ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ & ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Βιβλιογραφική επισκόπηση μοντέλων αποφάσεων για την επιλογή της τεχνολογίας Blockchain

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεωργίου Μ. Χρίστος

Επιβλέπων: Ασκούνης Δημήτρης
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ & ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Βιβλιογραφική επισκόπηση μοντέλων αποφάσεων για την επιλογή της τεχνολογίας Blockchain

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεωργίου Μ. Χρίστος

Επιβλέπων: Ασκούνης Δημήτρης
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 19η Ιουλίου 2022

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
……	……	……
Ασκούνης Δημήτρης	Ψαράς Ιωάννης	Δούκας Χάρης
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ

Αθήνα, Ιούλιος 2022

(Υπογραφή)
.....

ΓΕΩΡΓΙΟΥ ΧΡΙΣΤΟΣ

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Georgiou Christos,2022.
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Η ραγδαία ανάπτυξη που έχει γνωρίσει η τεχνολογία Blockchain τα τελευταία χρόνια οφείλεται στην επιτυχία της στο χώρο των κρυπτονομισμάτων. Λόγω της αυξανόμενης τάσης της, έχει απασχολήσει και άλλους τομείς εκτός του χρηματοοικονομικού χώρου, για παράδειγμα εκπαίδευση, υγεία, αγορά ακινήτων κ.τ.λ. Εκτός από τα οφέλη που προσφέρει η συγκεκριμένη τεχνολογία, όπως και κάθε ανερχόμενη τεχνολογία, ελλοχεύουν διάφορες προκλήσεις και κίνδυνοι για εφαρμογή της. Για το λόγο αυτό, υπάρχουν αρκετά μοντέλα αποφάσεων που προσπαθούν να κατευθύνουν τους ενδιαφερόμενους προς την κατάλληλη επιλογή.

Στη παρούσα διπλωματική εργασία αναλύονται, μέσω βιβλιογραφικής ανασκόπησης, μοντέλα αποφάσεων, που αξιολογούν την καταλληλότητα της τεχνολογίας Blockchain σε οποιοδήποτε τομέα. Επίσης, βοηθούν στην επιλογή του βέλτιστου τύπου Blockchain (public, private, hybrid, permissioned, permissionless) ανάλογα με τα διάφορα χαρακτηριστικά του κάθε προβλήματος. Στο τέλος, γίνεται μια ανάλυση ως προς την εφαρμογή της συγκεκριμένης τεχνολογίας στην επικύρωση της γνησιότητας τίτλων σπουδών ή άλλων δικαιολογητικών.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Δημόσιο , Ιδιωτικό, Permissioned, Permissionless, Blockchain, Έξυπνα Συμβόλαια, Μοντέλα Αποφάσεων, Επιχειρησιακή Έρευνα, Oracles, Κατακερματισμός, Δέντρα Αποφάσεων, Πιστοποίηση, Ψηφιακές Υπογραφές, Καθολικό

Abstract

The rapid growth of Blockchain technology in recent years is mainly due to its success in the field of cryptocurrencies. Because of its growing trend, it has occupied other domains outside the financial field, such as education, health, real estate etc. The benefits offered by this technology, as any emerging technology, come along with various challenges and risks to its implementation. Taking into account that existing and tested technologies may be a better choice, there are several decision models which try to guide stakeholders towards the proper decision.

The main purpose of this dissertation is to analyze, through a literature review, the decision models that evaluate the eligibility of Blockchain technology in any field and help in selecting the optimal Blockchain type (public, private, hybrid permissioned, permissionless), depending on the different characteristics of each problem. At the end, the implementation of this technology in the validation of diplomas and other documents will be analyzed.

KEY WORDS

Public, Private, Permissioned, Permissionless, Blockchain, Smart Contracts, Decision Models, Operational Research, Hashing, Decision Trees, Certification, Digital Signatures, Ledger

Ευχαριστίες

Με την ολοκλήρωση αυτής της διπλωματικής εργασίας θα ήθελα να ευχαριστήσω θερμά τον κύριο Ασκούνη Δημήτριο, για την εμπιστοσύνη που μου έδειξε και την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα, καθώς και τον κύριο Ζαραφίδη Παναγιώτη για τη καθοδήγηση και υποστήριξη του σε όλες τις φάσεις της διπλωματικής. Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, τους φίλους μου και γενικά όλους όσους βρέθηκαν δίπλα μου και με στήριξαν καθ' όλη διάρκεια των σπουδών μου.

Πίνακας περιεχομένων:

Περίληψη 5

Abstract 7

Ευχαριστίες 9

Πίνακας Εικόνων 13

1 Εισαγωγή 15

2 Συστήματα Αποφάσεων 17

2.1 Λήψη Αποφάσεων 17

2.2 Συστήματα Υποστήριξης Αποφάσεων (ΣΥΑ) 18

2.3 Δέντρα Αποφάσεων 18

3 Τεχνολογία Blockchain 20

3.1 Εισαγωγή στην Τεχνολογία Blockchain 20

3.2 Χαρακτηριστικά του Blockchain 21

3.3 Hashing 23

3.4 Public και Private Key 23

3.5 Smart Contracts 24

3.6 Oracles 25

3.7 Τύποι Blockchain 26

3.7.1 Public 26

3.7.2 Private 27

3.7.3 Διαφορές μεταξύ Private και Public Blockchain 27

4 Συστήματα Αποφάσεων για χρήση της τεχνολογίας Blockchain 29

4.1 Δέντρο Αποφάσεων Cathy Mulligan (April 2018) 29

4.2 Διάγραμμα ροής Karl Wüstl and Arthur Gervais (May 2017) 31

4.3 Δέντρο ροής CompTIA 2019 34

4.4 Ερωτηματολόγιο για την επιλογή permissionless Blockchain, My model (as of Aug.2016) 40

5 Επιλογή προτύπων (Patterns) σε εφαρμογές της Τεχνολογίας Blockchain 41

5.1 Εισαγωγή 41

5.2 Διαδικασία σχεδιασμού εφαρμογών βασισμένες στο blockchain 42
5.3 Διαχείριση και απόδοση δεδομένων εντός αλυσίδας 43
5.3.1 Διαχείριση Δεδομένων 44
5.3.2 Απόδοση 47
5.4 Έλεγχος πρόσβασης δεδομένων εκτός αλυσίδας 48
5.5 Ασφάλεια 49
5.5.1 Έλεγχος Ταυτότητας 49
5.5.2 Εξουσιοδότηση 52
5.6 Αλληλεπίδραση με τον εξωτερικό κόσμο 53
5.7 Έξυπνα Συμβόλαια 56
6 Blockchain για επικύρωση της γνησιότητας τίτλων σπουδών ή άλλων δικαιολογητικών 58
6.1 Εισαγωγή 58
6.2 Προβλήματα αποθήκευσης πιστοποιητικών με υπάρχουσες μεθόδους 59
6.3 Πλεονεκτήματα χρήσης Blockchain για τη διαχείριση πιστοποιητικών 60
6.4 Έκδοση πιστοποιητικών με την χρήση ψηφιακών υπογραφών (Digital Signatures) 61
6.5 Συστήματα διαχείρισης πιστοποιητικών που βασίζονται σε Blockchain 62
6.6 Εφαρμογή Blockchain για έκδοση ψηφιακών πιστοποιήσεων στην εκπαίδευση / Ανάλυση Use case 63
6.6.1 Επιλογή τύπου Blockchain: 63
6.6.2 Ανάλυση της εφαρμογής 65
6.6.3 Επιλογή pattern για πρόσβαση σε δεδομένα εκτός αλυσίδας βάσει της εφαρμογής. 66
7 Επίλογος 68
7.1 Συμπεράσματα 68
7.2 Μελλοντικές επεκτάσεις 68
8 Βιβλιογραφία 69

Πίνακας Εικόνων:

Εικόνα 1, Στάδια Λήψης Αποφάσεων (Πηγή: https://repository.kallipos.gr/handle/11419/1228) 17
Εικόνα 2, Παράδειγμα Δέντρου Απόφασης (Πηγή: https://www.lucidchart.com/pages/decision-tree) 19
Εικόνα 3, Blockchain (Πηγή: https://www.paiementor.com/blockchain-explained-application-payments/) 21
Εικόνα 4, Χαρακτηριστικά Blockchain (Πηγή: https://coingate.com/blog/post/blockchain-explained/characteristics) 22
Εικόνα 5, Hashing (Πηγή: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/) 23
Εικόνα 6, Smart Contracts (Πηγή: https://tallyfy.com/smart-contracts-on-the-blockchain/) 25
Εικόνα 7, Oracles (Πηγή: https://www.seba.swiss/research/Oracles-The%20Internet-of-Blockchains) 26
Εικόνα 8, Τύποι Blockchain (Πηγή: https://link.springer.com/chapter/10.1007/978-3-319-96806-3_8) 28
Εικόνα 9,Cathy Mulligan (April 2018) (Πηγή: https://medium.com/lean-into-blockchain/blockchain-beyond-the-hype-framework-exposed-5c252f529fe3) 29
Εικόνα 10, Karl Wüstl and Arthur Gervais (May 2017) (Πηγή: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1) 32
Εικόνα 11, CompTIA 2019 (Πηγή: https://connect.comptia.org/content/infographic/blockchain-decision-tree) 34
Εικόνα 12, My model (as of Aug.2016) (Πηγή: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1) 40
Εικόνα 13, Σχεδιασμός εφαρμογών Blockchain (Πηγή: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9426788) 42
Εικόνα 14, Διαχείριση και απόδοση δεδομένων εντός αλυσίδας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/performancemodel/) 45
Εικόνα 15, Έλεγχος δεδομένων εκτός αλυσίδας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/datamgnmodel/) 48
Εικόνα 16, Έλεγχος Ταυτότητας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/securitymodel/) 50
Εικόνα 17, Εξουσιοδότηση (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/securitymodel/) 52
Εικόνα 18, Oracle (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/oraclemodel/) 54
Εικόνα 19, Smart Contracts (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/contractmodel/) 56
Εικόνα 20,Πιστοποίηση τίτλων σπουδών με Blockchain (Πηγή: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf) 60
Εικόνα 21,Διαδικασία ψηφιακής υπογραφής εγγράφου (Πηγή: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf) 61
Εικόνα 22, Δέντρο απόφασης για επιλογή τύπου Blockchain στην περίπτωση χρήσης "Επικύρωση τίτλων σπουδών στην εκπαίδευση" 63
Εικόνα 23, Μοντέλο απόφασης για διαχείριση δεδομένων εκτός αλυσίδας για την περίπτωση χρήσης "Επικύρωση τίτλων σπουδών στην εκπαίδευση" (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/datamgnmodel/) 66

1 Εισαγωγή

Ο αυξανόμενος ανταγωνισμός μεταξύ των επιχειρήσεων έφερε στην επιφάνεια τον τομέα της επιχειρησιακής έρευνας, ο οποίος ορίζεται ως το βασικότερο εργαλείο για τη λήψη μιας απόφασης. Η κάθε επιχείρηση για να καταφέρει να παραμείνει βιώσιμη και κερδοφόρα, πρέπει συνεχώς να εξελίσσεται. Αναπόσπαστο κομμάτι της εξέλιξης στις μέρες είναι η χρήση της τεχνολογίας. Για να καταφέρει μια επιχείρηση να έχει συνεχή ανάπτυξη δεν αρκεί μόνο να ενημερώνεται σωστά, αλλά με βάση την υπάρχουσα κατάσταση να λαμβάνει τις κατάλληλες αποφάσεις. Για την επιλογή μιας απόφασης είναι αναγκαίο να γίνουν τέσσερα βασικά στάδια (Πληροφόρηση, Σχεδιασμός, Επιλογή, Υλοποίηση). Τα συστήματα αποφάσεων βασίζονται κυρίως στα πρώτα τρία στάδια της επιχειρησιακής έρευνας. Αρχικά, γίνεται μελέτη για το εκάστοτε πρόβλημα και στην συνέχεια κατασκευάζεται ένα μοντέλο απόφασης ή μελετάται ένα υπάρχον. Τέλος, ανάλογα με τις γνώσεις, τη μελέτη και τα δεδομένα που εμφανίζονται στη ομάδα λήψης αποφάσεων, λαμβάνονται οι κατάλληλες αποφάσεις. Βασικά είδη συστημάτων αποφάσεων που αναλύονται στην παρούσα εργασία είναι τα δέντρα αποφάσεων. Τα όσα αναφέρονται στην συγκεκριμένη παράγραφο αποτελούν το πρώτο μέρος του τόμου.

Βασικός πυλώνας της παρούσας εργασίας είναι η τεχνολογία Blockchain και πως αυτή θα βοηθήσει με τον βέλτιστο τρόπο μια επιχείρηση. Το Blockchain τα τελευταία χρόνια με την επιτυχία του στον χρηματοοικονομικό τομέα, κίνησε το ενδιαφέρον και άλλων τομέων. Πέραν όμως από την επιτυχία και τα ποικίλα οφέλη που μπορεί να προσφέρει το Blockchain, όπως για παράδειγμα αποκέντρωση, διαφάνεια, αμετάβλητο κ.α., σε περίπτωση λανθασμένης επιλογής και ανεπαρκούς ενημέρωσης μπορεί να προξενήσει πολλά προβλήματα στη λειτουργία της κάθε εφαρμογής. Στο δεύτερο μέρος της εργασίας γίνεται εκτενείς ανάλυση και σύγκριση των χαρακτηριστικών των διαφόρων τύπων του Blockchain. Επίσης αναλύεται ο τρόπος λειτουργίας κάποιων βασικών αρχών και λειτουργιών του Blockchain, όπως κατακερματισμός, smart contracts, oracles, ώστε να βοηθήσει τον αναγνώστη να κατανοήσει καλύτερα την μετέπειτα ανάλυση των κεφαλαίων.

Ένα μοντέλο απόφασης είναι ένας τρόπος για να βοηθήσει μια επιχείρηση να κατανοήσει τον τρόπο λειτουργίας του Blockchain καθώς και το ποιο είδος Blockchain ταιριάζει σε κάθε περίπτωση εφαρμογής. Σε

πρώτο στάδιο παρουσιάζονται μοντέλα αποφάσεων που επεξηγούν ανάλογα με τα δεδομένα ποια πρότυπα (patterns) θα πρέπει να ακολουθούνται κατά την λειτουργία της εφαρμογής. Για παράδειγμα, ποια δεδομένα θα αποθηκεύονται εντός και εκτός της αλυσίδας, ανάλογα με το μέγεθος τους.

Με βάση τα χαρακτηριστικά της κάθε επιχείρησης μπορούν να εφαρμοστούν διάφοροι τύποι Blockchain. Δηλαδή, αν το δίκτυο θα είναι αποκεντρωμένο, αν όλοι οι συμμετέχοντες θα μπορούν να προσθέτουν και να επεξεργάζονται δεδομένα εντός του Blockchain, αν υπάρχει εμπιστοσύνη μεταξύ των συμμετεχόντων κ.α. Οι πιο πάνω προδιαγραφές καθορίζουν αν το Blockchain είναι αναγκαίο για την επιχείρηση και ποιο είδος ταιριάζει καλύτερα σε αυτή (permissioned, permissionless, public, private). Όλα τα πιο πάνω αναλύονται μέσα από κάποια μοντέλα αποφάσεων με απώτερο στόχο την σωστή καθοδήγηση του κάθε ενδιαφερόμενου.

Στο τέλος της εργασίας, παρουσιάζεται πώς το Blockchain έρχεται να δώσει λύσεις σε κάποια προβλήματα που νωρίτερα δεν μπορούσαν να ξεπεραστούν σε διαφορετικούς τομείς, για παράδειγμα στην εκπαίδευση. Ένα σημαντικό πρόβλημα που αντιμετώπιζε η εκπαίδευση κατά καιρούς είναι η πλαστογράφηση τίτλων σπουδών. Αυτό το θέμα, δημιουργούσε προβλήματα στα εκπαιδευτικά ιδρύματα, στους υποψήφιους για αγορά εργασίας αλλά και στους εργοδότες. Έτσι, η συγκεκριμένη τεχνολογία με βάση τα χαρακτηριστικά που παρέχει, προτείνει στα εκπαιδευτικά ιδρύματα τρόπους για εξάλειψη του συγκεκριμένου προβλήματος.

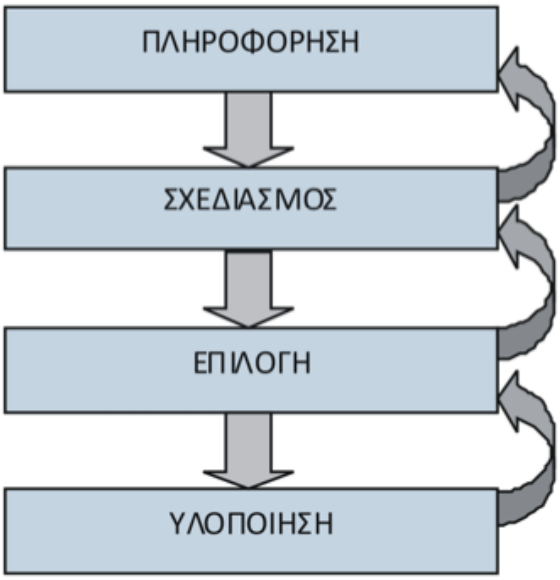
2 Συστήματα Αποφάσεων

2.1 Λήψη Αποφάσεων

Η λήψη αποφάσεων στις επιχειρήσεις είναι μια διαδικασία όπου συλλέγονται διάφορες προτάσεις για την λύση ενός προβλήματος, με απώτερο στόχο την επιλογή της καλύτερης [5].

Ο τομέας που ασχολείται με την παραπάνω διαδικασία είναι η επιχειρησιακή έρευνα, η οποία περιλαμβάνει κάποιες ενέργειες. Πιο συγκεκριμένα, αναζητούνται τα προβλήματα που υπάρχουν και προτείνονται λύσεις, οι οποίες παρουσιάζονται και αναλύονται με την βοήθεια των συστημάτων αποφάσεων, τα οποία θα επεξηγηθούν παρακάτω. Σύμφωνα με τις δοκιμές των προτεινόμενων μοντέλων εξάγεται μια λύση, όπου δοκιμάζεται και εφαρμόζεται ώστε να διορθώσει τα προβλήματα και τις αδυναμίες σε μια επιχείρηση [2].

Στο παρακάτω σχήμα φαίνεται το σχεδιάγραμμα του Herbert Simon με τα τέσσερα βασικά στάδια λήψης μιας απόφασης.



Εικόνα 1, Στάδια Λήψης Αποφάσεων (Πηγή: https://repository.kallipos.gr/handle/11419/1228)

Με βάση αυτό το σχεδιάγραμμα το κάθε στάδιο εξαρτάται από τα υπόλοιπα. Στο στάδιο της πληροφόρησης, γίνεται ο καθορισμός τους προβλήματος και γίνεται έρευνα για το τρέχον πρόβλημα. Στο δεύτερο

στάδιο, συλλέγονται όλες οι αποφάσεις που είναι πιθανόν να οδηγήσουν στην λύση του προβλήματος. Στο στάδιο επιλογή, σύμφωνα με τις δοκιμές και τις μελέτες που έγιναν για τις προτεινόμενες διαδικασίες επιλέγεται η πιο συμφέρουσα λύση. Τέλος στο στάδιο της υλοποίησης, εφαρμόζεται η επιλεγμένη απόφαση και τίθεται σε διαδικασία υλοποίησης [3].

2.2 Συστήματα Υποστήριξης Αποφάσεων (ΣΥΑ)

Η ανάγκη των ανθρώπων να καταλήξουν στην ορθότερη λήψη μιας απόφασης σε μία επιχείρηση οδήγησε στην εμφάνιση των Συστημάτων Υποστήριξης Αποφάσεων. Στην ουσία τα ΣΥΑ κατευθύνουν τους υπευθύνους λήψης αποφάσεων στο πως να χρησιμοποιούν δεδομένα και καταστάσεις για να καταλήξουν στην επιθυμητή επιλογή[4].

Κάποια από τα είδη συστημάτων αποφάσεων είναι τα δέντρα αποφάσεων, τα διαγράμματα ροής, οι Πολυκριτηριακές μέθοδοι αποφάσεων, ο γραμμικός προγραμματισμός και ο δυναμικός προγραμματισμός. Στην παρούσα διπλωματική θα αναπτυχθούν τα δέντρα αποφάσεων και τα διαγράμματα ροής, όπου βασίζονται τα μοντέλα αποφάσεων που αναλύονται στα επόμενα κεφάλαια.

2.3 Δέντρα Αποφάσεων

Ένα δέντρο αποφάσεων είναι μια διαγραμματική απεικόνιση πιθανών αποτελεσμάτων προερχόμενα από μια σειρά σχετικών επιλογών. Το άτομο ή ο οργανισμός που το μελετά έχει την δυνατότητα να σταθμίσει πιθανές ενέργειες μεταξύ τους με βάση το κόστος, τα οφέλη και τις πιθανότητες. Το βασικό δομικό στοιχείο ενός δέντρου απόφασης είναι ο κόμβος, από τον οποίο αρχίζει το δέντρο και διακλαδώνεται σε διάφορα πιθανά αποτελέσματα. Κάθε ένα από τα πιθανά αποτελέσματα οδηγούνται σε πρόσθετους κόμβους, οι οποίοι διακλαδώνονται σε άλλες καταστάσεις. Υπάρχουν τρείς διαφορετικοί τύποι κόμβων [5], [6].

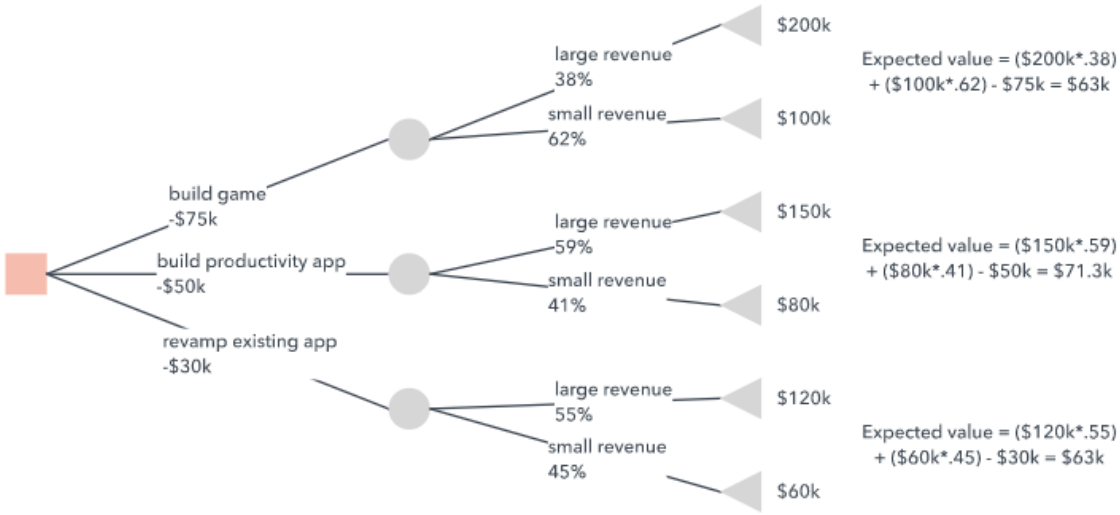
i. Οι κόμβοι πιθανότητας, οι οποίοι αναπαρίστανται σχηματικά με έναν κύκλο, δείχνοντας ορισμένα πιθανά αποτελέσματα.

ii. Οι κόμβοι απόφασης, οι οποίοι αναπαρίστανται σχηματικά με ένα τετράγωνο, παρουσιάζουν μια απόφαση η οποία πρέπει να ληφθεί.

iii. Ο τερματικός κόμβος, δείχνει το τελικό αποτέλεσμα μιας διαδρομής απόφασης.

