Πανεπιστήμιο Θεσσαλίας

Τμήμα Μηχανικών Χωροταξίας, Πολεοδομίας & Περιφερειακής Ανάπτυξης
ΔΠΜΣ Νέα επιχειρηματικότητα, Καινοτομία & Ανάπτυξη

Η ρηξικέλευθη καινοτομία στον Χρηματοπιστωτικό Τομέα

Η περίπτωση του Blockchain

Χριστοδούλου Θεόφιλος

Επιβλέπων: Δρ. Σταμπουλής Γεώργιος, Επίκουρος Καθηγητής του Πανεπιστημίου Θεσσαλίας

Βόλος 2018

Υπεύθυνη Δήλωση

Βεβαιώνω ότι η παρούσα διπλωματική εργασία εκπονήθηκε από εμένα και αντιπροσωπεύει τις προσωπικές μου απόψεις. Επίσης, έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες.

Βόλος, Ιούνιος 2018

Ευχαριστίες

Μετά την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή Δρ. Γεώργιο Σταμπουλή, Επίκουρο Καθηγητή του Τμήματος Οικονομικών Επιστημών του Πανεπιστημίου Θεσσαλίας, για την καθοδήγηση μου πρόσφερε κατά τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου, τους φίλους μου και την Χρύσα για την ψυχολογική στήριξη που μου παρείχαν καθ' όλη της διάρκεια της εκπόνησης της παρούσας εργασίας.

Περίληψη

Με την πάροδο των χρόνων παρατηρείται ένα διαρκώς αυξανόμενο ενδιαφέρον για την τεχνολογία του blockchain. Αν και η πρώτη εφαρμογή της τεχνολογίας έγινε από τον Satoshi Nakamoto το 2009 με την δημιουργία του Bitcoin, μία σειρά οργανισμών όπως η IBM, η J.P. Morgan και το Ίδρυμα Linux έχουν αρχίσει να ασχολούνται με την συγκεκριμένη τεχνολογία και τα πιθανά οφέλη της μέσα από την εφαρμογή της σε διάφορους κλάδους, διαδικασίες και επιχειρήσεις. Με την χρήση της μεθοδολογίας μελέτης περίπτωσης, γίνεται ανάλυση των τριών διαφορετικών κατηγοριών της τεχνολογίας του blockchain με στόχο την κατανόηση των πλεονεκτημάτων και μειονεκτημάτων σε κάθε μία από αυτές. Παράλληλα αξιολογείται το είδος και η ένταση της καινοτομίας όπως και τα συμπληρωματικά στοιχεία του ενεργητικού που απαιτούνται για την δημιουργία δικτύων blockchain σε κάθε κατηγορία. Με την ανάλυση των μελετών περίπτωσης συμπεραίνεται ότι η τεχνολογία του blockchain είναι μία καινοτομία διαδικασιών με στοιχεία ρηξικέλευθης καινοτομίας σε κάποιες περιπτώσεις.

Λέξεις-κλειδιά: τεχνολογία blockchain, καινοτομία, συμπληρωματικά στοιχεία του ενεργητικού, Bitcoin, Ethereum, Ripple, Project Ubin

Abstract

Over the years, there has been a growing interest in blockchain technology. Although the first application of blockchain technology was made by Satoshi Nakamoto in 200 (Haber S., Stonertta S. W., 1991)9 with the creation of Bitcoin, a number of organizations such as IBM, JP Morgan and the Linux Foundation have shown interest in blockchain technology and its potential benefits through the implementation on various sectors, processes and businesses. By using the case study methodology, the advantages and disadvantages, in each category, are analyzed. Furthermore, the type and the intensity of innovation as well as the additional complementary assets needed to create a blockchain platform are addressed. In conclusion, the analysis has shown that blockchain technlogy is a process innovation with elements of disruptive innovation in many cases.

Keywords: Blockchain technology, innovation, complementary assets, Bitcoin, Ethereum, Ripple, Project Ubin

Περιεχόμενα

Κατάλογος Πινάκων και Σχημάτων

Κατάλογος Γραφημάτων

Αρκτικόλεξο

DAO: Decentralized Autonomous Organization
Dapps: Decentralized applications
DDOs attack: Distributed denial-of-service attack
DR: Depository Receipt
Fintech: Financial technology
MAS: Monetary Authority Of Singapore
MEPS: MAS Electronic Payment System
P2P: Peer to Peer
POW: Proof of Work
RTGS: Real Time Gross Settlement System
ZSL: Zero Security Layer

