη	Αποκεντρωμένη	Διανέμονται
Λογοκρισία/Κανονισμός	Οχι	Ναί	Ναί

Πίνακας 1. Τύποι Blockchain.

Η τεχνολογία Blockchain παρέχει διάφορα οφέλη όπως:

- Διαφάνεια: Οι συναλλαγές που αποθηκεύονται στο Blockchain είναι διαφανείς για όλους τους συμμετέχοντες χρήστες. Το Blockchain χρησιμοποιεί το κατανεμημένο καθολικό (Distributed Ledger Technology – DLT) το οποίο είναι ένα κοινό αντίγραφο του εγγράφου που τηρείται από μεμονωμένα μέρη και μπορεί να ενημερωθεί μόνο από τον μηχανισμό συναίνεσης, πράγμα που σημαίνει ότι τα αρχεία μπορούν να ενημερωθούν μόνο εάν συμφωνήσουν όλα τα νόμιμα μέρη.

- Ενισχυμένη ασφάλεια: Το Blockchain είναι από πολλές απόψεις πιο ασφαλές από άλλα συστήματα διαχείρισης αρχείων. Προστίθενται οι συναλλαγές μετά από συναίνεση από όλα τα επιτρεπόμενα μέρη. Μόλις όλοι συμφωνήσουν για τη συναλλαγή, αυτή κρυπτογραφείται και συνδέεται με ασφάλεια με το προηγούμενο μπλοκ. Ασφαλείς μηχανισμοί κατακερματισμού που συνδέονται με κάθε μπλοκ χρησιμοποιούνται για την ασφάλεια των μπλοκ που συγκρατούν τον αριθμό των συναλλαγών. Επομένως, είναι πρακτικά αδύνατον να μεταβληθεί ένα μπλοκ καθώς απαιτεί τροποποιήσεις και σε άλλα μπλοκ στην αλυσίδα.

- Βελτιωμένη ιχνηλασιμότητα: Η παρακολούθηση δεδομένων/διαδικασιών είναι εύκολη με το Blockchain. Οι συναλλαγές είναι ορατές σε όλα τα μέρη, γεγονός που οδηγεί σε υψηλή ιχνηλασιμότητα σε οποιαδήποτε λειτουργία. Παραδείγματος χάρι εάν η επιχείρηση

ασχολείται με την αλυσίδα εφοδιασμού, η παρακολούθηση του προϊόντος είναι εύκολη μέσω αυτής της τεχνολογίας.

- Γρήγορο και αποτελεσματικό: Σε ένα παραδοσιακό σύστημα, η γραφειοκρατία είναι χρονοβόρα, κουραστική και επιρρεπής σε ανθρώπινα λάθη. Με την αυτοματοποίησή του με το Blockchain, η διαδικασία γίνεται πιο γρήγορη και αποτελεσματική και λειτουργεί χωρίς καμία παρέμβαση τρίτων.

- Μείωση Κόστους: Για κάθε επιχείρηση, το κέρδος/οικονομική αποδοτικότητα είναι σημαντική. Με αυτήν την τεχνολογία, μετριάζεται και πολλές εξαλείφεται η ανάγκη για μεσάζοντες ή τρίτους και ως εκ τούτου, έχουμε μείωση του κόστους και γίνεται η επιχείρηση οικονομικά πιο αποδοτική.

Φυσικά εκτός από τα πλεονεκτήματα που απαριθμήσαμε, είναι σημαντικό να εντοπίσουμε και να επιστήσουμε την προσοχή μας και στις διάφορες ερευνητικές προκλήσεις και ζητήματα που παρουσιάζονται. Πολλές από αυτές τις προκλήσεις έχουν ήδη μελετηθεί και αντιμετωπιστεί στο Blockchain (Manoj and Krishnan, 2020. Saad et al., 2019. Lin and Liao, 2017. Sankar et al., 2017. De La Rosa et al., 2017. Aras και Kulkarni, 2017. Lu, 2018. Gao et al., 2018. Mingxiao et al., 2017). Ωστόσο, υπάρχουν ακόμα κάποιες ελάχιστες προκλήσεις και περιορισμοί που χρειάζονται περισσότερη έρευνα και μελέτη για να επιλυθούν. Σε αυτό το σημείο θα παρουσιάσουμε της τεχνολογίας Blockchain, συζητώντας τις βασικές έννοιες, τον αρχιτεκτονικό σχεδιασμό, τις περιπτώσεις χρήσης/εφαρμογές τελευταίας τεχνολογίας καθώς και τις ερευνητικές προκλήσεις. Στόχος μας, με αυτήν την ανάλυση, είναι να παρέχουμε μια καλύτερη κατανόηση των βασικών θεμελιωδών αρχών και σχεδιαστικών προκλήσεων της αρχιτεκτονικής και των πρωτοκόλλων του Blockchain για να μπορέσουμε να εντοπίσουμε σημαντικές ερευνητικές κατευθύνσεις σε αυτήν την ενδιαφέρουσα τεχνολογία.

ΚΕΦΑΛΑΙΟ 2

ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ BLOCKCHAIN

Αυτή η ενότητα παρουσιάζει μια γενική επισκόπηση του Blockchain, συμπεριλαμβανομένου του ορισμού, της αρχιτεκτονικής, των σχετικών τεχνολογιών και των εφαρμογών του.

Η κύρια ιδέα πίσω από το Blockchain δεν είναι καινούργια. Οι Stuart Haber και W. Scott Stornetta (Haber and Stornetta, 1990) το έτος 1991 εργάστηκαν σε μια κρυπτογραφικά ασφαλισμένη αλυσίδα μπλοκ για τη χρονοσφραγίδα του συστήματος εγγράφων όπου ήθελαν το σύστημα να είναι ανθεκτικό στις επιθέσεις (Haber and Stornetta, 1990). Για τον ίδιο λόγο, χρησιμοποίησαν κρυπτογραφική συνάρτηση κατακερματισμού και Merkle tree (Becker, 2008) για να αποθηκεύσουν την ασφαλή συλλογή πιστοποιημένων εγγράφων σε ένα μπλοκ. Ωστόσο, αυτή η τεχνολογία έγινε δημοφιλής και γνωστή αφού εισήχθη και χρησιμοποιήθηκε σε κρυπτονομίσματα όπως το Bitcoin, που εισήχθη από τον Nakamoto το 2008. Το Bitcoin εισήχθη ως το πρώτο σύστημα ηλεκτρονικών πληρωμών χωρίς παρέμβαση τρίτων με χρήση αποκεντρωμένης διανομής σεpeer-to-peerδίκτυα. Ο όρος «Μπλοκ» και «αλυσίδα» χρησιμοποιείται ξεχωριστά από τον Σατόσι Νακαμότο και αργότερα αυτοί οι όροι χρησιμοποιήθηκαν και συλλογικά. Ο όρος «Μπλοκ» υποδηλώνει τη συλλογή πληροφοριών συμπεριλαμβανομένων των συναλλαγών και άλλων σχετικών πληροφοριών και η «αλυσίδα» υποδηλώνει τη σύνδεση/σύνδεσμο μεταξύ αυτών των μπλοκ χρησιμοποιώντας κρυπτογραφικό κώδικα κατακερματισμού. Αυτά τα κρυπτογραφικά συνδεδεμένα μπλοκ έκαναν αυτήν την τεχνολογία πιο ασφαλή. Η ευρεία χρήση και η επιτυχία του Bitcoin παρακίνησε άλλες βιομηχανίες να το χρησιμοποιήσουν. Επίσημα, το Blockchain μπορεί να οριστεί ως :

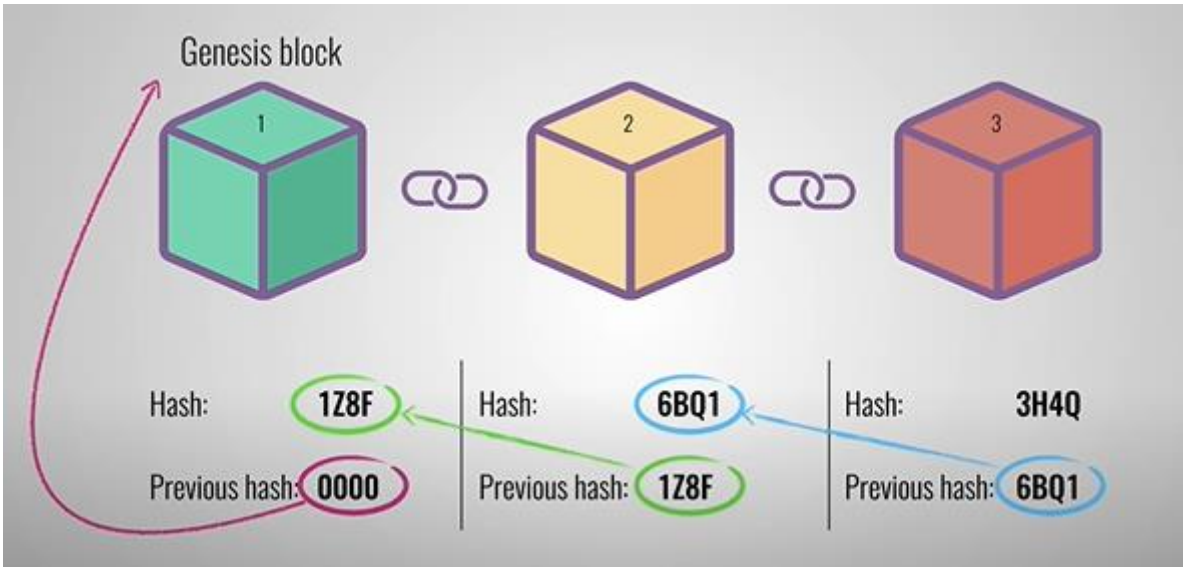
- Σύμφωνα με το NIST (Yaga et al., 2019), το Blockchain είναι κατανεμημένο ψηφιακό βιβλίο κρυπτογραφικά υπογεγραμμένων συναλλαγών που ομαδοποιούνται σε μπλοκ. Κάθε μπλοκ συνδέεται κρυπτογραφικά με το προηγούμενο μετά την επικύρωση και τη συναίνεση. Καθώς προστίθενται νέα μπλοκ, τα παλαιότερα μπλοκ γίνονται πιο δύσκολο να τροποποιηθούν (δημιουργώντας αντίσταση στην παραβίαση). Τα νέα μπλοκ αναπαράγονται σε αντίγραφα του καθολικού εντός του δικτύου και τυχόν διενέξεις επιλύονται αυτόματα χρησιμοποιώντας καθιερωμένους κανόνες.

- Ένα ανοιχτό κατανεμημένο βιβλίο που μπορεί να καταγράφει τις συναλλαγές μεταξύ δύο μερών αποτελεσματικά και με επαληθεύσιμο και μόνιμο τρόπο (Lakhani and Iansiti, 2017).
- Μια αποκεντρωμένη, κατανεμημένη και δημόσια ψηφιακή λογιστική που χρησιμοποιείται για την καταγραφή συναλλαγών σε πολλούς κόμβους για να καταστεί η εγγραφή και ο αποκλεισμός απαράβατος .
- Το Blockchain είναι μια εγγραφή που βασίζεται σε βάση δεδομένων συναλλαγών σε μια αμοιβαία κατανεμημένη κρυπτογραφική λογιστική που μοιράζεται μεταξύ όλων των κόμβων που συμμετέχουν σε ένα σύστημα (Mainelli and Smith, 2015).

Έτσι, το Blockchain, με απλά λόγια, είναι μια τεχνολογία που παρέχει προσβάσιμο και επαληθεύσιμο έλεγχο δεδομένων στο κατανεμημένο ή αποκεντρωμένο περιβάλλον σε κάθε συμμετέχοντα κόμβο με γρήγορο και βολικό τρόπο. Δεν υπάρχει ενιαία ή κεντρική αρχή για την επικύρωση/επαλήθευση των κόμβων. Αντίθετα, για να συμμετάσχει σε ένα δίκτυο, ένας κόμβος πρέπει να επικυρωθεί λύνοντας ένα μαθηματικό παζλ που ονομάζεται απόδειξη εργασίας (proof-of-work). Ένας κόμβος που πετυχαίνει μια απόδειξη εργασίας μπορεί να εισάγει ένα μπλοκ. Θα δούμε αναλυτικά το μπλοκ και το περιεχόμενό του στην επόμενη υποενότητα που ονομάζεται αρχιτεκτονική.

2.1. Αρχιτεκτονική

Το Blockchain είναι μια τεχνολογία όπου πολλά μέρη που εμπλέκονται και επικοινωνούν μπορούν να πραγματοποιήσουν διαφορετικές συναλλαγές χωρίς παρέμβαση τρίτων. Η επαλήθευση και η επικύρωση αυτών των συναλλαγών/επικοινωνιών πραγματοποιείται από ειδικά είδη κόμβων που ονομάζονται miners. Οι έγκυρες συναλλαγές περιλαμβάνονται στη δομή δεδομένων που ονομάζεται μπλοκ. Η εκτέλεση της τρέχουσας συναλλαγής εξαρτάται από τις προηγουμένως δεσμευμένες συναλλαγές. Με αυτόν τον τρόπο, αυτή η τεχνολογία είναι χρήσιμη για την αποφυγή/περιορισμό των διπλών δαπανών στο σύστημα κρυπτονομισμάτων. Η αρχιτεκτονική του Blockchain φαίνεται στην **Εικόνα 2** .

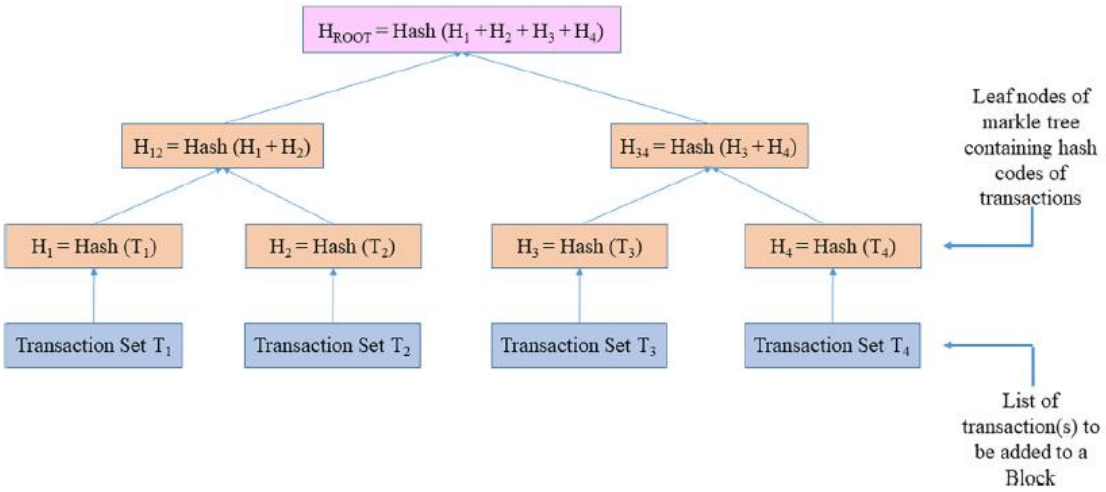


Εικόνα 2. Αρχιτεκτονική Blockchain(hhs.gov)

Μπορούμε να δούμε ότι η αλυσίδα των μπλοκ δημιουργείται από τον κατακερματισμό του προηγούμενου μπλοκ. Ένα μπλοκ χωρίζεται σε δύο συστατικά:

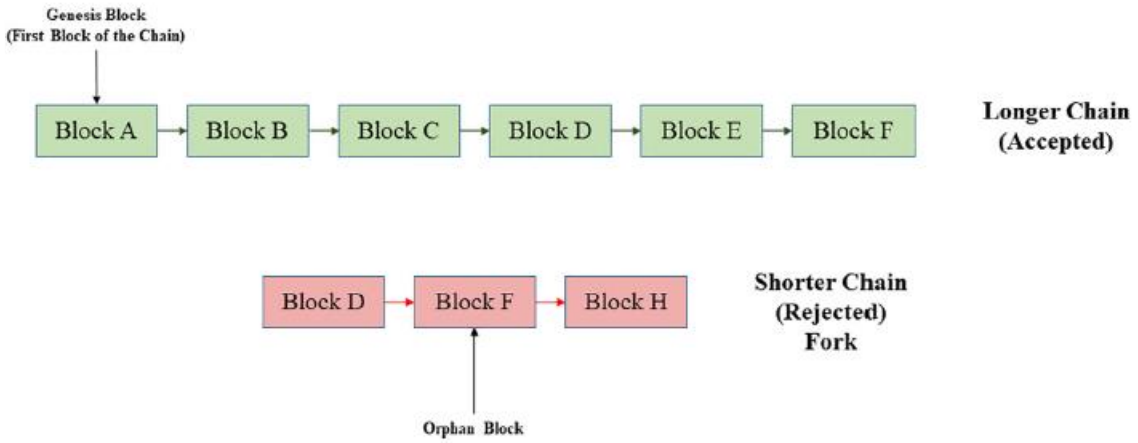
- Κεφαλίδα block
- Λίστα συναλλαγών

1. Η κεφαλίδα του μπλοκ αποτελείται από τρία στοιχεία. Το πρώτο στοιχείο είναι ο κατακερματισμός του προηγούμενου μπλοκ που συνδέει το τρέχον μπλοκ με το προηγούμενο. Το δεύτερο στοιχείο αποτελείται από στατιστικά στοιχεία εξόρυξης που χρησιμοποιούνται για τη δημιουργία του μπλοκ. Και το τελευταίο συστατικό είναι η ρίζα του δέντρου Merkle (που δεν είναι τίποτα άλλο από τον κατακερματισμό του τρέχοντος μπλοκ) που είναι η βάση για την επαλήθευση της ακεραιότητας όλων των συναλλαγών που βρίσκονται στο μπλοκ. Για να δημιουργήσουμε έναν κατακερματισμό του τρέχοντος μπλοκ, χρησιμοποιούμε τον κατακερματισμό του προηγούμενου μπλοκ. Επομένως, εάν ένας εισβολέας προσπαθήσει να τροποποιήσει τα περιεχόμενα του μπλοκ, πρέπει να τροποποιήσει όλο τον κωδικό κατακερματισμού της υπόλοιπης αλυσίδας, κάτι που είναι πρακτικά δύσκολο να πραγματοποιηθεί. Τα στατιστικά στοιχεία εξόρυξης περιλαμβάνουν τα nonce, timestamp (που είναι καταγεγραμμένος χρόνος) και δυσκολία εξόρυξης (Economist, 2015). Το δέντρο Merkle περιλαμβάνει την αλυσίδα κατακερματισμού μπλοκ δεδομένων όπου οι συναλλαγές κατακερματίζονται και συνδέονται με κόμβους φύλλων και ο μη φύλλο κόμβος περιλαμβάνει τον κρυπτογραφικό κατακερματισμό των θυγατρικών κόμβων του δέντρου Merkle. Η **Εικόνα 3** δείχνει το δέντρο Merkle Tree.



Εικόνα 3. Merkle tree (Shrimali& Patel, 2021).

2. Το δεύτερο στοιχείο του μπλοκ είναι μια λίστα έγκυρων συναλλαγών. Ο αριθμός των συναλλαγών σε ένα μπλοκ εξαρτάται από το μπλοκ και το μέγεθος της συναλλαγής. Η εξουσιοδότηση και η πιστοποίηση των συναλλαγών γίνονται με ασύμμετρη κρυπτογραφία. Μόλις μια συναλλαγή συμπεριληφθεί στην αλυσίδα, δεν μπορεί να αφαιρεθεί ή να τροποποιηθεί. Τα μπλοκ συνδέονται μεταξύ τους, όπου κάθε μπλοκ περιλαμβάνει έναν κατακερματισμό του προηγούμενου μπλοκ και δημιουργείται μια αλυσίδα μπλοκ (Blockchain). Το μπλοκ θα γίνει αποδεκτό στην αλυσίδα εάν είναι έγκυρο και έχει απόδειξη εργασίας, το οποίο είναι ένας υπολογιστικά δύσκολος κατακερματισμός που δημιουργείται από τη διαδικασία εξόρυξης. Καθώς διαθέτει μια ασφαλή τεχνική κατακερματισμού (π.χ. SHA-256) με ασφαλείς δείκτες κατακερματισμού που δείχνουν προς τον προηγούμενο κατακερματισμό, διασφαλίζει ότι, εάν τροποποιηθεί κάποιο από τα μπλοκ, όλα τα επόμενα μπλοκ θα πρέπει να υπολογιστούν εκ νέου. Ακολουθούν ορισμένες ταξινομήσεις που σχετίζονται με το block και το Blockchain. Η **εικόνα 4** απεικονίζει πώς γίνεται αποδεκτή η μεγαλύτερη αλυσίδα και προστίθεται στο Blockchain και άλλες μικρότερες αλυσίδες απορρίπτονται.



Εικόνα 4. Αποδοχή/ Απόρριψη αλυσίδας (Shrimali&Patel, 2021).

Ειδικές Περιπτώσεις μπλοκ:

-Ορφανό μπλοκ: Οι miners προσπαθούν να εξορύξουν μπλοκ μόνοι τους με τη λίστα των συναλλαγών που δεν έχουν ακόμη προστεθεί. Μόλις εξορυχθεί ένα μπλοκ από έναν miner, μεταδίδεται σε όλους τους άλλους κόμβους του δικτύου για επαληθεύσεις. Από τόσα πολλά μπλοκ στο δίκτυο, το μπλοκ με την υψηλότερη συναίνεση θα γίνει αποδεκτό να προστεθεί στο δίκτυο. Άλλα μπλοκ θεωρούνται ως ορφανά μπλοκ και απορρίπτονται αργότερα από το δίκτυο. Τα ορφανά μπλοκ έχουν ορισμένες συναλλαγές που έχουν ήδη συμπεριληφθεί στο έγκυρο μπλοκ που μόλις προστέθηκε, αλλά μπορεί να έχουν ορισμένες συναλλαγές που δεν έχουν ακόμη ληφθεί υπόψη. Τέτοιες συναλλαγές πρέπει να ληφθούν υπόψη σε περαιτέρω διαδικασίες εξόρυξης.

-Fork: Όλη η αλυσίδα εκτός από το έγκυρο block λέγεται fork. Ένα fork συμβαίνει κάθε φορά που μια κοινότητα κάνει μια αλλαγή στο πρωτόκολλο του blockchain ή σε ένα βασικό σύνολο κανόνων. Όταν συμβεί αυτό, η αλυσίδα χωρίζεται – παράγοντας ένα δεύτερο blockchain που μοιράζεται όλη την ιστορία του με το πρωτότυπο, αλλά κατευθύνεται προς μια νέα κατεύθυνση περιέχοντας τις αλλαγές. Μερικές φορές ένα μπλοκ που έχει εξορυχθεί πρόσφατα συνδέεται με την ορφανή αλυσίδα και ως εκ τούτου δεν γίνεται μέρος της μεγαλύτερης αλυσίδας. Τέτοια συνδεδεμένα μπλοκ δημιουργούν ένα fork.

-Genesis block: Είναι το όνομα που δίνεται στο πρώτο μπλοκ ενός κρυπτονομίσματος. Στην περίπτωση του δικτύου Bitcoin, το Genesis Block είναι το πρώτο μπλοκ που έχει εξορυχθεί ποτέ από τον δημιουργό Satoshi Nakamoto. Το Genesis Block μπορεί επίσης να ονομαστεί μπλοκ 0 οποιουδήποτε συστήματος Blockchain. Είναι δηλαδή το θεμέλιο το οποίο θα ακολουθήσει κάθε άλλο μπλοκ στην αλυσίδα

2.2. State-of-the-art

Σε αυτή την ενότητα, παρουσιάζουμε τις σύγχρονες υλοποιήσεις του Blockchain. Αρχικά συζητάμε τις βασικές τεχνολογίες που χρησιμοποιούνται επί του παρόντος για το Blockchain. Στη συνέχεια, ερευνούμε τις δημοφιλείς περιπτώσεις και εφαρμογές χρήσης Blockchain.

2.2.1. Σχετικές βασικές τεχνολογίες

Ακολουθούν μερικές από τις υποκείμενες τεχνολογίες Blockchain, καθεμία από τις οποίες μοιράζεται ορισμένες πτυχές με το Blockchain:

- Τεχνολογία Κατανεμημένου καθολικού (Distributed ledger technology - DLT): Το καθολικό έχει πρωταγωνιστικό ρόλο στο εμπόριο για την καταγραφή πληροφοριών όπως η αποτίμηση, η ιχνηλασιμότητα των ακινήτων, οι χρηματοοικονομικές συναλλαγές κ.λπ. Στην παραδοσιακή προσέγγιση επίσης, τα καθολικά ήταν πολύ σημαντικά. Λόγω της ευρείας χρήσης των υπολογιστών και της ψηφιοποίησης, τα λογιστικά βιβλία έχουν μετατοπιστεί από τα έντυπα σε ψηφιακές μορφές. Σε ένα απλό μηχανογραφικό σύστημα επίσης, τα λογιστικά βιβλία έχουν επικυρωθεί και διατηρηθεί από τρίτους. Η κατανεμημένη προσέγγιση δίνει αυτή τη δυνατότητα. Ο έλεγχος του καθολικού για τροποποίηση ή δημιουργία ορίζεται από την αμοιβαία συμφωνία που ονομάζεται συναίνεση. Αυτό θα καθορίσει ποιος μπορεί να κάνει τι στο κοινόχρηστο καθολικό.
- Έξυπνο συμβόλαιο (Smart Contract): Το έξυπνο συμβόλαιο αντιμετωπίζεται ως ένας αλγόριθμος υπολογιστή που επιτρέπει την αμοιβαία κατανόηση με τη μορφή συμφωνίας μεταξύ πολλών ενδιαφερόμενων μερών χωρίς την παρέμβαση οποιουδήποτε από τα εμπλεκόμενα μέρη ή τρίτου μέρους. Είναι μια σύμβαση στην οποία οι όροι της συμφωνίας μεταξύ αγοραστή και πωλητή είναι γραμμένοι στη γραμμή κώδικα που εκτελείται σύμφωνα με προκαθορισμένες απαιτήσεις. Με απλά λόγια, το έξυπνο συμβόλαιο είναι μια αυτό-εκτελέσιμη γραμμή κώδικα που εφαρμόζεται/συντηρείται/ρυθμίζεται με όρους και συμφωνίες που συνάπτονται μεταξύ δύο ή περισσότερων μερών. Τα κατανεμημένα καθολικά εφαρμόζονται και εκτελούνται μέσω έξυπνων συμβολαίων. Η τεχνολογία Blockchain βασίζεται σε έξυπνα συμβόλαια για την εφαρμογή της επιχειρηματικής λογικής στο κοινό καθολικό.
- Τεχνικές κρυπτογράφησης: Η ασφάλεια αποτελεί πρωταρχικό μέλημα σχεδόν σε κάθε εφαρμογή που εκτελείται στο Διαδίκτυο. Ακολουθούν οι δύο κύριες ανησυχίες για την ασφάλεια στο Blockchain.

1. Έλεγχος ταυτότητας και επικύρωση συναλλαγών από χρήστες.
2. Προστασία από παραβιάσεις χρησιμοποιώντας τεχνολογία Blockchain

Και για τα δύο, χρησιμοποιεί διαφορετικές κρυπτογραφικές τεχνικές. Για το 1, χρησιμοποιεί μια ψηφιακή υπογραφή χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού για έλεγχο ταυτότητας και για να αποτρέψει τη μη απόρριψη. Κανονικά, χρησιμοποιείται ένας αλγόριθμος κρυπτογράφησης ασύμμετρου κλειδιού, όπως ο RSA. Συγκεκριμένα, το Bitcoin χρησιμοποιεί τον αλγόριθμο ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA). Για να δημιουργήσει μια αμετάβλητη αλυσίδα μπλοκ, χρησιμοποιεί έναν ασφαλή αλγόριθμο κατακερματισμού (SHA) που δημιουργεί αποτελεσματικά υπολογιστικά επαληθεύσιμο κώδικα κατακερματισμού. Όπως περιεγράφηκε προηγουμένως, τα μπλοκ περιέχουν δύο μέρη, την κεφαλίδα μπλοκ και τις συναλλαγές. Η κεφαλίδα μπλοκ περιέχει έναν δείκτη κατακερματισμού που δείχνει στον κατακερματισμό του προηγούμενου μπλοκ. Η αλλαγή/μετριασμός σε ένα μπλοκ πρέπει να αντικατοπτρίζεται σε όλα τα μπλοκ και έτσι το Blockchain γίνεται ανθεκτικό. Συνοπτικά, το Blockchain αξιοποιεί την τεχνολογία κατανεμημένης λογιστικής για να επιτύχει την επιτυχή εκτέλεση έξυπνων συμβολαίων χρησιμοποιώντας ασφαλείς κρυπτογραφικές μεθόδους. Η χρήση αυτών των τεχνολογιών προσφέρει μοναδικά οφέλη και επιβάλλει ξεχωριστές προκλήσεις για την κάλυψη των απαιτήσεών της. Η εφαρμογή ασφαλών κατανεμημένων λογιστικών βιβλίων με ενσωματωμένα έξυπνα συμβόλαια θα μετατραπεί σε πολλές αποτελεσματικές εφαρμογές blockchain.