Όλοι οι παραπάνω κόμβοι συνδέονται μεταξύ τους σχηματίζοντας κλάδους, υποδεικνύοντας ένα πιθανό αποτέλεσμα ή μια ενέργεια [7], [8].

Παρακάτω, παρουσιάζεται ένα τυπικό παράδειγμα δέντρου αποφάσεων όπου αναπτύσσονται τρείς καταστάσεις που ενδεχομένως να επιφέρουν κέρδος σε μια εταιρία ανάπτυξης και υποστήριξης λογισμικού. Βάσει του δέντρου αποφάσεων, με την ανάπτυξη του λογισμικού ενός παιχνιδιού υπάρχει πιθανότητα υψηλών εσόδων 38% με κέρδος $200.000 και χαμηλών εσόδων 62% με κέρδος $100.000. Με βάση τις πιθανότητες, τα κέρδη και τα έξοδα της κάθε περίπτωσης υπολογίζεται η αναμενόμενη αξία της κάθε εφαρμογής. Έτσι οι υπεύθυνοι λήψης αποφάσεων επιλέγουν τον κατάλληλο κλάδο του δέντρου που θα φέρει τα βέλτιστα αποτελέσματα για την επιχείρηση. Στην προκειμένη περίπτωση βάση των υπολογισμών και των τριών κλάδων, η κατάλληλη επιλογή είναι ο δεύτερος κλάδος του δέντρου.



Εικόνα 2, Παράδειγμα Δέντρου Απόφασης (Πηγή: https://www.lucidchart.com/pages/decision-tree)

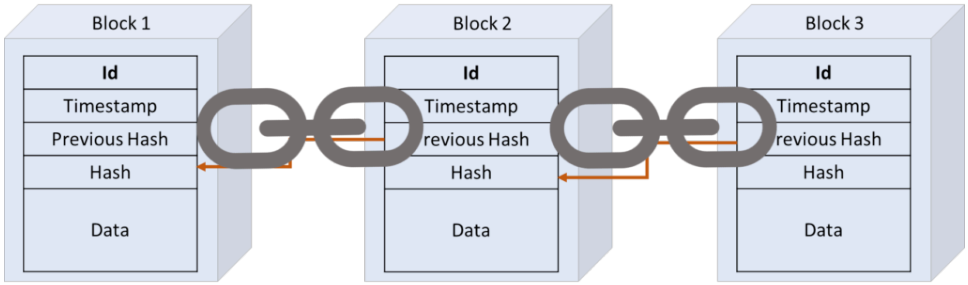
3 Τεχνολογία Blockchain

3.1 Εισαγωγή στην Τεχνολογία Blockchain

Στις μέρες μας η τεχνολογία Blockchain, με τις πρωτοπόρες ιδιότητες της, έχει καταφέρει να διεισδύσει για τα καλά στη σύγχρονη οικονομία. Ο κύριος λόγος που κατάφερε να κερδίσει αυτή την αναγνώριση, είναι το Bitcoin και ο τρόπος λειτουργίας του, αφού κατέρριψε πολλά στερεότυπα γύρω από το χώρο της οικονομίας και ειδικότερα των χρηματοπιστωτικών συναλλαγών. Το σπουδαίο γύρω από αυτή τη τεχνολογία είναι ότι δεν υποστηρίζεται από μια κεντρική αρχή, αλλά από ένα αυτοματοποιημένο αλγόριθμο συναίνεσης μεταξύ των χρηστών που βρίσκονται στο δίκτυο. Πιο συγκεκριμένα, το Bitcoin είναι ψηφιακό νόμισμα που διακινείται μέσα στο διαδίκτυο σε ένα αποκεντρωμένο σύστημα, χρησιμοποιώντας ένα δημόσιο καθολικό (ledger), το Blockchain.

Το Blockchain είναι μια κατανεμημένη βάση δεδομένων που διατηρεί ένα αμετάβλητο (immutability) καθολικό αποθηκεύοντας όλα τα δεδομένα των συναλλαγών που πραγματοποιούνται κάθε φορά σε ένα ξεχωριστό block και ο κάθε χρήστης διατηρεί ένα αντίγραφο αυτού. Το κάθε block χωρίζεται σε δύο μέρη, το σώμα (body) και την κεφαλίδα (header). Στο σώμα κατανέμονται όλα τα δεδομένα (π.χ. γεγονότα και συναλλαγές) και στην κεφαλίδα αποθηκεύονται η χρονική σφραγίδα (timestamp), ο κατακερματισμός των συναλλαγών (hashing) και ο κρυπτογραφημένος κατακερματισμός του προηγούμενου, διατηρώντας έτσι το αμετάβλητο του κάθε block. Είναι σημαντικό να επεξηγηθούν οι όροι hashing και timestamp, αφού θα βοηθήσουν την περαιτέρω κατανόηση του τρόπου λειτουργίας της συγκεκριμένης τεχνολογίας. Μια συνάρτηση κατακερματισμού είναι ένας αλγόριθμος που δέχεται ως είσοδο δεδομένα και παράγει έξοδο μια μονόδρομη στοιχειοσειρά (string) που δεν μπορεί να αλλάξει. Η χρονική σφραγίδα εμφανίζεται την ώρα που δημιουργείται το block, η οποία είναι μοναδική και συμμετέχει στον κατακερματισμό πιστοποιώντας το χρόνο της συναλλαγής. Καθώς αυξάνονται οι εγγραφές, το κάθε block συνδέεται με το επόμενο με μια γραμμική χρονολογική σειρά δημιουργώντας μια αλυσίδα. Με αυτό τον τρόπο το κάθε block της αλυσίδας είναι άρρηκτα συνδεδεμένο με το προηγούμενο αλλά και το επόμενο block, με αποτέλεσμα η παραβίαση ή αλλοίωση της αλυσίδας να είναι μια απίθανη διαδικασία [9], [10].

Η παραπάνω διαδικασία δημιουργεί ένα ομότιμο κατανεμημένο δίκτυο (peer to peer network), κατά το οποίο οι χρήστες αλληλοεπιδρούν μεταξύ τους, χωρίς την ανάγκη συμβολής ενός έμπιστου μεσολαβητή, με αξιόπιστο τρόπο. Έτσι, εφαρμογές που μέχρι πρότινος λειτουργούσαν κάτω από μια κεντρική αρχή, μπορούν με το ίδιο επίπεδο αυθεντικότητας να λειτουργούν αποκεντρωμένα (decentralized) χωρίς την ύπαρξη αυτής [11].



Εικόνα 3, Blockchain (Πηγή: https://www.paiementor.com/blockchain-explained-application-payments/)

3.2 Χαρακτηριστικά του Blockchain

- Ένα από τα κύρια χαρακτηριστικά της τεχνολογίας Blockchain είναι το **αμετάβλητο** (immutability), διασφαλίζοντας ότι το δίκτυο παραμένει ως έχει. Σε αντίθεση με ένα τυπικό τραπεζικό σύστημα που βασίζεται σε κεντρικές αρχές, αυτό εξασφαλίζει το αμετάβλητο με την συλλογή κόμβων. Κάθε κόμβος έχει αντίγραφο του ψηφιακού καθολικού. Για να προστεθεί μια συναλλαγή κάθε κόμβος θα πρέπει να ελέγξει την εγκυρότητα του. Εάν η πλειοψηφία θεωρεί ότι είναι έγκυρη, τότε προστίθεται στο βιβλίο. Αυτό προάγει την διαφάνεια και το καθιστά ανθεκτικό στη διαφθορά. Έτσι χωρίς την συγκατάθεση της πλειοψηφίας κανείς δεν μπορεί να προσθέσει μπλοκ στο καθολικό. Ένα άλλο γεγονός που ενισχύει αυτό το χαρακτηριστικό, είναι ότι μόλις προστεθεί ένα μπλοκ συναλλαγών, κανείς δεν μπορεί να επιστρέψει και να το αλλάξει. Έτσι, κανένας χρήστης στο δίκτυο δεν θα μπορεί να επεξεργαστεί, να διαγράψει ή να ενημερώσει ένα μπλοκ.

- Το δίκτυο μπορεί να είναι **αποκεντρωμένο**, δηλαδή να μην υπάρχει καμιά διοικούσα αρχή που να φροντίζει τη δομή του. Καθώς το σύστημα δεν χρειάζεται καμία διαχειριστική αρχή, ο κάθε χρήστης μπορεί να έχει άμεση πρόσβαση, να αποθηκεύει τα δεδομένα του και με τη βοήθεια του private key να έχει άμεσο έλεγχο σε αυτά. Έτσι, οι χρήστες έχουν πλήρη

έλεγχο των ιδιοτήτων τους χωρίς να βασίζονται σε τρίτα μέρη για να διατηρήσουν τα περιουσιακά τους στοιχεία. Επίσης, με την αποκέντρωση μειώνονται τυχόν σφάλματα και απάτες, αφού όλα είναι αυτοματοποιημένα και κανένας δεν μπορεί να επέμβει. Το αποκεντρωμένο blockchain μπορεί να επιβιώσει από κακόβουλες επιθέσεις λόγω του ότι χρειάζονται αρκετές δαπάνες από τους hackers να το αλλοιώσουν.

- Η χρήση κρυπτογράφησης μαζί με την αποκέντρωση εξασφαλίζει **ασφάλεια** στο δίκτυο, αφού λειτουργεί ως τείχος προστασίας από επιθέσεις. Κάθε πληροφορία για το blockchain κατακερματίζεται (hashing). Όλα τα μπλοκ στο καθολικό διαθέτουν το μοναδικό τους hash καθώς και το hash του προηγούμενου μπλοκ. Έτσι, η αλλαγή ή η προσπάθεια παραβίασης των δεδομένων θα σημαίνει αλλαγή όλων των ταυτοτήτων του κατακερματισμού, κάτι που είναι σχεδόν αδύνατον. Εάν κάποιος θέλει να καταστρέψει το δίκτυο, θα πρέπει να αλλάξει όλα τα δεδομένα που είναι αποθηκευμένα στον κόμβο του δικτύου και η παραβίαση εκατομμυρίων υπολογιστών είναι σχεδόν αδύνατη και δαπανηρή.

- Σε κάθε blockchain λειτουργεί με **συναίνεση (consensus)**, η οποία λειτουργεί σαν μια διαδικασία λήψης αποφάσεων για την ομάδα των κόμβων που δραστηριοποιούνται στο δίκτυο. Όταν εκατομμύρια κόμβοι πρέπει να επικυρώσουν μια συναλλαγή είναι απολύτως απαραίτητη η συναίνεση για να λειτουργήσει σωστά ένα σύστημα. Είναι σαν ένα είδος ψηφοφορίας όπου η πλειοψηφία κερδίζει και η μειοψηφία πρέπει να το υποστηρίξει. Οι κόμβοι μπορεί να μην εμπιστεύονται ο ένας τον άλλον, αλλά εμπιστεύονται τους αλγορίθμους συναίνεσης που λειτουργούν [12], [13].

Εικόνα 4, Χαρακτηριστικά Blockchain (Πηγή: https://coingate.com/blog/post/blockchain-explained/characteristics)

3.3 Hashing

Ο κατακερματισμός (hashing) είναι μια συνάρτηση που λειτουργεί για να υπογράψει ένα ψηφιακό έγγραφο ή μια συναλλαγή. Το hashing δηλαδή, είναι υπεύθυνο για την προστασία από παραβιάσεις, γιατί γίνει οποιαδήποτε αλλαγή στην συναλλαγή ή στο έγγραφο, δημιουργείται ένα διαφορετικό αναγνωριστικό.

Εικόνα 5, Hashing (Πηγή: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/)

Οι κατακερματισμοί είναι μονόδρομοι. Αυτό σημαίνει ότι η γεννήτρια κατακερματισμού μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός κατακερματισμού από το έγγραφο, αλλά είναι μαθηματικά αδύνατο να δημιουργηθεί ένα έγγραφο από έναν κατακερματισμό. Σε ένα blockchain, κάθε μπλοκ συναλλαγών διασφαλίζεται με τη συμπερίληψη ενός κατακερματισμού του μπλοκ πληροφοριών, καθώς και του προηγούμενου μπλοκ, επιτρέποντας έτσι σε όλα τα μέρη να εγγυηθούν ότι καμία από τις συναλλαγές δεν έχει τροποποιηθεί ή παραποιηθεί [14].

3.4 Public και Private Key

Ένα δημόσιο κλειδί (public key) είναι ουσιαστικά ένας δημόσια διαθέσιμος αριθμός ταυτότητας που μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός ατόμου. Ένα ιδιωτικό κλειδί (private key) είναι ουσιαστικά ένας κωδικός πρόσβασης, ο οποίος έχει συνδεθεί μαθηματικά με το δημόσιο κλειδί.

Όταν χρησιμοποιείτε ζεύγος δημόσιων/ιδιωτικών κλειδιών, ένας χρήστης μπορεί να πιστοποιήσει ότι είναι πραγματικά ο κάτοχος ενός δημόσιου κλειδιού εισάγοντας τα στοιχεία του ιδιωτικού κλειδιού στο λογισμικό. Αυτό, με τη σειρά του, θα ελέγξει εάν τα δύο κλειδιά είναι

πραγματικά μαθηματικά συνδεδεμένα. Αυτή η συνάρτηση δεν μπορεί πρακτικά να εκτελεστεί αντίστροφα, δηλαδή είναι σχεδόν αδύνατο να δημιουργηθεί το ιδιωτικό κλειδί εάν κάποιος έχει πληροφορίες μόνο για το δημόσιο κλειδί [15].

3.5 **Smart Contracts**

Τα έξυπνα συμβόλαια (smart contracts) είναι απλά προγράμματα αποθηκευμένα σε ένα blockchain που λειτουργούν όταν πληρούνται οι συνθήκες που προκαθορίζονται. Συνήθως, χρησιμοποιούνται για να αυτοματοποιείται η εκτέλεση μιας συμφωνίας, έτσι ώστε οι συμμετέχοντες να είναι άμεσα ενήμεροι και να διαβεβαιώνονται ότι όντως εκτελέστηκε η συμφωνία, χωρίς την επέμβαση ενδιάμεσου προσώπου. Επίσης, μπορούν να αυτοματοποιούν μια ροή εργασίας, δηλαδή όταν πληροί τις προϋποθέσεις η προηγούμενη ενέργεια να ενεργοποιείται η επόμενη. Μέσα σε ένα έξυπνο συμβόλαιο μπορεί να υπάρχουν όσες προϋποθέσεις χρειάζονται για να ικανοποιηθούν οι συμμετέχοντες, τις οποίες καθορίζουν οι ίδιοι. Τα κυριότερα πλεονεκτήματα που παρέχονται από τα έξυπνα συμβόλαια είναι: [16], [17]

- Ταχύτητα, αποτελεσματικότητα και ακρίβεια: Μόλις ολοκληρωθεί μια προϋπόθεση, η σύμβαση εκτελείται αμέσως, λόγω του ότι τα έξυπνα συμβόλαια είναι ψηφιακά και αυτοματοποιημένα.

- Εμπιστοσύνη και διαφάνεια: Επειδή δεν εμπλέκεται τρίτο μέρος και τα κρυπτογραφημένα αρχεία μοιράζονται στους συμμετέχοντες, δεν μπορεί να αμφισβητηθεί εάν οι πληροφορίες έχουν τροποποιηθεί για προσωπικό όφελος της οποιασδήποτε πλευράς.

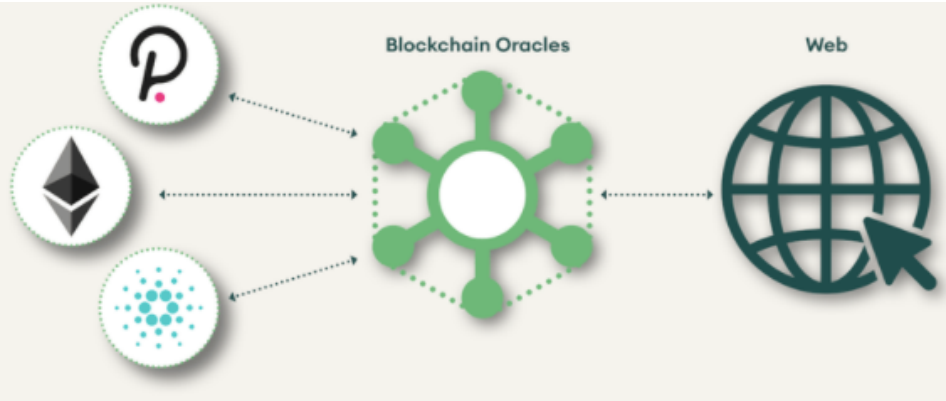
- Ασφάλεια: Τα αρχεία συναλλαγών σε ένα Blockchain είναι κρυπτογραφημένα και αλληλεξαρτώμενα εντός της αλυσίδας, με αποτέλεσμα να είναι πολύ δύσκολο να τα αλλάξει κάποιος κακόβουλα.

- Τα έξυπνα συμβόλαια καταργούν την ανάγκη μεσολαβητών για να χειρίζονται τις συναλλαγές, έτσι εξαλείφονται χρονικές καθυστερήσεις και χρεώσεις.

Εικόνα 6, Smart Contracts (Πηγή: https://tallyfy.com/smart-contracts-on-the-blockchain/)

3.6 Oracles

Τα Oracles του Blockchain αναλαμβάνουν στην ουσία το ρόλο του μεσολαβητή σε μια συναλλαγή. Παρέχουν εξωτερικές πληροφορίες σε έξυπνα συμβόλαια και γεφυρώνουν τις εφαρμογές του εξωτερικού κόσμου με τις υπηρεσίες που παρέχει το Blockchain. Στην ουσία τα oracles επιτρέπουν στο δίκτυο να έχει τον κατάλληλο τρόπο πρόσβασης σε δεδομένα εντός και εκτός αλυσίδας. Από την κατασκευή τους τα Blockchains δεν μπορούν να έχουν πρόσβαση σε δεδομένα που δεν βρίσκονται στην αλυσίδα, δηλαδή εκτός δικτύου.. Η δυνατότητα πρόσβασης σε δεδομένα εκτός αλυσίδας βελτιώνει και την λειτουργικότητα των έξυπνων συμβάσεων. Με άλλα λόγια το oracle είναι ένα επίπεδο λύσης που επαληθεύει πηγές δεδομένων που βρίσκονται έξω από το δίκτυο και μόλις το κάνει, αυτή τη διεργασία μεταδίδει αυτές τις πληροφορίες εντός του δικτύου. Για παράδειγμα, δύο οντότητες στοιχηματίζουν για το πότε θα ξεκινήσει ο εμβολιασμός για τον COVID-19, για να έχουν την καλύτερη δυνατή διαφάνεια στο στοιχηματισμό τους, δημιουργούν ένα smart contract, όπου έχουν θέσει τους κανόνες για το στοίχημα. Για να λειτουργήσει σωστά όμως πρέπει να δέχεται πληροφορίες από εξωτερικές πηγές, στην προκειμένη περίπτωση πότε ξεκίνησε ο εμβολιασμός. Έτσι, το oracle τροφοδοτεί δεδομένα στο έξυπνο συμβόλαιο διασφαλίζοντας εμπιστοσύνη και ασφάλεια μεταξύ των δύο οντοτήτων [17], [18].



Εικόνα 7, Oracles (Πηγή: https://www.seba.swiss/research/Oracles-The%20Internet-of-Blockchains)

3.7 Τύποι Blockchain

Ανάλογα με τις προδιαγραφές της κάθε εφαρμογής, το blockchain προσαρμόζεται για να είναι όσο το δυνατό πιο λειτουργικό. Η επιλογή του κάθε τύπου εξαρτάται από κάποιους βασικούς παράγοντες. Πρώτον, αν το βιβλίο θα είναι κατανεμημένο, δηλαδή ένα είδος βάσης δεδομένων που έχει την δυνατότητα να μοιράζεται και να αναπαράγει δεδομένα από πολλαπλά σημεία χωρίς να υπάρχει κεντρικός διαχειριστής. Δεύτερον, ποιοι χρήστες θα έχουν πρόσβαση σε αυτό και ποια θα είναι οι αρμοδιότητα τους [19].

3.7.1 Public

Το δημόσιο Blockchain είναι χωρίς άδεια χρήσης, δηλαδή ο οποιασδήποτε έχει την δυνατότητα να συμμετέχει στο δίκτυο, να παρακολουθήσει συναλλαγές και δεδομένα, να γράψει στο blockchain και να συμμετέχει στην διαδικασία επαλήθευσης και επικύρωσης συναλλαγών χωρίς την οποιαδήποτε έγκριση. Αυτοί είναι και οι λόγοι που ένα public blockchain είναι αποκεντρωμένο και καμία οντότητα δεν ελέγχει το δίκτυο. Τα δεδομένα εντός του δικτύου δεν μπορούν να τροποποιηθούν ή για να γίνει αυτό πρέπει να υπάρξει επικύρωση από τους υπόλοιπους χρήστες. Αν κάποιος κακόβουλος χρήστης προσπαθήσει να τροποποιήσει κάποια δεδομένα θα πρέπει να έχει μεγαλύτερη υπολογιστική ισχύ από αυτήν του δικτύου, πράγμα που στα δημόσια blockchain είναι σχεδόν αδύνατο, λόγω του μεγάλου αριθμού συμμετεχόντων στο κατανεμημένο. Τα πιο γνωστά παραδείγματα αυτού του τύπου είναι το Bitcoin και το Ethereum [20], [21].

