ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΜΗΧΑΝΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΤΟΜΕΑΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΈΡΕΥΝΑΣ
ΕΡΓΑΣΤΗΡΙΟ ΟΡΓΑΝΩΣΗΣ ΠΑΡΑΓΩΓΗΣ

ΑΝΑΛΥΣΗ ΕΡΓΑΛΕΙΩΝ BLOCKCHAIN ΓΙΑ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ: ΑΝΑΣΚΟΠΗΣΗ ΤΟΥ ΕΡΕΥΝΗΤΙΚΟΥ ΠΕΔΙΟΥ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΘΑΝΑΣΟΠΟΥΛΟΣ ΝΙΚΟΛΑΟΣ

Εποπτεία : Ηλίας Τατσιόπουλος
Καθηγητής Ε.Μ.Π.

Επίβλεψη: Γεώργιος Παπαδόπουλος
Δρ.,Ε.ΔΙ.Π., Ε.Μ.Π

Αθήνα, Ιούλιος 2021

Περίληψη

Είναι ευρέως γνωστό ότι ολοένα και περισσότερες προκλήσεις όπως η ψηφιοποίηση και αυτοματοποίηση των επιχειρήσεων καθώς και η ελαχιστοποίηση του κόστους των προϊόντων μέσα στο σύγχρονο ανταγωνιστικό επιχειρηματικό περιβάλλον οδηγούν τις εταιρείες σε καινοτόμες τεχνολογίες οι οποίες μπορούν να προσφέρουν λύση στα προβλήματα αυτά. Παράλληλα, οι μεγάλες και πολύπλοκες σύγχρονες εφοδιαστικές αλυσίδες παρουσιάζουν αρκετά εμπόδια για την επίτευξη διαφάνειας και αποτελεσματικότητας σε αυτές. Η τεχνολογία του blockchain αποτελεί μια από τις πιο ραγδαία αναπτυσσόμενες τεχνολογίες του σήμερα με εφαρμογή σε αρκετούς τομείς των επιχειρήσεων, επιτρέπει δε την ασφαλή και κρυπτογραφημένη καταγραφή ψηφιακών συναλλαγών μέσω της χρήσης ενός αποκεντρωμένου κατανεμημένου ledger. Έτσι, όλοι οι συμμετέχοντες στο δίκτυο του blockchain μπορούν να παρακολουθούν σε πραγματικό χρόνο τις λεπτομέρειες των συναλλαγών καθώς και την τοποθεσία προϊόντων της εταιρείας, με αποτέλεσμα την ανάπτυξη διαφάνειας και εμπιστοσύνης κατά μήκος όλης της εφοδιαστικής αλυσίδας.

Στην συγκεκριμένη διπλωματική εργασία παρουσιάζεται μια ανάλυση του τρόπου λειτουργίας των τεχνολογιών blockchain, των βασικών στοιχείων του και σκοπών του καθώς και τα θετικά αποτελέσματα που απορρέουν από την χρήση του σε επιχειρήσεις και ιδιαίτερα στην εφοδιαστική τους αλυσίδα. Δίνεται, επίσης, ιδιαίτερη σημασία στην σύγκριση του δημόσιου και του ιδιωτικού blockchain με έμφαση στο κομμάτι των smart contracts, για να προκύψει συμπέρασμα σχετικά με το ποιό από αυτά είναι καταλληλότερο για χρήση σε εφαρμογές εφοδιαστικής αλυσίδας. Ακόμη, αναλύονται εργαλεία βελτιστοποίησης κώδικα smart contracts και οι θετικές επιδράσεις αυτών στην απόδοση και την γενικότερη λειτουργία τους. Πραγματοποιείται, ακόμη, μια δομημένη βιβλιογραφική ανασκόπηση με την βοήθεια του scopus στο κομμάτι της χρήσης blockchain σε εφαρμογές ποτών και αναψυκτικών, για να προκύψουν χρήσιμα συμπεράσματα για τα οφέλη του στο πεδίο αυτό, ενώ τέλος ακολουθούν οι πρακτικές εφαρμογές των τεχνολογιών blockchain σε επιχειρήσεις με ορισμένες μελέτες περίπτωσης.

Abstract

Undoubtedly, today's highly competitive market environment demands ever increasing digitization while maintaining the highest possible level of transparency and trust, thus driving businesses to look for innovative technologies that can help. Moreover, the complex nature of modern supply chains imposes even more challenges regarding transparency and efficiency that need to be addressed. Blockchain is one of the most rapidly advancing technologies of the 21st century, allowing safe and encrypted transactions between participating parties, through the use of a decentralized, distributed and digitized ledger that records every transaction in the blockchain network. This provides the necessary framework for real-time tracking of products and the details of those transactions that ultimately allows for greater trust and transparency through the whole supply chain.

This thesis presents an in-depth analysis of the technologies used in blockchain networks, how they work and the advantages that they can offer if adopted by businesses for their supply chains. Moreover, it emphasizes the differences between public and private blockchains in order to provide some insight regarding which is the better choice for supply chain applications. It also explores the literature concerning smart contracts code analysis tools and their benefits to the overall performance of the network. Furthermore, a literature review and analysis is performed on blockchain applications in the beverages and wine sector with the help of Scopus database in order to find interesting conclusions, and last but not least some case studies of blockchain application in supply chain management are presented.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Ηλία Τατσιόπουλο για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον θέμα. Επίσης θα ήθελα να ευχαριστήσω τον κ. Γεώργιο Παπαδόπουλο για την καθοδήγηση και τη βοήθεια που μου προσέφερε.

Επιπλέον, ένα μεγάλο ευχαριστώ σε όλους μου τους φίλους και τους συμφοιτητές για τη βοήθειά και τη συμπαράστασή τους όλα αυτά τα χρόνια.

Τέλος, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για την απλόχερη υλική και ηθική συμπαράσταση σε όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

Κατάλογος Εικόνων

1.Θεωρητικό Υπόβαθρο Blockchain

Το blockchain είναι μια peer-to-peer κατανεμημένη βάση δεδομένων η οποία επιτρέπει τις διάφορες συναλλαγές μεταξύ των κόμβων (nodes) του δικτύου χωρίς την ανάγκη ύπαρξης ενός κεντρικού φορέα εμπιστοσύνης, όπως για παράδειγμα μια τράπεζα. Οι συναλλαγές αυτές καταγράφονται σε ένα ledger, και κάθε κόμβος στο δίκτυο έχει ένα αντίγραφό του. Οι πληροφορίες της κάθε συναλλαγής καταγράφονται σε ένα block, το οποίο προστίθεται μετά από το προηγούμενο block, το οποίο περιέχει την προηγούμενη συναλλαγή. Έτσι δημιουργείται μια δομή αλυσίδας, το blockchain. Τις πληροφορίες και τις λεπτομέρειες της συναλλαγής μπορούν να τις δουν όλοι οι συμμετέχοντες, ωστόσο η αλλαγή η ή αλλοίωση των πληροφοριών αυτών είναι πρακτικά αδύνατη για λόγους που θα εξηγηθούν στη συνέχεια. Αξίζει να σημειωθεί ότι κάθε μπλοκ περιέχει πληροφορίες για το προηγούμενο μπλοκ στην αλυσίδα και άρα συνδέεται με αυτό, πράγμα το οποίο ισχύει για όλα τα μπλοκ στο δίκτυο. Αυτός είναι και ένα από τα θεμελιώδη στοιχεία του blockchain και ο βασικός τρόπος διασφάλισης της αλυσίδας (Conway, 2020).

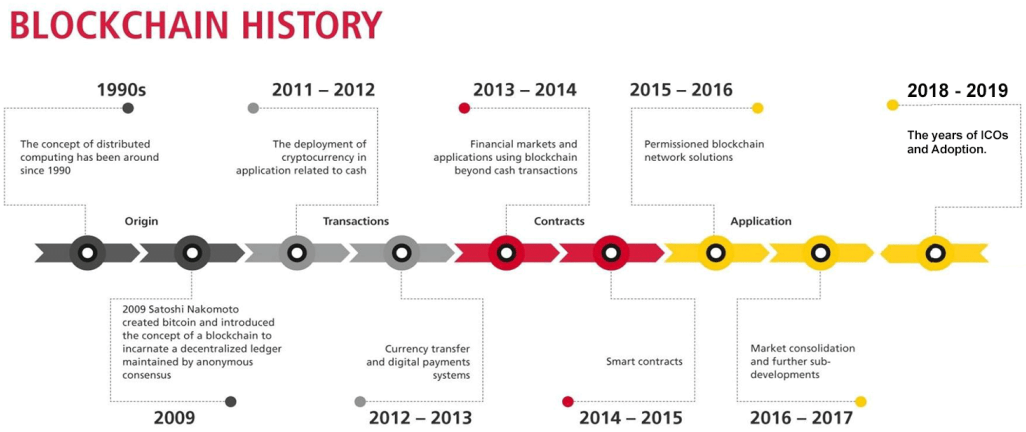
Εικόνα 1: Blockchain

Πηγή: www.insidehighered.com

1.1 Εξέλιξη του Blockchain

Το blockchain είναι μια από τις σημαντικότερες τεχνολογίες τον 21^{ο} αιώνα λόγω των πολλαπλών εφαρμογών που έχει σε όλους τους τομείς της καθημερινότητας, από τράπεζες, βιομηχανίες μέχρι και τρόφιμα αλλά και την εκπαίδεση. Αποτελεί μια σχετικά νέα

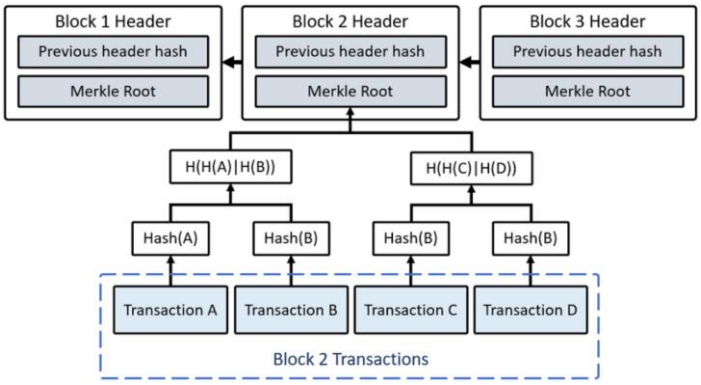
τεχνολογία η οποία έχει αρκετά στάδια ανάπτυξης. Για να γίνει πιο εύκολα αντιληπτή η τεχνολογία αυτή και το πώς μπορεί να βοηθήσει τους τομείς αυτούς, απαιτείται πρώτα να παρουσιασθεί η ιστορία της εξέλιξής της.



Εικόνα 2: Εξέλιξη του Blockchain

Πηγή: ecommerceguider.com

Το 1991 οι Stuart Haber και Scott Stornetta δημοσιεύουν το έργο τους το οποίο καλύπτει κρυπτογραφικά ασφαλισμένες αλυσίδες απο μπλοκ, τα οποία περιέχουν αρχεία τα οποία δεν μπορούν να παραβιαστούν και να αλλοιωθούν. Το 1992 ανανεώνουν την ιδέα τους ώστε να περιέχει δέντρα Merkle τα οποία αυξάνουν την αποδοτικότητα του blockchain και άρα επιτρέπουν την αποθήκευση περισσότερων αρχείων σε αυτό. Η δουλειά τους αυτή είναι αρκετά σημαντική, ωστόσο είναι το 2008 όταν η τεχνολογία του blockchain αρχίζει να λαμβάνει περισσότερη προσοχή (Iredale, 2020).



Εικόνα 3: Merkle Trees

Πηγή: www.researchgate.net

Το 2008, λοιπόν, ένα άτομο ή ομάδα ατόμων υπό το ψευδώνυμο Satoshi Nakamoto εφεύρει το blockchain όπως είναι γνωστό σήμερα, δηλαδή ως ένα transaction ledger για το κρυπτονόμισμα του Bitcoin. Η ομάδα αυτή δημοσιεύει το έργο αυτό για να προσπαθήσει να λύσει το πρόβλημα της εμπιστοσύνης και την αποκέντρωσης που απαιτούνται όταν λαμβάνουν χώρα ψηφιακές συναλλαγές. Αυτό σημαίνει ότι από τα συμβαλλόμενα μέρη, κανένας δεν έχει κεντρικό και κύριο έλεγχο στο σύστημα.

Όπως φαίνεται και στο παραπάνω σχήμα, περί το 2011 συμβαίνουν οι πρώτες χρηματικές συναλλαγές με cryptocurrency, ενώ το 2013 οι εφαρμογές blockchain αρχίζουν να ερευνώνται και να εφαρμόζονται και σε άλλους τομείς. Το 2014-2015 δημιουργούνται τα smart contracts και το 2016 το blockchain εφαρμόζεται σε πληθώρα τομέων που το χρησιμοποιούν ως δίκτυο ανταλλαγής δεδομένων. Συνεπώς οι φάσεις εξέλιξης του blockchain είναι 3:

Φάση 1η: Συναλλαγές Bitcoin

Στην πρώτη φάση εξέλιξης του blockchain διακρίνονται οι συναλλαγές σε Bitcoin. Ο/Οι Satoshi Nakamoto έφτιαξαν το αρχικό μπλοκ στην αλυσίδα του Bitcoin στο οποίο ακουλήθησαν και τα επόμενα μπλοκ, με μια διαδικασία mining η οποία θα αναλυθεί σε επόμενο κομμάτι. Το Bitcoin ήταν αρκετά πετυχημένο και ώθησε πολλούς οργανισμούς να επενδύσουν σε αυτό.

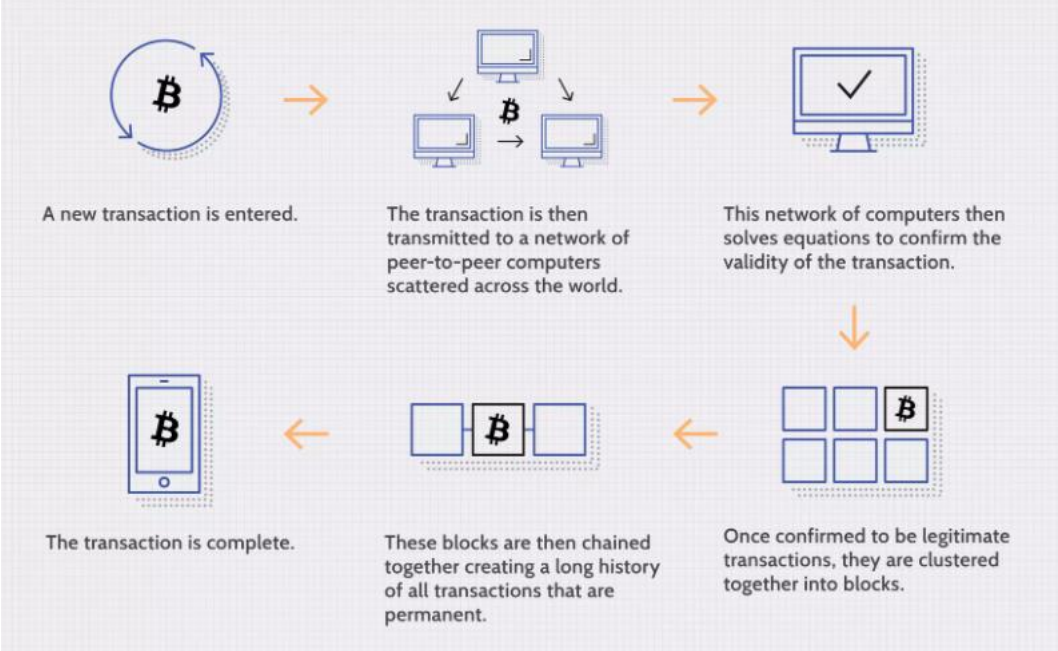
Φάση 2η: Contracts

Το 2013 ο Vitalik Buterman, ένας Ρωσοκαναδός προγραμματιστής ο οποίος συμμετείχε στο δίκτυο του blockchain , αναγνώρισε κάποιες δυσκολίες που περιείχε το δίκτυο αυτό όσον αφορά σε θέματα επεκτασιμότητας του για εφαρμογές πέρα των συναλλαγών. Έτσι, αποφάσισε να φτιάξει μια δικιά του πλατφόρμα η οποία θα περιείχε την ιδέα των συμβολαίων (contracts) μεταξύ συμβαλλόμενων μερών. Έτσι λοιπόν, φτιάχτηκε το Ethereum το οποίο αποτελεί μια πλατφόρμα ανάπτυξης αποκεντρωμένων εφαρμογών (decentralized applications). Σε αυτή την πλατφόρμα είναι δυνατή η διεκπεραίωση smart contracts, τα οποία είναι μεγάλης σημασίας σε εφαρμογές ιχνηλασιμότητας στην εφοδιαστική αλυσίδα, όπως θα φανεί άλλωστε και στο κεφάλαιο των case studies.

Φάση 3η: Εφαρμογές blockchain

Μετά την ανάπτυξη των Bitcoin και Ethereum, η τεχνολογία blockchain πέρασε στην φάση των ολοκληρωμένων εφαρμογών σε διάφορους τομείς. Χαρακτηριστικά παραδείγματα αποτελούν οι πλατφόρμες NEO και IOTA, οι οποίες έχουν αναπτυχθεί για να λύσουν προβλήματα όπως τα μεγάλα κόστη συναλλαγών (transaction fees). Άλλες τεχνολογίες blockchain όπως οι Monero Zcash και Dash λύνουν το πρόβλημα της επεκτασιμότητας του blockchain που υπάρχουν στις προηγούμενες φάσεις του. Σε αυτή τη φάση, επιπροσθέτως, υπάρχουν και αρκετές εταιρείες (όπως η Microsoft) που αναπτύσσουν ιδιωτικές πλατφόρμες blockchain, ώστε να μεγιστοποιήσουν την αποδοτικότητα τους στο εσωτερικό τους περιβάλλον (Iredale, 2020).

1.2 Λειτουργία του Blockchain



Εικόνα 4: Εκτέλεση συναλλαγής στο δίκτυο του blockchain

Πηγή: www.investopedia.com

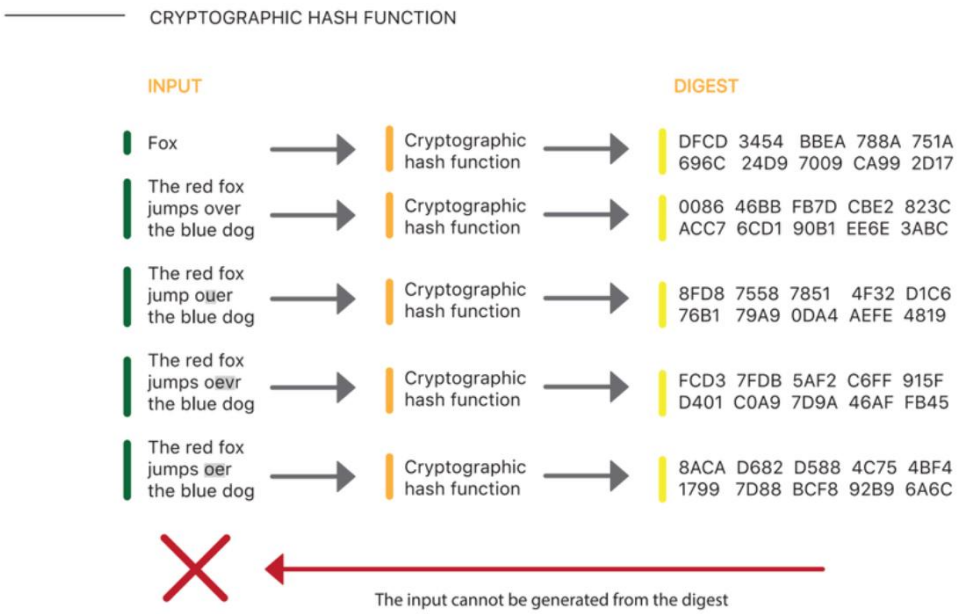
Για να προστεθεί μια καταγραφή στο δίκτυο του blockchain, πρέπει να λάβει χώρα μια συγκεκριμένη διαδικασία (IBM, 2021).

Καταρχάς, δημιουργείται ένα αρχείο το οποίο περιέχει όλες τις απαραίτητες πληροφορίες για τη συγκεκριμένη συναλλαγή. Αυτές μπορεί για παράδειγμα να είναι το ποσό της συναλλαγής, οι πληροφορίες του κάθε συμμετέχοντος, η ώρα της συναλλαγής και οι όροι υπό τους οποίους συμβαίνει. Το αρχείο αυτό περιέχει, επίσης, την ψηφιακή υπογραφή των συμμετέχοντων, η οποία είναι μοναδική για κάθε κόμβο στο δίκτυο. Το αρχείο, στη συνέχεια, μεταδίδεται μέσα στο peer-to-peer δίκτυο το οποίο ελέγχει την εγκυρότητα της συναλλαγής, με μια διαδικασία επίλυσης-ταυτοποίησης (Academy Binance, 2020).

Πολλές τέτοιες συναλλαγές συγκεντρώνονται και διαμορφώνουν ένα block. Το block αυτό προστίθεται μετά το προηγούμενο block, δημιουργώντας μια μορφή αλυσίδας. Το κάθε block περιέχει έναν κωδικό hash (hash code), καθώς και το hash code του προηγούμενου block. Οι κωδικοί αυτοί είναι ουσιαστικά κρυπτογραφημένες πληροφορίες για τη συναλλαγή, καθώς και η σειρά με την οποία έχουν προστεθεί στην αλυσίδα.

Οι κωδικοί αυτοί προκύπτουν από μια μαθηματική συνάρτηση ονόματι hash function, η οποία έχει ως είσοδο όλες τις πληροφορίες της συναλλαγής, και ως έξοδο μια σειρά από αλφαριθμητικούς χαρακτήρες (η οποία έχει πάντα σταθερό μήκος). Η μαθηματική αυτή συνάρτηση είναι το “κλειδί”της ασφάλειας στο δίκτυο του blockchain, λόγω των ιδιοτήτων που έχει (Rosic, 2020).

1.3 Hash Functions



Εικόνα 5: Λειτουργία των cryptographic hash functions

Πηγή: www.researchgate.net

Οι κρυπτογραφικές συναρτήσεις hash (cryptographic hash functions) έχουν μια σειρά από ιδιότητες οι οποίες προσφέρουν μεγάλη ασφάλεια σε εφαρμογές όπως το blockchain. Συνήθως, σε τέτοιες εφαρμογές, γίνεται λόγος για Trapdoor One Way Functions (TOWF). Οι ιδιότητες τους είναι (Rhodes, 2020):

Μονοδρομία (Pre-image Resistance): Το hash προκύπτει εύκολα από την είσοδο, ενώ γνωρίζοντας το hash είναι πρακτικά αδύνατο να υπολογιστεί η είσοδος. Αυτή η ιδιότητα προσφέρει προστασία σε περιπτώσεις που κάποιο κακόβουλο στοιχείο γνωρίζει το hash και θέλει να βρει τα στοιχεία της συναλλαγής.

Διάχυση (avalanche effect): Μια οσοδήποτε μικρή αλλαγή στην είσοδο της hash function επιφέρει τεράστια αλλά και απρόβλεπτη αλλαγή στην έξοδο της (δηλαδή το hash). Αυτή η ιδιότητα προσφέρει προστασία σε περίπτωση που υπάρχει προσπάθεια brute force για την εύρερη των στοιχείων της συναλλαγής.

Ντετερμινισμός: Η ίδια είσοδος στη συνάρτηση θα πρέπει να οδηγεί πάντα στην ίδια έξοδο (ίδιο hash).

Second Pre-image Resistance: Δεδομένου μιας εισόδου και μιας εξόδου hash code, θα πρέπει να είναι όσο το δυνατόν δυσκολότερο να βρεθεί μια διαφορετική είσοδος η οποία να οδηγεί στο ίδιο hash code. Αυτή η ιδιότητα προσφέρει προστασία ενάντια σε περιπτώσεις όπου κάποιο κακόβουλο στοιχείο προσπαθεί να αντικαταστήσει την πραγματική είσοδο-στοιχεία μιας συναλλαγής με μια άλλη.

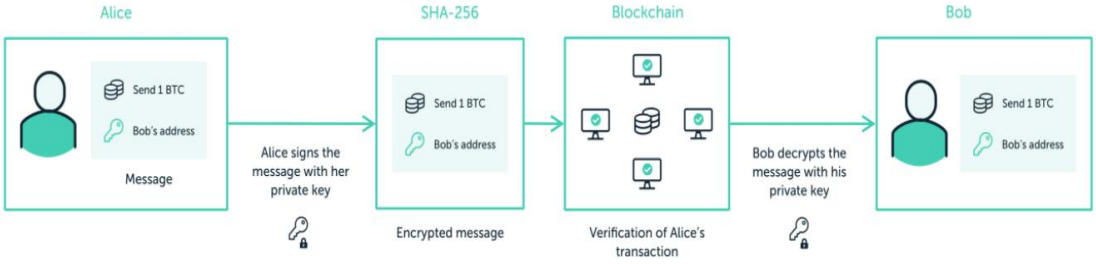
Collision Resistance: Θα πρέπει να είναι υπολογιστικά αδύνατο να βρεθούν 2 διαφορετικές είσοδοι (χωρίς την γνώση οποιασδήποτε από τις 2), οι οποίες θα οδηγούν στο ίδιο hash code. Αξίζει να σημειωθεί ότι αν μια TOWF είναι Collision Resistant, είναι και Second Pre-Image Resistant (Frankenfield, 2020).

1.4 Δημόσια-Ιδιωτικά Κλειδιά

Η διαδικασία ηλεκτρονικής υπογραφής της συναλλαγής που προαναφέρθηκε πραγματοποιείται με την βοήθεια των δημόσιων και των ιδιωτικών κλειδιών. Βασίζεται στην ίδια ιδέα με τις TOWF, δηλαδή ότι ο υπολογισμός προς μια κατεύθυνση θα πρέπει να είναι υπολογιστικά εύκολος, ενώ ο υπολογισμός προς την αντίθετη κατεύθυνση να είναι υπολογιστικά και πρακτικά ανέφικτος. Κάθε κόμβος στο δίκτυο του blockchain έχει ένα ζεύγος από ηλεκτρονικά κλειδιά, ένα δημόσιο (public) και ένα ιδιωτικό (private). Ο σκοπός των 2 αυτών κλειδιών είναι να μπορεί να αποδειχθεί ότι μια συναλλαγή όντως έχει υπογραφεί από τους κόμβους που την πραγματοποιούν, μέσα στο δίκτυο του blockchain (Tutorials Point, 2020).

Το ιδιωτικό κλειδί είναι αυτό που ουσιαστικά καθορίζει τον κάτοχο των «κεφαλαίων». Το κλειδί αυτό ξεκλειδώνει το δικαίωμα στον κάτοχο να χρησιμοποιήσει τα κεφάλαια αυτά. Εννοείται ότι στην γενική περίπτωση τα κεφάλαια αυτά δεν είναι απαραίτητα χρήματα ή κρυπτονομίσματα, αλλά μπορεί να είναι για παράδειγμα ψηφιακά δικαιώματα ή οτιδήποτε άλλο έχει αξία και μπορεί να αποδειχθεί ηλεκτρονικά. Το ιδιωτικό κλειδί, λοιπόν, θα πρέπει να είναι γνωστό μόνο στον κάτοχο των κεφαλαίων αυτών (Massessi, 2018).

Μαζί με το ιδιωτικό κλειδί, ο κάθε κόμβος έχει και ένα δημόσιο κλειδί, το οποίο σχετίζεται με το ιδιωτικό κλειδί μέσω μιας κρυπτογραφικής συνάρτησης. Το βασικό κομμάτι της εξίσωσης αυτής είναι ότι το δημόσιο κλειδί προκύπτει εύκολα από το ιδιωτικό, ενώ το αντίστροφο είναι πρακτικά αδύνατο (Well, 2019).



Εικόνα 6: Χρήση κλειδιών για την μεταφορά κεφαλαίων

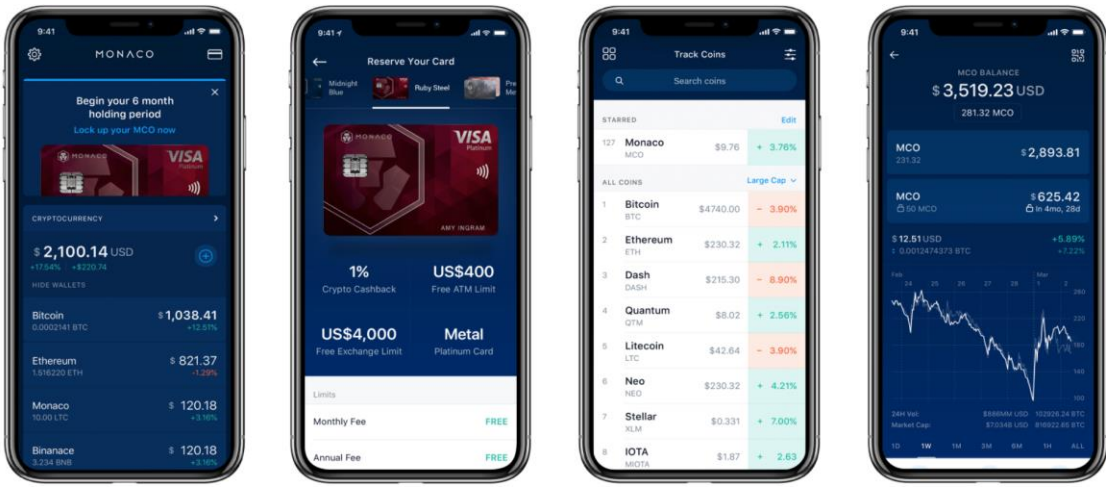
Πηγή: www.ledger.com

Ένα παράδειγμα συναλλαγής: Ο αποστολέας αποφασίζει να στείλει κάποια ποσότητα κρυπτονομισμάτων σε έναν δέκτη, μέσα στο δίκτυο του blockchain. Οι πληροφορίες της συναλλαγής είναι η ποσότητα κρυπτονομισμάτων και η ηλεκτρονική ταυτότητα του δέκτη. Ο αποστολέας υπογράφει ηλεκτρονικά την συναλλαγή με το ιδιωτικό κλειδί. Ολόκληρο το αρχείο, στη συνέχεια, κρυπτογραφείται με έναν αλγόριθμο (ο πιο κοινός είναι ο SHA-256). Το hash της συναλλαγής προκύπτει και από το δημόσιο κλειδί του δέκτη. Με τη σύγκριση αυτή του δημόσιου, του ιδιωτικού κλειδιού αλλά και του αποτελέσματος της κρυπτογράφησης (το hash) στο δίκτυο του blockchain, είναι δυνατή η επαλήθευση των συμμετεχόντων της συναλλαγής. Ωστόσο, για να γίνει η αποκρυπτογράφηση των λεπτομερειών, απαιτείται το ιδιωτικό κλειδί του δέκτη. Έτσι, όλο το δίκτυο γνωρίζει ότι το μήνυμα αυτό είναι σωστό και ταυτοποιημένο, ωστόσο οι λεπτομέρειες του μηνύματος είναι γνωστές μόνο στον αποστολέα και στον δέκτη. Συνεπώς, ακόμα και αν υπάρχει πρόσβαση στο μήνυμα κατά την μεταφορά, η οποιαδήποτε αλλαγή του είναι αδύνατη αφού καταρχάς θα αλλάξει το hash, και επίσης δεν είναι γνωστά τα ιδιωτικά κλειδιά του αποστολέα και του

δέκτη. Γι'αυτό, λοιπόν, τα ιδιωτικά κλειδιά θα πρέπει να παραμένουν αποθηκευμένα σε ασφαλές μέρος από κάθε κόμβο (Conway, 2020).

1.5 Εφαρμογές Wallet

Για να συμμετέχει κάποιος στις συναλλαγές μέσω blockchain θα πρέπει να χρησιμοποιεί κάποια εφαρμογή wallet (Rosic, 2020). Αυτή η εφαρμογή αποθηκεύει το δημόσιο και το ιδιωτικό κλειδί του χρήστη και αλληλεπιδρά με το δίκτυο του blockchain για την εκτέλεση των συναλλαγών σε αυτό. Γενικά χωρίζονται σε 3 διαφορετικά είδη, τα software, hardware και paper, με τα software να είναι τα πιο κοινά από άποψης χρηστικότητας (Sharma, 2021). Αξίζει να υπογραμμιστεί ότι τα crypto wallets δεν αποθηκέυουν τα διάφορα κρυπτονομίσματα, αλλά παρέχουν τα εργαλεία τα οποία απαιτούνται για την αλληλεπίδραση με το δίκτυο. Τα wallets αυτά παρέχουν και την μοναδική «διεύθυνση» του χρήστη (address), η οποία είναι ένας μοναδικός κωδικός ο οποίος προκύπτει από το δημόσιο και το ιδιωτικό κλειδί. Η διεύθυνση αυτή είναι ουσιαστικά ο ηλεκτρονικός τόπος στον οποίο μπορούν να σταλούν κρυπτονομίσματα. Ως εκ τούτου, η διεύθυνση αυτή είναι δημόσια και απαιτείται να την γνωρίζει αυτός που πρόκειται να στείλει κρυπτονομίσματα εκεί.



Εικόνα 7 : Εφαρμογή crypto wallet για κινητό

Πηγή: www.blog.crypto.com

1.5.1 Software wallets

Τα λογισμικά wallet είναι συνήθως hot wallets, δηλαδή συνδέονται μέσω διαδικτύου για την λειτουργία τους. Χωρίζονται σε web, desktop και mobile τύπους.

Web Wallets

Τα web wallets χρησιμοποιούν περιβάλλον από περιηγητή διαδικτύου για να λειτουργήσουν, και άρα δεν απαιτείται κάποια εγκατάσταση λογισμικού στον ίδιο τον υπολογιστή ή το κινητό τηλέφωνο. Αρκετές φορές, κάποια τέτοια wallets κρατούν το ζεύγος κλειδιών στους servers της εταιρείας, αντί για την ίδια την συσκευή, για να μην χρειάζεται η απομνημόνευση τους από τον χρήστη. Αυτό είναι ένα χαρακτηριστικό που βοηθάει αρκετά στην ευχρηστία του, ωστόσο τότε ο χρήστης εμπιστεύεται τα χρήματα του στην εταιρεία και την καλή λειτουργία της. Τα τελευταία χρόνια έχουν εμφανιστεί και αρκετά wallets τα οποία επιτρέπουν την πολλαπλή ψηφιακή υπογραφή και άρα επιτρέπουν στον χρήστη να έχει κάποιο ή εξ ολοκλήρου έλεγχο στα κρυπτονομίσματα του. Ένα παράδειγμα τέτοιου wallet είναι το Metamask.io το οποίο λειτουργεί σαν απλό browser extension.

Desktop Wallets

Τα Desktop Wallets είναι εφαρμογές οι οποίες εγκαθίστανται στον ηλεκτρονικό υπολογιστή του χρήστη και άρα αποθηκεύουν εκεί το χεύγος κλειδιών του. Έτσι, ο χρήστης έχει τον αποκλειστικό έλεγχο των κεφαλαίων του, οποιαδήποτε στιγμή τα χρειαστεί. Κατά την εγκατάσταση της εφαρμογής δημιουργείται ένα αρχείο wallet.dat το οποίο ουσιαστικά έχει το δημόσιο και το ιδιωτικό κλειδί του χρήστη. Αυτό το αρχείο, για την μεγιστοποίηση της ασφάλειας των κεφαλαίων, συνήθως θα πρέπει να κρυπτογραφείται από κάποιο πρόγραμμα, και να φυλάσσεται σε ασφαλές μέρος το οποίο δεν είναι εύκολα προσβάσιμο (για παράδειγμα όχι στην επιφάνεια εργασίας). Ωστόσο, αν ο χρήστης χάσει τον κωδικό για την αποκρυπτογράφηση, κατά πάσα πιθανότητα χάνει και το κεφάλαιο του. Συνεπώς, κρίνεται πολύ σημαντική η ύπαρξη backup του αρχείου αυτού (συνήθως σε ασφαλές USB stick) ώστε σε περίπτωση βλάβης του υπολογιστή ή του αρχείου αυτού, να μπορεί ο χρήστης να έχει πρόσβαση στον λογαριασμό του. Ένα παράδειγμα τέτοιου wallet είναι το Ledger.

Mobile Wallets

Τα Mobile Wallets είναι σχεδιασμένα ειδικά για χρήση σε smartphones και άρα είναι πολύ πιο εύχρηστα για καθημερινή χρήση κρυπτονομισμάτων, όπως για παράδειγμα σε βενζινάδικα και σούπερ μάρκετ. Συνήθως η ανταλλαγή κρυπτονομισμάτων μέσω αυτών των εφαρμογών γίνεται με σκανάρισμα κωδικών QR. Πάλι, η αποθήκευση των κλειδιών γίνεται τοπικά και άρα μόνο ο χρήστης έχει πρόσβαση σε αυτά, ωστόσο θα πρέπει να δωθεί προσοχή σε πιθανούς ιούς και malware τα οποία μπορεί να αποκτήσουν πρόσβαση στους κωδικούς. Ένα παράδειγμα τέτοιου wallet είναι το Trust wallet.