2.2.2. Μελέτες περίπτωσης

Μετά την εμφάνιση και τη δημοτικότητα του Bitcoin, οι χρήστες ήθελαν να μπορούν να χρησιμοποιήσουν την τεχνολογία Blockchain για τη δημιουργία κατανεμημένων και ασφαλών συστημάτων για αποθέματα (Palamara, 2018), κατασκευαστικές εργασίες (Polkowski et al., 2018), αλυσίδα εφοδιασμού (Osei et al., 2018), IoT, μείωση κόστους (Zhou et al., 2018), και πολλά άλλα. Αφού συζητήσαμε προηγουμένως για το Blockchain χωρίς άδεια και με άδεια, σε αυτήν την υποενότητα, θα συζητήσουμε διαφορετικές εφαρμογές και περιπτώσεις χρήσης δημόσιου/χωρίς άδεια Blockchain έναντι του ιδιωτικού/επιτρεπόμενου Blockchain.

- Public/Blockchain χωρίς άδεια: Είναι ένα ανοιχτό περιβάλλον του Blockchain όπου οποιοσδήποτε μπορεί να εγγραφεί, να συμμετάσχει και να αποχωρήσει από το δίκτυο χωρίς άδεια. Οι αλγόριθμοι συναίνεσης που βασίζονται σε δημόσια πρωτόκολλα Blockchain είναι

ανοιχτού κώδικα και χωρίς άδεια. Λίγα παραδείγματα δημόσιου Blockchain είναι τα Bitcoin (Nakamoto, 2008), Ethereum (Wood et al., 2014), Monero (Logo and van Saberhagen, 2014), Dash (Duffield και Diaz, 2015), Litecoin (Gibbs and Yordchim, 2014), Dodgecoin (Dinh et al., 2018) και άλλα. Πολύ δημοφιλείς εφαρμογές και περιπτώσεις χρήσης του Blockchain σε αυτήν την κατηγορία είναι το Bitcoin και το Ethereum. Εδώ, τα συζητάμε μαζί με μερικά ακόμη κρυπτονομίσματα όπως το Litecoin, το BitcoinCash, το Cardano και το Polkadot εν συντομία.

- Bitcoin: Είναι ένα αποκεντρωμένο ψηφιακό νόμισμα που βασίζεται σε Blockchain που επιτρέπει άμεσες πληρωμές σε οποιονδήποτε, οποτεδήποτε και οπουδήποτε στον κόσμο (Αρχική σελίδα, 2019c). Αυτό είναι ένα σύστημα μεταφοράς νομισμάτων peer-to-peer όπου το bitcoin δημιουργείται κατά τη διαδικασία εξόρυξης κάθε φορά που οι miners εξορύσσουν το νέο μπλοκ. Ο αριθμός των bitcoin που δημιουργούνται ανά μπλοκ έχει ρυθμιστεί να μειώνεται σταδιακά, με μείωση 50% για κάθε 210.000 μπλοκ, ή περίπου 4 χρόνια για τη διαχείριση του πληθωρισμού. Έτσι, οι ανταμοιβές των minersμειώνονται όσο προχωρά ο χρόνος. Έτσι, το δίκτυο Bitcoin, για να διατηρήσει το έπαθλο ανταμοιβής και το ενδιαφέρον των miners, αυξάνει το τέλος συναλλαγής. Χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού για τη δημιουργία και την επαλήθευση της ψηφιακής υπογραφής. Το Bitcoin δεν απαιτεί λογαριασμό ή διεύθυνση email για να συνδεθείτε στο πορτοφόλι Bitcoin. Μόνο η διεύθυνση bitcoin χρησιμοποιείται για συναλλαγές και ως εκ τούτου, ο χρήστης παραμένει ανώνυμος. Χρησιμοποιεί γλώσσα παρόμοια με το FORTH ως σενάριο Bitcoin (Sandip Chakraborty, 2018). Για την επικύρωση της συναλλαγής. Ο αλγόριθμος συναίνεσης που χρησιμοποιείται για το δίκτυο bitcoin είναι η Απόδειξη Εργασίας (PoW). Αναλύεται λεπτομερώς στην επόμενη ενότητα.

- Ethereum: Το Ethereum είναι μια άλλη δημοφιλής πλατφόρμα Blockchain. Στην πραγματικότητα διευκολύνει τους προγραμματιστές να δημιουργήσουν και να αναπτύξουν αποκεντρωμένες εφαρμογές. Χρησιμοποιεί το Ether ως αποκεντρωμένο ψηφιακό νόμισμα, γνωστό και ως ETH. Το Ether δεν χρησιμεύει μόνο ως κρυπτονόμισμα, αλλά επίσης επιτρέπει στο δίκτυο Ethereum την πληρωμή τελών συναλλαγών και τη διεκπεραίωση διαφόρων υπολογιστικών υπηρεσιών. Μια αποκεντρωμένη εφαρμογή (ή Dapp) εξυπηρετεί έναν συγκεκριμένο σκοπό στους χρήστες της. Για παράδειγμα, το Bitcoin είναι ένα Dapp που παρέχει στους χρήστες του ένα σύστημα ηλεκτρονικής μεταφοράς χρημάτων peer-to-peer που επιτρέπει διαδικτυακές πληρωμές Bitcoin. Καθώς είναι αποκεντρωμένο, το δίκτυο δεν ελέγχεται από κανένα άτομο ή κεντρική οντότητα. Οποιεσδήποτε κεντρικές υπηρεσίες μπορούν να αποκεντρωθούν χρησιμοποιώντας το Ethereum. Το Ethereum χρησιμοποιείται

επίσης από οργανισμούς για τη δημιουργία Αποκεντρωμένων Αυτόνομων Οργανισμών (Decentralized Autonomous Organization -DAO) που δεν είναι παρά ένας πλήρως αυτόνομος, αποκεντρωμένος οργανισμός χωρίς κεντρικό ιδιοκτήτη. Χρησιμοποιεί έναν κώδικα προγραμματισμού, σε μια συλλογή έξυπνων συμβολαίων που υλοποιούνται στο Ethereum Blockchain. Αυτός ο κώδικας θα αντικαταστήσει τον κεντρικό έλεγχο και θα αλλάξει τους κανόνες και τη δομή ενός παραδοσιακού οργανισμού. Το Ethereum χρησιμοποιείται επίσης ως πλατφόρμα για την παρουσίαση άλλων κρυπτονομισμάτων. Λόγω του προτύπου διακριτικού ERC20 που ορίζεται από το Ίδρυμα Ethereum, άλλοι προγραμματιστές μπορούν να εκδώσουν τις δικές τους εκδόσεις αυτού του διακριτικού και να συγκεντρώσουν κεφάλαια με μια αρχική προσφορά νομισμάτων (Initial Coin Offering - ICO). Σε αυτήν τη στρατηγική συγκέντρωσης κεφαλαίων, οι εκδότες του κουπονιού ορίζουν ένα ποσό που θέλουν να συγκεντρώσουν, το προσφέρουν σε μια πώληση πλήθους και λαμβάνουν Ether ως αντάλλαγμα. Δισεκατομμύρια δολάρια έχουν συγκεντρωθεί από ICO στην πλατφόρμα Ethereum τα τελευταία δύο χρόνια και ένα από τα πιο πολύτιμα κρυπτονομίσματα στον κόσμο, το EOS, είναι ένα διακριτικό ERC20 .

- Litecoin: Το Litecoin (Bhosale and Mavale, 2018 είναι ένα νέο κρυπτονόμισμα με δυνατότητα γρήγορης συναλλαγής. Όπως υποδηλώνει το όνομα, το Litecoin είναι Lite στην επεξεργασία και μπορεί να εξορυχθεί σε επιτραπέζιο μηχάνημα με λιγότερη επεξεργαστική ισχύ. Εισήχθη από τον Charles Lee τον Οκτώβριο του 2011. Το Bitcoin χρησιμοποιεί τον κρυπτογραφικό αλγόριθμο hash SHA-256 όπου το Litecoin χρησιμοποιεί έναν νεότερο αλγόριθμο που ονομάζεται Scrypt. Περίπου 84 εκατομμύρια Litecoins κυκλοφορούν στην αγορά, ενώ 21 εκατομμύρια Bitcoin κυκλοφορούν στην αγορά. Ο χρόνος επεξεργασίας συναλλαγών Litecoin είναι περίπου 2,5 λεπτά σε σύγκριση με περίπου 10 λεπτά για αυτόν του Bitcoin (Bhosale and Mavale, 2018).

- Cardano: Το Cardano (Houben and Snyers, 2018) είναι ένα περιβάλλον Blockchain χωρίς άδεια. Οι ανταλλαγές συναλλάγματος σε αυτήν την πλατφόρμα απαιτούν ειδικό πορτοφόλι και διεπαφή, καθώς αντιμετωπίζουν πολλές συναλλαγές. Διευκολύνει το αποκεντρωμένο κρυπτονόμισμα ανοιχτού κώδικα που ονομάζεται Ada (Augusta Ada King - ADA). που μπορεί να χρησιμοποιηθεί για την αποστολή και λήψη ψηφιακών κεφαλαίων. Χρησιμοποιείται στην πλατφόρμα Cardano, όπως ακριβώς το νόμισμα «Ether» χρησιμοποιεί στην πλατφόρμα Ethereum. Το Cardano παρέχει επίσης ένα κατανεμημένο περιβάλλον για αποκεντρωμένες εφαρμογές και έξυπνα συμβόλαια όπως το Ethereum. Η Cardano ιδρύθηκε με όραμα να ενισχύσει την ασφάλεια, την επεκτασιμότητα και τη διαλειτουργικότητα με συμβατικά χρηματοοικονομικά συστήματα και κανονισμούς,

κατανοώντας, μαθαίνοντας και αναλύοντας το Bitcoin και το Ethereum (Investopedia, 2019a) .

- BitcoinCash: Είναι ένα κρυπτονόμισμα που εισήχθη τον Αύγουστο του 2017. Σε σύγκριση με το Bitcoin, το BitcoinCash αύξησε το μέγεθος των μπλοκ και επέτρεψε περισσότερες συναλλαγές για τη βελτίωση της επεκτασιμότητας .Όπως το Bitcoin, το BitcoinCash χρησιμοποιεί επίσης τον ίδιο μηχανισμό συναίνεσης, αλγόριθμο κατακερματισμού και άλλες τεχνικές λεπτομέρειες (Houben and Snyers, 2018).

- Polkadot: Είναι ένα ξεχωριστό κρυπτονόμισμα που χρησιμοποιεί τη μέθοδο proof-of-stake. Ο κύριος ρόλος του είναι να παρέχει διαλειτουργικότητα μεταξύ άλλων blockchain. Οι μηχανισμοί/πρωτόκολλά του έχουν σχεδιαστεί για να συνδέουν αδειοδοτημένες και χωρίς άδεια blockchains. Επιτρέπει σε παράλληλα Blockchain να συνεργάζεται με τα δικά του token για συγκεκριμένες εφαρμογές.

Στο Ethereum, οι προγραμματιστές μπορούν να δημιουργήσουν απλώς αποκεντρωμένες εφαρμογές με τα δικά τους μέτρα ασφαλείας, όπου το Polkadot, οι προγραμματιστές μπορούν να δημιουργήσουν το δικό τους blockchain με ενσωματωμένη εγκατάσταση ασφαλείας (Qasse et al., 2019).

- Private / Permissioned Blockchain: Είναι ένα στενό περιβάλλον του Blockchain όπου προκαθορισμένοι κόμβοι μπορούν να ενωθούν και να λειτουργήσουν σύμφωνα με την άδεια που έχει οριστεί για αυτούς. Πολλοί οργανισμοί μπορούν να συμμετέχουν και κάθε οργανισμός θα έχει διαφορετικά δικαιώματα. Τα δικαιώματα εγγραφής διατηρούνται κεντρικά σε έναν οργανισμό. Τα δικαιώματα ανάγνωσης μπορεί να είναι δημόσια ή να περιορίζονται σε αυθαίρετο επίπεδο. Οι ιδιωτικές αλυσίδες μπλοκ είναι ένας τρόπος αξιοποίησης της τεχνολογίας Blockchain, δημιουργώντας ομάδες και συμμετέχοντες που μπορούν να επαληθεύουν τις συναλλαγές εσωτερικά. Το λιανικό εμπόριο, οι ασφάλειες, οι προμήθειες και τα logistics, η υγειονομική περίθαλψη, η κυβέρνηση και οι δημόσιοι τομείς είναι τεράστιες περιπτώσεις εφαρμογής/χρήσης επιτρεπόμενου blockchain από βιομηχανίες.

Εδώ, θα συζητήσουμε δύο επιτυχημένες περιπτώσεις χρήσης του επιτρεπόμενου Blockchain.

1. Project Ubin (Ubin URL, 2019): Το Project Ubin είναι ένα έργο συνεργασίας της κυβέρνησης της Σιγκαπούρης με τομείς της βιομηχανίας για τη διερεύνηση της χρήσης του DLT (Ethereum) για εκκαθάριση και διακανονισμό πληρωμών και τίτλων. Το Ethereum έχει δείξει δυνατότητες να κάνει τις οικονομικές συναλλαγές και διαδικασίες πιο διαφανείς,

ισχυρές και με χαμηλότερο κόστος. Ο στόχος στο συγκεκριμένο project είναι η κοινή λειτουργία της Νομισματικής Αρχής της Σιγκαπούρης (Monetary Authority of Singapore - MAS) και της βιομηχανίας για την κατανόηση της τεχνολογίας και τη χρήση των πιθανών οφελών από την πρακτική εφαρμογή. Το έργο υλοποιείται σε δύο φάσεις:

(α) Φάση 1: Η πρώτη φάση προσδιόρισε ποια στοιχεία χρηματοδότησης πρέπει να συμπεριληφθούν και ποια όχι. Αποφάσισαν να ξεκινήσουν με διατραπεζικές πληρωμές χρησιμοποιώντας τεχνολογία Blockchain.

(b) Φάση 2: Στη δεύτερη φάση τονίζεται ο επανασχεδιασμός του ακαθάριστου διακανονισμού σε πραγματικό χρόνο (Real-Time Gross Settlement - RTGS) σε πολλαπλές πλατφόρμες DLT. Επίσης, εισάγονται επιτυχώς αποκεντρωμένες διατραπεζικές πληρωμές και διακανονισμοί με μηχανισμούς εξοικονόμησης ρευστότητας με τρεις διαφορετικές πλατφόρμες DLT (Quorum, Hyperledger Fabric και R3 Corda). Επιπλέον, εκπλήρωσε επίσης στόχους όπως Ψηφιοποίηση πληρωμών, Αποκεντρωμένη, Επεξεργασία, Ουρά Πληρωμής, Απόρρητο Συναλλαγών και Διακανονισμός. Το Project Ubin εστιάζει σε νέες μεθόδους για τη διεξαγωγή διασυνοριακών πληρωμών με χρήση ψηφιακού νομίσματος κεντρικής τράπεζας ως μελλοντική εργασία στην επόμενη φάση (Ubin URL, 2019).

2. We. Trade (We-trade Homepage, 2019): Είναι μια ψηφιακή πλατφόρμα για εμπορικές συναλλαγές που βασίζεται στην πλατφόρμα Blockchain της IBM χρησιμοποιώντας Hyperledger (Androulaki et al., 2018) που προσφέρει στους πελάτες των τραπεζών πρόσβαση σε μια απλή χρήση με διεπαφή, αξιοποιώντας το καινοτόμο Έξυπνο Συμβόλαιο και ανοίγοντας πιθανές νέες ευκαιρίες συναλλαγών. Επιτρέπει ακριβείς πληροφορίες στάσης συναλλαγών, έλεγχο διακανονισμού, κάλυψη κινδύνου, επιλογές παρακολούθησης και ανίχνευσης. Η ανταλλαγή πληροφοριών σε σχεδόν πραγματικό χρόνο, η ψηφιοποίηση της χρηματοδότησης συναλλαγών και άλλων πολύπλοκων διαδικασιών, η συνεχής ετοιμότητα επιχειρηματικής δραστηριότητας και συμμόρφωσης, η επεκτασιμότητα και η ασφάλεια είναι τα οφέλη από την εφαρμογή συναλλαγών στο Blockchain.

2.2.3. Εφαρμογές

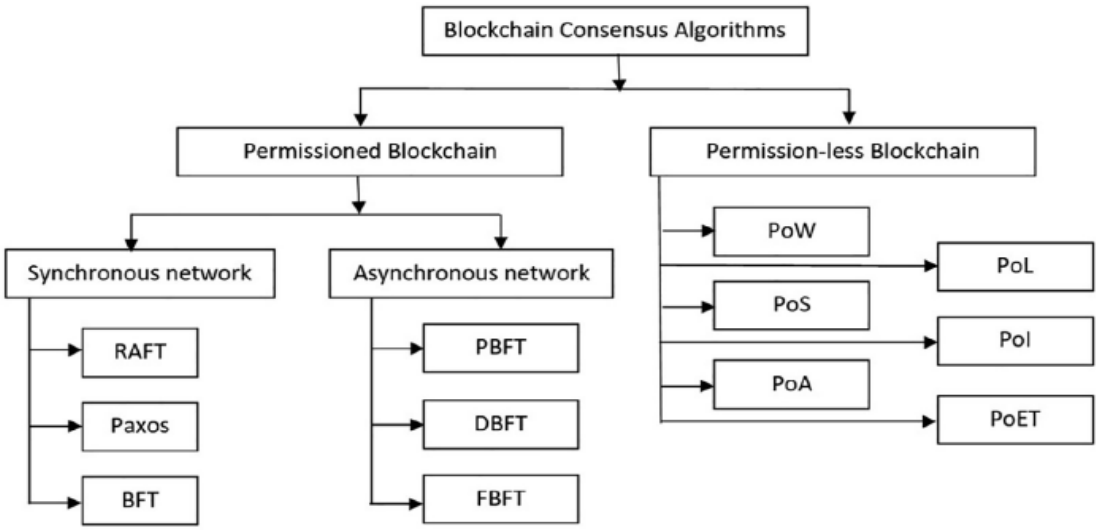
Το Blockchain αναδύεται ως μια νέα ευκαιρία για αυτόν τον ψηφιακό κόσμο. Υπάρχουν διάφορα πεδία όπου μπορεί να εφαρμοστεί. Αυτή η ενότητα καλύπτει τις δύο πολύ σημαντικές εφαρμογές του Blockchain στον πραγματικό κόσμο.

1. Blockchain με βιομηχανικό αυτοματισμό 5G: Το Διαδίκτυο των πραγμάτων (IoT) και το δίκτυο 5 γενεών (5G) είναι η ανάγκη αυτής της εποχής. Ιδιαίτερα όταν υπάρχει ποικιλία καταναλωτών και ποικιλία ψηφιακών εφαρμογών. Το IoT με δυνατότητα 5G (5G-IoT) θα συνδέσει τρισεκατομμύρια συσκευές IoT που επικοινωνούν μεταξύ τους σε πραγματικό χρόνο χωρίς παρεμβάσεις τρίτων που επιτρέπουν την ανάπτυξη μιας εφαρμογής με τεράστιο αριθμό συσκευών χωρίς να ανησυχείτε για την κυκλοφορία δικτύου ή ζητήματα που σχετίζονται με το δίκτυο. Ωστόσο, το περιβάλλον συσκευών IoT με δυνατότητα 5G υποφέρει από ζητήματα απορρήτου και ασφάλειας λόγω του ότι διαθέτει ένα κεντρικό σύστημα που είναι πιο ευάλωτο στους εισβολείς. Για να επιλυθεί αυτό, η ενσωμάτωση Blockchain εμφανίζεται ως μια πολλά υποσχόμενη τεχνολογία καθώς προσφέρει ένα ασφαλές, διαφανές, αξιόπιστο και ανθεκτικό περιβάλλον για IoT με δυνατότητα 5G λόγω της κατανεμημένης και peer-to-peer αρχιτεκτονικής του δικτύου (Surati et al. , 2021). Πολλοί ερευνητές (Liu et al., 2019; Zhang et al., 2019; Xiaoding et al., 2021; Jia et al., 2021; Wu et al., 2020). (Khujamatov et al., 2020; Srinivasu et al., 2021; Chamola et al., 2020; Wazid et al., 2020; Hewa et al., 2020) έχουν προτείνει και διεκδικούν τις μεθόδους για την ενοποίηση του Blockchain με το 5G industrial-IoT για τη βελτίωση της απόδοσης όσον αφορά την ασφάλεια, το απόρρητο, το αμετάβλητο και τη διαφάνεια.

2. Blockchain στην υγειονομική περίθαλψη 5G: Η υγειονομική περίθαλψη είναι ένας από τους σημαντικότερους κλάδους που επηρεάζει άμεσα τις ανθρώπινες ζωές. Το 5G φέρνει τόσες πολλές ευκαιρίες για τον κλάδο της ψηφιακής υγειονομικής περίθαλψης. Εξ αποστάσεως χειρουργικές επεμβάσεις, χειρουργικές επεμβάσεις και ιατρικές πρακτικές εξ αποστάσεως είναι δυνατές μέσω του 5G και τα ενδεχόμενα ζητήματα απορρήτου, ασφάλειας και αμετάβλητης μπορούν να επιλυθούν με την ενσωμάτωση του Blockchain. Πολλοί ερευνητές έχουν συζητήσει και προτείνουν τις δυνατότητες ενσωμάτωσης του Blockchain στην υγειονομική περίθαλψη 5G για την επίλυση ζητημάτων ασφάλειας, απορρήτου, αμετάβλητου και διαφάνειας.

2.3. Κατανεμημένη συναίνεση στο Blockchain

Το Blockchain είναι μια τυπική απεικόνιση της κατανεμημένης πληροφορικής στην οποία η αποκεντρωμένη συναίνεση είναι ένα πρωτόγονο ζήτημα, καθώς δεν υπάρχει κεντρική αρχή για την επίτευξη κοινής συμφωνίας. Διάφοροι αλγόριθμοι (όπως φαίνεται στην Ε**ικόνα 5**) έχουν προταθεί τις τελευταίες τρεις δεκαετίες για την αντιμετώπιση του ζητήματος της συναίνεσης με ποικίλες υποθέσεις. Με απλά λόγια, η συναίνεση αφορά πολλές οντότητες/μέλη/διακομιστές που συμφωνούν για την ίδια τιμή(ες).



Εικόνα 5. Ταξινόμηση Συναινετικών Αλγορίθμων(Shrimali&Patel, 2021)

Σύμφωνα με τη Wikipedia, η συναίνεση συνήθως αναφέρεται στη γενική συμφωνία μεταξύ των μελών μιας ομάδας ή κοινότητας. Η Wikipedia ορίζει την κοινή συμφωνία, τη συνεργασία, τη συνεργασία, τον εκδημοκρατισμό, τη συμπερίληψη και τη συμμετοχή ως βασικά στοιχεία για τη συναίνεση. Για εμάς, η συναίνεση στο Blockchain είναι βασικά μια απόφαση του παιχνιδιού εναρμόνισης μεταξύ πολλαπλών αναξιόπιστων οντοτήτων μέσω ενός μηχανισμού μετάδοσης μηνυμάτων για την επίτευξη αξιοπιστίας και ανοχής σφαλμάτων σε ένα σύστημα πολλαπλών πρακτόρων. Σε αντίθεση με την ψηφοφορία, όπου η πλειοψηφία εκλέγει έναν αρχηγό ο οποίος με τη σειρά του λαμβάνει αποφάσεις, η συναίνεση, από την άλλη πλευρά, είναι μια διαδικασία επίτευξης κοινής συμφωνίας (που προτείνεται από ένα μέλος μιας ομάδας μελών) που ισχύει για όλα τα μέλη στην επικοινωνία

.

Πολλοί από τους αλγόριθμους συναίνεσης λειτουργούν με βάση την απλή αρχή των συναλλαγών «συλλογή/επικύρωση/παραγγελία/καταγραφή/απόρριψη» και αποστολή των

συνεπών και επιβεβαιωμένων διακανονισμών (μετά τη διαδικασία εξόρυξης) στο κοινό κατανεμημένο δημόσιο βιβλίο, το οποίο είναι προσβάσιμο σε όλους ή στους εξουσιοδοτημένους φορείς. Η θεωρητική επίπτωση αυτών των αλγορίθμων τελευταίας τεχνολογίας είναι ένας τομέας όπου μπορεί να πραγματοποιηθεί πολλή δουλειά. Σε αυτή την ενότητα, στοχεύουμε να περιγράψουμε διάφορους αλγόριθμους συναίνεσης που χρησιμοποιούνται από διάφορες πλατφόρμες τεχνολογίας Blockchain.

Υπάρχουν διάφορες ιδιότητες (Watanabe et al., 2015) του κατανεμημένου αλγορίθμου συναίνεσης, δηλαδή: (i) τερματισμός - κάποια τιμή δημιουργείται ως αποτέλεσμα του μηχανισμού συναίνεσης από μια εξουσιοδοτημένη οντότητα (ii) εγκυρότητα - εάν η ίδια τιμή προτείνεται από όλες τις οντότητες, τότε οι εξουσιοδοτημένες οντότητες συμφωνούν σε αυτήν (iii) ακεραιότητα - κάθε εξουσιοδοτημένη οντότητα πρέπει να συμφωνήσει σε μια τιμή που έχει προταθεί προηγουμένως από κάποια εξουσιοδοτημένη οντότητα (iv) συμφωνία - κάθε εξουσιοδοτημένη οντότητα πρέπει να συμφωνήσει για την ίδια τιμή. Για να επιτευχθεί μια κοινή συμφωνία ή αξία, αυτά τα ακίνητα πρέπει να ικανοποιηθούν. Θα πρέπει να επιτυγχάνεται συναίνεση ακόμη και σε διάφορους τύπους σφαλμάτων στο κατανεμημένο σύστημα, όπως σφάλμα συντριβής, σφάλμα διαχωρισμού δικτύου ή βυζαντινά σφάλματα.

Όπως φαίνεται στην **Εικόνα 5** , οι αλγόριθμοι ταξινομούνται σε δύο μεγάλες κατηγορίες, δηλαδήBlockchainμε άδεια και Blockchain χωρίς άδεια. Τα περισσότερα από τα ψηφιακά νομίσματα που είναι διαθέσιμα στην αγορά λειτουργούν στην κατηγορία του Blockchain χωρίς άδεια, όπου ο καθένας μπορεί να γίνει μέρος της αλυσίδας χωρίς να απαιτείται έλεγχος ταυτότητας ή άλλο εμπόδιο. Οι χρήστες μπορούν απλώς να δημιουργήσουν τις προσωπικές τους διευθύνσεις και να αρχίσουν να αλληλεπιδρούν με το δίκτυο Blockchain χωρίς καμία λογοκρισία. Η αποκέντρωση, η ανωνυμία και η διαφάνεια είναι τα βασικά ζητήματα στο Blockchain χωρίς άδεια. Το Bitcoin είναι ένα παράδειγμα Blockchain χωρίς άδεια. Μερικά από τα πρωτόκολλα συναίνεσης στην κατηγορία του Blockchain χωρίς άδεια είναι :

1. Proof-of-Work (PoW)
2. Proof-of-Stake (PoS)
3. Proof-of-Activity (PoA)
4. Proof-of-Location (PoL)
5. Proof-of-Importance (PoI)
6. Proof-of-Elapsed-Time (PoET)

Το Permissioned blockchain, από την άλλη πλευρά, είναι ένα κλειστό ή ιδιωτικό δίκτυο στο οποίο οι χρήστες δεν επιτρέπεται να συμμετέχουν χωρίς άδεια/εξουσιοδότηση/λογοκρισία. Οι χρήστες αναμένεται να γνωρίζονται μεταξύ τους σε αυτήν την κατηγορία Blockchain. Το Permissioned Blockchain χρησιμοποιείται για οποιονδήποτε οργανισμό, όπως ιδιωτικές εταιρείες ή όμιλοι κοινοπραξιών, όπου ορισμένες έγκυρες οντότητες έχουν μόνο άδεια συμμετοχής. Σε αντίθεση με τους αλγόριθμους χωρίς άδεια, όπου οιminers πρέπει να χρησιμοποιούν ισχύ, χρόνο ή/και κρυπτονομίσματα, το εξουσιοδοτημένο Blockchain αποφεύγει τα γενικά έξοδα εξόρυξης (υπολογιστικών). Ωστόσο, η συναίνεση μεταξύ των χρηστών είναι μια πρόκληση που θα μπορούσε να αντιμετωπιστεί μέσω της έννοιας της αναπαραγωγής της κατάστασης μηχανής. Η κύρια πρόκληση για την επίτευξη της κατανεμημένης συναίνεσης στο επιτρεπόμενο Blockchain είναι ένα σφάλμα όπως σφάλμα συντριβής, σφάλμα δικτύου και βυζαντινό σφάλμα. Το Ripple(Gomez et al., 2019) είναι ένα παράδειγμα επιτρεπόμενου Blockchain. Η διαφορετική αποκέντρωση, η διαφάνεια, η ανωνυμία και η διακυβέρνηση είναι οι βασικές προκλήσεις στο επιτρεπόμενο Blockchain.
Λειτουργεί σε δύο σενάρια δικτύωσης, δηλαδή. σύγχρονο περιβάλλον και ασύγχρονο περιβάλλον. Στο σύγχρονο περιβάλλον, το σύστημα επικοινωνίας πρέπει να λειτουργεί κάτω από ένα κοινό ρολόι χρόνου με πεπερασμένη καθυστέρηση. Οι RAFT (Mingxiao et al., 2017), ο Paxos (Lamport et al., 2001) (Lamport et al., 2001) και η Byzantine Fault Tolerance (BFT) (Cachin and Vukolic´, 2017) είναι οι συναινετικοί μηχανισμοί που χρησιμοποιούνται στο επιτρεπόμενο Blockchain σε σύγχρονο περιβάλλον.
Σε ένα ασύγχρονο περιβάλλον, όπως το Διαδίκτυο, δεν υπάρχει όριο καθυστέρησης και ως εκ τούτου δεν θα πρέπει να υπάρχει περιορισμός χρόνου. Προφανώς, το τελευταίο είναι πιο περίπλοκο στη φύση, καθώς υπάρχουν πολλά διαφορετικά δυναμικά ζητήματα για λόγους όπως πχ. η ασφάλεια που θα συζητηθούν κατά τη συζήτηση για μεμονωμένους αλγόριθμους της κατηγορίας. Μερικά από τα πρωτόκολλα συναίνεσης που χρησιμοποιούνται στο επιτρεπόμενο Blockchain σε ασύγχρονο περιβάλλον:

1. Practical BFT (PBFT)
2. Delegated BFT(DBFT)
3. Federated Byzantine Fault Tolerance (FBFT)

Στην συνέχεια, αναλύουμε τους παραπάνω αλγόριθμους. Έχουμε κυρίως τρεις αλγόριθμους στην κατηγορία του επιτρεπόμενου Blockchain σε σενάριο σύγχρονου δικτύου, δηλαδή RAFT και Paxos που αντιμετωπίζουν τα σφάλματα δικτύου και BFT που είναι ο αλγόριθμος

Byzantine Fault Tolerance. Το Paxos εργάζεται πάνω σε μια απλή ιδέα να προτείνει μια πρόταση (που έχει μοναδικό αριθμό) από πολλούς προτείνοντες και αποδέκτες είτε αποδέχονται είτε απορρίπτουν την πρόταση με βάση τον αριθμό της. Ο μεγαλύτερος αριθμός πρότασης γίνεται αποδεκτός, ενώ οι άλλες προτάσεις με χαμηλότερο αριθμό απορρίπτονται. Ο προτείνων που συγκεντρώνει την πλειοψηφία των ψήφων εκλέγεται ως αρχηγός που θα λαμβάνει αποφάσεις εξ ονόματος της ομάδας. Το τελικό αποτέλεσμα κοινοποιείται σε όλους τους κόμβους του δικτύου μερικές φορές γνωστοί και ως μαθητές.