3.7.2 Private

Τα ιδιωτικά Blockchains είναι πολύ πιο μικρά σε σχέση με τα δημόσια. Για να έχει κάποιος χρήστης δικαίωμα συμμετοχής σε αυτό πρέπει να γίνει έλεγχος πρόσβασης από μια κεντρική αρχή. Όσον αφορά τα λειτουργικά του χαρακτηριστικά είναι ταχύτερα και δεν παρουσιάζουν καμία καθυστέρηση στο χρόνο επικύρωσης δεδομένων σε σχέση με άλλα είδη. Επίσης, έχουν χαμηλό κόστος λειτουργίας και δεν χρειάζεται μεγάλο χρονικό διάστημα για να κατασκευαστούν. Σε σχέση όμως με ένα δημόσιο blockchain δεν εξασφαλίζεται το ίδιο επίπεδο ασφάλειας. Αυτό το είδος blockchain χωρίζεται σε δύο κατηγορίες με βάση την άδεια χρήσης. Η πρώτη είναι χωρίς άδεια χρήσης, όπου ο οποιοσδήποτε μπορεί να συμμετέχει σε όλες τις διεργασίες και να συμβάλει στην ανάπτυξη του. Η δεύτερη είναι με άδεια χρήσης, όπου για την διαχείριση της επικύρωσης των συναλλαγών απαιτείται έγκριση από κάποια συγκεκριμένη οντότητα. Αυτό οδηγεί την εξάρτηση από τρίτους για συναλλαγές, στις οποίες έχουν γνώση μόνο όσοι έχουν συμμετέχουν σε αυτές [21].

3.7.3 Διαφορές μεταξύ Private και Public Blockchain

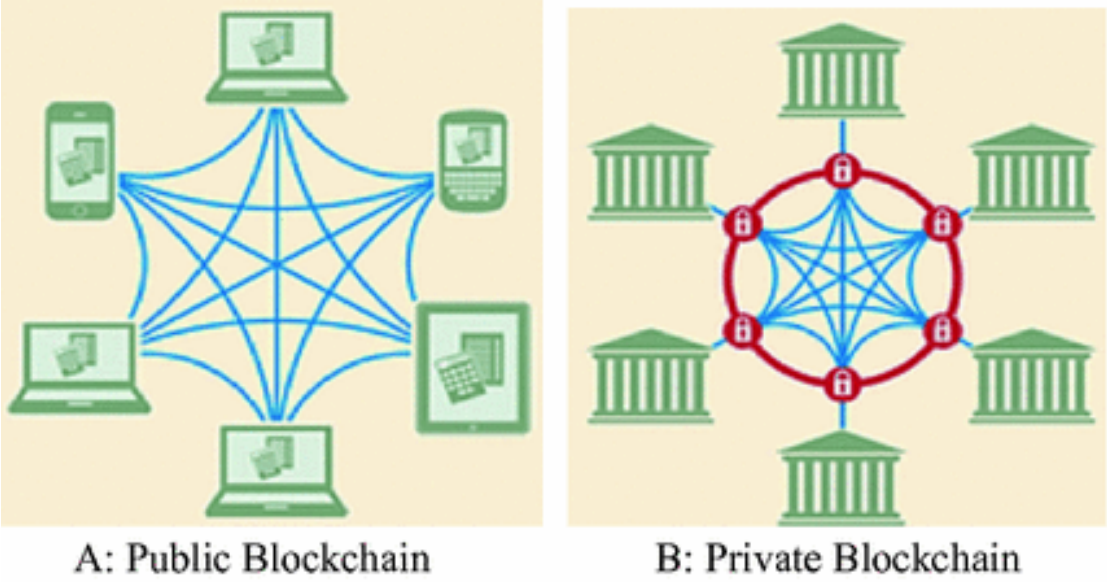
- Όσον αφορά το επίπεδο πρόσβασης προς τους συμμετέχοντες, σε ένα δημόσιο blockchain, ο καθένας μπορεί να λάβει μέρος επαληθεύοντας και προσθέτοντας δεδομένα σε αυτό. Σε ιδιωτικά blockchains, μόνο όσοι εξουσιοδοτούνται μπορούν να συμμετέχουν και να ελέγχουν το δίκτυο.

- Ένα δημόσιο blockchain είναι αποκεντρωμένο, ενώ ένα ιδιωτικό είναι πιο συγκεντρωτικό.

- Σε ένα δημόσιο blockchain, ο αριθμός των συναλλαγών που εκτελούνται ανά δευτερόλεπτο είναι πολύ λιγότερος σε σύγκριση με το ιδιωτικό. Αυτό οφείλεται στο λόγο ότι στα private blockchains ο αριθμός των εξουσιοδοτημένων συμμετεχόντων είναι μικρότερος, άρα μικρότερη καθυστέρηση στη διαδικασία της συναλλαγής.

- Τα ιδιωτικά blockchains καταναλώνουν λιγότερη ενέργεια σε σχέση με τα δημόσια, αυτό οφείλεται στο ότι ένα δημόσιο blockchain για να λειτουργήσει και να επιτευχθεί συναίνεση δικτύου απαιτεί σημαντική ποσότητα ηλεκτρικών πόρων, λόγω του τεράστιου όγκου δεδομένων και συμμετεχόντων σε αυτό.

- Σε ένα δημόσιο blockchain λόγω του τεράστιου αριθμού κόμβων στο δίκτυο, είναι σχεδόν αδύνατο από κακόβουλους χρήστες να επιτεθούν στο σύστημα και να αποκτήσουν τον έλεγχο του αλγόριθμου συναίνεσης. Ενώ, ένα ιδιωτικό blockchain είναι πιο επιρρεπές σε κινδύνους και παραβιάσεις δεδομένων [21].

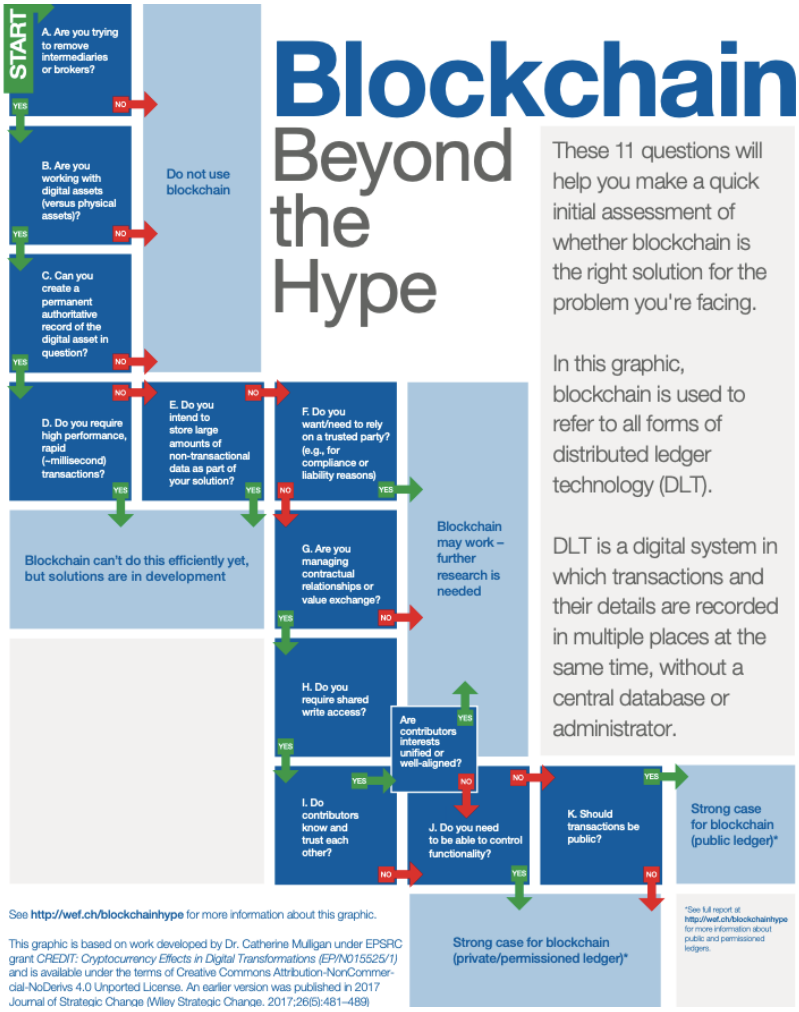


Εικόνα 8, Τύποι Blockchain (Πηγή: https://link.springer.com/chapter/10.1007/978-3-319-96806-3_8)

4 Συστήματα Αποφάσεων για χρήση της τεχνολογίας Blockchain

4.1 Δέντρο Αποφάσεων Cathy Mulligan (April 2018)

Ένα δέντρο απόφασης, του Cathy Mulligan, όπως αναλύθηκε τον Απρίλιο του 2018, έχει τεράστια συμβολή στην επιλογή της όσο το δυνατόν καταλληλότερης λύσης για ένα καθορισμένο πρόβλημα στον επιχειρησιακό τομέα. Αυτό, δεν εξασφαλίζει την απόλυτη εγκυρότητα της τελικής απάντησης, αλλά στην παροχή βοήθειας στους υπεύθυνους λήψης αποφάσεων, μειώνοντας ταυτόχρονα τον κίνδυνο λανθασμένων πειραματισμών.



Εικόνα 9,Cathy Mulligan (April 2018) (Πηγή: https://medium.com/lean-into-blockchain/blockchain-beyond-the-hype-framework-exposed-5c252f529fe3)

Το παραπάνω εργαλείο, Cathy Mulligan (April 2018), αποτελείται από μια σειρά ερωτήσεων που βοηθούν τον χρήστη να καταλάβει αν το Blockchain είναι μια σωστή προσέγγιση για την ανάλογη περίπτωση χρήσης. Περαιτέρω, η ανάλυση των ερωτήσεων που φαίνονται στο δέντρο, θα δώσει απαντήσεις για το ποια μορφή τεχνολογίας κατανεμημένου καθολικού θα πρέπει να επιλεχθεί. Σε κάποια άλλη περίπτωση, δίνει την απάντηση αν και πως η συγκεκριμένη τεχνολογία θα φανεί χρήσιμη με την πάροδο του χρόνου.

- Οι πρώτες τρείς ερωτήσεις (A-C) αποσκοπούν στο να κάνουν τον αναγνώστη να καταλήξει εάν όντως θα πρέπει να χρησιμοποιήσει το blockchain για να λύσει το πρόβλημα. Συγκεκριμένα, ρωτάει αν είναι προς το όφελος της επιχείρησης η αφαίρεση τρίτων προσώπων-μεσολαβητών από αυτήν. Δηλαδή, εάν θα ήταν καλύτερο για την οποιαδήποτε εταιρία η άμεση συνεργασία με προμηθευτές ή το παράδειγμα Corda, που χρησιμοποιείται στους τραπεζικούς κλάδους για τη διαχείριση εμβασμάτων και παρέχοντας υπηρεσίες ταχύτερα, φθηνότερα και με περισσότερη ασφάλεια από ό,τι στις υπάρχουσες τεχνολογίες. Η δεύτερη και τρίτη ερώτηση αναφέρονται στο αν η εταιρία δουλεύει με ψηφιακά περιουσιακά στοιχεία και αν ναι, αν μπορεί να δημιουργηθεί μόνιμη έγκυρη εγγραφή του περιουσιακού στοιχείου. Πρώτον, είναι αρκετά περίπλοκο το blockchain να διαχειριστεί περιουσιακά στοιχεία με φυσική υπόσταση. Δεύτερον, λόγω του ότι ένας από τους στόχους είναι η παροχή εμπιστοσύνης, είναι δύσκολο να λειτουργήσει σωστά, όταν το στοιχείο διαθέτει πολλές πηγές εμπιστοσύνης όσον αφορά την κατάσταση του.

- Στο δεύτερο σημείο (D-E) ρωτάει τον υποψήφιο χρήστη αν οι συναλλαγές χρειάζεται να είναι γρήγορες (δηλ. χιλιοστών δευτερολέπτου) και υψηλής απόδοσης. Μέχρι το 2018 τα διάφορα είδη είχαν χρόνο επεξεργασίας μεταξύ 2 και 10 λεπτών. Επίσης αν ο σκοπός είναι η αποθήκευση μεγάλων ποσοτήτων μη συναλλαγμένων δεδομένων, δηλαδή αν υπάρχουν δεδομένα με τοπικούς ή παγκόσμιους κανονισμούς, δεν πρέπει να αποθηκεύονται στο blockchain. Αν η απάντηση είναι θετική τότε το Blockchain δεν μπορεί να είναι αποτελεσματικό για τη λύση του προβλήματος προς το παρόν, αλλά υπάρχουν λύσεις υπό εξέλιξη.

- Μια βασική αρχή της συγκεκριμένης τεχνολογίας είναι η απαλοιφή

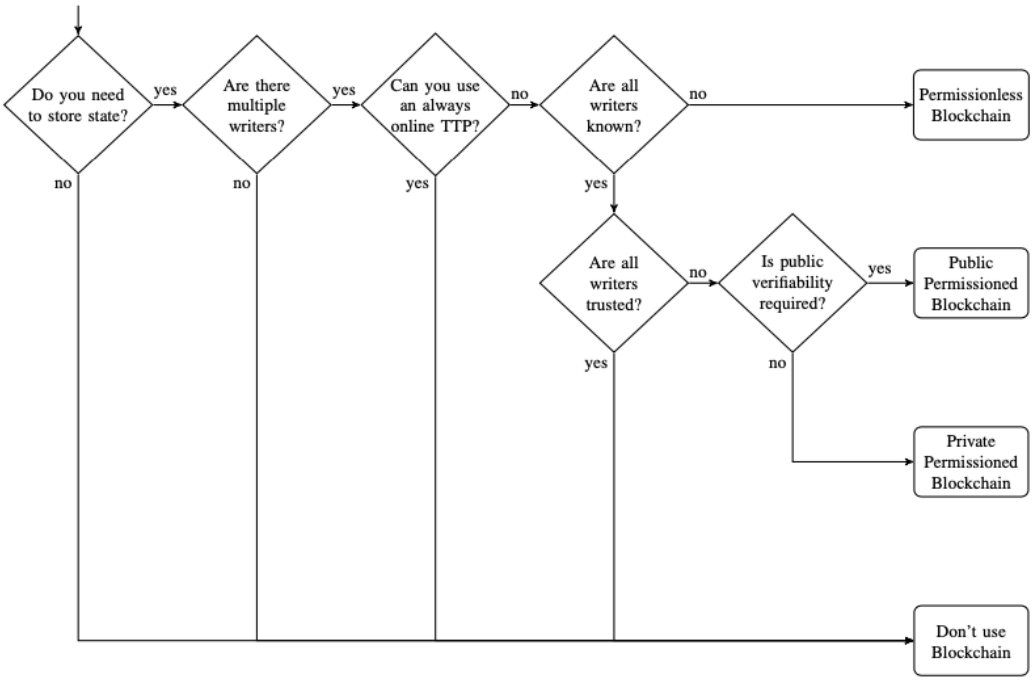
μεσολαβητών ή τρίτων προσώπων, αν η δομή των διαφόρων διεργασιών απαιτούν την συμβολή ενδιάμεσων συνεργατών, τότε χωρίς κάποιες αλλαγές, είναι αρκετά δύσκολο να εφαρμοστεί. Για να βοηθήσει το Blockchain στη μείωση του κόστους και στη παροχή πραγματικής επιχειρηματικής αξίας, είναι σημαντικό να εξετάζει τη διαχείριση συναλλαγών γύρω από ψηφιακά περιουσιακά στοιχεία. Αν ένα πρόβλημα δεν αφορά πραγματικά τη διαχείριση συμβατικών σχέσεων και ανταλλαγής αξιών, τότε υπάρχει μικρή ανάγκη χρήσης του. Μια άλλη βασική αξία είναι η κοινή πρόσβαση εγγραφής, αν ο ενδιαφερόμενος δεν θέλει κάποια ή όλα τα μέλη να γράφουν συναλλαγές στο καθολικό, τότε μια άλλη τεχνολογία ίσως να ταιριάζει καλύτερα στον οργανισμό του. Σε αυτό το μέρος (F-H), ο ενδιαφερόμενος οδηγείται στην απόφαση ότι υπάρχει μικρή ανάγκη χρήσης του Blockchain και παροτρύνει την ομάδα λήψης αποφάσεων να κάνει περισσότερη έρευνα ή συνεχίζει παρακάτω.

- Τέλος (I), αν οι οντότητες του οργανισμού/επιχείρησης γνωρίζουν και εμπιστεύονται ο ένας τον άλλον, τότε δεν υπάρχει ανάγκη χρήσης του. Ενώ, αν δεν γνωρίζουν ή δεν εμπιστεύονται ο ένας τον άλλον τότε είναι ένας βασικός λόγος να γίνει χρήση του blockchain.

- Αφού η ομάδα λήψης αποφάσεων μελέτησε τα παραπάνω και οδηγηθεί στο τελικό στάδιο του δέντρου (J,K), τότε το blockchain είναι η βέλτιστη λύση για τον οργανισμό/επιχείρηση. Το δέντρο διαχωρίζεται με βάση την λειτουργία του blockchain, εάν το καθολικό (ledger) θα είναι ιδιωτικό/με άδεια χρήσης ή εάν θα είναι δημόσιο. Για παράδειγμα, αν οι συναλλαγές θα πρέπει να διατηρηθούν ιδιωτικές τότε το δημόσιο καθολικό δεν αρμόζει στον οργανισμό. Αν χρειάζεται να υπάρχει δημόσια πρόσβαση σε διάφορες λειτουργικές διαδικασίας τότε το public blockchain είναι το κατάλληλο [22] [23].

4.2 Διάγραμμα ροής Karl Wüstl and Arthur Gervais (May 2017)

Το παρακάτω μοντέλο απόφασης του Karl Wüstl and Arthur Gervais που ανάλυσαν το Μάιο του 2017, με την βοήθεια κάποιων ερωτήσεων, κατευθύνει την ενδιαφερόμενη επιχείρηση/οργανισμό ποιος τύπος blockchain ταιριάζει κατάλληλα στην φιλοσοφία της. Εξετάζεται η αποθήκευση δεδομένων, οι οντότητες που θα συμμετέχουν και η προσβασιμότητα.



Εικόνα 10, Karl Wüstl and Arthur Gervais (May 2017) (Πηγή: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1)

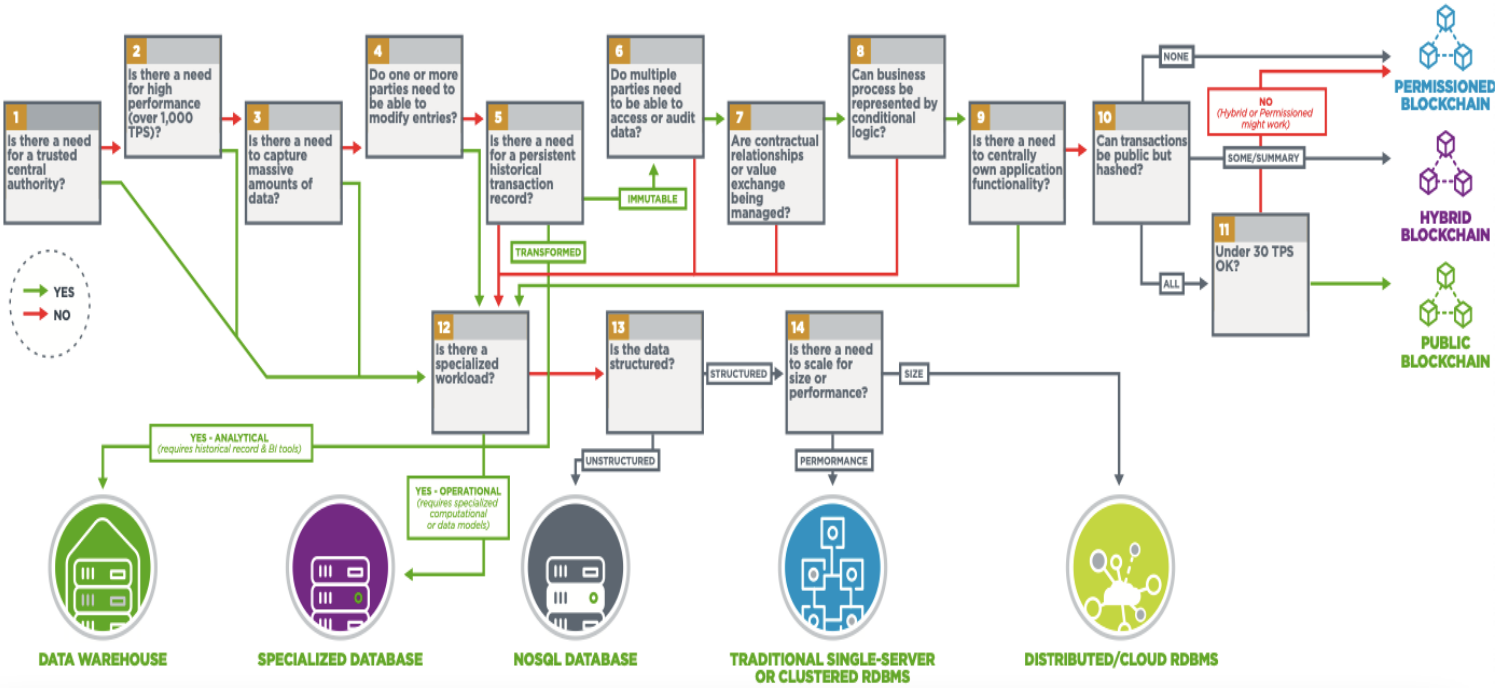
Ξεκινώντας από το πρώτο βήμα το διαγράμματος ροής. Αν δεν χρειάζεται να αποθηκευτούν δεδομένα, δεν απαιτείται καθόλου βάση δεδομένων, δηλαδή το blockchain, ως μορφή βάσης δεδομένων δεν έχει καμία χρησιμότητα. Ομοίως, εάν υπάρχει μόνο ένας writer (αυτός που συμμετέχει στην καταγραφή δεδομένων ή στην διαδικασίας συναλλαγών), το blockchain δεν παρέχει πρόσθετες εγγυήσεις, έτσι μια βάση δεδομένων είναι πιο κατάλληλη, αφού παρέχει καλύτερη απόδοση όσον αφορά την διακίνηση και την καθυστέρηση. Αν υπάρχει διαθέσιμο τρίτο μέρος(TTP-Trusted Third Party), υπάρχουν δύο επιλογές. Πρώτον, αν το TTP είναι πάντα συνδεδεμένο, οι λειτουργίες εγγραφής μπορούν να ανατεθούν σε αυτό και μπορεί να λειτουργήσει ως επαληθευτής για μεταβάσεις κατάστασης, άρα δεν υπάρχει ανάγκη χρήσης του Blockchain. Δεύτερον, εάν το TTP είναι συνήθως εκτός σύνδεσης, μπορεί να λειτουργεί ως αρχή έκδοσης πιστοποιητικών στη ρύθμιση ενός permissioned blockchain, δηλαδή όπου είναι γνωστοί όλοι οι συντάκτες του συστήματος. Αν όλοι οι συγγραφείς (writers) εμπιστεύονται ο ένας τον άλλον, δηλαδή θεωρούν ότι κανένας δε είναι κακόβουλος, μια βάση δεδομένων με κοινή πρόσβαση εγγραφής είναι πιθανώς η καλύτερη λύση. Αν όμως, δεν εμπιστεύονται ο ένας τον άλλον, η χρήση ενός blockchain με άδεια χρήσης θα είναι ωφέλιμη.