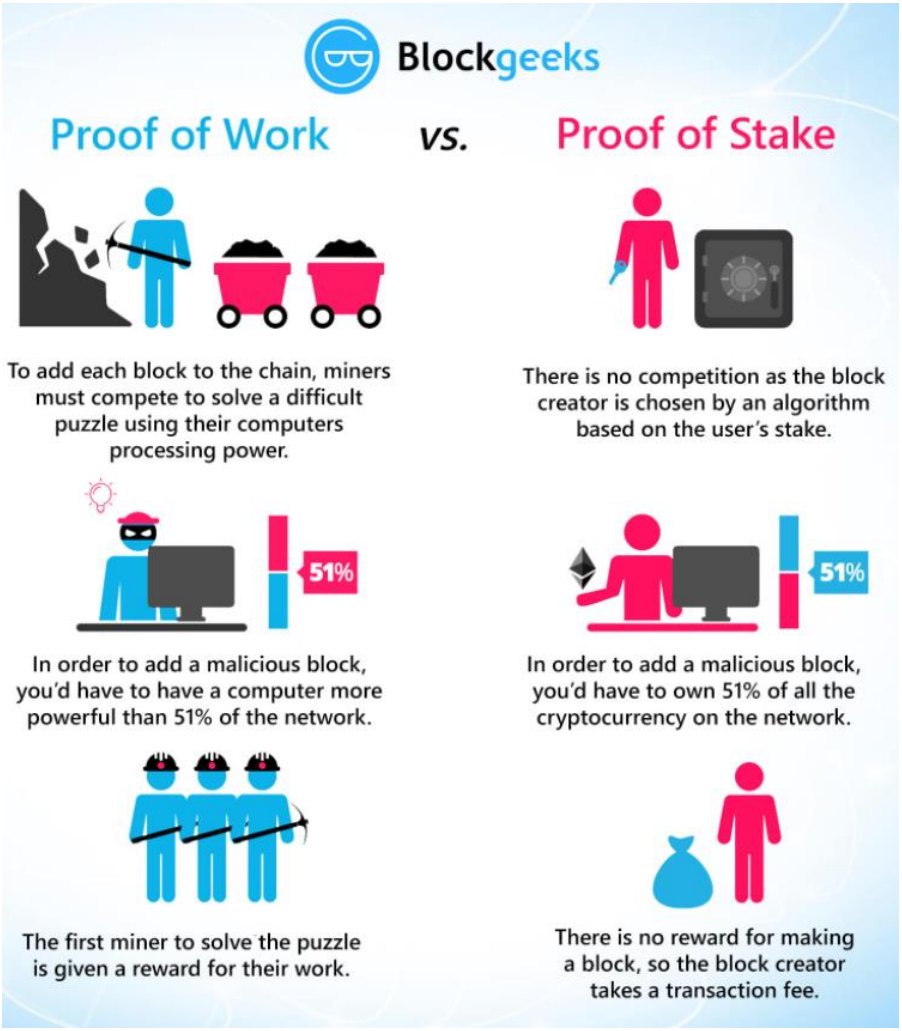
1.6.1 Hardware Wallets

Τα Hardware wallets είναι φυσικές ηλεκτρονικές συσκευές οι οποίες χρησιμοποιούν αλγορίθμους τυχαίων αριθμών (random number generators ή RNGs) για να παράξουν το δημόσιο και το ιδιωτικό κλειδί. Τα κλειδιά αυτά αποθηκεύοντα στην ίδια την συσκευή η οποία δεν συνδέεται στο διαδίκτυο (οπότε γίνεται λόγος για cold wallets σε αντίθεση με τα hot). Συνεπώς, προσφέρουν μεγαλύτερη ασφάλεια από τα software wallets, ωστόσο λόγω της φύσης του λογισμικού που χρησιμοποιούν, καθιστούν την χρήση κρυπτονομισμάτων πιο δύσκολη από τα hot wallets. Τα hardware wallets χρησιμοποιούνται κυρίως για περιπτώσεις όπου ο χρήστης έχει σκοπό να κρατήσει για μεγάλα χρονικά διαστήματα τα κρυπτονομίσματα του και άρα δεν θα κάνει πολλές συναλλαγές με αυτά. Οι περισσότερες τέτοιες συσκευές έχουν την δυνατότητα ορισμού κωδικού PIN αλλά και φράσης-κλειδιού σε περίπτωση recovery, για την μεγαλύτερη ασφάλεια των κεφαλαίων του χρήστη.

Επιπροσθέτως, τα paper wallets αναφέρονται ως ακόμα μια κατηγορία hardware wallet, και πρόκειται για χαρτί το οποίο έχει πάνω του τυπωμένο τον κωδικό QR για την χρήση των κρυπτονομισμάτων. Ωστόσο, με αυτά τα wallets δεν είναι δυνατή η μερική χρήση των κεφαλαίων, δηλαδή ο χρήστης σε κάθε συναλλαγή θα πρέπει να χρησιμοποιεί όλο τον αριθμό κρυπτονομισμάτων που ορίζει το χαρτί. Γι’αυτό τον λόγο, δεν προτείνεται η χρήση τέτοιων wallet.

1.6 Αλγόριθμοι Συναίνεσης (Consensus Algorithms)

Όπως έχει προαναφερθεί, για να ολοκληρωθεί μια συναλλαγή είναι απαραίτητο να την επικυρώσουν οι κόμβοι του δικτύου (Chawla, 2020). Αυτό γίνεται με κάποιους αλγορίθμους συναίνεσης (consensus algorithms), οι οποίοι συνήθως είναι οι Proof-of-Work (PoW) και Proof-of-Stake (PoS), χωρίς βέβαια αυτοί να είναι και οι μοναδικοί.



Εικόνα 8: PoW και PoS

Πηγή: www.blockgeeks.com

1.6.1 Proof-of-Work

Το PoW είναι ίσως η πιο ευρέως διαδεδομένη μέθοδος συναίνεσης σε δίκτυα blockchain και χρησιμοποιήθηκε για πρώτη φορά στο δίκτυο του Bitcoin. Σύμφωνα με αυτό, οι κόμβοι του δικτύου καλούνται να λύσουν ένα ολοένα και δυσκολότερο μαθηματικό πρόβλημα για να αποδείξουν ότι ανήκουν στο δίκτυο και να αποτρέψουν οποιαδήποτε κακόβουλα στοιχεία από την αλλοίωση των συναλλαγών σε αυτό. Το δίκτυο του blockchain, λοιπόν, καλεί τους κόμβους να δοκιμάζουν και να βρίσκουν συνεχώς hashes τα οποία ξεκινούν με ολοένα και μεγαλύτερο αριθμό απο μηδενικά. Κάθε φορά που βρίσκεται ένα τέτοιο hash, το block εκείνο προστίθεται στην αλυσίδα του blockchain και οι miners που δούλεψαν για να το βρουν ανταμείβονται για την δουλειά τους. Αυτή η διαδικασία είναι ευρέως γνωστή ως mining και οι κόμβοι που την πραγματοποιούν miners. Η διαδικασία απαιτεί εξαιρετικά

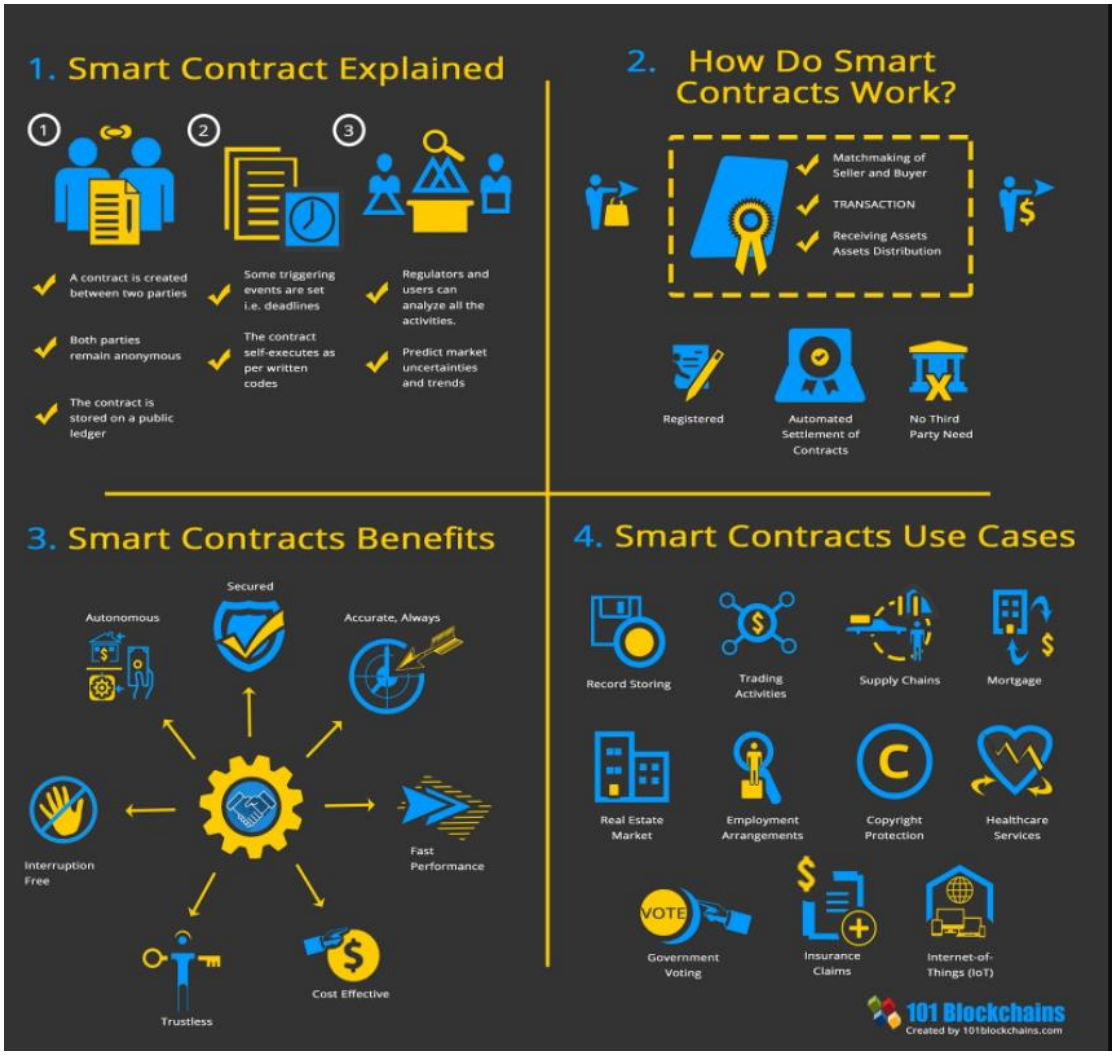
μεγάλο αριθμό προσπαθειών στον αλγόριθμο που παράγει το hash, και ως εκ τούτου απαιτεί μεγάλη υπολογιστική δύναμη, η οποία συνήθως παρέχεται από κάρτες γραφικών (GPUs). Οι miners δοκιμάζουν κάποια συγκεκριμένα data strings αλλάζοντας κάθε φορά έναν ακέραιο αριθμό nonce (number only used once).

Επειδή το δίκτυο απαιτεί ολοένα και περισσότερα μηδενικά στο παραγόμενο hash, η διαδικασία εξόρυξης γίνεται ολοένα και πιο δύσκολη. Γι'αυτό, τις περισσότερες φορές υπάρχει συνεργασία μεταξύ των κόμβων για γρηγορότερη εξόρυξη. Επιπροσθέτως, επειδή στην αλυσίδα κάθε block περιέχει το hash του προηγούμενου block, η οποιαδήποτε αλλαγή στο block θα απαιτούσε τον επαναυπολογισμό όλων των hash της αλυσίδας. Με αυτό τον τρόπο εξασφαλίεται το αδιάβλητο του blockchain. Αξίζει να σημειωθεί ότι το PoW απαιτεί τεράστια ποσά ενέργειας, μιας και οι κάρτες γραφικών δουλεύουν ασταμάτητα για πολλές ημέρες μέχρι να βρεθεί το hash. Σύμφωνα με στοιχεία από Sedlmeir, Buhl, Fridgen και Keller (2020), υπολογίζεται ότι η εξόρυξη για το Bitcoin ξεπερνά τις 125 TWh τον χρόνο, ξεπερνώντας έτσι τις ενεργειακές ανάγκες ολόκληρων χωρών όπως η Αργεντινή. Υπολογίζεται, επίσης, ότι ένα νέο hash παράγεται κάθε περίπου 10 λεπτά στο δίκτυο του Bitcoin. Για να αντιμετωπιστούν τα προβλήματα του PoW αναπτύχθηκε μια άλλη μέθοδος συναίνεσης, το Proof-of-Stake (Academy Binance, 2020).

1.6.2 Proof-of-Stake

Με την διαδικασία του PoS οι συναλλαγές στο δίκτυο επικυρώνονται μέσω ενός κόμβου ο οποίος επιλέγεται εν μέρει βάσει τυχαιότητας και εν μέρει βάσει του πόσα κρυπτονομίσματα (ή στην γενική περίπτωση «κεφάλαια») έχει και για πόσο καιρό τα έχει. Έτσι, δεν απαιτείται η εξόρυξη block και συνεπώς μειώνεται αρκετά η ενέργεια που απαιτείται για την λειτουργία του δικτύου και την ολοκλήρωση των συναλλαγών. Με αυτή τη μέθοδο συναίνεσης, η δύναμη εξόρυξης (mining power) που κατέχει ένας κόμβος είναι ανάλογη του ποσοστού των κρυπτονομισμάτων που κατέχει στο δίκτυο αυτό. Συνεπώς υπάρχει κίνητρο για τους κόμβους να αγοράσουν περισσότερα κρυπτονομίσματα ώστε να μπορούν να επικυρώσουν περισσότερες συναλλαγές και να ανταμειφθούν. Επίσης, ένας κόμβος που κατέχει x% των κρυπτονομισμάτων στο δίκτυο έχει την δυνατότητα να επικυρώσει-«εξορύξει «το ίδιο x% των συναλλαγών-block στο δίκτυο. Κάποια κρυπτονομίσματα που χρησιμοποιούν PoS είναι το Peercoin και το Nxt, ενώ το Ethereum είναι στη διαδικασία μετάβασης από PoW σε PoS. Ωστόσο, υπάρχουν κάποια αρνητικά με την μέθοδο του PoS, το σημαντικότερο των οποίων είναι η τάση κόμβων να μαζεύουν κρυπτονομίσματα και να μην τα χρησιμοποιούν (crypto hoarding).

1.7 Smart Contracts



Εικόνα 9: Smart Contracts

Πηγή: www.101blockchains.com

Τα έξυπνα συμβόλαια (smart contracts) είναι προγράμματα τα οποία λαμβάνουν χώρα-ενεργοποιούνται μέσα σε αλυσίδες blockchain όταν πληρούνται συγκεκριμένες προϋποθέσεις. Η πιο διαδεδομένη χρήση τους είναι η αυτοματοποίηση συμφωνιών-συμβολαίων χωρίς χάσιμο χρόνου, ώστε να προκύπτει με σιγουριά το αποτέλεσμα που έχει συμφωνηθεί. Μια επίσης διαδεδομένη χρήση τους είναι η αυτοματοποίση εφοδιαστικών αλυσίδων, ενεργοποιώντας την επόμενη πράξη-γεγονός σε αυτές όταν πληρούνται συγκεκριμένες προϋποθέσεις (Levi et al. 2018).

Τα smart contracts μοντελοποιούνται ως εντολές «αν ισχύει x τότε πραγματοποίησε y» πάνω σε blockchain. Το δίκτυο των υπολογιστών πραγματοποιεί τις πράξεις αυτές μόλις

λάβει εντολή από το smart contract. Για παράδειγμα, η πράξη αυτή θα μπορούσε να είναι η πληρωμή ενός μεταφορέα όταν συμπληρώσει τα δρομολόγια του. Η ενημέρωση του blockchain συμβαίνει αυτόματα από το smart contract και έτσι η αλλοίωση των στοιχείων και των αποτελεσμάτων του είναι αδύνατη. Είναι προφανές ότι οι προϋποθέσεις και οι ενέργειες που θα πραγματοποιούνται αυτόματα από ένα τέτοιο συμβόλαιο θα πρέπει να είναι καλά καθορισμένες και πολύ ακριβείς από τα συμβαλλόμενα μέρη ώστε να λειτουργήσει με την μέγιστη απόδοση το σύστημα (Mearian, 2019).

Εργαλεία Ανάπτυξης Smart contract

Υπάρχουν αρκετά εργαλεία που χρησιμοποιούνται για την ανάπτυξη smart contracts. Τα πιο σημαντικά από αυτά είναι:

Solidity: Αποτελεί γλώσσα προγραμματισμού για το δημόσιο δίκτυο blockchain του Ethereum. Βασίζεται σε Python, C++ και Javascript, ενώ υποστηρίζει διάφορες βιβλιοθήκες και τύπους δεδομένων που τους ορίζει ο χρήστης.

Solc: Αποτελεί τον compiler της γλώσσας Solidity, μετατρέποντας τον κώδικα της στο format που μπορεί να διαβάσει το Ethereum Virtual Machine. Έχει 2 εκδοχές, μια βασισμένη σε C++ και μια σε Javascript.

Geth: Άλλη μια γλώσσα προγραμματισμού για το Ethereum, βασισμένη στην Go. Χρησιμοποιείται με περιβάλλον server, command line και console και λειτουργεί σε λογισμικά Windows, Linux και Mac. Η πιο συνήθης χρήση της στα smart contracts είναι η μεταφορά κρυπτονομισμάτων και η ανάλυση της ιστορίας των προηγούμενων block στο δίκτυο.

Mist: Αποτελεί την επίσημη εφαρμογή wallet για το Ethereum, φτιαγμένο από τους προγραμματιστές του Ethereum. Κατά την διάρκεια του αρχικού setup, ο κωδικός που εισάγεται δεν μπορεί να ξανά αλλάξει, οπότε είναι αρκετά σημαντική η απομνημόνευση του. Αποτελεί ένα full node wallet, δηλαδή για να χρησιμοποιηθεί, πρέπει ο χρήστης να κατεβάσει ολόκληρο το δίκτυο του Ethereum στον υπολογιστή του, το οποίο είναι της τάξεως μεγέθους TB.

Remix: Αποτελεί ένα ακόμα εργαλείο ανάπτυξης smart contract στο Ethereum, ωστόσο όντας γραμμένο εξ'ολοκλήρου σε Javascript, μπορεί να χρησιμοποιηθεί από σχεδόν όλους του browsers. Μάλιστα, ο χρήστης μπορεί να επισκεφθεί την ιστοσελίδα του Remix και να αρχίσει απευθείας να κωδικοποιεί smart contracts.

Metamask: Αποτελεί ένα online wallet που λειτουργεί ως browser extension, και άρα συνδέει το δίκτυο του Ethereum με τον περιηγητή του χρήστη. Προσφέρει ειδική πλατφόρμα για την ανταλλαγή κρυπτονομισμάτων (αλλά και διασύνδεση με τις πλατφόρμες Coinbase και Shapeshift) καθώς και για την αλληλεπίδραση με decentralized applications (Dapps).

Truffle: Το Truffle αποτελεί ένα λογισμικό ανάπτυξης εφαρμογών Ethereum. Έχει ενσωματωμένη βιβλιοθήκη για ανάπτυξη smart contract, ενώ μπορεί να παραμετροποιηθεί αρκετά από τον χρήστη για την ευκολότερη ανάπτυξη τους. Το Truffle Suite παρέχει ένα ακόμα εργαλείο για την δοκιμή και ανάλυση των Dapps, χάρη στο οποίο ο χρήστης μπορεί να δοκιμάζει τις λύσεις του σε δικό του δίκτυο αντί για το δημόσιο δίκτυο του Ethereum, και άρα να αποφεύγει τα κόστη gas που αυτό συνεπάγεται. Αξίζει να σημειωθεί ότι και το ίδιο το Ethereum, καθώς και όλα τα υπόλοιπα δίκτυα blockchain, έχουν το δικό τους δοκιμαστικό δίκτυο ονόματι Testnet, τα οποία επιτρέπουν την δικιμή των Dapps χωρίς την σπατάλη πόρων από το κύριο δίκτυο.

Πλεονεκτήματα των Smart Contracts

Τα smart contracts μπορούν να προσφέρουν αρκετά πλεονεκτήματα με την χρήση τους λόγω των πολλών δυνατοτήτων τους. Τα κυριότερα είναι (Grybniak, 2017; Smith, 2019; Gluca, 2020; Banu, 2018):

Ταχύτητα, απόδοση και ακρίβεια: Όταν πληρούνται οι κατάλληλες προϋποθέσεις, το smart contract ενεργοποιείται κατευθείαν. Επίσης, όντας ψηφιακά, δεν εμπλέκεται γραφειοκρατία ούτε σπαταλείται χρόνος για τυχόν λάθη που μπορούν να προκύψουν από την χειροκίνητη ταξινόμηση τους.

Εμπιστοσύνη και διαφάνεια: Στα smart contracts δεν εμπλέκονται μεσάζοντες, ενώ παράλληλα τα στοιχεία που διατίθενται σε αυτά είναι φανερά ανά πάσα στιγμή στο δίκτυο του blockchain. Έτσι δεν υπάρχει αμφιβολία για το αν τα στοιχεία του συμβολαίου έχουν αλλάξει από οποιονδήποτε.

Ασφάλεια: Τα δεδομένα των smart contracts είναι κρυπτογραφημένα στο blockchain και άρα δεν μπορούν να αλλοιωθούν. Επίσης, επειδή το κάθε record συνδέεται άμεσα με το προηγούμενο του, η αλλαγή οποιουδήποτε στοιχείου, οσοδήποτε μικρό, απαιτεί τον επαναυπολογισμό όλων των υπολοίπων στοιχείων στην αλυσίδα του blockchain.

Χαμηλότερα κόστη συναλλαγών: Λόγω της απουσίας διαμεσολαβητών (πχ τραπεζών) για την ολοκλήρωση των συναλλαγών, οι καθυστερήσεις και τα κόστη των συναλλαγών μειώνονται σημαντικά.

Αντίγραφα Ασφαλείας: Χάρη στην τεχνολογία του blockchain, οι λεπτομέρειες των smart contracts καταγράφονται σε πολλά σημεία στο δίκτυο και άρα δεν υπάρχει κίνδυνος απώλειας τους.

1.9 Πλεονεκτήματα που προσφέρει το Blockchain

Είναι φανερό ότι το blockchain δύναται να προσφέρει πολλά πλεονεκτήματα στους χρήστες του, χάρη στις εξελιγμένες τεχνολογίες του. Τα κυριότερα από αυτά είναι (Geroni, 2021; Hooper, 2018; Koksal, 2019):

Ανάπτυξη εμπιστοσύνης

Το blockchain χρησιμοποιεί ένα κοινό και αδιάβλητο ledger στο οποίο μπορούν να προστεθούν στοιχεία μόνο με την συγκατάθεση όλων των κόμβων. Πολλές φορές το δίκτυο του blockchain θεωρείται trustless, επειδή για την ομαλή λειτουργία του δεν απαιτείται να υπάρχει εμπιστοσύνη μεταξύ των κόμβων του. Ωστόσο αυτό δεν σημαίνει ότι οι κόμβοι του συστήματος δεν εμπιστεύονται τους υπόλοιπους. Η εμπιστοσύνη αυτή χτίζεται χάρη στην αυξημένη ασφάλεια, διαφάνεια και ιχνηλασιμότητα που προσφέρει το δίκτυο αυτό.

Αυξημένη ασφάλεια

Τα hash functions και η λειτουργία των public-private keys οδηγεί σε records τα οποία είναι αδύνατο να αλλοιωθούν. Χάρη σε αυτά, οι λεπτομέρειες των συναλλαγών μεταξύ συμβαλλόμενων μερών μπορούν να είναι κρυπτογραφημένες από άκρο σε άκρο (end-to-end encrypted) και άρα ασφαλείς και κρυφές. Επίσης, το δίκτυο είναι P2P οπότε δεν υπάρχει κεντρική αρχή η οποία να ρυθμίζει την λειτουργία του και άρα σε αυτή να βασίζεται η ασφάλεια όλων των κόμβων. Αυτό σημαίνει ότι εάν κάποιο κακόβουλο στοιχείο θέλει να επιτεθεί στο δίκτυο, θα πρέπει να επιτεθεί σε όλους τους κόμβους του.

Ιχνηλασιμότητα

Με τη βοήθεια του blockchain, οι εταιρείες μπορούν να φτιάξουν μια εφοδιαστική αλυσίδα χρήσιμη όχι μόνο για τους πωλητές αλλά και για τους προμηθευτές. Στα παραδοσιακά μοντέλα εφοδιαστικών αλυσίδων η ιχνηλασιμότητα προϊόντων είναι αρκετά δύσκολο πρόβλημα αφού στις μέρες μας ένα μεγάλο ποσοστό των εταιρειών δραστηριοποιούνται σε αρκετές χώρες. Με το blockchain, η εφοδιαστική αλυσίδα γίνεται διαφανής. Οποιοδήποτε μέρος αυτής μπορεί μέσω του δικτύου να εντοπίσει την προέλευση και τον προορισμό οποιουδήποτε προϊόντος. Αυτό το χαρακτηριστικό είναι ιδιαίτερα χρήσιμο για εταιρείες οι οποίες είναι σημαντικό να αποδείξουν στους πελάτες τους ότι το προϊόν που πωλούν είναι γνήσιο ή έχει την επιθυμητήπροέλευση, για παράδειγμα σε εταιρείες με περιβαλλοντικό στόχο ή σε εταιρείες όπου το προϊόν τους υπόκειται συχνά σε παραποίηση (πχ βιομηχανίες ρούχων).

Αυξημένη απόδοση και ταχύτητα

ΟΙ παραδοσιακές διαδικασίες που περιλαμβάνουν γραφειοκρατία είναι αρκετά αργές, επιρρεπείς σε ανθρώπινα λάθη και απαιτούν αρκετούς μεσάζοντες (third parties) για την ολοκλήρωση τους. Το blockchain βοηθά στην απαλλαγή από third parties και βοηθά στην πιο γρήγορη και αποτελεσματική ολοκλήρωση συμφωνιών και συναλλαγών. Τα

απαιτούμενα έγγραφα αποθηκεύονται στο δίκτυο του blockchain, και οι λεπτομέρειες των συναλλαγών αυτών καταγράφονται στο distributed ledger. Έτσι είναι αδύνατη η απώλεια των πληροφοριών αυτών.

Αυτοματοποίηση

Η πραγματοποίηση συμβολαίων και συναλλαγών μπορεί να αυτοματοποιηθεί με την βοήθεια των smart contracts. Την στιγμή που πληρούνται οι απαιτούμενες προϋποθέσεις, η συναλλαγή ολοκληρώνεται αυτόματα και το επόμενο μέρος της συμφωνίας ξεκινά αυτόματα. Τα smart contracts μειώνουν τον ανθρώπινο παράγοντα και την εξάρτηση από third parties.

1.10 Προβλήματα με την λειτουργία του Blockchain

Παρά τα πολλά πλεονεκτήματα που προσφέρει το blockchain, υπάρχουν ακόμα κάποια θέματα που πρέπει να λυθούν ώστε να μπορέσουν αρκετές εταιρείες να υϊοθετήσουν την τεχνολογία αυτή πλήρως (Conway, 2020; Iredale, 2020).

Έλλειψη Τυποποίησης

Το βασικό πρόβλημα του blockchain είναι η έλλεψη της τυποποίησης και της διαλειτουργικότητας μεταξύ των δικτύων αυτών. Εκτιμάται ότι στις αρχές του 2020 τα projects που χρησιμοποιούσαν τεχνολογία blockchain ήταν γύρω στα 6500. Ωστόσο στα περισσότερα από αυτά, ο κώδικας, τα πρωτόκολλα, οι μηχανισμοί συναίνεσης και τα μέτρα για την εξασφάλιση της ιδιωτικότητας ήταν φτιαγμένα να λειτουργούν μόνο για την ιδία πλατφόρμα. Αυτό σημαίνει ότι η επικοινωνία μεταξύ των δικτύων αυτών είναι αρκετά δύσκολη και τα αποτρέπει από την απρόσκοπτη συνεργασία μεταξύ τους. Η υϊοθέτηση τυποποιήσεων στο κομμάτι του blockchain θα βοηθήσει τις εταιρείες να συνεργαστούν μεταξύ τους, να ανατπύξουν πιο γρήγορες διαδικασίες ολοκλήρωσης συναλλαγών και συμφωνιών, ενώ παράλληλα θα βοηθήσει στην ευκολότερη συνεργασία των συστημάτων blockchain με τα υπάρχοντα υπολογιστικά συστήματα του παρόντος.

Έλλειψη Επεκτασιμότητας

Η έλλειψη επεκτασιμότητας είναι ένα από τα κυριότερα προβήματα στα δίκτυα blockchain. Τα παραδοσιακά συστήματα στα οποία γίνονται συναλλαγές (πχ Visa) έχουν την δυνατότητα να επεξεργάζονται περίπου 2000 συναλλαγές ανά λεπτό. Ωστόσο, στο δίκτυο του Bitcoin το νούμερο αυτό είναι 7 ενώ στο δίκτυο του Ethereum είναι περίπου 20. Το πρόβλημα αυτό εμφανίζεται κυρίως στα δημόσια blockchain, αφού στα ιδιωτικά blockchain οι συναλλαγές είναι πιο γρήγορες.

Υψηλή Κατανάλωση Ενέργειας

Το πρόβλημα της κατανάλωσης ενέργειας εμφανίζεται στα blockchain όπου ο μηχανισμός συναίνεσης είναι το Proof-of-Work. Σε αυτά, όλο το δίκτυο εργάζεται για να βρει το hash το οποίο πληροί τις προϋποθέσεις που θέτει το δίκτυο. Ο κάθε κόμβος δοκιμάζει εξαιρετικά μεγάλο αριθμό λύσεων ανά δευτερόλεπτο, γεγονός το οποίο οδηγεί σε δαπάνη τεράστιων ποσών ενέργειας. Η κατανάλωση ενέργειας μάλιστα για PoW έχει ξεπεράσει την κατανάλωση ενέργειας κάποιων χωρών στον κόσμο. Πέρα από το PoW, υπάρχουν και άλλοι αλγόριθμοι συναίνεσης όπως το PoS, ωστόσο και αυτοί έχουν ορισμένα προβλήματα που τους αποτρέπουν από την καθολική υϊοθέτηση. Θα πρέπει άρα να δωθεί αρκετή σημασία ώστε να βρεθούν άλλοι μηχανισμοί συναίνεσης που να πληρούν τις προϋποθέσεις του blockchain, ενώ παράλληλα να μην παρουσιάζουν τα προβλήματα που έχουν τα τωρινά μοντέλα.

2. Δημόσια δίκτυα Blockchain

Το δημόσιο blockchain είναι το δίκτυο στο οποίο μπορεί να συμμετάσχει οποιοσδήποτε επιθυμεί δίχως περιορισμούς, ενώ επιπλέον ο κάθε συμμετέχων κόμβος έχει πρόσβαση στο δημόσιο ledger και συμμετέχει στην διαδικασία συναίνεσης στο δίκτυο. Το δημόσιο δίκτυο αποτελεί τον πρώτο τύπο δικτύων blockchain που αναπτύχθηκαν, με το Bitcoin. Τα βασικά πλεονεκτήματα των δικτύων αυτών είναι η ισότητα των κόμβων που συμμετέχουν, η ευκολία συμμετοχής στο δίκτυο, η αυξημένη ασφάλεια χάρη στους ισχυρούς αλγορίθμους συναίνεσης, η διαφάνεια μιας και όλοι οι συμμετέχοντες μπορούν να βλέπουν το δημόσιο ledger καθώς και η ανωνυμία που επικρατεί στο δίκτυο (Geroni, 2020).

Ωστόσο, τα δημόσια δίκτυα έχουν και ορισμένα μειονεκτήματα τα οποία καθιστούν την χρήση τους σε ορισμένες εφαρμογές εφοδιαστικής αλυσίδας δύσκολη. Το πιο βασικό είναι η σχετικά μικρή ταχύτητα επικύρωσης των συναλλαγών, μιας και για να ολοκληρωθεί αυτή η διαδικασία θα πρέπει να συμφωνήσουν οι κόμβοι του δικτύου, οι οποίοι στα δημόσια δίκτυα είναι μεγάλος αριθμός. Συνεπώς, η ταχύτητα ολοκλήρωσης των συναλλαγών είναι μικρότερη από ότι στα ιδιωτικά δίκτυα.

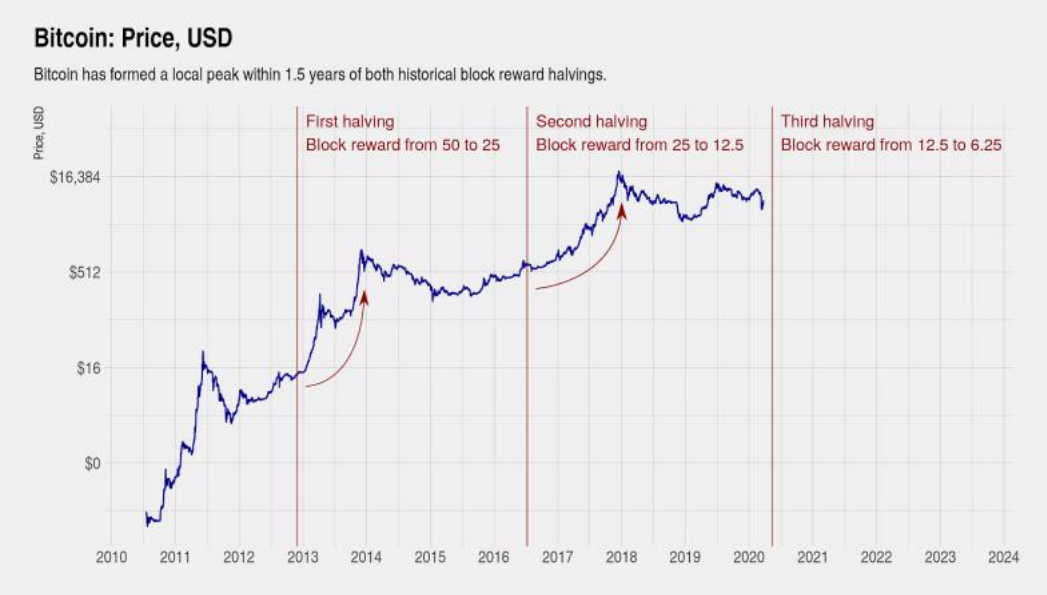
Τα πιο βασικά δημόσια blockchains είναι το Bitcoin και το Ethereum. Όπως προαναφέρθηκε, το Bitcoin αποτελεί το πρώτο δίκτυο blockchain που αναπτύχθηκε, και ακόμα και σήμερα αποτελεί ένα από τα πιο ευρέως χρησιμοποιούμενα δίκτυα παγκοσμίως. Το δίκτυο του Ethereum αναπτύχθηκε ως μια πιο πρακτική λύση για αυτοματοποιημένες επιχειρηματικές συναλλαγές, χάρη στην ευκολία ανάπτυξης smart contracts σε αυτό.

2.1 Bitcoin

Αποτελεί την πρώτη διαδεδομένη πλατφόρμα κρυπτονομισμάτων παγκοσμίως. Είναι open-source και ο κύριος σκοπός του είναι η ανταλλαγή κρυπτονομισμάτων. Αποτελεί έναν αρκετά διαδεδομένο τρόπο πληρωμών τον οποίο πια δέχονται αρκετές εταιρείες ανά τον κόσμο χάρη στις χαμηλές προμήθειες επεξεργασίας των μεταφορών. Στο δίκτυο του συμμετέχουν, σύμφωνα με τον προγραμματιστή του Luke Dash, περίπου 12,000 κόμβοι. Από την αρχή του έως το σήμερα, το κρυπτονόμισμα του Bitcoin έχει αρκετές αναταραχές όσον αφορά στην αξία του, η οποία συνδέεται άμεσα με τον αριθμό των κόμβων στο δίκτυο, την ολοένα και μεγαλύτερη δυσκολία λύσης των hash functions του αλλά και τις μεγάλες εταιρείες και οργανισμούς που το υϊοθετούν (ή όχι) σαν μέσο πληρωμής. Χρησιμοποιεί το Proof-of-Work σαν αλγόριθμο συναίνεσης, ενώ ένα από τα βασικά στοιχεία του είναι το halving.

Το halving είναι μια διαδικασία μείωσης κατά το ήμισυ της αξίας επίλυσης του mining. Ουσιαστικά, τα κρυπτονομίσματα Bitcoin που κερδίζουν οι κόμβοι μόλις λύσουν το επόμενο

στάδιο του hash function μειώνονται στο μισό. Αυτή η διαδικασία βοηθά στην μείωση του ρυθμού πληθωρισμού του κρυπτονομίσματος αυτού αλλά και στην μείωση του ρυθμού με τον οποίο εισέρχονται νέα Bitcoin στο δίκτυο. Αξίζει να σημειωθεί ότι η διαδικασία του halving συμβαίνει κάθε 210,000 blocks ή περίπου κάθε 4 χρόνια, με την τελευταία να έχει συμβεί στις 11 Μαϊου 2020. Αφού η αξία του νομίσματος αυξάνει όσο μειώνεται η διαθεσιμότητα του, αυτό σημαίνει ότι το halving αυξάνει την αξία του κρυπτονομίσματος αυτού. Ενδιαφέρον παρουσιάζει και το γεγονός ότι σύμφωνα με τον Krause (2018), το 20% των συνολικών Bitcoin που έχουν παραχθεί έχει χαθεί είτε σε αποθηκευτικά μέσα είτε επειδή ο ιδιοκτήτης τους έχασε το ιδιωτικό κλειδί του. Ακόμη, σύμφωνα με το Κογκρέσο των ΗΠΑ υπάρχει απαγόρευση χρήσης των Bitcoin σε συνολικά 24 χώρες παγκοσμίως, λόγω χρήσης του σε παράνομες συναλλαγές χάρη στην ανώνυμη φύση του.