Κεφάλαιο 1: Εισαγωγή

1.1 Εισαγωγή- Σκοπός της διπλωματικής εργασίας

Η τεχνολογία του blockchain και τα εικονικά νομίσματα έχουν προκαλέσει έντονα το παγκόσμιο ενδιαφέρον. Αν και η τεχνολογία πρωτοεμφανίστηκε το 2009 από το Satoshi Nakamoto, μέσω της δημιουργίας μιας πλατφόρμας συναλλαγών που χρησιμοποιεί το εικονικό νόμισμα Bitcoin, στο ευρύ κοινό άρχισε να γίνεται γνωστή στα τέλη του 2014. Πλέον μία σειρά εταιριών και χρηματοπιστωτικών ιδρυμάτων όπως η IBM, η J.P. Morgan και το Ίδρυμα Linux ασχολούνται με την συγκεκριμένη τεχνολογία και τα πιθανά οφέλη της μέσα από την εφαρμογή της σε διάφορους κλάδους και διαδικασίες. Στην συγκεκριμένη διπλωματική, με την χρήση των μελετών περίπτωσης, αξιολογείται η τεχνολογία του blockchain ως καινοτομία, περιγράφονται τα εμπόδια και τα κίνητρα για την υιοθέτησή της και αναφέρονται τα συμπληρωματικά στοιχεία του ενεργητικού για την δημιουργία και την λειτουργία δικτύων που χρησιμοποιούν την τεχνολογία.

Στο δεύτερο κεφάλαιο αναλύονται βασικές έννοιες που αφορούν την καινοτομία. Παράλληλα γίνεται αναφορά στην τεχνολογία στο χρηματοπιστωτικό τομέα και τις εφαρμογές του blockchain σε αυτόν, ως μία τεχνολογία Fintech.

Στο τρίτο κεφάλαιο αναλύεται η τεχνολογία του blockchain μέσα από τις τρείς μελέτες περιπτώσεις Bitcoin, Ethereum και Ripple και τις αρχιτεκτονικές Hyperldger Fabric, Quorum και Corda. Παράλληλα αναφέρονται τα βασικά δομικά στοιχεία της τεχνολογίας και γίνεται η κατηγοριοποίησή της.

Στο τέταρτο κεφάλαιο αρχικά αναλύεται το πιλοτικό εγχείρημα Ubin, στην συνέχεια αναφέρονται τα πλεονεκτήματα και μειονεκτήματα κάθε περίπτωσης, αξιολογείται η τεχνολογία ως καινοτομία και αναφέρονται τα συμπληρωματικά στοιχεία του ενεργητικού για την δημιουργία την χρήση και την λειτουργία σε κάθε κατηγορία

Τέλος στο πέμπτο κεφάλαιο καταλήγει στα συμπεράσματα και προτάσεις για μελλοντική έρευνα.

Κεφάλαιο 2: Καινοτομία και Fintech

2.1 Εισαγωγή

Σε αυτό το κεφάλαιο αναλύεται η έννοια της καινοτομίας, οι βασικές κατηγορίες καινοτομίας ως προς την δραστηριότητα και την ένταση, οι παράγοντες και τα εμπόδια της καινοτομίας και η ρηξικέλευθη καινοτομία. Στην συνέχεια γίνεται αναφορά στην έννοια του Fintech και στην τεχνολογία του blockchain ως μία τεχνολογία του χρηματοπιστωτικού τομέα.

2.2 Ορισμός της καινοτομίας

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης στο εγχειρίδιο του Όσλο (2005) ορίζει ως καινοτομία την εφαρμογή ενός νέου ή ενός εξαιρετικά βελτιωμένου προϊόντος (αγαθού ή υπηρεσίας), μιας νέας μεθόδου σχετική με το μάρκετινγκ ή μιας νέας οργανωσιακής μεθόδου που σχετίζεται με εσωτερικές πρακτικές της επιχείρησης, τον χώρο εργασίας του οργανισμού ή της εξωτερικές σχέσεις του. Ο συγκεκριμένος ορισμός καλύπτει όλο το φάσμα της καινοτομίας ωστόσο υπάρχει δυνατότητα κατηγοριοποίησης της. Στην πράσινη βίβλος της καινοτομίας (European Comission, 1995), αναφέρει ότι η καινοτομία λειτουργεί ως μία δύναμη που οδηγεί τις επιχειρήσεις σε αισιόδοξους μακροπρόθεσμους στόχους. Παράλληλα οδηγεί στην ανανέωση των βιομηχανικών υποδομών και βρίσκεται πίσω από την εμφάνιση νέων κλάδων οικονομικής δραστηριότητας. Συγκεκριμένα την διαχωρίζει σε τρείς κατηγορίες:

1. Την ανανέωση και την μεγέθυνση του εύρους των προϊόντων, των υπηρεσιών και των συ σχετιζόμενων αγορών.
2. Την δημιουργία νέων μεθόδων παραγωγής, εφοδιασμού και διανομής των προϊόντων και των υπηρεσιών.
3. Την εισαγωγή των αλλαγών στην διοίκηση και την εργασία του οργανισμού όπως και τις εργασιακές συνθήκες και δεξιότητες των εργαζομένων.