Ανάλογα με τον αν απαιτείται δημόσια χρήση, μπορεί να επιτραπεί σε οποιονδήποτε να διαβάσει την κατάσταση (public permissioned blockchain) ή να περιοριστεί το σύνολο των αναγνωστών (private permissioned blockchain). Όταν το σύνολο των συγγραφέων δεν είναι σταθερό και γνωστό στους συμμετέχοντες, όπως για παράδειγμα το Bitcoin, η κατάλληλη λύση είναι ένα permissionless blockchain.

Σε συγκεντρωτικά συστήματα, η απόδοση και η απόκλιση είναι γενικά πολύ καλύτερη από ότι τα συστήματα blockchain, καθώς τα blockchain προσθέτουν επιπλέον πολυπλοκότητα μέσω του μηχανισμού τους. Για παράδειγμα ένα κεντρικό σύστημα Visa μπορεί να χειριστεί πολύ περισσότερες συναλλαγές από το Bitcoin. Επιπρόσθετα, ένα άλλο κόλλημα που πρέπει να σημειωθεί είναι η αντιστάθμιση μεταξύ της αποκέντρωσης, δηλαδή πόσο καλά προσαρμόζεται ένα σύστημα σε μεγάλο αριθμό writers χωρίς αμοιβαία εμπιστοσύνη, και της απόδοσης, δηλαδή πόσες ενημερώσεις κατάστασης μπορεί να χειριστεί το σύστημα σε ένα χρονικό διάστημα. Αυτά τα δεδομένα πρέπει να ληφθούν υπόψη για την βέλτιστη επιλογή [24].

4.3 **Δέντρο ροής CompTIA 2019**

Το παρακάτω δέντρο αποφάσεων φτιάχτηκε, αναλύθηκε και δημοσιεύτηκε το 2019 από τη CompTIA, για να κατευθύνει τους χρήστες, με μια σειρά διαδρομών-ερωτήσεων, να προσδιορίσουν εάν το blockchain ή κάποια άλλη λύση εξυπηρετεί τις ανάγκες τους. Πιο κάτω παρατίθεται μια ανάλυση για τον κάθε κλάδο του δέντρο και πως κάθε απόφαση θα επηρέαζε την επιχείρηση. Όπως φαίνεται οι διαδρομές με πράσινο ορίζουν την θετική και με κόκκινο την αρνητική απάντηση.



Εικόνα 11, CompTIA 2019 (Πηγή: https://connect.comptia.org/content/infographic/blockchain-decision-tree)

- Μια θεμελιώδης αρχή του Blockchain είναι η εξάλειψη μιας αξιόπιστης κεντρικής αρχής. Ως γνωστόν, το Blockchain σχεδιάστηκε για να παρέχει εμπιστοσύνη, όπου δεν είναι απαραίτητη για συναλλαγές ή καταχωρήσεις σε αυτό. Κάθε συναλλαγή επαληθεύεται ανεξάρτητα, μέσω ενός μαθηματικού αλγορίθμου συναίνεσης. Η αρχιτεκτονική του, κάποιες φορές, μπορεί να οδηγήσει σε μια λύση χαμηλού κόστους και προσφέρει ταχύτερη διευθέτηση. Αν μια περίπτωση χρήσης μπορεί να καταργήσει μια αξιόπιστη κεντρική αρχή, το blockchain μπορεί να είναι μια καλή επιλογή, καθώς βελτιστοποιεί την επιχειρηματική διαδικασία αυξάνοντας την ταχύτητα του διακανονισμού, μειώνοντας τα σφάλματα

και το λειτουργικό κόστος. Για την επίτευξη αυτού, μπορεί να χρειαστεί επανασχεδιασμός της ροής εργασίας της διαδικασίας για καλύτερη αξιοποίηση των ιδιοτήτων του και την εκπλήρωση των στόχων. Οι αλγόριθμοι στον πυρήνα της συναλλαγής είναι αρκετά αργοί. Εάν μια εφαρμογή απαιτεί λιγότερο από 1.000TPS (Transactions Per Second) το blockchain μπορεί να είναι μια κατάλληλη λύση. Όσο υψηλότερος είναι ο αριθμός συναλλαγών ανά δευτερόλεπτο τόσο περισσότερο είναι το κόστος και η μειωμένη πρακτικότητα (σημεία 1 και 2).

- Το blockchain δεν υποστηρίζει μεγάλα σύνολα δεδομένων εντός αλυσίδας. Κατά τον έλεγχο της αποθήκευσης δεδομένων, υπάρχουν τρεις κύριοι παράγοντες που πρέπει να ληφθούν υπόψη. Ο πρώτος είναι το μέγεθος, το μέγεθος του μπλοκ του Bitcoin περιορίζεται σε 1MB και ένα τυπικό τραγούδι σε 3.5MB. Ο λόγος είναι επειδή τα βιβλία του Blockchain αντιγράφονται σε χιλιάδες υπολογιστές σε όλο τον κόσμο, οι περισσότεροι από τους οποίους δεν είναι βιομηχανικής ποιότητας, οπότε τα αρχεία θα αυξηθούν σε μη υποστηριζόμενα μεγέθη εάν τα δεδομένα ανά συναλλαγή δεν περιορίζονται. Δεύτερο είναι το κόστος μεταφοράς, εντός της αλυσίδας είναι δυνατή η διαίρεση των αρχείων σε μικρότερα κομμάτια. Ωστόσο, αυτό όχι μόνο δεν θα λύσει το πρόβλημα επειδή το συνολικό αρχείο θα εξακολουθεί να έχει το ίδιο μέγεθος, αλλά θα αυξήσει το κόστος συναλλαγής. Κάθε συναλλαγή που γράφεται σε δημόσια αλυσίδα απαιτεί τεράστιες αμοιβές στους επικυρωτές (validators). Οι μεγάλες βάσεις δεδομένων συνήθως υποδηλώνουν υψηλά ποσά συναλλαγών για αρχή και το κόστος ανάρτησης δεδομένων είναι σημαντικά υψηλότερο από το γράψιμο παραδοσιακών βάσεων δεδομένων. Τρίτος παράγοντας είναι η απόδοση, που επηρεάζεται σημαντικά. Για παράδειγμα το Bitcoin κατά μέσω όρο εκτελεί περίπου 7 TPS και το Ethereum 15 TPS, ενώ η Visa εκτελεί περίπου 15.000 ως 25.000 TPS. Υπάρχουν τακτικές που χρησιμοποιούν τα permissioned Blockchains, καθώς εκτελούνται σε λιγότερους διακομιστές, βελτιώνοντας σημαντικά το κόστος, την απόδοση και την ταχύτητα αποθήκευσης δεδομένων. Μια τέτοια στρατηγική είναι να αποθηκεύει μόνο τις κατακερματισμένες συναλλαγές στο Blockchain και τα ακατέργαστα δεδομένα σε μια παραδοσιακή βάση δεδομένων. Ωστόσο, μια τέτοια δομή προσθέτει πολυπλοκότητα στο σύστημα και η ταχύτητα των συναλλαγών εξακολουθεί να είναι αργή. Συμπερασματικά, το Blockchain είναι κατάλληλη λύση όταν οι ανάγκες αποθήκευσης είναι

μικρές ή όταν τα μεγάλα σύνολα δεδομένων αποθηκεύονται εκτός αλυσίδας (σημείο 3).

- Το επόμενο σημείο αναφέρεται στο αμετάβλητο της τεχνολογίας του Blockchain. Οι καταχωρήσεις δηλαδή, παρόλο που είναι διαθέσιμες προς όλους τους εξουσιοδοτημένους χρήστες, δεν μπορούν να τροποποιηθούν. Άρα, αν η περίπτωση χρήσης απαιτεί διαγραφή ή τροποποίηση καταχωρήσεων, το Blockchain δεν είναι η κατάλληλη λύση. Η καταγραφή των δεδομένων αμετάβλητα στο καθολικό διασφαλίζει ότι όλα τα δεδομένα έχουν ιστορικά αρχεία. Στην περίπτωση της διαχείρισης της εφοδιαστικής αλυσίδας, η παρακολούθηση των προϊόντων από το αγρόκτημα στο πελάτη μειώνει τον κίνδυνο για το καταναλωτικό κοινό, αφού γίνεται παρακολούθηση των αμετάβλητων ιστορικών αρχείων για το κάθε προϊόν. Άρα αν απαιτείται ιστορική καταγραφή των συναλλαγών ή των καταχωρήσεων, μια τέτοια τεχνολογία είναι μια αρκετά καλή λύση (σημεία 4 και 5).

- Η κοινή χρήση δεδομένων με άλλα μέρη δεν είναι πάντα εύκολο να εκτελεστεί με ασφαλή και αξιόπιστο τρόπο, το Blockchain όμως μπορεί να προσφέρει τα μέσα για αυτό. Η παροχή πρόσβασης σε δεδομένα μπορεί να είναι πολύτιμη για την αποτελεσματική συνεργασία και να ανοίξει πόρτες σε νέες ροές εσόδων. Επιπλέον, σε καταστάσεις στις οποίες ένα μέρος μπορεί να χρειαστεί να διενεργήσει έλεγχο, αυτή η τεχνολογία τους επιτρέπει να εμπιστευτούν ότι τα δεδομένα παραμένουν αμετάβλητα. Οι έλεγχοι γύρω από τον κανονισμό και τη νομοθεσία είναι σημεία δεδομένων που το Blockchain μπορεί να βοηθήσει στη δημιουργία μιας αμετάβλητης διαδρομής ελέγχου. Αυτό, μπορεί να μειώσει το κόστος ελέγχου και συμμόρφωσης αυξάνοντας παράλληλα την εμπιστοσύνη (σημείο 6).

- Ένα έξυπνο συμβόλαιο είναι ένας κώδικας υπολογιστή, ο οποίος, όταν εμφανιστεί μια συγκεκριμένη κατάσταση, είναι ικανός να λειτουργεί αυτόματα σύμφωνα με τις προκαθορισμένες λειτουργίες. Τα έξυπνα συμβόλαια χωρίζονται σε δύο μέρη, τα εξωτερικά και τα εσωτερικά έξυπνα συμβόλαια. Τα εσωτερικά περιλαμβάνουν ολόκληρη τη συμφωνία μεταξύ των μερών ενώ τα εξωτερικά αυτοματοποιούν την εκτέλεση ορισμένων όρων μιας σύμβασης που έχει κάποια άλλη μορφή. Αν είναι σημαντικό μια σύμβαση να τροποποιείται κατά την διάρκεια ισχύς της, τότε τα έξυπνα συμβόλαια δεν είναι τόσο κατάλληλη λύση.

Συμπερασματικά, αν μια επιχειρηματική περίπτωση μπορεί να δηλωθεί με σαφής, απλούς όρους που δεν απαιτούν ανθρώπινη κρίση και δεν χρειάζεται τροποποίηση κατά τη διάρκεια του κύκλου ζωής της, το Blockchain μπορεί να είναι μια καλή λύση (σημείο 7 και 8).

- Οποιοσδήποτε έχει άδεια πρόσβασης σε blockchain μπορεί να δημιουργήσει μια εφαρμογή για ανάγνωση ή εγγραφή στο blockchain. Επομένως, εάν η λειτουργικότητα της εφαρμογής πρέπει να ελέγχεται από κεντρική οντότητα τότε το blockchain δεν είναι εφικτή λύση. Ωστόσο, αν οι χρήστες με άδεια μπορούν να είναι ελεύθεροι να αναπτύξουν τις δικές τους εφαρμογές, το Blockchain μπορεί να είναι η κατάλληλη λύση για την εφαρμογή. (σημείο 9)

- Ο καθένας θα πρέπει να μπορεί να διαβάζει και να γράφει στο Blockchain. Προφανώς, τα permissioned blockchains δεν το επιτρέπουν αυτό. Υπάρχουν αρκετοί καλοί λόγοι για τη χρήση permissioned blockchain, αλλά μια εσφαλμένη αντίληψη για τα public είναι ότι επειδή οι συναλλαγές είναι δημόσια αναγνώσιμες, δεν είναι ασφαλείς. Όλες οι πληροφορίες σχετικά με το blockchain μπορούν να κατακερματιστούν και να είναι ανεξάρτητες από την ταυτότητά τους. Τα Cryptowallets παρέχουν σε οποιονδήποτε κάτοχο ένα ιδιωτικό κλειδί για κρυπτογράφηση, οπότε οποιαδήποτε πληροφορία μέσα σε μια συναλλαγή που έχει κατακερματιστεί με ένα δημόσιο κλειδί που προέρχεται από το ιδιωτικό κλειδί είναι διαθέσιμη μόνο σε όποιον κατέχει το ιδιωτικό κλειδί. Επομένως, εάν οι κρυπτογραφημένες πληροφορίες συναλλαγών μιας εφαρμογής είναι διαθέσιμες στο κοινό, ένα δημόσιο blockchain μπορεί να είναι η κατάλληλη λύση καθώς θα μειώσει το κόστος (π.χ. υλικό, συντήρηση, εργασία) και θα επιτρέψει ανεξάρτητη καινοτομία (σημείο 10).

- Για να είναι αποδοτική μια εφαρμογή με public blockchain θα πρέπει να εκτελεί λιγότερο από 15TPS, για περισσότερο και ως 1000TPS καλύτερα να χρησιμοποιηθεί permissioned ή permissioned hybrid blockchain (σημείο 11).

- Κάθε βάση δεδομένων έχει σχεδιαστεί για να χειρίζεται διαφορετικούς τύπους αποθήκευσης και ανάκτησης δεδομένων. Μια σημαντική διαφοροποίηση είναι αν τα δεδομένα που αποθηκεύονται έχουν μια άκαμπτη, καθορισμένη δομή ή είναι μη δομημένα. Οι βάσεις δεδομένων

NoSQL έχουν σχεδιαστεί για να χειρίζονται μη δομημένα δεδομένα ενώ το RDBMS είναι το καλύτερο για δομημένα δεδομένα. Όταν ένα RDBMS διαπιστωθεί ότι είναι η κατάλληλη βάση δεδομένων, γεννιέται το ερώτημα τι είναι πιο σημαντικό η βελτιστοποίηση του μεγέθους ή η απόδοση. Αν η εφαρμογή πρέπει να βελτιστοποιηθεί λόγο της απόδοσης, ένα παραδοσιακό, locally hosted RDBMS, είναι η κατάλληλη επιλογή. Ενώ, αν η εφαρμογή πρέπει να βελτιστοποιηθεί για το μέγεθος της βάσης δεδομένων, όπου η τοπική αποθήκευση θα μπορούσε να αποτελέσει πρόβλημα, πιθανότατα ένα cloud ή κατανεμημένο RDBMS είναι καλύτερη επιλογή (σημεία 12, 13, 14).

- **Public Permissionless Blockchain:** Το Bitcoin και το Ethereum είναι παραδείγματα χρήσης public permissionless blockchains. Σε τέτοιου είδους περιπτώσεις χρήσης όπως αναφέρθηκε σε προηγούμενα, ο οποιοσδήποτε μπορεί να εκτελέσει διαδικασίες πάνω σε αυτό. Το συγκεκριμένο είδος είναι μια πολύ επιλογή όταν τα μέλη που θα εντάσσονται στο δίκτυο προσφέρουν περιουσιακά στοιχεία για την ανάπτυξη του δικτύου. Αυτό το είδος blockchain, βασίζεται στην προσφορά δεδομένων από τους συμμετέχοντες για την ανάπτυξη και την κλιμάκωση του δικτύου, προσπαθώντας να αποτρέψουν μια οντότητα ή ακόμη και μια μικρή ομάδα οντοτήτων, από τον έλεγχο του δικτύου και όταν προσπαθούν να δώσουν κίνητρα σε άλλους να συμμετέχουν στην κοινότητα. Ουσιαστικά, οι οντότητες προσφέρουν περιουσιακά στοιχεία όπως ανεκμετάλλευτη υπολογιστική ισχύ, χωρητικότητα αποθήκευσης και/ή εύρος ζώνης δικτύου και σε αντάλλαγμα προσφέρονται κέρματα, μάρκες ή άλλα ισοδύναμα.

- **Private Permissioned Blockchain:** Το Hyperledger είναι ένα παράδειγμα που αποτελείται από permissioned blockchains και εργαλεία, που μπορούν να αξιοποιηθούν ιδιωτικά από οργανισμούς που θα ήθελαν τα οφέλη από τη χρήση της τεχνολογίας blockchain χωρίς να εγκαταλείψουν τον έλεγχο. Όταν χρησιμοποιείται ιδιωτικό blockchain με άδεια χρήσης, μια επιχείρηση μπορεί να χρησιμοποιήσει τα δικά της κρυπτογραφικά κλειδιά, να καθορίσει ποια υποδομή, συνεργάτες ή άλλα τρίτα μέρη επιτρέπεται να συμμετέχουν στο δίκτυο, να καθορίσει τι είδους υποδομή μπορεί να χρησιμοποιηθεί και για ποιους ρόλους κόμβων, να καθορίσει ποια οι οντότητες ή οι κόμβοι μπορούν να διαβάσουν, να γράψουν ή να έχουν πλήρη πρόσβαση στο blockchain και να καθορίσουν το πρόγραμμα κινήτρων για συμμετοχή. Τα blockchains

με ιδιωτική άδεια συγκεντρώνονται και ελέγχονται από την οντότητα που αναθέτει το blockchain. Τα blockchains με ιδιωτική άδεια αντιπροσωπεύουν μια εξαιρετική επιλογή όταν μια οντότητα θα ήθελε να ελέγξει ποια άτομα ή οργανισμοί μπορούν να συμμετέχουν στο δίκτυο και με ποια ιδιότητα. Για παράδειγμα, μια επιχείρηση μπορεί να επιτρέψει σε όλες τις συναλλασσόμενες οντότητες στο οικοσύστημά της να συμμετάσχουν σε συναίνεση και να προσθέσουν μπλοκ στην αλυσίδα, αλλά να επιτρέψει στα μέλη του οικοσυστήματος ελέγχου να διαβάζουν, αλλά όχι να γράφουν, στον ψηφιακό καθολικό. Αυτή η προσέγγιση επιτρέπει στις επιχειρήσεις να αξιοποιήσουν την τεχνολογία blockchain διατηρώντας ταυτόχρονα τους απαιτούμενους ελέγχους, μειώνοντας τον επιχειρηματικό κίνδυνο και τηρώντας τους σχετικούς κανονισμούς.

- **Hybrid Blockchain:** Μια οντότητα μπορεί να θέλει να χρησιμοποιήσει ένα υβριδικό blockchain για να επιτρέψει μόνο σε συγκεκριμένους κόμβους να επικυρώσουν συναλλαγές και να προσθέσουν μπλοκ στην αλυσίδα (permissioned), αλλά να επιτρέψει σε κάθε άτομο ή οργανισμό να προσφέρει το δίκτυό του ή να υπολογίσει τους πόρους υποδομής (permissionless) στο δίκτυο. Σε αυτήν την περίπτωση, ο έλεγχος μπορεί να διατηρηθεί, το κόστος μπορεί να μειωθεί και μια οντότητα μπορεί να αξιοποιήσει τεχνολογίες blockchain όπου κρίνει κατάλληλα [25].

4.4 Ερωτηματολόγιο για την επιλογή permissionless Blockchain, My model (as of Aug.2016)

Το παρακάτω εναλλακτικό μοντέλο αποφάσεων παρουσιάζει μια σειρά ερωτήσεων, τις οποίες ο χρήστης καλείται να συμπληρώσει με αρνητική ή θετική απάντηση. Σύμφωνα με τον σχεδιαστή του υπάρχουν τρεις κατηγορίες αποτελεσμάτων που μπορούν να εξαχθούν, με βάση τις απαντήσεις που θα δώσει ο εκάστοτε ενδιαφερόμενος. Αν οι θετικές απαντήσεις που θα δοθούν είναι λιγότερες από 7/10 τότε μια κοινή βάση δεδομένων είναι καλύτερη λύση. Αν κυμαίνονται από 7 ως 9 τότε υπάρχει μια πιθανότητα το blockchain να βοηθήσει την επιχείρηση. Αν όμως όλες οι ερωτήσεις απαντηθούν θετικά τότε η τεχνολογία ενός permissionless blockchain (π.χ. Bitcoin, Ethereum) ταιριάζει απόλυτα στην εφαρμογή της επιχείρησης.

	Assertion	Answer
Network	A significant number of participants will be transacting on the network (>100)	Agree/Yes ☐
	You don't trust the participants in the network and don't need/want to know them	Agree/Yes ☐
Performance	A limited amount of data needs to be stored for every transaction (a few fields)	Agree/Yes ☐
	The business process doesn't requires a high throughput (scalability)	Agree/Yes ☐
Business logic	The business logic is simple	Agree/Yes ☐
	Privacy of transactions is not an important feature	Agree/Yes ☐
	The system will be standalone, it doesn't need to access external data or be integrated in the IT legacy	Agree/Yes ☐
Consensus	No arbitrator shall be involved in case of a dispute	Agree/Yes ☐
	All participants can be involved in the validation of transactions (Vs only a group of known validators)	Agree/Yes ☐
	You need strict immutability of the record (no amend & cancel, even by admin)	Agree/Yes ☐

Εικόνα 12, My model (as of Aug.2016) (Πηγή: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1)

Οι συγκεκριμένες ερωτήσεις χωρίζονται σε 4 πολύ βασικούς πυλώνες για την λειτουργία του permissionless Blockchain. Πρώτος, είναι το δίκτυο και πιο συγκεκριμένα ο αριθμός των συμμετεχόντων και το αν υπάρχει εμπιστοσύνη μεταξύ τους. Δεύτερος η απόδοση, δηλαδή αν αριθμός των δεδομένων θα είναι περιορισμένος και αν δεν χρειάζεται υψηλή απόδοση στις επιχειρηματικές διαδικασίες. Τρίτος είναι η λογική της επιχείρησης, για να είναι ένα permissionless blockchain αποδοτικό σύμφωνα με το δέντρο, πρέπει να μην είναι πολύπλοκη. Τελευταίος πυλώνας είναι ο αλγόριθμος κοινής συναίνεσης.