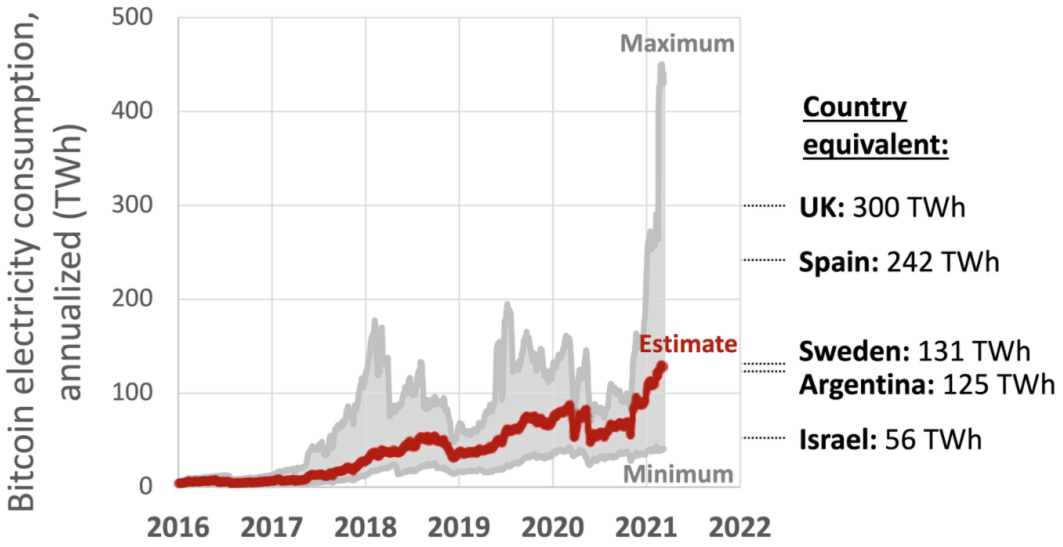


Εικόνα 10: Η αξία του Bitcoin συναρτήσει των halvings

Πηγή: www.investopedia.com

Αξίζει να αναφερθεί ότι το Bitcoin έχει υϊοθετηθεί από πολλές μεγάλες εταιρείες σαν μέσο πληρωμής όπως τις Tesla, Microsoft, Paypal, Newegg και Microstrategy, γεγονός που ολοένα και αυξάνει την αξία του κρυπτονομίσματος. Σύμφωνα με τον αλγόριθμο του mining που έχουν θέσει οι προγραμματιστές του Bitcoin, ο μέγιστος αριθμός του κρυπτονομίσματος αυτού είναι 21 εκατομμύρια Bitcoin. Επιπροσθέτως, αποτελεί το μεγαλύτερο μερίδιο της αγοράς των κρυπτονομισμάτων στα 625 δισεκατομμύρια δολλάρια, ενώ το Ethereum που έρχεται στη δεύτερη θέση είναι μόλις στα 247 δισεκατομμύριοα δολλάρια (Coinmarketcap.com). Αυτό συμβαίνει κυρίως επειδή αποτελεί το πρώτο κρυπτονόμισμα που έλυσε το πρόβλημα του double-spending αλλά και διότι αποτελεί διαχρονικά ένα ανοιχτό και αποκεντρωμένο νόμισμα. Ένα ακόμη ενδιαφέρον

χαρακτηριστικό του Bitcoin είναι η ασφάλεια του σε σχέση με τα υπόλοιπα δίκτυα blockchain και ειδικά το ότι δεν έχει υπάρξει ποτέ επιτυχημένη επίθεση στο δίκτυο αυτό σε αντίθεση για παράδειγμα με το Ethereum και το DAO attack το 2016. Κάθε 2016 blocks (ή περίπου κάθε 14 ημέρες) η δυσκολία του μαθηματικού μοντέλου που λύνουν οι miners προσαρμόζεται ανάλογα με την απόδοση και τον φόρτο εργασίας που ξοδεύουν οι miners. Αυτό γίνεται για να εξασφαλιστεί ότι ο μέσος χρόνος μεταξύ κάθε block θα είναι γύρω στα 10 λεπτά, ώστε οι συναλλαγές στο δίκτυο να μην αργούν πάνω από αυτό το όριο. Σύμφωνα με μελέτη του Cambridge, το Bitcoin καταναλώνει για mining περισσότερη ενέργεια από ολόκληρες χώρες:



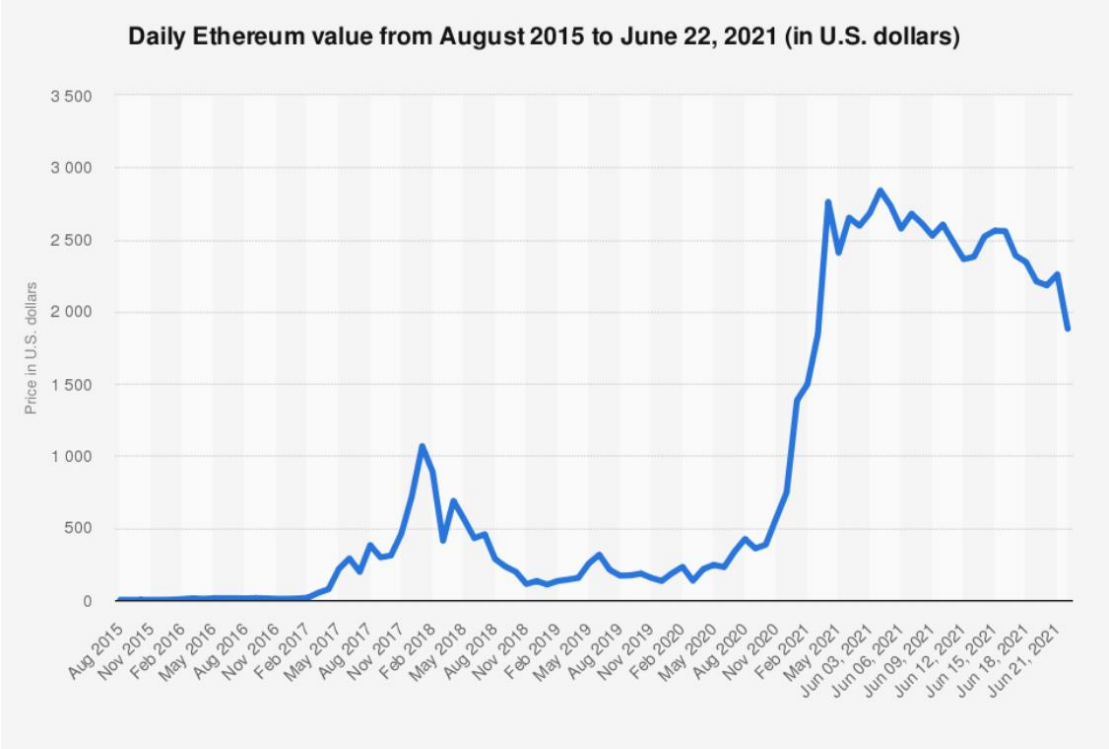
Εικόνα 11: Κατανάλωση ενέργειας από το δίκτυο του Bitcoin

Πηγή: www.cbeci.org

Το Bitcoin έχει γραφτεί κυρίως σε C++, αλλά υπάρχουν clients οι οποίοι τρέχουν σε Java και Python. Το βασικό του μειονέκτημα σε σχέση με το Ethereum, όσον αφορά στα smart contracts και τις εφαρμογές στην εφοδιαστική αλυσίδα, είναι η λιγότερη εξειδίκευση του στους τομείς αυτούς: Ενώ και οι 2 πλατφόρμες αυτές διαθέτουν δικό τους κρυπτονόμισμα και εργαλεία ανάπτυξης smart contracts, το Ethereum αναπτύχθηκε ειδικά για τα smart contracts και διαθέτει την εξειδικευμένη γλώσσα Solidity για την ανάπτυξη τους, γεγονός το οποίο το κάνει αρκετά πιο αποδοτικό στον τομέα αυτό.

2.2 Ethereum

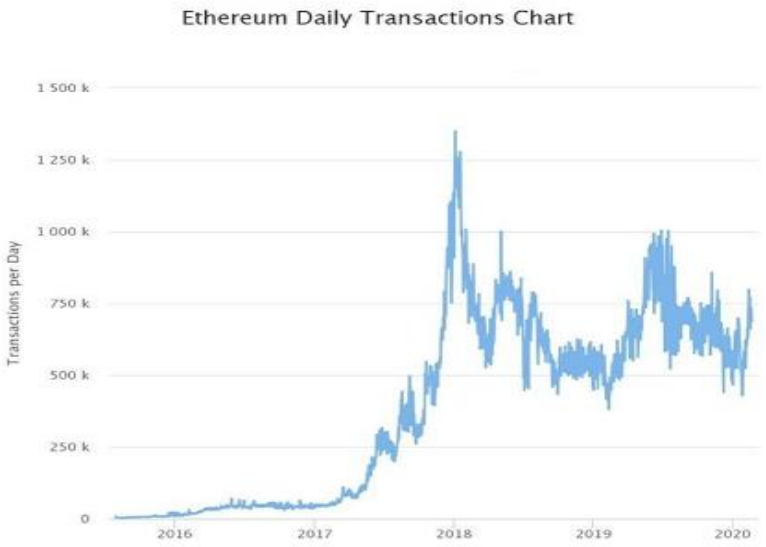
Το δίκτυο του Ethereum αποτελεί ίσως το πιο γνωστό δημόσιο δίκτυο blockchain. Αναπτύχθηκε το 2015, είναι open-source και έχει αναπτυχθεί ειδικά για την εύκολη ανάπτυξη και εφαρμογή smart contracts. Έχει δικό του κρυπτονόμισμα ονόματι Ether, το οποίο διευκολύνει τις συναλλαγές των smart contracts μιας και είναι ενσωματωμένο στο δίκτυο, το οποίο μάλιστα το δέχονται ως μέθοδο πληρωμής αρκετές εταιρείες, όπως συμβαίνει και με το Bitcoin. Η βασική διαφορά των 2 κρυπτονομισμάτων αυτών είναι ότι το Bitcoin αναπτύχθηκε για να χρησιμοποιείται ως τρόπος πληρωμής, ενώ το Ether αναπτύχθηκε για την διευκόλυνση των διαδικασιών μέσα στο δίκτυο του Ethereum. Το Ethereum είναι γραμμένο σε Python, Go και C++ και σαν αλγόριθμο συναίνεσης χρησιμοποιεί το Proof-of-Work. Ωστόσο, τα τελευταία χρόνια το mining που απαιτείται για το PoW έχει προκαλέσει αρκετές συζητήσεις για τις ενεργειακές και περιβαλλοντικές επιπτώσεις του όπως έχει φανεί και από το Bitcoin, και οι προγραμματιστές του Ethereum έχουν αποφασίσει ότι ο αλγόριθμος συναίνεσης θα έχει γίνει Proof-of-Stake το πρώτο μισό του 2022. Αυτή η αλλαγή θα προσφέρει και μεγαλύτερη ταχύτητα συναλλαγών, αλλά και θα αυξήσει τις συναλλαγές που μπορεί να επεξεργαστεί το δίκτυο ανά μονάδα χρόνου. Το βασικό πλεονέκτημα του Ethereum είναι η ενσωματωμένη γλώσσα προγραμματισμού του ονόματι Solidity, η οποία έχει αναπτυχθεί για εφαρμογές smart contracts.



Εικόνα 12: Η αξία του Ether

Πηγή: www.statista.com

Το gas αναφέρεται στο κόστος το οποίο υπάρχει κατά την ολοκλήρωση μιας συναλλαγής ή ενός smart contract στο blockchain του Ethereum. Το gas χρησιμοποιείται για την κατανομή των πόρων του Ethereum Virtual Machine έτσι ώστε οι αποκεντρωμένες εφαρμογές όπως τα smart contracts να μπορούν να αυτό-εκτελεστούν με ασφαλή τρόπο. Συνήθως, το gas έχει τιμή μικρών ποσοτήτων ether, τα οποία ονομάζονται gwei ή nanoeth. Η ακριβής τιμή του gas καθορίζεται από την προσφορά και ζήτηση μεταξύ των miner του δικτύου, οι οποίοι έχουν την δυνατότητα να απορρίψουν την επεξεργασία μιας συναλλαγής αν η τιμή του gas ξεπερνά το όριο που οι ίδιοι έχουν θέσει.



Εικόνα 13: Συναλλαγές στο Ethereum

Πηγή: Joshi και Walvekar (2020)

Το gas εισήχθη στο Ethereum ώστε να προσδίδει μια αντικειμενική αξία των υπολογιστικών αναγκών για την εκτέλεση των συναλλαγών. Οι τιμές του gas ουσιαστικά αποζημιώνουν τους χρήστες του δικτύου οι οποίοι επικυρώνουν τις συναλλαγές χάρη στις υπολογιστικές τους δυνατότητες. Το gas limit αναφέρεται στο μέγιστο όριο gas που είναι διατεθειμένος ένας χρήστης να πληρώσει για να ολοκληρώσει τη συναλλαγή του. Οι miners στο Ethereum, οι οποίοι πραγματοποιούν τις σημαντικές διεργασίες για την επικύρωση και την επεξεργασία των συναλλαγών στο δίκτυο λαμβάνουν την τιμή του gas ως αντάλλαγμα για τη δουλειά τους. Αν η τιμή αυτή τους φάινεται μικρή, έχουν την δυνατότητα να απορρίψουν την συναλλαγή αυτή και, γι’αυτό τον λόγο, η τιμή του gas έχει διακύμανση στο δίκτυο.

```
template FixedSupplyTokenProposal
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        signatory issuer -- Issuer creates proposal

        controller owner can -- Proposed owner can choose to accept
            Accept : ContractId FixedSupplyToken
                do create FixedSupplyToken with owner, issuer, amount -- Which creates the token

template FixedSupplyToken
    with
        owner: Party
        issuer: Party
        amount: Decimal
    where
        Signatory issuer, owner
```

Εικόνα 14: Παράδειγμα κώδικα smart contract σε γλώσσα Solidity

Πηγή: www.daml.com

2.2.1 Περιγραφή βημάτων για την ανάπτυξη smart contract στο Ethereum

Σε αυτή την ενότητα θα αναλυθεί η διαδικασία ανάπτυξης smart contract στο δίκτυο του Ethereum μιας και αυτό είναι το βασικό δημόσιο δίκτυο blockchain για εφαρμογές smart contract.

Στο Ethereum τα smart contracts αναπτύσσονται συνήθως στην γλώσσα προγραμματισμού Solidity, ενώ σε κάποιες περιπτώσεις χρησιμοποιείται και η Java. Για την χρήση των γλωσσών αυτών απαιτείται η εγκατάσταση ενός λογισμικού προσομοίωσης smart contract. Ένα από τα πιο ευρέως διαδεδομένα τέτοια λογισμικά είναι το Truffle το οποίο προσφέρει και την δυνατότητα επαλήθευσης της ορθής λειτουργίας του smart contract (validity check). Τα βήματα της ανάπτυξης αυτής είναι τα εξής:

1) Η προετοιμασία και η εγκατάσταση του λογισμικού: Για το Truffle (https://www.trufflesuite.com/tutorial) η εγκατάσταση γίνεται σε terminal με ορισμένες εντολές.

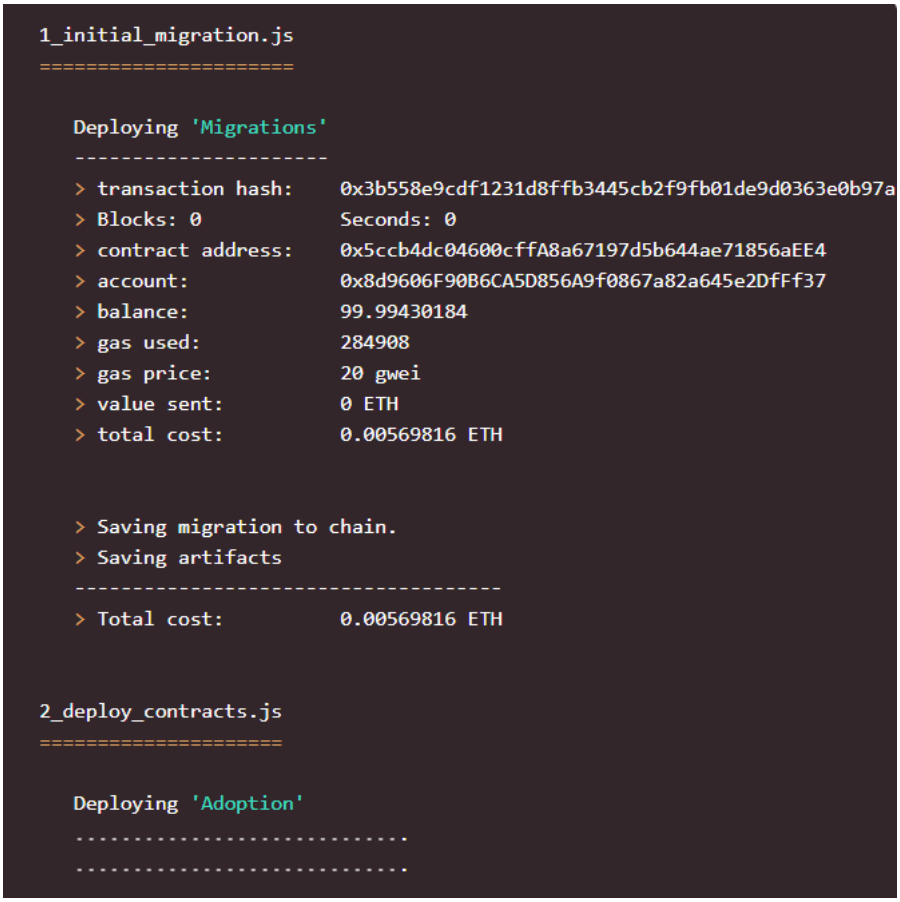
2) Ο ορισμός των μεταβλητών του smart contract: Κάθε smart contract έχει κάποιες συγκεκριμένες μεταβλητές όπως οι διευθύνσεις των εμπλεκόμενων μερών (οι οποίες στην Solidity έχουν μήκος 20 bytes), ο ορισμός των ποσών του καθώς και οι καταστάσεις στις οποίες ενεργοποιείται αλλά και απενεργοποιείται, τα directories στα οποία βρίσκονται τα δεδομένα εισόδου και ορισμένα configuration files. Αυτά ορίζονται σε αυτό το βήμα μιας και η Solidity γλώσσα είναι στατικού τύπου γλώσσα, δηλαδή οι μεταβλητές, πίνακες και

γενικά τα δεδομένα που χρησιμοποιεί θα πρέπει να οριστούν στην αρχή, πριν οποιαδήποτε προσπάθεια γραφής κώδικα.

3) Ορισμός των συναρτήσεων που θα χρησιμοποιούνται στο smart contract: Οι συναρτήσεις αυτές μπορεί να είναι οι διάφοροι υπολογισμοί οι οποίοι θα συμβαίνουν κατά την διάρκεια τρεξίματος του, καθώς και η ταξινόμηση και κατηγοριοποίηση των μεταβλητών του.

4) Μετάφραση του προγράμματος: Η Solidity απαιτεί compile για να τρέξει στο Ethereum Virtual Machine.

5) Η μεταφορά του smart contract στο δίκτυο του Blockchain: Το δίκτυο του blockchain στην προκειμένη περίπτωση μπορεί είτε να είναι δημόσιο είτε ιδιωτικό. Το Truffle suite, για παράδειγμα, προσφέρει την δυνατότητα δοκιμής του smart contract σε δίκτυο το οποίο τρέχει στον ηλεκτρονικό υπολογιστή του χρήστη (local hosting). Για την χρήση τέτοιου δικτύου απαιτείται η εγκατάσταση του λογισμικού Ganache του Truffle suite.



Εικόνα 15: Η μεταφορά του smart contract στο δίκτυο του blockchain

Πηγή: www.trufflesuite.com/tutorial

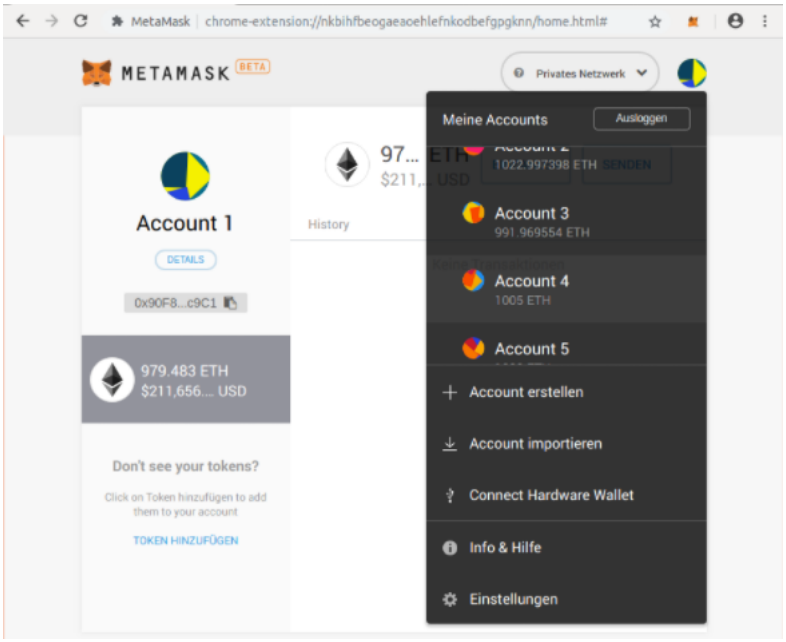
Σε περίπτωση που είναι επιθυμητή η ανάπτυξη διεπαφής με το διαδίκτυο (web interface) απαιτείται ένα ακόμη βήμα.

6) Η ανάπτυξη της διεπαφής: Εδώ συνήθως χρησιμοποιείται η γλώσσα Javascript η οποία είναι αρκετά εύκολη για διεπαφές διαδικτύου. Η διεπαφή αυτή είναι ουσιαστικά ο κρίκος που συνδέει το πρόγραμμα του smart contract και τα κρυπτονομίσματα τα οποία έχουν οι χρήστες. Για την χρήση του Truffle, η εταιρεία προτείνει το ψηφιακό web wallet Metamask, το οποίο συνδέεται κατευθείαν με το Truffle μέσω του διαδικτύου.

Εικόνα 16: Αποτελέσματα επιτυχούς ελέγχου smart contract στο Truffle

Πηγή: www.trufflesuite.com/tutorial

Συνεπώς η διαδικασία σαν πρόγραμμα ακολουθεί τον εξής δρόμο: Ο κώδικας του smart contract καλεί τα δεδομένα των χρήστών από τα wallet καθώς και λεπτομέρειες από το δίκτυο του blockchain, μέσω της διεπαφής του Javascript. Στην συνέχεια υπολογίζει μέσω των functions τις διάφορες μεταβλητές εξόδου που απαιτούνται, και ολοκληρώνει τις απαιτούμενες πληρωμές από και προς τους χρήστες, ανανεώνοντας έτσι και τα wallets των χρηστών αλλά και τις πληροφορίες στο blockchain.



Εικόνα 17: Το γραφικό περιβάλλον του Metamask

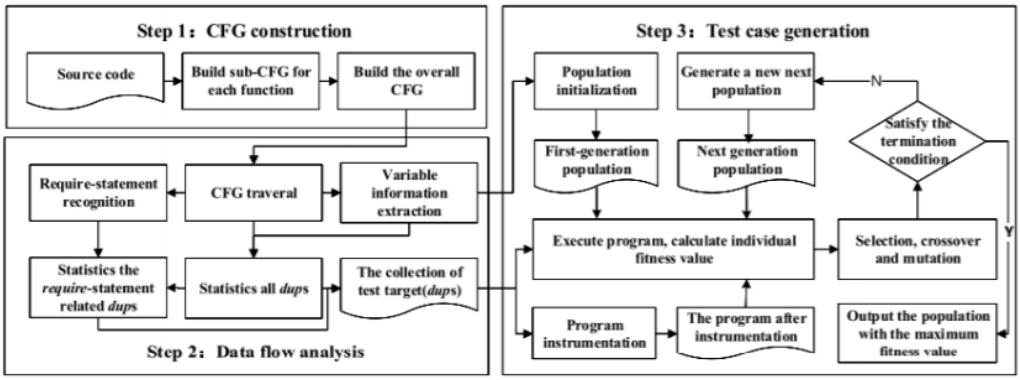
Πηγή: www.xbr.network/docs/project/metamask.html

2.2.2 Εργαλεία βελτιστοποίησης κώδικα smart contract στο Ethereum

Μιας και το Ethereum αποτελεί το βασικό δημόσιο δίκτυο blockchain για επιχειρηματικές εφαρμογές, το παρόν κομμάτι θα παρουσιάσει κάποια βασικά εργαλεία τα οποία αναλύουν και βελτιστοποιούν τον κώδικα των smart contracts στο δίκτυο αυτό.

Τα Ethereum Smart Contracts (ESCs) είναι προγράμματα βάσει gas, δηλαδή οι επιλογές των προγραμματιστών έχουν ως στόσο την ελαχιστοποίηση του gas. Για αυτό τον λόγο, τα smart contracts θα πρέπει να έχουν όσο το δυνατόν μεγαλύτερη αποδοτικότητα και όσο το δυνατόν ελάχιστα λειτουργικά κόστη. Οι Wang et al. (2019) μοντελοποίησαν το πρόβλημα αυτό ως μια βελτιστοποίηση πολλαπλών κριτηρίων, τα οποία είναι η ελαχιστοποίηση του μήκους διακλαδώσεων, η ελαχιστοποίηση του χρόνου ολοκλήρωσης και η ελαχιστοποίηση του κόστους gas. Μια άλλη προσέγγιση από τους Zhang et al. (2020) προτείνει την δημιουργία test cases (ADF-GA: All-uses Data Flow criterion based test case χρησιμοποιώντας Γενετικούς αλγόριθμους) χρησιμοποιώντας την προγραμματιστική γλώσσα Solidity. Χάρη στην χρήση γενετικών αλγορίθμων, το μοντέλο αυτό καταφέρνει να

μειώσει τον συνολικό αριθμό επαναλήψεων των test cases και άρα να μειώσει το συνολικό κόστος των smart contracts.

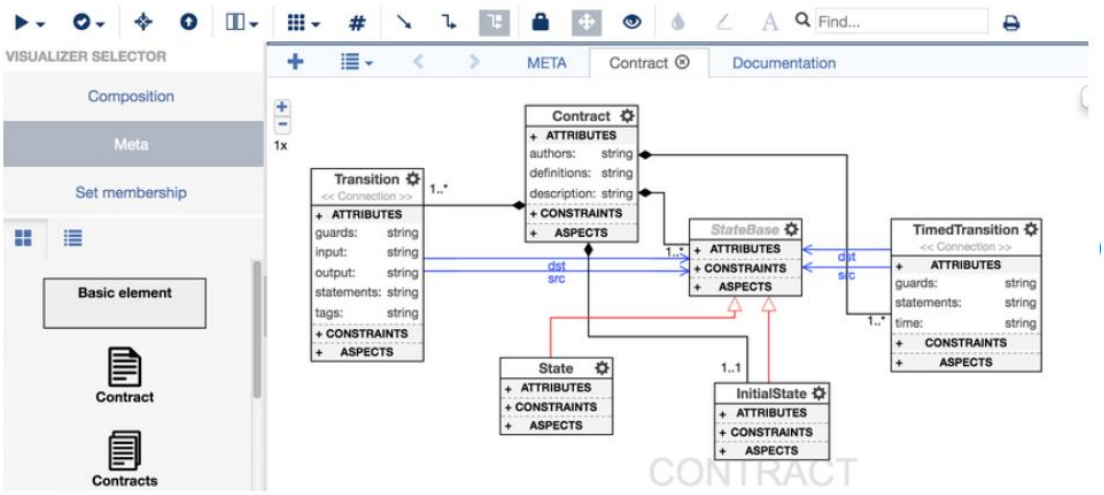


Εικόνα 18: ADF-GA αλγόριθμοι στα Ethereum smart contracts

Πηγή: Zhang et al. (2020)

Όσον αφορά στον συνολικό χρόνο ολοκλήρωσης των smart contracts (runtime), μπορούν να χρησιμοποιηθούν διάφορες τεχνικές ελέγχου. Οι Ellul και Pace (2018) ανέπτυξαν ένα εργαλείο ονόματι CONTRACTLARVA το οποίο ελέγχει και διορθώνει αυτόματα τα κενά ασφαλείας που μπορεί να υπάρχουν σε ένα smart contract. Ωστόσο, μια έρευνα από τους Chen et al. (2020) δείχνει ότι τα εργαλεία που εντοπίζουν λάθη στα συμβόλαια αυτά έχουν την ικανότητα να βρίσκουν μόνο τους 7 από τους 20 συνολικά τύπους λαθών που υπάρχουν στην βιβλιογραφία, δείχνοντας έτσι την ανάγκη ανάπτυξης περισσότερων και γενικότερων πλατφόρμων για την λύση των προβλημάτων αυτών.

Οι Μαυρίδου και Laszka (2018) ανέπτυξαν ένα λογισμικό FSolidM για την δημιουργία ασφαλών smart contracts. Το λογισμικό αυτό βασίζεται στην θεωρία των Finite State Machines (FSMs) έτσι ώστε να βοηθήσει τους προγραμματιστές blockchain να αναπτύξουν ευκολότερα και ασφαλέστερα smart contracts. Το λογισμικό αυτό περιέχει γραφικό περιβάλλον το οποίο επιτρέπει την αυτόματη παραγωγή κώδικα για smart contracts. Το λογισμικό αυτό περιέχει ακόμα μια σειρά από plugins, τα οποία βοηθούν όχι μόνο στην επικύρωση της ασφάλειας της ιδιωτικότητας των smart contracts αλλά και στην επίλυση κοινών προβλημάτων τους όπως η κακή συμπεριφορά τους σε περιπτώσεις όπου οι είσοδοι ή τα αποτελέσματα ήταν μη ορθώς ορισμένα.



Εικόνα 19: Γραφικό περιβάλλον του εργαλείου FSolidM

Πηγή: Μαυρίδου και Laszka (2018)

Το Smartcheck (Tikhomirov et al. 2018) είναι ένα εργαλείο στατικής και δυναμικής ανάλυσης για smart contract στο πλαίσιο του Ethereum. Μεταφράζει τον πηγαίο κώδικα σε ένα ενδιάμεσο αρχείο XML και έπειτα το συγκρίνει με μοντέλα από το XPath. Το εργαλείο αυτό έχει δοκιμαστεί σε περισσότερα από 4600 επιβεβαιωμένα smart contract τα οποία έχουν βρεθεί στο Etherscan. Το Smartcheck μπορεί να εντοπίζει προβλήματα ασφαλείας, λειτουργικότητας και ανάπτυξης τα οποία κάνουν τον κώδικα του smart contract δύσκολο στην κατανόηση και στο debugging. Σύμφωνα με τα στατιστικά της έρευνας των συγγραφέων, το λογισμικό αυτό εντοπίζει ότι στο 99,9% των smart contract παρουσιάζουν κάποιου είδους πρόβλημα, ενώ 63,2% έχουν σημαντικές ευπάθειες στον σχεδιασμό τους. Το λογισμικό Securify (Tsankov et al. 2018) έχει δείξει ότι μπορεί να δουλεύει παράλληλα με το Smartcheck και να διορθώνει διάφορα από τα προβλήματα που προκύπτουν.

Εικόνα 20: Το γραφικό περιβάλλον του εργαλείου Smartcheck

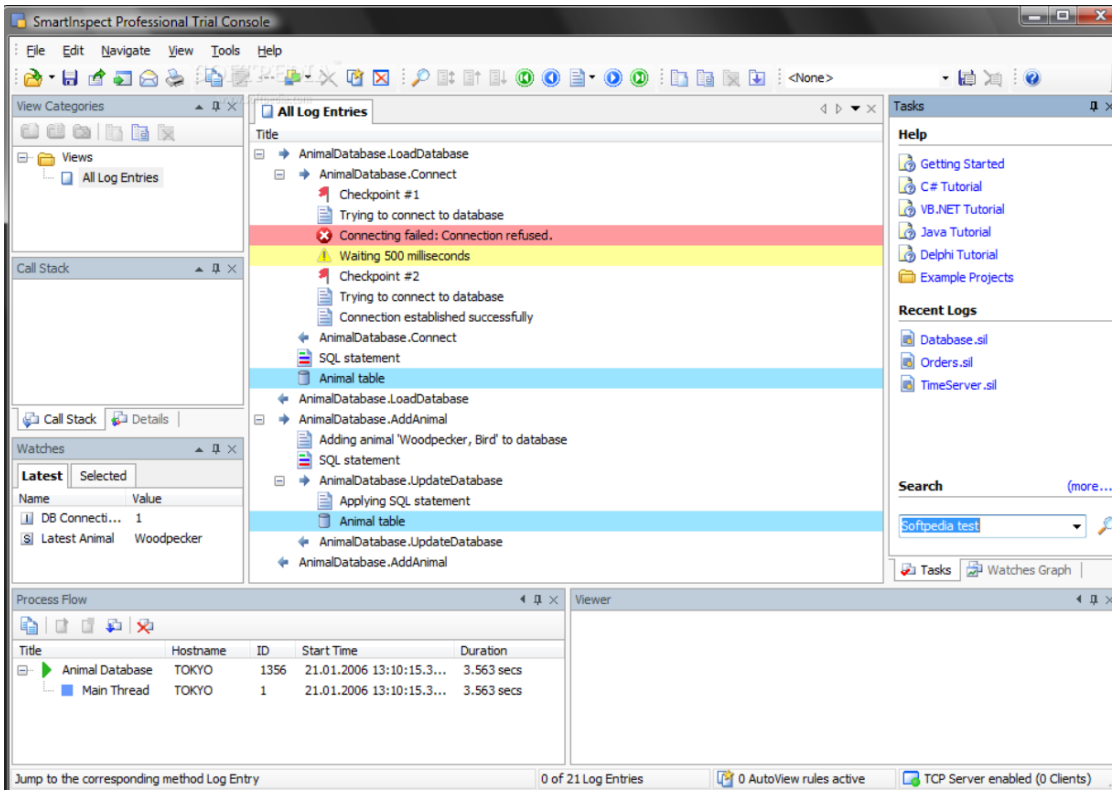
Πηγή: Duarte Teles, 2018

Αρκετές έρευνες, επίσης, έχουν επικεντρωθεί στην ανάπτυξη εφαρμογών fuzz testing, δηλαδή λογισμικών αυτόματου ελέγχου τα οποία δοκιμάζουν πολλά λάθος, απρόβλεπτα ή τυχαία δεδομένα εισόδου στα smart contracts προκειμένουν να εντοπίσουν λάθη στις εξόδους τους. Τέτοια εργαλεία στην βιβλιογραφία είναι τα EVMFuzz (Fu et al. 2019), ContractsFuzzer (Jiang et al. 2018) ReGuard (Liu et al. 2018) και Fuse (Chan και Chiang 2018). Συγκεκριμένα, το EVMFuzz παράγει πολλά seed contracts από το γονικό contract με διαφορετικές εισόδους το καθένα, ώστε να βρεθούν τυχόν λάθη και ασυνέπειες σε αυτά. Οι μετρικές του πειράματος έδειξαν ότι από τα 253,153 smart contracts, το 66,2% έδινε λάθος αποτελέσματα βάσει των εισόδων και των αναμενόμενων αποτελεσμάτων.

Ένα άλλο εργαλείο είναι το Slither (Feist et al. 2019). Το συγκεκριμένο λογισμικό μπορεί να δίνει τις σημασιολογικές πληροφορίες (semantic information) ενός smart contract που είναι γραμμένο σε γλώσσα Solidity μετατρέποντας το σε ένα SlithIR. Η μετατροπή αυτή διευκολύνει την κατανόηση του κώδικα του smart contract και άρα δίνει την δυνατότητα στους προγραμματιστές να δουλεύουν με μεγαλύτερη ευκολία και κατανόηση κώδικες τέτοιων συμβολαίων.

Το SmartInspect (Bragagnolo et al. 2018) χρησιμοποιεί τεχνικές αποσύνθεσης του κώδικα για να μπορέσει να παρέχει στον χρήστη μια γραφική αναπαράσταση της κατάστασης στην οποία βρίσκεται το smart contract. Αξίζει να σημειωθεί ότι το συγκεκριμένο πρόγραμμα δεν αναπτύσσει δικό του κώδικα για το συμβόλαιο. Χάρη στην γραφική αναπαράσταση του εργαλείου αυτού, το smart contract μπορεί να εξεταστεί εις βάθος και άρα να εντοπιστούν

πιθανές ασυνέπειες ή ελλείψεις σε συγκεκριμένες καταστάσεις στις οποίες μπορεί να βρεθεί το σύστημα.



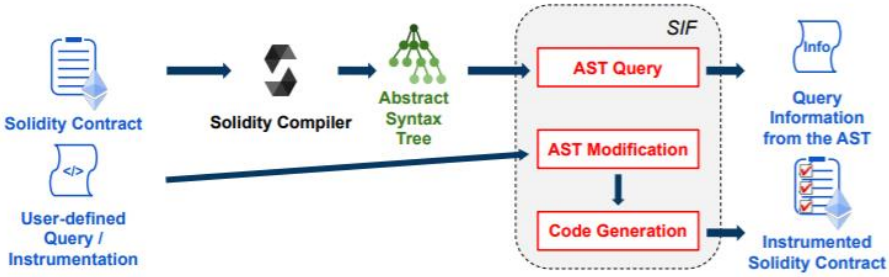
Εικόνα 21: Το γραφικό περιβάλλον του SmartInspect

Πηγή: www.softpedia.com

Ένα ακόμα εργαλείο το οποίο ελέγχει αυτόματα τις ιδιότητες των smart contract είναι το VERX (Permenev et al. 2020). Το εργαλείο αυτό βασίζεται σε τεχνικές μείωσης χρόνου εκτέλεσης και συμβολικής εκτέλεσης για την ακριβή και αποδοτική λειτουργία του Ethereum Virtual Machine. Το εργαλείο αυτό επικεντρώνεται στις διάφορες ιδιότητες που έχουν τα smart contracts και η έρευνα δείχνει ότι έχει μεγάλη απόδοση στην εύρεση τους.