2.3.1. Επιτρεπόμενο Blockchain

Οι επιτρεπόμενοι μηχανισμοί συναίνεσης Blockchain χωρίζονται σε δύο μεγάλες κατηγορίες με βάση το περιβάλλον που λειτουργούν:

(i) Σύγχρονη

(ii) Ασύγχρονη

Προτού αρχίσουμε να κατανοούμε τα πρωτόκολλα στο σύγχρονο ή ασύγχρονο περιβάλλον, πρέπει να κατανοήσουμε την ιδέα του State Machine Replication (SMR) που είναι πολύ χρήσιμη για την επίτευξη συναίνεσης στην εξουσιοδοτημένη αλυσίδα μπλοκ. Το έξυπνο συμβόλαιο μπορεί να αναπαρασταθεί μέσω μιας μηχανής πεπερασμένης κατάστασης (FSM). Μια εφαρμογή crowdfunding είναι ένα ωραίο παράδειγμα σύμβασης που παρουσιάζεται μέσω του FSM. Αντί να εκτελείται το έξυπνο συμβόλαιο σε κάθε μηχανή/κόμβο του δικτύου, συνιστάται η εκτέλεση του σε ένα υπό σύνολο κόμβων και το δίκτυο διασφαλίζει ότι η ίδια κατάσταση μεταδίδεται σε άλλους κόμβους του δικτύου μέσω ενός ορισμένο μηχανισμό συναίνεσης. Μια τυπική μηχανή κατάστασης αποτελείται από ένα σύνολο καταστάσεων (ST) με κάθε κατάσταση να έχει ένα σύνολο εισόδων (IN), σύνολο εξόδων (OUT), συνάρτηση μετάβασης (STXIN ->ST), συνάρτηση εξόδου (STXOUT ->ST) και μια κατάσταση έναρξης (π.χ. ST1). Μέσω του κατανεμημένου SMR, οι μηχανές κατάστασης συγχρονίζονται σε πολλούς διακομιστές για να αποφευχθεί οποιαδήποτε πιθανή βλάβη.

(i) Περιβάλλον Σύγχρονου Δικτύου: Σε αυτήν την κατηγορία, υπάρχουν διαφορετικά πρωτόκολλα. Εδώ τα συζητάμε ένα προς ένα.

- PAXOS: Υπάρχουν διάφοροι τύποι σφαλμάτων στην κατανεμημένη συναίνεση. Σφάλμα συντριβής, σφάλματα δικτύου ή διαμερισμάτων και βυζαντινά σφάλματα. Τα βυζαντινά σφάλματα υποδιαιρούνται περαιτέρω σε κακόβουλους κόμβους συμπεριφοράς, σφάλματα υλικού και σφάλματα λογισμικού. Για τον χειρισμό σφαλμάτων συντριβής και δικτύου, χρησιμοποιούνται PAXOS και RAFT ενώ για την αντιμετώπιση σφαλμάτων που άπτονται

του βυζαντινού συστήματος (συμπεριλαμβανομένων σφαλμάτων σύγκρουσης και δικτύου), BFT και PBT χρησιμοποιούνται. Η ιδέα πίσω από τη λειτουργία των PAXOS είναι απλή. Από το σύνολο των κόμβων στο δίκτυο, ένας ή περισσότεροι κόμβοι προτείνουν μια τιμή (με τη μορφή της πρότασης με έναν μοναδικό και συνεχώς αυξανόμενο αριθμό) η οποία διαδίδεται σε ολόκληρο το δίκτυο. Αυτοί οι κόμβοι είναι γνωστοί ως proposers. Άλλοι κόμβοι (γνωστοί ως αποδέκτες) είτε αποδέχονται είτε απορρίπτουν την πρόταση με βάση τη σύγκριση του αριθμού που σχετίζεται με την τρέχουσα πρόταση με αυτόν της πρότασης που ελήφθη. Η τρίτη κατηγορία του κόμβου γνωρίζει ως εκπαιδευόμενος, μαθαίνει την τιμή που επιλέγουν οι αποδέκτες μέσω της αρχής της πλειοψηφίας.

- RAFT: Σχεδιασμένο κυρίως για να λειτουργεί ως εναλλακτική του PAXOS, μαζί με παράγοντες όπως η ανοχή σφαλμάτων και η απόδοση. Το RAFT εστιάζει κυρίως στην ιδέα του διαχωρισμού των κύριων προβλημάτων σε υποπροβλήματα και της αντιμετώπισης μεμονωμένων υποπροβλημάτων ανεξάρτητα. Συνεργατικά, όλοι οι κόμβοι του συστήματος επιλέγουν έναν ηγέτη και άλλοι κόμβοι γίνονται ακόλουθοι του ηγέτη. Κατά την επιλογή ενός ηγέτη, εφαρμόζεται η έννοια της πλειοψηφίας μεταξύ των διαθέσιμων υποψηφίων για ηγεσία. Ο ηγέτης διατηρεί και αναπαράγει τη μετάβαση κατάστασης (π.χ. καταγράφει) μεταξύ των ακολούθων. Ο αρχηγός συνεχίζει να ενημερώνει όλους τους followers για την ύπαρξή του στέλνοντας ένα ειδικό μήνυμα (που ονομάζεται καρδιακός παλμός). Οι ακόλουθοι δεν υποβάλλουν κανένα αίτημα μόνοι τους, αλλά απλώς ανταποκρίνονται στα αιτήματα των ηγετών. Αν δεν λάβουν καρδιακό παλμό από έναν ηγέτη (μετά από ένα ορισμένο χρόνο), οι ακόλουθοι ξεκινούν μια διαδικασία επανεκλογής του αρχηγού. Σε περίπτωση αποτυχίας ή συντριβής ενός κόμβου οδηγού, επιλέγεται νέος αρχηγός (μετά από προκαθορισμένο timeout) με ψηφοφορία. Όταν ένας αποτυχημένος κόμβος ανακτάται, γίνεται ακόλουθος. Όπως και οι Παξοί, το RAFT ακολουθεί τις έννοιες της πλειοψηφίας, δηλαδή, όσο λειτουργούν οι κόμβοι N/2 + 1 (ή με άλλα λόγια οι N/2–1 είναι αποτυχημένοι κόμβοι), είναι ανθεκτικό στη βυζαντινή ανοχή σφαλμάτων. Το πρόβλημα με το RAFT είναι ότι ο ηγέτης υποτίθεται ότι είναι σωστός (ή ειλικρινής) καθώς όλοι οι άλλοι κόμβοι ακολουθούν τυφλά τον αρχηγό.

- BFT (Byzantine Fault Tolerance): Το βασικό ζήτημα με το κατανεμημένο σύστημα είναι η επίτευξη αξιοπιστίας συμφωνώντας σε μια κοινή συναίνεση μεταξύ των διαφόρων αποφάσεων που λαμβάνονται από πολλούς φορείς του συστήματος. Αυτό το ζήτημα είναι σημαντικό όταν υπάρχουν ελαττωματικοί ή κακής συμπεριφοράς παράγοντες στο σύστημα που μπορεί να βάλουν το σύστημα με ασυνέπεια. Επομένως, η ανοχή σφαλμάτων είναι απαραίτητη για την πτυχή της επίτευξης συναίνεσης. Για να κατανοήσουμε την ανησυχία,

το Πρόβλημα των Βυζαντινών Στρατηγών περιγράφηκε στο (Lamport et al., 2019) όπου υπάρχουν πολλοί στρατηγοί (ο ένας είναι ο διοικητής και ο άλλος οι υπολοχαγοί) που επικοινωνούν μέσω ενός συστήματος μετάδοσης μηνυμάτων.. Έχουν συζητηθεί διάφορες περιπτώσεις θεωρώντας έναν ή περισσότερους υπολοχαγούς είτε πιστούς είτε προδότη, συμπεριλαμβανομένης μιας περίπτωσης όπου ο διοικητής θεωρείται επίσης ως πιστός ή προδότης. Το πρόβλημα μπορεί να επισημοποιηθεί καθώς η συναίνεση μπορεί να επιτευχθεί σε ένα σύστημα με 3 Ν κόμβους (γενικά) όπου οι μέγιστοι Ν κόμβοι (γενικά) είναι ελαττωματικοί (προδότης). Με άλλα λόγια, με 66,66% (2 Ν/3) τίμιους/κανονικούς/πιστούς κόμβους και 33,33% (Ν/3) ανέντιμους/ελαττωματικούς/προδοτικούς κόμβους, ένα σύστημα μπορεί να επιτύχει συναίνεση. Το Byzantine Fault Tolerance είναι ένα σύστημα που παραμένει ανεκτικό απέναντι στην αστοχία κόμβου .

(ii) Ασύγχρονο Περιβάλλον Δικτύου

- PBFT (Practical BFT): (Castro et al. (1999), Σχεδιάστηκε για ασύγχρονο περιβάλλον επικοινωνίας τύπου Διαδικτύου όπου δεν υπάρχει ανώτατο όριο (σε χρονική διάρκεια) σχετικά με το πότε θα ληφθεί η απάντηση σε ένα συγκεκριμένο αίτημα. Σκοπός ήταν να αντιμετωπιστούν τα ζητήματα που τέθηκαν στον μηχανισμό BFT (όπως η αποτυχία επιστροφής ενός αποτελέσματος, η απάντηση με εσφαλμένα/σκόπιμα παραπλανητικά αποτελέσματα κ.λπ.). Το PBFT λειτουργεί με βάση την αρχή της αναπαραγωγής της μηχανής κατάστασης όπου ένας κόμβος είναι πρωτεύων (κύριος/αρχηγός) (ο οποίος επιλέγεται κατά τρόπο στρογγυλό) και άλλοι κόμβοι είναι δευτερεύοντες (σκλάβος/εφεδρικός/ακόλουθος). Όπως το BFT, για να λειτουργήσει σωστά το PBFT, οι ανέντιμοι/ελαττωματικοί/προδότης κόμβοι δεν πρέπει να είναι μεγαλύτεροι από (Ν/3), όπου Ν είναι ο συνολικός αριθμός των κόμβων στο δίκτυο. Με άλλα λόγια, το PBFT απαιτεί 3F + 1 αντίγραφα έτσι ώστε να ανέχονται F ελαττωματικούς κόμβους. Το PFBT λειτουργεί σε τέσσερις φάσεις. Στην πρώτη φάση, ο πελάτης στέλνει ένα αίτημα στον πρωτεύοντα κόμβο ο οποίος με τη σειρά του μεταδίδει το αίτημα σε δευτερεύοντες κόμβους στη δεύτερη φάση. Όλοι οι κόμβοι (πρωτεύοντες και δευτερεύοντες) ανταποκρίνονται στον πελάτη μετά την εκτέλεση του αιτήματος υπηρεσίας στην τρίτη φάση. Στην τελευταία φάση, το αίτημα θεωρείται επιτυχές εάν οι απαντήσεις Μ + 1 έχουν πανομοιότυπα αποτελέσματα όπου Μ είναι ο μέγιστος αριθμός ελαττωματικών κόμβων.

Το PBFT στοχεύει να αντιμετωπίσει τις ανησυχίες με τρόπο ενεργειακά αποδοτικό, δηλαδή χωρίς να κάνει πολλούς μαθηματικούς υπολογισμούς. Η PBFT σκοπεύει επίσης να παρέχει οριστικότητα συναλλαγής, δηλαδή αφού οι συναλλαγές συμφωνηθούν (ή

οριστικοποιηθούν), σε αντίθεση με το PoW, δεν χρειάζονται πολλαπλές επιβεβαιώσεις. Επιπλέον, καθώς όλοι οι κόμβοι στο δίκτυο συμμετέχουν στη λήψη αποφάσεων (ανταποκρινόμενοι στο αίτημα) οδηγεί σε χαμηλή διακύμανση ανταμοιβής. Ωστόσο, το PBFT είναι επιρρεπές στο να είναι ευάλωτο στην επίθεση Sybil και δεν κλιμακώνεται καλά λόγω του μεγάλου κόστους επικοινωνίας.

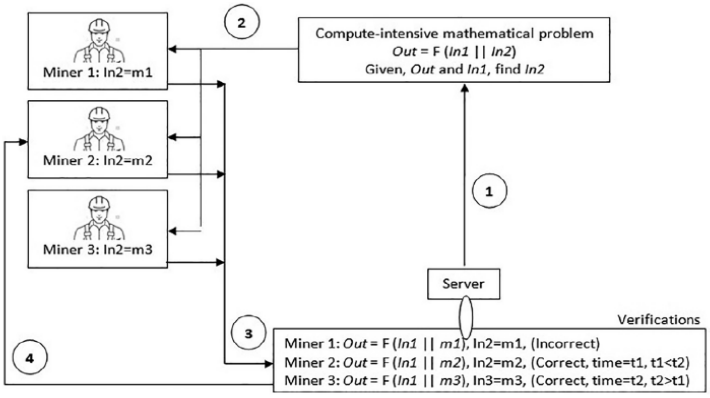
- DBFT (Delegated BFT): Το DBFT(Hackfeld, 2019) υποστηρίζεται ότι έχει σχεδιαστεί για να αντιμετωπίζει τις προκλήσεις της κλιμάκωσης και της απόδοσης που είναι οι πρωταρχικές ανησυχίες για την εφαρμογή του Blockchain. Στο DBFT, ο αριθμός των ελαττωματικών κόμβων δεν πρέπει να είναι μεγαλύτερος από [(N-1)/3] όπου N είναι ο αριθμός των ενεργών κόμβων. Όλοι οι ενεργοί κόμβοι (κόμβοι συναίνεσης) χωρίζονται σε μικρές ομάδες και κάθε ομάδα επιλέγει τον αρχηγό τους (εκπρόσωπο) με ψηφοφορία. Όλοι αυτοί οι εκπρόσωποι εργάζονται για την επίτευξη συναίνεσης και τη δημιουργία νέων μπλοκ, ενώ άλλοι κόμβοι λαμβάνουν και επαληθεύουν μπλοκ. Θα υπάρχει ένας γενικός αρχηγός από αυτήν την ομάδα αντιπροσώπων που θα είναι ο λήπτης των αποφάσεων. Εάν μια ομάδα διαφωνεί με τον εκπρόσωπό της, μπορεί να εκλέξει νέο εκπρόσωπο. Για την επικύρωση ενός μπλοκ, ο ομιλητής στέλνει ένα μήνυμα σε κάθε εκπρόσωπο και οι εκπρόσωποι που έχουν αρκετά διαπιστευτήρια (για παράδειγμα κάποια χρήματα αερίου) επαληθεύουν κάθε μπλοκ. Ο αντιπρόσωπος που δεν συμπεριφέρεται σωστά μπορεί να χάσει τα χρήματα του φυσικού αερίου του. Για τακτική συμπεριφορά, ο εκπρόσωπος λαμβάνει ανταμοιβές με τη μορφή προμηθειών συναλλαγής. Εάν τα 2/3 των αντιπροσώπων συμφωνούν με τον ομιλητή, το μπλοκ επικυρώνεται και προστίθεται στην αλυσίδα. Εάν μόνο το 1/3 των αντιπροσώπων συμφωνεί με τον ομιλητή, τότε ο ομιλητής μπορεί να αντικατασταθεί. Ως εκ τούτου, ο ομιλητής δεν μπορεί να χειραγωγήσει τη διαδικασία επικύρωσης του μπλοκ για προσωπικό του όφελος λόγω των εκπροσώπων. Και ο πληρεξούσιος δεν μπορεί να χειριστεί λόγω των εκλογικών κόμβων του, διαφορετικά θα αντικατασταθεί.

- Federated Byzantine Fault Tolerance (FBFT): Αυτή η παραλλαγή του BFT χρησιμοποιείται στην πλατφόρμα Blockchain που σχετίζεται με το πρωτόκολλο πληρωμής. Παραδείγματα τέτοιων πρωτοκόλλων είναι το Ripple (Armknecht et al., 2015)
και το Stellar (URL, 2019c). Καθώς οι χρηματοοικονομικές συναλλαγές είναι κρίσιμες για την εκτέλεση, το FBFT θα πρέπει να είναι μια αντιμετώπιση οποιουδήποτε είδους σφάλματος/επίθεσης. Στο FBFT, η συναίνεση επιτυγχάνεται μέσω τμημάτων απαρτίας. Δημιουργούνται απαρτίες σε επίπεδο συστήματος οι οποίες ενώνουν το σύστημα μαζί. Το FBFT προωθεί την ανοιχτή ιδιότητα μέλους στο δίκτυο που οδηγεί σε οργανική ανάπτυξη

του δικτύου. Σε αντίθεση με το πρωτόκολλο χωρίς άδεια όπως το PoW και το PoS, το FBFT έχει ως αποτέλεσμα λιγότερες υπολογιστικές και οικονομικές ανάγκες.

2.3.2. Blockchain χωρίς άδεια

- Proof of Work (PoW) (Vukolic, 2015): Είναι ένας μηχανισμός συναίνεσης (που χρησιμοποιείται στο Bitcoin στο Litecoin στο Ethereum κ.λπ. δίνεται να λυθεί ένα υπολογιστικό μαθηματικό πρόβλημα. Ένας τρόπος αναπαράστασης του μαθηματικού προβλήματος είναι μέσω της παραγοντοποίησης Ακέραιου/Πρώτου, όπου ένας αριθμός αναπαρίσταται χρησιμοποιώντας τον πολλαπλασιασμό δύο άλλων πρώτων ακεραίων. Για παράδειγμα, το 589 μπορεί να αναπαρασταθεί ως ο πολλαπλασιασμός δύο πρώτων ακεραίων 19 και 31. Επομένως, δεδομένου του 589, η ανακάλυψη των πρώτων πολλαπλασιαστών του είναι μια πρόκληση, αλλά δεδομένων των πολλαπλασιαστών, είναι πολύ εύκολο να υπολογιστεί ο πολλαπλασιασμός. Η πρωτόγονη ιδιότητα ενός τέτοιου προβλήματος είναι ότι είναι δύσκολο να λυθεί αλλά εύκολο να επαληθευτεί (η σωστή λύση). Η **Εικόνα 6** δείχνει τη λειτουργία του PoW. Σε σχέση με το Blockchain, το πρόβλημα επιπλέει σε διάφορους ενδιαφερόμενους της αλυσίδας και το (ειδικό) μέλος (ονομάζεται επίσης miner) που λύνει πρώτο το πρόβλημα, επιτρέπεται να εξορύξει το μπλοκ και να διεκδικήσει την επακόλουθη ανταμοιβή εξόρυξης. Το Bitcoin PoW χρησιμοποιεί SHA-256.



Εικόνα 6. Λειτουργία του μηχανισμού PoW(Shrimali&Patel, 2021).

Εδώ, οι miners καλούνται να κάνουν κάποια εργασία για να υπολογίσουν έναν αριθμό Nonce έτσι ώστε να ικανοποιεί την εξίσωση:

$$\textbf{Hash of Blocks} = \textbf{Hash}\,(\textbf{Hash of Previous Block} \,|\!+\!|\, \textbf{Merkle Root} \,|\!+\!|\, \textbf{Nonce}).$$

όπου όλες οι άλλες μεταβλητές δίνονται στους miners εκτός από το Nonce.

Εδώ, μια σημαντική πτυχή που πρέπει να σημειωθεί είναι η εισαγωγή της δυσκολίας που δεν είναι παρά να κάνει το υπολογιστικό μαθηματικό πρόβλημα μετρίως πολύπλοκο στην επίλυση. Η δυσκολία προσαρμόζεται με βάση διάφορους παράγοντες όπως **(i)** ο αναμενόμενος χρόνος εξόρυξης του τελευταίου συγκεκριμένου μπλοκ **(ii)** ο πραγματικός χρόνος που απαιτείται για την εξόρυξη του τελευταίου συγκεκριμένου μπλοκ, **(iii)** ο αριθμός των χρηστών στο δίκτυο **(iv)** τρέχουσα ισχύς και **(v)** φορτίο δικτύου. Το επίπεδο δυσκολίας ικανοποιεί τις οικονομικές πτυχές του Blockchain και βοηθά στον έλεγχο του πληθωρισμού του κρυπτονομίσματος. Η χαμηλότερη/εύκολη δυσκολία εγείρει ζητήματα όπως η επίθεση Sybil, η επίθεση DoS, το Spam και άλλες ευπάθειες. Η υψηλότερη/σκληρή δυσκολία εγείρει ζητήματα ταχύτητας δημιουργίας μπλοκ και απομάκρυνσης κινήτρων για τους miners. Ως εκ τούτου, η δυσκολία πρέπει να προσαρμόζεται σκόπιμα. Ωστόσο, λόγω της εγγενούς φύσης του PoW, η διόρθωση του αριθμού των minersπου έχουν περισσότερους υπολογιστικούς πόρους μπορεί να οδηγήσει σε ένα πρόβλημα γνωστό ως Monopoly ή πρόβλημα επίθεσης 51%. Επιπλέον, έχει τεράστια υπολογιστική ισχύ με αποτέλεσμα τεράστια ηλεκτρική ισχύ που οδηγεί σε αύξηση του κόστους λόγω εξειδικευμένου υλικού.

-Proof of Stake (PoS) (Zheng et al., 2017): Δημιουργήθηκε ως εναλλακτική λύση στο PoW. Σε αντίθεση με το PoW, όπου οι miners υποτίθεται ότι λύνουν ένα υπολογιστικό μαθηματικό παζλ για να επιτύχουν κατανεμημένη συνεισφορά, εδώ στο PoS, ο εξορυκτής (στην πραγματικότητα, ο δημιουργός του μπλοκ) επιλέγεται (τυχαία) με βάση το ποντάρισμα ή τα νομίσματα που κόπηκαν. Το Ether κλειδώνεται κατά τη διαδικασία προσθήκης του μπλοκ στο δίκτυο. Και όταν το μπλοκ προστεθεί με επιτυχία, το κλειδωμένο Ether απελευθερώνεται. Σε περίπτωση οποιασδήποτε παράνομης προσπάθειας κατά την προσθήκη του μπλοκ, η ποινή μπορεί να επιβληθεί και να αφαιρεθεί από τον ήδη κλειδωμένο Ether. Επιπλέον, δεν υπάρχει ανταγωνισμός μεταξύ των minersστο PoS. Επιπλέον, δεν υπάρχει ανταμοιβή στο PoS, αλλά ο δημιουργός μπλοκ χρειάζεται ορισμένες χρεώσεις συναλλαγών (ως ανταμοιβή) για να προσθέσετε το μπλοκ στο δίκτυο. Ωστόσο, μπορεί να προκύψει ένα προφανές ερώτημα ότι ο miner με υψηλότερο ποντάρισμα μπορεί να συμπεριφερθεί κακόβουλα αλλά μπορεί να μην είναι εμπειρικά εφικτό.

Για να προσθέσει έναν δημιουργό μπλοκ ένα πλαστό μπλοκ στο δίκτυο, πρέπει να έχει περισσότερο από ή ίσο με το 51% του συνολικού ποντάρισματος κρυπτονομισμάτων του δικτύου, κάτι που είναι πρακτικά πολύ απίθανο. Μια επίθεση 51% ακολουθεί όταν ένας miner κυβερνά το 51% της υπολογιστικής ισχύος του δικτύου, κάτι που είναι απίθανο. Είναι επιζήμιο για έναν δημιουργό μπλοκ να επιτίθεται στο δίκτυο όπου κατέχει μερίδιο 51%.

Ωστόσο, οι ειδικοί είναι δύσπιστοι σχετικά με το PoS, καθώς, χωρίς την πτυχή της ποινής, το PoS φαίνεται να είναι εύκολο να επιτεθεί. Ορισμένοι ερευνητές συζητούν ότι το PoS δεν είναι τέλεια απόφαση για ένα κατανεμημένο πρωτόκολλο συναίνεσης.

Το κύριο πλεονέκτημα του PoS είναι η εξοικονόμηση ενέργειας λόγω της αποφυγής υψηλής έντασης υπολογισμού.

-Proof of Activity (PoA) (Bach et al., 2018): Το PoA είναι μια υβριδική προσέγγιση για την επίτευξη κατανεμημένων συναλλαγών για να διασφαλιστεί ότι οι συναλλαγές είναι νόμιμες και ότι επιτυγχάνεται συναίνεση. Το PoA βρίσκεται κάπου μεταξύ PoW και PoS. Η διαδικασία εξόρυξης του PoW χρησιμοποιείται για τη δημιουργία μπλοκ, αλλά για την προσθήκη του μπλοκ στο δίκτυο που χρησιμοποιείται η προσέγγιση τύπου PoS όπου οι επικυρωτές τοποθετούν το ποντάρισμα τους για να επιλεγούν για την εξόρυξη του μπλοκ. Το νέο μπλοκ περιλαμβάνει μια κεφαλίδα και τη διεύθυνση ανταμοιβής του miner. Επιλέγεται μια νέα τυχαία ομάδα validator (με βάση τις λεπτομέρειες της κεφαλίδας) που υπογράφουν το νέο μπλοκ. Ανάλογα με το ποντάρισμα, επιλέγεται ένας υπογράφων. Έμμεσα το κληρονομεί τα του PoW και του PoS. Όσον αφορά την ασφάλεια του PoA, ο εισβολέας πρέπει να έχει τόσο **(i)** δύναμη εξόρυξης όσον αφορά τον υπολογισμό όσο και **(ii)** επαρκή κομμένα νομίσματα ως προς το ποντάρισμα, προσθέτοντας έτσι μια επιπλέον γραμμή άμυνας.

- Proof of Location (PoL) (Brambilla et al., 2016): Επαληθεύει την τοποθεσία κάποιου και οι τοποθεσίες κωδικοποιούνται σε μπλοκ. Το PoL είναι χρήσιμο για λειτουργίες που εξαρτώνται από τη θέση. Οι υπηρεσίες Proof of Location λειτουργούν σε χάρτες ανοιχτού κώδικα και επαληθεύσιμα και αδιάψευστα γεωχωρικά δεδομένα.

- Proof of Importance (PoI)(Bozic et al., 2016): Ιδρύθηκε από μια ομάδα που ονομάζεται NEM (New Economic Movement), ο συναινετικός μηχανισμός (PoI) αποφασίζει τους επιλέξιμους κόμβους που μπορούν προσθέστε ένα μπλοκ στην αλυσίδα, μέσω μιας διαδικασίας που ονομάζεται συγκομιδή (όπως η εξόρυξη). Οι κόμβοι με υψηλότερη βαθμολογία σημασίας (της φήμης τους) θα έχουν περισσότερες πιθανότητες να επιλεγούν για να προσθέσουν ένα μπλοκ. Ο κόμβος θα πρέπει να έχει τουλάχιστον 10.000 κατοχυρωμένα XEM (κρυπτονόμισμα) για να είναι κατάλληλος για συγκομιδή. Σε αντίθεση με το PoS ,όπου μόνο μία παράμετρος λήφθηκε υπόψη για την επιλογή του κόμβου που μπορεί να προσθέσει το μπλοκ στην αλυσίδα, το PoI θεωρεί τη συνολική υποστήριξη του δικτύου για τη μέτρηση της βαθμολογίας με πολλαπλές παραμέτρους, όπως η κατοχύρωση, συνεργάτες συναλλαγών και τον αριθμό και το μέγεθος των συναλλαγών τις τελευταίες 30 ημέρες. Το PoI έχει πολλά πλεονεκτήματα, όπως δεν χρειάζεται υλικό, φθηνό λόγω της

μικρότερης έντασης πόρων και διατηρεί τη διαδικασία συλλογής δίκαιη, διαφανή και σωστή (από την άποψη της προσφοράς κινήτρων).