5 Επιλογή προτύπων (Patterns) σε εφαρμογές της Τεχνολογίας Blockchain

5.1 Εισαγωγή

Τα Blockchains, όπως αναλύθηκε σε προηγούμενες ενότητες, παρέχουν μοναδικές ιδιότητες από την άποψη αρχιτεκτονικής λογισμικού, συμπεριλαμβανομένου του αμετάβλητου, της ακεραιότητας των δεδομένων, της διαφάνειας και των ίσων δικαιωμάτων. Ωστόσο, ο σχεδιασμός του blockchain θυσιάζει την εμπιστευτικότητα και την απόδοση σε σύγκριση με τις συμβατικές λύσεις αποθήκευσης δεδομένων. Επομένως, για να αξιοποιηθούν καλύτερα οι θετικές ιδιότητες του blockchain, απαιτεί σωστή καθοδήγηση για το σχεδιασμό εφαρμογών που βασίζονται σε αυτό.

Αυτή η ενότητα βασίζεται στην παρουσίαση ενός συνόλου μοντέλων αποφάσεων για την καθοδήγηση της επιλογής προτύπων (patterns) blockchain. Τα μοντέλα απόφασης παρουσιάζουν τις αντισταθμίσεις ποιότητας κάθε προτύπου και τη σχέση που έχουν μεταξύ τους. Η πιο κάτω ανάλυση, βοηθά τους προγραμματιστές με βάση τα ποιοτικά χαρακτηριστικά του κάθε πρότυπου να επιλέξουν του κατάλληλους συνδυασμούς για να ικανοποιήσουν τους σχεδιαστικούς τους στόχους. Με την συλλογή των πληροφοριών που εξάγουν τα παρακάτω μοντέλα δίνουν στους προγραμματιστές μια σωστή αίσθηση για να λάβουν ορθολογιστικές αποφάσεις.

Σε γενικές γραμμές τα πρότυπα (patterns) είναι μια επαναχρησιμοποιήσιμη λύση σε προβλήματα που εμφανίζονται συνήθως σε ένα δεδομένο πλαίσιο κατά τη διάρκεια σχεδιασμού του λογισμικού. Τα προτεινόμενα πρότυπα είναι χρήσιμα για αρχιτέκτονες λογισμικού, προγραμματιστές, διαχειριστές συστήματος και τεχνικούς που πρέπει να σχεδιάσουν, να αναπτύξουν και να παρακολουθήσουν έργα που βασίζονται σε blockchain, ανάλογα με την περίπτωση χρήσης και τις προδιαγραφές που μπορούν να εφαρμοστούν [26], [27].

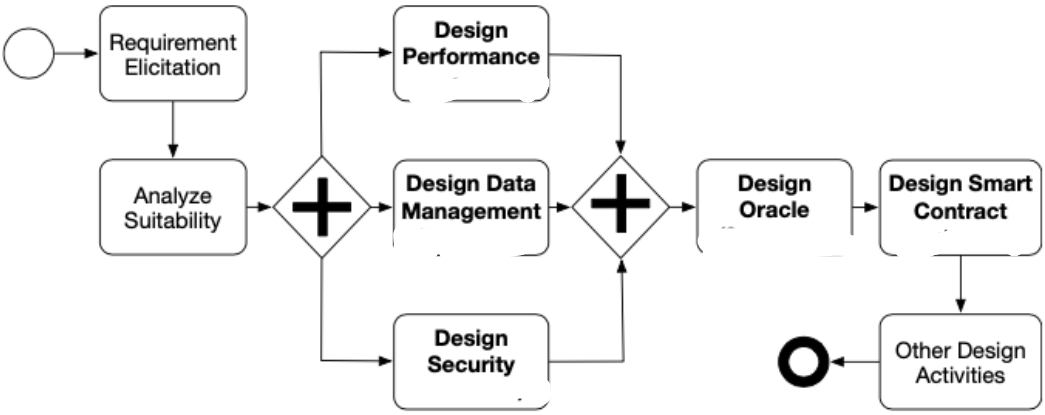
Η συγκεκριμένη ενότητα αποτελείται από την επεξήγηση των διαφόρων προτύπων που εμφανίζονται στα μοντέλα αποφάσεων, καθώς και την ανάλυση των διαφόρων μοντέλων αποφάσεων, που διαχωρίζονται

ανάλογα με την περίπτωση χρήσης κάθε φορά στην τεχνολογία Blockchain, όπως αναλύονται από την csiro.au και την DATA61 [17].

5.2 Διαδικασία σχεδιασμού εφαρμογών βασισμένες στο blockchain

Στο πιο κάτω σχήμα φαίνεται η διαδικασία σχεδιασμού για μια εφαρμογή που βασίζεται σε Blockchain. Τα ορθογώνια σχήματα με έντονα γράμματα αντιπροσωπεύουν τις δραστηριότητες που καλύπτονται από τα διάφορα μοντέλα αποφάσεων.

Όπως συμβαίνει με κάθε σύστημα λογισμικού, η διαδικασία ξεκινά με την συλλογή απαιτήσεων (**Requirement Elicitation**) των ενδιαφερόμενων και του εκάστοτε τομέα που πρόκειται να υλοποιηθεί η περίπτωση. Επίσης, είναι απαραίτητο να εκτιμηθεί αν είναι κατάλληλη η εφαρμογή της της συγκεκριμένης τεχνολογίας με βάση της απαιτήσεις και τα χαρακτηριστικά της κάθε περίπτωσης (**Analyze Suitability**). Τα δύο παραπάνω στάδια αφορούν στην ουσία τα όσα αναπτύχθηκαν στο κεφάλαιο 4 της διπλωματικής. Δηλαδή, ανάλογα με τα χαρακτηριστικά του κάθε τύπου Blockchain, που παρουσιάζονται στα μοντέλα αποφάσεων, και τα χαρακτηριστικά της κάθε περίπτωσης, επιλέγεται αν θα γίνει η χρήση της συγκεκριμένης τεχνολογίας.



Εικόνα 13, Σχεδιασμός εφαρμογών Blockchain (Πηγή: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9426788)

Δεδομένου ότι αποφασίστηκε η εφαρμογή της τεχνολογίας Blockchain, το επόμενο βήμα είναι να ελεγχθεί ποια δεδομένα θα αποθηκευτούν εντός αλυσίδας και ποια θα διατηρηθούν εκτός αλυσίδας (**Design Data Management**), η επιλογή των δεδομένων εξαρτάται από την υπολογιστική ισχύ και την αποθηκευτική τους ικανότητα. Η σωστή διαχείριση δεδομένων βασίζεται επίσης στις πτυχές της απόδοσης και της ασφάλειας (**Design Performance and Design Security**), άρα η κατάλληλη επιλογή προτύπου ασφάλειας και απόδοσης είναι ένα άλλο σημαντικό στοιχείο για την ποιότητα του Blockchain.

Στις πλείστες περιπτώσεις χρήσης του Blockchain απαιτείται αλληλεπίδραση με τον εξωτερικό κόσμο. Είναι σημαντικό να διασφαλιστεί ότι τα δεδομένα που σχετίζονται με τα αγαθά και τα μέρη σε ένα Blockchain αντικατοπτρίζουν σωστά τα φυσικά αντικείμενα και την κατάσταση τους. Οι λύσεις αυτές, λαμβάνουν/στέλνουν συνήθως δεδομένα από/προς στοιχεία εκτός αλυσίδας για να επεκτείνουν τις δυνατότητες των εφαρμογών (**Design Oracle**). Το στοιχείο που συνδέει το blockchain με τον εξωτερικό κόσμο ονομάζεται oracle. Το επόμενο στάδιο είναι τα έξυπνα συμβόλαια (**Design Smart Contracts**), τα οποία είναι μέρη προγραμμάτων που αναπτύσσονται και εκτελούνται σε ένα blockchain.

Τα στάδια σχεδιασμού Design Data Management, Design Performance και Design Security μπορούν να εκτελεστούν παράλληλα, καθώς είναι ως επί των πλείστων ανεξάρτητα, ενώ το Design Oracle και Design Smart Contracts εξαρτώνται από τον σχεδιασμό διαχείρισης των δεδομένων. Ωστόσο, τα βήματα σχεδιασμού μπορούν να εφαρμοστούν και με διαφορετική σειρά ανάλογα με το τι ταιριάζει καλύτερα σε ένα δεδομένο πρόβλημα [26].

5.3 Διαχείριση και απόδοση δεδομένων εντός αλυσίδας

Ανάλογα με τα χαρακτηριστικά των δεδομένων που θα πρέπει να διαχειρίζεται ένα Blockchain καθορίζονται ποια patterns πρέπει να εκτελούνται. Στο παρακάτω σχήμα απεικονίζεται ένα προτεινόμενο μοντέλο απόφασης για την επιλογή προτύπων για διαχείριση δεδομένων εντός αλυσίδας και απόδοσης. Ο λόγος που περιλαμβάνονται στο ίδιο μοντέλο απόφασης είναι ότι τόσο τα πρότυπα διαχείρισης δεδομένων όσο και τα πρότυπα απόδοσης διαχωρίζονται ανάλογα με το μέγεθος των δεδομένων. Η αποκλειστική πύλη (ρόμβος με το σχήμα X) ελέγχει αν ο

όγκος των δεδομένων είναι μεγάλος ή μικρός, δηλαδή αν το μέγεθος των δεδομένων είναι μικρότερος από το μέγεθος της συναλλαγής εκτελούνται τα πρότυπα διαχείρισης δεδομένων, στην αντίθετη περίπτωση εκτελούνται τα πρότυπα απόδοσης. Η επιλογή των προτύπων των δύο περιπτώσεων μπορεί να εκτελεστεί παράλληλα.

5.3.1 Διαχείριση Δεδομένων

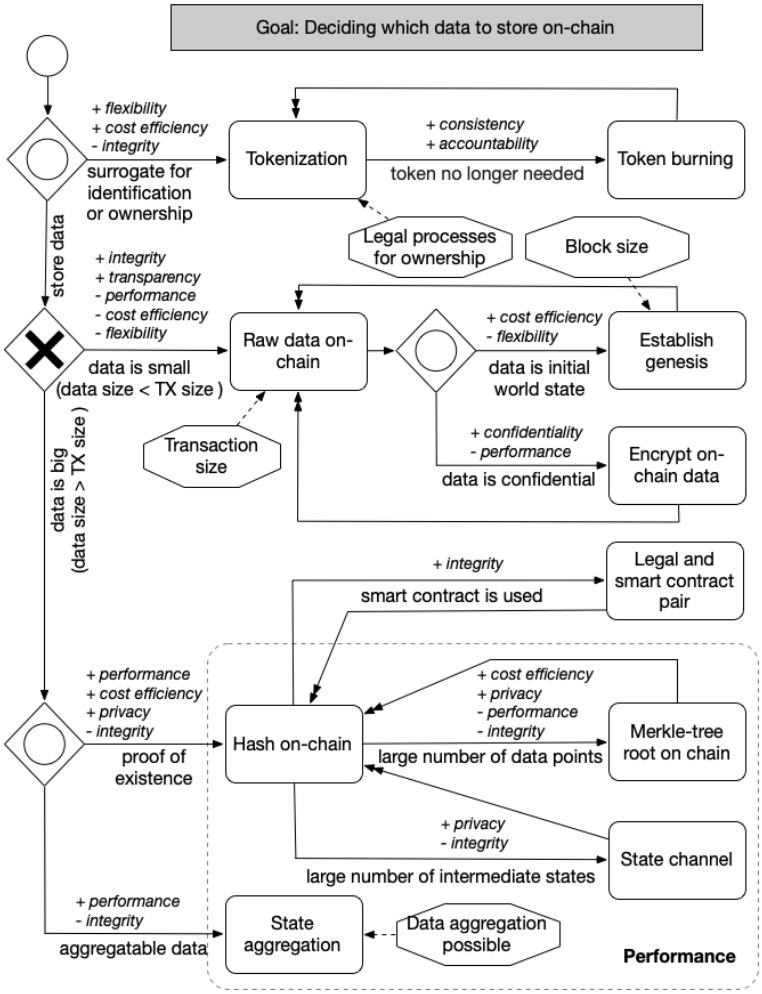
Αν τα δεδομένα που πρόκειται να αποθηκευτούν, αντικαθιστούν ιδιοκτησία περιουσιακών στοιχείων ή ταυτοποίηση, τότε το **tokenization pattern** μπορεί να χρησιμοποιηθεί για την δημιουργία και διαχείριση ψηφιακών, έγκυρων αρχείων που αντικαθιστούν περιουσιακά στοιχεία στο blockchain. Ένα αρχείο που πρόκειται να ενταχθεί στο σύστημα αντικαθίσταται με ένα token. Ένα token μπορεί επίσης να χρησιμοποιηθεί για την αναπαράσταση μιας ταυτότητας ενός χρήστη, η οποία χρησιμοποιείται κυρίως στο κομμάτι της ασφάλειας. Η διαδικασία αυτή μειώνει τον κίνδυνο χειρισμού ψηφιακών και φυσικών, ανταλλάξιμων και μη, στοιχείων, υψηλής αξίας.

Με την δημιουργία, μεταφορά και πώληση ενός token, κατά τη διαδικασία μιας συναλλαγών εντός του Blockchain, ενισχύεται η ευελιξία και η αποδοτικότητα του συστήματος. Ωστόσο, θα μπορούσε ένα περιουσιακό στοιχείο που αντιπροσωπεύεται από ένα token να υποβληθεί σε διαδικασία εκτός του Blockchain, χωρίς να καταγραφεί κάποια συναλλαγή. Αυτή η περίπτωση θέτει σε κίνδυνο την ακεραιότητα των δεδομένων [28].

Στην περίπτωση που ένα token δεν είναι πλέον χρήσιμο θα πρέπει να χαρακτηρισθεί ως μη αναλώσιμο και να καταστραφεί, αποφεύγοντας τη κακόβουλη χρήση του, για παράδειγμα τη διπλή δαπάνη του. Περιπτώσεις χρήσης του **Token Burning Pattern** είναι:

- Όταν τα μη ανταλλάξιμα tokens δεν είναι πλέον χρήσιμα.
- Τα ανταλλάξιμα tokens καταστρέφονται για να αυξηθεί η αξία των υπόλοιπων, μειώνοντας την προσφορά.

- Ένα token θα πρέπει να καταστραφεί από το Blockchain-προέλευσης προτού αντικατασταθεί ή μεταφερθεί στο Blockchain-στόχος. Αν δηλαδή υπάρχει ανάγκη μεταφοράς αρχείων-token από ένα Blockchain σε άλλο, το token, αν δεν είναι χρήσιμο πλέον, θα πρέπει να διαγραφεί από το χώρο προέλευσης του.



Εικόνα 14, Διαχείριση και απόδοση δεδομένων εντός αλυσίδας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/performancemodel/)

Η χρήση του Token Burning εφαρμόζεται για να καταστήσει τα tokens ή τα smart contracts άχρηστα, διασφαλίζοντας ταυτόχρονα συνέπεια και υπευθυνότητα. Το Token Burning συμπληρώνει την διαδικασία του Tokenization [29].

Όπως αναφέρθηκε παραπάνω, ο όγκος των δεδομένων που αποθηκεύονται χρησιμοποιώντας μια συναλλαγή εξαρτάται από το μέγεθος της συναλλαγής και το μέγεθος του μπλοκ της εκάστοτε

πλατφόρμας. Επομένως, η δυνατότητα εφαρμογής των patterns εντός αλυσίδας εξαρτάται αποκλειστικά από το μέγεθος των δεδομένων που πρόκειται να αποθηκευτούν και την υπολογιστική πολυπλοκότητα.

Όταν το μέγεθος της συναλλαγής είναι μικρότερο από το μέγεθος του μπλοκ, δηλαδή τα δεδομένα της εφαρμογής είναι μικρά και μη ευαίσθητα γίνεται αποθήκευση όλων των δεδομένων στο Blockchain. Σε τέτοιες περιπτώσεις το **Raw-on-Chain pattern** εκτελείται για την αποθήκευση όλων των δεδομένων στην αλυσίδα, αμετάβλητα και με διαφάνεια. Μερικοί τρόποι αποθήκευσης δεδομένων στην αλυσίδα είναι ενσωματωμένα σε μια συναλλαγή και ως smart contracts. Αυτές οι επιλογές έχουν διαφορετικούς συμβιβασμούς, συμπεριλαμβανομένου του κόστους και της ευελιξίας. Γενικότερα, η εγγραφή δεδομένων, χωρίς να γίνεται έλεγχος ως προς τον τύπο του, είναι αργή, δαπανηρή, αλλά και λιγότερο ευέλικτη [30].

Αν τα δεδομένα της εφαρμογής πρέπει να οριστούν κατά την αρχικοποίηση της εφαρμογής, χρησιμοποιείται το **Establish Genesis pattern**, για να οριστεί η κατάσταση στο **genesis block**. Για παράδειγμα, κατά την έναρξη ενός νέου Blockchain, η αρχική κατανομή των εγγενών tokens ορίζεται από αυτό το πρότυπο, με την προϋπόθεση ότι τα δεδομένα που περιλαμβάνονται στο genesis block περιορίζονται από το μέγεθος του μπλοκ όπως αναφέρθηκε. Λόγω του ότι υπάρχει περιορισμός στο ποια και πόσα δεδομένα θα καταγραφούν κατά την έναρξη, η ευελιξία είναι χαμηλή. Με την εφαρμογή του Establish Genesis και την αποθήκευση δεδομένων στο genesis block διασφαλίζονται οι παρακάτω δυνατότητες.

- **Συνέπεια:** Λόγω του ότι το όργανο διακυβέρνησης (government body) του blockchain δημιουργεί και ενημερώνει το genesis block, η αυθαίρετη δημιουργία καταστάσεων στο μπλοκ δεν θεωρείται παραβίαση συνέπειας καθώς το περιεχόμενο του μπλοκ είναι διαφανές.

- **Αφάνεια (Latency):** Η μεταφορά αρχείων από το genesis block είναι γρήγορη, καθώς μόνο αυτό χρησιμοποιείται για την αναδημιουργία κατάστασης.

- **Μειωμένο Κόστος:** Δεν υπάρχουν χρεώσεις συναλλαγής, καθώς η καθολική κατάσταση αρχικοποιείται στη διαμόρφωση του genesis block, σε σχέση με τη χρήση των υπόλοιπων συναλλαγών.

Το συγκεκριμένο πρότυπο μπορεί να χρησιμοποιηθεί για την αναδημιουργία εγγενών στοιχείων οποιασδήποτε νέας παρουσίας στην αλυσίδα [31].

Καθώς οι χρήστες εντός του δικτύου του Blockchain έχουν τα ίδια προνόμια, τα δεδομένα αυτού είναι προσβάσιμα από όλους. Στην περίπτωση όμως που τα δεδομένα μιας συναλλαγής θα πρέπει να είναι προσβάσιμα μόνο από αυτούς που την πραγματοποιούν, δηλαδή είναι είτε ευαίσθητα είτε αφορούν εμπορική συναλλαγή, χρησιμοποιείται το **Encrypting on-Chain Data pattern,** σε συνέχεια του Raw on-chain pattern, για την κρυπτογράφηση των δεδομένων πριν αυτά προστεθούν στην αλυσίδα.

Το **Legal and Smart Pair pattern** επέρχεται του Hash on-chain pattern, το οποίο εμφανίζεται στο μοντέλο απόφασης απόδοσης. Παρέχει μία αμφίδρομη δέσμευση μεταξύ μιας νομικής συμφωνίας και του αντίστοιχου smart contract για την παροχή έγκυρης πηγής στη νομική σύμβαση. Η δέσμευση των δύο κατευθύνσεων βασίζεται στον κατακερματισμό της νομικής συμφωνίας και στην αμετάβλητη διεύθυνση του έξυπνου συμβολαίου [30].

5.3.2 Απόδοση

Στην συνέχεια αναλύονται τα πρότυπα που χρησιμοποιούνται για να αντιμετωπίζουν περιπτώσεις εφαρμογών με μεγάλο όγκο δεδομένων.

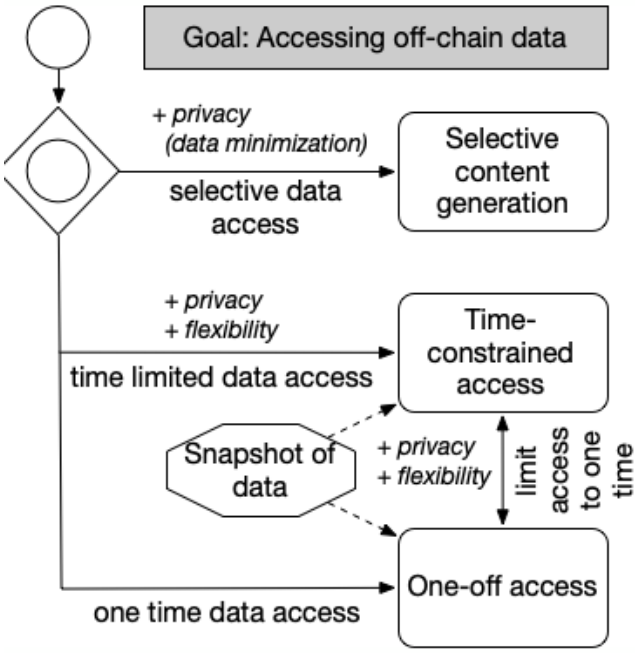
Αν ο όγκος δεδομένων είναι μεγαλύτερος από το μέγεθος της συναλλαγής τότε δεν μπορεί να αποθηκευτεί εντός της αλυσίδας, έτσι το **Hash-on-chain pattern** χρησιμοποιείται για να αποθηκεύσει μια κρυπτογραφική αναπαράσταση των δεδομένων (π.χ. hashing τιμή), εντός του Blockchain, για να αποδείξει ότι αυτή η αναπαράσταση αντικατοπτρίζει τον μεγάλο όγκο δεδομένων που βρίσκεται εκτός αλυσίδας. Για περαιτέρω βελτίωση της επεκτασιμότητας και υποστήριξης μεγάλου όγκου δεδομένων, μπορούν να χρησιμοποιηθούν πιο σύνθετες δομές δεδομένων που βασίζονται στο κατακερματισμό, όπως ένα δέντρο Merkle, με το **Merkle tree root on chain pattern**.