2.2.1 Κατηγοριοποίηση της καινοτομίας ως προς την δραστηριότητα

Η καινοτομία όπως αναλύθηκε στον ορισμός της μπορεί να μετασχηματίσει ή να επηρεάσει μία συγκεκριμένη δραστηριότητα σε ένα οργανισμό. Οι βασικές κατηγορίες καινοτομίας σε ότι αφορά τις δραστηριότητες είναι:

1. Καινοτομία προϊόντος: Η καινοτομία προϊόντος αναφέρεται στην εμφάνιση ενός νέου ή εξαιρετικά βελτιωμένου προϊόντος ή υπηρεσίας. Η καινοτομία σε αυτή την περίπτωση μπορεί να συνδέεται με βελτιώσεις στα τεχνικά χαρακτηριστικά, στα υλικά, στο ενσωματωμένο λογισμικό, στην εμπειρία του χρήστη ή σε τεχνικά χαρακτηριστικά. Σε ότι αφορά την τεχνολογία, στην συγκεκριμένη κατηγορία, η καινοτομία μπορεί να συνδέεται με νέες τεχνολογίες ή με συνδυασμό παλαιότερων τεχνολογιών.

2. Καινοτομία διαδικασιών: Η συγκεκριμένη κατηγορία αφορά την εφαρμογή μιας καινούργιας ή εξαιρετικά βελτιωμένης διαδικασίας παραγωγής ή μεθόδου παράδοσης του προϊόντος ή της υπηρεσίας. Η συγκεκριμένη περίπτωση μπορεί να σχετίζεται με αλλαγές σε επίπεδο τεχνικών, εξοπλισμού ή λογισμικού. Μέσα από την καινοτομία στις διαδικασίες μπορεί να επιτευχθεί η μείωση του κόστους στην παραγωγή ή μεταφορά των προϊόντων και των υπηρεσιών, η αύξηση της ποιότητας ή η παράγωγή βελτιωμένων προϊόντων.

3. Καινοτομία στο Μάρκετινγκ: Η καινοτομία σε αυτή την περίπτωση αφορά την εφαρμογή μια νέας μεθόδου Μάρκετινγκ που μπορεί να επιφέρει αλλαγές στην σχεδίαση του προϊόντος, στην συσκευασία, στην τοποθέτηση του προϊόντος και στην τιμή του.

4. Οργανωτική καινοτομία: Η οργανωτική καινοτομία αναφέρεται στην εφαρμογή νέων οργανωτικών μεθόδων μέσα την επιχείρηση και που μετατρέπουν τον εργασιακό χώρο της ή της σχέσεις με το εξωτερικό περιβάλλον. Συγκεκριμένα αναφέρεται, σε αλλαγές των εργασιακών ρουτινών και διαδικασιών εντός της επιχείρησης ή στην εφοδιαστική αλυσίδα.

2.2.2 Η κατηγοριοποίηση βάσει του επιπέδου της καινοτομίας

Η καινοτομία μπορεί να διαχωριστεί όχι μόνο βάσει των δραστηριοτήτων αλλά και βάσει της έντασης της καινοτομίας σε κάθε περίπτωση. Ο Christensen 1997 διαχωρίζει την καινοτομία σε δύο βασικές κατηγορίες. Η πρώτη αναφέρεται στην συντηρητική ή επαυξημένη καινοτομία και αφορά βελτιώσεις στα υπάρχοντα προϊόντα ή διαδικασίες. Ο Assnik (1998) αναφέρεται στην συντηρητική καινοτομία ως την βελτίωση των προϊόντων (ή των υπηρεσιών) και των διαδικασιών εντός των «ορίων» της υπάρχουσας αγοράς και τεχνολογίας. Η συντηρητική ή επαυξημένη καινοτομία εμπεριέχει χαμηλό ρίσκο από την υιοθέτηση τους από τις επιχειρήσεις και αντίστοιχα

χαμηλό αντίκτυπο στην επίδοσή τους. Ο Souto (2015) αναφέρει ότι η επαυξημένη καινοτομία δεν αλλάζει τις διαδικασίες, προϊόντα, τεχνολογίες ή οργανωσιακές μεθόδους αλλά τις βελτιώνει.