Σε αντίθεση με άλλα λογισμικά, έχουν προταθεί και αρκετά τα οποία βοηθούν στην εκτέλεση και την ανάπτυξη κώδικα στις υπάρχουσες γλώσσες smart contract όπως την Solidity. Το Solidity Instrumentation Framework (SIF) προσφέρει έναν τρόπο query του Abstract Syntax Tree (AST): βοηθά στην προσθήκη, διαγραφή και επεξεργασία των κόμβων του AST και στην ανάπτυξη κώδικα στο AST ο οποίος προκύπτει από τις αλλαγές που πραγματοποιεί ο χρήστης στο σύστημα. Ο κύριος στόχος του SIF είναι η παρατήρηση, η ανάλυση, η βελτιστοποίηση και η παραγωγή κώδικα σε γλώσσα Solidity. Το πρόγραμμα αυτό αξιολογήθηκε σε 51 smart contracts στα οποία εισήχθησαν λάθη για σκοπούς έρευνας. Το SIF κατάφερε να αναλύσει σωστά το AST και να το παρουσιάσει ως κλάσεις σε

γλώσσα C++, παρέχοντας στον χρήστη μια διεπαφή με την οποία μπορεί να λάβει πληροφορίες από το σύστημα αλλά και να κάνει αλλαγές στο AST, ενώ παράλληλα μπορεί και να αναπτύξει κώδικα Solidity από το ίδιο το AST.



Εικόνα 22: Η λειτουργία του SIF

Πηγή: www.semanticscholar.org

Μια ακόμη ερευνητική κατεύθυνση που υπάρχει στην βιβλιογραφία αφορά την εύρεση bugs στον κώδικα των smart contracts αφού αυτά έχουν δημιουργηθεί. Οι Destefanis et al. (2018) υποστηρίζουν ότι πρέπει να βρεθεί μια αρχή βάσει της οποίας θα μπορεί να αξιολογηθεί η ορθότητα του κώδικα αυτού. Αναλύουν, ακόμη, την επίθεση στο Parity, μια εφαρμογή wallet, η οποία βασίστηκε σε ένα bug το οποίο υπήρχε σε μια από τις βιβλιοθήκες του κώδικα smart contract. Το bug αυτό επέτρεψε σε έναν ανώνυμο χρήστη να παγώσει περίπου 500 χιλιάδες Ether (τα οποία αντιστοιχούσαν σε 150 εκατομμύρια αμερικανικά δολλάρια τον Νοέμβριο του 2017). Η ευπάθεια στην βιβλιοθήκη αυτή προήλθε τελικά από κακό προγραμματισμό και όχι από κάποιο πηγαίο λάθος στον κώδικα Solidity. Γι'αυτό τον λόγο τονίζεται ότι θα πρέπει να αναπτυχθούν τέτοια εργαλεία ανάλυσης και εύρεσης bug.

Η ανάλυση και η μείωση της κατανάλωσης gas αποτελεί μια από τις κύριες κατευθύνσεις έρευνας στο πεδίο των smart contract. Για κάθε εκτέλεση κώδικα, υπάρχει ένα αντίστοιχο κόστος gas. Οι Aldweesh et al. (2018) ερεύνησαν το κατά πόσο το κόστος του gas είναι ανάλογο του χρόνου επεξεργασίας CPU, αλλά και το κατά πόσο ο χρόνος επεξεργασίας CPU είναι ανάλογος της ανταμοιβής σε gas. Βάσει των αποτελεσμάτων της έρευνάς τους, η κατανάλωση gas δεν είναι ανάλογη του υπολογιστικού φόρτου για την δημιουργία και την ολοκλήρωση smart contract. Οι Chen et al. (2017) πρότειναν την χρήση ενός εργαλείου ονόματι GASPER για τον αυτόματο εντοπισμό προγραμματιστικών μοτίβων τα οποία κοστίζουν gas. Οι κατηγορίες των μοτίβων αυτών χωρίζονται σε 2 είδη: τα Useless Code Related Patterns και τα Loop Related Patterns. Ο τύπος των μοτίβων είναι 7 ενώ το GASPER καταφέρνει να βρει τα 3 από αυτά: τα Dead Code, τα Opaque Predicates και τα Expensive Looped Operations. Στην έρευνα τους ανέλυσαν 4240 smart contracts και βρήκαν ότι πάνω από 80% αυτών είχε τουλάχιστον ένα τέτοιο μοτίβο στον κώδικα του. Η ίδια ομάδα το 2020 πρότεινε ένα ακόμη εργαλείο αυτόματου εντοπισμού μη αποδοτικού κώδικα όσον αφορά

στο gas, το GasChecker, το οποίο χρησιμοποιεί το προγραμματιστικό μοντέλο Mapreduce.Οι Marchesi et al. (2020) έχουν εντοπίσει 24 διαφορετικά σχεδιαστικά μοτίβα smart contract τα οποία οδηγούν σε υψηλή κατανάλωση gas. Τα έχουν χωρίσει στις εξής κατηγορίες: τις εξωτερικές συναλλαγές, την αποθήκευση, τις λειτουργίες και τις υπόλοιπες. Για κάθε τέτοια κατηγορία έχουν προτείνει κάποιες πιθανές λύσεις.

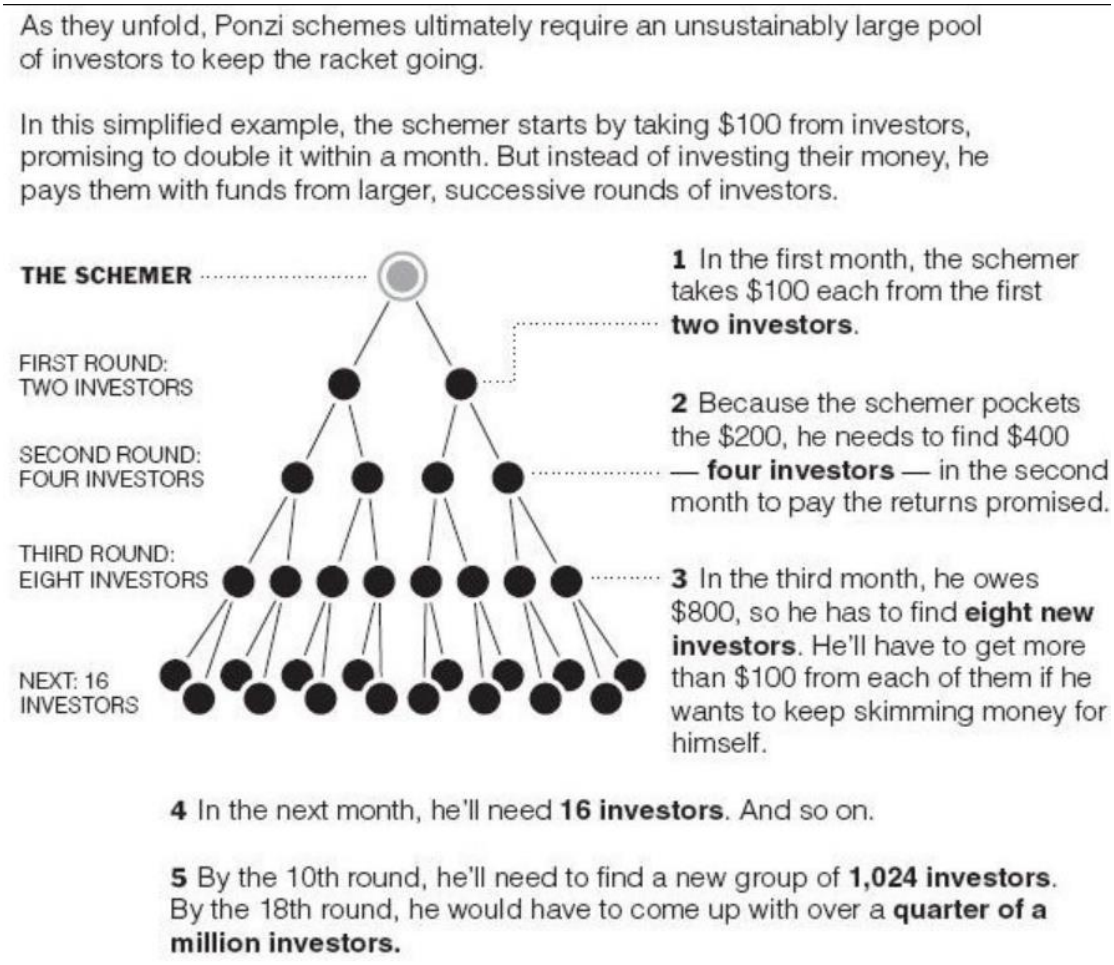
Απο αρχιτεκτονικής πλευράς, οι εφαρμογές που βασίζονται σε blockchain πολλές φορές έχουν κεντρικά στοιχεία όπως σέρβερ τα οποία τελικά συνδέονται με αποκεντρωμένα στοιχεία όπως smart contracts. Η σωστή ισορροπία μεταξύ των στοιχείων αυτών είναι το κλειδί για την ασφαλή, αποδοτική και φθηνή λειτουργία του όλου συστήματος. Σε μια έρευνα από τους Wessling et al. (2019) αναλύθηκε η αρχιτεκτονική των χτησίματος των blockchain. Σε αυτή την έρευνα βρέθηκε ότι συγκεκριμένα μοτίβα software design δεν αποδίδουν πάντα καλά στο πλαίσιο του blockchain και μάλιστα δύναται να έχουν μεγάλη αρνητική επίπτωση στην ταχύτητα και το κόστος ολοκλήρωσης των smart contract. Σαν συμπέρασμα, οι συγγραφείς τόνισαν ότι πρέπει να δοθεί μεγαλύτερη σημασία στην εύρεση νέων τακτικών προσέγγισης του κώδικα σε smart contract και blockchain ώστε να μπορούν να υϊοθετηθούν μαζικώς.

Σημαντική, επίσης, κρίνεται και η ικανότητα να προσφέρεται στους προγραμματιστές μια σειρά από μετρικές για την ανάλυση του κώδικα των smart contracts. Αυτές οι μετρικές στην βιβλιογραφία εμφανίζονται ως Object Oriented Metrics (OO). Ο Hegedus (2019) χρησιμοποιήσε τέτοιες μετρικές για την εκτίμηση των ιδιοτήτων smart contracts που είναι γραμμένα σε γλώσσα Solidity. Χρησιμοποίησε ένα εργαλείο ονόματι SolMet για να αναλύσει τα αρχεία πηγαίου κώδικα 10,000 smart contracts και κατέληξε στο συμπέρασμα ότι αυτά είναι συνήθως μικρού μήκους, όχι πολύ περίπλοκα και έχουν ελάχιστα σχόλια. Γι’αυτό τον λόγο πρότεινε την χρήση εξωτερικών βιβλιοθηκών από άλλες γλώσσες για να μπορούν κομμάτια του κώδικα των smart contracts να επαναχρησιμοποιηθούν.

Οι Pierro και Tornelli (2020) χρησιμοποίησαν ένα code parser για να υπολογίσουν μετρικές όπως οι συνολικές γραμμές κώδικα, τις κενές γραμμές, τις γραμμές με σχόλια, τις στατικές ανακλήσεις και τον αριθμό των συναρτήσεων σε smart contracts. Τελικά, κατέληξαν στο συμπέρασμα ότι η μετρική στα smart contracts που ακολουθεί την ίδια στατιστική κατανομή και άρα συμπεριφορά με τα παραδοσιακά λογισμικά είναι οι συνολικές γραμμές κώδικα.

Η ασφάλεια στα smart contracts είναι μια πολύ βασική ερευνητική κατεεύθυνση στον χώρο του blockchain. Ένας κίνδυνος στο δίκτυο του Ethereum είναι τα σχέδια Ponzi (Ponzi schemes), τα οποία δεν είναι κίνδυνοι που σχετίζονται με τον τρόπο ανάπτυξης των smart contracts αλλά αποτελούν μια μορφή εξαπάτησης από κακόβουλα στοιχεία. Το σχέδιο Ponzi είναι μια απάτη στην οποία υπό την υπόσχεση τεράστιων κερδών, οι χρήστες «επενδύουν» αρκετά χρήματα. Τα «κέρδη» που παρουσιάζονται σε κάθε χρήστη είναι βασικά τα λεφτά από τις προηγούμενες εξαπατήσεις άλλων χρηστών. Όσο, λοιπόν, υπάρχουν νέοι επενδυτές στο δίκτυο, το Ponzi scheme συνεχίζεται (το ίδιο το όνομα της εξαπάτησης αυτής προέρχεται από τον Ponzi πριν από 100 χρόνια περίπου). Οι Bartoletti et al. (2020) διεξήγαγαν μια έρευνα σχετικά με τις συμπεριφορές και τα αποτελέσματα των

σχεδίων Ponzi στο δίκτυο του Ethereum. Η ανάλυση τους έδειξε ότι οι οικονομικές επιπτώσεις των σχεδίων αυτών είναι περιορισμένες και ότι ο αριθμός των smart contracts που επηρρεάζεται είναι σχετικά μικρός.



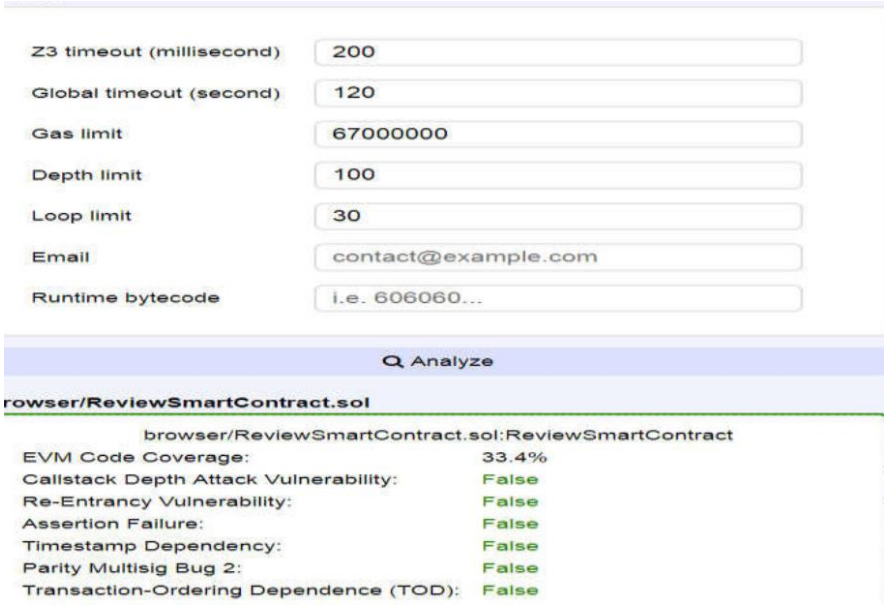
Εικόνα 23: Παράδειγμα Ponzi scheme

Πηγή: www.nyujlb.org

Χρησιμοποιώντας δείγματα από πραγματικά smart contracts οι Chen et al. (2019) πρότειναν την χρήση machine learning για την ανίχνευση Ponzi schemes στα smart contracts (smart Ponzi schemes). Στην έρευνα τους ανέλυσαν περίπου 3000 smart contracts και βρήκαν ότι σε περίπου 200 από αυτά υπήρχε Ponzi scheme. Επιπροσθέτως, οι Wohrer και Zdun (2018) έχουν προτείνει ένα εργαλείο Checks Effects Interaction το οποίο εξηγεί τα μοτίβα με τα οποία πρέπει να είναι ανεπτυγμένο ένα smart contract ώστε να μην μπορεί να χρησιμοποιηθεί για τέτοιες απειλές.

Υπάρχουν αρκετοι ερευνητές οι οποίοι έχουν προτείνει εργαλεία για την αναγνώριση ευάλωτων smart contracts στο Ethereum, όπως το TEETHER (Krupp και Rossow, 2018), το MAIAN (Nikolic et al. 2018), το Oyente (Luu et al. 2016), και το MadMax (Grech et al. 2018).

Η εμφάνιση bugs στα smart contract μπορεί να προκαλέσει τεράστιες οικονομικές ζημιές, γι'αυτό τον λόγο είναι πολύ σημαντική η εύρεση και η διόρθωση τους. Το TEETHER είναι ένα εργαλείο το οποίο προσπαθεί να παράξει bugs για να βρει σε ποιο κομμάτι είναι ευάλωτο ένα smart contract. Το εργαλείο χρησιμοποιήθηκε σε 38,757 Ethereum smart contracts, από τα οποία παρατηρήθηκε ότι τα 815 είχαν κάποιο χαρακτηριστικό το οποίο μπορούσε να το εκμεταλλευτεί το εργαλείο. Το Oyente είναι ένα εργαλείο symbolic execution το οποίο αναζητεί bugs στον κώδικα του smart contract. Από 20,000 Ethereum smart contracts, το Oyente βρήκε ότι σε 8833 από αυτά υπήρχε bug που το έκανε ευάλωτο. Το MadMax χρησιμοποιεί στατικό προγραμματισμό για να βρει αυτόματα ευπάθειες που σχετίζονται με το gas. Αυτές οι ευπάθειες εκμεταλλεύονται την συμπεριφορά του smart contract όταν χρησιμοποιεί όλο το διαθέσιμο gas για να ολοκληρωθεί. Τα αποτελέσματα έδειξαν ότι το 81% των smart contracts που αναλύθηκαν έχουν τέτοιες ευπάθειες.



Εικόνα 24: Report που προκύπτει από εφαρμογή του Oyente σε smart contract

Πηγή: Salah et al. (2019)

Μια ακόμη επίθεση που μπορεί να χρησιμοποιηθεί στο δίκτυο του Ethereum είναι η re-entrancy, η οποία σκοπεύει στην κλοπή Ether. Οι Chinen et al. (2020) πρότειναν το Re-entrancy Analyzer (RA), ένα λογισμικό στατικής συμβολικής ανάλυσης για να εντοπίζει τέτοιου είδους επιθέσεις.

Η κατηγοριοποίηση των τεχνικών εκμετάλλευσης του blockchain είναι 4 ανάλογα με τον τρόπο λογικής στην οποία στοχεύει η επίθεση (Sayeed et al. 2020), και αυτές είναι τα πρωτόκολλα συναίνεσης, τα bugs στο smart contract, τα malware στα λειτουργικά συστήματα και οι κακόβουλοι χρήστες. Η ανάλυση της έρευνας αυτής δείχνει ότι οι πιο συνήθεις επιθέσεις στο blockchain είναι η επίθεση DAO, η επίθεση Parity, η Govern Mental, και οι Dynamic libraries. Τα πιο συνήθη εργαλεία για την επίλυση τους, σύμφωνα με την έρευνα αυτή, είναι το Fuse, το BUG framework, το GOATX Casino, το Truffle και το Oyente.

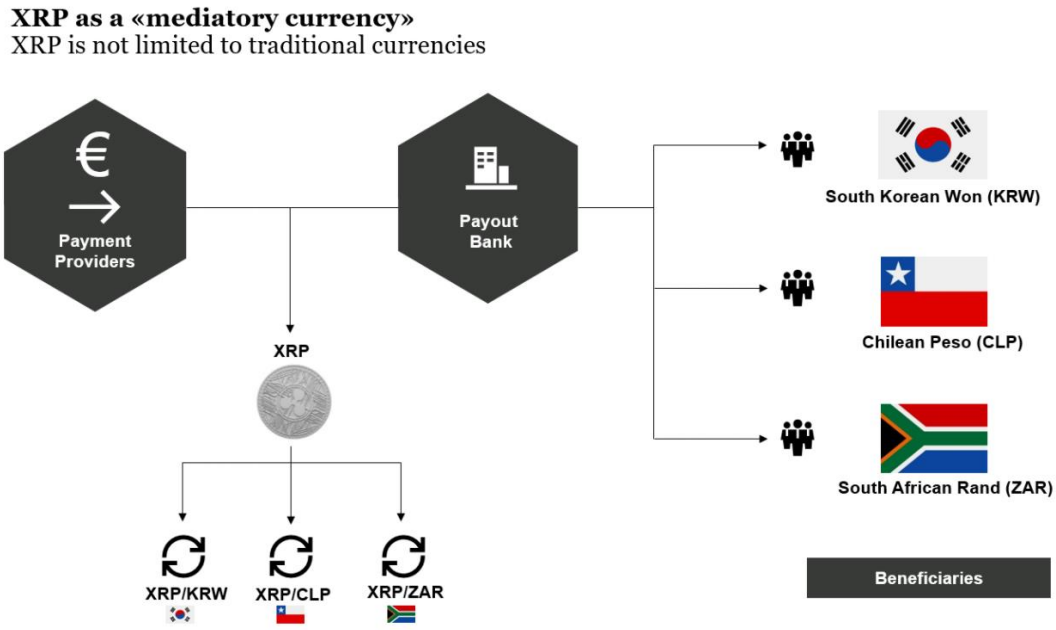
3. Ιδιωτικά δίκτυα Blockchain

Τα ιδιωτικά δίκτυα blockchain έχουν αναπτυχθεί ως μια διαφορετική λύση από τα δημόσια για επιχειρηματικές εφαρμογές. Σε αντίθεση με τα δημόσια, τα ιδιωτικά δίκτυα δεν είναι ανοιχτά προς συμμετοχή οποιουδήποτε κόμβου. Αντιθέτως, για να συμμετέχει κάποιος σε ένα τέτοιο δίκτυο θα πρέπει να λάβει κάποια πρόσκληση από την οντότητα η οποία δημιούργησε το δίκτυο. Οι βασικές λειτουργίες της προσπέλασης, της εγγραφής και της επικύρωσης των συναλλαγών στο δίκτυο απαιτούν ειδικά δικαιώματα τα οποία τα διαχειρίζεται η κεντρική οντότητα, η οποία συνήθως είναι εταιρεία. Έτσι, ένας κόμβος μπορεί να μην έχει πρόσβαση και στις 3 αυτές λειτουργίες αλλά μόνο σε συγκεκριμένες από αυτές. Έτσι, σε αυτό το δίκτυο δεν υπάρχει ισότητα μεταξύ των κόμβων. Ο βασικός λόγος για τον οποίο δημιουργήθηκαν τα ιδιωτικά δίκτυα blockchain είναι διότι επιτρέπουν την ανταλλαγή πληροφοριών μόνο μεταξύ συνεργαζόμενων εταιρειών, αλλά και επειδή επιτρέπουν την γρηγορότερη επικύρωση των συναλλαγών χάρη στον μικρότερο αριθμό κόμβων που συμμετέχουν στο δίκτυο, ωστόσο αξίζει να σημειωθεί ότι δεν είναι όσο ασφαλή όσο τα δημόσια δίκτυα, μιας και υπάρχει κεντρική εξουσία η οποία διαχειρίζεται τα δεδομένα (Sharma, 2021).

Τα βασικότερα ιδιωτικά δίκτυα blockchain που έχουν αναπτυχθεί είναι τα Hyperledger Fabric, Ripple και Quorum.

3.1 Ripple

Ripple: Αποτελεί ένα ευρέως χρησιμοποιούμενο permissioned δίκτυο blockchain από εταιρείες και ειδικά τράπεζες οι οποίες μεταφέρουν χρήματα διασυνοριακά, ανεπτυγμένο το 2012. Η δυνατότητα μεταφοράς χρημάτων μεταξύ εταιρειών σε διαφορετικές χώρες προσδίδει μεγάλη σημασία στο Ripple, καθώς σχεδόν όλες οι εφοδιαστικές αλυσίδες του σήμερα εκτείνονται σε πολλές διαφορετικές χώρες. Είναι γραμμένο σε Python, είναι open source και ο αλγόριθμος συναίνεσης είναι το Probabilistic Voting βάσει σέρβερ οι οποίοι ανήκουν σε τράπεζες, στο οποίο η συναίνεση προκύπτει βάσει ψηφοφορίας μεταξύ των μεγαλύτερων consortium members του δικτύου. Διαθέτει το δικό του κρυπτονόμισμα ονόματι XRP, ωστόσο το σύστημα των μεταφορών του υποστηρίζει όλα τα νομίσματα που κυκλοφορούν. Το κρυπτονόμισμα XRP ουσιαστικά χρησιμοποιείται για την εύκολη μετατροπή μεταξύ διαφορετικών νομισμάτων. Η μεταφορά χρημάτων μεταξύ 2 διευθύνσεων γίνεται μέσω ενός μεσάζοντα (credit intermediary) ονόματι Gateway ο οποίος είναι υπεύθυνος για την αποστολή και την παραλαβή των χρημάτων ή των κρυπτονομισμάτων. Αξίζει να υπογραμμιστεί ότι το νόμισμα που στέλνει η μια πλευρά δεν χρειάζεται να είναι το ίδιο που λαμβάνει η άλλη πλευρά, διότι η μετατροπή γίνεται μέσω του Gateway. Σύμφωνα με το Ripple, η επικύρωση μιας συναλλαγής στο δίκτυο απαιτεί περίπου 5 δευτερόλεπτα.

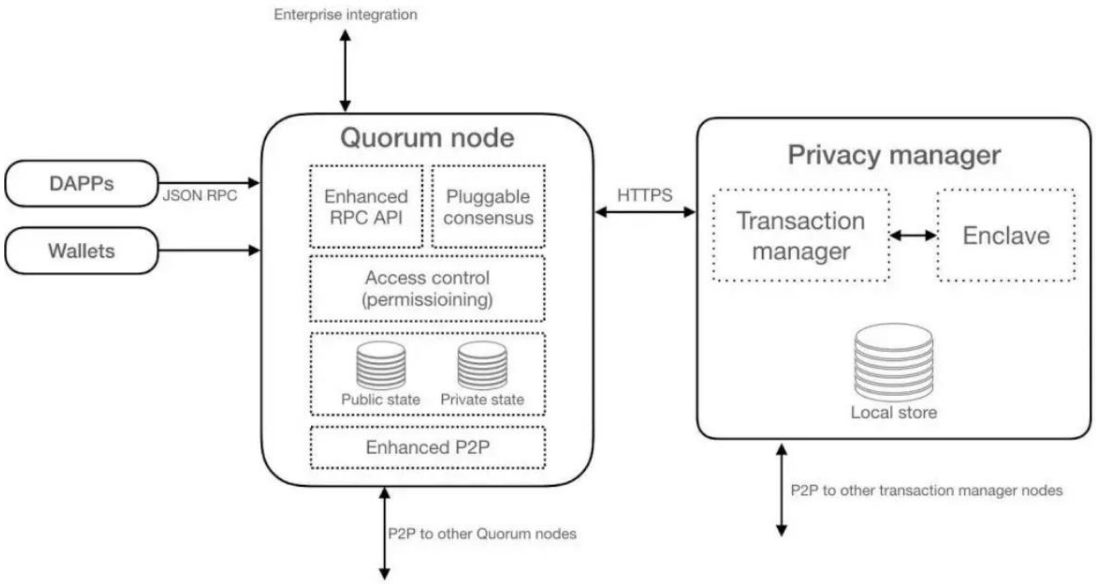


Εικόνα 25: Οι συναλλαγές στο δίκτυο του Ripple

Πηγή: www.ripple.com

3.2 Quorum

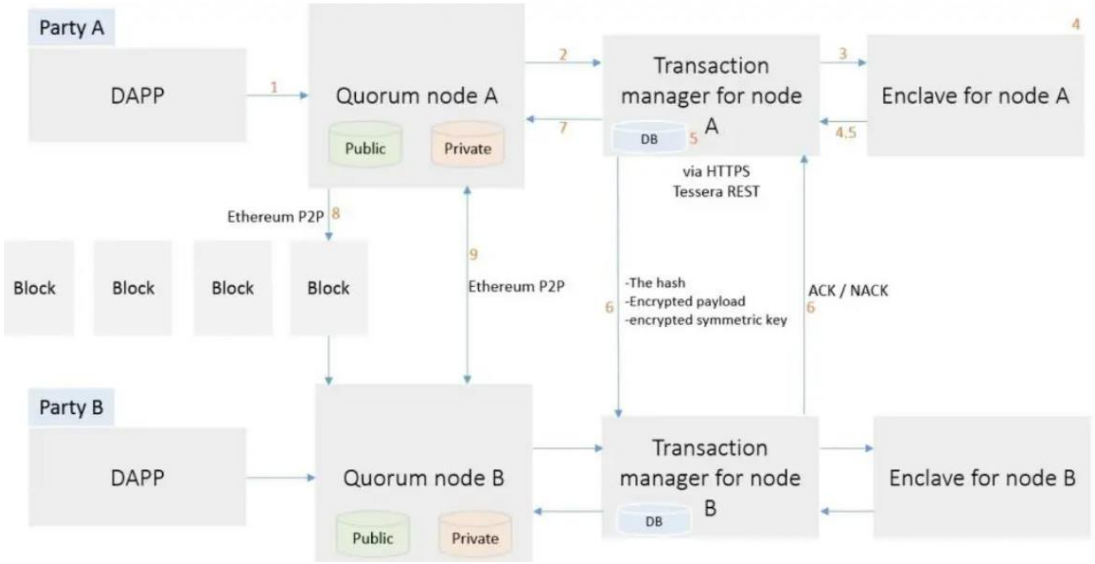
Το Quorum blockchain αναπτύχθηκε από την εταιρεία JPMorgan και αποτελεί fork από τον client geth του δημόσιου δικτύου Ethereum. Είναι ουσιαστικά μια τροποποιημένη έκδοση του με αρκετά πρόσθετα χαρακτηριστικά για επιχειρηματικές εφαρμογές. Όπως το Ethereum, έτσι και το Quorum είναι open source και μάλιστα αναβαθμίζεται και βελτιώνεται με κάθε ενημέρωση του Ethereum. Τα βασικά πρόσθετα χαρακτηριστικά του είναι η ιδιωτικότητα των συναλλαγών, οι πολλαπλοί υποστηριζόμενοι αλγόριθμοι συναίνεσης, η διαχείριση των δικαιωμάτων για τους συμμετέχοντες κόμβους (permissions management) και η βελτιωμένη ταχύτητα των συναλλαγών. Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική του Quorum (αξίζει να σημειωθεί ότι ο privacy manager είναι το στοιχείο που ενσωματώνει την εκτός αλυσίδας ιδιωτικότητα των κόμβων).



Εικόνα 26: Η αρχιτεκτονική του Quorum

Πηγή: www.blockgeeks.com

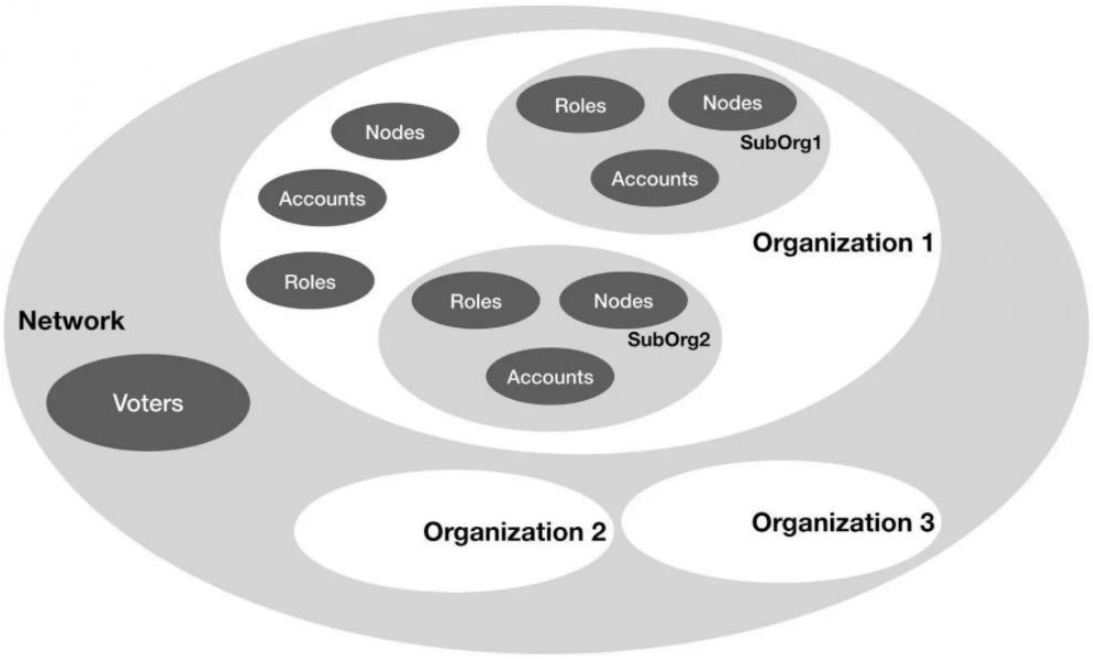
Ο αλγόριθμος συναίνεσης στο δίκτυο αυτό είναι συνήθως ένας από τους RAFT, Proof-of-Authority ή Istanbul Byzantine Fault Tolerant. Η ευκολία αλλαγής από τον έναν στον άλλο προσδίδει στην εταιρεία αυξημένη ευελιξία για τις εφαρμογές της. Για τις ιδιωτικές συναλλαγές στο δίκτυο, το Quorum υποστηρίζει και off-chain signing επιτρέποντας στους κόμβους να πραγματοποιούν συναλλαγές χωρίς την επικύρωση από το υπόλοιπο δίκτυο, προσφέροντας έτσι ακόμα μεγαλύτερη ευελιξία στους συμμετέχοντες κόμβους. Στο παρακάτω σχήμα φαίνεται με λεπτομέρεια μια ιδιωτική συναλλαγή στο δίκτυο αυτό:



Εικόνα 27: Οι ιδιωτικές συναλλαγές στο Quorum

Πηγή: www.blockgeeks.com

Ο μηχανισμός των δικαιωμάτων στο Quorum βασίζεται στην λογική του Role Based Access Control (RBAC) μηχανισμού, αποτελεί δε ένα πρότυπο ANSI για επιχειρηματικό μηχανισμό access control. Βάσει αυτού, λοιπόν, μοιράζονται τα δικαιώματα μέσα στο δίκτυο καθώς και τα δικαιώματα συμμετοχής στο ίδιο το δίκτυο. Τα βασικά στοιχεία βάσει των οποίων λειτουργεί το πρότυπο αυτό είναι τα: δίκτυο, οργανισμός, υπο-οργανισμός, λογαριασμός, ψηφοφόρος, ρόλος, κόμβος και το δικαίωμα. Στο παρακάτω σχήμα φαίνονται αναλυτικά:



Εικόνα 28: Το permissioning στο Quorum

Πηγή: www.blockgeeks.com

Χάρη, λοιπόν, στο permissioning system και στην ευελιξία των ιδιωτικών συναλλαγών του, το Quorum αποτελεί ένα από τα βασικά ιδιωτικά blockchains παγκοσμίως με εφαρμογή κυρίως σε εταιρείες του οικονομικού τομέα.

3.3 Hyperledger Fabric

Το Hyperledger Fabric είναι είναι ένα πλαίσιο ανάπτυξης για permissioned blockchains το οποίο δημιουργήθηκε από το Linux Foundation και χρηματοδοτήθηκε από την IBM και την Digital Asset το 2015. Τα smart contracts στο Hyperledger Fabric ονομάζονται και chaincode.

Αποτελεί το μοναδικό permissioned blockchain δίκτυο το οποίο επιτρέπει στον χρήστη την ανάπτυξη εφαρμογών με αρθρωτή αρχιτεκτονική (modular architecture). Όντας permissioned, οι εταιρείες που το χρησιμοποιούν μπορούν να καθορίζουν ποιές άλλες εταιρείες και χρήστες μπορούν να συμμετάσχουν σε αυτό και άρα να μπορούν να ανταλλάξουν ευαίσθητες πληροφορίες μόνο με συγκεκριμένους κόμβους. Είναι γραμμένο σε Python, είναι open source, ενώ ο αλγόριθμος συναίνεσης διαφέρει από δίκτυο σε δίκτυο μιας και χάρη στην αρχιτεκτονική του, ο χρήστης είναι αυτός που τελικά καθορίζει το πως τελικά θα φτάνουν σε συναίνεση οι κόμβοι.

Το πλαίσιο αυτό αναπτύχθηκε για χρήση σε περιβάλλοντα εταιρειών οι οποίες δεν επιθυμούν να συμμετάσχουν σε δημόσιο blockchain, αποκρύπτοντας έτσι την διαρροή πληροφοριών όπως για παράδειγμα οι τιμές των προϊόντων της εταιρείας προς το υπόλοιπο δίκτυο. Η βασική διαφορά με το Ethereum είναι ότι το Hyperledger Fabric πρόκειται για ιδιωτικό blockchain, σε αντίθεση με το Ethereum που είναι δημόσιο, και άρα οι αλγόριθμοι συναίνεσης και οι μαθηματικές πράξεις που πρέπει να λυθούν για την διαδικασία συναίνεσης διαφέρουν αρκετά σε σχέση με δημόσια blockchains. Συνεπώς, και η διαδικασία ανάπτυξης αλλά και η λειτουργία των smart contract αλλάζει αρκετά σε σχέση με αυτά. Η γλώσσα των smart contract στο Hyperledger είναι συνήθως η Javascript ή η Go.

3.3.1 Περιγραφή βημάτων για την ανάπτυξη smart contract στο Hyperledger

Στο παρόν κομμάτι της εργασίας θα αναλυθεί η ανάπτυξη και η λειτουργία των smart contracts στο Hyperledger Fabric μιας και αυτό αποτελεί το βασικό ιδιωτικό permissioned δίκτυο που χρησιμοποιείται σε επιοχειρηματικές εφαρμογές στην εφοδιαστική αλυσίδα.

Η αρχιτεκτονική του Hyperledger αναλύεται στα εξής κομμάτια (layers):

Consensus layer: Αυτό το κομμάτι είναι υπεύθυνο για την ολοκλήρωση της διαδικασίας συναίνεσης και την επικύρωση της.