Ένα άλλο πρότυπο, για την διαχείριση μεγάλου όγκου δεδομένων είναι το **State Aggregation pattern**, το οποίο συγκεντρώνει ένα σύνολο καταστάσεων σε ένα μικρό ή ενιαίο υποσύνολο καταστάσεων. Για

παράδειγμα κατά την ανταλλαγή δεδομένων στο Blockchain, το υπόλοιπο κλεισίματος ενός συνόλου λογαριασμών μπορεί να αντικαταστήσει το υπόλοιπο κλεισίματος μεμονωμένων λογαριασμών. Ωστόσο, αυτό το πρότυπο περιορίζεται από τον τύπο δεδομένων που θα συγκεντρωθεί. Από την άλλη, το **State Channel pattern** καταγράφει μόνο την τελική διακανονισμένη συναλλαγή στο Blockchain και τις ενδιάμεσες συναλλαγές τις διαχειρίζεται εκτός αλυσίδας. Επειδή όμως, τα ακατέργαστα δεδομένα είναι εκτός αλυσίδας, υπάρχει ο κίνδυνος αλλαγής δεδομένων χωρίς εξουσιοδότηση, επηρεάζοντας την ακεραιότητα του συστήματος [32].

5.4 Έλεγχος πρόσβασης δεδομένων εκτός αλυσίδας

Καθώς τα δεδομένα που είναι αποθηκευμένα μέσα στο Blockchain είναι προσβάσιμα από όλους τους χρήστες του δικτύου, ένας τρόπος για να διασφαλιστεί το απόρρητο είναι να διατηρηθούν τα ευαίσθητα δεδομένα εκτός αλυσίδας. Ανάλογα με την περίπτωση χρήσης και τα πρότυπα που υπάρχουν εκτελείται έλεγχος πρόσβασης στα δεδομένα που βρίσκονται εκτός αλυσίδας όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 15, Έλεγχος δεδομένων εκτός αλυσίδας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/datamgnmodel/)

Κατά την αποθήκευση των δεδομένων εκτός αλυσίδας θα πρέπει να ληφθούν υπόψιν κάποιοι περιορισμοί που αφορούν το περιεχόμενο και τον

χρόνο πρόσβασης στα δεδομένα. Αν η πρόσβαση στα δεδομένα θα πρέπει να είναι περιορισμένη για να διασφαλιστεί το απόρρητο θα πρέπει να εφαρμοστεί το **Selective Content Generation pattern.** Με αυτό το πρότυπο εμφανίζονται τα δεδομένα με βάση τους κανόνες πρόσβασης που έχουν τεθεί, προς αποφυγή της διαρροής περιττών δεδομένων. Δηλαδή, οι εκδότες πιστοποιητικών θα μπορούσαν να εκδίδουν ένα προσαρμοσμένο διαπιστευτήριο με βάση τις απαιτήσεις των κατόχων, για παράδειγμα το πιστοποιητικό να περιλαμβάνει μόνο το βαθμό για ένα μάθημα χωρίς να αποκαλύπτει ολόκληρο το αντίγραφο με τους βαθμούς των υπόλοιπων μαθημάτων.

Όταν η πρόσβαση στα δεδομένα εκτός αλυσίδας θα πρέπει να είναι χρονικά περιορισμένη αντιστοιχεί το **Time Constrained Access pattern** για επιβολή χρόνου πρόσβασης σε αυτά. Για παράδειγμα, ένας εργαζόμενος μπορεί να προωθήσει στον εργοδότη έναν σύνδεσμο με το πιστοποιητικό του, θέτοντας ένα χρονικό πλαίσιο πρόσβασης σε αυτό. Τέλος, το **One-off access pattern** εφαρμόζεται για να επιτρέπει μόνο μια φορά πρόσβαση στα δεδομένα. Επίσης, μπορεί να γενικευτεί παρέχοντας πρόσβαση ως ένα προκαθορισμένο αριθμό φορών.

Ένας κίνδυνος που ελλοχεύει στις τελευταίες δύο περιπτώσεις είναι ότι ένας κακόβουλος χρήστης μπορεί να τραβήξει στιγμιότυπο των περιεχομένων και να μπορεί να διαβάσει τα δεδομένα μετά τη λήξη του χρονικού περιορισμού πρόσβασης [26].

5.5 Ασφάλεια

Η ασφάλεια τόσο των δεδομένων όσο και των χρηστών σε ένα δίκτυο Blockchain είναι η κυριότερη ανησυχία που υπάρχει καθ' όλη εφαρμογή του. Σε αυτήν την ενότητα αναλύονται δύο μοντέλα απόφασης που αφορούν την ασφάλεια (έλεγχος ταυτότητας και εξουσιοδότηση). Η βασική διαφορά των δύο είναι ότι με τον έλεγχο ταυτότητας επαληθεύεται ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι, ενώ με την εξουσιοδότηση εξετάζεται εάν ο χρήστης έχει άδεια πρόσβασης σε μια υπηρεσία.

5.5.1 Έλεγχος Ταυτότητας

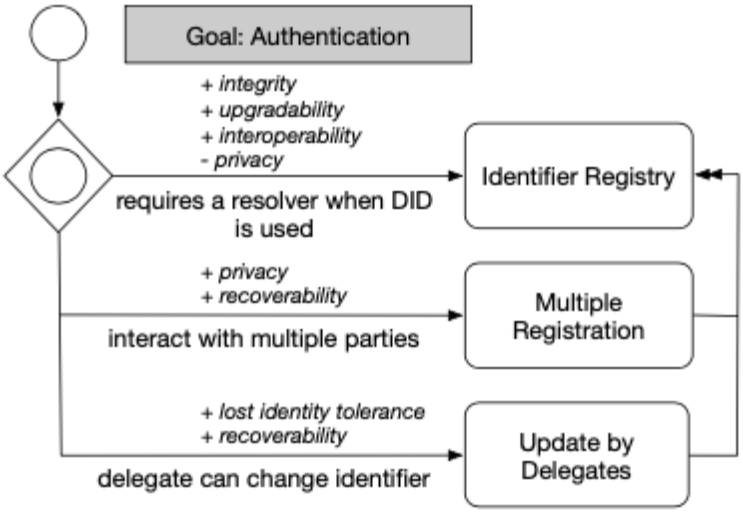
Ο έλεγχος ταυτότητας στο Blockchain διασφαλίζει ότι ένας λογαριασμός είναι αυτός που ισχυρίζεται. Η ταυτότητα ενός λογαριασμού

ορίζεται ως ένα σύνολο χαρακτηριστικών που πιστοποιούν έναν χρήστη. Υπάρχουν διάφορα είδη ελέγχου που μπορούν να χρησιμοποιηθούν για την διαχείριση της ταυτότητας μιας οντότητας, τα οποία εμφανίζονται στο παρακάτω μοντέλο απόφασης [33].

- Το **Identifier Registry**, διατηρεί τις συνδέσεις μεταξύ ενός αναγνωριστικού(identifier) και των αντίστοιχων χαρακτηριστικών ταυτότητας με την βοήθεια ενός μητρώου.

- Το **Multiple Registration**, εγγράφει ή χρησιμοποιεί ξεχωριστό αναγνωριστικό για κάθε σχέση συναλλαγής.

- Το **Update by Delegates**, διατηρεί μια λίστα εκπροσώπων που μπορούν να βοηθήσουν τον χρήστη να ανακτήσει μια χαμένη ταυτότητα.



Εικόνα 16, Έλεγχος Ταυτότητας (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/securitymodel/)

Ένα αναγνωριστικό (identifier) είναι μια μοναδική συμβολοσειρά που μπορεί να προσδιορίσει αποκλειστικά μια οντότητα. Όπως αναφέρθηκε και πιο πάνω η αντιστοίχιση μεταξύ αναγνωριστικών και αντίστοιχων στοιχείων ταυτότητας μπορεί να καταχωρηθεί σε ένα μητρώο. Η διατήρηση ενός τέτοιου κοινόχρηστου μητρώου βελτιώνει σε μεγάλο βαθμό τη λειτουργικότητα του συστήματος, καθώς μπορεί να χρησιμοποιηθεί ως λύση για ένα αποκεντρωμένο αναγνωριστικό από διαφορετικά Blockchains. Ωστόσο, η χρήση ενός μόνο αναγνωριστικού για

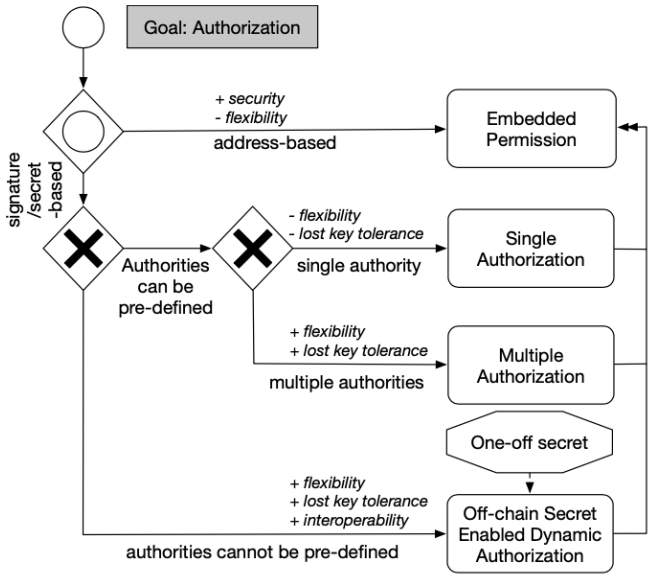
συναλλαγές από διαφορετικές εφαρμογές μπορεί να οδηγήσει σε προβλήματα απορρήτου, αφού μπορεί να εκθέσει πληροφορίες για τον κάθε χρήστη [34].

Το Multiple Registration, επιτρέπει σε έναν χρήστη να έχει ξεχωριστό αναγνωριστικό για κάθε εφαρμογή/ρόλο. Ένα τέτοιο είδος απομονώνει τις αλληλεπιδράσεις του ενός μέρους με το άλλο, ελαχιστοποιώντας την δυνατότητα σύνδεσης μιας ταυτότητας.

Το Update by Delegates συμπληρώνει το Identifier Registry και επιτρέπει σε ένα identifier να συσχετιστεί με μια λίστα εκπροσώπων ανάκτησης που θα μπορούσαν να χειριστούν την αντίστοιχη ταυτότητα στη θέση του κατόχου. Δηλαδή, αν ένα private key χαθεί, ο κάτοχος του δεν θα έχει πρόσβαση στο δίκτυο. Ο κάτοχος του κλειδιού θα πρέπει να δημιουργήσει ένα νέο ζεύγος κλειδιών (private και public key) και να κάνει αίτηση ανάκτησης του παλιού ζεύγους κλειδιών και να το συσχετίσει με το νέο ζεύγος με τη συμβολή των εκπροσώπων ανάκτησης. Παρόμοιο παράδειγμα με τις πλατφόρμες κοινωνικής δικτύωσης που σε περίπτωση απώλειας στοιχείων πρόσβασης, μετά από επικοινωνία με το τμήμα εξυπηρέτησης πελατών ανακτώνται τα στοιχεία πρόσβασης του χρήστη [35].

5.5.2 Εξουσιοδότηση

Οι έξυπνες συμβάσεις που αναπτύσσονται στο blockchain είναι προσβάσιμες σε όλους τους χρήστες της πλατφόρμας. Έτσι, μια permissionless λειτουργία μπορεί να ενεργοποιηθεί από οποιονδήποτε [33].



Εικόνα 17, Εξουσιοδότηση (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/securitymodel/)

Το **Embedded Permission pattern** περιορίζεται στην επίκληση μεμονωμένων λειτουργιών στο έξυπνο συμβόλαιο σε ένα επιτρεπόμενο σύνολο λογαριασμών και μπορεί να εφαρμοστεί σε μια έξυπνη σύμβαση για την παροχή εξουσιοδότησης σε επίπεδο λειτουργίας. Για κάθε επίκληση μιας λειτουργίας, μπορούν να χρησιμοποιηθούν διάφορα πρότυπα εξουσιοδότησης, τα οποία παρέχουν διαφορετικά επίπεδα ευελιξίας και κόστους.

- Όταν μόνο μια αρχή επιτρέπεται να εγκρίνει μόνο μια δραστηριότητα, τότε χρησιμοποιείται το **Single Authorization pattern**.

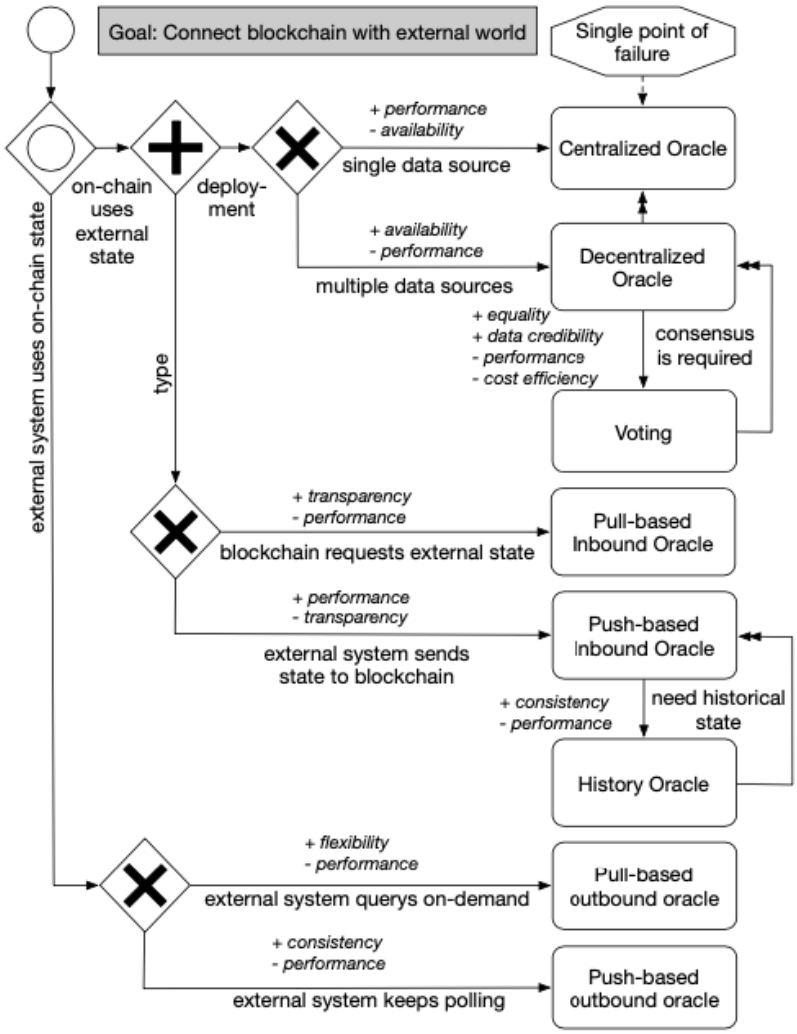
- Κάποιες φορές, μπορεί να χρειαστούν πολλές υπογραφές για τον καθορισμό του αριθμού των αρχών που απαιτούνται για την έγκριση μιας συναλλαγής, αυτό είναι χρήσιμο όταν απαιτούνται περισσότερες

από μία αρχές για την έγκριση μιας δραστηριότητας ή όταν ένα υποσύνολο αρχών δεν είναι διαθέσιμο την στιγμή της εξουσιοδότησης. Σε τέτοιες περιπτώσεις, το **Multiple Authorization pattern** παρέχει μεγαλύτερη ευελιξία. Παρόλο που εδώ επιτρέπεται η ευέλικτη διασύνδεση μεταξύ της λειτουργίας και των αρχών εξουσιοδότηση, θα πρέπει αυτές οι αρχές να οριστούν από πριν στο smart contract.

- Όταν η αρχή για την εξουσιοδότηση μιας δραστηριότητας δεν είναι γνωστή εκ των προτέρων, χρησιμοποιείται το **off-chain Secret Enable Dynamic Authorization pattern**. Η κλήση της συνάρτησης που εξουσιοδοτεί μια λειτουργία παίρνει μια τιμή κατακερματισμού, η οποία βρίσκεται εκτός αλυσίδας. Όποιος γνωρίζει αυτή την τιμή μπορεί να εξουσιοδοτεί την συνάρτηση εξουσιοδότησης μιας λειτουργίας χρησιμοποιώντας μια συναλλαγή. Το έξυπνο συμβόλαιο γνωρίζει από πριν την προκαθορισμένη τιμή κατακερματισμού και την συγκρίνει με αυτή που έδωσε ο εξουσιοδότης της λειτουργίας. Αν συμφωνούν οι δύο τιμές τότε εκτελείται η λειτουργία. Μια εσφαλμένη τιμή κατακερματισμού που δίνεται δεν μπορεί να ξαναχρησιμοποιηθεί.

5.6 Αλληλεπίδραση με τον εξωτερικό κόσμο

Από την άποψη της αρχιτεκτονικής λογισμικού, ένα Blockchain θα μπορούσε να χρησιμοποιηθεί ως σύνδεσμος σε ένα μεγάλο σύστημα λογισμικού. Οι λύσεις που βασίζονται σε Blockchain συνήθως λαμβάνουν/στέλνουν δεδομένα από/προς μέρη που βρίσκονται εκτός αλυσίδας. Ένα oracle χρησιμοποιείται για να γεφυρώσει το Blockchain με τον έξω κόσμο. Ένα oracle εξαρτάται από τρείς περιπτώσεις, ανάλογα με την κατεύθυνση ροής των δεδομένων, από που προέρχεται η ροή δεδομένων και την αποκέντρωση ανάπτυξης. Τα πρότυπα που παρουσιάζονται στο παρακάτω μοντέλο απόφασης καλύπτουν αυτές τις τρεις περιπτώσεις.



Εικόνα 18, Oracle (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/oraclemodel/)

Όταν πρόκειται για περιπτώσεις ανάπτυξης του oracle, εφαρμόζεται το **Centralized Oracle** για να συλλέξει μια εξωτερική κατάσταση. Το Centralized Oracle εισάγει ένα αξιόπιστο τρίτο μέρος στο σύστημα για να επαληθεύσει την εξωτερική κατάσταση που σύλλεξε. Το συγκεκριμένο στοιχείο που σύλλεξε το centralized oracle μετατρέπεται σε ένα σημείο αποτυχίας (single point of failure), το οποίου η μη διαθεσιμότητα, η αποτυχία ή ο συμβιβασμός μπορεί να εμποδίσει το Blockchain να ολοκληρώσει την συναλλαγή. Για να ξεπεραστεί αυτό το σημείο αποτυχίας χρησιμοποιείται ένα **Decentralized Oracle** που αποτελείται από πολλούς εξωτερικούς διακομιστές και ανεξάρτητες πηγές δεδομένων. Σε αυτή την περίπτωση, χρησιμοποιείται το **Voting pattern** μαζί με τα πολλαπλά Decentralized Oracles για να επιτευχθεί συναίνεση σχετικά με την εξωτερική κατάσταση που εισήγαγε το Centralized Oracle. Εάν το

αποτέλεσμα που θα δοθεί είναι αμφιλεγόμενο, τότε οποιοσδήποτε με λογαριασμό μπορεί να προτείνει μια νέα απάντηση και να ψηφίσει νέο αποτέλεσμα έως ότου επιτευχθεί συναίνεση.

Ο πρώτος παράγοντας που λαμβάνεται υπόψη για το ποιο πρότυπο πρόκειται να επιλεχθεί είναι η κατεύθυνση ροής δεδομένων. Αν τα δεδομένα ρέουν από τον εξωτερικό κόσμο προς το blockchain, χρησιμοποιείται ένα **Inbound Oracle** για να μεταφέρει τα δεδομένα από τον εξωτερικό κόσμο προς το σύστημα. Ανάλογα με το από που ξεκινά η ροή των δεδομένων επιλέγεται ένα **Pull-based Inbound Oracle** ή ένα **Push-based Inbound Oracle**.

- Όταν ένα smart contract ζητά δεδομένα που βρίσκονται εκτός αλυσίδας, το Pull-based Inbound Oracle λαμβάνει το αίτημα, συγκεντρώνει την κατάσταση από τα στοιχεία εκτός αλυσίδας και στέλνει πίσω την κατάσταση στο smart contract εκτελώντας μια συναλλαγή. Η συγκεκριμένη διαδικασία είναι διαφανής καθώς υλοποιείται χρησιμοποιώντας έξυπνα συμβόλαια. Η απόδοση του Pull-based Inbound Oracle περιορίζεται από τον ρυθμό συναλλαγής του δικτύου και από τον χρόνο που απαιτείται για την συλλογή εξωτερικών δεδομένων αφότου υποβληθεί το αίτημα στο oracle.

- Ένα Push-based Inbound Oracle χρησιμοποιεί στοιχεία εκτός αλυσίδας για να επιβλέπει τις εξωτερικές αλλαγές δεδομένων και να εισάγει τυχόν ενημερώσεις στο Blockchain. Αυτό βελτιώνει την απόδοση καθώς το smart contract που καλεί το oracle δεν χρειάζεται να περιμένει για να τελειώσει ολόκληρη η συλλογή δεδομένων. Ωστόσο, επειδή αυτό το oracle δεν αναπτύσσεται στο blockchain ως έξυπνο συμβόλαιο και η παροχή δεδομένων εξαρτάται από ένα στοιχείο εκτός αλυσίδας δεν διαθέτει τις ίδιες εγγυήσεις ασφάλειας όπως προηγουμένως.

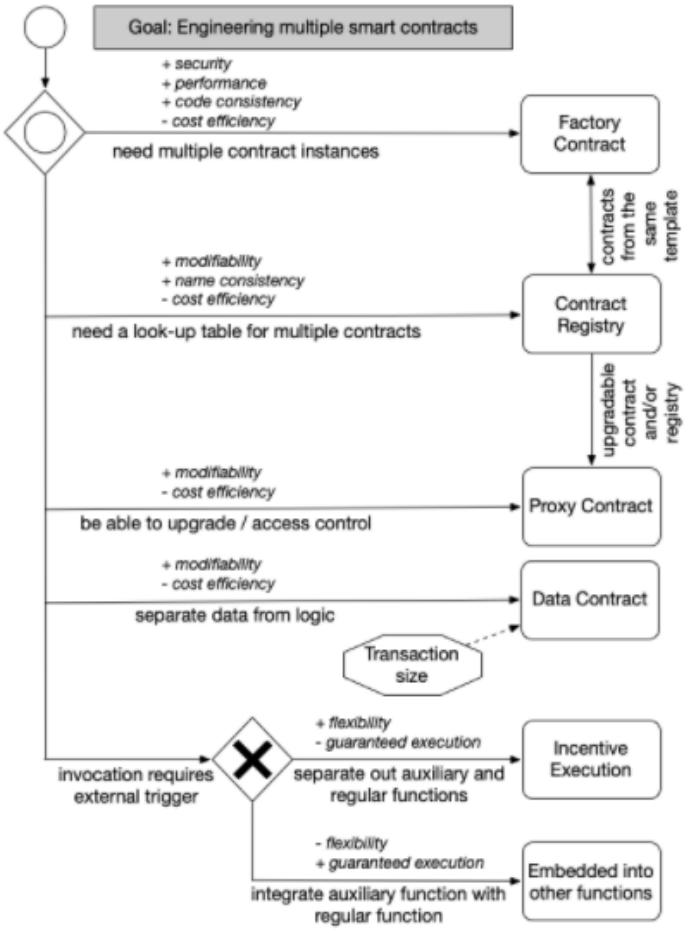
- Αν η περίπτωση χρήσης πρέπει να επιλύσει χρονικές διενέξεις, το **History Oracle** μπορεί να εφαρμοστεί για να συμπληρώσει το Push-based Inbound Oracle για να παρέχει ιστορικές τιμές στα δεδομένα εκτός αλυσίδας.