- Proof of Elapsed Time (PoET) (Bach et al., 2018): Εφευρέθηκε από την Intel το 2016, είναι ένας μηχανισμός συναίνεσης που χρησιμοποιείται σε επιτρεπόμενο Blockchain που βασίζεται σε ένα απλό σχέδιο λοταρίας με μοναδικό σκοπό να προσφέρει ίσες ευκαιρίες σε κάθε συμμετέχοντα κόμβο στο δίκτυο για την προσθήκη ενός μπλοκ. Αποφεύγει τη χρήση μιας υπολογιστικής εντατικής διαδικασίας εξόρυξης, επομένως είναι εξαιρετικά αποδοτικό και χαμηλής κατανάλωσης ενέργειας. Η λειτουργικότητα αυτού του αλγορίθμου είναι απλή. Κάθε κόμβος μεταβαίνει σε κατάσταση αναστολής λειτουργίας για μια τυχαία χρονική περίοδο. Ο κόμβος που ξυπνά πρώτος, προσθέτει το μπλοκ και το οικείο στο υπόλοιπο δίκτυο. Εδώ, δύο παράγοντες πρέπει να ληφθούν υπόψη. Πρώτον, η γνήσια διαδικασία δημιουργίας τυχαίας και δεύτερον, κανείς δεν απατά και δεν ξυπνά πριν από την ώρα του.

2.3.3. Ερευνητικές προκλήσεις και προοπτικές μελλοντικές κατευθύνσεις

Το blockchain αναγνωρίζεται και υιοθετείται ευρέως. Η εκτεταμένη έρευνα και ανάπτυξη τόσο από τον ακαδημαϊκό χώρο όσο και από τη βιομηχανία βρίσκονται στο αποκορύφωμά τους. Ωστόσο, υπάρχουν ακόμη μεγάλες προκλήσεις που πρέπει να ξεπεραστούν πριν ολοκληρωθεί η υιοθέτησή του. Πολλές περιοχές πρέπει να συγκεντρωθούν. Πολλά υπάρχοντα ζητήματα δεν έχουν αντιμετωπιστεί πλήρως, ενώ νέες προκλήσεις συνεχίζουν να αναδύονται από τις εφαρμογές που υιοθετήθηκαν από τις βιομηχανίες.

Σε αυτή την ενότητα, συζητάμε τις κύριες ερευνητικές προκλήσεις και κατευθύνσεις που πιστεύουμε ότι είναι σημαντικό να διερευνηθούν. Ο Swan απαριθμεί επτά τεχνικές προκλήσεις και περιορισμούς για την πλήρη προσαρμογή της τεχνολογίας Blockchain στο μέλλον είναι:

1. Διακίνηση: Η απόδοση αυτής της τεχνολογίας αντικατοπτρίζεται από τον αριθμό των συναλλαγών που προστίθενται ανά καθορισμένο χρόνο. Εάν ληφθεί υπόψη το δίκτυο Bitcoin, τότε η απόδοση είναι έως 7 tps (συναλλαγές ανά δευτερόλεπτο). Σε σύγκριση με άλλα δίκτυα επεξεργασίας συναλλαγών όπως το VISA και το Twitter που έχουν 2000 tps (Transactions Per Second) και 5000 tps αντίστοιχα, η τεχνολογία Blockchain πρέπει επίσης να βελτιώσει την ικανότητα διακίνησης .

2. Διαφάνεια: Τα ασφαλή και αδιάψευστα μπλοκ είναι το κύριο μέλημα της τρέχουσας τεχνολογίας Blockchain. Για την αποφυγή διπλών δαπανών και μη εξουσιοδοτημένων συναλλαγών, ο περισσότερος χρόνος δαπανάται για επαλήθευση και επικύρωση. Η δημιουργία μπλοκ και η επιβεβαίωση των συναλλαγών καταναλώνουν πολύ χρόνο λόγω

ανησυχιών για την ασφάλεια. Έτσι, επί του παρόντος, η καθυστέρηση είναι μια σημαντική ανησυχία στο Blockchain.

3. Μέγεθος και εύρος ζώνης: Το μέγεθος ενός Blockchain εξαρτάται από τον αριθμό των μπλοκ που δημιουργούνται. Στο Bitcoin, το μέγεθος ενός μπλοκ είναι 1 MB και δημιουργείται κάθε δέκα λεπτά. Ως εκ τούτου, υπάρχει περιορισμός στον αριθμό των συναλλαγών που μπορούν να συμπεριληφθούν στο μπλοκ. Εάν το Blockchain περιλαμβάνει/διαχειρίζεται περισσότερες συναλλαγές, τα ζητήματα μεγέθους και εύρους ζώνης του Blockchain μπορούν να επιλυθούν.

4. Ασφάλεια: Επί του παρόντος, το Blockchain έχει πιθανότητα επίθεσης 51%. Υπάρχουν πολλές περιπτώσεις όπου ακόμη και μια μεμονωμένη οντότητα μπορεί να έχει τον πλήρη έλεγχο της πλειοψηφίας του δικτύου. Αυτό μπορεί να θεωρηθεί ανησυχία και πρόκληση για την ασφάλεια. Έτσι, για να ξεπεραστεί αυτό το πρόβλημα, απαιτείται περισσότερη έρευνα σχετικά με τους αλγόριθμους ασφαλείας.

5. Σπατάλη πόρων: Η διαδικασία εξόρυξης σε περιβάλλον χωρίς άδεια απαιτεί πολύ υπολογιστική εργασία εξόρυξης από τους miners. Πολύ χρόνο, λόγω του πρωτοκόλλου συναίνεσης και των χρονικών περιορισμών, ορισμένες από τις εργασίες εξόρυξης αποτυγχάνουν. Έτσι, χάνεται χρόνος και πόροι εξόρυξης. Αυτό το ζήτημα της σπατάλης πόρων απαιτείται να επιλυθεί για να έχουμε πιο αποτελεσματική εξόρυξη στο Blockchain.

6. Ευχρηστία: Οι εφαρμογές blockchain θα πρέπει να διαθέτουν φιλικά προς τον χρήστη API. Έχει διαπιστωθεί ότι το Bitcoin API για την ανάπτυξη υπηρεσιών είναι δύσκολο να χρησιμοποιηθεί. Απαιτείται η ανάπτυξη ενός πιο φιλικού API για προγραμματιστές για το Blockchain για να γίνει πιο δημοφιλές μεταξύ των προγραμματιστών.

7.Πολλαπλές αλυσίδες: Μια μικρή αλυσίδα ή/και πολλαπλές αλυσίδες με μικρότερο αριθμό κόμβων έχουν περισσότερες πιθανότητες επίθεσης. Ένα άλλο ζήτημα προκύπτει όταν οι αλυσίδες χωρίζονται για λόγους διαχείρισης. Μαζί με αυτές τις προκλήσεις, συζητάμε επίσης άλλες σημαντικές προκλήσεις από τη μελέτη ανασκόπησης στις ακόλουθες υποενότητες.

2.3.1.1. Ανάλυση μπλοκ σε πραγματικό χρόνο

Σε ένα κατανεμημένο κοινόχρηστο ασύγχρονο περιβάλλον, ένα μπλοκ εισάγεται από τους miners μέσω του ελέγχου ταυτότητας. Μαζί με τα δεδομένα συναλλαγής, το μπλοκ περιέχει επίσης μεταδιδόμενα σε μια κεφαλίδα μπλοκ που περιλαμβάνει χρονική σήμανση, έκδοση, κατακερματισμό του προηγούμενου μπλοκ και nonce. Η ανάλυση αυτού του μπλοκ είναι η διαδικασία αναγνώρισης, επιθεώρησης, επαλήθευσης και αναπαράστασης μεταδιδόμενων

του μπλοκ για την ανακάλυψη χρήσιμων πληροφοριών σχετικά με τη συνάφεια του προηγούμενου μπλοκ, των συναλλαγών, του nonce και της χρονικής σφραγίδας. Τα μπλοκ εισάγονται σε τεράστιους αριθμούς. Η ανάλυση του μπλοκ σε πραγματικό χρόνο θα μειώσει τις πιθανότητες διακλάδωσης και επίθεσης. Ωστόσο, για την εκτέλεση ανάλυσης μπλοκ, ο πραγματικός χρόνος είναι μια σημαντική πρόκληση λόγω του ανώνυμου και ασύγχρονου περιβάλλοντος του.

2.3.1.2. Επεκτασιμότητα

Με την αυξημένη δημοτικότητα των κρυπτονομισμάτων και της τεχνολογίας Blockchain, ο αριθμός των συναλλαγών αυξάνεται μέρα με τη μέρα με αποτέλεσμα το πυκνό Blockchain. Προς το παρόν, το Bitcoin Blockchain έχει ξεπεράσει τα 100 GB αποθηκευτικού χώρου (Zheng et al., 2018). Η μεθοδολογία Blockchain χρειάζεται να αποθηκεύονται όλες οι συναλλαγές για την επικύρωση κάθε συναλλαγής. Επιπλέον, λόγω του περιορισμού στο μέγεθος του μπλοκ και της πολυπλοκότητας του αλγορίθμου για τη δημιουργία του νέου μπλοκ, το bitcoin Blockchain δεν μπορεί να προχωρήσει/λειτουργήσει σε περιβάλλον πραγματικού χρόνου, περιορίζεται να επεξεργάζεται μόνο 7 συναλλαγές . Επίσης, καθώς η χωρητικότητα των μπλοκ είναι πολύ μικρή, πολλές μικρές συναλλαγές ενδέχεται να καθυστερήσουν, καθώς οι miners προτιμούν αυτές τις συναλλαγές με υψηλή χρέωση συναλλαγής. Ωστόσο, το μεγάλο μέγεθος μπλοκ θα επιβράδυνε την ταχύτητα διάδοσης και θα οδηγούσε σε κλάδους Blockchain. Άρα το πρόβλημα επεκτασιμότητας είναι αρκετά περίπλοκο. Υπάρχουν πολλές προσπάθειες που προτείνονται για την αντιμετώπιση του προβλήματος επεκτασιμότητας του Blockchain, οι οποίες θα μπορούσαν να κατηγοριοποιηθούν σε δύο τύπους:

2.3.1.3. Βελτιστοποίηση αποθήκευσης Blockchain

Σύμφωνα με την τεκμηρίωση αποθήκευσης Blockchain της IBM (Mencias et al., 2018), το καθολικό Blockchain απαιτεί 6.912 MB, δηλαδή 0,00659 TiB/- συναλλαγή/έτος για 1000 Συναλλαγές ανά Μπλοκ (TPB). Επομένως, εάν ληφθούν υπόψη μέτρια ποσοστά συναλλαγών, ο χώρος αποθήκευσης για το καθολικό Hyperledger Blockchain έχει μέγεθος terabyte ή πολλαπλών terabyte. με βάση διαφορετικές εκτιμήσεις σχετικά με το συνολικό μέγεθος του καθολικού και τον συνολικό αριθμό των αποθηκευμένων συναλλαγών, το bitcoin είναι κατά μέσο όρο κοντά στα 555 byte ανά συναλλαγή (BPT) ή 1889 TPB και το Ethereum είναι κοντά στα 2 KB ανά συναλλαγή ή 512 TPB. Το Blockchain διαθέτει επίσης χώρο αποθήκευσης εκτός αλυσίδας για αποθήκευση άλλων δεδομένων. Η αποθήκευση

εκτός αλυσίδας είναι η προσωπική αποθήκευση του κόμβου που συμμετέχει. Στην αλυσίδα, η αποθήκευση είναι μια κρίσιμη οντότητα καθώς ο αριθμός των συναλλαγών αυξήθηκε και πρέπει να χρησιμοποιηθεί αποτελεσματικά.

Ένα νέο σχήμα κρυπτονομισμάτων προτάθηκε στον Bruce (2014) για να λύσει το πρόβλημα του όγκου. Το σχήμα τους αφαιρεί τις παλιές εγγραφές συναλλαγών από το δίκτυο και χρησιμοποίησε μια βάση δεδομένων που ονομάζεται δέντρο λογαριασμού για να διατηρεί το υπόλοιπο όλων των μη κενών διευθύνσεων. Έτσι, οι κόμβοι δεν χρειάζεται να αποθηκεύουν κάθε συναλλαγή για να ελέγξουν αν μια συναλλαγή είναι έγκυρη ή όχι. Το VerSum εισήχθη για να χειριστεί πελάτες μικρού βάρους. Το VerSum επιτρέπει σε ελαφρούς πελάτες να αναθέτουν σε εξωτερικούς συνεργάτες ακριβούς υπολογισμούς σε μεγάλες εισόδους. Διασφαλίζει ότι το αποτέλεσμα υπολογισμού είναι σωστό συγκρίνοντας αποτελέσματα από πολλούς διακομιστές.

2.3.1.4. Επανασχεδιασμός Blockchain

Το Bitcoin-NG (Next Generation). Είναι η επόμενη γενιά η οποία αποσυνδέει το συμβατικό μπλοκ σε δύο μέρη: **(i)** κλειδί για εκλογή αρχηγού και **(ii)** micro block για αποθήκευση συναλλαγών. Σε αυτή τη μέθοδο επίσης οι miners ανταγωνίζονται για να γίνουν αρχηγοί. Ο αρχηγός θα είναι υπεύθυνος για τη δημιουργία micro block μέχρι να εμφανιστεί ένας νέος αρχηγός. Το Bitcoin-NG επέκτεινε επίσης τη βαρύτερη (μεγαλύτερη) στρατηγική αλυσίδας όπου μετρούν μόνο τα βασικά μπλοκ και τα micro block δεν έχουν κανένα βάρος. Με αυτόν τον τρόπο, το Blockchain επανασχεδιάζεται και έχει αντιμετωπιστεί η αντιστάθμιση του μεγέθους του μπλοκ και της ασφάλειας του δικτύου.

2.3.1.5. Ασφάλεια και ιδιωτικότητα

Ένα από τα βασικά πλεονεκτήματα της τεχνολογίας Blockchain είναι ο κατανεμημένος τρόπος αποθήκευσης, δημιουργίας και επικύρωσης δεδομένων. Το μπλοκ είναι μετριασμένη απόδειξη λόγω της μεθόδου ελέγχου ταυτότητας του. Υπάρχουν διάφοροι αλγόριθμοι συναίνεσης που αναφέρθηκαν προηγουμένως που επιτρέπουν στους miners να επικυρώσουν και να εισαγάγουν το μπλοκ στο δίκτυο. Ένας από τους διάσημους αλγόριθμους συναίνεσης που ονομάζεται απόδειξη εργασίας χρειάζεται μια ισχύ κατακερματισμού για να ενταχθούν στο δίκτυο και για τους ίδιους οι miners συνδυάζονται για να ενταχθούν στο δίκτυο για να εξορύξουν περισσότερα μπλοκ. Τέτοιοι miners δημιουργούν συλλογικά μπλοκ εξόρυξης που έχουν μέγιστη ισχύ κατακερματισμού. Εάν σε ένα δίκτυο κατέχει το 51% της υπολογιστικής ισχύος, μπορεί να ελέγξει το συνολικό

Blockchain και να επηρεάσει την ασφάλεια του Blockchain. Επίσης, (εάν κάποιος έχει πάνω από 51% υπολογιστική ισχύ) μπορεί να αποφασίσει την άδεια αποκλεισμού, μπορεί να προκαλέσει διπλή δαπάνη τροποποιώντας τα δεδομένα συναλλαγών, μπορεί να σταματήσει την εξόρυξη διαθέσιμου μπλοκ από τους miners και μπορεί να σταματήσει την επαλήθευση συναλλαγής) (Lin and Liao, 2017).

ΚΕΦΑΛΑΙΟ 3

ΤΟΜΕΙΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΔΕΔΟΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ

3.1 Blockchain για χρηματοοικονομικές δραστηριότητες

Η τεχνολογία Blockchain έχει χρησιμοποιηθεί μαζικά στον χρηματοοικονομικό τομέα σε πολλούς τομείς όπως για τον διακανονισμό συναλλαγών χρηματοπιστωτικών αγορών, για εμπορική χρηματοδότηση, για ασφάλιση, για μεταφορά χρημάτων σε πραγματικό χρόνο κ.λπ. Το Bitcoin εκτός του ότι υπήρξε ιστορικά το πρώτο αποκεντρωμένο κρυπτονόμισμα στον κόσμο είναι και ένα σύστημα πληρωμών που δεν υποστηρίζεται από κεντρική τράπεζα. Για αυτό ακριβώς το λόγο παραλείπεται η ανάγκη μεσάζοντα και έτσι οι διάφορου τύπου οικονομικές συναλλαγές πραγματοποιούνται απευθείας μεταξύ των χρηστών μέσω του δικτύου P2P (Tschorsch et al, 2016. Άλλα κρυπτονομίσματα, όπως τα BitcoinCash, Ethereum, Ripple και Dash μπορούν να χρησιμοποιηθούν με παρόμοιο τρόπο για αυτόν τον σκοπό. Αυτά ακριβώς τα χαρακτηριστικά έρχονται σε αντίθεση με το συμβατικό τραπεζικό σύστημα διασυνοριακών πληρωμών, το οποίο έχει σαν μειονεκτήματα ότι είναι ακριβό, χρονοβόρο και λιγότερο ασφαλές. Ωστόσο, με τη χρήση του blockchain για τη μεταρρύθμιση αυτού του συστήματος πληρωμών, όλοι αυτοί οι περιορισμοί μπορούν να παρθούν ενώ παράλληλα το σύστημα να λειτουργεί αποτελεσματικά. Πέρα από τις οικονομικές συναλλαγές η τεχνολογία του Blockchain μπορεί να χρησιμοποιηθεί και στην διαχείριση των περιουσιακών στοιχείων (π.χ. αυτοκίνητο, σπίτι, μετοχές κ.λπ.) αφού μπορεί να καταγραφεί, να πραγματοποιήσει τη διαδικασία των μεταβιβάσεων και να επαληθεύει συναλλαγές συνδυάζοντας πάντα τα χαρακτηριστικά της ακεραιότητας και της εγκυρότητας ευαίσθητων εγγράφων ή δεδομένων. Οι Chhabra et al (2019) πραγματοποίησαν μια εκτενή ανάλυση των διαφορών μεταξύ των κύριων γνωστών κρυπτονομισμάτων και τα σύγκριναν λαμβάνοντας υπόψη παράγοντες όπως την ημερομηνία κυκλοφορίας, τον ιδρυτή, τον αλγόριθμο κατακερματισμού που χρησιμοποιήθηκε και τη γλώσσα που χρησιμοποιήθηκε για την ανάπτυξή τους .

Φυσικά, παρόλο που η χρήση τεχνολογιών blockchain στον οικονομικό και χρηματοοικονομικό τομέα φαίνεται να είναι πολλά υποσχόμενη, εξακολουθεί να έχει ορισμένους περιορισμούς τους οποίους απαριθμούμε παρακάτω (Demirkan et al, 2020. Hassani et al, 2018):

• Το Blockchain είναι πολύ αργό αφού επιτρέπει μόνο οκτώ συναλλαγές ανά δευτερόλεπτο. Αυτό αποτελεί ένα σημαντικό μειονέκτημα σε σχέση με τρέχοντα σύστημα πληρωμών τρίτων μερών τα οποία μπορούν να πραγματοποιήσουν ταχύτερα συναλλαγές που πολλές φορές μπορούν να φτάσουν και τις εκατοντάδες ανά δευτερόλεπτο.
• Σημαντικός περιορισμός αποτελεί και η απώλεια του ιδιωτικού κλειδιού ή η αποκάλυψη αφού αυτό το γεγονός συνεπάγεται τη μη αναστρέψιμη απώλεια περιουσιακών στοιχείων των καταναλωτών αφού το σύστημα blockchain είναι αδύνατο να ανακτηθεί.
• Παρά το γεγονός ότι το blockchain είναι θεωρητικά δύσκολο να σπάσει με βίαιο τρόπο δυστυχώς ο κίνδυνος παραβίασης δεδομένων είναι ακόμα υπαρκτός.
• Δεν έχει διαμορφωθεί ακόμα μια καλύτερη κατανόηση και αποδοχή της τεχνολογίας blockchain από τον ευρύ κόσμο, γεγονός που καθιστά δύσκολο τον εντοπισμό γνήσιων και χρήσιμων οικονομικών λύσεων blockchain.
• Έχουν παρατηρηθεί φαινόμενα στήριξης της εγκληματικότητα αφού η έλλειψη κεντρικής δομής ενώ έχε αρκετά θετικά στοιχεία, έχει καταστήσει πιο βολικό το ξέπλυμα χρήματος, την απάτη και τη φοροδιαφυγή, καθιστώντας παράλληλα την εποπτεία και τον έλεγχο πιο πολύπλοκα.

Παραδείγματα εφαρμογών blockchain στα χρηματοοικονομικά είναι τα κρυπτονομίσματα (Bitcoin, Ethereum, Cardano, Polkadot) καθώς και τα Stablecoins όπως το Tether, το USD Coin, το Binance USD και το Terra USD, τα οποία είναι κρυπτονομίσματα κλειδωμένης ισοτιμίας 1-προς-1 με το δολάριο των ΗΠΑ και χρησιμοποιούνται ευρέως στη βιομηχανία blockchain, ειδικά ως ζεύγη συναλλαγών σε χρηματιστήρια

3.2 Blockchain για την Υγεία

Παρά τη σημασία της ανταλλαγής ιατρικών δεδομένων, τα συστήματα υγείας συνήθως υποχρεώνουν έναν ασθενή να εκτελεί εκείνος ένα μεγάλο μέρος της διαδικασίας με το να τον αναγκάζουν να συλλέγει και να ανταλλάσσει τις ιατρικές του πληροφορίες με το ιατρικό προσωπικό, είτε σε έντυπη μορφή είτε με κάποιο ηλεκτρονικό τρόπο αποθήκευσης και μεταφοράς της πληροφορίας. Αυτή η μέθοδος διανομής ιατρικών αρχείων είναι προβληματική, αργή, δεν εγγυάται την ασφαλή μεταφορά των δεδομένων και πολλές φορές είναι ελλιπής. Επιπλέον, έχει σαν αυτοσκοπό τη διαδικασία της παροχής της υπηρεσίας και τα τεχνικά ζητήματα της και όχι τον ίδιο τον ασθενή ο οποίος αποτελεί το σημαντικότερο κομμάτι του παζλ που λέγεται Παροχή Υγείας. Η αναποτελεσματικότητα αυτής της μεθόδου έγκειται κατά βάση στην έλλειψη αξιοπιστίας μεταξύ των ιδρυμάτων υγειονομικής περίθαλψης και στην έλλειψη συνδεσιμότητας, αλληλεπίδρασης και διαλειτουργικότητας

μεταξύ των διαφορετικών πλατφορμών πληροφορικής που χρησιμοποιούνται από τα ιδρύματα. Το πρόβλημα αυτό όσο μεγάλο και αν φαίνεται μπορεί να επιλυθεί χρησιμοποιώντας τεχνολογία blockchain (Jabbar et al, 2020. Zhuang et al, 2020). Χρησιμοποιώντας την εφαρμογή blockchain, οι ιατρικές πληροφορίες των ασθενών θα μπορούν να κοινοποιούνται με τις απαραίτητες άδειες χρησιμοποιώντας έξυπνες συμβάσεις (smart contract). Στη συνέχεια, παρουσιάζονται ορισμένα παραδείγματα που η χρήση της τεχνολογίας blockchain μπορεί να "λύσει τα χέρια" στον ευαίσθητο τομέα της υγειονομικής περίθαλψης (Zhang et al, 2018):

- Ταυτότητα ασθενούς: Η ταυτοποίηση του ασθενούς είναι ένα κρίσιμο στοιχείο της ανταλλαγής πληροφοριών για την υγεία. Σύμφωνα με τον Ασφαλιστικό Όμιλο Allianz τα ιατρικά λάθη προκαλούν 195.000 θανάτους κάθε χρόνο στις ΗΠΑ, με τα προβλήματα ταυτοποίησης να αντιστοιχούν στο 57% του συνολικού αριθμού σφαλμάτων. Σε μια τέτοια περίπτωση τα νούμερα μιλάνε από μόνα τους και καλούν την τεχνολογία blockchain να λύσει το πρόβλημα με μια επαληθεύσιμη τυποποιημένη ταυτότητα για κάθε ασθενή η οποία επιτυγχάνεται μέσω μιας καθολικής βάσης δεδομένων ευρετηρίου ασθενών που μπορεί να είναι κοινή σε όλες τις εγκαταστάσεις υγειονομικής περίθαλψης.
- Μητρώα υγείας: Γενικά, τα κλασικά ηλεκτρονικά κεντρικά συστήματα (Chen et al, 2014. Barua et al, 2011. Li et al, 2010) αδυνατούν να αντιμετωπίσουν τη ρίζα του προβλήματος κοινής χρήσης δεδομένων ασθενών. Ωστόσο, χάρη στα blockchains , ένας ασθενής μπορεί απλώς να συλλέξει το ιατρικό του ιστορικό χωρίς να ζητήσει αντίγραφο από κάθε πάροχο που έχει επισκεφτεί αφού η τεχνολογία blockchain επιτρέπει τη δημιουργία ευρέως ασφαλών και προσβάσιμων υπηρεσιών διανομής δεδομένων τα οποία διασυνδέονται με τα ήδη υπάρχοντα συστήματα υγείας . Με αυτόν τον τρόπο καθίσταται η ανταλλαγή δεδομένων μεταξύ του ασθενούς και του γιατρού ευκολότερη και ασφαλέστερη (Panigrahi et al, 2022).
- Τηλεϊατρική: Οι ασθενείς που είναι συνδεδεμένοι στο διαδίκτυο μπορούν να αποφύγουν να περάσουν χρόνο στο κέντρο υγείας και να λάβουν γρήγορη θεραπεία για μικρά αλλά την εκάστοτε στιγμή κρίσιμα προβλήματα. Δυστυχώς όμως οι μακρινοί ιατροί δεν έχουν πάντα συνεχή πρόσβαση σε δεδομένα υγείας που λαμβάνονται κατά τη διάρκεια επεισοδίων θεραπείας τηλεϊατρικής, με αποτέλεσμα να δημιουργείται ιατρικό ιστορικό το οποίο είναι ελλιπές , με κίνδυνο να υποβαθμιστεί η συνολική ποιότητα της περίθαλψης. Στον αντίποδα αυτής της μεθόδου, η τεχνολογία blockchain (Ahmad et al, 2021. Wang et al, 2021. Kordestani

et al, 2020. Parikh et al, 2022) μπορεί να γεφυρώσει το χάσμα επικοινωνίας μεταξύ διαφορετικών παρόχων εξαλείφοντας την ανάγκη για τρίτους και επιτρέπει στους συμμετέχοντες να αλληλεπιδρούν μεταξύ τους (Clohessy&Acton, 2019. Park et al, 2019. Hawig et al, 2019).

Ενδεικτικά παραδείγματα εφαρμογών είναι τα εξής:

- Το MediLedger είναι ένα κορυφαίο παράδειγμα πρωτοκόλλου blockchain που επιτρέπει στις εταιρείες σε όλη την αλυσίδα εφοδιασμού συνταγογραφούμενων φαρμάκων να επαληθεύουν τη γνησιότητα των φαρμάκων, καθώς και τις ημερομηνίες λήξης και άλλες σημαντικές πληροφορίες.
- Η Medicalchain είναι ένα κορυφαίο παράδειγμα εταιρείας που συνεργάζεται με παρόχους υγειονομικής περίθαλψης για την εφαρμογή EMR με δυνατότητα blockchain.
- Εταιρείες όπως η Chronicled και η Curisium παρέχουν συστήματα που βασίζονται σε blockchain όπου διάφοροι παίκτες στον τομέα της υγειονομικής περίθαλψης, όπως φαρμακευτικές εταιρείες, OEM ιατρικών συσκευών, χονδρέμποροι, ασφαλιστές και πάροχοι υγειονομικής περίθαλψης, μπορούν να πιστοποιήσουν την ταυτότητά τους ως οργανισμοί, να καταγράψουν λεπτομέρειες συμβολαίων και να παρακολουθήσουν τη συναλλαγή αγαθών και υπηρεσιών και λεπτομέρειες διακανονισμού πληρωμών για αυτά τα αγαθά και τις υπηρεσίες. Αυτός ο τύπος περιβάλλοντος προχωρά ένα βήμα πέρα από τη διαχείριση της εφοδιαστικής αλυσίδας για να επιτρέψει επίσης στους εμπορικούς εταίρους και τους ασφαλιστικούς φορείς στον τομέα της υγειονομικής περίθαλψης να λειτουργούν με βάση πλήρως ψηφιακούς και σε ορισμένες περιπτώσεις αυτοματοποιημένους όρους συμβολαίου.
- Παρόμοια με την παρακολούθηση της προέλευσης ενός ιατρικού αγαθού, η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την παρακολούθηση της εμπειρίας των επαγγελματιών υγείας, όπου αξιόπιστα ιατρικά ιδρύματα και οργανισμοί υγειονομικής περίθαλψης μπορούν να καταγράψουν τα διαπιστευτήρια του προσωπικού τους, βοηθώντας με τη σειρά του στον εξορθολογισμό της διαδικασίας πρόσληψης για οργανισμούς υγειονομικής περίθαλψης. Η ProCredEx με έδρα τις ΗΠΑ έχει αναπτύξει ένα τέτοιο σύστημα επαλήθευσης ιατρικών διαπιστευτηρίων χρησιμοποιώντας το πρωτόκολλο blockchain R3 Corda.