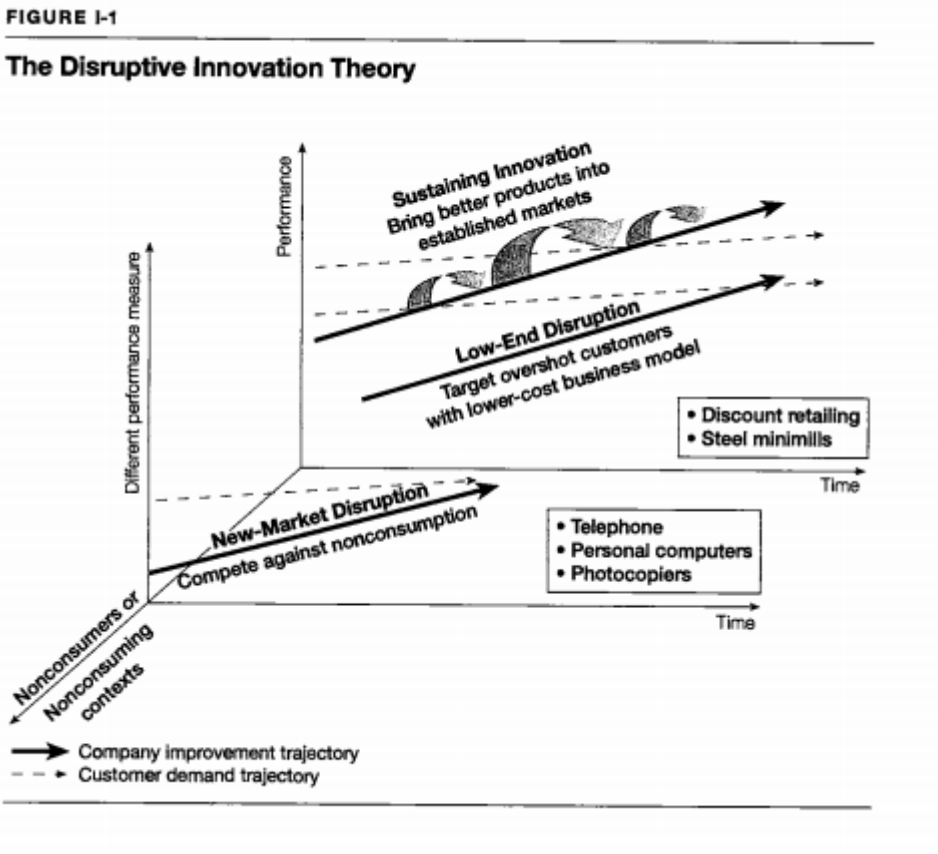
Η δεύτερη κατηγορία είναι αυτή της ρηξικέλευθης καινοτομίας. Ο Teece (2010) αναφέρεται στην ρηξικέλευθη καινοτομία ως την καινοτομία που έρχεται σε αντίθεση με τα υπάρχοντα προϊόντα και διαδικασίες, και είναι αποτέλεσμα διαφορετικών ιδεών σε σχέση με τα υπάρχοντα επιχειρηματικά μοντέλα. Ο Christensen (1997) θεωρεί ότι οι ρηξικέλευθες καινοτομίες εισάγουν μία νέα πρόταση αξίας σύμφωνα. Η νέα πρόταση αξίας μπορεί να οδηγήσει παράλληλα σε καινοτομία σε επίπεδο επιχειρηματικών μοντέλων δηλαδή στην δημιουργία νέων ή τον επαναπροσδιορισμό των υπαρχόντων επιχειρηματικών μοντέλων. Ο Teece (2010) επισημαίνει ότι μία ρηξικέλευθη καινοτομία θα πρέπει να συνδυαστεί με την καινοτομία σε επίπεδο επιχειρησιακού μοντέλου για να μπορέσει αποκτήσει αξία. Ο Christensen ωστόσο διαχωρίζει την ρηξικέλευθη καινοτομία σε δύο περιπτώσεις, την χαμηλού επιπέδου ρηξικέλευθη καινοτομία και την ρηξικέλευθη καινοτομία νέας αγοράς.

Η περίπτωση του χαμηλού επιπέδου ρηξικέλευθης καινοτομίας συμβαίνει σε περιπτώσεις όπου τα υπάρχοντα προϊόντα ή υπηρεσίες είναι «πολύ καλά» και επομένως είναι υπερτιμημένα σε σχέση με την αξία που μπορούν να αντλήσουν οι καταναλωτές τους. Σε αυτές τις περιπτώσεις οι επιχειρήσεις που υιοθετούν αυτού τους είδους καινοτομίες προσφέρουν στους καταναλωτές ένα προϊόν χαμηλού κόστους και σχετικά απλό (Christensen 1997).

Η περίπτωση ρηξικέλευθης καινοτομίας νέας αγοράς μπορεί να προκύψει όταν τα χαρακτηριστικά των υπαρχόντων προϊόντων περιορίζουν τον αριθμό των πιθανών καταναλωτών ή όταν η κατανάλωση των συγκεκριμένων προϊόντων γίνεται αναγκαστικά κάτω από συνθήκες που δεν διευκολύνουν το χρήστη (Christensen 1997). Η ρηξικέλευθη καινοτομία νέας αγοράς δημιουργεί συνθήκες για την κατανάλωση των προϊόντων ή των υπηρεσιών από «μη καταναλωτές» και σε περιβάλλοντα που η κατανάλωση των προϊόντων ήταν αδύνατη.