Στην περίπτωση που τα δεδομένα ρέουν από το Blockchain στον εξωτερικό κόσμο χρησιμοποιείται ένα **Outbound Oracle** για να μεταφέρει τα δεδομένα από το Blockchain στον εξωτερικό κόσμο. Παρόμοια στο

τρόπο λειτουργίας με τα Inbound Oracles υπάρχουν τα **Push-based Outbound Oracle** και **Pull-based Outbound Oracle**. Το πρώτο όπως και το inbound επιβλέπει το Blockchain και ενημερώνει τον εξωτερικό κόσμο για τυχόν ενημερώσεις, δίνοντας έγκριση για σχετικές δραστηριότητες εκτός αλυσίδας. Εναλλακτικά, το pull-based outbound oracle αναζητά δεδομένα εντός της αλυσίδας κατόπιν αιτήματος [36].

5.7 Έξυπνα Συμβόλαια

Η δομή ενός έξυπνου συμβολαίου επηρεάζει το κόστος εκτέλεσης του. Σε ένα δημόσιο Blockchain, το κόστος ανάπτυξης ενός έξυπνου συμβολαίου εξαρτάται από το μέγεθος του. Στη περίπτωση που ενσωματωθούν επιπρόσθετα δεδομένα σε αυτό καταβάλλονται πρόσθετες χρεώσεις. Έτσι, το κόστος αποθήκευσης δεδομένων είναι ανάλογο με το μέγεθος του έξυπνου συμβολαίου και την κατάσταση του. Το παρακάτω μοντέλο απόφασης αναλύει τα όσα αναφέρθηκαν [37].



Εικόνα 19, Smart Contracts (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/contractmodel/)

Ανάλογα με το τι αναμένεται να πετύχουν τα έξυπνα συμβόλαια γίνεται επιλογή των κατάλληλων προτύπων.

Για να διατηρηθεί ένα κεντρικό μητρώο με όλα τα έξυπνα συμβόλαια που σχετίζονται με μια εφαρμογή, χρησιμοποιείται το **Contract Registry** εντός αλυσίδας [38]. Ένα τέτοιο μητρώο συσχετίζει τα ονόματα που δίνει ο χρήστης στα έξυπνα συμβόλαια με την διεύθυνση των αντίστοιχων έξυπνων συμβολαίων μέσα στο Blockchain. Όταν θα πρέπει να χρησιμοποιηθούν περιπτώσεις από διαφορετικά έξυπνα συμβόλαια που έχουν ήδη αναπτυχθεί στο σύστημα, ώστε να δημιουργηθεί ένα νέο smart contract, χρησιμοποιείται το **Factory Contract pattern** [39]. Όλες οι περιπτώσεις δημιουργίας έξυπνων συμβολαίων από την περίπτωση του Factory Contract μπορούν να καταγραφούν στο μητρώο έξυπνων συμβάσεων (Contract Registry). Το **Proxy Contract pattern** ενεργοποιεί τα αναβαθμίσιμα έξυπνα συμβόλαια και κάνει έλεγχο πρόσβασης κατά την επίκληση ενός smart contract. Όλα τα έξυπνα συμβόλαια που καλούνται περνούν μέσω του διακομιστή μεσολάβησης (proxy), ο οποίος με την σειρά του ανακατευθύνει τη συναλλαγή με βάσει την πιο πρόσφατη έκδοση του έξυπνου συμβολαίου. Μόλις γίνει νέα έκδοση ενός έξυπνου συμβολαίου ο διακομιστής μεσολάβησης ενημερώνεται για να αναφέρεται στις νέες συμβάσεις.

Το **Data Contract pattern** ακολουθεί την αρχή με την οποία σχεδιάστηκε το λογισμικό διαχωρίζοντας τα δεδομένα βάσει της λογικής της εκάστοτε επιχείρησης. Επίσης, ενσωματώνει δεδομένα και δημιουργεί/διαβάζει/ενημερώνει/διαγράφει στα ενσωματωμένα δεδομένα των έξυπνων συμβολαίων μέσω εξουσιοδοτημένων συναλλαγών. Το μέγεθος των δεδομένων εντός της αλυσίδας περιορίζεται από το μέγεθος του μπλοκ, όπως στα πλείστα πρότυπα εντός της αλυσίδας. Το Data contract pattern αυξάνει το κόστος λόγω του μεγάλου μεγέθους του κώδικα έξυπνης σύμβασης και της πρόσθετης πολυπλοκότητας κατά την εκτέλεση του [40].

Τα έξυπνα συμβόλαια βασίζονται σε συμβάντα που δεν μπορούν να εκτελεστούν αυτόνομα. Μια συναλλαγή ή ένα έξυπνο συμβόλαιο ενεργοποιεί τις λειτουργίες αλλαγής κατάστασης που ορίζονται σε άλλο έξυπνο συμβόλαιο. Στην περίπτωση που μπορεί να χρειαστεί να εκτελούνται βοηθητικές λειτουργίες ασύγχρονα για την πραγματοποίηση διάφορων εργασιών, όπως αυτόματες πληρωμές μερισμάτων και καθαρισμός ληγμένων αρχείων, χρησιμοποιούνται τα **Incentive Execution pattern** και **Embedded into other functions pattern.**

6 Blockchain για επικύρωση της γνησιότητας τίτλων σπουδών ή άλλων δικαιολογητικών

6.1 Εισαγωγή

Στον σύγχρονο ψηφιακό κόσμο οι παραδοσιακοί τρόποι να εκτελούνται κάποιες διαδικασίες αλλάζουν. Οι περισσότερες από τις συναλλαγές πλέον είναι διαδικτυακές. Τα έγγραφα που προκύπτουν από αυτές τις συναλλαγές αποθηκεύονται σε βάσεις δεδομένων υπό τον έλεγχο ενός κεντρικού διαχειριστή. Αυτό δημιουργεί κινδύνους για επιθέσεις από μη εξουσιοδοτημένα άτομα ή υπάρχει δυνατότητα από τον κεντρικό διαχειριστή να τροποποιήσει ή να διαγράψει τα υπάρχοντα δεδομένα προς το δικό του όφελος.

Το πρόβλημα των πλαστών πιστοποιητικών ξεκίνησε από πολλά χρόνια πριν. Υπάρχουν αρκετά περιστατικά όπου πλαστογραφούνται εκπαιδευτικά πιστοποιητικά, με αντίκτυπο την υποβάθμιση της ποιότητας του εκπαιδευτικού συστήματος. Οι επιπτώσεις του παραπάνω προβλήματος δεν περιορίζονται μόνο στην εκπαίδευση αλλά και στο τομέα της αγοράς εργασίας, αφού πολλοί εργοδότες εξαπατώνται από πλαστά πιστοποιητικά εκπαιδευτικών ιδρυμάτων από τους υποψήφιους αγοραστές εργασίας[41] [42].

Η κοινωνία χρειάζεται μια τεχνολογία που θα μπορεί να εμποδίσει την αλλοίωση και την πλαστογραφία αυτών των πιστοποιητικών. Εδώ, είναι που έρχεται η τεχνολογία Blockchain να διασώσει αυτό το μείζον πρόβλημα. Όπως αναφέρθηκε, το Blockchain είναι μια τεχνολογία κατανεμημένου βιβλίου όπου τα δεδομένα διανέμονται σε όλους τους κόμβους. Παρέχει διαφάνεια, δημόσια επαλήθευση και αμετάβλητο στα δεδομένα που αποθηκεύονται σε αυτό, εξασφαλίζοντας ακεραιότητα των δεδομένων με την βοήθεια ενός μηχανισμού προστασίας [43].

6.2 Προβλήματα αποθήκευσης πιστοποιητικών με υπάρχουσες μεθόδους

Τα περισσότερα έγραφα που χρησιμοποιούμε καθημερινά είναι σε έντυπη μορφή. Οι υποψήφιοι για εργασία ετοιμάζουν αντίγραφα εκπαιδευτικών και επαγγελματικών πιστοποιητικών παραθέτοντας τα στους οργανισμούς και χρειάζεται αρκετός χρόνος για τον χειροκίνητο έλεγχο τους. Αυτά τα περιστατικά αποδεικνύουν ότι οι τρέχουσες μέθοδοι διατήρησης των πιστοποιητικών δεν είναι αποτελεσματικές. Παρακάτω αναφέρονται τα κύρια προβλήματα που τυχόν να παρουσιάζονται με την διατήρηση αυτών των μεθόδων [44].

i. Οι υπάρχουσες μέθοδοι διαδικασίας πιστοποίησης είναι αρκετά χρονοβόρες και υπάρχουν κίνδυνοι να προκληθούν σφάλματα καθώς οι διαδικασίες αυτές έχουν να κάνουν με ανθρώπους.

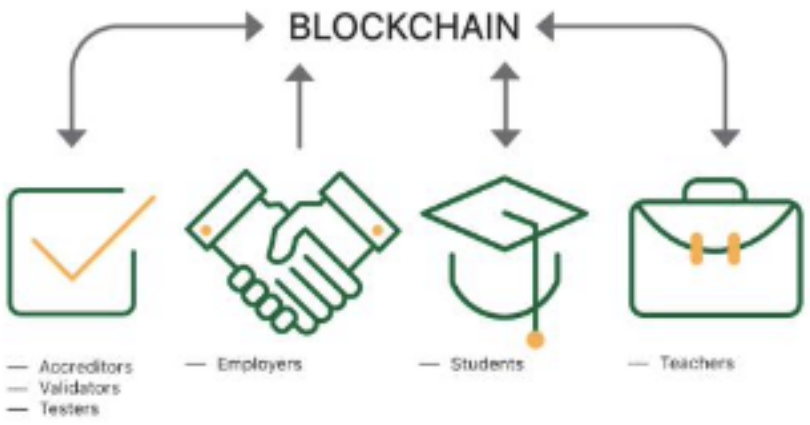
ii. Δεν υπάρχει αξιόπιστος τρόπος ελέγχου της γνησιότητας του πιστοποιητικού, καθώς χρειάζεται αρκετός χρόνος να ελεγχθεί η εγκυρότητα ενός εγγράφου.

iii. Τα πιστοποιητικά που εκδίδονται από ιδρύματα είναι επιρρεπή σε κακόβουλες ενέργειες.

iv. Η ανάκτηση χαμένων πιστοποιητικών είναι περίπλοκη αφού περιλαμβάνει πολύ διαδικασία και κόστος.

6.3 Πλεονεκτήματα χρήσης Blockchain για τη διαχείριση πιστοποιητικών

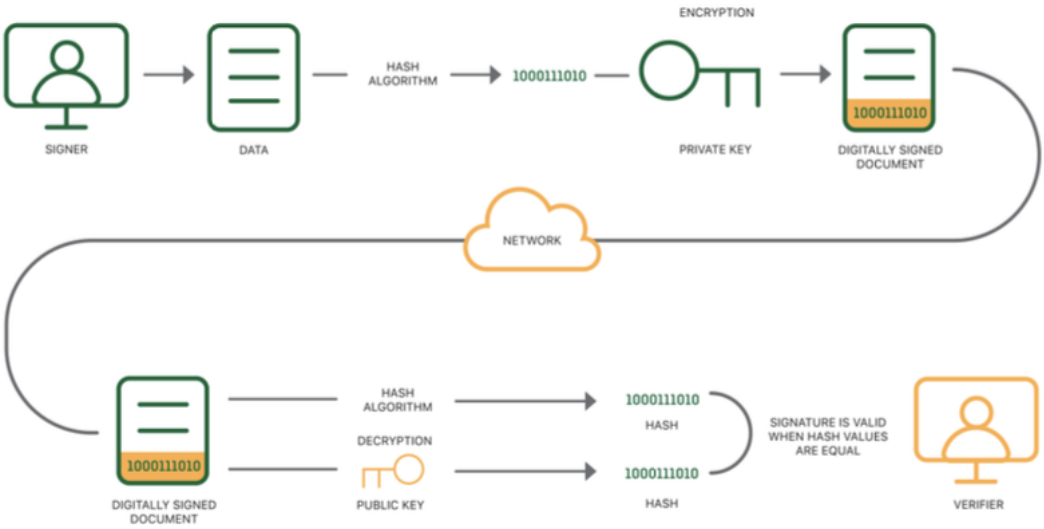
Παρόλο που το Blockchain ξεκίνησε ως κρυπτονόμισμα, αργότερα εξελίχθηκε σε μια πλατφόρμα που λειτουργεί για την ανάπτυξη εφαρμογών, που χρησιμοποιούνται σε τομείς όπως η υγεία, η οικονομία, συστήματα πληρωμών κλπ. Καθώς, όπως αναφέρθηκε, το Blockchain είναι αμετάβλητο και επαληθεύσιμο, ταιριάζει ακριβώς στην φιλοσοφία της διαχείρισης των πιστοποιητικών, παρέχοντας ποικίλα πλεονεκτήματα [44], [43]. Πρώτον, τα πιστοποιητικά αποθηκεύονται μόνιμα με κρυπτογράφηση και είναι σχεδόν αδύνατον κάποιος να αλλάξει την κατάσταση τους. Δεύτερον, οτιδήποτε θα αλλάξει πάνω στο έγγραφο, δημιουργείται μια νέα συναλλαγή και προστίθεται σε νέο block στο καθολικό. Άρα θα φαίνεται πως είναι ανεξάρτητο από το αρχικό. Τέλος, η επαλήθευση ατόμων και συναλλαγών σε αυτό γίνεται αυτοματοποιημένα χωρίς να επεμβαίνει ο άνθρωπος, άρα αυξάνεται η ταχύτητα και μειώνονται τα λάθη και αυξάνεται η ασφάλεια.



Εικόνα 20,Πιστοποίηση τίτλων σπουδών με Blockchain (Πηγή: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf)

6.4 Έκδοση πιστοποιητικών με την χρήση ψηφιακών υπογραφών (Digital Signatures)

Κάθε φορά που πιστοποιείται ένα ψηφιακό έγγραφο χρησιμοποιείται η ψηφιακή υπογραφή, η οποία είναι διαφορετική από την χειρόγραφη υπογραφή που χρησιμοποιείται στα σαρωμένα έγγραφα. Η κύρια διαφορά τους είναι ότι η ψηφιακή υπογραφή παρέχει περισσότερη ασφάλεια στην πιστοποίηση λόγω της συνάρτησης λειτουργίας της[45].



Εικόνα 21,Διαδικασία ψηφιακής υπογραφής εγγράφου (Πηγή: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf)

Στις ψηφιακές υπογραφές χρησιμοποιείται ένα ιδιωτικό και ένα δημόσιο κλειδί, για να πιστοποιηθεί ένα ψηφιακό πιστοποιητικό γίνεται συνδυασμός των δύο. Για να ενισχυθεί η ασφάλεια του πιστοποιημένου εγγράφου προστίθεται στο συνδυασμό και ο χρόνος στον οποίο έγινε η διαδικασία, άρα εξασφαλίζεται η μοναδικότητα του παραγόμενου εγγράφου.

Αν κάποιο άλλο άτομο θέλει να ελέγξει την εγκυρότητα της πιστοποίησης του εγγράφου πρέπει να γνωρίζει το δημόσιο κλειδί. Δεν τίθεται θέμα να εκτεθούν επιπλέον αχρείαστες πληροφορίες μέσω του δημόσιου κλειδιού αφού αν κάποιος το γνωρίζει δεν σημαίνει ότι γνωρίζει περαιτέρω πληροφορίες για την ταυτότητα που υπέγραψε το έγγραφο. Με

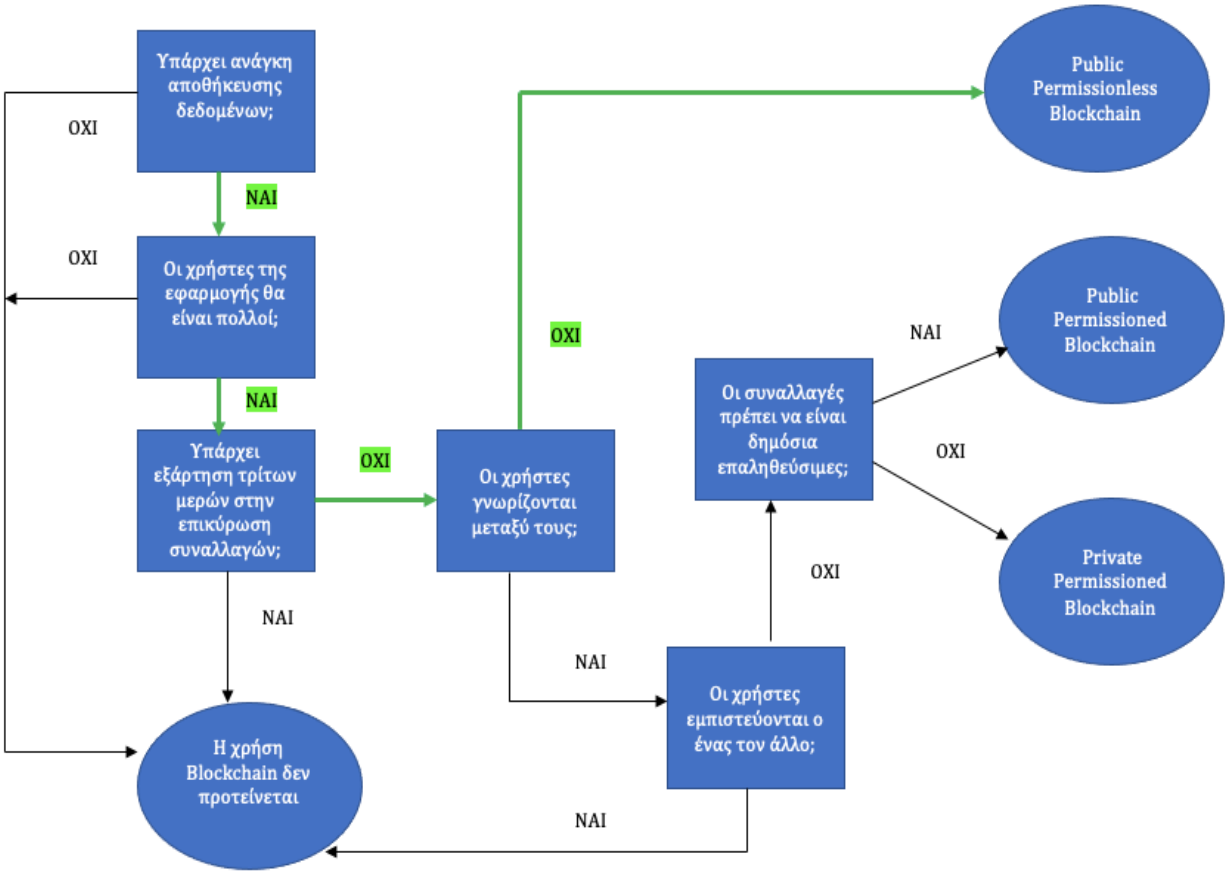
την εισαγωγή του δημόσιου κλειδιού στο σύστημα που πιστοποιεί το έγγραφο ελέγχεται η εγκυρότητα της ψηφιακής υπογραφής, διασφαλίζοντας πάντα ότι το ιδιωτικό κλειδί δεν γίνεται γνωστό από κανέναν άλλον πλην του ιδιοκτήτη του [46].

6.5 Συστήματα διαχείρισης πιστοποιητικών που βασίζονται σε Blockchain

Ένα σύστημα που χρησιμοποιείται για την ανάπτυξη εφαρμογών για την επαλήθευση και την ακαδημαϊκών και επαγγελματικών πιστοποιητικών στο Blockchain είναι το Blockerts, το οποίο παρέχει μηχανισμούς για τη δημιουργία, προβολή, έκδοση και επαλήθευση πιστοποιητικών βασισμένο σε blockchain δημόσιου κώδικα. Το Blockerts χρησιμοποιείται από ορισμένα πανεπιστήμια συμπεριλαμβανομένου του MIT, του πανεπιστημίου Λευκωσίας (UNIC) και του Πανεπιστημίου του Birmingham. Το UNIC χρησιμοποιεί το blockchain για χορήγηση εκπαιδευτικού πιστοποιητικού. Το εργαστήριο του MIT το χρησιμοποιεί για τη διαχείριση ψηφιακών πιστοποιητικών. Παρέχει στους χρήστες έλεγχο στα πιστοποιητικά και απαλείφει τη συμμετοχή τρίτων προσώπων για την έκδοση, αποθήκευση και επαλήθευση διαπιστευτηρίων. Η μεθοδολογία πιστοποίησης λειτουργεί στη διαδικασία που ο χρήστης υπογράφει και αποθηκεύει το hash του στο blockchain κατά τη συναλλαγή, η έξοδος της οποίας δίνεται στον χρήστη. Απαιτεί έναν αποτελεσματικό μηχανισμό απορρήτου καθώς όλοι μπορούν να έχουν πρόσβαση στα δεδομένα της αλυσίδας. Άλλα συστήματα διαχείρισης πιστοποιητικών είναι το Digicert, το Smartect και το RecordsKeeper, τα οποία είναι και αυτά βασισμένα σε ένα public Blockchain [46].

6.6 Εφαρμογή Blockchain για έκδοση ψηφιακών πιστοποιήσεων στην εκπαίδευση / Ανάλυση Use case

6.6.1 Επιλογή τύπου Blockchain:



Εικόνα 22, Δέντρο απόφασης για επιλογή τύπου Blockchain στην περίπτωση χρήσης "Επικύρωση τίτλων σπουδών στην εκπαίδευση"

Ο τελικός στόχος της παρούσας διπλωματικής είναι να κάνει τον αναγνώστη, με βάση το περιεχόμενο της, να κατανοήσει τις βασικές αρχές του Blockchain και σύμφωνα με το πρόβλημα που εμφανίζεται κάθε φορά να μπορεί να επιλέγει την πιο σωστή λύση από τα μοντέλα αποφάσεων.