3.3 Blockchain για Πληροφοριακά Συστήματα

Ένα πληροφοριακό σύστημα (Obrien&Marakas, 2005) είναι μια συλλογή πολλών διαφορετικών τύπων δεδομένων που διασφαλίζουν την επίτευξη ενός επιχειρηματικού στόχου. Τα συστήματα πληροφοριών δεν είναι πραγματικά αυτόνομα επιχειρηματικά μοντέλα πληροφορικής και η ενοποίηση με δεδομένα από τις διάφορες επιχειρηματικές λειτουργίες αποτελούν ένα κρίσιμο μέρος τους. Αν μπορούσαμε να δώσουμε μια μορφή στην έννοια του τι είναι πληροφορικό σύστημα αυτό θα ήταν ένα τρίγωνο του οποίου οι τρείς κορυφές είναι οι διαδικασίες, οι άνθρωποι και οι υπολογιστές. Για να μπορεί να πετύχει ένα πληροφοριακό σύστημα πρέπει να έχει όλα αυτά τα στοιχεία και να λειτουργούν σωστά. Η επιλογή της ενσωμάτωσης της τεχνολογίας blockchain σε συστήματα πληροφοριών επιτρέπει στους οργανισμούς να επωφεληθούν από την τεράστια γκάμα εφαρμογών και πλεονεκτημάτων που προσφέρει. Για παράδειγμα, σημαντικό κομμάτι του τομέα των Πληροφοριακών Συστημάτων είναι η εμπιστοσύνη μεταξύ των εμπλεκόμενων εταίρων, ειδικά μάλιστα όταν εμπλέκονται ευαίσθητες πληροφορίες. Το Blockchain δίνει τη δυνατότητα μιας πιο αυξημένες ασφάλειας και μειώνει κατά πολύ τον κίνδυνο αποκάλυψης ευαίσθητων πληροφοριών σε τρίτα μέρη. Επιπλέον, χάρις στην δια λειτουργικότητα που προσφέρει καθιστά την τεχνολογία του blockchain μια ευρέως αποδεκτή λύση με πολλαπλά οφέλη. Τέλος, το αποκεντρωμένο του χαρακτήρα της τεχνολογίας αυτής διασφαλίζει την ακεραιότητα των συναλλαγών. Το συγκεκριμένο πλεονέκτημα συνδυάζεται με τη χρήση του «έξυπνου συμβολαίου» το οποίο έχει ως στόχο να διασφαλίσει ότι δύο μέρη έχουν μια συμφωνία και ότι οι ανταλλαγές είναι ανιχνεύσιμες και μη αναστρέψιμες. Εάν είναι απαραίτητο, το blockchain θα μπορούσε να χρησιμοποιηθεί για την επίλυση τυχόν διαφωνιών που προκύπτουν επιβεβαιώνοντας την αυθεντικότητα των ψηφιακών υπογραφών με ασφαλή, αποκεντρωμένο τρόπο (Francisco&Swanson, 2018. Dujak&Sajter, 2019. Azzi et al, 2019).

Η σημασία και τα οφέλη της χρήσης της τεχνολογίας του blockchain στον τομέα αυτό έχει ήδη σημειωθεί από πολλές επιχειρήσει ακόμα στην πιο εύκολη παρακολούθηση της προέλευσης ενός προϊόντος λόγω των τοπικών κανονισμών, των προτιμήσεων, των φορολογικών μειώσεων και άλλων κινήτρων για τον εντοπισμό της παρακολούθησης προέλευσης και έτσι ένα είδος μπορεί να επιβεβαιωθεί επίσημα ανά πάσα στιγμή και οι συναλλαγές δεν μπορούν να παραποιηθούν ή να τροποποιηθούν με σκοπό την εξαπάτηση των τελικών καταναλωτών των προϊόντων. Βέβαια αξίζει να σημειωθεί ότι το κόστος της τεχνολογίας του blockchain μπορεί να είναι αποτρεπτικό για μικρομεσαίες επιχειρήσεις.

Παραδείγματα τέτοιων εφαρμογών είναι:

- Το Ligero παρέχει ελαφριά, κλιμακούμενα πρωτόκολλα για ασφαλή υπολογισμούς πολλαπλών μερών και αποδείξεις μηδενικής γνώσης, παρέχοντας μια πλατφόρμα υψηλής ικανότητας για τη διευκόλυνση της αποκεντρωμένης συνεργασίας τόσο εντός όσο και εκτός blockchain. Η πλατφόρμα καθιστά δυνατή την ολοκλήρωση εμπιστευτικών συναλλαγών, ιδιωτικών έξυπνων συμβάσεων, ασφαλείς δημοπρασίες για αποκεντρωμένες ανταλλαγές, ενεργοποιεί επαληθεύσιμες δυνατότητες μηχανικής μάθησης, και καθοδηγείται από μια ομάδα ειδικών στην κρυπτογραφία, με εμπειρία δεκαετιών.
- Το Civic είναι ένα οικοσύστημα που βασίζεται σε blockchain που δίνει στα άτομα πληροφορίες για το ποιος έχει τις πληροφορίες τους. Οι χρήστες της εταιρείας συνάπτουν έξυπνα συμβόλαια, όπου αποφασίζουν ποιος μπορεί να μοιραστεί τα προσωπικά τους στοιχεία και πόσο. Εάν το συμβόλαιο σπάσει ή μια μη εξουσιοδοτημένη πηγή προσπαθήσει να αποκτήσει πρόσβαση σε προσωπικά δεδομένα, το άτομο ειδοποιείται αμέσως.
- Το οικοσύστημα ταυτότητας Sovrin της Evernym επιτρέπει στα άτομα να διαχειρίζονται την ταυτότητά τους σε όλο τον ιστό χρησιμοποιώντας τεχνολογία κατανεμημένης λογιστικής. Το Sovrin αποθηκεύει ιδιωτικές πληροφορίες, λειτουργεί ως μέσο επικοινωνίας μεταξύ του ατόμου και οντοτήτων που επιθυμούν ιδιωτικές πληροφορίες και επαληθεύει τις πληροφορίες ως αληθείς σε πραγματικό χρόνο.
- Η πλατφόρμα συμμόρφωσης της Ocular για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες αξιοποιεί την ασφάλεια με δυνατότητα blockchain για να διασφαλίσει ότι τα δεδομένα δεν μπορούν να χειραγωγηθούν. Η τεχνολογία χρησιμοποιεί βιομετρικά συστήματα για τη σάρωση των προσώπων ατόμων που υποβάλλουν αίτηση για διαβατήρια, άδειες οδήγησης και άλλες κρατικές ταυτότητες. Με την προβολή βιομετρικών συστημάτων σε blockchains, οι κυβερνήσεις μπορούν πιο εύκολα να πιάσουν κλέφτες ταυτότητας που πλαστογραφούν πλαστά διαβατήρια, πιστοποιητικά και ταυτότητες από άλλες χώρες.

3.4 Blockchain για ασύρματα δίκτυα

Οι ασύρματες εφαρμογές οι οποίες στηρίζουν την καθημερινότητα μας, όπως για παράδειγμα οι ευρυζωνικές συνδέσεις στο Διαδίκτυο, τα smartphones και το GPS (Jabbar et al, 2022. Jabbar et al, 2021) απαιτούν ραδιοφάσμα δηλαδή ένα φάσμα ραδιοκυμάτων, για τη μεταφορά πληροφοριών. Καθημερινά λοιπόν απαιτούνται διαφορετικά καθεστώτα διαχείρισης φάσματος για τη βελτιστοποίηση των πλεονεκτημάτων τους, επιβάλλοντας την όλο και πιο αποτελεσματική χρήση τους ελαχιστοποιώντας παράλληλα τις παρεμβολές μεταξύ των καταναλωτών (Weissetal, 2019).

Το παραδοσιακό καθεστώς διαχείρισης φάσματος έχει δύο σημαντικά μειονεκτήματα. Πρώτον, μεγάλα τμήματα του αδειοδοτημένου φάσματος υποχρησιμοποιούνται. Δεύτερον, αυτό το καθεστώς διαχείρισης φάσματος εντολών και ελέγχου αργεί να ανταποκριθεί στις αλλαγές της αγοράς και της τεχνολογίας (Anker, 2017). Η ανίχνευση φάσματος (Ariyarathna et al, 2019), η υποστήριξη δευτερευουσών αγορών συναλλαγών φάσματος , η κοινή χρήση τους και η θέσπιση και η σωστή επιβολή πολιτικών χρήσης τους είναι όλα πιθανά σημεία που η blockchain τεχνολογία μπορεί να αλλάξει τον τομέα της διαχείρισης φάσματος , παραδείγματα των οποίων αναφέρουμε παρακάτω.

Η τεχνολογία Blockchain μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός ασφαλούς συστήματος ανίχνευσης φάσματος καθώς και για την ενεργοποίηση της συνεργατικής ανίχνευσης , συστήματα που βελτιώνουν την ακρίβεια των συστημάτων φάσματος. Οι πάροχοι δικτύων κινητής τηλεφωνίας μπορούν να χρησιμοποιήσουν την ανίχνευση φάσματος για να συνδυάσουν τις διαθέσιμες κενές συχνότητες με τις αδειοδοτημένες συχνότητες για να ενισχύσουν τη χωρητικότητα του δικτύου καλύπτοντας έτσι τις κενές θέσεις. Η συνεργατική ανίχνευση, η οποία περιλαμβάνει τη σύντηξη των ευρημάτων ανίχνευσης από έναν αριθμό δευτερευόντων αισθητήρων ή χρηστών, μπορεί να εξασφαλίσει την αποτελεσματικότητα των αποτελεσμάτων ανίχνευσης φάσματος. Το blockchain χρησιμοποιήθηκε για πρώτη φορά ως σύστημα πληρωμών peer-to-peer. Ως αποτέλεσμα, προσφέρεται και στη δημιουργία ενός συστήματος πληρωμών πλήρους φάσματος που βασίζεται σε ψηφιακό νόμισμα που μπορεί να μετατραπεί γρήγορα σε νόμισμα fiat (παραστατικό – χάρτινο χρήμα).

Επιπρόσθετα, η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την ολοκλήρωση των πολλών λειτουργιών μιας βάσης δεδομένων γεωεντοπισμού καθώς και των αναγκών διαχείρισης φάσματος. Η χρήση του blockchain (Tangsen et al, 2020) για την ενεργή αποθήκευση πληροφοριών σχετικά με μη κατειλημμένες ζώνες φάσματος και γεωγραφικές

τοποθεσίες χρηστών αναμένεται να αυξήσει επίσης την πρόσβαση στο φάσμα και την αποτελεσματικότητα χρήσης.

Η διαχείριση φάσματος με χρήση blockchains είναι μια νέα εφαρμογή με πολλές ευκαιρίες και προκλήσεις. Επειδή το blockchain είναι μια τεχνολογία βάσης δεδομένων, μπορεί να χρησιμοποιηθεί για τη δημιουργία μιας ενοποιημένης μεθόδου στην οποία οι τεχνικές ανίχνευσης φάσματος και η τεχνολογία της βάσης δεδομένων γεωεντοπισμού λειτουργούν παράλληλα. Ένα πιο ισχυρό δυναμικό πλαίσιο διαχείρισης φάσματος θα προκύψει από το συνδυασμό αυτών των δύο στρατηγικών πρόσβασης στο φάσμα.

Για να διευκολυνθεί η ενσωμάτωση του blockchain και του WN, πολλοί ερευνητές έχουν προτείνει αρκετές προόδους αιχμής στο WN με δυνατότητα blockchain. Για παράδειγμα, οι Nguyenetal (2020) παρουσίασαν μια εκτενή συζήτηση σχετικά με τις διαφορετικές ευκαιρίες που έχει φέρει το blockchain στον κόσμο του 5G και των ασύρματων δικτύων μελλοντικής γενιάς. Ωστόσο, δεν έχουν συζητήσει τις κρίσιμες ελλείψεις του blockchain στο WN, όπως τα τρωτά σημεία ασφαλείας και τα ζητήματα απορρήτου. Περαιτέρω, ο Wangetal (2021) εισήγαγε μια ολοκληρωμένη μελέτη του πλαισίου που βασίζεται στο δίκτυο ραδιοπρόσβασης της αλυσίδας μπλοκ (B-RAN) για το 6G. Επεξεργάστηκαν περαιτέρω την αναγκαιότητα ενός μηχανισμού συναίνεσης, των ψηφιακών συμβάσεων, της ανταλλαγής δεδομένων μεταξύ των δικτύων και ενός μοντέλου εμπιστοσύνης στο WN για τη διατήρηση του απορρήτου των πιστοποιημένων χρηστών. Δυστυχώς, το μεγαλύτερο μέρος της ενοποίησης μεταξύ blockchain και WN καθορίζει τις επιμέρους πτυχές των ζητημάτων ασφάλειας και απορρήτου στο WN. Πολλοί ερευνητές έχουν προτείνει λύσεις που βασίζονται σε blockchain για ασφαλή ασύρματη επικοινωνία. Ωστόσο, ελάχιστοι από αυτούς συζήτησαν σε βάθος θέματα ασφάλειας και τα αντίμετρα τους. Επομένως, υπάρχει η απαίτηση να ακολουθηθεί ένας προληπτικός τρόπος και να ενοποιηθούν οι αναδυόμενες ερευνητικές εργασίες για ζητήματα ιδιωτικότητας και ασφάλειας των WN. Ως εκ τούτου, αυτό το έγγραφο υπογραμμίζει την πτυχή της ασφάλειας και της ιδιωτικής ζωής και την επίδραση της στα μελλοντικά WN με πιθανές λύσεις με την προσφυγή στην τεχνολογία blockchain.

3.5 Blockchain για το Διαδίκτυο των πραγμάτων(IoT)

Το Διαδίκτυο των Πραγμάτων (IoT) Mukhtar et al, 2021. Krichen&Alroobaea, 2019. Jabbaretal, 2019) είναι η σύνδεση έξυπνων συσκευών για συλλογή δεδομένων και έξυπνη λήψη αποφάσεων. Ωστόσο, το IoT είναι επιρρεπές σε κινδύνους για το απόρρητο και την ασφάλεια λόγω της απουσίας εγγενών μέτρων ασφαλείας. Εκεί ουσιαστικά που κερδίζει σε επικοινωνία, χάνει δυστυχώς σε ασφάλεια καθιστώντας πιο ριψοκίνδυνο και η λύση αυτού του προβλήματος αποτελεί μια σημαντική πρόκληση. Ταυτόχρονα θέματα μπορούν να εμφανιστούν και όσον αφορά την εμπιστευτικότητα των δεδομένων και τον έλεγχο ταυτότητας.

Τα δεδομένα του IoT θα μπορούσαν να παραβιαστούν και να χρησιμοποιηθούν καταχρηστικά εάν δεν εδραιωθεί η ασφάλεια των δεδομένων Η ακεραιότητα των δεδομένων είναι ένα άλλο ζήτημα για το IoT. Τα συστήματα υποστήριξης αποφάσεων είναι μια από τις πιο σημαντικές εφαρμογές IoT. Ως αποτέλεσμα, η προστασία του συστήματος από επιθέσεις που επιχειρούν να εισαγάγουν ψευδή μέτρα και επομένως, να επηρεάσουν τους παράγοντες και κατ' επέκταση τη λήψη αποφάσεων, είναι κρίσιμη. Το Blockchain μπορεί να βοηθήσει στην επίλυση σημαντικών προβλημάτων ασφάλειας στο IoT με τη λειτουργία «ασφάλεια από κατασκευής» (Li et al, 2020. Peši´c et al, 2019).

Το Blockchain είναι το τελευταίο κομμάτι του παζλ αφού τα εγγενή, αξιόπιστα, αυτόνομα και αποκεντρωμένα χαρακτηριστικά του το καθιστούν κατάλληλο για χρήση σε διάφορα σενάρια. Η τεχνολογία blockchain, για παράδειγμα, μπορεί να αποθηκεύει ένα μόνιμο αρχείο έξυπνων gadget (Kshetri, 2017. Dorri et al, 2017). Επιπλέον, η εφαρμογή έξυπνων συμβάσεων μπορεί να επιτρέψει στις έξυπνες συσκευές να λειτουργούν αυτόνομα, αποφεύγοντας την ανάγκη για συνεχή επιτήρηση είτε μέσω ανθρώπινου ελέγχου είτε από κάποια κεντρική εξουσία. Επιπλέον, το blockchain μπορεί να δημιουργήσει ένα ασφαλές μέσο για τις έξυπνες συσκευές να επικοινωνούν μεταξύ τους και έτσι να πετύχουμε τη διαλειτουργικότητα ανάμεσα στα μέρη που αποτελούν το σύστημα του IoT (Suliman et al, 2019).

Οι ερευνητές Wörner von Bomhard ανέπτυξαν έναν μηχανισμό που θα επέτρεπε στους αισθητήρες να ανταλλάσσουν το Bitcoin για δεδομένα. Κάθε κόμβος έχει μια μοναδική διεύθυνση που αντιστοιχεί στο public key (δημόσιο κλειδί), έννοια που είδαμε στο μηχανισμό λειτουργίας του Bitcoin. Όταν ένας χρήστης χρειάζεται δεδομένα από έναν αισθητήρα αφού τον εντοπίσει σε ένα αποθετήριο αισθητήρων, στέλνει μια συναλλαγή που κατευθύνεται στο δημόσιο κλειδί αυτού του αισθητήρα. Ο αισθητήρας θα απαντήσει

στέλνοντας μια συναλλαγή που περιέχει δεδομένα στον πελάτη. Ακόμα υπάρχει και ο μηχανισμός Enigma που προσφέρει μια ακόμη ενδιαφέρουσα λύση χρησιμοποιώντας μια εντελώς συγκρίσιμη έννοια - τη διανομή δεδομένων σε πολλούς κόμβους, ενώ διαχωρίζει τα δεδομένα από τις αναφορές του. Επιπλέον, εκτός από το ότι καθιστά δύσκολη την ανακατασκευή της αρχικής μορφής δεδομένων, το Enigma προσφέρει ένα επιπλέον επίπεδο προστασίας κρυπτογραφώντας τέτοια κομμάτια δεδομένων Όλα αυτά τα χαρακτηριστικά καθιστούν το Enigma, ένα δίκτυο peer-to-peer που επιτρέπει σε πολλούς συμμετέχοντες να αποθηκεύουν και να επεξεργάζονται δεδομένα ταυτόχρονα, διατηρώντας παράλληλα το απόρρητο.

Ενδεικτικά παραδείγματα τέτοιων εφαρμογών είναι τα εξής:

- Το HYPR αποτρέπει τους κινδύνους κυβερνοασφάλειας στις συσκευές IoT με τις αποκεντρωμένες λύσεις διαπιστευτηρίων του. Αφαιρώντας τους κωδικούς πρόσβασης από έναν κεντρικό διακομιστή, ενώ χρησιμοποιεί βιομετρικές λύσεις και λύσεις χωρίς κωδικό πρόσβασης, η εταιρεία καθιστά τις συσκευές IoT ουσιαστικά δύσκολα έως και απίθανα παραβιάσιμες.
- Το Xage είναι η πρώτη στον κόσμο πλατφόρμα κυβερνοασφάλειας με δυνατότητα blockchain για εταιρείες IoT. Η τεχνολογία διαχειρίζεται δισεκατομμύρια συσκευές ταυτόχρονα και μπορεί ακόμη και να αυτοδιαγνώσει και να θεραπεύσει πιθανές παραβιάσεις. Το Xage χρησιμοποιείται κυρίως από εταιρείες IoT στις βιομηχανίες μεταφορών, ενέργειας και μεταποίησης.
- Βασισμένο σε blockchain, το Helium's People's Network είναι το μεγαλύτερο συνεχόμενο ασύρματο δίκτυο στον κόσμο που συνδέει και μεταφέρει πληροφορίες μεταξύ συσκευών IoT. Το δίκτυο είναι σε θέση να παρακολουθεί και να αναφέρει δεδομένα περιουσιακών στοιχείων σε πραγματικό χρόνο, ενισχύοντας τις προσπάθειες παρακολούθησης και διαχείρισης για έξυπνη γεωργία, έξυπνες πόλεις, έξυπνο νερό και logistics. Οι συσκευές hotspot συμβατές με το People's Network μπορούν ακόμη και να χρησιμοποιηθούν για την εξόρυξη κρυπτονομισμάτων HNT.

3.6 Blockchain για έξυπνα δίκτυα

Ένα έξυπνο δίκτυο (Zidi et al, 2022. Fang et al, 2011. Farhangi, 2099. Gungor et al, 2011) είναι ένα δίκτυο βασισμένο σε ψηφιακές επικοινωνίες που παρέχει αμφίδρομη ροή ηλεκτρικής ενέργειας και δεδομένων, καθώς και την αναγνώριση, αντίδραση και αποφυγή αλλαγών στη χρήση καθώς και την επίλυση άλλων δυσκολιών. Τα τρέχοντα έξυπνα δίκτυα ενσωματώνουν τεχνικές επικοινωνίας και ελέγχου στα δίκτυα ισχύος, επιτρέποντας σημαντικά κέρδη στην ενεργειακή απόδοση και την ασφάλεια του συστήματος. Οι παραδοσιακές συγκεντρωτικές τεχνικές διαχείρισης έξυπνων δικτύων θέτουν σημαντικά εμπόδια. Για παράδειγμα, η κεντρική μέθοδος ελέγχου δημιουργεί ένα επικίνδυνο ενιαίο σημείο αστοχίας για ολόκληρο το δίκτυο. Επιπλέον, πολλά ζητήματα ασφάλειας αυξάνονται και οι εξωτερικές επιθέσεις ασφαλείας θα μπορούσαν να οδηγήσουν σε σημαντικές οικονομικές απώλειες.

Για να ξεπεραστούν αυτοί οι περιορισμοί, η χρήση τεχνολογιών blockchain θεωρείται μια καλή επιλογή σε πολλά ερευνητικά και βιομηχανικά έργα (Goranovic et al, 2017. Xie et al, 2019. Andoni et al, 2019. Πράγματι, η χρήση blockchain για έξυπνα δίκτυα μπορεί να έχει τα ακόλουθα πλεονεκτήματα:

• Το blockchain έχει τη δυνατότητα να μετατρέψει την κεντρική διαχείριση δικτύου σε κατανεμημένη έξυπνη διαχείριση.

• Όσον αφορά τις συναλλαγές ενέργειας, ένα έξυπνο δίκτυο με τεχνολογία blockchain μπορεί να επιτύχει τη βέλτιστη ροή δεδομένων και ταμειακή ροή.

• Λόγω της αποκέντρωσής του και της ανοχής σε σφάλματα, το blockchain μπορεί να βελτιώσει δραματικά το απόρρητο και την ασφάλεια των δικτύων ηλεκτρικής ενέργειας.

Η ενσωμάτωση κρυπτονομισμάτων σαν μέθοδο πληρωμής είναι μια από τις πιο σημαντικές εφαρμογές του blockchain όσον αφορά τα έξυπνα δίκτυα.

Σημαντική είναι και η χρήση blockchain και στην τεχνολογία των ηλεκτρικών οχημάτων. Τα ηλεκτρικά οχήματα (Li et al, 2019. Das et al, 2020) μπορούν να θεωρηθούν ως τερματικά κινητού δικτύου ηλεκτρικής ενέργειας που εκτελούν βασικές υπηρεσίες. Αυτή είναι γνωστή ως τεχνολογία V2G και έχει τη δυνατότητα να αυξήσει την αξιοπιστία, την αποτελεσματικότητα και τη σταθερότητα του ηλεκτρικού δικτύου. Τα ηλεκτρικά οχήματα όμως δεν συνδέονται σωστά με τα έξυπνα δίκτυα και υπάρχουν ορισμένα ζητήματα, όπως οι ελλείψεις ενέργειας, οι κίνδυνοι ασφάλειας και οι διαρροές δεδομένων. Σε αυτό το πλαίσιο, τα υπερβολικά φορτία φόρτισης και η ασταθής τάση στα ηλεκτρικά οχήματα

μπορούν να αντιμετωπιστούν με την τεχνολογία blockchain και με ένα αποδοτικότερο , οικονομικά, τρόπο ειδικά μέσω των Smart Contract (Liu et al, 2018).

Αν και η χρήση της τεχνολογίας blockchain για έξυπνα δίκτυα φαίνεται να είναι πολλά υποσχόμενη, όπως αποδείχθηκε προηγουμένως, εξακολουθούν να υπάρχουν εμπόδια στην πλήρη μετατροπή σε αυτή τη νέα τεχνολογία. Η εφαρμογή blockchain στο έξυπνο δίκτυο απαιτεί μεγάλα έξοδα υποδομής, τα οποία πιθανότατα θα κάνουν τους φορείς εκμετάλλευσης δικτύων να διστάζουν να ενσωματώσουν blockchain στις δομές δικτύου τους.

Ενδεικτικό παράδειγμα αποτελεί η BAS Nederland, που ήταν η πρώτη εταιρεία που χρησιμοποίησε το Bitcoin ως πληρωμή για λογαριασμούς ενέργειας. Αυτό ώθησε πολλές επιπλέον εταιρείες να αναπτύξουν υπηρεσίες χρέωσης και μέτρησης βασισμένες σε blockchain, με αρκετές από αυτές να προσφέρουν κίνητρα στους καταναλωτές που πληρώνουν με κρυπτονομίσματα.

3.7 Blockchain για κυβερνητικές υπηρεσίες

Κεντρικό σημείο και σκοπός των πρωτοβουλιών της ηλεκτρονικής διακυβέρνησης είναι να παρέχουν δημόσιες υπηρεσίες που είναι πιο απλές, κατανεμημένες και προσαρμοσμένες στις ανάγκες των κατοίκων (Molnar et al, 2015). Φυσικά, αυτό δεν έχει καταφέρει ποτέ να αλλάξει πραγματικά τις λειτουργίες των κρατικών υπηρεσιών σε ικανοποιητικό βαθμό , όσον αφορά την τήρηση αρχείων και τη διαχείριση τους . Ένα από τα πιο σημαντικά οφέλη της τεχνολογίας blockchain είναι η ικανότητα προώθησης άμεσων αλληλεπιδράσεων μεταξύ κρατικών υπηρεσιών, πολιτών και επιχειρήσεων. Η συνδεσιμότητα και η αλληλεπίδραση που δημιουργείται καταφέρνει να επαναπροσδιορίσει τον τρόπο με τον οποίο οι κυβερνήσεις αλληλεπιδρούν με τα άτομα και μεταξύ τους.

Οι κυβερνήσεις ενδέχεται να χρησιμοποιήσουν αυτήν την τεχνολογία για να αναλάβουν εποπτικές λειτουργίες σε μια υποδομή που βασίζεται σε blockchain. Το Blockchain έχει τη δυνατότητα να εξαλείψει ένα σημαντικό μέρος των διοικητικών λειτουργιών που διαδραματίζουν επί του παρόντος οι κυβερνήσεις στην κοινωνία, γεγονός που καθιστά αναγκαία μια αλλαγή στην κατεύθυνση και τη λειτουργία της παροχής υπηρεσιών. Αυτό έχει τη δυνατότητα να αλλάξει τα υπάρχοντα θεσμικά πλαίσια και κατά συνέπια τους νόμους αλλά και τους ίδιους τους θεσμούς (Martinovic et al, 2017).

Στη συνέχεια, παρέχουμε μια σύντομη επισκόπηση της υιοθέτησης της τεχνολογίας blockchain από διαφορετικές κυβερνήσεις ανά τον κόσμο:

• Κίνα: η κινεζική κυβέρνηση δήλωσε ότι θα αρχίσει να χρησιμοποιεί blockchain για την έκδοση τιμολογίων και τη συλλογή φόρων.
• Ιαπωνία: Η ιαπωνική κυβέρνηση ανακοίνωσε ότι θα πειραματιστεί με ένα σύστημα βασισμένο σε blockchain για το χειρισμό κρατικών διαγωνισμών. Η τεχνολογία συνίσταται στο να επιτρέπει στους χρήστες να λαμβάνουν πληροφορίες ηλεκτρονικά.
• ΗΠΑ: η κυβέρνηση των ΗΠΑ αναζητούσε εργολάβους για να αξιολογήσει πώς μπορεί να ενσωματωθεί η τεχνολογία blockchain στον μηχανισμό υποβολής προσφορών συμβάσεων.
• Βρετανία: Η ενσωμάτωση της τεχνολογίας blockchain σε κυβερνητικές λειτουργίες στο Ηνωμένο Βασίλειο προσφέρθηκε ως μια ενδιαφέρουσα μελέτη περίπτωσης. Η κύρια ιδέα πίσω από τη χρήση του blockchain είναι η αυτοματοποίηση της αίτησης και πληρωμής των κρατικών επιχορηγήσεων και προνομίων.
• Εσθονία: η τεχνολογία blockchain έχει ενσωματωθεί από την κυβέρνηση της Εσθονίας σε επίσημες ανακοινώσεις, ψηφιακά δικαστικά αρχεία, μητρώα ιδιοκτησίας, μητρώα διαδοχής, μητρώα επιχειρήσεων κ.λπ.
• Σουηδία: η σουηδική κυβέρνηση έχει αρχίσει να διερευνά τη χρήση της τεχνολογίας blockchain για την υποστήριξη των συναλλαγών ακινήτων.