Και οι δύο περιπτώσεις (συντηρητικής και ρηξικέλευθης) καινοτομίας, υποκινούνται από δύο βασικές δυνάμεις ή όπως τις αναφέρει ο Christensen «τροχιές». Η πρώτη σχετίζεται με την βελτίωση της εταιρίας και αναφέρεται στην βελτίωση των προϊόντων και των υπηρεσιών με την πάροδο του χρόνου ενώ η δεύτερη σχετίζεται με

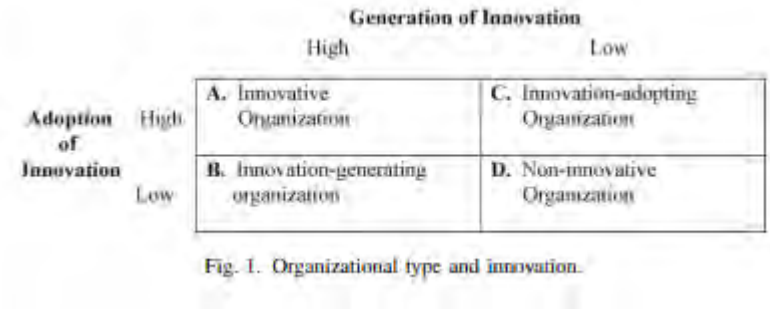
την ζήτηση των καταναλωτών και αναφέρεται στην αξία που λαμβάνουν από την καινοτομία.



Σχήμα 2.1: Η ένταση της καινοτομίας (Christensen, 1997)

2.2.3 Η διαδικασία τα οφέλη και τα εμπόδια της καινοτομίας

Οι Damanpour και Wischnevsky (2006) διαχωρίζουν τις επιχειρήσεις σε 4 κατηγορίες βάσει της καινοτομίας όπως φαίνεται στο σχήμα.



		Generation of Innovation: High	Generation of Innovation: Low
Adoption of Innovation	High	A. Innovative Organization	C. Innovation-adopting Organization
	Low	B. Innovation-generating organization	D. Non-innovative Organization

Fig. 1. Organizational type and innovation.

Πίνακας 2.2: Κατηγοριοποιηση των καινοτόμων επιχειρήσεων (Damanpour και Wischnevsky, 2006)

Οι οργανισμοί που δημιουργούν καινοτομία ακολουθούν μία σειρά διαδικασιών. Συγκεκριμένα, πρώτα απαιτείται η αναγνώριση της ευκαιρίας, η έρευνα, ο σχεδιασμός και τέλος οι διαδικασίες σχετικές με το μάρκετινγκ και την διανομή. Οι παραπάνω ενέργειες ουσιαστικά περιγράφουν όλη την διαδικασία από την σύλληψη της ιδέας μέχρι την υλοποίηση τους (Damanpour και Wischnevsky 2006).

Οι οργανισμοί που υιοθετούν καινοτομίες ακολουθούν δύο διαδικασίες. Η πρώτη αφορά την αναγνώριση μίας συγκεκριμένης ανάγκης, την ενημέρωση για μία συγκεκριμένη καινοτομία την αξιολόγηση για την καταλληλόλητα της και τέλος την υιοθέτησή της. Η δεύτερη κατηγορία αναφέρεται στις διαδικασίες που σχετίζονται με την τροποποίηση της καινοτομίας και του οργανισμού που την υιοθετεί, την αρχική της χρήση και την συνέχεια της χρήσης της μέχρι αυτή να γίνει οργανωσιακή ρουτίνα (Damanpour και Wischnevsky 2006).

Οι καινοτόμες επιχειρήσεις είναι αυτές που καταφέρνουν να επιβιώσουν και να αναπτυχθούν μακροπρόθεσμα (Tidd 2001). Παράλληλα, η καινοτομία θεωρείται σύμφωνα με τον Schumpeter (1934) κριτήριο για την οικονομική μεγέθυνση και πηγή για την απόκτηση ανταγωνιστικού πλεονεκτήματος έναντι των ανταγωνιστών τους. Μέσα από την καινοτομία μπορεί να επιτευχθεί βελτίωση των προϊόντων (ή των υπηρεσιών) ή μείωση του κόστους της παραγωγής των προϊόντων και των διαδικασιών που σχετίζονται με αυτό (ΟΟΣΑ, 2015).