Smart Contract layer: Το κομμάτι υπεύθυνο για την επεξεργασία των αιτημάτων συναλλαγών και την διαδικασία επαλήθευσης τους με βάση επιχειρηματική λογική.

Communication layer: Το κομμάτι υπεύθυνο για τα peer-to-peer μηνύματα στο δίκτυο μεταξύ των κόμβων που διαθέτουν το κοινό ledger.

Data Store Abstraction: Το κομμάτι στο οποίο αποθηκεύονται τα δεδομένα και είναι υπεύθυνο για την διάθεση των δεδομένων αυτών στα υπόλοιπα κομμάτια.

Crypto Abstraction: Το κομμάτι της κρυπτογραφίας το οποίο επιτρέπει την αλλαγή ορισμένων αλγορίθμων κρυπτογραφίας στο δίκτυο, για την μεγαλύτερη ευελιξία του δικτύου.

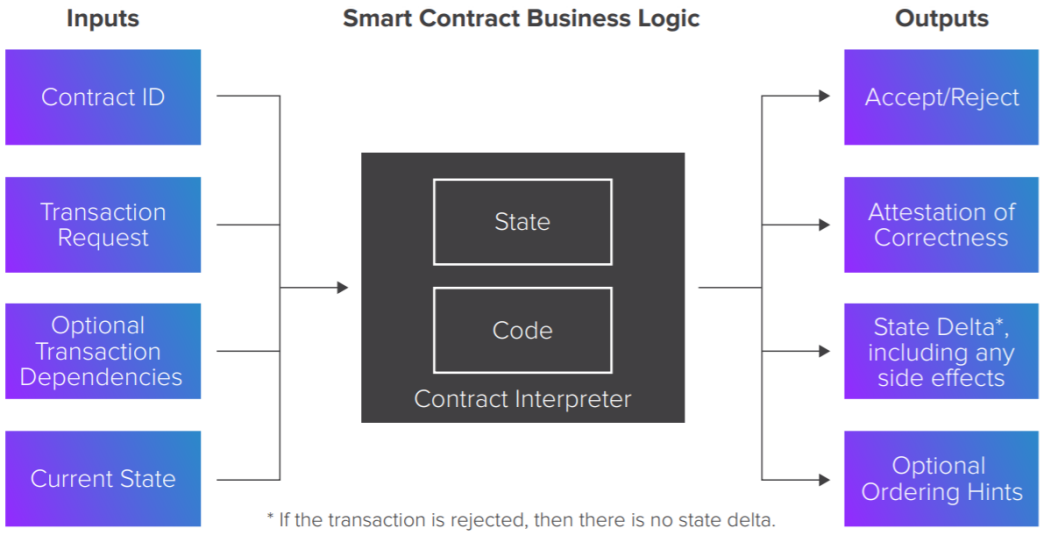
Identity Services: Το κομμάτι που είναι υπεύθυνο για την ανάπτυξη της εμπιστοσύνης μεταξύ των κόμβων, την εγγραφή νέων χρηστών στο δίκτυο, την διαγραφή χρηστών από αυτό καθώς και την αυθεντικοποίηση των υπάρχοντων χρηστών στο δίκτυο κατά την διάρκεια των συναλλαγών.

Policy Services: Το κομμάτι που είναι υπεύθυνο για τις διάφορες πολιτικές που ισχύουν στο δίκτυο όπως η πολιτική συναίνεσης και η διαχείριση του group χρηστών.

APIs: Τα κομμάτια που επιτρέπουν την διεπαφή των χρηστών με το δίκτυο του blockchain.

Interoperation: Το κομμάτι που επιτρέπει την διαλειτουργικότητα μεταξύ των υπόλοιπων κομματιών του Hyperledger.

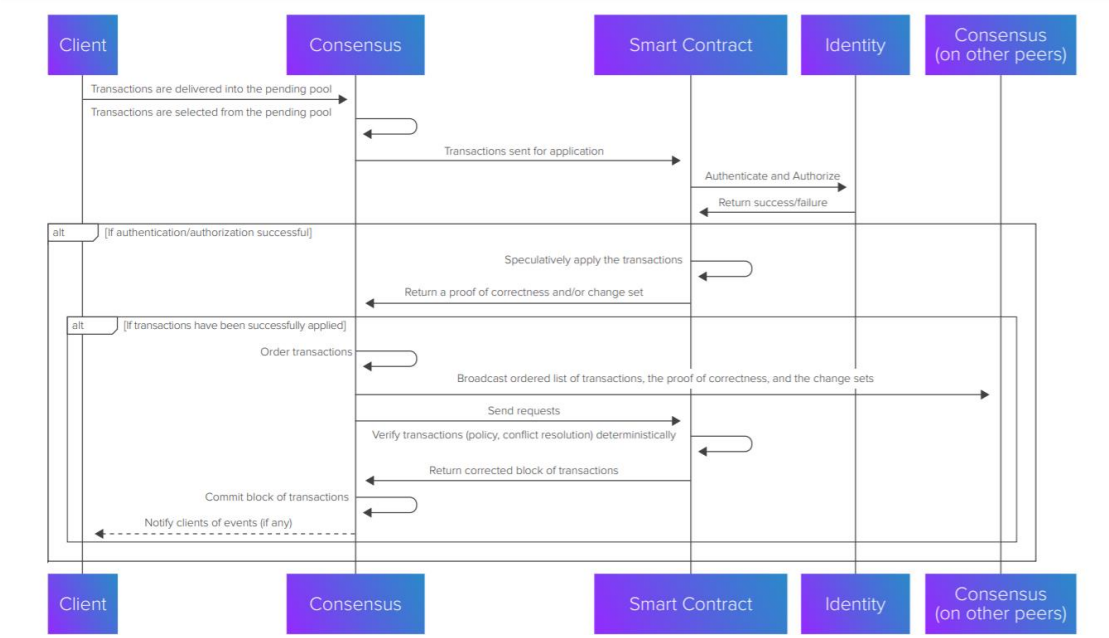
Αξίζει να παρατηρηθεί ότι σε σχέση με το δίκτυο του Ethereum, το Hyperledger Fabric παρουσιάζει μεγαλύτερη δυσκολία στην ανάπτυξη των smart contract, μιας και περιέχει πολλές μεταβλητές που πρέπει να ορισθούν από τους χρήστες, σε ένα ιδιωτικό δίκτυο blockchain το οποίο έχει από μόνο του χαμηλότερη ασφάλεια από ένα δημόσιο δίκτυο blockchain.



Εικόνα 29: Διαδικασία smart contract στο Hyperledger fabric

Πηγή: www.hyperledger.org

Η αναλυτική διαδικασία για τον τρόπο με τον οποίο τα smart contracts αλληλεπιδρούν με τις διάφορες οντότητες στο δίκτυο φαίνεται στο παρακάτω σχήμα:



Εικόνα 30: Αλληλεπίδραση του smart contract με τις οντότητες του δικτύου

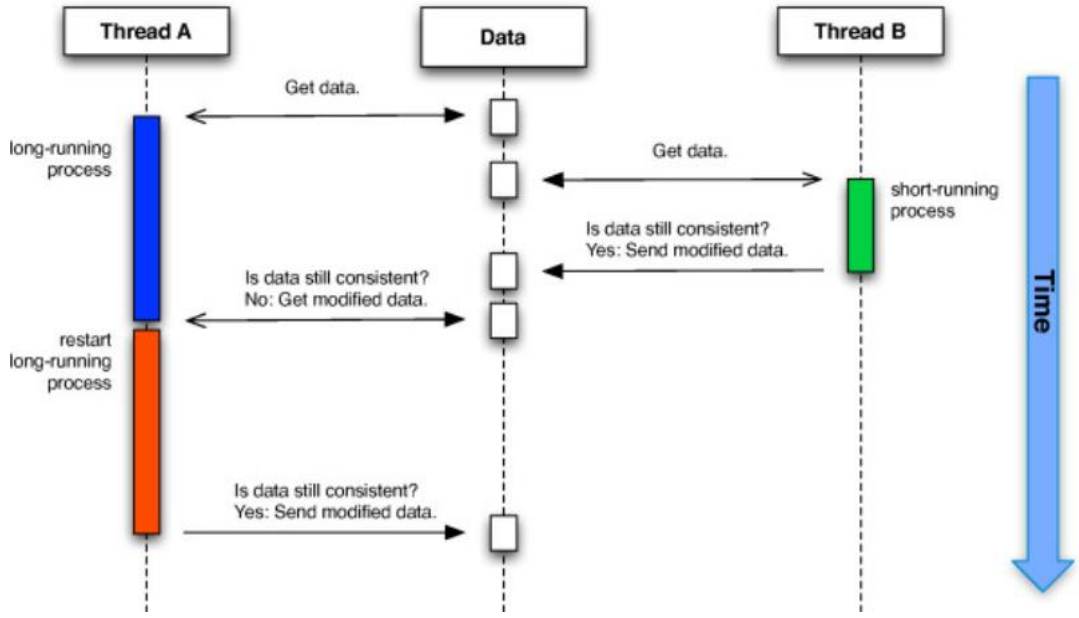
Πηγή: www.hyperledger.org

3.3.2 Εργαλεία βελτιστοποίησης κώδικα smart contract στο Hyperledger Fabric

Το Hyperledger Fabric αποτελεί το βασικό ιδιωτικό δίκτυο blockchain στο οποίο εφαρμόζονται smart contracts για χρήση σε εφοδιαστικές αλυσίδες, συνεπώς σε αυτή την ενότητα θα παρουσιαστούν κάποια εργαλεία ανάλυσης και βελτιστοποίησης κώδικα smart contracts, όπως έγινε και για το δίκτυο του Ethereum.

Ένα θέμα που παρουσιάζεται σε αρκετά smart contracts είναι η παρουσίαση bugs στον κώδικα τους. Τα προβλήματα αυτά είναι ιδιαίτερα δύσκολα να λυθούν μετά την ανάπτυξη τους, γεγονός το οποίο μπορεί να οδηγήσει σε απώλεια χρημάτων. Οι Kalra et al. (2018) ανέπτυξαν ένα μοντέλο ονόματι Zeus το οποίο μπορεί να ελέγχει και να επικυρώνει την ορθότητα των smart contracts, δηλαδή την ασφάλεια των δεδομένων τους και την συμμόρφωση τους με επιχειρηματική λογική. Αξίζει να σημειωθεί ότι το μοντέλο αυτό έχει χρησιμοποιηθεί σε περισσότερα από 20,000 smart contracts, από τα οποία έχει αποδειχθεί ότι περισσότερα από 90% έχουν προβλήματα ασφαλείας.

Μια ακόμη σημαντική ερευνητική κατεύθυνση που υπάρχει στο δίκτυο των blockchain είναι η βελτιστοποίηση του τρόπου με τον οποίο συμβαίνουν οι συναλλαγές σε αυτό. Ένα block αποτελείται από πολλές συναλλαγές smart contract οι οποίες προστίθενται σε αυτό από τους miners, η μία μετά την άλλη. Για να εξασφαλιστεί ότι τα blocks που προστίθενται στην αλυσίδα είναι σωστά, οι κόμβοι-validators εκτελούν τις συναλλαγές αυτές σειριακά. Το block μπορεί να προστεθεί στην αλυσίδα μόνο εάν οι κόμβοι-validators συμφωνούν με το τελικό αποτέλεσμα των miner. Η σειριακή αυτή συμπεριφορά οδηγεί σε χαμηλή ταχύτητα εκτέλεσης των συναλαλγών και άρα χαμηλή απόδοση του συστήματος. Η ιδέα που πρότειναν οι Anjana et al. (2019) είναι η παραλληλοποίηση του συστήματος αυτού, δηλαδή η επεξεργασία πολλών συναλλαγών ταυτόχρονα, με την χρήση ενός λογισμικού Software Transactional Memory System (STM). Χρησιμοποιώντας το μαζί με block graphs μπορούν να παραλληλοποιήσουν την μέχρι τώρα σειριακή διαδικασία και άρα να μειώσουν δραματικά τον χρόνο εκτέλεσης των smart contract.



Εικόνα 31: Λειτουργία των STM

Πηγή: Johann M. Kraus, Hans Kestler, 2010

Το Hyperledger Fabric είναι ένα permissioned blockchain δίκτυο το οποίο χρησιμοποιεί γνωστές προγραμματιστικές γλώσσες όπως Java και Go για την ανάπτυξη smart contracts (τα οποία ονομάζονται chaincode). Αυτές οι γλώσσες έχουν προφανώς και πλεονεκτήματα και μειονεκτήματα. Τα βασικά μειονεκτήματα είναι ότι οι γλώσσες αυτές δεν έχουν ανατπυχθεί για την δημιουργία smart contracts, συνεπώς μπορεί να περιέχουν κενά ασφαλείας τα οποία δεν υπάρχουν σε άλλες γλώσσες ειδικά για smart contracts. Οι Yamashita et al. (2019) ανέλυσαν τον κώδικα της Go και βρήκαν ότι υπάρχουν 14 διαφορετικοί κίνδυνοι ασφαλείας όσον αφορά στα smart contracts. Επισήμαναν, ακόμη, ότι

κάποια από τα προαναφερθέντα εργαλεία μπορούν να καλύψουν κάποια από τακενά αυτά, ωστόσο όχι όλα. Η έρευνα αυτή δείχνει ότι και άλλες γλώσσες μπορούν να χρησιμοποιηθούν για την ανάπτυξη smart contract, ωστόσο προτύ την εφαρμογή τους θα πρέπει να αναλυθεί ο πηγαίος κώδικας τους για τυχον τέτοια κενά ασφαλείας.

Σύμφωνα με ερευνητές (Marchesi at al. 2018, Ortu et al. 2019) υπάρχουν αρκετά κοινά αλλά και αρκετές διαφορές μεταξύ των παραδοσιακών λογισμικών και των λογισμικών ειδικά για blockchain (ή αλλιώς blockchain oriented software ή BOS).

Χάρη στην μεγάλη αύξηση των τεχνολογιών του blockchain, τα BOS έχουν επίσης αυξηθεί, χωρίς αυτό να σημαίνει βέβαια ότι όλα τηρούν τα ίδια πρότυπα ασφαλείας και ποιότητας. Οι ερευνητές πρότειναν μεθόδους αξιολόγησης όπως τα διαγράμματα UML για να μπορούν να απεικονιστούν όλες οι λεπτομέρειες και οι ιδιαιτερότητες των συστημάτων αυτών. Με αυτό τον τρόπο, οι εταιρείες που χρησιμοποιούν τέτοια συστήματα θα καταφέρουν να επωφεληθούν από το σωστό software engineering. Πέρα από αυτό, τονίστηκε η ανάγκη να αναπτυχθούν εργαλεία μοντελοποίησης BOS για την διευκόλυνση ανάπυξης υψηλής ποιότητας κώδικα smart contract.

Για να εκμεταλλευτούν πλήρως όλες οι δυνατότητες των τεχνολογιών blockchain, είναι απαραίτητη η κατανόηση της δομής και της συμπεριφοράς των συστημάτων BOS, και ειδικά του τρόπου με τον οποίο αυτά διαφέρουν από τα παραδοσιακά συστήματα λογισμικών. Σε αυτό το πλαίσιο, οι Ortu et al (2019) ανέπτυξαν μια στατιστική κατηγοριοποίηση των BOS, συγκρίνοντας τα blockchain oriented και τα Java software συστήματα βάσει 10 μετρικών. Στα αποτελέσματα τους βρήκαν ότι τα συστήματα αυτά διαφέρουν αρκετά, ειδικά όσον αφορά στις μετρικές Average Cyclomatic, Ration Comment to Code και Number of Statements.

4. Δομημένη βιβλιογραφική ανασκόπηση εφαρμογής τεχνολογιών blockchain στον κλάδο των ποτών

Το παρόν κεφάλαιο έχει ως σκοπό την παρουσίαση και ανάλυση της βιβλιογραφίας στο ερευνητικό πεδίο γύρω από την εφαρμογή τεχνολογιών blockchain στον κλάδο των ποτών. Επίσης, στόχος είναι να εξαχθούν χρήσιμα συμπεράσματα για το κατά πόσο και πώς οι τεχνολογίες blockchain εφαρμόζονται στην πράξη, σε ποιό στάδιο εφαρμογής είναι αυτές αλλά και ποιές είναι οι σύγχρονες τάσεις για την εφαρμογή τους στο πεδίο αυτό. Αρχικά, θα παρουσιαστεί ο τρόπος με τον οποίο διεξήχθη η έρευνα αυτή και έπειτα θα παρουσιαστούν τα αποτελέσματα της και τα συμπεράσματα που προκύπτουν από αυτή.

4.1 Διαδικασία έρευνας

Καταρχάς, πρέπει να επιλεγεί η βάση δεδομένων που θα χρησιμοποιηθεί στην έρευνα αυτή, η οποία είναι το Scopus. Το πρωτόκολλο έρευνας και τα κριτήρια επιλογής ή μη καθορίζονται έτσι ώστε να οδηγούν στο επιθυμητό αποτέλεσμα. Ο πίνακας που ακολουθεί επεξηγεί ολόκληρη την διαδικασία που διεξήχθη:

Research Protocol	**Title: Set of "Blockchain AND (wine OR beverages OR spirits OR alcohol OR drinks)"**
Βάση Δεδομένων	Scopus: Είναι μια παγκόσμια βάση δεδομένων, καλύπτει ένα ευρύ φάσμα ακαδημαϊκών δημοσιεύσεων περισσότερες από 20,000 εγκεκριμένων από ομότιμους συναδέλφους.
Είδη Δημοσιεύσεων	Μόνο εγκεκριμένα από ομότιμους συναδέλφους άρθρα.
Γλώσσα	Αγγλικά: Ευρύ φάσμα πληροφορίας.
Data range	Δεν τέθηκαν όρια μιας και οι δημοσιεύσεις ξεκινούν από το 2016.
Πεδίο Αναζήτησης	Οι όροι της αναζήτησης εφαρμόστηκαν μόνο στα Titles, abstracts και Keywords.
Όροι Αναζήτησης	TITLE-ABS-KEY (blockchain AND (wine OR beverages OR spirits OR alcohol OR drinks))
Επεξήγηση Όρου Αναζήτησης	Ο όρος αναζήτησης αποσκοπεί να βρεί αποτελέσματα χρήσης και ανάλυσης τεχνολογιών blockchain στον τομέα των ποτών και των αναψυκτικών. Επειδή τα αποτελέσματα που προκύπτουν δεν είναι μεγάλου όγκου, οι θεματικές ενότητες, ο τύπος του εγγράφου καθώς και το Source Type δεν περιορίζονται.

Deselection Criteria	Το κριτήριο μη επιλογής είναι σχετικό με το εκάστοτε αποτέλεσμα. Μερικά άρθρα είναι ξεκάθαρα μη σχετικά βάσει του τίτλου και της σύνοψης τους, ενώ κάποια άλλα περιέχουν τους όρους αναζήτησης στις λέξεις κλειδιά, αλλά δεν αναφέρονται σε αυτό το θέμα στην σύνοψη τους. Σε αρκετές περιπτώσεις, ακόμη, ο όρος spirits μεταφράζεται σε «στο πνεύμα του blockchain» και όχι σαν «οινοπνευματώδη ποτά», οπότε και το αντίστοιχο αποτέλεσμα απορρίπτεται. Όσον αφορά στα σχετικά άρθρα, ελέγχθηκε ολόκληρο το περιεχόμενο τους για την αναλυτική τους κατηγοριοποίηση.

Από τον όρο αναζήτησης προκύπτουν 52 αποτελέσματα, από τα οποία, βάση των κριτηρίων απόρριψης, είναι δεκτά τα 34. Ακολουθεί, η ανάλυση τους, ενώ η κατηγοριοποίηση τους φαίνεται σε παράρτημα.

4.2 Μεθοδολογία έρευνας

Η έρευνα που έχει διεξαχθεί χωρίζεται στα εξής κομμάτια: ανάλογα με το έτος που έχει δημοσιευθεί το άρθρο, ανάλογα με το είδος του άρθρου. ανάλογα με τον τομέα εφαρμογής και ανάλογα με τον τύπο του δικτύου της εφαρμογής.

4.2.1 Έτος δημοσίευσης

Ανάλογα με το έτος της δημοσίευσης, έχουμε τα εξής στοιχεία:

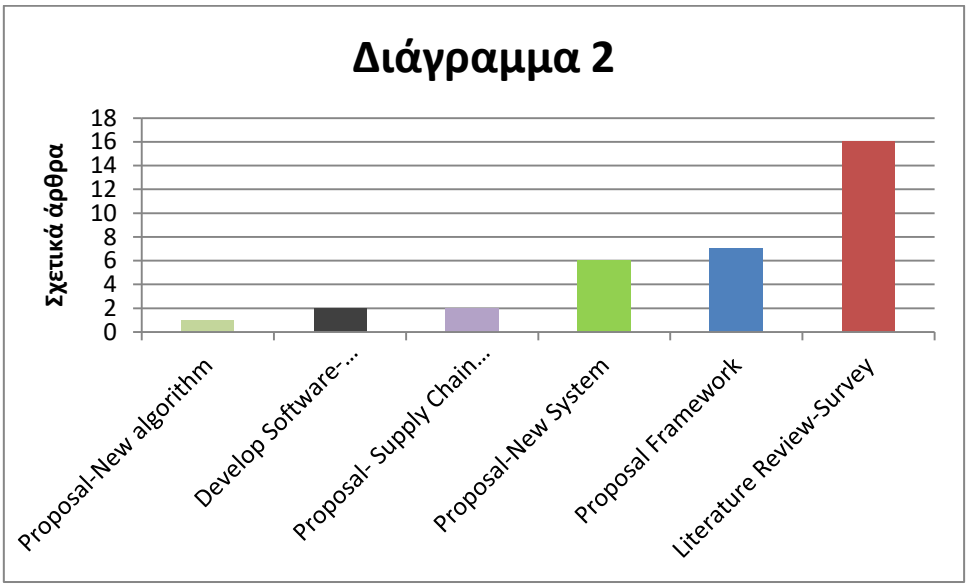
Έτος Δημοσίευσης	Σχετικά άρθρα
2017	1
2018	2
2019	9
2020	15
2021	7

Μπορεί να παρατηρηθεί, ότι τα άρθρα αυξάνονται ενώ περνούν τα έτη, το οποίο είναι λογικό μιας και η τεχνολογία του blockchain είναι αρκετά νέα και καινοτόμα (υπάρχει μόλις από το 2008 σαν εφαρμογή). Μπορεί να σημειωθεί, επίσης, ότι τα σχετικά άρθρα ξεκινούν από το 2017, το οποίο και πάλι προκύπτει εύκολα αν σκεφτεί κανείς ότι το blockchain και ειδικά οι πρακτικές εφαρμογές του σε πραγματικές επιχειρήσεις είναι αρκετά νέα. Ο ίδιος λόγος εξηγεί και τον σχετικά μικρό αριθμό άρθρων που προκύπτουν από την αναζήτηση αυτή.

4.2.2 Είδη άρθρων

Σχετικά με το είδος των άρθρων που προκύπτουν από την έρευνα αυτή, φτιάχνεται ο επόμενος πίνακας:

Είδος άρθρου	Σχετικά άρθρα
Develop Software-System	2
Proposal-New algorithm	1
Proposal- Supply Chain Support Method	2
Proposal-New System	6
Proposal Framework	7
Literature Review-Survey	16

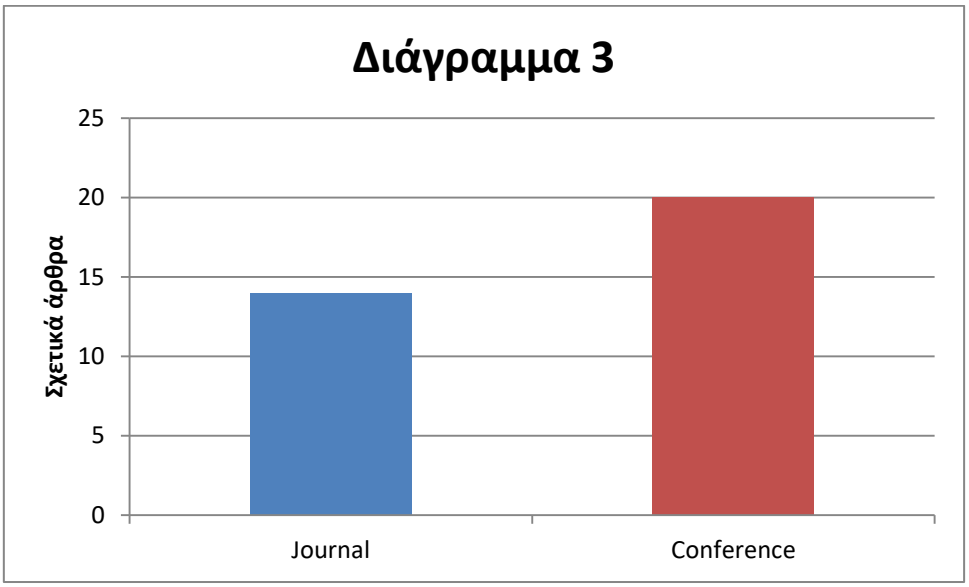


Παρατηρείται ότι συγκεντρωτικά τα άρθρα που αφορούν πρόταση για κάποια χρήση του blockchain στον τομέα των ποτών είναι ισάριθμα σε πλήθος με τα άρθρα ανασκόπησης του πεδίου και τέλος είναι τα ολοκληρωμένα δοκιμασμένα συστήματα-λογισμικά που έχουν αναπτυχθεί για χρήση στον τομέα αυτόν, τα οποία είναι και αρκετά λιγότερα.

4.2.3 Είδος Δημοσίευσης

Σχετικά με το είδος της δημοσίευσης στην οποία βρέθηκε το άρθρο, η κατηγοριοποίηση είναι ως εξής:

Είδος Δημοσίευσης	Σχετικά άρθρα
Journal	14
Conference	20

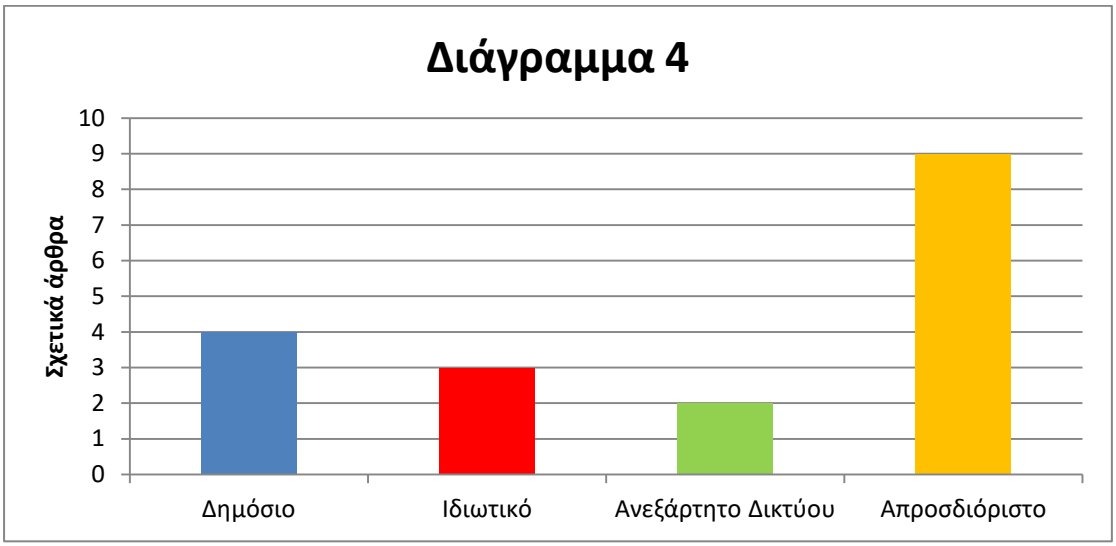


Είναι εύκολο να παρατηρηθεί ότι τα περισσότερα άρθρα έχουν δημοσιευθεί σε κάποιο συνέδριο, ενώ ακολουθούν σε αριθμό τα άρθρα σε journals.

4.2.4 Είδος Δικτύου blockchain εφαρμογής

Σχετικά με το αν το δίκτυο του blockchain που προτείνεται-εφαρμόζεται είναι δημόσιο ή ιδιωτικό, η κατηγοριοποίηση είναι ως εξής:

Τύπος Δικτύου Blockchain	Σχετικά άρθρα
Δημόσιο	4
Ιδιωτικό	3
Ανεξάρτητο Δικτύου	2
Απροσδιόριστο	9



Μπορεί να παρατηρηθεί ότι από τα 18 άρθρα που αφορούν προτάσεις για εφαρμογή ή αποτελούν ολοκληρωμένες εφαρμογές-λύσεις, τα περισσότερα δεν κάνουν λόγο για κάποιο συγκεκριμένο είδος δικτύου blockchain, ενώ ακολουθούν κατά σειρά τα δημόσια, τα ιδιωτικά αλλά και αυτά που θα μπορούσαν να εφαρμοστούν είτε σε δημόσιο είτε σε ιδιωτικό δίκτυο blockchain.

4.3 Ανάλυση άρθρων

Από την έρευνα που διεξήχθη και μετά τον ενδελεχή έλεγχο των άρθρων προκύπτουν αρκετά συμπεράσματα:

Η εφαρμογή του blockchain, όπως φαίνεται και από τα συμπεράσματα του κάθε άρθρου, φαίνεται να έχει αρκετά θετική επιρροή στην εφοδιαστική αλυσίδα της εκάστοτε εφαρμογής. Προσφέρει μεγάλο βαθμό ασφάλειας στις συναλλαγές, ενώ παράλληλα απλουστεύει σημαντικά την αλληλεπίδραση των συμμετέχοντων με αυτή και άρα ελαττώνει δραματικά τον χρόνο που απαιτείται για τον ακριβή εντοπισμό προϊόντων. Επίσης, η εφαρμογή του blockchain μπορεί να αποδείξει την αυθεντικότητα ενός προϊόντων καθώς και ολόκληρη την διαδρομή του κατά την παραγωγή και μεταφορά του προς τον τελικό του προορισμό, ένα χαρακτηριστικό που θεωρείται αρκετά σημαντικό στην βιομηχανία των ποτών και ειδικά του κρασιού, στο οποίο αναφέρονται και αρκετά άρθρα της ανασκόπησης αυτής. Η τιμή του κρασιού πολλές φορές καθορίζεται κυρίως από την προέλευση και την φήμη του παραγωγού, γι'αυτό είναι πολύ σημαντικό αυτή η πληροφορία να είναι διαθέσιμη στον τελικό καταναλωτή. Σε πολλά άρθρα, ακόμη, αναφέρεται και η εφαρμογή του blockchain για την καταπολέμηση της παραποίησης (counterfeiting) προϊόντων, ένα πρόβλημα το οποίο κοστίζει αρκετά στην εταιρεία παραγωγής και στον καταναλωτή.

Όσον αφορά στος έτος δημοσίευσης, παρατηρείται μια αύξηση των σχετικών άρθρων όσο περνούν τα έτη. Αυτό δείχνει ότι η τάση στη σημερινή βιομηχανία είναι η υϊοθέτηση των τεχνολογιών του blockchain λόγω των πολλών πλεονεκτημάτων που προσφέρει. Αυτό μπορεί να φανεί και από το κεφάλαιο της μελέτης περιπτώσεων, όπου ήδη πολλές εταιρείες φαίνεται ότι προτιμούν το blockchain για την εφοδιαστική τους αλυσίδα. Η μείωση του κόστους του τελικού προϊόντος, η ιχνηλασιμότητα αλλά και η ασφάλεια των συναλλαγών είναι κοινοί στόχοι για κάθε εταιρεία στην αγορά, και άρα και για τις εταιρείες παραγωγής και εμφιάλωσης ποτών. Μάλιστα, λόγω του αριθμού των entries ανα έτος, προβλέπεται ακόμα μεγαλύτερη αύξηση των εφαρμογών αυτών στα επόμενα έτη, γεγονός που επιβεβαιώνει τα θετικά αποτελέσματα της πρακτικής εφαρμογής του blockchain στην βιομηχανία.

Σχετικά με το είδος των άρθρων, μπορούν να εξαχθούν τα εξής συμπεράσματα. Καταρχάς, τα entries που αφορούν proposals, τα οποία είναι προτάσεις του ερευνητών για το πως θα μπορούσε να εφαρμοστεί blockchain σε κάποιες συγκεκριμένες περιπτώσεις είναι ισάριθμα με τα reviews τα οποία πρόκειται για ανασκοπήσεις-συνόψεις του ερευνητικού πεδίου, τα οποία δεν προτείνουν κάτι συγκεκριμένο για εφαρμογή στον τομέα των ποτών. Τέλος, είναι τα software, τα οποία είναι ολοκληρωμένες λύσεις εφαρμογής blockchain οι οποίες έχουν αναπτυχθεί και δοκιμαστεί σε εταιρείες της βιομηχανίας, τα οποία entries εδω είναι μόλις 2. Αυτό είναι και το λογικό μιας και οι ολοκληρωμένες λύσεις έχουν ένα σημαντικό κόστος ανάπτυξης, ενώ ακόμη πολλές εταιρείες δεν είναι πρόθυμες να μοιραστούν τεχνογνωσία σε αυτό το στάδιο της βιομηχανίας.

Σχετικά με το αν η πρόταση ή η εφαρμογή που αναλύεται αφορά δημόσιο ή ιδιωτικό δίκτυο, μπορούν να εξαχθούν τα εξής συμπεράσματα. Στα περισσότερα άρθρα δεν γίνεται λόγος για κάποιο συγκεκριμένο δίκτυο ή είδος δικτύου blockchain. Αυτό συμβαίνει είτε επειδή η πρόταση είναι σε πολύ αρχικό στάδιο και δεν έχουν προσδιοριστεί ακόμα όλες οι απαιτήσεις του συστήματος, είτε διότι η επιλογή του δικτύου δεν παίζει σημαντικό ρόλο για την συγκεκριμένη πρόταση (θα μπορούσαν να επιλεγούν πολλά δίκτυα ή οι ερευνητές θέλουν να τονίσουν κάποιο συγκεκριμένο χαρακτηριστικό της πρότασης τους χωρίς να θέλουν να μπουν σε λεπτομέρειες για κάποιο συγκεκριμένο δίκτυο). Μπορεί να παρατηρηθεί, επίσης, ότι ακολουθούν σε πλήθος τα δημόσια δίκτυα, ενώ τέλος είναι τα ιδιωτικά δίκτυα και οι προτάσεις στις οποίες αναφέρονται και δημόσια και ιδιωτικά δίκτυα blockchain ως πιθανές λύσεις (ανεξάρτητα δικτύου).

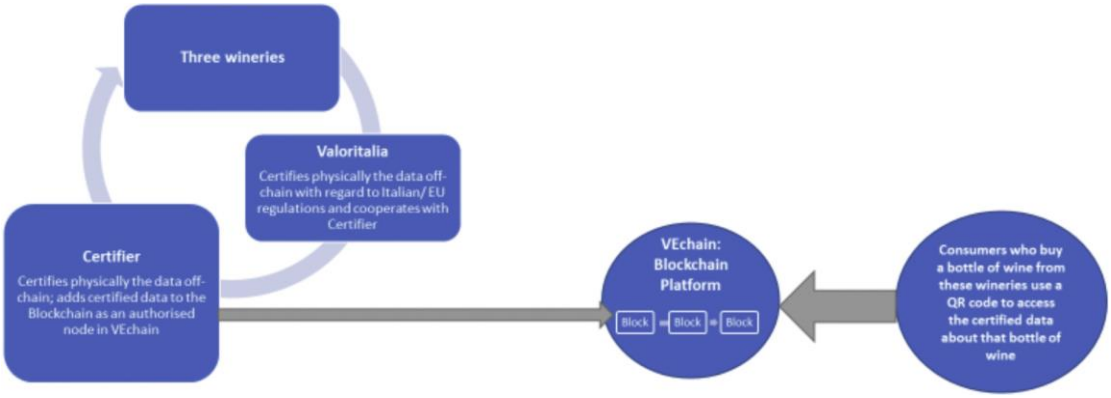
Τέλος, αξίζει να σημειωθεί ότι σύμφωνα με το ερευνητικό πεδίο, το blockchain είναι ο μοναδικός τρόπος ο οποίος έχει τόσο μεγάλο ερευνητικό ενδιαφέρον για εφαρμογή στο πεδίο της ιχνηλασιμότητας στην εφοδιαστική αλυσίδα. Μάλιστα, δεν φαίνεται από την

έρευνα αυτή να υπάρχει αναφορά σε άλλον τρόπο κρυπτογράφησης των συναλλαγών και διασφάλισης της αυθεντικότητας των προϊόντων ο οποίος να λαμβάνει σημαντικό ενδιαφέρον από την επιστημονική κοινότητα. Αυτό δείχνει ότι το blockchain έχει ακόμα πολλά βήματα εξέλιξης, και ταυτόχρονα ότι κατά πάσα πιθανότητα θα υϊοθετηθεί από πολλές εταιρείες στο μέλλον.

Ιδιαίτερο ενδιαφέρον έχει η περίπτωση των άρθρων 3 και 10 από την έρευνα αυτή (Danese P., Mocellin R., Romano P., 2021 και Helliar C.V., Crawford L., Rocca L., Teodori C., Veneziani M., 2020 αντίστοιχα).