Απαιτείται περισσότερη έρευνα σχετικά με τις επιρροές του blockchain στη διεπαφή τεχνολογίας – ιδρύματος. Η υιοθέτηση της τεχνολογίας blockchain για δημόσιες υπηρεσίες θα μπορούσε να οδηγήσει όχι μόνο σε αλλαγή της λειτουργίας των κυβερνήσεων, αλλά και σε απώλεια θέσεων εργασίας και σε επιδείνωση του ψηφιακού χάσματος που δημιουργείται περισσότερο και λόγω ηλικίας των πολιτών. Για να ελαχιστοποιηθούν οι απρόβλεπτες επιπτώσεις κατά τη χρήση αυτής της τεχνολογίας στον δημόσιο τομέα, οι ερευνητές θα πρέπει να διεξάγουν έρευνα για να συντάξουν μια λίστα με αυτές τις επιπτώσεις.

Παραδείγματα τέτοιων εφαρμογών είναι το e-Estonia και το Smart Dubai. Η Εσθονία ήταν από τις πρώτες χώρες που πειραματιζόταν με την τεχνολογία ήδη από το 2008, όταν και έκανε τα πρώτα της βήματα. Σήμερα η κυβέρνηση έχει δημιουργήσει μια πλατφόρμα την e-Estonia, η οποία διαθέτει πάνω από το 99% των κρατικών υπηρεσιών που θα χρειαστεί ένας πολίτης άμεσα διαθέσιμο στο διαδίκτυο, προσβάσιμο από κάθε είδους συσκευή με πρόσβαση σε αυτό. Ήδη πάνω από το 44% του πληθυσμού χρησιμοποίει την πλατφόρμα για ηλεκτρονική ψηφοφορία στη διαδικασία των εκλογών. Σημαντικά ποσοστά είναι και το 98% των φορολογικών δηλώσεων που γίνονται online καθώς και ότι το 98% του πληθυσμού της χώρας έχουν ψηφιακή ταυτότητα. Η Εσθονία επενδύει συνεχώς στο Blockchain και σε καινοτόμες υπηρεσίες βάζοντας τέλος στην γραφειοκρατία και στους αργούς ρυθμούς που ταλανίζουν τους κρατικούς μηχανισμούς. Επίσης, η κυβέρνηση των Ηνωμένων Αραβικών

Εμιράτων (ΗΑΕ) δημιούργησε μια πλατφόρμα με όνομα Smart Dubai. Στόχος του προγράμματος είναι η αξιοποίηση του Blockchain και η ψηφιοποίηση κρατικών διαδικασιών σε ομοσπονδιακό επίπεδο. Με την υιοθέτηση της τεχνολογίας, εκτιμάτε ότι τα ΗΑΕ θα σώσουν 11 δις σε συναλλαγές και έγγραφα, 398 εκατομμύρια έντυπα ετησίως και 77 εκατομμύρια ώρες εργασίας ετησίως. Επιπλέον θα μειωθούν κατά 1,6 δισεκατομμύρια τα χιλιόμετρα οδήγησης καθώς οι πολίτες θα μπορούν να κάνουν τις απαραίτητες διαδικασίες από το σπίτι.

3.8 Blockchain για τον στρατό και την άμυνα

Στρατιωτικοί ηγέτες που αγκάλιασαν την τεχνολογία στον κυβερνοχώρο στη δεκαετία του 1990 και στις αρχές της δεκαετίας του 2000 προσπαθούν τώρα να αντιμετωπίσουν τα τεράστια τρωτά σημεία που παρήγαγαν αυτές οι ίδιες ψηφιακές τεχνολογίες (Karaman et al, 2016. Armitage et al, 2016). Δεκαετίες πειρατείας και εκμετάλλευσης συστημάτων κυβερνοασφάλειας έχουν επανειλημμένα αποδείξει πώς ένας αποφασισμένος εισβολέας στον κυβερνοχώρο μπορεί να θέσει σε κίνδυνο στρατιωτικά και πολιτικά δίκτυα τα οποία αποτελούν τα πιο κομβικά και "ευαίσθητα" ως προς το περιεχόμενο τους, για ένα Κράτος.
Η απειλή των εξελιγμένων οπλικών συστημάτων που βλάπτονται ή απενεργοποιούνται από μη κινητικές κρούσεις έχουν αναγκάσει τους στρατούς να αναπτύξουν μια μακροπρόθεσμη και ιδανικά οικονομικά αποδοτική άμυνα για στρατιωτικά συστήματα. Το Blockchain έχει τη δυνατότητα να μετατρέψει, τα τρωτά σημεία ασφαλείας ορισμένων συστημάτων στον κυβερνοχώρο, από ένα μοντέλο ευπάθειας στο οποίο ένας εισβολέας χρειάζεται να παραβιάσει μόνο έναν κόμβο για να παραβιάσει ολόκληρο το σύστημα, σε ένα μοντέλο ευπάθειας στο οποίο ένας κακόβουλος παράγοντας δεν μπορεί να εκμεταλλευτεί ένα μόνο σημείο αποτυχίας και θα πρέπει να προσπαθήσει περισσότερο και με περισσότερα μέσα. Βέβαια οι στρατιωτικές χρήσεις του Blockchain αξίζει να σημειωθεί ότι δεν έχουν ακόμη δοκιμαστεί σε ευρύ φάσμα λειτουργίας. Η υιοθέτηση του blockchain στον στρατιωτικό τομέα μπορεί να καλύπτει τις ακόλουθες πτυχές: (1) ανίχνευση εισβολής, (2) παρακολούθηση υποδομής, (3) διαχείριση μαχών, (4) Διαχείριση UAV, (5) διαχείριση της εφοδιαστικής αλυσίδας, (6) κρυπτογραφημένες επικοινωνίες.
Η εργασία που παρουσιάζεται στο Lilly & Lilly (2021) προτείνει μια ενδιαφέρουσα σύγκριση της υιοθέτησης της τεχνολογίας blockchain από τρεις από τις ισχυρότερες ένοπλες δυνάμεις στον κόσμο:

• ΗΠΑ: εκτός της σφαίρας των κρυπτονομισμάτων, οι στρατιωτικές συνομιλίες των ΗΠΑ επικεντρώθηκαν στη βελτίωση της ανθεκτικότητας δεδομένων, με την προϋπόθεση ότι ο

αμερικανικός στρατός θα μπορούσε να εξαλείψει τον παραβιασμό και τη διαφθορά δεδομένων ως απειλές για τα δεδομένα του και ότι η τεχνολογία blockchain μπορεί να λειτουργήσει ως ασφάλεια στον κυβερνοχώρο ασπίδα.

• Ρωσία: το ρωσικό Υπουργείο Άμυνας ανακοίνωσε τη δημιουργία ενός ερευνητικού εργαστηρίου με αποστολή τη δημιουργία ενός συστήματος blockchain για τον εντοπισμό και τον μετριασμό των επιθέσεων στον κυβερνοχώρο σε ζωτικής σημασίας στρατιωτικές ψηφιακές υποδομές.

• Κίνα: το ενδιαφέρον για στρατιωτικές εφαρμογές της τεχνολογίας blockchain στην Κίνα επικεντρώθηκε στη διαχείριση εξοπλισμού, την επαγγελματική μάθηση, την επιμελητεία και τη μετατροπή των εμπορικών τεχνολογιών πληροφοριών σε αμυντικά προγράμματα.

Φυσικά, όπως προαναφέραμε οι δυνατότητες του blockchain δεν φαίνεται να είναι εντελώς έτοιμες για χρήση. Η αμυντική εφοδιαστική αλυσίδα και η ασφάλεια δεδομένων είναι πιθανό να είναι οι εφαρμογές που θα εφαρμοστούν στο εγγύς μέλλον. Από την άλλη πλευρά, η υιοθέτηση του blockchain από τους ισχυρότερους στρατούς του κόσμου είναι κάπως παράδοξη. Αξίζει να σημειωθεί και το παράδοξο της χρήσης του blockchain το οποίο έχει ως σκοπό τη δυνατότητα να εγγυάται περισσότερες ατομικές ελευθερίες που όμως προς το παρόν φαίνεται να δελεάζει και τους πιο συγκεντρωτικούς ανθρώπινους οργανισμούς οι οποίοι δεσμεύονται να χρησιμοποιούν την ίδια τεχνολογία για να δημιουργήσουν μια αποκεντρωμένη τεχνολογία για στρατιωτικές και αμυντικές εφαρμογές.

Ενδεικτικά παραδείγματα είναι τα εξής:

Η DARPA προσπαθεί να αναπτύξει μια ασφαλή και αξιόπιστη πλατφόρμα πληροφοριών βασισμένη στην τεχνολογία blockchain. Θα ήταν ένα ασφαλές σύστημα υπηρεσίας πληροφοριών ικανό να προστατεύει αποτελεσματικά ευαίσθητα δεδομένα και να αποτρέπει την παραβίαση.

Τον Απρίλιο του 2016, το Υπουργείο Άμυνας των ΗΠΑ και οι σύμμαχοί του στο ΝΑΤΟ άρχισαν να δίνουν προσοχή στην πιθανή εφαρμογή της τεχνολογίας blockchain στην άμυνα, συμπεριλαμβανομένης της αυτόματης εκτέλεσης έξυπνων συμβολαίων, της ασφαλούς αποθήκευσης ευαίσθητων αρχείων και της μείωσης σφαλμάτων και διακοπών κατά την εκτέλεση αμυντικών συμβολαίων . Επιπλέον, η τεχνολογία blockchain μπορεί επίσης να εφαρμοστεί στην απόκριση έκτακτης ανάγκης όταν συμβαίνουν καταστροφές και στη βελτίωση της διαφάνειας της προμήθειας πρώτων υλών στην αλυσίδα εφοδιασμού και στη μεταφορά φορτηγίδων στη διαδικασία logistics.

Τον Ιούνιο του 2017, το Ναυτικό των ΗΠΑ χρησιμοποίησε την τεχνολογία blockchain για να βελτιώσει την ασφάλεια των συστημάτων κατασκευής πρόσθετων. Κατέγραψαν όλη τη

διαδικασία σχεδιασμού εξαρτημάτων, κατασκευής πρωτοτύπων, δοκιμών, παραγωγής και τελικής επεξεργασίας, έτσι ώστε οι χρήστες να μπορούν να εξετάζουν συγκεκριμένα δεδομένα και να δίνουν ειδοποιήσεις σε περιπτώσεις ζημιάς εξαρτήματος ή στο τέλος του κύκλου ζωής τους.

Το Ρωσικό Κβαντικό Κέντρο και η Ρωσική Ακαδημία Επιστημών δοκίμασαν με επιτυχία το πρώτο σύστημα κβαντικής αλυσίδας μπλοκ.

Τον Μάιο του 2017, η εταιρεία Technology and Manufacturing Company με έδρα την Ιντιάνα, που χρηματοδοτείται από την DARPA, χρησιμοποίησε την τεχνολογία blockchain για να αναπτύξει μια «απρόσιτη πλατφόρμα ανταλλαγής μηνυμάτων και συναλλαγών για τον στρατό. Αυτή η πλατφόρμα διαχωρίζει τη δημιουργία και τη μετάδοση πληροφοριών για να διασφαλίσει ότι τα δεδομένα που αποστέλλονται και λαμβάνονται δεν μπορούν να παραβιαστούν και επιτρέπει την ασφαλή επικοινωνία μεταξύ του αρχηγείου και των επίγειων δυνάμεων, καθώς και μεταξύ του Υπουργείου Άμυνας και αξιωματούχων πληροφοριών. Τον Ιούλιο του 2019, ως μέρος της στρατηγικής ψηφιακού εκσυγχρονισμού του DOD, η DARPA άρχισε να αξιοποιεί την τεχνολογία blockchain για να δημιουργήσει μια πιο αποτελεσματική, ισχυρή και ασφαλή πλατφόρμα επικοινωνίας, προκειμένου να διευκολύνει την ασφαλή μετάδοση πληροφοριών για οποιοδήποτε σύστημα εντολών, ελέγχου και επικοινωνίας. Προσωπικό για την παρακολούθηση των συναλλαγών μέσω ενός καναλιού κατανεμημένου λογιστικού και εγγυάται την ασφάλεια επικοινωνίας μεταξύ του αρχηγείου και των επίγειων δυνάμεων και μεταξύ του Υπουργείου Άμυνας και αξιωματούχων πληροφοριών στο μέλλον.

ΚΕΦΑΛΑΙΟ 4

ΣΥΓΧΡΟΝΕΣ ΠΛΑΤΦΟΡΜΕΣ BLOCKCHAIN

Ο όρος blockchain χρησιμοποιήθηκε αρχικά για να περιγράψει το κατανεμημένο σύστημα τήρησης αρχείων που χρησιμοποιείται από το πρωτόκολλο Bitcoin, αλλά τώρα χρησιμοποιείται γενικά για να περιγράψει οποιεσδήποτε τεχνολογίες κατανεμημένου καθολικού που είναι εμπνευσμένες από το σχεδιασμό blockchain του Bitcoin. Ο όρος Τεχνολογία Κατανεμημένης Λογιστικής (DLT) ή Αναπαραγόμενο, Κοινόχρηστο Καθολικό αναφέρεται σε ένα κατανεμημένο σύστημα τήρησης αρχείων που είναι μόνο προσαρτημένο και ασφαλίζεται μέσω πρωτοκόλλων συναίνεσης. Ο όρος ιδιωτικό blockchain (permissioned ledger) αναφέρεται στο Blockchain που απαιτεί έλεγχο ταυτότητας των ταυτοτήτων των συμμετεχόντων και εξουσιοδότηση του επιπέδου άδειας πρόσβασης του συμμετέχοντος στο Blockchain. Ο όρος δημόσιο blockchain (καθολικό χωρίς άδεια) αναφέρεται σε Blockchain που δεν απαιτεί έγκριση ή εξουσιοδότηση για πρόσβαση .

Η τεχνολογία Blockchain είναι μια επανάσταση στο σύστημα αρχείων. Η τεχνολογία Blockchain μπορεί να ενσωματωθεί σε πολλούς τομείς. Τα πρωτόκολλα blockchain διευκολύνουν τις επιχειρήσεις να χρησιμοποιούν μια νέα μέθοδο επεξεργασίας ψηφιακών συναλλαγών. Παραδείγματα είναι το σύστημα πληρωμών και το ψηφιακό νόμισμα, οι πωλήσεις πλήθους, οι αγορές προβλέψεων και τα γενικά εργαλεία διακυβέρνησης. Το Blockchain μπορεί να θεωρηθεί ως ένα αυτόματο συμβολαιογραφικό καθολικό. Το Blockchain έχει μεγάλη ποικιλία εφαρμογών, τόσο σε χρηματοοικονομικούς όσο και σε μη χρηματοοικονομικούς τομείς. Οι κύριες εφαρμογές του Blockchain περιλαμβάνουν κρυπτονομίσματα όπως το Bitcoin και πολλές άλλες πλατφόρμες όπως το Factom ως κατανεμημένο μητρώο, το Gems για αποκεντρωμένη ανταλλαγή μηνυμάτων, το Storj για την κατανεμημένη αποθήκευση cloud, κ.λπ. (Kuo et al, 2017).

Πολλές startups και εταιρείες έχουν αυτοπροσδιοριστεί ως πλατφόρμες blockchain ανοιχτού κώδικα. Μια εταιρεία blockchain επικεντρώνεται στην παροχή μεγαλύτερης επεκτασιμότητας και απρόσκοπτων διαδικασιών συναλλαγών για την αντιμετώπιση ψηφιακών περιουσιακών στοιχείων. Η ενσωμάτωση κατανεμημένων λογιστικών βιβλίων σε αυτές τις πλατφόρμες blockchain ανοιχτού κώδικα βοηθά σε διαφανή και αποτελεσματικό φόρτο εργασίας.

Μερικές Πλατφόρμες Blockchain είναι :

- Το **Hyperledger Fabric** είναι μία από τις κορυφαίες πλατφόρμες blockchain ανοιχτού κώδικα για την ανάπτυξη εφαρμογών ή λύσεων με αρθρωτή αρχιτεκτονική. Αυτή η εταιρεία blockchain επιτρέπει υπηρεσίες συναίνεσης και ιδιότητας μέλους αξιοποιώντας την τεχνολογία blockchain. Βοηθά να γίνουν οι οικονομικές συναλλαγές ευκολότερες, ταχύτερες και πιο προσιτές. Προωθεί ένα ευρύ φάσμα επιχειρηματικών χαρτοφυλακίων τεχνολογίας blockchain, συμπεριλαμβανομένων κατανεμημένων λογιστικών βιβλίων και πλαισίων.
- Η **Stellar** είναι μια κορυφαία πλατφόρμα blockchain που επικεντρώνεται στη δημιουργία, αποστολή και εμπορία ψηφιακών περιουσιακών στοιχείων και στο σχεδιασμό των χρηματοοικονομικών συστημάτων του κόσμου ώστε να συνεργάζονται σε ένα ενιαίο δίκτυο. Τα API και SDK συμβάλλουν στον μετασχηματισμό του κόσμου των οικονομικών με την τεχνολογία blockchain και τις υπηρεσίες μικροπληρωμών. Προσφέρει μια πλατφόρμα εξερεύνησης λογιστικών βιβλίων και αναλυτικών στοιχείων για αποτελεσματικά κατανεμημένα λογιστικά βιβλία με στατιστικά στοιχεία ψηφιακών περιουσιακών στοιχείων, 24ωρα στατιστικά λογιστικής, στατιστικά στοιχεία δικτύου και πολλά άλλα.
- Η **Ripple** είναι μία από τις βασικές πλατφόρμες blockchain ανοιχτού κώδικα με επιχειρηματικό αντίκτυπο στα ψηφιακά στοιχεία. Αξιοποιεί την τεχνολογία blockchain για λύσεις εταιρικού επιπέδου ώστε να είναι πιο γρήγορες, πιο διαφανείς και πιο αποδοτικές. Η εταιρεία blockchain προσφέρει αυτές τις λύσεις για την πηγή κρυπτογράφησης, τη διευκόλυνση των άμεσων πληρωμών και την προσέλκυση νέου κοινού για την επίτευξη καλύτερων εσόδων.
- Η **Klaytn** είναι μια από τις δημοφιλείς πλατφόρμες blockchain ανοιχτού κώδικα για το κοινό για να εργαστεί στο μετασύμπαν με ψηφιακά στοιχεία. Ο στόχος είναι να προσφέρει την απόδοση, την αποκέντρωση, την επεκτασιμότητα και τη διαλειτουργικότητα για ένα νέο επίπεδο στο μετασύμπαν. Ανοικοδομεί την εταιρεία blockchain σε μια πλατφόρμα blockchain μεταγενέστερης κλίμακας για να βασίζεται στον συντονισμό και τα πρότυπα ανοιχτού κώδικα. Θα επιτρέψει στις Προτάσεις Βελτίωσης Ethereum (EIPs) καθώς και στις Προτάσεις Βελτίωσης Klaytn (KIPs) να συνεισφέρουν και στα δύο οικοσυστήματα.
- Η **OpenChain** είναι μια δημοφιλής πλατφόρμα blockchain ανοιχτού κώδικα με τεχνολογία κατανεμημένης λογιστικής. Αυτή η εταιρεία blockchain είναι

κατάλληλη για οργανισμούς που διαχειρίζονται ψηφιακά στοιχεία με ασφαλή και ισχυρό τρόπο. Η τεχνολογία Blockchain δεν απαιτεί τέλη για την εξόρυξη και το blockchain Bitcoin είναι σημαντικό για την αμετάβλητη του.

- Η **Hyperledger Iroha** είναι μία από τις κορυφαίες πλατφόρμες blockchain ανοιχτού κώδικα με λογισμικό κατανεμημένο λογιστικό βιβλίο. Έχει σχεδιαστεί για να είναι απλό να ενσωματωθεί σε έργα υποδομής ή IoT που απαιτούν τεχνολογία κατανεμημένης λογιστικής. Υπάρχουν χαρακτηριστικά που περιλαμβάνουν μια απλή κατασκευή, σπονδυλωτή σχεδίαση C++ με γνώμονα τον τομέα και έναν νέο συναινετικό αλγόριθμο ανεκτικό σε σφάλματα σύγκρουσης, γνωστό ως YAC.
- Η **Hyperledger Sawtooth** είναι μια εταιρεία blockchain που επικεντρώνεται σε επιχειρηματικές λύσεις για τη δημιουργία και την ανάπτυξη κατανεμημένων λογιστικών βιβλίων παρέχοντας μια εξαιρετικά αρθρωτή και ευέλικτη πλατφόρμα για την εφαρμογή ενημερώσεων βάσει συναλλαγών σε κοινές καταστάσεις μεταξύ μη αξιόπιστων μερών που συντονίζονται από αλγόριθμους συναίνεσης. Είναι επίσης ένα έργο ανοιχτού κώδικα στο GitHub για βοήθεια με την κατεύθυνση του έργου και την παροχή περιπτώσεων χρήσης.
- Το **Corda** επικεντρώνεται στη γρήγορη δημιουργία ψηφιακών περιουσιακών στοιχείων όπως χρηματοοικονομικές λύσεις στην ιδιωτική και ασφαλή κλιμακούμενη πλατφόρμα DLT που έχει σχεδιαστεί για ρυθμιζόμενες αγορές. Είναι μια επεκτάσιμη και εξουσιοδοτημένη πλατφόρμα τεχνολογίας κατανεμημένων λογιστικών καταστάσεων P2P για την παροχή ψηφιακής εμπιστοσύνης μεταξύ των μερών σε ρυθμιζόμενες αγορές. Βοηθά στην εκτέλεση της πρώτης εφαρμογής Corda μέσα σε λίγα λεπτά με κώδικα ανοιχτού κώδικα έτοιμο για παραγωγή και δείγματα εφαρμογών.
- Το **Tron** είναι ένα από τα μεγαλύτερα λειτουργικά συστήματα που βασίζονται σε blockchain στον κόσμο με υψηλή απόδοση, υψηλή επεκτασιμότητα και υψηλή διαθεσιμότητα. Στόχος είναι να βοηθηθούν οι αποκεντρωμένες εφαρμογές να λειτουργούν στο TRON με χαμηλότερη κατανάλωση ενέργειας, μεγαλύτερη ταχύτητα, καθώς και βελτιωμένη ασφάλεια με απεριόριστη χωρητικότητα για το κύριο δίκτυο. Το οικοσύστημα τεχνολογίας blockchain περιλαμβάνει διακριτικά όπως TRX, BTT, USDT, USDC, JST και NFT.
- Η **BigChainDB** είναι μια από τις γνωστές πλατφόρμες blockchain ανοιχτού κώδικα με βάση δεδομένων blockchain. Η τεχνολογία Blockchain βοηθά στην υψηλή

απόδοση, τη χαμηλή καθυστέρηση, τον αποκεντρωμένο έλεγχο και την αμετάβλητη αποθήκευση δεδομένων για τις εταιρείες. Ξεκινά με τα κατανεμημένα λογιστικά βιβλία και βάσεις δεδομένων μεγάλων δεδομένων, ενώ προσθέτει ορισμένα χαρακτηριστικά της τεχνολογίας blockchain.

Επιλέχθηκε να πραγματοποιηθεί σύγκριση μεταξύ Corda και Ripple, διότι πολύ συχνά στη βιβλιογραφία αυτές οι δύο πλατφόρμες συγκρίνονται, με σκοπό να γίνει ξεκάθαρη η διαφορά τους. Επιλέγοντας αυτές τις δύο πλατφόρμες οι οποίες έχουν αρκετές διαφορές μεταξύ τους θέλαμε να αναδείξουμε με πιο εμφανή τρόπο ότι η τεχνολογία του blockchain μπορεί να καλύψει ένα ευρύ φάσμα επαγγελματικών αναγκών και να χρησιμοποιηθεί με διαφορετικούς τρόπους και όχι μόνο για συγκεκριμένες και μεμονωμένες καταστάσεις. Μέσα από τις διαφορές μπορούμε να δούμε διαφορετικές περιπτώσεις χρήσης της τεχνολογίας του blockchain, σε αντίθεση με το αν παίρναμε δύο πλατφόρμες οι οποίες είναι όμοιες μεταξύ τους. Οι οποίες θα είχαν ένα πολύ στοχευμένο κοινό που θα μπορούσε να τη χρησιμοποιήσει.

4.1 Corda

Το Corda είναι μια πλατφόρμα κατανεμημένης λογιστικής φτιαγμένης από κόμβους αμοιβαίας δυσπιστίας που επιτρέπει σε μια ενιαία παγκόσμια βάση δεδομένων να καταγράφει την κατάσταση των συμφωνιών μεταξύ ιδρυμάτων και ανθρώπων. Αυτό εξαλείφει μεγάλο μέρος της χρονοβόρας προσπάθειας που απαιτείται επί του παρόντος για να διατηρηθούν όλα τα λογιστικά βιβλία συγχρονισμένα μεταξύ τους. Αυτό επιτρέπει επίσης ένα μεγαλύτερο επίπεδο διευκόλυνσης κοινής χρήσης κώδικα που χρησιμοποιείται στον χρηματοπιστωτικό κλάδο, μειώνοντας έτσι το κόστος των χρηματοοικονομικών υπηρεσιών. Τα νομικά έγγραφα της συναλλαγής είναι ορατά μόνο σε εκείνους τους νόμιμους συμμετέχοντες στη συναλλαγή και οι τιμές κατακερματισμού χρησιμοποιούνται για να εξασφαλιστεί αυτό μαζί με τη συναίνεση κρυπτογράφησης κόμβου. Τα κύρια χαρακτηριστικά του Corda (Brown et al, 2014) είναι τα αυτοματοποιημένα έξυπνα συμβόλαια και η χρονική σήμανση των εγγράφων για τη διασφάλιση της μοναδικότητας.
Η συναίνεση περιλαμβάνει την απόκτηση των αξιών που είναι διαθέσιμες αυτήν τη στιγμή, τον συνδυασμό τους με έξυπνα συμβόλαια και την παραγωγή νέων αποτελεσμάτων ή καταστάσεων. Οι δύο βασικές πτυχές για την επίτευξη συναίνεσης είναι η εγκυρότητα της συναλλαγής και η μοναδικότητα της συναλλαγής. Η συναίνεση εγκυρότητας διατηρείται

ελέγχοντας την εγκυρότητα του κωδικού έξυπνου συμβολαίου που χρησιμοποιείται και επίσης ελέγχοντας εάν εκτελούνταν με τις κατάλληλες υπογραφές. Η συμβολαιογραφική επικύρωση, η χρονοσήμανση και άλλοι περιορισμοί που εμπλέκονται στα έξυπνα συμβόλαια διατηρούν τη μοναδικότητα της συναλλαγής.

Στο Corda υπάρχει η έννοια της αμετάβλητης κατάστασης και αποτελείται από ψηφιακά υπογεγραμμένες ασφαλείς συναλλαγές. Το bytecode Java του Corda είναι επίσης μέρος της κατάστασης. Αυτό εκτελείται με τη βοήθεια του εικονικού περιβάλλοντος χρόνου εκτέλεσης που παρέχεται από την εικονική μηχανή Java (JVM). Ως αποτέλεσμα η εκτέλεση του πρωτοκόλλου συναίνεσης λαμβάνει χώρα σε περιβάλλον Sandbox (περιβάλλοντα προστατευμένης εκτέλεσης) καθιστώντας το πιο ασφαλές. Στη διαδικασία επαλήθευσης, καλεί τη συνάρτηση επαλήθευσης που ελέγχει εάν η συναλλαγή έχει υπογραφεί ψηφιακά από όλους τους συμμετέχοντες, γεγονός που διασφαλίζει ότι μια συγκεκριμένη συναλλαγή θα εκτελεστεί εάν επαληθευτεί και επικυρωθεί από όλους τους συμμετέχοντες. Το δίκτυο Corda είναι ημι-ιδιωτικό. Όλες οι επικοινωνίες είναι αδιάκοπες, όπου ένα κρυπτογραφημένο με TLS δεδομένα αποστέλλεται μέσω AMQP/1.0,(πρωτόκολλο ανταλλαγής μηνυμάτων σε επίπεδο καλωδίου) πράγμα που σημαίνει ότι τα δεδομένα μοιράζονται με βάση την ανάγκη γνώσης. Κάθε κόμβος έχει έναν εκλεγμένο «θυρωρό» (https://docs.corda.net/key-concepts.html) που προετοιμάζει αυστηρά κανόνες σχετικά με τις πληροφορίες που πρέπει να παρέχουν οι κόμβοι και τις διαδικασίες Know Your Customer (KYC) που πρέπει να ολοκληρώσουν πριν προστεθούν στο δίκτυο.

Δεν υπάρχει ενιαία κεντρική αποθήκευση δεδομένων στο Corda, αντίθετα, κάθε κόμβος διατηρεί μια ξεχωριστή βάση δεδομένων γνωστών γεγονότων. Κάθε ταυτότητα Corda μπορεί να αναπαρασταθεί ως νομική ταυτότητα και ταυτότητα υπηρεσίας. Η ταυτότητα μπορεί να είναι γνωστή ταυτότητα ή εμπιστευτική, κάτι που βασίζεται στο αν το πιστοποιητικό X.509(δημόσια πιστοποιητικά κλειδιού, ψηφιακά έγγραφα που συσχετίζουν με ασφάλεια κρυπτογραφικά ζεύγη κλειδιών με ταυτότητες όπως ιστότοπους, άτομα ή οργανισμούς.) τους έχει δημοσιευτεί ή όχι. Μια κατάσταση είναι ένα αμετάβλητο αντικείμενο που αντιπροσωπεύει ένα γνωστό γεγονός που μοιράζεται μεταξύ διαφορετικών κόμβων σε μια συγκεκριμένη χρονική στιγμή. Η κατάσταση περιέχει αυθαίρετα δεδομένα. Καθώς οι καταστάσεις είναι αμετάβλητες, δεν μπορούν να τροποποιηθούν άμεσα για να αντικατοπτρίζουν μια αλλαγή στην κατάσταση. Κάθε κόμβος διατηρεί μια βάση δεδομένων που παρακολουθεί όλη την τρέχουσα και την ιστορική κατάσταση.