Στο εγχειρίδιο του Όσλο ο ΟΟΣΑ (2015) διαχωρίζει τους παράγοντες που εμποδίζουν τις επιχειρήσεις να καινοτομούν σε 4 κατηγορίες:

1. Παράγοντες σχετικοί με το κόστος: Σε αυτή την κατηγορία περιλαμβάνονται το υψηλό ρίσκο της επιχείρησης, το υψηλό κόστος σχετικά με την έρευνα και ανάπτυξη της καινοτομίας και την έλλειψη των απαραίτητων κεφαλαίων για την χρηματοδότησή της.
2. Παράγοντες σχετικοί με την γνώση που κατέχει η επιχείρηση: Σε αυτή την κατηγορία περιλαμβάνονται εμπόδια όπως η πιθανή αδυναμία της επιχείρησης να καινοτομήσει λόγω έλλειψης εξειδικευμένου είτε εντός της επιχείρησης, είτε στην αγορά εργασίας, η έλλειψη ενημέρωσης για μία νέα τεχνολογία, αδυναμίες σε ότι αφορά την εύρεση των κατάλληλων συνεργατών για την χρήση της καινοτομίας με στόχο την εξέλιξη των προϊόντων και διαδικασιών, η οργανωσιακη «ακαμψία» λόγω

της δομής της επιχείρησης και η αρνητική στάση των εργαζομένων ή των διευθυντικών στελεχών στην αλλαγή.

3. Παράγοντες σχετικοί με την αγορά: Αυτή την κατηγορία, αναφέρεται περιπτώσεις που σχετίζονται με την ζήτηση της αγοράς για καινοτόμα προϊόντα ή υπηρεσίες.

4. Θεσμικοί παράγοντες: Εμπόδια όπως η αδυναμία κατοχύρωσης των δικαιωμάτων ιδιοκτησίας, η υψηλή φορολογία, νομοθετικοί φραγμοί και κανονισμοί που αποτρέπουν την επιχείρηση από το να καινοτομεί περιλαμβάνονται σε αυτή την κατηγορία.

Ο Assnik (2010) αναφέρει συγκεκριμένα ότι τα εμπόδια που αντιμετωπίζουν οι μεγάλες εταιρίες για την ανάπτυξη και τη εμπορευματοποίηση της ρηξικέλευθης καινοτομίας σχετίζονται με την οργανωσιακή ακαμψία σε ότι αφορά την δομή της, με εξωτερικούς παράγοντες όπως η ζήτηση της αγοράς, την έλλειψη των απαραίτητων ικανοτήτων (όπως δεξιότητες και γνώσεις) και την αδυναμία να «ξεμάθουν» παλιότερες γνώσεις και διαδικασίες είτε επιχειρησιακό είτε σε ατομικό επίπεδο. Σε επίπεδο δεξιοτήτων και γνώσεων περιλαμβάνονται και η δημιουργικότητα των οργανισμών ή των ατομών αλλά και η αξιολόγηση του ρίσκου (κυρίως από τα διευθυντικά στελέχη) από την υιοθέτηση μίας καινοτομίας.

2.2.4 Συμπληρωματικά στοιχεία του ενεργητικού μίας καινοτομίας και το κυριάρχο μοντέλο σχεδίασης

Ο Teece (1986) αναφέρει ότι μία καινοτομία για να μπορέσει επιτυχημένα να εμπορευματοποιηθεί απαιτείται μία σειρά άλλων ικανοτήτων και περιουσιακών στοιχείων. Για παράδειγμα σε κάθε περίπτωση εμπορευματοποίησης της καινοτομίας απαιτούνται υπηρεσίες μια επιτυχημένη καμπάνια μάρκετινγκ, η ανταγωνιστική κατασκευή και οι υπηρεσίες υποστήριξης μετά την πώληση των προϊόντων και των υπηρεσιών. Ωστόσο, διαχωρίζει τα συμπληρωματικά στοιχεία του ενεργητικού σε τρεις κατηγορίες, βάσει της αλληλεξάρτησης που υπάρχει με την καινοτομία. Η πρώτη κατηγορία αναφέρεται σε γενικά συμπληρωματικά στοιχεία του ενεργητικού που δεν χρειάζεται να προσαρμοστούν για την καινοτομία. Η δεύτερη κατηγορία αφορά τα εξειδικευμένα συμπληρωματικά στοιχεία του ενεργητικού που υπάρχει μονόδρομη εξάρτηση με την καινοτομία. Η τρίτη κατηγορία αναφέρεται στα περιουσιακά στοιχεία που υπάρχει αμφίδρομη εξάρτηση με την καινοτομία και αναφέρονται ως αμοιβαία εξειδικευμένα (cospecialized).