Στην πρώτη περίπτωση οι ερευνητές πραγματοποίησαν μια ανάλυση από 5 case studies ιταλικών εταιρειών παραγωγής και εμφιάλωσης κρασιού (τις οποίες ονομάζουν A, B, C, D, E αντίστοιχα). Μελέτησαν για κάθε περίπτωση αρκετές παραμέτρους όπως τον τρόπο με τον οποίο τα δεδομένα εισάγονται στο δίκτυο του blockchain, με ποιόν τρόπο γίνεται η αυθεντικοποίηση του μπουκαλιού από τον καταναλωτή και τον τρόπο με τον οποίο εξασφαλίζεται ότι το τελικό προϊόν δεν είναι πλαστό. Βρήκαν, λοιπόν, ότι το data entry σε όλες τις περιπτώσεις γίνεται χειροκίνητα, και στις περιπτώσεις A και E η συχνότητα της εισαγωγής δεδομένων είναι αρκετά μικρή (συνήθως εβδομάδες ή και μήνες) ενώ στις υπόλοιπες περιπτώσεις είναι λιγότερο από 24 ώρες. Αν σκεφτεί κανείς ότι όσο πιο συχνό είναι το data entry, τόσο μικρότερες πιθανότητες υπάρχουν για την παραποίηση των προϊόντων (μιας και το data entry διορθώνει τυχόν λάθη που υπάρχουν και ανανεώνει ολόκληρο το σύστημα κωδικών της εταιρείας), τότε προκύπτει το συμπέρασμα ότι σε αρκετές περιπτώσεις, παρόλο που χρησιμοποιείται blockchain, θα μπορούσαν να παραποιηθούν τα προϊόντα χωρίς η εταιρεία να το καταλάβει. Αξίζει να σημειωθεί ακόμη, ότι σε όλες τις περιπτώσεις, οι πληροφορίες σχετικά με την αυθεντικότητα των προϊόντων που μπορεί να δει ο πελάτης αποθηκεύονται σε εξωτερικούς σέρβερ και η πρόσβαση γίνεται μέσω ιστοσελίδων, οπότε ο ίδιος δεν έχει απευθείας σύνδεση με το δίκτυο του blockchain, αλλά με τα hashes των πληροφοριών του δικτύου. Αυτό οδηγεί στο συμπέρασμα ότι λόγω των κεντρικών σέρβερ στους οποίους αποθηκεύεται η πληροφορία του blockchain, το σύστημα δεν είναι τελείως αποκεντρωμένο και άρα υπάρχει κάποιος κίνδυνος ασφαλείας σε πιθανή περίπτωση επίθεσης στους σέρβερ. Όσον αφορά στην πιθανότητα παραποίησης των προϊόντων, οι ερευνητές βρήκαν ότι οι εταιρείες A, E και D παράγουν κρασιά σχετικά χαμηλών τιμών, και άρα δεν διατρέχουν σοβαρό κίνδυνο παραποίησης των προϊόντων τους, σε αντίθεση με τις εταιρείες B και C, οι οποίες λόγω των ειδικών τεχνικών παραγωγής και εμφιάλωσης του κρασιού παράλληλα με τους ισχυρούς κανόνες τυποποίησης που πρέπει να τηρούν για αυτές, πουλούν το κρασί τους σε αρκετά ψηλές τιμές και άρα διατρέχουν περισσότερο κίνδυνο παραποίησης των προϊόντων τους (high level of counterfeiting chances). Αξίζει, ακόμα, να σημειωθεί ότι και οι 5 εταιρείες χρησιμοποιούν RFID tags και QR codes για την ταυτοποίηση των προϊόντων τους, τεχνολογίες οι οποίες φαίνεται και από την βιβλιογραφία ότι χρησιμοποιούνται σε τέτοιες περιπτώσεις.

Στην δεύτερη περίπτωση οι ερευνητές ανέλυσαν το permissioned δίκτυο blockchain που αναπτύχθηκε στην Ιταλική αγορά κρασιού το 2019, ονόματι MyStory[tm]. Χάρη σε αυτό, μπορεί ο καταναλωτής να ελέγχει την αυθεντικότητα του κρασιού που αγοράζει μέσω σκαναρίσματος ενός QR code. Σε αυτό το consortium blockchain συμμετέχουν 3 εταιρείες παραγωγής κρασιού-οινοποιεία, 4 οργανισμοί ανάπτυξης, πιστοποίησης και επαλήθευσης της προέλευσης του κρασιού (Certifier, Valoritalia, Federdoc και μία εταιρεία Big4) καθώς και ο ιδρυτής του blockchain VEChain (το οποίο blockchain βασίζεται σε Proof-of-Authority). Σε αυτή την περίπτωση, τα οινοποιεία πουλούν υψηλής ποιότητας κρασιά και άρα είναι σημαντικό να μπορούν να αποδείξουν στον πελάτη ότι το κρασί του είναι αυθεντικό και άρα να προφυλάξουν και αυτόν αλλά και τον εαυτό τους από διάφορα παραποιημένα (counterfeit) προϊόντα. Οι ερευνητές πραγματοποίησαν συνεντεύξεις με τις εταιρείες αυτές καθώς και 2 ακόμα οινοποιεία τα οποία δεν συμμετέχουν σε αυτό το blockchain ακόμα, αλλά ενδιαφέρονται να συμμετάσχουν.



Εικόνα 32: Το δίκτυο Blockchain του MyStorytm

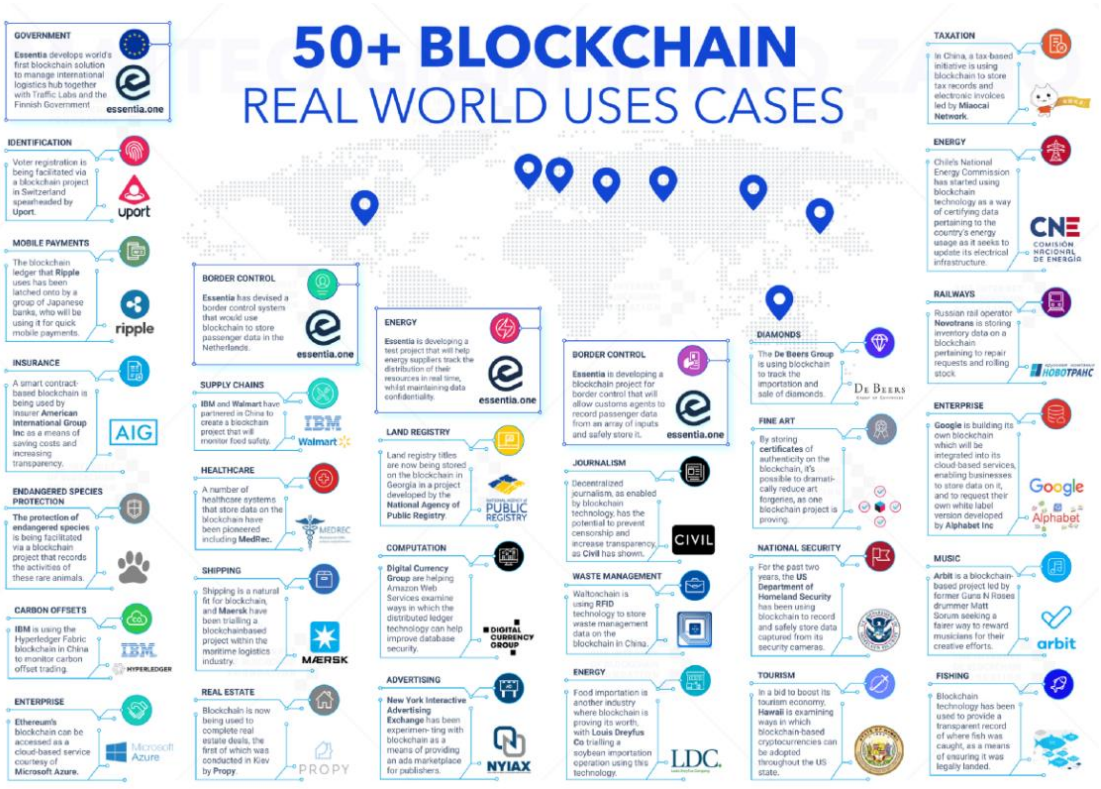
Πηγή: Helliar et al. (2020)

Το δίκτυο αυτό αναπτύχθηκε, σύμφωνα με τους ερευνητές, σε λίγους μήνες, ενώ πριν μετακινηθεί σε δημόσιο permissioned, το δίκτυο λειτούργησε ως ιδιωτικό permissioned για περισσότερα τεστ. Από αυτή την έρευνα και τις συνεντεύξεις, οι ερευνητές κατέληξαν σε αρκετά χρήσιμα συμπεράσματα. Καταρχάς, οι διαδικασίες που συμβαίνουν εκτός αλυσίδας blockchain, όπως για παράδειγμα το φύτεμα των σταφυλιών και η ωρίμανση τους είναι ένας παράγοντας που μπορεί να οδηγήσει σε μικρό ποσοστό χρήσης της τεχνολογίας του blockchain στον τομέα αυτόν. Το γεγονός ότι οι διαδικασίες αυτές δεν μπορούν να αυθεντικοποιηθούν και να παρουσιαστούν με απόλυτη διαφάνεια στο δίκτυο του blockchain σημαίνει ότι ο καταναλωτής δεν μπορεί να είναι απολύτως σίγουρος ότι αυτές οι διαδικασίες έχουν πραγματοποιηθεί όπως υποστηρίζουν τα οινοποιεία. Επίσης, οι ερευνητές υπογραμμίζουν ότι οι διάφοροι αλγόριθμοι συναίνεσης που δύνανται να χρησιμοποιηθούν μπορεί να διαφέρουν από τους κλασσικούς PoW και PoS, μιας και αν συγκεκριμένες εταιρείες και οινοποιεία συμμετέχουν σε ένα δίκτυο blockchain για αρκετό καιρό και παρουσιάζουν μεγάλα ποσοστά εμπιστοσύνης από τους καταναλωτές και τις υπόλοιπες εταιρείες, τότε δεν υπάρχει ανάγκη χρήσης χρονοβόρων και ακριβών μεθόδων

συναίνεσης όπως το PoW, αλλά μπορεί για παράδειγμα να χρησιμοποιηθεί το προαναφερθέν Proof-of-Authority. Σημειώνεται, επιπροσθέτως, ότι στο μέλλον μπορεί να προκύψουν αρκετές αλλαγές στο πως λειτουργούν τα δίκτυα blockchain αλλά και η βιομηχανία του κρασιού λόγω συγκεκριμένων νομοθεσιών που ενδεχομένως να αλλάξουν τα επόμενα χρόνια. Τέλος, οι ερευνητές υποστηρίζουν ότι για να γενικευθούν τα συμπεράσματα της έρευνας τους, απαιτείται η ανάλυση κάποιων ακόμα case studies που τυχόν υπάρχουν, ώστε να μπορούν να ληφθούν περισσότερα δεδομένα.

5. Case Studies

Το παρόν κεφάλαιο θα αναλύσει συγκεκριμένες εφαρμογές blockchain που έχουν χρησιμοποιήσει εταιρείες, και έχει ως σκοπό να δείξει ότι το blockchain και το Distributed Ledger Technology αποτελούν λύση οι οποία μπορεί να διορθώσει αρκετά από τα προβλήματα που εμφανίζονται στην καθημερινή λειτουργία εταιρειών σε κάθε τομέα.



Εικόνα 33: Παραδείγματα εφαρμογών του Blockchain

Πηγή: www.medium.com

Οι μελέτες περίπτωσης που έχουν αναλυθεί μπορούν να φανούν συνοπτικά στον παρακάτω πίνακα:

A/A Μελέτη Περίπτωσης	Case Study	Δημόσιο/Ιδιωτικό Blockchain
1	NTT Data-Skuchain	Ιδιωτικό
2	Bosch-IOTA	Ιδιωτικό
3	Renault-IBM	Ιδιωτικό
4	Accenture	Δημόσιο
5	CargoX	Δημόσιο

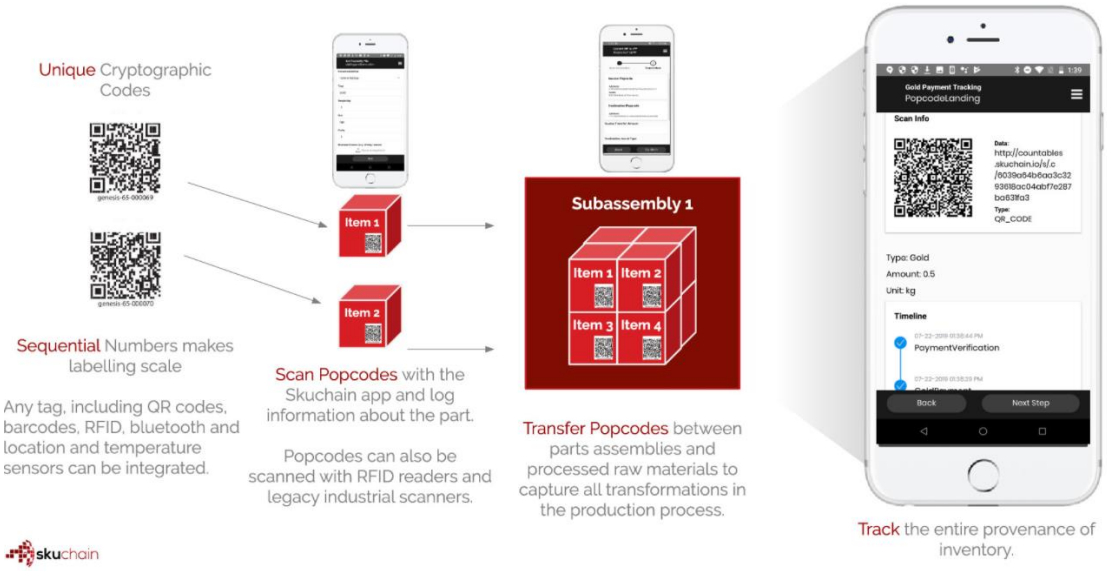
5.1 NTT Data-Skuchain

Προφίλ εταιρείας

Η NTT Data είναι μια ιαπωνική πολυεθνική εταιρεία παροχής υπηρεσιών και προϊόντων IT, θυγατρική της Nippon Telegraph and Telephone. Ιδρύθηκε το 1967, έχει την έδρα της στο Τόκιο, ενώ σήμερα αποτελεί την μεγαλύτερη IT εταιρεία με έδρα στην Ιαπωνία και την 5η μεγαλύτερη τέτοια εταιρεία παγκοσμίως. Οι τομείς δραστηριοποίησης της είναι κυρίως οικονομικοί και οι τομείς επικοινωνίας. Οι υπάλληλοι της, σύμφωνα με στατιστικά του 2019, είναι 133,000.

Τομέας εφαρμογής

Ο τομέας του IT αναμφίβολα μπορεί να επωφεληθεί από την εφαρμογή των τεχνολογιών του blockchain. Αποτελεί έναν από τους ταχύτερα αναπτυσσόμενους τομείς, ενώ πια έχει εφαρμογή σχεδόν σε όλες τις εταιρείς παγκοσμίως. Το blockchain μπορεί να βοηθήσει στην ιχνηλασιμότητα των προϊόντων, αλλά και στην ασφάλεια και στην ιδιωτικότητα των δικτύων, βάσεων δεδομένων και συναλλαγών. Συνεπώς, οι τεράστιες και πολύπλοκες εφοδιαστικές αλυσίδες εταιρειών όπως η NTT μπορούν όχι μόνο να απλοποιηθούν σε μεγάλο βαθμό, αλλά και να διασφαλιστεί ότι τα δεδομένα που κυκλοφορούν σε αυτές είναι ασφαλή και ιδιωτικά, αλλά και ότι μπορούν να είναι διαθέσιμα σε οποιδήποτε μέρος της εφοδιαστικής αλυσίδας γρήγορα και εύκολα, χωρίς τις καθυστερήσεις και την γραφειοκρατία που απαιτούν αρκετά συστήματα του σήμερα, ειδικά όταν πρόκειται για πληροφορίες που πρέπει να περάσουν μεταξύ εταιρειών διαφορετικών χωρών.

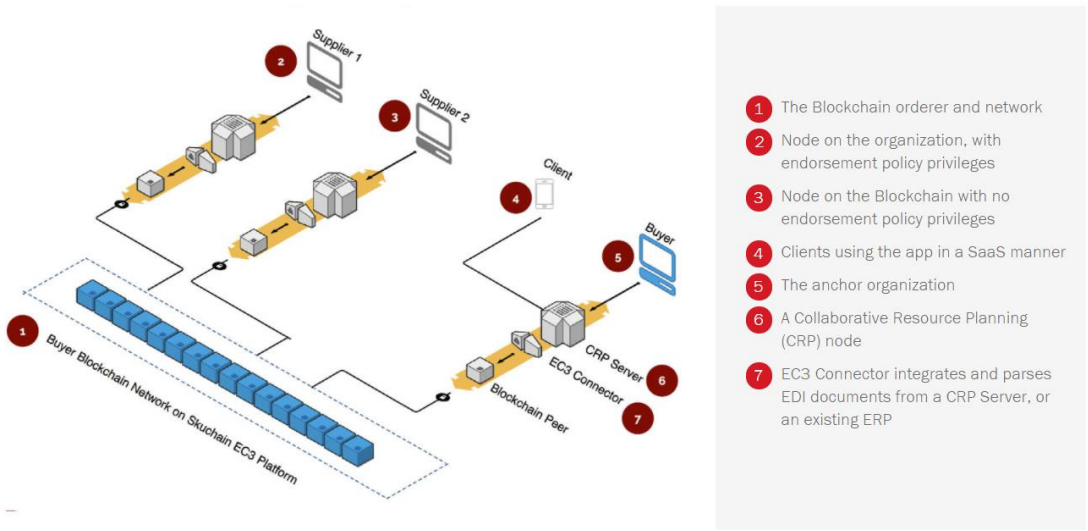


Εικόνα 34: Η εφαρμογή popcodes της Skuchain

Πηγή: www.skuchain.com/inventory-tracker/

Εφαρμογή του blockchain

Το Skuchain είναι μια υπηρεσία cloud η οποία επιτρέπει την διαχείριση προμηθειών και την ανίχνευση και εντοπισμό αποθεμάτων μιας εταιρείας. Σύμφωνα με την εταιρεία, αυτό επιτρέπει την ύπαρξη μιας ρευστής αλυσίδας εφοδιασμού (Liquid Supply chain), στην οποία οι πληρωμές, οι εντοπισμοί προϊόντων και τα διάφορα queries συμβαίνουν σε πραγματικό χρόνο επιτρέποντας έτσι την μείωση του επιχειρηματικού κινδύνου και την βελτιστοποίηση της εφοδιαστικής αυτής αλυσίδας. Η υπηρεσία αυτή χρησιμοποιεί blockchain για τον ασφαλή και ακριβή έλεγχο των προϊόντων αυτών και άρα επιτρέπει τον εντοπισμό ενός αγαθού από την φάση της πρώτης ύλης μέχρι και το τελικό προϊόν. Η εταιρεία έχει αναπτύξει δικιές της εφαρμογές smart contracts (ονόματι Popcodes και Brackets) οι οποίες ενσωματώνονται μέσα στην αλυσίδα του blockchain για να επιτρέψουν τον συντονισμό της κίνησης των αποθεμάτων και των συναλλαγών μέσα στην εφοδιαστική αλυσίδα, το οποίο επιτρέπει την ύπαρξη συσσωρευμένου και άρα άχρηστου αποθέματος, βελτιώνοντας έτσι το κέρδος της επιχείρησης. Η εταιρεία Skuchain έχει ήδη χρησιμοποιήσει την τεχνολογία αυτή με την πλατφόρμα EC3 για να βελτιώσει την εφοδιαστική αλυσίδα της Ιαπωνικής IT εταιρείας NTT, η οποία έχει αναπτύξει την πλατφόρμα iQuattro για την ενσωμάτωση διάφορων τεχνολογιών. Η λύση που εφαρμόστηκε περιείχε χρήση τεχνολογιών RFID, IoT και blockchain για την αποδοτικότερη και ευκολότερη επικοινωνία των διαφόρων κομματιών κατά το μήκος όλης της εφοδιαστικής αλυσίδας της εταιρείας. Τα αποτελέσματα ήταν η υψηλότερη αποδοτικότητα, η ελάχιστη σπατάλη πόρων και ο καλύτερος έλεγχος των προϊόντων της NTT, αφού μέσω της εφαρμογής Popcodes και του RFID, τα προϊόντα δεν σκανάρονται ένα-ένα αλλά αυτόματα μέσω κινητών τηλεφώνων, ενώ η εφαρμογή Brackets για smart contracts εξασφαλίζει την συνεχή ροή των δεδομένων και επιτρέπει τον αυτόματο έλεγχο από απόσταση.



Εικόνα 35: Η πλατφόρμα EC3 της Skuchain

Πηγή: www.skuchain.com/ec3/

5.2 Bosch-IOTA

Προφίλ εταιρείας

Η Bosch είναι γερμανική πολυεθνικη εταιρεία με έδρα στο Gerlingen. Ιδρύθηκε το 1886 στην Στουτγάρδη από τον γερμανό μηχανικό Robert Bosch, απασχολεί περίπου 400,000 υπαλλήλους παγκοσμίως ενώ τα καθαρά κέρδη της εταιρείας ανέρχονται στο 1 δισεκατομμύριο ευρώ για το έτος 2020. Οι κύριοι τομείς δραστηριοποίησης της είναι ο τεχνολογικός και ο μηχανολογικός γενικότερα, με προϊόντα μετάδοσης κίνησης, οικιακές συσκευές, ηλεκτρικά εργαλεία και ενεργειακά προϊόντα.

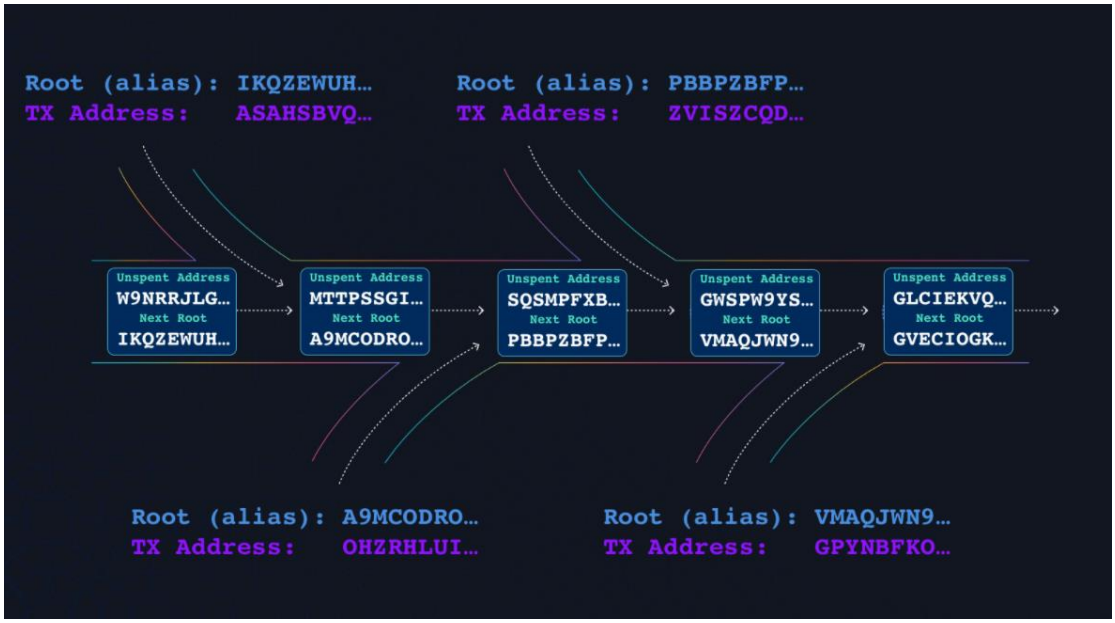
Εικόνα 36: Η πλατφόρμα XDK της Bosch

Πηγή: www.bosch-connectivity.com/products/cross-domain/cross-domain-developement-kit/

Τομέας εφαρμογής

Ο τομέας της παραγωγής και της εφοδιαστικής αλυσίδας γενικότερα μπορεί να επωφεληθεί από την εφαρμογή του blockchain. Οι μεγάλες εταιρείες όπως η Bosch απασχολούν εκατοντάδες χιλιάδες υπαλλήλους σε διάφορες χώρες του κόσμου, οι οποίοι είναι απαραίτητο να ανταλλάσσουν συνεχώς δεδομένα για την εύρυθμη λειτουργία της εφαδιαστικής αλυσίδας. Παράλληλα, εταιρείες όπως η Bosch δραστηριοποιούνται και στον

τομέα του Internet of Things, όπου οι συσκευές, αισθητήρες και μηχανήματα της παραγωγής συνδέονται σε πραγματικό χρόνο για να βελτιστοποιηθεί η παραγωγή και να ελαχιστοποιηθεί το κόστος και ο χρόνος παραγωγής. Η εταιρεία έχει αναπτύξει δικιά της τέτοια πλατφόρμα ονόματι XDK (Cross Domain Development Kit), δηλαδή μια πλατφόρμα προγραμματιζόμενων συσκευών και προτυποποίησης IoT για οποιαδήποτε χρήση. Χρησιμοποιεί αισθητήρες MEMS (micro electromechanical systems), WiFi, Bluetooth, κάρτες SD και έτοιμα πακέτα λογισμικών για την υλοποίηση της πλατφόρμας αυτής.



Εικόνα 37: Σχηματική Απεικόνιση των MAM

Πηγή: www.blog.iota.org

Εφαρμογή του blockchain

Η εφαρμογή του blockchain στο XDK ήρθε με την βοήθεια της πλατφόρμας IOTA. Το IOTA είναι μια open source πλατφόρμα DLT (Distributed Ledger Technology) η οποία έχει σχεδιαστεί για το Internet of Things. Παρέχει μεγαλύτερη επεκτασιμότητα από τις παραδοσιακές πλατφόρμες όπως Bitcoin και Ethereum, μιας και η επικύρωση των συναλλαγών στο δίκτυο δεν συμβαίνει μέσω Proof of Work ή Proof of Stake, αλλά μέσω κατευθυνόμενων άκυκλων γράφων (Directed Acyclic Graphs ή DAGs). Αυτό πρακτικά σημαίνει ότι αντί να υπάρχουν miners στο δίκτυο, η δημιουργία μιας συναλλαγής στο δίκτυο συμβαίνει από κόμβους οι οποίοι προηγουμένως θα πρέπει να έχουν επικυρώσει 2 άλλες συναλλαγές. Συνεπώς, στο IOTA δεν υπάρχουν transaction fees, και άρα τα micro transactions, τα οποία υπάρχουν σε πληθώρα στο IoT, καθίστανται ευκολότερα και

γρηγορότερα. Επίσης, χάρη στην τεχνολογία επικύρωσης, η ασφάλεια και η ταχύτητα του δικτύου αυξάνονται όσο αυξάνονται οι συμμετέχοντες κόμβοι του δικτύου, σε αντίθεση με το Bitcoin και το Ethereum. Στο IOTA, τα δεδομένα που συλλέγονται από το XDK μπορούν να διαμοιραστούν μέσω του Data Marketplace από τις διασυνδεδεμένες συσκευές. Χάρη στην τεχνολογία του DLT, τα δεδομένα αυτά είναι ασφαλή και κρυπτογραφημένα, και ονομάζονται Masked Authenticated Messaging (MAM). Σύμφωνα με την Bosch, η λύση αυτή, πέρα από την τωρινή υλοποίηση της, μπορεί να χρησιμοποιηθεί και σε περιπτώσεις όπου η εταιρεία θέλει να χρεώσει σε κρυπτονόμισμα IOTA έναν πελάτη που έχει δανειστεί μηχανήματα της, ανάλογα με την ώρα χρήσης τους η οποία θα μετράτει από τις συσκευές IoT. Επιπροσθέτως, η βαθμονόμηση και η συντήρηση των μηχανών μπορεί να καταστεί ευκολότερη μιας και δύναται να υπάρχουν συσκευές και αισθητήρες οι οποίοι να μετρούν διάφορες παραμέτρους των μηχανών, ενώ σε περίπτωση βλάβης οι αισθητήρερς αυτοί ειδοποιούν άμεσα την εταιρεία και άρα επιδιορθώνονται σε ελάχιστο χρόνο.

5.3 Renault-IBM

Προφίλ εταιρείας

Η Renault (γνωστή και ως Renault Group) είναι γαλλική πολυεθνική εταιρεία παραγωγής οχημάτων. Σχηματίστηκε το 1899 από τα αδέρφια Louis, Marcel και Fernand Renault, έχει έδρα στο Boulogne Billancourt κοντά στο Παρίσι, και απασχολεί περίπου 180,000 υπαλλήλους, ενώ το 2019 πούλησε περίπου 3,800,000 οχήματα παγκοσμίως, με συνολικό καθαρό κέρδος τα 2 δικεσατομμύρια ευρώ. Στατιστικά του 2016 δείχνουν ότι ήταν η 9^{η} μεγαλύτερη εταιρεία παραγωγής οχημάτων στον κόσμο, ενώ το 2017 η στρατηγική συνεργασία μεταξύ Renault-Nissan-Mitsubishi έφτασε την 1^{η} θέση πωλήσεων ελαφριών οχημάτων παγκοσμίως. Κατέχει, ακόμη, και αρκετά τμήματα για ειδικές εφαρμογές, όπως η πιο σπορ μάρκα Alpine η οποία αγωνίζεται και στην Formula 1, ενώ της ανήκει επίσης και η μεγαλύτερη ρουμανική εταιρεία αυτοκινήτων Dacia.

Εικόνα 38: Γραμμή παραγωγής Renault

Πηγή: www.wardsauto.com

Τομέας εφαρμογής

Ο τομέας παραγωγής αυτοκινήτων είναι ένας από τους μεγαλύτερους και άρα πολυπλοκότερους τομείς παγκοσμίως. Αξίζει να σημειωθεί ότι κατά μέσο όρο, κάθε αυτοκίνητο αποτελείται από περίπου 30,000 εξαρτήματα και κομμάτια,σύμφωνα με στατιστικά της Toyota. Τα εξαρτήματα αυτά αλλά και οι πρώτες ύλες που τα αποτελούν προέρχονται από πολλές διαφορετικές χώρες, καθιστώντας έτσι την εφοδιαστική αλυσίδα περίπλοκη. Επιπροσθέτως, τα σύγχρονα αυτοκίνητα έχουν επίσης μεγάλο βαθμό πολυπλοκότητας, αφού τις περισσότερες φορές είναι υβριδικά ή ηλεκτρικά. Έτσι, το blockchain μπορεί να βοηθήσει σε 2 πτυχές: καταρχάς στην ιχνηλασιμότητα και την επικύρωση της αυθεντικότητας των διαφόρων εξαρτημάτων των οχημάτων αλλά και στην διαλειτουργικότητα και την επικοινωνία των διαφόρων μηχανών παραγωγής αλλά και μεταξύ των ίδιων των αυτοκινήτων, για την αύξηση της οδικής ασφάλειας. Έτσι, ο ιδιοκτήτης ενός οχήματος μπορεί να είναι σίγουρος ότι τα ανταλλακτικά που χρησιμοποιεί είναι γνήσια και να κρατάει ένα αρχείο με αυτά σε περίπτωση που θέλει να το πουλήσει. Ακόμη, η βιομηχανία κινείται προς ολοένα και πιο αυτοματοποιημένα εργοστάσια παραγωγής στα οποία η επικοινωνία μεταξύ των μηχανών κρίνεται απαραίτητη τόσο για την αναγνώριση και επιδιόρθωση βλαβών όσο και για την βελτίωση της απόδοσης και της παραγωγής. Έτσι, το blockchain μπορεί να βοηθήσει και στην αυτοματοποίηση των εργοστασίων και την επικοινωνία μεταξύ όλων των μερών της εφοδιαστικής αλυσίδας.

Εφαρμογή του blockchain

Η Renault, λοιπόν, ανέπτυξε την blockchain πλατφόρμα XCEED (eXtended Compliance End-to-End Distributed) για την επικύρωση της αυθεντικότητας των εξαρτημάτων οχημάτων της. Πολλές φορές, νομικοί περιορισμοί στην αυτοκινητοβιομηχανία θα πρέπει να ισχύουν και για οχήματα τα οποία έχουν ήδη πουληθεί. Έτσι, η πλατφόρμα XCEED καταγράφει σε δίκτυο blockchain όλα τα εξαρτήματα των οχημάτων της αλλά και την διαδρομή τους μέσα στην εφοδιαστική της αλυσίδα, ώστε να μπορεί να αποδείξει ότι τα οχήματα της τηρούν τις νομικές προϋποθέσεις που ισχύουν σε κάθε χώρα. Η πλατφόρμα XCEED βασίζεται στο δίκτυο του Hyperledger Fabric, ένα τύπου permissioned blockchain σχεδιασμένο από την IBM και την Digital Asset. Πρόκειται, λοιπόν, για ένα δίκτυο εμπιστοσύνης μεταξύ των κατασκευαστών των εξαρτημάτων και των κατασκευαστών των αυτοκινήτων. Από τη φύση του, το blockchain διασφαλίζει ότι κάθε συμμετέχουσα εταιρεία μπορεί με ασφάλεια και ιδιωτικότητα να μοιράζεται δεδομένα από την παραγωγή της και τις αποστολές και παραλαβές της, χωρίς να υπάρχει κίνδυνος υποκλοπής ή αλλοίωσης των δεδομένων αυτών. Η πλατφόρμα χρησιμοποιήθηκε για πρώτη φορά το 2019 στο εργοστάσιο της Renault στο Douai, ενώ σύμφωνα με στοιχεία της Renault μπορεί να φτάσει μέχρι και την αποθήκευση 1 εκατομμυρίων αρχείων και 500 συναλλαγές το δευτερόλεπτο. Αυτό σημαίνει ότι καλύπτει όλα τα διάφορα micro transactions που απαιτείται για τις IoT συσκευές στο δίκτυο παραγωγής της και κάνει δυνατή την περαιτέρω βελτιστοποίηση της εφοδιαστικής

αλυσίδας της. Η πλατφόρμα αυτή σχεδιάζεται να χρησιμοποιηθεί στο μέλλον, με ορισμένες τροποποιήσεις, και για την επικοινωνία μεταξύ των αυτοκινήτων Renault, ώστε να μπορούν να ανταλλάσσουν οδικά δεδομένα αυξάνοντας έτσι την ασφάλεια στο δρόμο. Ενδιαφέρον, επίσης, παρουσιάζει και ένα πείραμα της Renault σε συνεργασία με την Microsoft και την Viseo, στο οποίο περιγράφεται μια διαδικασία ηλεκτρονικής αποθήκευσης ενός ακριβούς αντιτύπου όλων των συστημάτων των αυτοκινήτων της Renault (digital twins). Αυτό θα επιτρέπει, για παράδειγμα, την ακριβή ψηφιοποίηση συγκεκριμένων αυτοκινήτων και καταγραφή τους στο σύστημα της Renault, ώστε να μπορεί άμεσα η εταιρεία να προσπελάσει τις πληροφορίες του αυτοκινήτου σε περίπτωση βλάβης. Επιπροσθέτως, σε αυτό το digital twin θα μπορεί να καταγράφεται και το ιστορικό της συντήρησης του αυτοκινήτου ακόμη και σε περίπτωση αλλαγής του ιδιοκτήτη, ώστε να υπάρχει διαφάνεια και άρα ελάχιστες πιθανότητες εξαπάτησης. Στο πείραμα αυτό αναπτύχθηκε ένα συγκεκριμένο εργαλείο το οποίο συνδέεται με την OBD θύρα του οχήματος, και καταγράφει όλες τις πληροφορίες όπως τα χιλιόμετρα και η κατάσταση των διαφόρων εξαρτημάτων με την βοήθεια των αισθητήρων του οχήματος. Αυτά τα δεδομένα μπορεί, για παράδειγμα, να μεταφέρονται μέσα στο περιβάλλον του blockchain από την εταιρεία στα διάφορα συνεργεία, ώστε να μπορεί να εξακριβωθεί ακριβώς η κατάσταση που βρίσκεται το όχημα. Αξίζει να αναφερθεί, ακόμη, ότι ένα παρόμοιο πείραμα έχει σχεδιαστεί και από την Bosch και την γερμανική εταιρεία πιστοποιήσεων TUV Rheinand για την ανάπτυξη digital twin οχημάτων, αφού τα στατιστικά δείχνουν ότι μόνο στην Γερμανία, η παράνομη αλλαγή των χιλιομέτρων σε αυτοκίνητα φτάνει σε αξία 3,700 ευρώ ανα όχημα, ενώ ένα κάθε τρία αυτοκίνητα έχει δεχθεί τέτοια παράνομη αλλαγή στο οδόμετρο για την αύξηση της αξίας του.

Εικόνα 39: Γραφική απεικόνιση digital twin ενός κινητήρα

Πηγή: Dassault Systemes

5.4 Accenture

Προφίλ εταιρείας

Η Accenture πρόκειται για μια πολυεθνική συμβουλευτική εταιρεία (consulting) με έδρα στο Δουβλίνο της Ιρλανδίας η οποία δημιουργήθηκε το 1989 . Ανήκει στην λίστα με τις Fortune 500 εταιρείες στον κόσμο, με συνολικά έσοδα 44 δισεκατομμύρια ευρώ για το 2020, ενώ οι υπάλληλοι της ανέρχονται στους 537,000. Αξίζει να σημειωθεί ότι 91 από τις 100 Fortune 100 εταιρείες είναι πελάτες της Accenture.