Κάθε κατάσταση είναι μια σύμβαση και λαμβάνει τη συναλλαγή ως είσοδο και την επαληθεύει με βάση τους κανόνες της σύμβασης. Μια συναλλαγή που δεν είναι συμβατικά

έγκυρη δεν είναι έγκυρη πρόταση ενημέρωσης του καθολικού και, επομένως, δεν μπορεί ποτέ να δεσμευτεί στο καθολικό. Η επαλήθευση της συναλλαγής πρέπει να είναι ντετερμινιστική, δηλαδή θα πρέπει είτε να γίνεται πάντα αποδεκτή είτε πάντα να απορρίπτεται. Για αυτό, το συμβόλαιο αξιολογεί τη συναλλαγή σε ένα ντετερμινιστικό Sandbox (https://docs.corda.net/key-concepts.html) που προετοιμάζει τη λίστα επιτρεπόμενων που αποτρέπει τη σύμβαση από την εισαγωγή ανεπιθύμητων βιβλιοθηκών. Χρησιμοποιεί ένα μοντέλο UTXO (μη δαπανημένη έξοδο συναλλαγής) όπου όλες οι καταστάσεις στο καθολικό είναι σταθερές. Κατά τη δημιουργία μιας νέας συναλλαγής, η κατάσταση εξόδου πρέπει να δημιουργηθεί από τους προτείνοντες. Η κατάσταση εισόδου υπάρχει ήδη ως έξοδος προηγούμενων συναλλαγών.

Αυτές οι αναφορές κατάστασης εισόδου συνδυάζουν όλες τις συναλλαγές μαζί και σχηματίζουν μια αλυσίδα. Οι εξουσιοδοτημένοι υπογράφοντες υπογράφουν τη συναλλαγή μόνο εάν πληρούνται οι προϋποθέσεις της εγκυρότητας και της μοναδικότητας συναλλαγής. Το δίκτυο Corda χρησιμοποιεί μηνύματα από σημείο σε σημείο αντί για καθολική μετάδοση. Αντί να χρειάζεται να καθορίσετε αυτά τα βήματα με μη αυτόματο τρόπο, το Corda αυτοματοποιεί τη διαδικασία χρησιμοποιώντας ροές όπου η ροή λέει σε έναν κόμβο πώς να επιτύχει μια συγκεκριμένη ενημέρωση του καθολικού. Εάν η προτεινόμενη συναλλαγή είναι έγκυρη, η ενημέρωση του καθολικού περιλαμβάνει την απόκτηση δύο τύπων συναίνεσης.

Συναίνεση εγκυρότητας — επαληθεύεται από πιστοποιημένο υπογράφοντα πριν υπογράψει τη συναλλαγή.

Συναίνεση μοναδικότητας — επαληθεύεται από συμβολαιογραφική υπηρεσία. Ο συμβολαιογράφος παρέχει το σημείο οριστικοποίησης στο σύστημα.

Το βασικό στοιχείο της αρχιτεκτονικής είναι ένα επίπεδο εμμονής για την αποθήκευση δεδομένων, μια διεπαφή δικτύου για αλληλεπίδραση με άλλους κόμβους, μια διεπαφή RPC για αλληλεπίδραση με τον κάτοχο κόμβων, ένας κόμβος υπηρεσιών που επιτρέπει στους κατόχους κόμβων να καλούν τους κόμβους άλλες υπηρεσίες και να συνδέσουν -στο μητρώο για την επέκταση του κόμβου με την εγκατάσταση του CorDapps. Τέλος, ιδιαίτερο χαρακτηριστικό για τη συγκεκριμένη πλατφόρμα ανάπτυξης αποτελεί και η έλλειψη παρουσίας κάποιου κρυπτονομίσματος.

Βασικά χαρακτηριστικά του Corda:

1. Μόνο οι χρήστες που έχουν έννομο συμφέρον μπορούν να συμμετέχουν στο δίκτυο, το οποίο εμποδίζει τη μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων.

2. Γνωστός για τη διαχείριση πολύπλοκων οικονομικών καταστάσεων και την ευκολία ενσωμάτωσης με παλαιού τύπου συστήματα.
3. Χρησιμοποιεί Συμβολαιογράφους (συγκεντρωμένους ή διανεμημένους) στο δίκτυο για να αντιμετωπίσει τα προβλήματα απορρήτου, εξαλείφοντας την ανάγκη εκτέλεσης δαπανηρών αλγορίθμων συναίνεσης.

4.2 Ripple

Το Ripple είναι ένα σύστημα ακαθάριστου διακανονισμού σε πραγματικό χρόνο (RTGS) που ειδικεύεται στις μεταφορές χρημάτων, τις ανταλλαγές νομισμάτων και τα εμβάσματα. Αναφέρεται επίσης ως Πρωτόκολλο συναλλαγών Ripple (RTXP). Το Πρωτόκολλο Ripple, είναι χτισμένο σε κατανεμημένο συναινετικό βιβλίο πρωτοκόλλου Διαδικτύου ανοιχτού κώδικα και το κρυπτονόμισμα του ονομάζεται XRP . Το Ripple αναπτύχθηκε και κυκλοφόρησε το 2012 και επιτρέπει ασφαλείς, γρήγορες και ανεξάρτητες παγκόσμιες οικονομικές συναλλαγές οποιουδήποτε μεγέθους χωρίς απολύτως καμία αντιστροφή χρέωσης (Todd, 2015). Το Ripple στηρίζεται σε tokens που αντιπροσωπεύουν το νόμισμα fiat, το εικονικό νόμισμα ή οποιοδήποτε πολύτιμο περιουσιακό στοιχείο. Το Ripple βασίζεται σε ένα κοινόχρηστο, δημόσιο καθολικό πρότυπο, το οποίο χρησιμοποιεί μια διαδικασία συναίνεσης που επιτρέπει να πραγματοποιούνται συναλλαγές, όπως πληρωμές και διακανονισμοί σε μια κατανεμημένη διαδικασία.

Το Ripple υιοθετείται από εταιρείες όπως η UniCredit, η UBS, η Santander και συγκεκριμένα σε λογιστικά πρότυπα τραπεζών και έχει πολλά πλεονεκτήματα σε σχέση με άλλα εικονικά νομίσματα όπως το Bitcoin. Είναι ένα σύστημα ψηφιακών νομισμάτων στο οποίο οι συναλλαγές επαληθεύονται με συναίνεση μεταξύ των μελών του δικτύου και όχι με τη διαδικασία εξόρυξης που χρησιμοποιείται από το Bitcoin. Αυτή η νέα έκδοση του συστήματος Ripple σχεδιάστηκε επομένως για να εξαλείψει την εξάρτηση του Bitcoin από κεντρικές ανταλλαγές, να χρησιμοποιεί λιγότερη ηλεκτρική ενέργεια και να εκτελεί συναλλαγές πολύ πιο γρήγορα. Το πρωτόκολλο ανοιχτού κώδικα περιγράφει τον ιστότοπο του Ripple ως βασική τεχνολογία υποδομής για διατραπεζικές συναλλαγές. Τόσο οι χρηματοοικονομικές όσο και οι μη χρηματοοικονομικές εταιρείες ενσωματώνουν το πρωτόκολλο Ripple στο σύστημά τους. Για να πραγματοποιηθεί μια συναλλαγή απαιτούνται δύο μέρη. **Πρώτον**, ένα ρυθμιζόμενο χρηματοπιστωτικό ίδρυμα που διατηρεί κεφάλαια και εκδίδει υπόλοιπα για λογαριασμό πελατών και **Δεύτερον**, διαπραγματευτές αγοράς όπως αμοιβαία κεφάλαια αντιστάθμισης κινδύνου που παρέχει ρευστότητα στο νόμισμα στο οποίο θέλουν να διαπραγματευτούν.

Ο αλγόριθμος συναίνεσης ξεκινά με ένα γνωστό σύνολο κόμβων που είναι γνωστό ότι συμμετέχουν στη συναίνεση. Αυτή η λίστα είναι γνωστή ως λίστα μοναδικών κόμβων. Αυτή η λίστα είναι μια συλλογή από δημόσια κλειδιά ενεργών κόμβων που είναι μοναδικά. Μέσω του αλγόριθμου συναίνεσης, οι κόμβοι στο UNL ψηφίζουν για να καθορίσουν τα περιεχόμενα του καθολικού. Ενώ το πραγματικό πρωτόκολλο περιέχει έναν αριθμό από γύρους προτάσεων και ψηφοφοριών, το αποτέλεσμα μπορεί να περιγραφεί βασικά ως ψήφος υπερπλειοψηφίας, μια συναλλαγή εγκρίνεται μόνο εάν το 80% του UNL ενός διακομιστή συμφωνεί με αυτό (Todd, 2015). .

Αρχικά, κάθε διακομιστής λαμβάνει όλες τις έγκυρες συναλλαγές που έχει πριν από την έναρξη της συναίνεσης και τις δημοσιοποιεί με τη μορφή μιας λίστας γνωστής ως το υποψήφιο σύνολο. Στη συνέχεια, κάθε διακομιστής συνδυάζει κάθε ένα από τα υποψήφια σύνολα όλων των διακομιστών στο UNL (Unique Node List) του και ψηφίζει για την ακρίβεια όλων των συναλλαγών. Όλες οι συναλλαγές που πληρούν αυτή την ψήφο του 80% εφαρμόζονται στο καθολικό και αυτό το καθολικό κλείνει και γίνεται το νέο καθολικό κλειστό (Siba&Prakash, 2016).

Μία βασική διαφορά από τα υπόλοιπα νομίσματα Blockchain είναι ότι δεν απαιτείται η διαδικασία της εξόρυξης για την επιβεβαίωση των συναλλαγών. Η επιβεβαίωση αυτών γίνεται μέσω της χρήσης ενός διαφορετικού μοντέλου συναίνεσης και εξαλείφεται η χρήση τεράστιας ενεργειακής και υπολογιστικής ισχύς που θα χρειαζόταν άλλα δίκτυα για παρόμοια διαδικασία.

Βασικά χαρακτηριστικά του Ripple:

1. Οι χαμηλές χρεώσεις συναλλαγών, η γρήγορη διεκπεραίωση των συναλλαγών και η διαφάνεια είναι μερικά από τα χαρακτηριστικά του Ripple που το διακρίνει από άλλα.
2. Παρέχει μια επιλογή συναλλαγών σε πολλαπλά περιουσιακά στοιχεία blockchain όπως BTC/LTC, μη εγγενή περιουσιακά στοιχεία και νομίσματα όπως USD, Yen κ.λπ.
3. Ένα συγκεκριμένο περιουσιακό στοιχείο στο blockchain μπορεί να κλειδωθεί χρησιμοποιώντας τη λειτουργία "Εκδοση". Το ίδιο μπορεί να μεταφερθεί σε άλλους λογαριασμούς χωρίς να επιβαρυνθεί με μεγάλο κόστος, καθώς η Ripple προσφέρει υπηρεσίες χαμηλών χρεώσεων.

4.3 Σύγκριση μεταξύ Corda και Ripple

Το Corda είναι ένα blockchain, αλλά όχι με την παραδοσιακή έννοια. Χρησιμοποιεί τεχνολογία κατανεμημένης λογιστικής ομότιμης, αλλά δεν συγκεντρώνει πολλές συναλλαγές σε ένα μπλοκ. Επεξεργάζεται όλες τις ανταλλαγές σε πραγματικό χρόνο, επιτρέποντας υψηλότερη απόδοση για τα DApps. Οι προγραμματιστές μπορούν να χρησιμοποιήσουν οποιαδήποτε γλώσσα συμβατή με JVM για να δημιουργήσουν λύσεις στην πλατφόρμα και τα αρθρωτά API της προσφέρουν εντυπωσιακή επεκτασιμότητα. Το R3 παρέχει επίσης υποστήριξη από άκρο σε άκρο για το Corda, βελτιώνοντας περαιτέρω την προσβασιμότητά του. Ωστόσο, όσο αξιοσημείωτο κι αν είναι αυτό, ορισμένες εναλλακτικές λύσεις blockchain μπορούν να εκτελέσουν πολλές από τις ίδιες λειτουργίες πιο γρήγορα και με χαμηλότερο κόστος.

Το Corda χρησιμοποιεί ειδικούς αλγόριθμους συναίνεσης για την επικύρωση των συναλλαγών και τη διατήρηση της σωστής λειτουργίας του δικτύου, ενώ ταυτόχρονα δίνει τη δυνατότητα επιλογής του αντίστοιχου αλγορίθμου. Στους συγκεκριμένους αλγόριθμους θεσμοθετούνται κάποιοι κόμβοι που λειτουργούν ως συμβολαιογράφοι και διαχειρίζονται τα έξυπνα συμβόλαια καθώς και την πρόοδο που έχουν. Το λογισμικό διαθέτει δύο βασικά χαρακτηριστικά των σύγχρονων δικτύων Blockchain, τα έξυπνα συμβόλαια και τη λειτουργία χρονικής σήμανσης διεργασιών εγγράφων. Επιπλέον, περιλαμβάνει ένα άλλο χαρακτηριστικό που ονομάζεται πλαίσιο ροής, το οποίο απλοποιεί τη διαδικασία σύνταξης πολύπλοκων πρωτοκόλλων μεταξύ πολλών μερών που πρόκειται να συμμετάσχουν σε μια συναλλαγή. Τέλος, ένα ιδιαίτερο χαρακτηριστικό αυτής της πλατφόρμας ανάπτυξης είναι η έλλειψη οποιουδήποτε κρυπτονομίσματος.

Ήδη μεγάλα χρηματοπιστωτικά ιδρύματα όπως η HSBC, η ING, η BBVA και η Royal Bank of Scotland το έχουν χρησιμοποιήσει για τις εμπορικές τους συναλλαγές, όπως και άλλες επιχειρήσεις, στον κόσμο της εφοδιαστικής αλυσίδας, της ενέργειας, της υγειονομικής περίθαλψης και πολλά άλλα.

Η πλατφόρμα αναπτύσσεται σε γλώσσα Kotlin και Java, ενώ ταυτόχρονα λειτουργεί στην Εικονική Μηχανή Java. Αυτή η τελευταία δυνατότητα επιτρέπει στην πλατφόρμα να χρησιμοποιεί μια τεράστια γκάμα βιβλιοθηκών που υπάρχουν ήδη για την πλατφόρμα Java.

Το Ripple είναι μια άλλη πλατφόρμα blockchain που εστιάζει στα οικονομικά και είναι μια δημοφιλής λύση. Χρησιμοποιείται από εκατοντάδες χρηματοπιστωτικά ιδρύματα χάρη στη διαφάνεια, τον γρήγορο χρόνο απόκρισης και το χαμηλό κόστος συναλλαγής. Το Ripple έχει ένα εγγενές κρυπτονόμισμα που μπορούν να χρησιμοποιήσουν οι προγραμματιστές,

αλλά οι εφαρμογές που δημιουργείτε στην πλατφόρμα δεν χρειάζεται να το χρησιμοποιούν. Οι διασυνοριακές πληρωμές είναι η κύρια περίπτωση χρήσης για το Ripple και οι γρήγορες συναλλαγές με χαμηλή χρέωση της πλατφόρμας παρέχουν τον ιδανικό χώρο για αυτές τις ανταλλαγές. Ωστόσο, το Ripple δεν υποστηρίζει έξυπνα συμβόλαια, τα οποία μπορεί να χρειάζονται ορισμένοι προγραμματιστές.

Παρουσιάζει μια βασική διαφορά από άλλα νομίσματα Blockchain. Η διαδικασία εξόρυξης δεν απαιτείται για την επιβεβαίωση συναλλαγών. Η επιβεβαίωση αυτών γίνεται μέσω της χρήσης ενός διαφορετικού μοντέλου συναίνεσης και εξαλείφει τη χρήση τεράστιας ενέργειας και υπολογιστικής ισχύος που θα χρειάζονταν άλλα δίκτυα για μια παρόμοια διαδικασία.

Αξίζει να σημειωθεί ότι το συγκεκριμένο δίκτυο διαθέτει και τη δική του πλατφόρμα ανάπτυξης, το Xpring, το οποίο διαθέτει τη δική του βιβλιοθήκη (SDK Library) για αρκετές από τις δημοφιλείς γλώσσες προγραμματισμού και συγκεκριμένα για Javascript (NodeJS), Java και Swift.

Τα θετικά της χρήσης του Ripple είναι η τεράστια χωρητικότητα του δικτύου που μπορεί να εκτελέσει 1000 λειτουργίες ανά δευτερόλεπτο. Επιπλέον, θετική είναι και η υποστήριξη από τις τράπεζες, χαρακτηριστικό που προσδίδει επίσης κύρος στην πλατφόρμα. Η πλατφόρμα έχει ελάχιστες χρεώσεις συναλλαγής και παρέχει τη δυνατότητα ακύρωσής τους. Ωστόσο, στο Ripple πάνω από το 60% του συνολικού XRP που υπάρχει ανήκει στην εταιρεία που το διαχειρίζεται, επομένως έχουν πάνω από το 51% του δικτύου που απαιτείται για τον πλήρη έλεγχο του Blockchain.

Τέλος, αξίζει να σημειωθεί η σημαντικότερη διαφορά του σε σχέση με άλλα κρυπτονομίσματα. Το Ripple είναι ένα κρυπτονόμισμα που έχει ήδη εξορυχθεί και για αυτό το λόγο τα κίνητρα για την εκτέλεση κόμβων στο δίκτυο είναι ελάχιστα έως μηδενικά. Επομένως, εταιρείες που το χρησιμοποιούν, όπως οι τράπεζες, θα πρέπει να παρέχουν τους κόμβους επικύρωσης. Η πλατφόρμα, λόγω της ιδιαιτερότητας ότι διαθέτει ελάχιστους κόμβους για τη λειτουργία της, δεν μπορεί να θεωρηθεί αποκεντρωμένη.

Από την ανάλυση των Corda και Ripple, μπορεί να συναχθεί το συμπέρασμα ότι είναι πλατφόρμες blockchain ανοιχτού κώδικα με έμφαση στην εξυπηρέτηση επιχειρήσεων. Τα χαρακτηριστικά ασφαλείας που υπάρχουν και στις δύο πλατφόρμες αποδεικνύονται ζωτικής σημασίας για τη διασφάλιση της ασφάλειας και της αυθεντικότητας των συναλλαγών. Ωστόσο, τα χαρακτηριστικά συμβολαιογραφικής επικύρωσης δίνουν στην πλατφόρμα Corda ένα ανταγωνιστικό πλεονέκτημα έναντι του Ripple. Τα χαρακτηριστικά μοναδικότητας και συμβολαιογραφικής επικύρωσης προσφέρουν στην Corda περισσότερη

αξιοπιστία και σταθερότητα στην απόδοση, αποδεικνύοντας ότι είναι μια πιο αξιόπιστη και επιλεγμένη πλατφόρμα μέσω Blockchain για τη διεξαγωγή οικονομικών συναλλαγών. Περαιτέρω βελτίωση στη συναίνεση ή εάν η Corda προσαρμοστεί στην πλατφόρμα blockchain ως ψευδή απόδειξη, μπορεί να προσφερθεί περαιτέρω βελτιωμένη ασφάλεια από την πλατφόρμα, αναδεικνύοντας έτσι την Corda ως μελλοντική πλατφόρμα για τη διεξαγωγή οικονομικών συναλλαγών. Ο παρακάτω πίνακας συνοψίζει τη σύγκριση.

	Corda	**Ripple**
Εταιρεία	R3 Labs	Ripple Labs
Αρχική έκδοση	2014	2012
Τύπος	Υβριδικό Blockchain	Ιδιωτικό Blockchain
Νόμισμα	Όχι	XRP
Εστιάζει Στον Κλάδο	Χρηματοπιστωτικές Υπηρεσίες	Χρηματοπιστωτικές Υπηρεσίες
Σκοπός (Προτεινόμενη Χρήση)	Κλάδο Χρηματοοικονομικών Υπηρεσιών	Τράπεζες και Χρηματοπιστωτικά Ιδρύματα
Πρωτόκολλο	AMQP στο TLS	SMTP στο TLS
Συμμετέχοντες	Μόνο αποστολέας και παραλήπτης	Η λίστα UNL
Γλώσσα	Kotlin. Java	XRP Ledger σε C++
Συναίνεση	Ειδική κατανόηση της συναίνεσης (δηλαδή συμβολαιογραφικοί κόμβοι)	Λίστα μοναδικού κόμβου
Διακίνηση	~170 tps	~ 1500 tps
Βάση Δεδομένων & Ερώτημα	Πλούσιο ερώτημα χρησιμοποιώντας βάση δεδομένων SQL μέσω H2	*RocksDB και κόμβος

Πίνακας 2. Σύγκριση Corda και Ripple

Συμπερασματικά όπως μπορούμε να καταλάβουμε από τη σύγκριση αυτών των δύο πλατφορμών η καθεμία έχει τη δική της χρήση και εφαρμογή σε διάφορους τομείς της επιχειρηματικότητας. Ανάλογα με την πρόσβαση που δίνει, την ταχύτητα , τις δυνατότητες που προσφέρει ,αξιολογείται και επιλέγετε από κάποιον υπεύθυνο του επιχειρηματικού τομέα που θέλει να τη χρησιμοποιήσει . Έτσι λοιπόν αν ο φορέας αυτός αφορά Κλάδο Χρηματοοικονομικών Υπηρεσιών θα επιλέξει το Corda διότι προσφέρει επεκτάσιμες και ασφαλείς συναλλαγές δεδομένων μεταξύ των συμμετεχόντων, ενώ ταυτόχρονα διατηρεί ένα κορυφαίο επίπεδο ιδιωτικότητας και προστασίας, δεν αποθηκεύει δεδομένα συναλλαγών στους κόμβους του δικτύου. Όλοι οι κόμβοι επαληθεύονται, γεγονός που

καταργεί την ανάγκη για συναίνεση, διασφαλίζοντας την εμπιστοσύνη ακόμη και στο περιβάλλον μηδενικής εμπιστοσύνης. Ωστόσο, αυτή η δυνατότητα καθιστά το Corda μη εφαρμόσιμο σε έργα όπου πρέπει να χτιστεί εμπιστοσύνη σε ένα επαληθευμένο αλλά συνεχώς μεταβαλλόμενο σύνολο χρηστών. Το Corda ταιριάζει σε έργα όπου όλοι οι χρήστες γνωρίζονται μεταξύ τους και είναι σίγουροι για το επίπεδο εμπιστοσύνης που μπορούν να δώσουν σε συγκεκριμένες πτυχές. Αυτό είναι εφικτό για συνεργαζόμενες επιχειρήσεις, διαφορετικά τμήματα μεγάλων εταιρειών και διατραπεζικές λειτουργίες. Σε άλλη περίπτωση αν αυτός ο φορέας αφορά Τράπεζες και Χρηματοπιστωτικά Ιδρύματα θα επιλέξει το Ripple διότι είναι ένα δίκτυο σχεδιασμένο να μεταφέρει αξεία. Διευκολύνει τις διασυνοριακές πληρωμές και την ανταλλαγή νομισμάτων, είναι γρήγορο (διαρκεί μερικά δευτερόλεπτα ανά συναλλαγή) και έχει τη δυνατότητα να παρέχει μια καλύτερη μέθοδο για την ολοκλήρωση διεθνών πληρωμών . Ωστόσο στο Ripple δεν είναι εύκολο να παρακολουθήσετε την αξία του κρυπτονομίσματος XRP καθώς οι επενδυτές δεν γνωρίζουν πότε θα μπορούσαν να τεθούν σε κυκλοφορία οι μεγάλες του ποσότητες . Επίσης είναι λιγότερο αποκεντρωμένο σε σύγκριση με άλλα κρυπτονομίσματα επειδή διατηρεί μια προεπιλεγμένη λίστα επικυρωτών συναλλαγών. Με αυτό ακριβώς το γνώμονα μπορεί να γίνει σύγκριση σε όλες τις πλατφόρμες του blockchain και να γίνει η άμεση εφαρμογή τους στον κλάδο και στον συγκεκριμένο τομέα που μπορούν να μεγιστοποιήσουν τα οφέλη τους.

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Blockchain είναι ένα εργαλείο που χρησιμοποιείται από οργανισμούς κυρίως στον τομέα των επιχειρήσεων και για να είμαστε πιο συγκεκριμένοι, στον τομέα των οικονομικών που επιτρέπει στις συναλλαγές να είναι πιο αποτελεσματικές και ασφαλείς. Τα δεδομένα στην επεξεργασμένη τους μορφή έχουν μεγάλη χρηματική αξία στις μέρες μας, ιδιαίτερα αν αφορούν τον επιχειρηματικό τομέα. Έτσι, η ασφάλεια των δεδομένων αξίζει πρωταρχικής σημασίας, επειδή οι επιχειρηματικές οργανώσεις που υφίστανται υποκλοπή ή χειραγώγηση των μεταδιδόμενων δεδομένων υπόκεινται σε μεγάλη οικονομική ζημία. Στην εποχή όπου σημειώνεται μια απότομη άνοδος στον τομέα των επιχειρηματικών συναλλαγών που είναι φυσικά χρηματοοικονομικού χαρακτήρα, η ανάγκη πραγματοποίησης συναλλαγών είναι πιο ασφαλής και αυθεντική αξίζει κρίσιμης σημασίας. Η εφαρμογή του Blockchain εξυπηρετεί αυτόν τον σκοπό παρέχοντας αποτελεσματικότητα, ασφάλεια και αυθεντικότητα στις συναλλαγές.

Το Blockchain είναι μια επαναστατική και συναρπαστική τεχνολογία με τεράστιες δυνατότητες χρήσης σε ένα ευρύ φάσμα σύγχρονων εφαρμογών. Ωστόσο, προτού τα οφέλη του blockchain γίνουν πλήρως αντιληπτά, πρέπει να αντιμετωπίσουν, μια σειρά από ανησυχίες και προκλήσεις. Μια προσέγγιση για την αντιμετώπιση της χαμηλής απόδοσης του blockchain είναι η δημιουργία νέων αρχιτεκτονικών και επιχειρησιακών πρωτοκόλλων για το σύστημα. Τα δεδομένα της αλυσίδας μπλοκ, για παράδειγμα, ενδέχεται να μην αντιγράφονται σε κάθε κόμβο του δικτύου. Αντίθετα, μόνο οι ισχυροί κόμβοι διατηρούν ένα αντίγραφο της αλυσίδας μπλοκ, ενώ άλλοι κόμβοι απλώς αποθηκεύουν τις κεφαλίδες μπλοκ ή δεν αποθηκεύουν καθόλου δεδομένα. Για να κλείσει το χάσμα απόδοσης μεταξύ ενός συστήματος blockchain και ενός τυπικού συστήματος βάσης δεδομένων, απαιτούνται επίσης τεχνικές συναίνεσης.

Ενώ η κατακόρυφη και οριζόντια κλιμάκωση ενός συστήματος blockchain μπορεί να βοηθήσει με προβλήματα επεκτασιμότητας, μια άλλη ερευνητική στρατηγική είναι μια διασυνδεδεμένη ιεραρχική δομή πολλαπλών μπλοκ αλυσίδων με εσωτερικές διασυνδέσεις. Θα μπορούσαν να υπάρχουν και άλλες προσεγγίσεις για τη μείωση του ποσού των συναλλαγών εντός της αλυσίδας. Ορισμένες συναλλαγές, για παράδειγμα, θα μπορούσαν να πραγματοποιηθούν απευθείας μεταξύ των μερών χωρίς να περάσουν από το δίκτυο blockchain. Ως εκ τούτου, ενισχύοντας την επεκτασιμότητα του blockchain. Η διατήρηση

της ασφάλειας και του απορρήτου των δεδομένων είναι δύσκολη, καθώς όλες οι συναλλαγές που δεσμεύονται σε ένα blockchain και είναι ορατές σε όλους τους συμμετέχοντες. Η παροχή δυνατότητας ελέγχου δεδομένων, από την άλλη πλευρά, μπορεί να έχει ως αποτέλεσμα την απώλεια δεδομένων και την ανωνυμία των χρηστών. Τα δεδομένα κατασκευής και εταιρικών λύσεων μπορεί να έχουν τεράστια εμπορική αξία. Ως αποτέλεσμα, στα έξυπνα συστήματα παραγωγής που βασίζονται σε blockchain, η ασφάλεια και το απόρρητο αποτελούν κρίσιμα ζητήματα. Προτού η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί σε ευρεία βάση, πρέπει να αντιμετωπιστούν αυτές και άλλες ανησυχίες για την ασφάλεια και το απόρρητο.

Για πιο αποτελεσματικές, επεκτάσιμες και ασφαλείς βιομηχανικές χρήσεις blockchain, απαιτείται πρόσθετη εργασία στο μέλλον. Για παράδειγμα, θα είναι ενδιαφέρον να διερευνήσουμε πώς οι τεχνικές μηχανικής μάθησης (ML) (Abu Al-Haija et al, 2022. Mihoub et al, 2022. Ben Fredj et al, 2020) μπορούν να χρησιμοποιηθούν στο πλαίσιο της τεχνολογίας blockchain για αύξηση στα επίπεδα ασφάλειας και στις επιδόσεις συστημάτων που βασίζονται σε blockchain. Θα είναι επίσης εξαιρετικά χρήσιμο να εφαρμοστούν ορισμένες επίσημες τεχνικές δοκιμών για λύσεις που βασίζονται σε blockchain για να βελτιώσουν την ποιότητά τους και να αυξήσουν την ευρωστία τους (Lahami&Krichen, 2021. Lahami et al, 2015. Lahami e tal, 2015).