Σύμφωνα με τον Teece (1996) οι Abernathy και Utterback (1978) αναφέρουν ότι υπάρχουν δύο στάδια που διαχωρίζουν την τεχνολογική εξέλιξη ενός κλάδου σε δύο στάδια. Το πρώτο που χαρακτηρίζεται ως προπαραδειγματικό στάδιο αφορά τα πρώτα στάδιο της εξέλιξης του κλάδου όπου η σχεδίαση του προϊόντος διαφέρει σε κάθε επιχείρηση και οι παραγωγικές διαδικασίες οργανώνονται «πρόχειρα». Ο ανταγωνισμός των επιχειρήσεων σε αυτό το στάδιο έγκειται σε επίπεδο σχεδιασμού προϊόντων και διαδικασιών. Με την εμφάνιση ενός κυρίαρχου μοντέλου προϊόντος και παραγωγής, ο ανταγωνισμός μεταφέρεται σε επίπεδο τιμών. Σε αυτή την περίπτωση οι επιχειρήσεις προσπαθούν να εκμεταλλευτούν τις οικονομίες κλίμακας και μάθησης. Ωστόσο η ύπαρξης ενός κυρίαρχου σχεδιασμού δεν σημαίνει απαραίτητα την παύση της καινοτομίας.

2.3 Η τεχνολογία στον χρηματοπιστωτικό τομέα (Fintech)

Ο όρος Fintech (που είναι συντομογραφία του όρου Financial Technology) αναφέρεται στις τεχνολογίες που χρησιμοποιούνται στον χρηματοπιστωτικό τομέα. Ως όρος διατυπώθηκε για πρώτη φορά στο Συνέδριο Χρηματοπιστωτικών Υπηρεσιών Τεχνολογίας από την Citigroup στις αρχές της δεκαετίας του 1990. Στόχος της ήταν να ξεπεραστεί η αρνητική στάση των χρηματοπιστωτικών ιδρυμάτων για συνεργασία με τεχνολογικές εταιρίες που δεν ανήκαν στον κλάδο (Hochstein, 2015). Ο όρος καλύπτει πλέον ένα ευρύ φάσμα τεχνολογιών και υπηρεσιών που παρέχονται από νέες επιχειρήσεις και οργανισμούς, παγκόσμιους, τεχνολογικούς «κολοσσούς» αλλά και τα παραδοσιακά χρηματοπιστωτικά ιδρύματα.

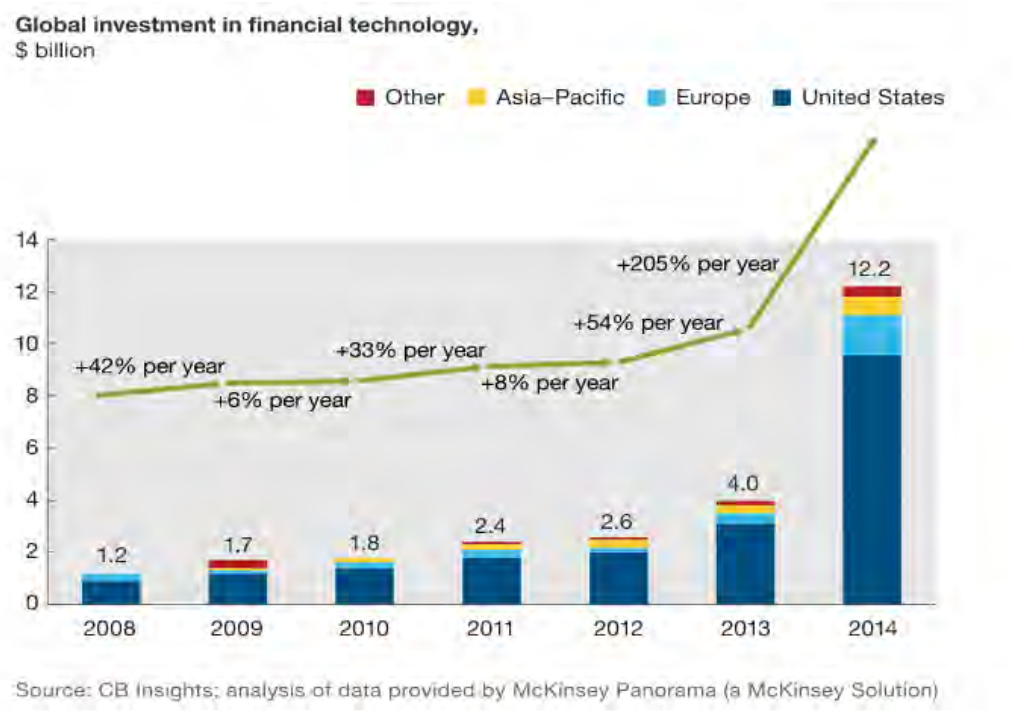
Ο Arner (2016) διαχωρίζει την τεχνολογία στο χρηματοπιστωτικό τομέα σε τρεις περιόδους. Η πρώτη αναφέρεται στην χρονική περίοδο από τα μέσα του 19ο αιώνα έως τα τέλη της δεκαετίας του ’70 και χαρακτηρίζεται ως Fintech 1.0. Σε αυτή την περίοδο οι σημαντικότερες τεχνολογίες που αναφέρονται είναι η εμφάνιση των πιστωτικών καρτών το 1950, του φαξ από την εταιρία Xerox ενώ το 1967 εγκαθίσταται το πρώτο ATM από την Barclays του Ηνωμένου Βασιλείου που σηματοδοτεί στο πέρασμα στην δεύτερη χρονική περίοδο που αναφέρεται ως Fintech 2.0.