BILL OF LADING

Page 1 of _____

Date:

SHIP FROM
Name:
Address:
City/State/Zip:
SID#:
FOB: ☐

SHIP TO
Name:
Location #: _____
Address:
City/State/Zip:
CID#:
FOB: ☐

THIRD PARTY FREIGHT CHARGES BILL TO:
Name:
Address:
City/State/Zip:

SPECIAL INSTRUCTIONS:

Bill of Lading Number: _____
BAR CODE SPACE

CARRIER NAME: _____
Trailer number:
Seal number(s):

SCAC:
Pro number:
BAR CODE SPACE

Freight Charge Terms: *(freight charges are prepaid unless marked otherwise)*
Prepaid _____ Collect _____ 3rd Party _____
☐ (check box) Master Bill of Lading: with attached underlying Bills of Lading

CUSTOMER ORDER INFORMATION

CUSTOMER ORDER NUMBER	# PKGS	WEIGHT	PALLET/SLIP (CIRCLE ONE)		ADDITIONAL SHIPPER INFO
			Y	N	
			Y	N	
			Y	N	
			Y	N	
			Y	N	
			Y	N	
			Y	N	
			Y	N	
GRAND TOTAL					

CARRIER INFORMATION

HANDLING UNIT QTY	HANDLING UNIT TYPE	PACKAGE QTY	PACKAGE TYPE	WEIGHT	H.M. (X)	COMMODITY DESCRIPTION	LTL ONLY NMFC #	LTL ONLY CLASS
						GRAND TOTAL		

RECEIVING STAMP SPACE

Where the rate is dependent on value, shippers are required to state specifically in writing the agreed or declared value of the property as follows:
"The agreed or declared value of the property is specifically stated by the shipper to be not exceeding _____ per _____."

COD Amount: $ _____
Fee Terms: Collect: ☐ Prepaid: ☐
Customer check acceptable: ☐

NOTE: Liability Limitation for loss or damage in this shipment may be applicable. See 49 U.S.C. • 14706(c)(1)(A) and (B).

RECEIVED, subject to individually determined rates or contracts that have been agreed upon in writing between the carrier and shipper, if applicable, otherwise to the rates, classifications and rules that have been established by the carrier and are available to the shipper, on request, and to all applicable state and federal regulations.

The carrier shall not make delivery of this shipment without payment of freight and all other lawful charges.

_____ Shipper Signature

SHIPPER SIGNATURE / DATE
This is to certify that the above-named materials are properly classified, packaged, marked and labeled, and are in proper condition for transportation according to the applicable regulations of the DOT.

Trailer Loaded: ☐ By Shipper ☐ By Driver
Freight Counted: ☐ By Shipper ☐ By Driver/pallets said to contain ☐ By Driver/Pieces

CARRIER SIGNATURE / PICKUP DATE
Carrier acknowledges receipt of packages and required placards. Carrier certifies emergency response information was made available and/or carrier has the DOT emergency response guidebook or equivalent documentation in the vehicle. Property described above is received in good order, except as noted.

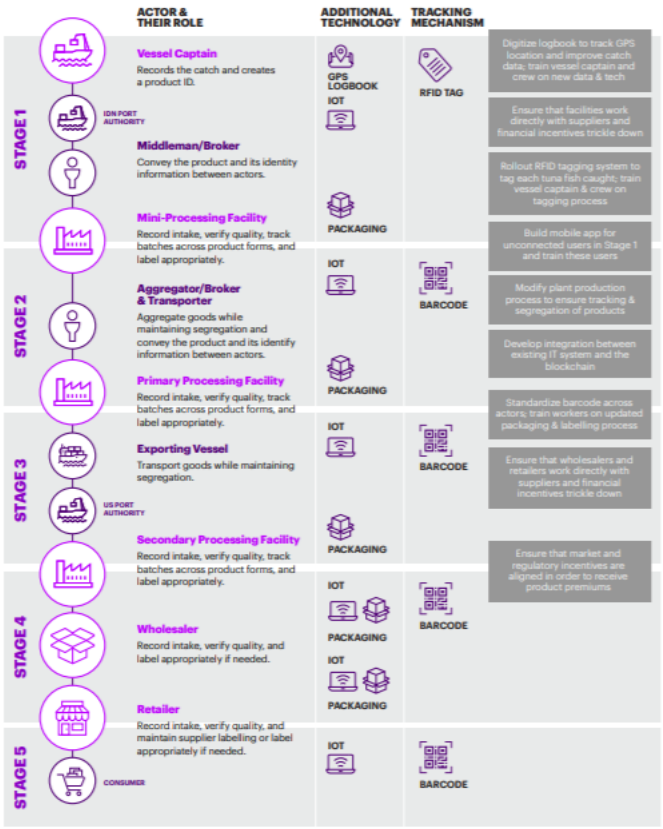
Εικόνα 40: Έγγραφο Bill of Lading

Πηγή: www.tradefinanceglobal.com

Τομέας εφαρμογής

Η Accenture εφάρμοσε blockchain στον τομέα των logistics και συγκεκριμένα για την ιχνηλάτιση και τον έλεγχο εμπορευματοκιβωτίων. Η διαδρομή των προϊόντων μέσα στα εμπορευματοκιβώτια καταγράφεται, με τον παραδοσιακό τρόπο, σε αρκετά έγγραφα τα οποία απαιτείται να μεταφέρονται μαζί με τα προϊόντα, γεγονός που πολλές φορές καθιστά την διαδικασία ελέγχου της τοποθεσίας ενός προϊόντος αρκετά δύσκολη. Τα τελευταία χρόνια ολοένα και περισσότερες εταιρείες προσπαθούν να βρούν λύσεις για την διαχείριση της εφοδιαστικής τους αλυσίδας, προσπαθώντας να καταστήσουν τα προϊόντα τους

ευκολότερα διαχειρίσιμα και με όση περισσότερη διαφάνεια. Ωστόσο, τα μεγαλύτερα προβλήματα που αντιμετωπίζουν στην υϊοθέτηση ψηφιακών λύσεων είναι η απουσία ουσιαστικής και γρήγορης συνεργασίας μεταξύ των εμπλεκόμενων μερών της αλυσίδας αυτής με ψηφιακό τρόπο, η αδυναμία διαχείρισης μεγάλου όγκου από ανόμοια δεδομένα που δεν ακολουθούν συγκεκριμένα πρότυπα αλλά και η πιθανή απουσία τέτοιων λύσεων από τους διάφορους συνεργάτες της εταιρείας. Το blockchain, χάρη στις ιδιότητες του, μπορεί να λύσει τα προβλήματα αυτά και άρα να βοηθήσει εταιρείες με την διαχείριση και την ιχνηλασιμότητα των εφοδιαστικών τους αλυσίδων. Το blockchain προσφέρει μεγαλύτερη αποδοτικότητα στους χρόνους ανίχνευσης, πλήρη διαφάνεια όλων των συναλλαγών που λαμβάνουν χώρα σε αυτό αλλά και μειωμένο κόστος και γραφειοκρατία χάρη στην τεχνολογία του.



Εικόνα 41: Στάδια εφαρμογής του blockchain στην εφοδιαστική αλυσίδα

Πηγή: www.accenture.com

Εφαρμογή του Blockchain

Κατα την μεταφορά εμπορευματοκιβωτίων, το έγγραφο Bill of Lading (BOL) αποτελεί ουσιαστικά την απόδειξη που εκδίδει ο μεταφορέας στον παραλήπτη για να καταγραφεί η παράδοση του εμπορευματοκιβωτίου. Το έγγραφο αυτό είναι ουσιαστικά το κλειδί για την ανίχνευση των προϊόντων στα παραδοσιακά συστήματα εφοδιαστικής αλυσίδας, αφού

δείχνει την σειρά με την οποία το προϊόν φτάνει στον τελικό του προορισμό. Η Accenture, σε συνεργασία με τις AB InBev, APL και Kuehne & Nagel ανέπτυξε μια λύση βασισμένη σε consortium blockchain για την ψηφιοποίηση του συστήματος ανίχνευσης των εμπορευματοκιβωτίων. Το Bill of Lading αντικαταστάθηκε με κρυπτογραφημένα αρχεία τα οποία αποθηκεύονται σε ένα τροποποιημένο Ethereum blockchain, το οποίο είναι permissioned. Αυτό σημαίνει ότι, σε αντίθεση με τα δημόσια blockchains, για να συμμετέχει ένας κόμβος στο δίκτυο θα πρέπει πρώτα να έχει λάβει άδεια από τους υπόλοιπους κόμβους. Έτσι, εξασφαλίζεται ότι οι όλες οι ευαίσθητες πληροφορίες για τα προϊόντα θα είναι διαθέσιμες μόνο στους φορείς που εμπλέκονται πραγματικά στην εφοδιαστική αλυσίδα. Σύμφωνα με έρευνα της Accenture, ο παραδοσιακός τρόπος ιχνηλάτησης των προϊόντων απαιτεί περίπου 20 διαφορετικά έγγραφα, τα περισσότερα των οποίων είναι σε φυσική μορφή. Σύμφωνα με την εφαρμογή του σχεδίου της, η Accenture υπολόγισε ότι ο όγκος των δεδομένων που απαιτείται να αποθηκεύονται στο σύστημα μειώνεται κατά 80%. Αυτό σημαίνει ότι τα queries από τους διαφόρους ενδιαφερόμενους στην εφοδιαστική αλυσίδα απαιτούν ελάχιστο χρόνο για να ολοκληρωθουν, το οποίο οδηγεί σε ιχνηλάτιση σε πραγματικό χρόνο (real time tracking). Η εφαρμογή του σχεδίου αυτού έγινε σε 12 διαφορετικά φορτία (shipments), το καθένα με διαφορετικό προορισμό ώστε τα αποτελέσματα να είναι αντικειμενικά και να μπορούν να γενικευθούν. Η AB InBev εκπροσώπησε τον εξαγωγέα, η APL τον αποστολέα και η Kuehne & Nagel τον μεταφορέα των εμπορευμάτων. Ο strategic manager της APL, Eddie Ng, τόνισε ότι η APL έχει ιδιαίτερο ενδιαφέρον στην τεχνολογία του blockchain, και ότι η εφαρμογή αυτή δείχνει ότι το blockchain είναι ξεκάθαρα το μέλλον για την ιχνηλασιμότητα και την βελτιστοποίηση της εφοδιαστικής αλυσίδας. Επιπροσθέτως, ο Vice President Danillo Figueiredo της AB InBev χαρακτήρισε το blockchain ως μια τεχνολογία η οποία θα μεταμορφώσει ριζικά την ιδέα της εφοδιαστιής αλυσίδας, μειώνοντας τα ανθρώπινα λάθη, αυξάνοντας την διαθέσιμη πληροφορία για τα προϊόντα και βελτιστοποιώντας τις διαδικασίες μεταφοράς τους.

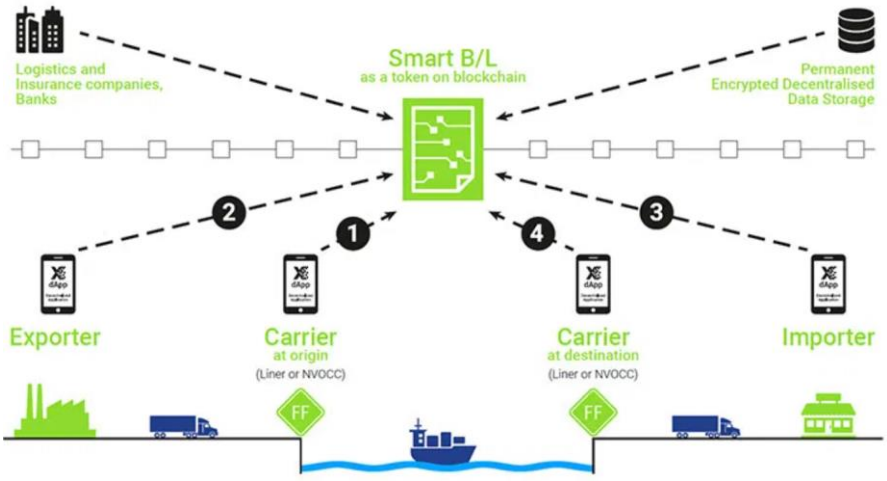
5.5 CargoX

Προφίλ εταιρείας

Η CargoX πρόκειται για εταιρεία που ειδικεύεται σε λύσεις εφοδιαστικής αλυσίδας και ειδικά για μεταβίβαση εγγράφων με την βοήθεια του blockchain. Τα κεντρικά γραφεία της εταιρείας βρίσκονται στην Λιουμπλιάνα της Σλοβενίας ενώ το γραφείο της στρατηγικής πολιτικής της είναι στο Hong Kong. Ο κύριος σκοπός της είναι να παρέχει άμεσα και γρήγορα λύσεις ψηφιοποίησης σε τεχνολογικές εταιρείες σε τομείς παραγωγής, οικονομικούς και ενεργειακούς ώστε να μπορούν να βελτιώσουν την εφοδιαστική τους αλυσίδα και να κατέχουν συγκριτικό πλεονέκτημα έναντι των αντιπάλων τους.

Τομέας εφαρμογής

Ο τομέας εφαρμογής είναι αρκετά παρόμοιος με τον τομέα εφαρμογής στο προηγούμενο case study. Η αξία του θαλάσσιου εμπορίου είναι τεράστια και τα εμπορευματοκιβώτια που μετακινούνται περνούν από αρκετά σημεία-κόμβους στα οποία πρέπει να καταχωρούνται τα στοιχεία τους. Όπως έχει προαναφερθεί, το bill of lading (BoL) είναι το βασικό έγγραφο που αποτελεί την ταυτότητα του εμπορευματοκιβωτίου, το οποίο παραδοσιακά είναι υλικό έγγραφο. Η τεχνολογία του blockchain μπορεί να βοηθήσει στην ψηφιοποίηση του και άρα να μειώσει τον χρόνο ιχνηλάτησης των προϊόντων αλλά και να βελτιώσει την διαφάνεια των προϊόντων αυτών αποδεικνύοντας στον πελάτη από ποια σημεία και πότε πέρασε το προϊόν που σκέφτεται να αγοράσει.



Εικόνα 42: Η πλατφόρμα CargoX

Πηγή: www.cargox.io

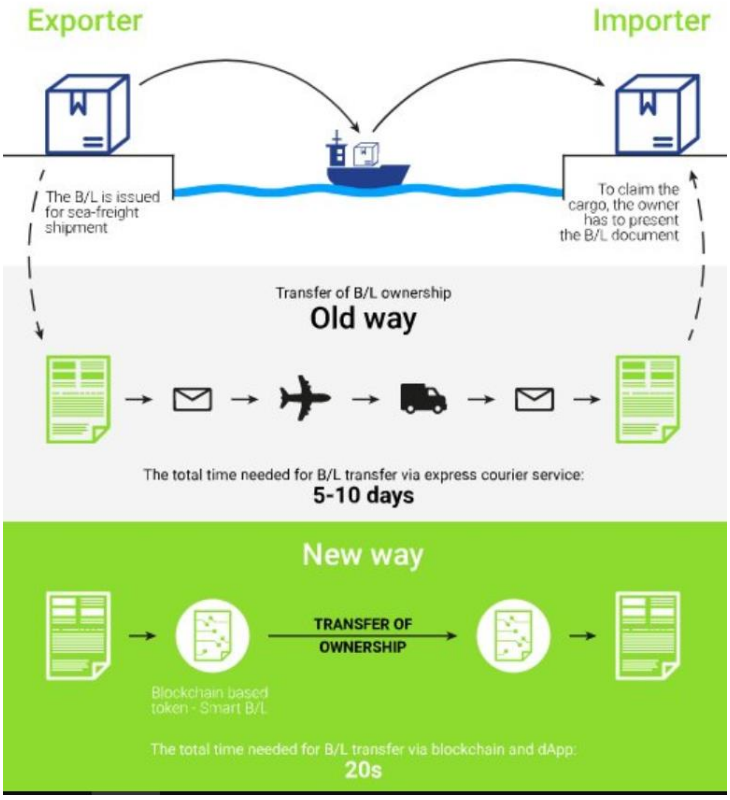
Εφαρμογή του Blockchain

Η CargoX έχει αναπτύξει μια πλατφόρμα εφαρμογής blockchain σε εφοδιαστική αλυσίδα η οποία είναι υπεύθυνη για την ανταλλαγή και την διαμοίραση των εγγράφων των εμπορευματοκιβωτίων εταιρειών, με έμφαση στο Bill of Lading. Η πλατφόρμα που χρησιμοποιεί λειτουργεί στο δημόσιο δίκτυο του Ethereum, γεγονός το οποίο σύμφωνα με την εταιρεία ελαχιστοποιεί την πιθανότητα να βρεθεί κάποιος ανταγωνιστής στο δίκτυο της εταιρείας, όπως θα μπορούσε να συμβεί με ένα ιδιωτικό blockchain. Η εταιρεία έχει επίσης δηλώσει ότι η πλατφόρμα της είναι απολύτως ουδέτερη και δεν θα μοιραστεί ποτέ επιχειρηματικές πληροφορίες με τρίτους για οποιονδήποτε σκοπό. Το ηλεκτρονικό BL (eBL ή αλλιώς smartBL) το οποίο χρησιμοποιεί η πλατφόρμα μπορεί να είναι οποιασδήποτε μορφής αρχείο. Το αρχείο αυτό μεταβιβάζεται από τον αποστολέα στον παραλήπτη μέσω της πλατφόρμας, ενώ αξίζει να σημειωθεί ότι ο παραλήπτης τότε έχει την κυριότητα του εγγράφου και μπορεί να την αποδείξει πάλι μέσω της πλατφόρμας.

Ένα έγγραφο Bill of Lading παρέχει τις εξής πληροφορίες:

- Την ταυτότητα του εκναυλωτή, του φορτωτή, του παραλήπτη, του πλοιάρχου καθώς και τις πληροφορίες του μέσου με το οποίο μεταφέρεται το προϊόν, για παράδειγμα τον αριθμό και δρομολόγιο του τρένου, το όνομα του πλοίου, ή του αεροπλάνου.
- Πληροφορίες για το σημείο επιβίβασης και αποβίβασης του προϊόντος, για παράδειγμα αεροδρόμιο, λιμάνι, στάση τρένου.
- Αριθμό τεμαχίων, βάρος, ποσότητα μεταφοράς.
- Ημερομηνία και ώρα έκδοσης του ίδιου του εγγράφου.

Οι πληροφορίες αυτές, χάρη στο blockchain, είναι κρυπτογραφημένες και αποκεντρωμένες και άρα δεν μπορούν να προσπελαστούν και να παραποιηθούν, όπως συμβαίνει με τα παραδοσιακά έγγραφα από χαρτί. Σύμφωνα με την εταιρεία, η διαδικασία αυτή μέσω της πλατφόρμας μειώνει δραματικά τον χρόνο μεταφοράς του BL, από 5-10 μέρες στα μόλις 20 δευτερόλεπτα. Εδώ μπορεί να φανεί κιόλας σε πρακτικό επίπεδο ότι παρόλο που θεωρητικά σε ένα δημόσιο δίκτυο blockchain η επικύρωση συναλλαγών είναι πιο αργή από ότι σε ένα ιδιωτικό δίκτυο, στην περίπτωση της CargoX αυτός ο χρόνος αποδεικνύει ότι τα δημόσια δίκτυα μπορούν να πετύχουν και αυτά πολύ μικρούς χρόνους συναλλαγών, και άρα ένα ιδιωτικό blockchain δεν θα προσέφερε κάτι παραπάνω σε μια τέτοια εταιρεία.



Εικόνα 43: Σύγκριση χρόνου μεταφοράς BL

Πηγή: www.cargox.io

Αξίζει να αναφερθεί ότι η ίδια πλατφόρμα παρέχει και υπηρεσία messaging για του χρήστες για πιο εύκολη συνομιλία των εμπλεκόμενων στην εφοδιαστική αλυσίδα, ενώ όλα τα ηλεκτρονικά έγγραφα μπορούν να προσπελαστούν με διαδικασίες query και text search για ταχύτερη ιχνηλάτιση των προϊόντων. Όλες αυτές οι υπηρεσίες καθιστούν τις μεταφορές προϊόντων πιο ασφαλείς, φθηνές, ταχύτερες, ουδέτερες και άρα πιο φιλικές τόσο για τον χρήστη όσο και για την εταιρεία και τα μέλη της εφοδιαστικής της αλυσίδας.

Συμπεράσματα

Συμπεράσματα σύγκρισης δημόσιων και ιδιωτικών δικτύων blockchain

Τα δημόσια και τα ιδιωτικά δίκτυα blockchain, όπως φαίνεται και από την ανάλυση που έχει προαναφερθεί, έχουν αρκετές θεωρητικές και πρακτικές διαφορές για τους απλούς χρήστες αλλά και τις επιχειρήσεις που υϊουθετούν λύσεις blockchain. Συνεπώς, κρίνεται σημαντική η σύγκριση των δύο αυτών λύσεων για την επιλογή της καταλληλότερης, ανάλογα με το σενάριο χρήσης. Οι δύο αυτές λύσεις, λοιπόν, μπορούν να συγκριθούν ανάλογα με τα εξής κριτήρια (Iredale, 2021; Sahu, 2020; Sandner, 2017):

Σκοπός

Η βασική διαφορά του ιδιωτικού με το δημόσιο δίκτυο είναι ο σκοπός για τον οποίο έχουν αναπτυχθεί. Στο δημόσιο δίκτυο μπορεί να συμμετάσχει ο καθένας, και όλοι οι κόμβοι συμμετέχουν στην διαδικασία συναίνεσης, ενώ στο ιδιωτικό δίκτυο απαιτείται να στηθεί από την εταιρεία που ενδιαφέρεται, ενώ πρέπει να ρυθμιστούν αρκετές διαφορετικοί παράμετροι για την σωστή λειτουργία του, όπως για παράδειγμα ποιά θα είναι η δυσκολία του μαθηματικού μοντέλου το οποίο θα λύνεται για την συναίνεση. Για παράδειγμα, αν αυτό το πρόβλημα είναι πολύ εύκολο, θα σημαίνει ότι οι συναλλαγές στο δίκτυο θα συμβαίνουν πολύ γρήγορα, ωστόσο η ασφάλεια του δικτύου θα είναι μειωμένη καθώς με μικρή υπολογιστική ισχύ θα μπορεί κάποιος εξωτερικός του δικτύου, αν αποκτήσει πρόσβαση σε αυτό, να αλλάξει τα δεδομένα που κρατούνται σε αυτό.

Εμπιστευτικότητα

Στο δημόσιο δίκτυο υπάρχει η μέγιστη διαφάνεια μιας και οι συναλλαγές είναι δημόσια διαθέσιμες σε όλους του συμμετέχοντες κόμβους, γεγονός το οποίο οδηγεί στην καλή εμπιστοσύνη μεταξύ των συμβαλλόμενων μερών μιας εταιρείας που θέλει να αναπτύξει λύση βασισμένη σε blockchain. Αν, ωστόσο, η εταιρεία επιθυμεί να αποκρύπτει συγκεκριμένες πτυχές και λεπτομέρειες των συναλλαγών της, το ιδιωτικό permissioned δίκτυο προσφέρει καλύτερη τέτοια δυνατότητα λόγω του permission layer.

Γλώσσα προγραμματισμού

Ειδικά στο Ethereum, η γλώσσα προγραμματισμού που χρησιμοποιείται για την ανάπτυξη smart contract είναι η υψηλού επιπέδου Solidity, η οποία έχει αναπτύχθεί συγκεκριμένα για την χρήση σε smart contract. Σε αντίθεση με αυτή, το Hyperledger χρησιμοποιεί πιο κοινότυπες γλώσσες προγραμματισμού όπως η Javascript και η Golang, οι οποίες βέβαια

δεν έχουν αναπτυχθεί για την χρήση μόνο σε smart contracts, οπότε απαιτείται περισσότερος χρόνος και γραμμές κώδικα για την ίδια εφαρμογή σε σχέση με την Solidity. Επιπρόσθετα, σε γλώσσες όπως Javascipt και Golang μπορεί να υπάρχουν ενδεχόμενα κενά ασφαλείας όσον αφορά smart contracts, και άρα απαιτείται περαιτέρω έρευνα για την διαπίστωση του αν αυτές οι γλώσσες μπορούν να χρησιμοποιηθούν σε πλήρεις εφαρμογές εταιρειών με απόλυτη ασφάλεια.

Κρυπτονόμισμα

Τα 2 κύρια δημόσια δίκτυα του Bitcoin και του Ethereum προσφέρουν δικά τους ενσωματωμένα κρυπτονομίσματα τα οποία μπορούν να χρησιμοποιηθούν για τις συναλλαγές σε αυτά. Ορισμένα ιδιωτικά δίκτυα όπως τα Ripple και Quorum προσφέρουν και αυτά δικό τους κρυπτονόμισμα. Ωστόσο, στο δίκτυο του Hyperledger δεν υπάρχει τέτοια δυνατότητα, και άρα οι συναλλαγές πρέπει να γίνονται με άλλα νομίσματα, γεγονός το οποίο μπορεί ενδεχομένως να περιπλέξει την διαδικασία του smart contract.

Αριθμός συναλλαγών ανά μονάδα χρόνου

Στο δημόσιο blockchain η κάθε συναλλαγή πρέπει να επικυρωθεί από όλους του κόμβους που επικυρώνουν, συνεπώς αυτό σημαίνει ότι περίπου 20 συναλλαγές ανά δευτερόλεπττο μπορούν να επικυρώνονται σε ολόκληρο το δίκτυο του Ethereum. Αντιθέτως, στο ιδιωτικό blockchain το μαθηματικό πρόβλημα που λύνεται είναι αρκετά πιο εύκολο, και επίσης συμμετέχουν και λιγότεροι κόμβοι μιας και είναι permissioned, συνεπώς στο δίκτυο του Hyperledger μπορούν να επικυρώνονται περίπου 2000 συναλλαγές ανά δευτερόλεπτο σε μια τυπική επιχειρηματική εφαρμογή.

Κριτήριο	**Δημόσια δίκτυα**	**Ιδιωτικά Δίκτυα**
Διαφάνεια	Περισσότερο	Λιγότερο
Βαθμός αποκέντρωσης	Περισσότερο	Λιγότερο
Αδιάβλητο	Περισσότερο	Λιγότερο
Ειδική γλώσσα προγραμματισμού για smart contracts	Ειδικά για Ethereum-Solidity	-
Ταχύτητα Συναλλαγών	Λιγότερο	Περισσότερο
Βαθμός επεκτασιμότητας	Λιγότερο	Περισσότερο

Ο κύριος στόχος των εταιρειών που αναζητούν λύσεις blockchain για την εφοδιαστική τους αλυσίδα είναι να αποδείξουν στους πελάτες τους ότι τα προϊόντα προέρχονται από συγκεκριμένες πιστοποιημένες πηγές και πρώτες ύλες, καθώς και να δώσουν στους πελάτες αυτούς την δυνατότητα να μπορούν να το επικυρώσουν με την βοήθεια κάποιας

εφαρμογής. Επιπροσθέτως, ένας ακόμη στόχος των εταιρειών αυτών είναι ο ταχύτερος και ακριβέστερος εντοπισμός των προϊόντων τους καθώς μετακινούνται μέσα στην εφοδιαστική τους αλυσίδα. Τέλος, ένας βασικός ακόμα στόχος τους είναι τα ασφαλή και γρήγορα smart contracts τα οποία θα βοηθήσουν στην ασφάλεια, την ταχύτητα και την εμπιστοσύνη για τις συναλλαγές μεταξύ συνεργαζόμενων εταιρειών.

Με βάση, λοιπόν, αυτούς τους σκοπούς καθώς και τα στοιχεία των δημοσίων και των ιδιωτικών blockchain που έχουν αναλυθεί σε προηγούμενη ενότητα, η καλύτερα λύση για μια εταιρεία που αναζητεί λύση blockchain για εφαρμογή στην εφοδιαστική της αλυσίδα κρίνεται το δημόσιο blockchain. Καταρχάς, προσφέρει την μέγιστη διαφάνεια τόσο στον τελικό πελάτη όσο και στην ίδια την εταιρεία, καθώς όλοι οι κόμβοι του δικτύου συμμετέχουν στην διαδικασία επικύρωσης των συναλλαγών, και έτσι είναι αδύνατη η τροποποίηση των στοιχειών του blockchain, κάτι που είναι πιο πιθανό να συμβεί στο permissioned ιδιωτικό δίκτυο blockchain, το οποίο δεν κατέχει πολλά από τα στοιχεία του δημοσίου blockchain για τον σκοπό αυτό. Ακόμη, η γλώσσα προγραμματισμού Solidity που χρησιμοποιείται για τα smart contracts στο Ethereum έχει σχεδιαστεί συγκεκριμένα για την χρήση αυτή, και άρα προσφέρει καλύτερη απόδοση των smart contract από τις υπόλοιπες γλώσσες που χρησιμοποιούνται στο ιδιωτικό δίκτυο του Hyperledger και άρα δύναται να έχουν περισσότερα κενά ασφαλείας. Αξίζει να σημειωθεί, ακόμη, ότι παρόλο που η ταχύτητα των συναλλαγών στο δημόσιο δίκτυο του Ethereum είναι μικρότερη από αυτή στο Hyperledger, το δίκτυο του Ethereum επεξεργάζεται περίπου 20 συναλλαγές ανά δευτερόλεπτο, γεγονός το οποίο σημαίνει ότι για εφαρμογές ιχνηλασιμότητας η ταχύτητα αυτή αρκεί για να προσφέρει ικανοποιητή απόδοση στην εταιρεία αλλά και στον τελικό πελάτη. Επίσης, τα transacton fees για μια συναλλαγή είναι της τάξης των 5-10 δολλαρίων, ένα κόστος αρκετά μικρό σε σχέση με την αξία ολόκληρων εμπορευματοκιβωτίων που μπορεί να ενδιαφέρεται να εντοπίσει είτε η εταιρεία είτε ο πελάτης που επιθυμεί να αγοράσει το αντίστοιχο προϊόν. Έτσι, προκύπτει το συμπέρασμα ότι ένα δημόσιο δίκτυο blockchain όπως το Ethereum προσφέρει συνολικά καλύτερα χαρακτηριστικά σε εφαρμογές ιχνηλασιμότητας στην εφοδιαστική αλυσίδα από ένα ιδιωτικό δίκτυο όπως το Hyperledger Fabric, τόσο στην εταιρεία που υϊοθετεί τέτοια λύση όσο και στον πελάτη που αγοράζει το τελικό προϊόν.

Από τις μελέτες περίπτωσης προκύπτουν τα ακόλουθα συμπεράσματα. Φαίνεται, λοιπόν, ότι 3 από αυτές αφορούν ιδιωτικό δίκτυο blockchain ενώ οι 2 αφορούν δημόσιο δίκτυο blockchain και ειδικά το Ethereum. Αναλύοντας τις εφαρμογές αυτές μπορεί να εξαχθεί το εξής συμπέρασμα για την επιλογή του δημόσιου ή του ιδιωτικού δικτύου: Οι NTT, Bosch και Renault αποτελούν εταιρείες που εφαρμόζουν το blockchain σε εργοστάσια παραγωγής τα οποία επεξεργάζονται τεράστιο αριθμό εξαρτημάτων και συσκευών καθημερινά. Συνεπώς, το blockchain που έχουν επιλέξει είναι το ιδιωτικό μιας και αυτό προσφέρει την μεγαλύτερη ταχύτητα συναλλαγών αλλά και τον μεγαλύτερο βαθμό επεκτασιμότητας (scalability), δηλαδή την ευκολία και την ταχύτητα χρήσης του δικτύου όσο μεγαλώνει ο αριθμός των κόμβων και των συναλλαγών. Σε ένα δημόσιο δίκτυο blockchain οι εφαρμογές αυτές δεν θα

μπορούσαν να χρησιμοποιηθούν με την ίδια απόδοση μιας και οι συναλλαγές εκεί συμβαίνουν με μικρότερη ταχύτητα. Αντίθετα, στην περίπτωση της Accenture και της CargoX, οι εταιρείες αυτές χρησιμοποιούν την τεχνολογία του blockchain για την ιχνηλάτηση εμπορευματοκιβωτίων και ειδικά του εγγράφου Bill of Lading. Συνεπώς, δεν απαιτείται η χρήση ιδιωτικού blockchain μιας και η ταχύτητα επικύρωσης στο δίκτυο του Ethereum αρκεί για να καλύπτει όλα τα BoL που απαιτούνται. Μάλιστα, από έρευνα της CargoX προκύπτει ότι για την συγκεκριμένη εφαρμογή της, ένα ιδιωτικό δίκτυο δεν θα παρείχε μεγαλύτερη ταχύτητα συναλλαγών από ότι επιτυγχάνεται στο Ethereum.

Συμπεράσματα ανάλυσης εργαλείων βελτιστοποίησης κώδικα smart contract

Αναλύοντας την υπάρχουσα βιβλιογραφία για εφαρμογές blockchain στο πεδίο του software engineering δύναται να εξαχθεί το συμπέρασμα ότι οι περισσότερες αναφορές γίνονται για την πλατφόρμα του Ethereum, ενώ ακολουθούν το Bitcoin και το Hyperledger. Ωστόσο, για να ολοκληρωθεί σωστά η έρευνα και να μπορούν να γενικευθούν τα συμπεράσματα που προκύπτουν από το Ethereum, θα πρέπει οι ίδιες έρευνες να διεξαχθούν και τις υπόλοιπες πλατφόρμες. Μπορεί να παρατηρηθεί, ακόμη, ότι τα περισσότερα dataset στις έρευνες είναι της τάξης των χιλιάδων, ενώ σε μερικές περιπτώσεις φτάνουν ακόμα και τις εκατοντάδες χιλιάδες, συνήθως όταν πρόκειται για έλεγχο smart contracts. Είναι λογικό ότι όσο μεγαλύτερο το μέγεθος του dataset, τόσο πιο ορθά είναι τα συμπεράσματα που προκύπτουν, αλλά και τόσο περισσότερο υλικό υπάρχει για περαιτέρω επόμενες έρευνες.

Επίσης, οι έρευνες του κώδικα των smart contract επικεντρώνονται κυρίως στην ανίχνευση προβλημάτων ασφαλείας και ποιότητας, στην αναγνώριση κομματιών κώδικα που μπορούν να αναπαραχθούν σε πολλαπλά smart contracts και στην ανίχνευση κώδικα ο οποίος κοστίζει σε gas. Αφού η διαδικασία ολοκλήρωσης και επικύρωσης των smart contract κοστίζει σε gas κρίνεται απαραίτητη η περαιτέρω έρευνα σε τεχνικές οι οποίες αναγνωρίζουν τέτοια κομμάτια και μοτίβα κώδικα, αλλά και τεχνικές οι οποίες αυτόματα βελτιστοποιούν τον κώδικα αυτό για επίτευξη του ελάχιστου δυνατού gas. Αξίζει να αναφερθεί ότι οι περισσότερες έρευνες επικεντρώνονται κυρίως στις γλώσσες Solidity και Go, ωστόσο και πάλι τα αποτελέσματα θα πρέπει να ελεγχθούν σε περισσότερες γλώσσες για να γίνει σωστή γενίκευση.

Αρκετή προσοχή έχει δεχθεί και το κομμάτι της ασφάλειας των smart contract και ειδικά η αναγνώριση απειλών και ευάλωτων σημείων τους. Ωστόσο, η ασφάλεια των smart contract είναι ακόμη σε αρκετά πρώιμο στάδιο, μιας και τα ίδια τα smart contracts είναι σχετικά νέα τεχνολογία. Ακόμα και αν οι ερευνητές βρίσκουν συνεχώς καινούργια εργαλεία για αναγνώριση των απειλών αυτών, η βιβλιογραφία δείχνει ότι λείπει μια ομαδοποίηση και κατηγοριοποίηση τους ανάλογα με τα κοινά τους στοιχεία όπως το πιθανό κόστος και ο

τρόπος με τον οποίο σπάει η ασφάλεια των smart contract. Άρα, λοιπόν, κρίνεται απαραίτητη η τυποποίηση των τεχνικών δοκιμής τους, για την ευκολότερη και γρηγορότερη κατανόηση και κατηγοριοποίηση τους.

Ένα ακόμη σημαντικό πρόβλημα που πρέπει να λυθεί στο πεδίο του blockchain είναι η ταχύτητα και η απόδοση των smart contracts. Από την ανάλυση της βιβλιογραφίας κρίνεται απαραίτητο να βρεθούν εργαλεία και frameworks τα οποία αξιολογούν αλλά και βελτιστοποιούν τα διάφορα bottlenecks που μπορεί να βρίσκονται στον κώδικα του smart contract. Τα 2 κυριότερα προβλήματα που οδηγούν σε bottlenecks είναι η επεκτασιμότητα και η διαθεσιμότητα του κώδικα που χρησιμοποιείται σε αυτά. Άρα, θα πρέπει τα εργαλεία που θα αναπτυχθούν να παρέχουν την αξιολόγηση και την βελτιστοποίηση του κώδικα, την δυνατότητα επέκτασης σε περισσότερες συναλλαγές χωρίς αισθητή μείωση της απόδοσης και την δυνατότητα αλλαγής του πρωτόκολλου συναίνεσης χωρίς την αλλαγή της ταχύτητας ολοκλήρωσης του smart contract.

Η τεχνολογία του blockchain ολοένα και αναπτύσσεται και υΙοθετείται από αρκετούς τομείς της καθημερινότητας. Γι΄αυτό τον λόγο, θα πρέπει να βρεθούν οι σωστές μέθοδοι με τις οποίες θα μπορεί να αξιολογηθεί συνολικά ο τρόπος με τον οποίο θα πρέπει να αναπτύσσονται οι τεχνικές σχεδίασης του. Τα διάφορα εργαλεία αξιολόγησης και βελτιστοποίησης θα βοηθήσουν τους προγραμματιστές να ανατπύξουν νέες αποδοτικές μεθόδους και λογισμικά blockchain, και άρα να βοηθήσουν στην υϊοθέτηση του blockchain σε κάθε τομέα της καθημερινότητας.