Με βάση τα αποτελέσματά μας, ένας ερευνητής πληροφορικής, ένας ειδικός πληροφορικής ή ένας τεχνικός ηγέτης σε ένα ίδρυμα μπορεί να αξιολογήσει τις διάφορες πρακτικές πτυχές, όπως ο χρόνος εγκατάστασης/εκμάθησης και μοναδικά τεχνικά χαρακτηριστικά, των πλατφορμών. Η επιλογή της κατάλληλης πλατφόρμας εξαρτάται από τις απαιτήσεις της εφαρμογής. Μια τέτοια αξιολόγηση μπορεί να επιταχύνει τη διαδικασία και να μειώσει τους κινδύνους στην υιοθέτηση της αλυσίδας μπλοκ, μιας αμετάβλητης, κατανεμημένης και αυτοματοποιημένης τεχνολογίας, για εφαρμογές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Abu Al-Haija, Q.; Krichen, M.; Abu Elhaija, W. Machine-Learning-Based Darknet Traffic Detection System for IoT Applications.Electronics **2022**, 11, 556.

Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Ellahham, S.; Omar, M. The role of blockchain technology in telehealth and telemedicine. Int. J. Med. Inform. **2021**, 148, 104399.

Alliance, S.C. Effective Healthcare Identity Management: A Necessary First Step for Improving US Healthcare Information Systems. 2014. Available online: https://www.securetechalliance.org/resources/pdf/Healthcare_Identity_Brief.pdf

Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. **2019**, 100, 143–174.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyart, D, D, D., Ferris, C., Laventman, G., Manevich, Y., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the Thirteenth EuroSys Conference, 1–15.

Anker, P. From spectrum management to spectrum governance. Telecommun. Policy **2017**, 41, 486–497.

Aras, S.T., Kulkarni, V., 2017. Blockchain and Its Applications–A Detailed Survey. Int.J. Comput. Appl. 180 (3), 29–35.

Ariyarathna, T.; Harankahadeniya, P.; Isthikar, S.; Pathirana, N.; Bandara, H.D.; Madanayake, A. Dynamic spectrum access via smart contracts on blockchain. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.

Armitage, W.D.; Gauvin, W.; Sheffield, A. Design and Launch of an Intensive Cybersecurity Program for Military Veterans. In Proceedings of the 17th Annual Conference on Information Technology Education, Boston, MA, USA, 28 September–1 October 2016; pp. 40–45.

Armknecht, F., Karame, G.O., Mandal, A., Youssef, F., Zenner, E., 2015. Ripple: Overview and outlook, in: International Conference on Trust and Trustworthy Computing, Springer, 163–180.

Atzori, M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? 2015. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713

Azzi, R.; Chamoun, R.K.; Sokhn, M. The power of a blockchain-based supply chain. Comput. Ind. Eng. **2019**, 135, 582–592.

Bach, L., Mihaljevic, B., Zagar, M., 2018. Comparative analysis of blockchainconsensus algorithms. In: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, pp. 1545–1550.

Barua, M.; Liang, X.; Lu, R.; Shen, X. PEACE: An efficient and secure patient-centric access control scheme for eHealth care system. In Proceedings of the 2011 IEEE Conference on Computer CommunicationsWorkshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011; pp. 970–975.

Becker, G. 2008. Merkle signature schemes, Merkle trees and their cryptanalysis, Ruhr-University Bochum, Tech. Rep.

Ben Fredj, O.; Mihoub, A.; Krichen, M.; Cheikhrouhou, O.; Derhab, A. CyberSecurity attack prediction: A deep learning approach. In Proceedings of the 13thInternational

Conference on Security of Information and Networks, Merkez, Turkey, 4–7 November2020; pp. 1–6.

Bhandari, K.S.; Cho, G.H. An energy efficient routing approach for cloud-assisted green industrial IoT networks. Sustainability **2020**, 12, 7358.

Bhandari, K.S.; Cho, G.H. Resource oriented topology construction to ensure high reliability in IoT based smart city networks. Int. J. Syst. Assur. Eng. Manag. **2020**, 11, 798–805.

Bhandari, K.S.; Ra, I.H.; Cho, G. Multi-topology based QoS-differentiation in RPL for internet of things applications. IEEE Access **2020**, 8, 96686–96705.

Bhosale, J., Mavale, S., 2018. Volatility of select crypto-currencies: A comparison ofBitcoin, Ethereum and Litecoin, Annu. Res. J. SCMS, Pune 6.

Bozic, N., Pujolle, G., Secci, S., 2016. A tutorial on blockchain and applications to secure network control-planes. In: 3rd Smart Cloud Networks & Systems (SCNS), IEEE, pp. 1–8.

Brambilla, G., Amoretti, M., Zanichelli, F., 2016. Using blockchain for peer-to-peer proof-of-location, arXiv preprint arXiv:1607.00174.

Brandon, D. The blockchain: The future of business information systems. Int. J. Acad. Bus. World **2016**, 10, 33–40.

Brown, R.G., Carlyle, J., Grigg, I., Hearn, M. (2016). Corda: An Introduction. R3 CEV Careem, M.A.A.; Dutta, A. Sense chain: Blockchain based reputation system for distributed spectrum enforcement. In Proceedings of the 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Newark, NJ, USA, 11–14 November 2019; pp. 1–10.

Bruce, J., 2014. The Mini-Blockchain Scheme: White Paper, White Paper.

Cachin, C., Vukolic´, M. 2017. Blockchain consensus protocols in the wild, arXivpreprint arXiv:1707.01873.

Casado-Vara, R.; Prieto, J.; De la Prieta, F.; Corchado, J.M. How blockchain improves the supply chain: Case study alimentary supply chain. Procedia Comput. Sci. **2018**, 134, 393–398.

Castro, M., Liskov, B., et al., 1999. Practical Byzantine fault tolerance, in: OSDI, vol.99, 173–186.

Chamola, V., Hassija, V., Gupta, V., Guizani, M., 2020. A comprehensive review of theCOVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access 8, 90225–90265.

Chen, D.; Chen, L.; Fan, X.; He, L.; Pan, S.; Hu, R. Securing patient-centric personal health records sharing system in cloud computing. China Commun. **2014**, 11, 121–127.

Chhabra, V.; Bathla, S.; Maheshwari, H. An overview of blockchain technology and comparison between various cryptocurrencies. J. Emerg. Technol. Innov. Res. **2019**, 6, 68–71.

Chiu, W.Y.; Meng, W.; Jensen, C.D. NoPKI-a Point-to-Point Trusted Third Party Service Based on Blockchain Consensus Algorithm. In International Conference on Frontiers in Cyber Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 197–214.

Clohessy, T.; Acton, T. Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. Ind. Manag. Data Syst. **2019**, 119, 1457–1491.

Cong, L.W.; He, Z. Blockchain disruption and smart contracts. Rev. Financ. Stud. **2019**, 32, 1754–1797.

Das, H.; Rahman, M.; Li, S.; Tan, C. Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review. Renew. Sustain. Energy Rev. **2020**, 120, 109618.

De La Rosa, J.L., Torres-Pedrosa, V., El-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., Miralles, F., 2017. A survey of blockchain technologies for open innovation. In: Proceedings of the 4th Annual World Open Innovation Conference, pp. 14–15.

Demirkan, S.; Demirkan, I.; McKee, A. Blockchain technology in the future of business cyber security and accounting. J. Manag. Anal. **2020**, 7, 189–208.

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J., 2018. Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowl.Data Eng. 30 (7), 1366–1385.

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

Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and CommunicationsWorkshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

Dos Santos, R.B.; Torrisi, N.M.; Pantoni, R.P. Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens. Sensors **2021**, 21, 5307.

Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. J. Med. Internet Res. **2020**, 22, e13598.

Duffield, E., Diaz, D., 2015 Dash: A privacy centric cryptocurrency, GitHub.

Dujak, D.; Sajter, D. Blockchain applications in supply chain. In SMART Supply Network; Springer: Berlin/Heidelberg, Germany, 2019; pp. 21–46.

Economist, T. 2015. Blockchains: The great chain of being sure about things, Ediciónimpresa 31.

Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. IEEE Commun. Surv. Tutor. **2011**, 14, 944–980.

Farhangi, H. The path of the smart grid. IEEE Power Energy Mag. **2009**, 8, 18–28.

Francisco, K.; Swanson, D. The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics **2018**, 2, 2.

Fredj, O.B.; Cheikhrouhou, O.; Krichen, M.; Hamam, H.; Derhab, A. An OWASP top ten driven survey on web application protection methods. In International Conference on Risks and Security of Internet and Systems; Springer: Cham, Switzerland, 2020; pp. 235–252.

Fullan, O.; Ruiz, J. Accounting information systems in the blockchain era. Int. J. Intellect. Prop. Manag. **2021**, 11, 63–80.

Gao, W., Hatcher, W.G., Yu, W., 2018. A survey of blockchain: techniques, applications, and challenges, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 1–11.

Garriga, M.; Dalla Palma, S.; Arias, M.; De Renzis, A.; Pareschi, R.; Andrew Tamburri, D. Blockchain and cryptocurrencies: A classification and comparison of architecture drivers. Concurr. Comput. Pract. Exp. **2021**, 33, e5992.

Gibbs, T., Yordchim, S., 2014. Thai perception on Litecoin value. Int. J. Soc. Behav.Educ. Econom. Bus. Ind. Eng. 8 (8), 2613–2615.

Gomez, M., Bustamante, P., Weiss, M.B., Murtazashvili, I., Madison, M.J., Law, W., Mylovanov, T., Bodon, H., Krishnamurthy, P., 2019. Is Blockchain the Next Step-in the Evolution Chain of [Market] Intermediaries? Available at SSRN 3427506(3427506), 3–22.

Goranovic, A.; Meisel, M.; Fotiadis, L.; Wilker, S.; Treytl, A.; Sauter, T. Blockchain applications in microgrids an overview of current projects and concepts. In Proceedings of the 43rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2017), Beijing, China, 29 October–1 November 2017; pp. 6153–6158.

Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. IEEE Trans. Ind. Inform. **2011**, 7, 529–539.

Haber, S., Stornetta, W.S. 1990. How to time-stamp a digital document, in: Conference on the Theory and Application of Cryptography, Springer, 437–455.

Hackfeld, J., 2019. A lightweight BFT consensus protocol for blockchains, arXivpreprint arXiv:1903.11434.

Han, S.; Zhu, X. Blockchain based spectrum sharing algorithm. In Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 16–19 October 2019; pp. 936–940.

Hardjono, T.; Lipton, A.; Pentland, A. Toward an interoperability architecture for blockchain autonomous systems. IEEE Trans. Eng. Manag. **2019**, 67, 1298–1309.

Hassani, H.; Huang, X.; Silva, E. Banking with blockchained big data. J. Manag. Anal. **2018**, 5, 256–275.

Hawig, D.; Zhou, C.; Fuhrhop, S.; Fialho, A.S.; Ramachandran, N. Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data. J. Med. Internet Res. **2019**, 21, e13665.

Hearn, M. (2016). Corda-A distributed ledger. Corda Technical White Paper.

Hewa, T., Bracken, A., Ylianttila, M., Liyanage, M. 2020. Multi-access edge computing and blockchain-based secure telehealth system connected with 5Gand IoT, in: GLOBECOM 2020–2020 IEEE Global Communications Conference, IEEE, 1–6.

Houben, R., Snyers, A. 2018. Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion.

https://docs.corda.net/key-concepts.html

IBM Home Page, 2016. https://www.ibm.com/blockchain, url: https://www.ibm.com/blockchain, accessed: 12/12/ 2019.

Investopedia, 2019a. https://medium.com/on-the-origin-of-smart-contractplatforms/on-the-origin-of-cardano-a6ce4033985c, accessed: 20/06/2021.

Jabbar, R.; Dhib, E.; ben Said, A.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. IEEE Access **2022**, 10, 20995–21031.

Jabbar, R.; Fetais, N.; Kharbeche, M.; Krichen, M.; Barkaoui, K.; Shinoy, M. Blockchain for The Internet of Vehicles: How to use Blockchain to secure Vehicle-to-Everything (V2X) Communication and Payment? IEEE Sens. J. **2021**, 21, 15807–15823.

Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 310–317.

Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum. Sensors **2020**, 20, 3928.

Jabbar, R.; Krichen, M.; Fetais, N.; Barkaoui, K. Adopting Formal Verification and Model-Based Testing Techniques for Validating a Blockchain-based Healthcare Records Sharing System. In Proceedings of the 22nd International Conference on Enterprise Information Systems, Prague, Czech Republic, 5–7 May 2020; pp. 261–268.

Jabbar, R.; Shinoy, M.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Urban traffic monitoring and modeling system: An iot solution for enhancing road safety. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, 20–22 December 2019; pp. 13–18.

Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., Liang, Y., 2021. Blockchain-enabled Federated Learning Data Protection Aggregation Scheme with Differential Privacy and Homomorphic Encryption in IIoT, IEEE Trans. Ind. Inform.

Just, B.H.; Marc, D.; Munns, M.; Sandefer, R. Why patient matching is a challenge: Research on master patient index (MPI) data discrepancies in key identifying fields. Perspect. Health Inf. Manag. **2016**, 13.

Karaman, M.; Hayrettin, Ã.; Aybar, C. Institutional cybersecurity from military perspective. Int. J. Inf. Secur. Sci. **2016**, 5, 1–7.

Khujamatov, K., Reypnazarov, E., Akhmedov, N., Khazanov, D., 2020. Blockchain for5G Healthcare architecture, in: 2020 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 1–5.

Kordestani, H.; Barkaoui, K.; Zahran, W. HapiChain: A blockchain-based framework for patient-centric telemedicine. In Proceedings of the 2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH), Vancouver, BC, Canada, 12–14 August 2020; pp. 1–6.

Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.

Krichen, M.; Alroobaea, R. A New Model-based Framework for Testing Security of IoT Systems in Smart Cities using Attack Trees and Price Timed Automata. In Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2019), Heraklion, Greece, 4–5 May 2019.

Krichen, M.; Lahami, M.; Cheikhrouhou, O.; Alroobaea, R.; Maâlej, A.J. Security testing of internet of things for smart city applications: A formal approach. In Smart Infrastructure and Applications; Springer: Cham, Switzerland, 2020; pp. 629–653.

Kshetri, N. Can blockchain strengthen the internet of things? IT Prof. **2017**, 19, 68–72.

Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inf. Assoc. 2017. **24**(6), 1211–1220.

Lafourcade, P.; Lombard-Platet, M. About blockchain interoperability. Inf. Process. Lett. **2020**, 161, 105976.

Lahami, M.; Krichen, M. A survey on runtime testing of dynamically adaptable and distributed systems. Softw. Qual. J. **2021**,29, 555–593.

Lahami, M.; Krichen, M.; Barhoumi, H.; Jmaiel, M. Selective test generation approach for testing dynamic behavioral adaptations. In IFIP International Conference on Testing Software and Systems; Springer: Cham, Switzerland, 2015; pp. 224–239.

Lahami, M.; Krichen, M.; Jmaïel, M. Runtime testing approach of structural adaptations for dynamic and distributed systems. Int.J. Comput. Appl. Technol. **2015**, 51, 259–272.

Lai, R., & LEE KuoChuen, D. 2018. Blockchain – From Public to Private. Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2, 145–177. doi:10.1016/b978-0-12-812282-2.00007-3

Lakhani, K.R., Iansiti, M., 2017. The truth about blockchain. Harvard Bus. Rev. 95,118–127.

Lamport, L. et al., 2001. Paxos made simple. ACM Sigact News 32 (4), 18–25.

Lamport, L., Shostak, R., Pease, M., 2019. The Byzantine generals' problem, in: Concurrency: The Works of Leslie Lamport, ACM, 203–226.

Leyton-Brown, K.; Milgrom, P.; Segal, I. Economics and computer science of a radio spectrum reallocation. Proc. Natl. Acad. Sci. USA **2017**, 114, 7202–7209.

Li, D.; Deng, L.; Cai, Z.; Souri, A. Blockchain as a service models in the Internet of Things management: Systematic review. Trans. Emerg. Telecommun. Technol. **2020**, 33, e4139.

Li, J.; Wang, J.; Wangh, S.; Zhou, Y. Mobile payment with alipay: An application of extended technology acceptance model. IEEE Access **2019**, 7, 50380–50387.

Li, M.; Yu, S.; Ren, K.; Lou, W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In International Conference on Security and Privacy in Communication Systems; Springer: Berlin/Heidelberg, Germany, 2010; pp. 89–106.

Li, Y.; Hu, B. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. IEEE Trans. Ind. Inform. **2020**, 17, 1968–1977.

Li, Y.; Hu, B. An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. IEEE Trans. Smart Grid **2019**, 11, 2627–2637.

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., Zhang, Y., 2017. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Trans. Ind. Inf. 14 (8),3690–3700.

Li, Z.; Khajepour, A.; Song, J. A comprehensive review of the key technologies for pure electric vehicles. Energy **2019**, 182, 824–839.

Liang, Y.C. Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence; Springer: Berlin/Heidelberg, Germany, 2020.

Lilly, B.; Lilly, S. Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia. RUSI J. **2021**, 166, 46–56.

Lin, I.-C., Liao, T.-C., 2017. A survey of blockchain security issues and challenges. IJNetw. Secur. 19 (5), 653–659.

Liu, C.; Chai, K.K.; Lau, E.T.; Chen, Y. Blockchain based energy trading model for electric vehicle charging schemes. In International Conference on Smart Grid Inspired Future Technologies; Springer: Cham, Switzerland, 2018; pp. 64–72.

Liu, D., Alahmadi, A., Ni, J., Lin, X., Shen, X., 2019. Anonymous reputation system forIIoT-enabled retail marketing atop PoS blockchain. IEEE Trans. Industr. Inf. 15(6), 3527–3537.

Logo, M., van Saberhagen, N., 2014 Monero (cryptocurrency), WikiZER.

Lu, Y., 2018. Blockchain: A survey on functions, applications and open issues. J. Ind.Integr. Manage. 3 (04), 1850015.

Lumpkin, J.; Cohn, S.P.; Blair, J.S. Uniform data standards for patient medical record information. Natl. Comm. Vital Health Stat. **2003**, 53.

Maâlej, A.J.; Krichen, M. A Model Based Approach to Combine Load and Functional Tests for Service Oriented Architectures. 2016. Available online: https://dblp.org/rec/conf/vecos/MaalejK16.html.

Mainelli, M., Smith, M. 2015. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), J. Finan. Perspect. 3(3).

Manoj, M., Krishnan, S.S.R. 2020. Decentralizing Privacy Using Blockchain to Protect Private Data and ChallangesWith IPFS, in: Transforming Businesses with Bitcoin Mining and Blockchain Applications, IGI Global, 207–220, 2020.

Martinovic, I.; Kello, L.; Sluganovic, I. Blockchains for Governmental Services: Design Principles, Applications, and Case Studies; Centre for Technology and Global Affairs, University of Oxford: Oxford, UK, 2017.

Mencias, A.N., Dillenberger, D., Novotny, P., Toth, F., Morris, T.E., Paprotski, V., Dayka, J., Visegrady, T., O'Farrell, B., Lang, J., et al., 2018. An optimized blockchain solution for the IBM z14. IBM J. Res. Dev. 62 (2/3), 1–4.

Michael, J., Cohn, A., Butcher, J.R., 2018. Blockchain Technol. 1, 7.

Mihoub, A.; Fredj, O.B.; Cheikhrouhou, O.; Derhab, A.; Krichen, M. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Comput. Electr. Eng. **2022**, 98, 107716.

Min, H. Blockchain technology for enhancing supply chain resilience. Bus. Horiz. **2019**, 62, 35–45.

Mingxiao, D., Xiao Feng, M., Zhe, Z., Xiangwei, W., Qijun, C. 2017. A review on consensus algorithm of blockchain, in: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2567–2572.

Molnar, A.; Janssen, M.; Weerakkody, V. E-government theories and challenges: Findings from a plenary expert panel. In Proceedings of the 16th Annual International Conference on Digital Government Research, Phoenix, AZ, USA, 27–30 May 2015; pp. 160–166.

Mrowiec, R.; Housman, D.; White, M.; Filipova, M.; Quarre, F.; Barr, D.; Nesbitt, A.; Fedosova, K.; Killmeyer, J.; Israel, A. Blockchain: Opportunities for health care. In Proceedings of the NIST Workshop Blockchain Healthcare, Gaithersburg, MD, USA, 26–27 September 2016; pp. 1–16.

Mukhtar, H.; Rubaiee, S.; Krichen, M.; Alroobaea, R. An IoT framework for screening of COVID-19 using real-time data from wearable sensors. Int. J. Environ. Res. Public Health **2021**, 18, 4022.

Mut-Puigserver, M.; Cabot-Nadal, M.A.; Payeras-Capellà, M.M. Removing the trusted third party in a confidential multiparty registered eDelivery protocol using blockchain. IEEE Access **2020**, 8, 106855–106871.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentral. Bus.Rev., 21260

Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. J. Netw. Comput. Appl. 2020, 166, 102693.

O'brien, J.A.; Marakas, G.M. Introduction to Information Systems; McGraw-Hill/Irwin: New York, NY, USA, 2005; Volume 13.

Osei, R.K., Canavari, M., Hingley, M., 2018. An Exploration into the Opportunities for Blockchain in the Fresh Produce Supply Chain.

Palamara, P., 2018. Tracing and tracking with the blockchain.

Panigrahi, A.; Nayak, A.K.; Paul, R. HealthCare EHR: A Blockchain-Based Decentralized Application. Int. J. Inf. Syst. Supply Chain. Manag. **2022**, 15, 1–15.

Parikh, D.P.; Dhanotiya, A.; Vetrivelan, P. Blockchain-Based Secure IoT Telemedicine System. In Futuristic Communication and Network Technologies; Springer: Berlin/Heidelberg, Germany, 2022; pp. 923–935.

Park, Y.R.; Lee, E.; Na, W.; Park, S.; Lee, Y.; Lee, J.H. Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility. J. Med. Internet Res. **2019**, 21, e12533.

Pei, Y.; Hu, S.; Zhong, F.; Niyato, D.; Liang, Y.C. Blockchain-enabled dynamic spectrum access: Cooperative spectrum sensing, access and mining. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.

Peši´c, S.; Radovanovi´c, M.; Ivanovi´c, M.; Toši´c, M.; Ikovi´c, O.; Boškovi´c, D. Hyperledger fabric blockchain as a service for the IoT: Proof of concept. In International Conference onModel and Data Engineering; Springer: Berlin/Heidelberg, Germany, 2019; pp. 172–183.

Polkowski, Z., Nycz, M., Borah, S., 2018. Blockchain Implementation in Business. Sci.Bull. Econ. Sci. 17 (3), 187–196.

Qasse, I.A., Abu Talib, M., Nasir, Q., 2019. Inter blockchain communication: A survey. In: Proceedings of the ArabWIC 6th Annual International Conference Research Track, pp. 1–6.

Qiu, J.; Grace, D.; Ding, G.; Yao, J.; Wu, Q. Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective. IEEE Internet Things J. **2019**, 7, 451–466.

Rossi, M.; Mueller-Bloch, C.; Thatcher, J.B.; Beck, R. Blockchain research in information systems: Current trends and an inclusive future research agenda. J. Assoc. Inf. Syst. **2019**, 20, 14.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., Mohaisen, A.,2019. Exploring the attack surface of blockchain: A systematic overview, arXivpreprint arXiv:1904.03487.

Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. **2019**, 57, 2117–2135.

Sandip Chakraborty, P.J., 2018 Blockchain architecture, design and use case, nptellecture series.

Sankar, L.S., Sindhu, M., Sethumadhavan, M., 2017. Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 1–5, 2017.

Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards blockchain interoperability. In International Conference on Business Process Management; Springer: Berlin/Heidelberg, Germany, 2019; pp. 3–10.

Shaverdian, P. Start with Trust: Utilizing Blockchain to Resolve the Third-Party Data Breach Problem. UCLA L. Rev. **2019**, 66, 1242.

Shrobe, H.; Shrier, D.L.; Pentland, A. Enigma: Decentralized Computation Platform with Guaranteed Privacy. In New Solutions for Cybersecurity; MIT Press: Cambridge, MA, USA, 2018; Chapter 15, pp. 425–454.

Siba, T.K., Prakash, A. (2016). Block-chain: an evolving technology. Glob. J. Enterp. Inf. Syst. **8**(4).

Singh, A.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R.; Dehghantanha, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Comput. Secur. **2020**, 88, 101654.

Srinivasu, P.N., Bhoi, A.K., Nayak, S.R., Bhutta, M.R., Woz´ niak, M., 2021. Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. Electronics 10 (12), 1437.

Suliman, A.; Husain, Z.; Abououf, M.; Alblooshi, M.; Salah, K. Monetization of IoT data using smart contracts. IET Netw. **2019**, 8, 32–37.

Surati, S., Shrimali, B., Patel, H., 2021. Introduction of Blockchain and 5G-enabled IoTDevices, chap. 4. Springer International Publishing, Cham, pp. 83–105.

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

Tangsen, H.; Li, X.; Ying, X. A Blockchain-Based Node Selection Algorithm in CognitiveWireless Networks. IEEE Access **2020**, 8, 207156–207166.

Todd, P. (2015). Ripple Protocol Consensus Algorithm Review.

Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. **2016**, 18, 2084–2123.

Ubin URL, 2019. https: ://www.mas.gov.sg/singapore-financial-centre/smartfinancial-centre/project-ubin.aspx.

URL, 2019c. https://fortune.com/2014/07/31/stripe-launches-bitcoin-challengergives-it-away-for-free.

Vukolic´, M., 2015. The quest for scalable blockchain fabric: Proof-of-work vs. BFTreplication, in: International workshop on open problems in network security, Springer, 112–125.

Vukolic´, M., 2017. Rethinking permissioned blockchains, in: Proceedings of the ACMWorkshop on Blockchain, Cryptocurrencies and Contracts, 3–7, 2017.

Wang, J.; Ling, X.; Le, Y.; Huang, Y.; You, X. Blockchain-enabled wireless communications: A new paradigm towards 6G. Natl. Sci. Rev. 2021, 8, nwab069.

Wang, W.; Wang, L.; Zhang, P.; Xu, S.; Fu, K.; Song, L.; Hu, S. A privacy protection scheme for telemedicine diagnosis based on double blockchain. J. Inf. Secur. Appl. **2021**, 61, 102845.

Watanabe, H.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J. Blockchain contract: Securing a blockchain applied to smart contracts. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–11 January 2016; pp. 467–468.

Wazid, M., Bera, B., Mitra, A., Das, A.K., Ali, R., 2020. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. In: Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, pp. 37–42.

Weiss, M.B.; Werbach, K.; Sicker, D.C.; Bastidas, C.E.C. On the application of blockchains to spectrum management. IEEE Trans. Cogn. Commun. Netw. **2019**, 5, 193–205.

Wikipedia, 2019. https://en.wikipedia.org/wiki/wikipedia:what-is-consensus.

Wood, G. et al., 2014. Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper 151. **2014**, 1–32.

Wörner, D.; von Bomhard, T. When your sensor earns money: Exchanging data for cash with Bitcoin. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014; pp. 295–298.

Wu, Y., Dai, H.-N., Wang, H., 2020. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE IoT J. 8(4), 2300–2317.

Xiaoding, W., Garg, S., Lin, H., Jalilpiran, M., Hu, J., Hossain, M.S., 2021. Enabling secure authentication in industrial iot with transfer learning empowered blockchain, IEEE Trans. Indus. Inform.

Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. **2019**, 21, 2794–2830.

Yaga, D., Mell, P., Roby, N., Scarf one, K., 2019. Blockchain technology overview, arXivpreprint arXiv:1906.11078.

Yao, X.; Zhu, T. Blockchain is to create a new ecology of cross-border payment. Financ. Expo **2017**, 5, 46–48.

Zhang, K., Zhu, Y., Maharjan, S., Zhang, Y., 2019. Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things. IEEE Network 33(5), 12–19.

Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain technology use cases in healthcare. In Advances in Computers; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.

Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **2018**, 16, 267–278.

Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 184–191.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE international congress on big data (Bigdata congress), IEEE, pp. 557–564.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 14 (4), 352–375.

Zhou, Q., Yang, Y., Chen, J., Liu, M., 2018. Review on Blockchain Application for Internet of Things. In: International Conference on Cloud Computing and Security, Springer, pp. 724–733.

Zhu, Y.; Zhang, X.; Ju, Z.Y.; Wang, C.C. A study of blockchain technology development and military application prospects. In Journal of Physics: Conference Series; IOP Publishing: Bristol, UK, 2020; Volume 1507, p. 052018.

Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. IEEE J. Biomed. Health Inform. **2020**, 24, 2169–2176.

Zidi, S.; Mihoub, A.; Qaisar, S.M.; Krichen, M.; Al-Haija, Q.A. Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. J. King Saud-Univ.-Comput. Inf. Sci. **2022**.

IBAX Network.; ibaxnetwork.medium.com/blockchain-evolution-from-1-0-to-4-0-

18aa9ca2dbbb

hhs.gov.; https://www.hhs.gov/sites/default/files/blockchain-for-healthcare-tlpwhite.pdf