Στην περίπτωση χρήσης για επικύρωση της γνησιότητας τίτλων σπουδών στην εκπαίδευση, χρησιμοποιείται το μοντέλο απόφασης που φαίνεται πιο πάνω, βασισμένο στο μοντέλο απόφασης των Karl Wüstl and Arthur Gervais (May 2017) που εμφανίζεται στο κεφάλαιο 4.2, για να

εξετασθεί ποιος τύπος Blockchain θα δώσει τις πιο αποδοτικές λύσεις για το συγκεκριμένο πρόβλημα. Παρακάτω θα αναλυθούν τα βήματα που ακολουθούνται στο συγκεκριμένο διάγραμμα ροής με βάση το τρέχον πρόβλημα. Οι γραμμές με πράσινο χρώμα δείχνουν την διαδρομή που επιλέχθηκε για την λήψη απόφασης στην συγκεκριμένη περίπτωση χρήσης.

1. Υπάρχει **ανάγκη αποθήκευσης δεδομένων** στην συγκεκριμένη εφαρμογή, αφού θα πρέπει να αποθηκεύονται τα στοιχεία και τα πιστοποιητικά των διπλωματούχων από το κάθε εκπαιδευτικό ίδρυμα.

2. Οι **χρήστες της εφαρμογής θα είναι πολλοί**, αφού στο Blockchain θα συμμετέχουν άτομα από πολλά εκπαιδευτικά ιδρύματα, για παράδειγμα οι φοιτητές, οι εργαζόμενοι σε αυτά, αλλά και οι εργοδότες.

3. **Δεν υπάρχει ανάγκη ενός online TTP (third-trusted-party).** Η εξάρτηση τρίτων μερών στην διαδικασία αποθήκευσης ή επικύρωσης των πιστοποιητικών είναι χρονοβόρα διαδικασία. Σκοπός της εφαρμογής είναι να αφαιρεθούν καθυστερήσεις ή λάθη από τους χρήστες και να γίνονται αυτοματοποιημένες διαδικασίες.

4. **Οι χρήστες δεν γνωρίζονται μεταξύ τους**, άρα η βέλτιστη επιλογή για την συγκεκριμένη εφαρμογή, σύμφωνα με το παραπάνω μοντέλο απόφασης είναι ένα Public Permissionless Blockchain , οι οποίοι θα λειτουργούν βασισμένοι στον αλγόριθμο συναίνεσης . Οι χρήστες που θα συμμετέχουν στο Blockchain είναι από πολλά πανεπιστήμια και από πολλούς χώρους εργασίας, άρα είναι αδύνατο να γνωρίζει ο ένας τον άλλον.

Συμπερασματικά και με βάση τα πιο πάνω στάδια του συστήματος αποφάσεων, η κατάλληλη λύση για αποθήκευση, επικύρωση και διατήρηση τίτλων σπουδών στην εκπαίδευση επιτυγχάνεται με εφαρμογή ενός Public Permissionless Blockchain.

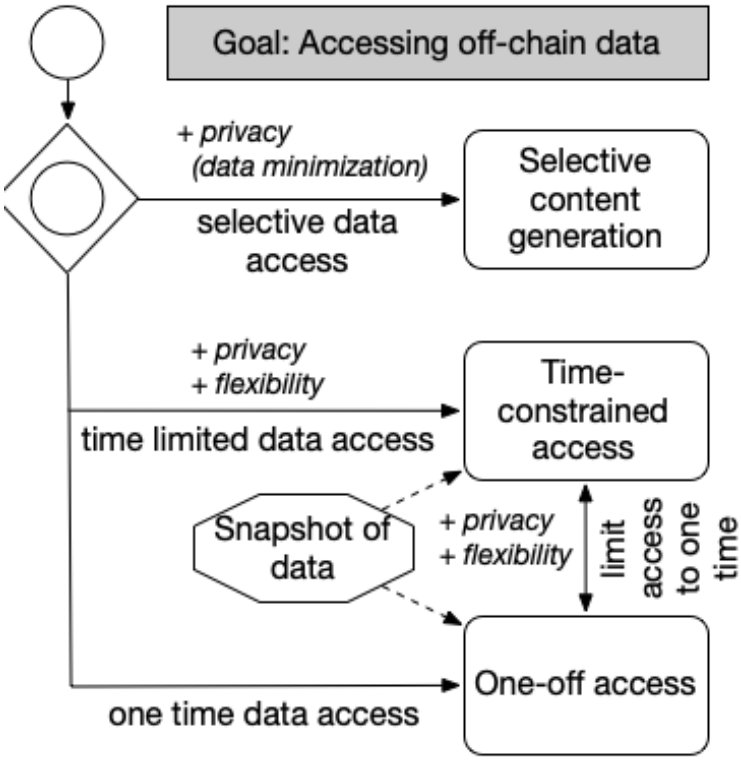
6.6.2 Ανάλυση της εφαρμογής

Στην τρέχουσα κατάσταση, σύμφωνα με την έρευνα JRC SCIENCE OF POLICY REPORT, οι εκπαιδευτικοί οργανισμοί εκδίδουν πιστοποιητικά είτε σε έντυπη μορφή είτε σε ηλεκτρονική. Αυτά τα πιστοποιητικά είναι χρονοβόρα και δαπανηρά ως προς την έκδοση, την συντήρηση του συστήματος και την επαλήθευση. Οι τρέχουσες υποδομές απαιτούν την χρήση μιας αρχής πιστοποίησης, ως ενδιάμεσου μεσολαβητή, για την έκδοση των πιστοποιητικών δημιουργώντας μια εξάρτηση που κάποιες φορές πιθανόν να καταχραστεί. Επίσης, τα τρέχον αρχεία επαλήθευσης ενδέχεται σε κάποιες περιπτώσεις να καταστραφούν ή να χαθούν.

Μια καλή περίπτωση για αποφυγή των παραπάνω προβλημάτων είναι οι εκπαιδευτικοί οργανισμοί που εκδίδουν ψηφιακές πιστοποιήσεις να χρησιμοποιούν ένα δημόσιο Blockchain για την αποθήκευση των ψηφιακών υπογραφών που θα σχετίζονται με τις ψηφιακές πιστοποιήσεις. Οι μοναδικές υπογεγραμμένες ψηφιακές πιστοποιήσεις θα δίνονται κατευθείαν στους χρήστες. Έτσι η επαλήθευση της γνησιότητας ενός πιστοποιητικού θα απαιτεί μόνο την ψηφιακή υπογραφή-hashing που είναι αποθηκευμένη στο Blockchain. Οι αποδείξεις των πιστοποιητικών θα αποθηκευτούν πλήρως, με ασφάλεια και αμετάβλητα στο Blockchain. Σε περίπτωση που ένα εκπαιδευτικό ίδρυμα που εξέδωσε πιστοποιητικά κλείσει, αυτά τα πιστοποιητικά θα εξακολουθούν να επαληθεύονται έναντι των αρχείων που είναι αποθηκευμένα στο blockchain. Με την έκδοση ενός πιστοποιητικού δεν χρειάζεται να ξοδευτούν επιπλέον πόροι για να επιβεβαιωθεί η εγκυρότητα του από τρίτους, αφού θα μπορούν να το επαληθεύουν απευθείας στο καθολικό. Δεν απαιτείται μόνο από τους εκπαιδευτικούς οργανισμούς να χρησιμοποιούν ψηφιακά πιστοποιητικά αλλά και οι οργανισμοί που τους πιστοποιούν θα πρέπει να καταχωρούν τις ψηφιακές υπογραφές τους στο blockchain. Για παράδειγμα, αυτό το δίκτυο θα ελέγχει όχι μόνο ότι ο φοιτητής Χ, έλαβε τίτλο σπουδών από το εκπαιδευτικό ίδρυμα Υ, αλλά και ότι το εκπαιδευτικό ίδρυμα Υ έχει πιστοποιηθεί από τον οργανισμό Ζ. Ένα τέτοιο σύστημα θα μπορούσε να χρησιμοποιηθεί για να διασφαλίσει ότι ο εκπαιδευτικός οργανισμός που εκδίδει την πιστοποίηση έχει τις κατάλληλες πιστοποιήσεις αυθεντίας. Χρησιμοποιώντας ένα blockchain τα ιδρύματα που χρειάζεται να ελέγξουν το ιστορικό του πτυχίου θα μπορούσαν εύκολα να το κάνουν με ένα μόνο κλικ. Μια πλήρως αυτοματοποιημένη διαδικασία θα μπορούσε στη συνέχεια να απεικονίσει την αλυσίδα διαπίστευσης και να επαληθεύσει ότι τα πιστοποιητικά είχαν πράγματι εκδοθεί και ότι εξακολουθούν να ισχύουν

για κάθε βήμα της αλυσίδας. Οι οργανισμοί διαπίστευσης θα μπορούσαν να δημιουργήσουν επαληθευτές, οι οποίοι θα επέτρεπαν σε οποιονδήποτε να ανεβάσει το πιστοποιητικό του και να ελέγξει εάν έχει εκδοθεί πραγματικά από διαπιστευμένο οργανισμό. Επίσης, οι οργανισμοί διαπίστευσης θα μπορούσαν να δημοσιεύσουν οι ίδιοι τα εκδοθέντα πιστοποιητικά σε δημόσιο μητρώο. Αυτό θα επιτρέψει σε κάθε τρίτο μέρος να επαληθεύσει εάν εκδόθηκε πιστοποιητικό από ΑΕΙ σε ένα φοιτητή, εάν το ΑΕΙ διαθέτει πιστοποιητικό στο δημόσιο μητρώο και αν όλα αυτά τα πιστοποιητικά είναι γνήσια. Τα ιδρύματα θα μπορούσαν να δημιουργήσουν αυτοτελείς ταυτότητες για την αποθήκευση των δεδομένων [46].

6.6.3 Επιλογή pattern για πρόσβαση σε δεδομένα εκτός αλυσίδας βάσει της εφαρμογής.



Εικόνα 23, Μοντέλο απόφασης για διαχείριση δεδομένων εκτός αλυσίδας για την περίπτωση χρήσης "Επικύρωση τίτλων σπουδών στην εκπαίδευση" (Πηγή: https://research.csiro.au/blockchainpatterns/decision-models/datamgnmodel/)

Η διαχείριση δεδομένων εκτός αλυσίδας σε ένα Blockchain για την επικύρωση τίτλων σπουδών στην εκπαίδευση είναι μια σημαντική πρόκληση για τους προγραμματιστές της εφαρμογής. Σύμφωνα με το μοντέλο αποφάσεων του κεφαλαίου 5.2, για την βέλτιστη λύση της εφαρμογής θα πρέπει να χρησιμοποιηθούν όλα τα patterns.

Είναι σημαντικό στην εφαρμογή να χρησιμοποιηθεί το Selective content generation pattern για να εμφανίζει μόνο τα δεδομένα που με βάσει κάποιος κανόνες έχουν τεθεί. Για παράδειγμα, στο πιστοποιητικό να εμφανίζονται βαθμολογίες μόνο για συγκεκριμένα μαθήματα και όχι για ολόκληρο το σύνολο μαθημάτων. Αυτό εξυπηρετεί τους διπλωματούχους των εκπαιδευτικών ιδρυμάτων να δείχνουν στον εργοδότη μόνο τις βαθμολογίες των μαθημάτων της κατεύθυνσης του συγκεκριμένου επαγγέλματος. Ακόμη, είναι σημαντικό να χρησιμοποιηθούν και τα Time constrained access και One-off access patterns, για να δίνουν την δυνατότητα στους εκπαιδευόμενους να προωθούν τα πιστοποιητικά τους σε κάποιους οργανισμούς για κάποιο περιορισμένο χρονικό διάστημα ή για ένα πεπερασμένο αριθμό προσβάσεων. Τα τρία αυτά patterns ενισχύουν την ασφάλεια των δεδομένων που εκτίθενται εκτός αλυσίδας.

Τόσο η επιλογή του σωστού τύπου Blockchain αλλά και των προγραμματιστικών διαδικασιών (patterns) που θα εκτελούνται κατά την διάρκεια της εφαρμογής είναι μια σημαντική πρόκληση για τους υπεύθυνους λήψης αποφάσεων. Γι' αυτό το λόγο είναι πολύ σημαντικό να γίνεται σωστή μελέτη των χαρακτηριστικών της κάθε περίπτωσης και σύμφωνα με τα ποικίλα μοντέλα αποφάσεων που καλύπτουν σχεδόν όλες τις ανάγκες να λαμβάνεται η καλύτερη απόφαση.

7 Επίλογος

7.1 Συμπεράσματα

Η επιλογή του σωστού τύπου Blockchain σε μια επιχείρηση είναι μια πολύ σημαντική διαδικασία. Πιο πάνω έχουν αναλυθεί διάφορες δομημένες μεθοδολογίες στη λήψη της κατάλληλης απόφασης για το ποια τεχνολογική λύση είναι η βέλτιστη επιλογή ανάλογα με το σενάριο εφαρμογής. Οι μεθοδολογίες που παρουσιάζονται λαμβάνουν υπόψιν τις απαιτήσεις της κάθε εφαρμογής, τα εμπλεκόμενα μέρη και τα τεχνικά χαρακτηριστικά. Αφού γίνει η κατάλληλη επιλογή του τύπου Blockchain, είναι σημαντικό πριν την εφαρμογή του να αναλυθούν τα μοντέλα αποφάσεων που αφορούν τον τρόπο λειτουργίας του. Δηλαδή, τον τρόπο που τα πρότυπα χρησιμοποιούνται για αξιόπιστη αποθήκευση δεδομένων και έλεγχο πρόσβασης. Τα συγκεκριμένα μοντέλα αποφάσεων μπορούν να βοηθήσουν τους αρμόδιους στην επιλογή των κατάλληλων προτύπων και διαδικασιών που βασίζονται στη συγκεκριμένη τεχνολογία.

7.2 Μελλοντικές επεκτάσεις

Με βάση τη περίπτωση χρήσης στην εκπαίδευση, καταλήγουμε στο συμπέρασμα ότι, ανάλογα με το σενάριο εφαρμογής, υπάρχουν έγκυρες περιπτώσεις χρήσης της τεχνολογίας Blockchain, οι οποίες θα πρέπει να αναλυθούν εκτενώς. Λόγω της τεράστιας φήμης που έχει γνωρίσει το Blockchain και της σημαντικότητας των μοντέλων για την σωστή λήψη αποφάσεων αναμένεται πολλές επιχειρήσεις να αναζητήσουν τέτοια μοντέλα για να καταλήξουν στην πιο σωστή επιλογή. Η αυξανόμενη ζήτηση για εφαρμογή της συγκεκριμένης τεχνολογίας από διάφορους τομείς, θα γεννήσει την ανάγκη ολοένα και περισσότερων μοντέλων αποφάσεων για καλύτερη αξιοπιστία και εφαρμογή του, τα οποία θα παρέχουν τα βέλτιστα αποτελέσματα.

8 Βιβλιογραφία

[1] Π. Κουρουθιανάκη, "Συστήματα Υποστηριξης Αποφασεων," ΤΕΧΝΟΛΟΓΙΚΟ ΕΠΚΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ, 2012.

[2] Ι. ΚΟΛΕΤΣΟΣ and Δ. ΣΤΟΓΙΑΝΝΗΣ, *ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΡΕΥΝΑ*, 3η Έκδοση. Αθήνα, 2017.

[3] S. Morton, "2 Συστήματα Υποστήριξης Αποφάσεων," no. 1971. pp. 39–57, 2015.

[4] S. Belciug and F. Gorunescu, "A Brief History of Intelligent Decision Support Systems," *Intelligent Systems Reference Library*, vol. 157. pp. 57–70, 2020, doi: 10.1007/978-3-030-14354-1_2.

[5] L. Rokach and M. Oded, "DATA MINING AND KNOWLEDGE DISCOVERY HANDBOOK, Chapter 9:DECISION TREES," *Cycle*, vol. 1897, no. Figure 1. Tel Aviv, pp. 44–45, 1989.

[6] D. N. Bhargava, S. Girja, D. R. Bhargava, and M. Mathuria, "Decision Tree Analysis on J48 and CART Algorithm for Data Mining," vol. 3, no. 6. pp. 1114–1119, 2013.

[7] "What is a Decision Tree Diagram," *LUCID SOFTWARE*. https://www.lucidchart.com/pages/decision-tree.

[8] Ψ. ΔΗΜΗΤΡΙΟΣ, "¨ Ο Ρόλος Των Συστημάτων Υποστήριξης Αποφάσεων Στη Σύγχρονη Επιχείρηση (Case Study)," ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ, 2012.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Artif. Life*, 2009, doi: 10.1162/ARTL_a_00247.

[10] E. Polytidou, "Τεχνολογίες Blockchain σε Συστήματα Υποδομής Δημόσιου Κλειδιού και Διαχείρισης Ηλεκτρονικής Ταυτότητας," 2018.

[11] X. Xu *et al.*, "A Taxonomy of Blockchain-Based Systems for Architecture Design," *Annali di radiologia diagnostica*, vol. 43, no. 6. pp. 401–403, 1971.

[12] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," *2018 IEEE 6th Work. Adv. Information, Electron. Electr. Eng. AIEEE 2018 - Proc.*, pp. 32–37, 2018, doi: 10.1109/AIEEE.2018.8592253.

[13] I. Gwyneth, "6 Key Blockchain Features You Need To Know Now," *101 Blockchains*, 2020. https://101blockchains.com/introduction-to-blockchain-features/.

[14] Ameer Rosic, "What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]," *Blockgeeks*, 2020. https://blockgeeks.com/guides/what-is-hashing/.

[15] 101Blockchains, "Newbie's Guide: Private Key Vs Public Key – How They Work?," 2021. https://101blockchains.com/private-key-vs-public-key/.

[16] H. Anwar, "Smart Contracts: The Ultimate Guide For The Beginners," *101 Blockchains*, 2018. https://101blockchains.com/smart-contracts/.

[17] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, "A pattern collection for blockchain-based applications," *ACM International Conference Proceeding Series*. 2018, doi: 10.1145/3282308.3282312.
[18] 101Blockchains, "Blockchain Oracles: Know About The Fundamentals," 2020. https://101blockchains.com/blockchain-oracles/.
[19] Ε. Μπεκρή, "Σύγκριση Τεχνολογιών Κατανεμημένης Εγγραφής," 2020.
[20] E. Ben-Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," *Proceedings - IEEE Symposium on Security and Privacy*. IEEE, pp. 459–474, 2014, doi: 10.1109/SP.2014.36.
[21] T. Kumar Sharma, "PUBLIC VS. PRIVATE BLOCKCHAIN : A COMPREHENSIVE COMPARISON," *Blockchain Council*. https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/.
[22] I. Wladawsky-Berger, "Blockchain Beyond the Hype A Practical Framework for Business Leaders," *World Economic Forum*, no. April. pp. 1–7, 2018, [Online]. Available: https://blogs.wsj.com/cio/2018/12/19/blockchain-beyond-the-hype/.
[23] S. Farshidi, S. Jansen, S. Espana, and J. Verkleij, "Decision Support for Blockchain Platform Selection: Three Industry Case Studies," *IEEE Transactions on Engineering Management*, vol. 67, no. 4. IEEE, pp. 1109–1128, 2020, doi: 10.1109/TEM.2019.2956897.
[24] K. Wust and A. Gervais, "Do you need a blockchain?," *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, no. i. pp. 45–54, 2018, doi: 10.1109/CVCBT.2018.00011.
[25] CompTIA's Blockchain Advisory Council, "WHEN IS BLOCKCHAIN OR ANOTHER DATABASE THE RIGHT CHOICE ?," *CompTIA*. p. 8, 2019, [Online]. Available: https://connect.comptia.org/content/infographic/blockchain-decision-tree.
[26] X. Xu, H. M. N. Dilum Bandara, Q. Lu, I. Weber, L. Bass, and L. Zhu, "A Decision Model for Choosing Patterns in Blockchain-Based Applications," *Proceedings - IEEE 18th International Conference on Software Architecture, ICSA 2021*, no. February. pp. 47–57, 2021, doi: 10.1109/ICSA51549.2021.00013.
[27] I. Weber, Q. Lu, A. B. Tran, A. Deshmukh, M. Gorski, and M. Strazds, "A platform architecture for multi-tenant blockchain-based systems," *Proceedings - 2019 IEEE International Conference on Software Architecture, ICSA 2019*. pp. 101–110, 2019, doi: 10.1109/ICSA.2019.00019.
[28] CSIRO and DATA-61, "Tokenisation," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/data-management-patterns/tokenisation/.

[29] CSIRO and DATA-61, "Token Burning," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/migration-patterns/token-burning/.
[30] CSIRO and DATA-61, "Data Management Decision Model," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/decision-models/datamgnmodel/.
[31] CSIRO and DATA-61, "Establish Genesis," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/migration-patterns/establish-genesis/.
[32] CSIRO and DATA-61, "Performance Decision Model," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/decision-models/performancemodel/.
[33] CSIRO and DATA-61, "Security Decision Model," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/decision-models/securitymodel/.
[34] CSIRO and DATA-61, "Identifier Registry," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/identifier-registry/.
[35] CSIRO and DATA-61, "Delegate List," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/self-sovereign-identity-patterns/update-by-delegates/.
[36] CSIRO and DATA-61, "Oracle Decision Model," *Blockchain Patterns*, 2018. .
[37] CSIRO and DATA-61, "Smart Contract Desicion Model," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/decision-models/contractmodel/.
[38] CSIRO and DATA-61, "Contract Restistry," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/contract-structural-patterns/contract-registry/.
[39] CSIRO and DATA-61, "Factory Contract," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/contract-structural-patterns/factory-contract/.
[40] CSIRO and DATA-61, "Data Contract," *Blockchain Patterns*, 2018. https://research.csiro.au/blockchainpatterns/general-patterns/contract-structural-patterns/data-contract/.
[41] G. Gilles, L. Tarik, and M. Naoufel, "An introduction to the Economics of Fake degrees." pp. 673–693, 2016.
[42] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3. pp. 79–84, 2020, doi: 10.31838/jcr.07.03.13.
[43] Α. Παντοπούλου, "Εξασφάλιση της εγκυρότητας των πτυχίων εξ ' αποστάσεως εκπαίδευσης με χρήση τεχνολογίας Blockchain." 2019.

[44] N. K. Dumpeti and R. Kavuri, "A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain," *Materials Today: Proceedings*. 2021, doi: 10.1016/j.matpr.2021.01.740.
[45] OneSpan, "What is the difference between electronic signature and digital signature?" https://www.onespan.com/products/digital-signature.
[46] A. Grech and A. F.Camilleri, "Blockchain in education," *JRC Science Hub*. p. 136, 2017, doi: 10.31145/1999-513x-2019-6-32-35.