Σύνοψη Εργασίας

Στην παρούσα διπλωματική εργασία πραγματοποιήθηκε μια ανάλυση των τεχνολογιών blockchain σε εφαρμογές ιχνηλασιμότητας στην εφοδιαστική αλυσίδα. Αρχικά παρουσιάστηκαν οι βασικές λειτουργίες του blockchain, ο τρόπος με τον οποίο λειτουργεί αλλά και το πώς επικυρώνονται οι συναλλαγές και οι συμφωνίες μέσα σε αυτό χάρη στους αλγορίθμους συναίνεσης. Το δημόσιο και το ιδιωτικό blockchain αποτελούν τις 2 διαφορετικές πτυχές της τεχνολογίας αυτής, γι’αυτό στη συνέχεια έγινε μια παρουσίαση αλλά και σύγκρισή τους, ώστε να προκύψουν χρήσιμα συμπεράσματα για το ποιό από τα 2 είναι το καταλληλότερο για μια εφαρμογή σε εφοδιαστική αλυσίδα. Από την σύγκριση αυτή προκύπτει ότι το δημόσιο δίκτυο είναι καταλληλότερο χάρη στα χαρακτηριστικά διαφάνειας και ασφάλειας του, ωστόσο τα ιδιωτικά permissioned blockchains χρησιμοποιούνται σε αρκετές επιχειρήσεις όπως φάνηκε και από το κεφάλαιο των μελετών περίπτωσης. Παράλληλα πραγματοποιήθηκε και η ανάλυση των εργαλείων βελτιστοποίησης smart contracts, όπου ουσιαστικά αναφέρθηκαν αρκετά εργαλεία τα οποία μπορούν να χρησιμοποιηθούν για να βελτιώσουν την ασφάλεια, την ταχύτητα αλλά και την αποτελεσματικότητα τους. Στο επόμενο κεφάλαιο πραγματοποιήθηκε μια δομημένη βιβλιογραφική ανασκόπηση του ερευνητικού πεδίου σχετικά με την χρήση του blockchain

σε εφαρμογές ιχνηλασιμότητας στον κλάδο των ποτών, από την οποία προέκυψαν αρκετά χρήσιμα συμπεράσματα για την χρήση του σε πρακτικές εφαρμογές. Για να ολοκληρωθεί η έρευνα αυτή, η εργασία περνάει στο κεφάλαιο των μελετών περίπτωσης, όπου αναλύονται με λεπτομέρεια αρκετές εφαρμογές blockchain από εταιρείες στον τομέα της εφοδιαστικής αλυσίδας.

Ορισμοί

Οι παρακάτω ορισμοί παρατίθενται ως μια προσπάθεια ακριβέστερης και τεχνικής κατανόησης για τους όρους που έχουν αναφερθεί στα υπόλοιπα κομμάτια της εργασίας.

Δημόσιο blockchain (Public Blockchain)

Σε ένα δημόσιο blockchain, κάθε κόμβος έχει το δικαίωμα να συμμετάσχει στα δεδομένα του δικτύου, ενώ τα ίδια τα δεδομένα αυτά είναι δημόσια και μπορούν να εξακριβωθούν από οποιονδήποτε κόμβο. Κάθε κόμβος έχει δικαίωμα να αναπτύξει και να ολοκληρώσει smart contracts μέσω συναλλαγών.

Consortium blockchain

Σε ένα consortium blockchain, οι κόμβοι που είναι υπεύθυνοι για την εκτέλεση συναλλαγών (οι οποίοι έχουν τα δεδομένα των συναλλαγών αυτών) είναι προκαθορισμένοι εκ των προτέρων. Ο τρόπος με τον οποίο τα δεδομένα του blockchain (οι συναλλαγές και τα smart contracts) μπορούν να προταθούν και να προσπελαστούν εξαρτάται από το consortium:

Κλειστό consortium: Μόνο οι προκαθορισμένοι κόμβοι μπορούν να προτείνουν records και να προσπελάσουν τα δεδομένα.

Ανοιχτό consortium: Οποιοσδήποτε μπορεί να εγγραφεί (μέσω κεντρικών κόμβων) ώστε να λάβει το δικαίωμα να προτείνει ή να προσπελαύνει τα δεδομένα των records στο blockchain.

Ιδιωτικό blockchain (Private blockchain)

Το ιδιωτικό blockchain αναφέρεται σε blockchain το οποίο ελέγχεται πλήρως από ένα πρόσωπο ή ομάδα.Χρησιμοποιείται για να καταγράφει ιδιωτικές πληροφορίες και μόνο ο ιδιοκτήτης του έχει το δικαίωμα να προσπελαύνει και να διατηρεί τα αρχεία. Στην πράξη, δημόσια blockchain όπως το Bitcoin και το Ethereum δεν θέτουν όρια για τους κόμβους που επιθυμούν να συμμετάσχουν στο P2P δίκτυο τους. Κλειστά consortium blockchain είναι για παράδειγμα τα Corda, Quorum και Hyperledger Fabric. Αυτά τα blockchain είναι κυρίως σχεδιασμένα για την καλύτερη συνεργασία επιχειρηματικών συνεταίρων. Τα ανοικτά consortium blockchain, όπως τα Ripple και Libra, προσφέρουν μεγαλύτερη διαφάνεια επιτρέποντας σε οποιονδήποτε να εγγραφεί ώστε να συμμετάσχει στο δίκτυο. Μια σύντομη σύγκριση των τύπων blockchain μπορεί να φανεί στον επόμενο πίνακα. Η λέξη «εγγεγραμμένος» σημαίνει ότι ένα μέλος-ομάδα πρέπει να εγγραφεί πρώτα στον κατάλληλο κεντρικό οργανισμό προκειμένου να λάβει το δικαίωμα πρόσβασης σε δεδομένα και πραγματοποίησης συναλλαγών, ενώ η λέξη «επιτρεπόμενοι» αναφέρεται σε ένα πιο περιορισμένο τρόπο εξουσιοδότησης των δικαιωμάτων, η οποία συμβαίνει και λιγότερο συχνά. Οι επόμενοι ορισμοί της συναίνεσης δίνονται από τους Garay et al. Και Pass et al.

Συναίνεση

Ένας μηχανισμός συναίνεσης επιτρέπει σε όλους τους συμμετέχοντες κόμβους , είτε πραγματικούς είτε κακόβουλους, να συμφωνήσουν για τα περιεχόμενα σε ένα blockchain. Σε έναν μηχανισμό συναίνεσης πρέπει να τηρούνται τα εξής κριτήρια:

Liveness: Κάθε συναλλαγή θα πρέπει να επεξεργάζεται μέχρι τέλους.

Persistence: Εαν ένα πραγματικός κόμβος επικυρώσει μια συναλλαγή (είτε την δεχτεί, είτε την απορρίψει), τότε και όλοι οι άλλοι πραγματικοί κόμβοι του δικτύου τελικά θα έχουν την ίδια απόφαση.

Miner

Η λέξη miner αναφέρεται σε κόμβο ο οποίος παρέχει μη ασήμαντο φόρτο εργασίας σε έναν μηχανισμό συναίνεσης με τον σκοπό της ανταμοιβής σε ένα blockchain. Κατά την διαδικασία συναίνεσης στο δίκτυο, μπορεί να προκύψουν καταστάσεις στις οποίες οι κόμβοι διαφωνούν ως προς τα τελικά αποτελέσματα. Αυτό ονομάζεται fork:

Fork

Το fork αναφέρεται στην διαφωνία των κόμβων όσον αφορά στις καταγραφές του blockchain. Τα forks είναι συνήθως χρονικά σύντομα και τελικά θα λυθούν από τον κανόνα της συναίνεσης. Ωστόσο, υπό κάποιες προϋποθέσεις μπορεί να δημιουργηθεί επίτηδες ένα fork για να ανανεωθεί η κατάσταση στο blockchain. Τα forks χωρίζονται σε soft και hard:

Soft fork

Το soft fork αναφέρεται στο fork που δημιουργείται από την ανανέωση ενός non backward compatible μηχανισμού συναίνεσης. Μετά από ένα soft fork, κάποιες συναλλαγές ή blocks τα οποία είναι έγκυρα με τους «παλιούς κανόνες» μπορεί να γίνουν άκυρα, ενώ μετά από ένα hard fork, οι συναλλαγές και τα blocks υπό τους νέους κανόνες είναι άκυρα με τους παλιούς. Τα soft fork χρησιμοποιούνται κυρίως για να εισάγουν νέες κατηγορίες συναλλαγών ή να φτιάξουν ορισμένα προβλήματα με το πρωτόκολλο συναίνεσης. Επίσης, δεν απαιτεί να αλλάξουν όλοι οι κόμβοι στο καινούργιο πρωτόκολλο συναίνεσης. Οι κόμβοι οι οποίοι χρησιμοποιούν το παλιό πρωτόκολλο μπορούν ακόμη να αναγνωρίσουν τις συναλλαγές και τα blocks υπό τους νέους κανόνες, ενώ συγκριτικά, το hard fork χρησιμοποιείται όταν συμβαίνουν σημαντικά γεγονότα (όπως για παράδειγμα κάποια επίθεση στο δίκτυο ή μια μαζική ασυμφωνία στην συναίνεση) και οι κόμβοι πρέπει να επιλεξουν ένα από τα forks (μονοπάτια) και να καταλήξουν με 2 διαφορετικά blockchains τα οποία δεν συναύδουν το ένα με το άλλο.

Συναλλαγές (Transactions)

Μια συναλλαγή Tx αποτελείται από 5 στοιχεία, δηλαδή Tx=(t, in, out, s, pld), όπου t είναι ο χρόνος (timestamp) όπου ο miner λαμβάνει την Tx. Γίνεται η υπόθεση ότι μόνο 1 συναλλαγή μπορεί να λάβει ο κάθε miner ανα χρονική στιγμή t, δηλαδή ισχύει

$$\forall\, i \neq j, Tx_i \neq Tx_j, \forall\, t.$$

Με αυτή την υπόθεση οι συναλλαγές θα πραγματοποιούνται με χρονολογική σειρά (η οποία μπορεί να διαφέρει από κόμβο σε κόμβο). Το in είναι το input της συναλλαγής ενώ το out είναι το output. Το s είναι η υπογραφή (signature) της συναλλαγής, η οποία δείχνει τον ιδιοκτήτη στον οποίο θα μεταφερθούν τα περιεχόμενα της συναλλαγής.Το pld αναφέρεται σε μηνύματα τα οποία εμπεριέχονται στην συναλλαγή και καλούνται payload data. Τα ακριβή στοιχεία της συναλλαγής (όπως το format και η δομή κάθε στοιχείου σε αυτήν) διαφέρει από blockchain σε blockchain ανάλογα με το user model που έχει επιλεχθεί. Στο Bitcoin, για παράδειγμα, χρησιμοποιεί το unspent transaction account model (UTXO), ενώ το Ethereum χρησιμοποιεί το account model. Αυτή είναι και μια από τις βασικές διαφορές μεταξύ των 2 αυτών blockchain, ενώ τα υπάρχοντα blockchain υϊοθετούν ένα από τα 2 αυτά μοντέλα.

UTXO model

Στο μοντέλο UTXO, τα αχρησιμοποίητα χρήματα αποθηκεύονται σε UTXO. Κάθε συναλλαγή καταναλώνει τα υπάρχοντα UTXO και παράγει νέα UTXO. Ένα UTXO U, περιέχει πληροφορίες όπως η πηγαία διεύθυνση και οι αξίες που έχει αυτή. Για μια συναλλαγή Tx μέσα στο μοντέλο UTXO, το σύνολο των τιμών στην έξοδο του UTXO θα πρέπει να είναι μικρότερο ή ίσο από τις εισόδους του UTXO, δηλαδή:

$$\sum_{U \in Tx\ out} U, v \leq \sum_{U \in Tx\ in} U, v$$

Όπου το U,v αναφέρεται στην τιμή του U και την τιμή του input η οποία συγκεντρώνεται από τους miners ως τα «τέλη εκτέλεσης».

Account model

Στο account model κάθε χρήστης ή συμβόλαιο έχει ένα προκαθορισμένο λογαριασμό και διεύθυνση. Ο λογαριασμός αυτός κρατάει το balance, τους κωδικούς του συμβολαίου και τα διάφορα δεδομένα για να δημιουργηθεί το συμβόλαιο. Το υπόλοιπο Fbalance (a) ενός λογαριασμού ο οποίος αντιστοιχεί σε μια διεύθυνση θα πρέπει να είναι μη αρνητικό. Επιπροσθέτως, για να είναι μια συναλλαγή έγκυρη, το εισαγόμενο ποσό Tx in το οποίο θα ξοδευτεί θα πρέπει να είναι μικρότερο ή ίσο από το υπόλοιπο του λογαριασμού δηλαδή να ισχύει:

$$Fbalance(a) \geq 0, Fvalue(Tx\ in) \leq Fbalance(a)$$

Όπου το Fvalue(Tx in) είναι η τιμή η οποία περιέχεται στο Tx in.

Η δομή των δεδομένων διαφέρει ανάμεσα στα blockchain. Στο μοντέλο UTXO, το Tx in περιέχει ένα σετ από UTXO τα οποία πρόκειται να ξοδευτούν, ενώ στο account model περιέχει την αξία που θα μεταφερθεί. Ακόμη, στο μοντέλο UTXO το Tx out περιέχει ένα νέο σετ UTXO, ενώ στο μοντέλο account περιέχει απαντήσεις και πληροφορίες από την

λαμβάνουσα διεύθυνση (target address), για παράδειγμα τα επιστρεφόμενα μηνύματα από ένα smart contract.

Smart contracts

Ένα smart contract είναι ένα πρόγραμμα Η/Υ C το οποίο χρησιμοποιείται σε blockchain και το οποίο ικανοποιεί την:

$$C(S_i, Tx_i) = (S_i, R_i)$$

Όπου $S = \{S_{i \in N^*}\}$ είναι το σύνολο με όλες τις πιθανές καταστάσεις στο C, το $T = \{T\chi_{\iota \in N^*} = (t, in, out, s, pld)_{i \in N^*}\}$ είναι το σύνολο των συναλλαγών, και $R = \{R_{i \in N^*}\}$είναι το σύνολο όλων των πιθανών απαντήσεων από το συμβόλαιο, για παράδειγμα η επιτυχία ή αποτυχία εκτέλεσης του, ή οποιεσδήποτε άλλες προκαθορισμένες τιμές του. Αφού το C ενεργοποιηθεί από ένα έγκυρο Tx in, η νέα κατάσταση Sj και η απάντηση Ri προκύπτουν από το C.

Ασφάλεια στα smart contracts

Η ασφάλεια στα smart contracts αναφέρεται στην ικανότητα να αντιστέκονται σε μη εξουσιοδοτημένες αλλαγές κατάστασης, οι οποίες μπορεί να είναι μεταφορά κεφαλαίων, αλλαγή της υπάρχουσας κατάστασης (state tampering), και τυχαίας αυτο-καταστροφής.

Ορθότητα στα smart contracts

Η ορθότητα στα smart contracts αναφέρεται στην ικανότητα να μπορούν να ολοκληρώνουν την αναμενόμενη λειτουργικότητα με ορθό τρόπο.

Ασφαλής υπολογισμός από πολλά μέρη (secure multi-party computation).

Σε ένα ασφαλές υπολογιστικό πρωτόκολλο π πολλών μερών, οι συμμετέχοντες P1, P2, P3,…,Pn μπορούν από κοινού να αξιολογήσουν μια πιθανολογική πολυωνυμική συνάρτηση χρόνου f(x1, x2,…, xn)=(y1, y2,…, yn) όπου xi είναι οι κρυφές είσοδοι και yi οι έξοδοι των Pi, για τα οποία ισχύουν:

Ορθότητα: Κάθε Pi βρίσκει το σωστό αποτέλεσμα

Ιδιωτικότητα: Κάθε Pi δεν μπορεί να λάβει περισσότερη πληροφορία εκτός από την δική του είσοδο και έξοδο, ειδικά δε τις εισόδους και εξόδους από άλλους συμμετέχοντες Pj όπου $i \neq j$.

Βιβλιογραφία

Academy Binance. (2020) How Does Blockchain Work [Online]. Available at: https://academy.binance.com/en/articles/how-does-blockchain-work (Accessed at: 23 May 2021)

Academy Binance. (2020) What Is a Blockchain Consensus Algorithm? [Online]. Available at: https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm (Accessed at: 23 May 2021)

Aldweesh, A., Alharby, M., van Moorsel, A., 2018a. Performance benchmarking for Ethereum opcodes. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications. AICCSA, IEEE, pp. 1–2.

Anjana, P.S., Kumari, S., Peri, S., Rathor, S., Somani, A., 2019. An efficient framework for optimistic concurrent execution of smart contracts. In: 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing. PDP, IEEE, pp. 83–92.

Anna Vacca, Andrea Di Sorbo, Corrado A. Visaggio, Gerardo Canfora. 2020. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. The Journal of Systems & Software 174 (2021) 110891

Atzei, N., Bartoletti, M., Lande, S., Yoshida, N., Zunino, R., 2019. Developing secure bitcoin contracts with BitML. In: Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pp. 1124–1128.

Banu, Juhi. (2018) Pros and Cons of Smart Contracts [Online]. Available at: https://atozmarkets.com/news/pros-and-cons-of-smart-contracts/ (Accessed at: 24 May 2021)

Bartoletti, M., Carta, S., Cimoli, T., Saia, R., 2020. Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. Future Gener. Comput. Syst. 102, 259–277.

Bin Hu, Zongyang Zhang, Jianwei Liu,Yizhong Liu, Jiayuan Yin, Rongxing Lu, and Xiaodong Lin. 2020. A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. https://doi.org/10.1016/j.patter.2020.100179

Bragagnolo, S., Rocha, H., Denker, M., Ducasse, S., 2018. Smartinspect: solidity smart contract inspector. In: 2018 International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 9–18.

Bragagnolo, S., Rocha, H., Denker, M., Ducasse, S., 2018b. Ethereum query language. In: Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, pp. 1–8.

Chan, W., Jiang, B., 2018. Fuse: An architecture for smart contract fuzz testing service. In: 2018 25th Asia-Pacific Software Engineering Conference. APSEC, IEEE, pp. 707–708

Chawla, Vishal. (2020) What Are The Top Blockchain Consensus Algorithms? [Online]. Available at: https://analyticsindiamag.com/blockchain-consensus-algorithms/ (Accessed at: 23 May 2021)

Chen, J., Xia, X., Lo, D., Grundy, J., Luo, X., Chen, T., 2020. Defining smart contract defects on Ethereum. IEEE Trans. Softw. Eng. Accesed from https://www.researchgate.net/publication/340684289_Defining_Smart_Contract_Defects_on_Ethereum

Chen, T., Li, X., Luo, X., Zhang, X., 2017. Under-optimized smart contracts devour your money. In: 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering. SANER, IEEE, pp. 442–446.

Chinen, Y., Yanai, N., Cruz, J.P., Okamura, S., 2020. Hunting for re-entrancy attacks in Ethereum smart contracts via static analysis. arXiv preprint arXiv: 2007.01029.

Conway, Luke. (2020) Blockhain Explained [Online]. Available at: https://www.investopedia.com/terms/b/blockchain.asp (Accessed: 23 May 2021)

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., Vera-Rodriguez, R., 2019. Biometric template storage with blockchain: a first look into cost and performance tradeoffs. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops.

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., Hierons, R., 2018. Smart contracts vulnerabilities: a call for blockchain software engineering? In: 2018 International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 19–25.

Ellul, J., Pace, G.J., 2018. Runtime verification of Ethereum smart contracts. In: 2018 14th European Dependable Computing Conference. EDCC, IEEE, pp.158–163

Feist, J., Grieco, G., Groce, A., 2019. Slither: A static analysis framework for smart contracts. In: 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain. WETSEB, IEEE, pp. 8–15.

Frankenfield, Jake. (2020) Cryptographic Hash Functions [Online]. Available at: https://www.investopedia.com/news/cryptographic-hash-functions/ (Accessed at: 23 May 2021)

Fu, Y., Ren, M., Ma, F., Jiang, Y., Shi, H., Sun, J., 2019. EVMFuzz: Differential fuzz testing of Ethereum virtual machine. arXiv preprint arXiv:1903.08483.

Garay, J.A., Kiayias, A., and Leonardos, N. (2015). The bitcoin backbone protocol: analysis and applications. In Advances in Cryptology – EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part II, pp. 281–310.

Geroni, Diego. (2020) What is a public Blockchain [Online]. Available at: https://101blockchains.com/what-is-a-public-blockchain/ (Accessed at: 24 May 2021)

Geroni, Diego. (2021) Top 5 Benefits Of Blockchain Technology [Online]. Available at: https://101blockchains.com/benefits-of-blockchain-technology/ (Accessed at: 24 May 2021)

Gluca (2020) What is a Smart Contract? Advantages and Disadvantages [Online]. Available at: https://content.enkronos.com/what-is-a-smart-contract-advantages-and-disadvantages/ (Accessed at: 24 May 2021)

Gonczol Peter, Katsikouli Panagiota, Herskind Lasse and Nicola Dragoni (2019). Blockchain Implementations and Use Cases for Supply Chains – A Survey [Online]. Available at: https://www.researchgate.net/publication/338467246_Blockchain_Implementations_and_Use_Cases_for_Supply_Chains_-_A_Survey (Accessed: 26 May 2021)

Grech, N., Kong, M., Jurisevic, A., Brent, L., Scholz, B., Smaragdakis, Y., 2018. MadMax: Surviving out-of-gas conditions in Ethereum smart contracts. Proc. ACM Prog. Lang. 2 (OOPSLA), 1–27.

Grybniak, Sergey. (2017) Advantages and Disadvantages of Smart Contracts in Financial Blockchain Systems [Online]. Available at: https://hackernoon.com/advantages-and-disadvantages-of-smart-contracts-in-financial-blockchain-systems-3a443145ae1c (Accessed at: 24 May 2021)

Hegedűs, P., 2019. Towards analyzing the complexity landscape of solidity based Ethereum smart contracts. Technologies 7 (1), 6.

Hooper, Matthew. (2018) Top five blockchain benefits transforming your industry [Online]. Available at: https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/ (Accessed at: 24 May 2021)

Hukkinen, T., Mattila, J., Smolander, K., Seppala, T., Goodden, T., 2019. Skimping on gas–reducing Ethereum transaction costs in a blockchain electricity market application. In: Proceedings of the 52nd Hawaii International Conference on System Sciences.

IBM. (2021) What is Blockchain Technology [Online]. Available at: https://www.ibm.com/topics/what-is-blockchain (Accessed at: 23 May 2021)

Iredale, Gwyneth. (2020) History of Blockchain Technology: A Detailed Guide [Online]. Available at: https://101blockchains.com/history-of-blockchain-timeline/ (Accessed: 23 May 2021)

Iredale, Gwyneth. (2020) Top Disadvantages Of Blockchain Technology [Online]. Available at: https://101blockchains.com/disadvantages-of-blockchain/ (Accessed at: 24 May 2021)

Iredale, Gwyneth. (2021) Hyperledger Fabric Vs Ethereum: Head-to-Head Battle [Online]. Available at: https://101blockchains.com/ethereum-vs-hyperledger-fabric/ (Accessed at: 26 May 2021)

Jiang, B., Liu, Y., Chan, W., 2018. Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, pp. 259–269.

Jiang, Y., Wang, C., Wang, Y., Gao, L., 2019. A privacy-preserving e-commerce system based on the blockchain technology. In: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 50–55.

"Kalra, S., Goel, S., Dhawan, M., Sharma, S., 2018. ZEUS: Analyzing Safety of Smart Contracts. In: NDSS, pp. 1–12. Accessed from http://pages.cpsc.ucalgary.ca/~joel.reardon/blockchain/readings/ndss2018_09-1_Kalra_paper.pdf

Kfoury, E.F., Khoury, D.J., 2018. Secure end-to-end volte based on Ethereum blockchain. In: 2018 41st International Conference on Telecommunications and Signal Processing. TSP, IEEE, pp. 1–5.

Koksal, Ilker. (2019) The Benefits of Applying Blockchain Technology In Any Industry [Online]. Available at: https://www.forbes.com/sites/ilkerkoksal/2019/10/23/the-benefits-of-applying-blockchain-technology-in-any-industry/ (Accessed at: 24 May 2021)

Krause, Elliott (5 July 2018). "A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help". The Wall Street Journal. Retrieved 8 July 2018

Krupp, J., Rossow, C., 2018. TEETHER: Gnawing at Ethereum to automatically exploit smart contracts. In: 27th {USENIX} Security Symposium. {USENIX} Security 18, pp. 1317–1333.

Levi, S., Lipton, A., Skadden. (2018) An Introduction to Smart Contracts and Their Potential and Inherent Limitations [Online]. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (Accessed at 24 May 2021)

Liu, C., Liu, H., Cao, Z., Chen, Z., Chen, B., Roscoe, B., 2018. ReGuard: finding reentrancy bugs in smart contracts. In: 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion. ICSE-Companion, IEEE, pp.65–68.

Liu, X., 2018. A small java application for learning blockchain. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference. IEMCON, IEEE, pp. 1271–1275.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A., 2016. Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 254–269.

Manzoor, A., Hu, Y., Liyanage, M., Ekparinya, P., Thilakarathna, K., Jourjon, G., Seneviratne, A., Kanhere, S., Ylianttila, M.E., 2018. A delay-tolerant payment scheme on the Ethereum blockchain. In: 2018 IEEE 19th International Symposium on ‘‘a World of Wireless, Mobile and Multimedia Networks’’. WoWMoM, IEEE, pp. 14–16.

Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., Tigano, D., 2020. Design patterns for gas optimization in Ethereum. In: 2020 IEEE International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 9–15.

Massessi, Demiro. (2018) Blockchain Public/Private Key Cryptography In a Nutshell [Online]. Available at: https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c (Accessed at: 23 May 2021)

Mavridou, A., Laszka, A., 2018. Designing secure Ethereum smart contracts: A finite state machine based approach. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 523–540.

Mearian, Lucas. (2019) What's a smart contract (and how does it work) [Online]. Available at: https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html (Accessed at: 24 May 2021)

Meng, M.H., Qian, Y., 2018a. A blockchain aided metric for predictive delivery performance in supply chain management. In: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics. SOLI, IEEE, pp. 285–290.

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., Hobor, A., 2018. Finding the greedy, prodigal, and suicidal contracts at scale. In: Proceedings of the 34th Annual Computer Security Applications Conference, pp. 653–663.

Nizamuddin, N., Salah, K., Azad, M.A., Arshad, J., Rehman, M., 2019. Decentralized document version control using Ethereum blockchain and IPFS. Comput. Electr. Eng. 76, 183–197.

Ortu, M., Orrú, M., Destefanis, G., 2019. On comparing software quality metrics of traditional vs blockchain-oriented software: An empirical study. In: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 32–37.

Pass, R., Seeman, L., and Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. In Advances in Cryptology – EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II, pp. 643–673.

Permenev, A., Dimitrov, D., Tsankov, P., Drachsler-Cohen, D., Vechev, M., 2020. VerX: Safety verification of smart contracts. In: 2020 IEEE Symposium on Security and Privacy. SP, pp. 18–20.

Pierro, G.A., Tonelli, R., 2020. PASO: A web-based parser for solidity language analysis. In: 2020 IEEE International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 16–21.

Ranganthan, V.P., Dantu, R., Paul, A., Mears, P., Morozov, K., 2018. A decentralized marketplace application on the Ethereum blockchain. In: 2018 IEEE 4th International Conference on Collaboration and Internet Computing. CIC, IEEE, pp. 90–97.

Rhodes, Delton. (2020) Cryptographic Hash Functions Explained: A Beginner's Guide [Online]. Available at: https://komodoplatform.com/en/blog/cryptographic-hash-function/ (Accessed at: 23 May 2021)

Rosic, Ameer. (2020) Cryptocurrency Wallet Guide: A Step-by-Step Tutorial [Online]. Available at: https://blockgeeks.com/guides/cryptocurrency-wallet-guide/ (Accessed at: 23 May 2021)

Rosic, Ameer. (2020) What is Blockchain Technology? A Step-by-Step Guide For Beginners [Online]. Available at: https://blockgeeks.com/guides/what-is-blockchain-technology/ (Accessed at: 23 May 2021)

Sahu, Mayank. (2020) Hyperledger vs Ethereum: Difference Between Hyperledger and Ethereum [Online]. Available at: https://www.upgrad.com/blog/hyperledger-vs-ethereum-difference-between-hyperledger-and-ethereum/ (Accessed at: 26 May 2021)

Sandner, Philipp. (2017) Comparison of Ethereum, Hyperledger Fabric and Corda [Online]. Available at: https://philippsandner.medium.com/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6 (Accessed at: 26 May 2021)

Sayeed, S., Marco-Gisbert, H., Caira, T., 2020. Smart contract: Attacks and protections. IEEE Access 8, 24416–24427.

Sharma, Toshendra Kumar. (2021) Public vs Private Blockchain, A comprehensive Comparison [Online]. Available at: https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (Accessed at: 24 May 2021)

Sharma, Toshendra Kumar. (2021) Types of Crypto Wallets Explained [Online]. Available at: https://www.blockchain-council.org/blockchain/types-of-crypto-wallets-explained/ (Accessed at: 23 May 2021)

Smith, Chris. (2019) Advantages and Disadvantages of Using Smart Contracts-How to Create a Smart Contract? [Online]. Available at:https://knowtechie.com/advantages-and-disadvantages-of-using-smart-contracts-how-to-create-a-smart-contract/ (Accessed at: 24 May 2021)

Suankaewmanee, K., Hoang, D.T., Niyato, D., Sawadsitang, S., Wang, P., Han, Z., 2018. Performance analysis and application of mobile blockchain. In: 2018 International Conference on Computing, Networking and Communications. ICNC, IEEE, pp. 642–646

Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E.,Alexandrov, Y., 2018. Smartcheck: Static analysis of Ethereum smart contracts. In: Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, pp. 9–16.

Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., Vechev, M.,2018. Securify: Practical security analysis of smart contracts. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 67–82.

Tutorials Point. (2020) Cryptography Tutorial [Online]. Available at: https://www.tutorialspoint.com/cryptography/index.htm (Accessed at: 23 May 2021)

Wang, X., Wu, H., Sun, W., Zhao, Y., 2019. Towards generating cost-effective test-suite for Ethereum smart contract. In: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering. SANER, IEEE, pp. 549–553.

Well, Mark. (2019) Blockchain Public Key & Private Key: A Detailed Guide [Online]. Available at: https://www.mycryptopedia.com/public-key-private-key-explained/ (Accessed at: 23 May 2021)

Wessling, F., Ehmke, C., Meyer, O., Gruhn, V., 2019. Towards blockchain tactics: Building hybrid decentralized software architectures. In: 2019 IEEE International Conference on Software Architecture Companion. ICSA-C, IEEE, pp. 234–237.

Wohrer, M., Zdun, U., 2018. Smart contracts: Security patterns in the Ethereum ecosystem and solidity. In: 2018 International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 2–8.

Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., Vasilakos, A.V., 2019. Designing blockchainbased applications a case study for imported product traceability. Future Gener. Comput. Syst. 92, 399–406.

Yamashita, K., Nomura, Y., Zhou, E., Pi, B., Jun, S., 2019. Potential risks of hyperledger fabric smart contracts. In: 2019 IEEE International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 1–10.

Zhang, P., Yu, J., Ji, S., 2020. ADF-GA: Data flow criterion based test case generation for Ethereum smart contracts Published as a conference paper at 3rd International Workshop on Emerging Trends in Software Engineering for Blockchain, 2020

Zinca, D., Negrean, V.-A., 2018. Development of a road tax payment application using the Ethereum platform. In: 2018 International Symposium on Electronics and Telecommunications. ISETC, IEEE, pp. 1–4.

Παράρτημα: Κατηγοριοποίηση επιλεγμένων άρθρων

A/A	Authors	Title	Year	Είδος Δημοσίευσης	Develop Software-System	Proposal-New algorithm	Proposal- Supply Chain Support Method	Proposal-New System	Proposal Framework	Literature Review-Survey	Δημοσιο/Ιδιωτικο
1	Yiu N.C.K.	Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology	2021	Journal				x			Ανεξάρτητο
2	Galanakis C.M., Rizou M., Aldawoud T.M.S., Ucak I., Rowan N.J.	Innovations and technology disruptions in the food sector within the COVID-19 pandemic and post-lockdown era	2021	Journal						x	
3	Danese P., Mocellin R., Romano P.	Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study	2021	Journal						x	
4	Cakic S., Ismailisufi A., Popovic T., Krco S., Gligoric N., Kupresanin S., Maras V.	Digital Transformation and Transparency in Wine Supply Chain Using OCR and DLT	2021	Conference Paper				x			Ιδιωτικό
5	Saurabh S., Dey K.	Blockchain technology adoption, architecture, and sustainable agri-food supply chains	2021	Journal						x	
6	Baralla G., Pinna A., Tonelli R., Marchesi M., Ibba S.	Ensuring transparency and traceability of food local products: A blockchain application to a Smart Tourism Region	2021	Conference Paper	x						Απροσδιόριστο
9	Matsuyama Y.	Divergence Family Contribution to Data Evaluation in Blockchain Via Alpha-EM and Log-EM Algorithms	2021	Journal						x	
10	Helliar C.V., Crawford L., Rocca L., Teodori C., Veneziani M.	Permissionless and permissioned blockchain diffusion	2020	Journal						x	
12	Hew J.-J., Wong L.-W., Tan G.W.-H., Ooi K.-B., Lin B.	The blockchain-based Halal traceability systems: a hype or reality?	2020	Journal					x		Απροσδιόριστο
14	Miron R., Hulea M., Folea S.	Food Allergens Monitoring System Backed-up by Blockchain Technology	2020	Conference Paper				x			Απροσδιόριστο
17	Miatton F., Amado L.	Fairness, transparency and traceability in the coffee value chain through blockchain innovation	2020	Conference Paper				x			Ιδιωτικό
19	An J., Cheng J., Gui X., Zhang W., Liang D., Gui R., Jiang L., Liao D.	A Lightweight Blockchain-Based Model for Data Quality Assessment in Crowdsensing	2020	Journal					x		Ιδιωτικό

21	Casper H., Jung A., Saberi A., Awwad M.	Blockchain-enabled campus wine supply chain	2020	Conference Paper				x			Δημόσιο
22	Simonis D.	Blockchain, AR changing food and beverage operations	2020	Journal						x	Απροσδιόριστο
23	Cuel R., Cangelosi G.M.	In Vino Veritas? Blockchain Preliminary Effects on Italian Wine SMEs	2020	Conference Paper						x	
26	Lim H.C.	Enterprises and future disruptive technological innovations: Exploring blockchain ledger description framework (BLDF) for the design and development of blockchain use cases	2020	Journal					x		Απροσδιόριστο
29	[No author name available]	Annual conference of the Italian Chapter of AIS, 2019	2020	Conference Review						x	
30	[No author name available]	HAICTA 2020 - Proceedings of the 9th International Conference on Information and Communication Technologies in Agriculture, Food and Environment	2020	Conference Review						x	
31	[No author name available]	International Conference of Modelling and Simulation in Engineering, Economics, and Management, MS 2018	2020	Conference Review						x	
32	Saini D.K., Sandhiyaa B.Y.	Smart City and Challenges	2020	Journal					x		Απροσδιόριστο
33	[No author name available]	3rd International Conference on Computational Intelligence and Informatics, ICCII 2018	2020	Conference Review						x	
34	Rahmah M., Barizah N.	Halal certification of patented medicines in Indonesia in digital age: A panacea for the pain?	2020	Journal					x		Απροσδιόριστο
35	[No author name available]	International Conference on Informatics, Technology and Engineering	2019	Conference Review						x	
36	Spadoni R., Nanetti M., Bondanese A., Rivaroli S.	Innovative solutions for the wine sector: The role of startups	2019	Journal						x	
37	Osmov V., Kurbanniyazov A., Hussain R., Oracevic A., Ahsan Kazmi S.M., Hussain F.	On the blockchain-based general-purpose public key infrastructure	2019	Conference Paper					x		Ανεξάρτητο
38	Hu F., Peng X.-Q.	Research in the Design of Cloud Service Platform for Tea Product Design Based on Consumers' Will in the Background of Blockchain	2019	Conference Paper						x	
39	Matsuyama Y.	Divergence Family Attains Blockchain Applications via α-EM Algorithm	2019	Conference Paper		x					
40	[No author name available]	Proceedings - 2018 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2018	2019	Conference Review						x	
41	Baralla G., Ibba S., Marchesi M., Tonelli R., Missineo S.	A blockchain based system to ensure transparency and reliability in food supply chain	2019	Conference Paper	x						Δημόσιο
42	Hsueh S.-C., Zeng J.-H.	Mobile coupons using blockchain technology	2019	Conference Paper			x				Απροσδιόριστο

44	Ng S., Tauber T.	ECDSA-compatible delegable undeniable signature	2019	Conference Paper			x				Δημόσιο
45	Yadav A., Yadav D., Gupta S., Kumar D., Kumar P.	Online Food Court Payment System using Blockchain Technolgy	2018	Conference Paper				x			Δημόσιο
46	Igarashi T., Watanobe Y.	Distributed authority management method based on blockchains	2018	Conference Paper					x		Απροσδιόριστο
50	Pendrous R.	Blockchain takes off in food and drink	2017	Journal						x	

Η λίστα με όλα τα άρθρα όπως προκύπτει από την βάση δεδομένων του Scopus μπορεί να βρεθεί στο ακόλουθο λινκ:

https://www.scopus.com/results/results.uri?src=s&sot=b&sdt=b&origin=searchbasic&rr=&sl=81&s=TITLE-ABS-KEY(BLOCKCHAIN%20AND%20(WINE%20OR%20BEVERAGES%20OR%20SPIRITS%20OR%20ALCOHOL%20OR%20DRINKS))&searchterm1=BLOCKCHAIN%20AND%20(WINE%20OR%20BEVERAGES%20OR%20SPIRITS%20OR%20ALCOHOL%20OR%20DRINKS)&searchTerms=&connectors=&field1=TITLE_ABS_KEY&fields=