Η δεύτερη περίοδος που διήρκησε έως το 2008 χαρακτηρίζεται κυρίως από την μετατροπή των χρηματοπιστωτικών υπηρεσιών σε ψηφιακές. Η εισχώρηση του Διαδικτύου για την παροχή υπηρεσιών από τα χρηματοπιστωτικά ιδρύματα είναι έντονη αυτή τη χρονική περίοδο. Συγκεκριμένα μέχρι το 2001, οκτώ τράπεζες στις

Ηνωμένες Πολιτείες κατείχαν πάνω από 1 εκατομμύριο πελάτες που εξυπηρετούνταν μέσω Διαδικτύου ενώ το 2005, στο Ηνωμένο Βασίλειο, εμφανίστηκαν οι πρώτες τράπεζες χωρίς φυσικά καταστήματα. Η ψηφιοποίηση, στις αρχές του 21ου αιώνα, των εσωτερικών διαδικασιών των τραπεζών αλλά και των αλληλεπιδράσεων τους με εξωτερικούς παράγοντες, άλλαξε ολοκληρωτικά τον τρόπο της διάθεσης των υπηρεσιών, επηρεάζοντας θετικά τους καταναλωτές, ενώ παράλληλα αύξησε τον ανταγωνισμό μεταξύ των χρηματοπιστωτικών ιδρυμάτων. Ωστόσο, η ψηφιοποίηση των υπηρεσιών επέτρεπε την είσοδο νέων εταιριών, οι οποίες δεν ανήκαν στο χρηματοπιστωτικό τομέα, γεγονός που αποτελεί βασικό στοιχείο για την είσοδο στην 3η περίοδο του Fintech. Η παγκόσμια χρηματοπιστωτική κρίση του 2008 επηρέασε την εικόνα των παραδοσιακών πάροχων χρηματοπιστωτικών υπηρεσιών προς τους πελάτες τους. Η εμπιστοσύνη από την πλευρά των πελατών τους χάθηκε (Menat, 2016), φαινόμενο που αποτυπώνεται σε έρευνα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες (Medici Insights, 2015). Συγκεκριμένα, η έρευνα έδειξε ότι η εμπιστοσύνη των Αμερικανών προς τη CitiBank ανέρχεται στο 37%, σε αντίθεση με τις δύο μεγάλες τεχνολογικές εταιρίες, Amazon και Google, τις οποίες εμπιστεύονται κατά 71% και 64% αντίστοιχα. Αξίζει να σημειωθεί, ότι οι νεοεισερχόμενοι στη προσφορά των χρηματοπιστωτικών υπηρεσιών δεν είναι μόνο εδραιωμένες εταιρίες, αλλά και νέες start up επιχειρήσεις.

Στην είσοδο των νέων εταιριών, βοήθησε και η έλλειψη ρυθμιστικού πλαισίου που θα τις απέτρεπε από την συμμετοχή τους στη προσφορά των υπηρεσιών. Σε αρκετές χώρες, κυρίως της Ασίας και της Αφρικής (χαρακτηριστικά παραδείγματα είναι η Κίνα, η Ινδία και η Νιγηρία), τα κίνητρα για την ανάπτυξη του Fintech ήταν αυξημένα. Η έλλειψη τραπεζικών υποδομών ή η περιορισμένη πρόσβαση σε αυτές λειτούργησε καταλυτικά για την είσοδο νέων εταιριών, που έδιναν λύση στη αδυναμία επίτευξης συναλλαγών. Σύμφωνα με τα στοιχεία της ιστοσελίδας WorldBank, το ποσοστό των κατοίκων της Κίνας, που δεν έχει πρόσβαση σε τραπεζικούς λογαριασμούς για το έτος 2015, ανέρχεται σε 36% ενώ για τους κατοίκους του Ηνωμένων Πολιτειών και του Ηνωμένου Βασιλείου, σε 2.7% και 2.5% αντίστοιχα.

Στην τρίτη περίοδο του Fintech (Fintech 3.0), έχουμε μία έξαρση σε ότι αφορά τις επενδύσεις σε Fintech τεχνολογίες. Συγκεκριμένα συμφωνα με τους Dietz και άλλους (2016) μόνο για το 2014 επενδύθηκαν περίπου 12.2 δισεκατομμύρια δολάρια από κεφάλαια επιχειρηματικών συμμετοχών (venture capitals).



Σχήμα 2.3: Επενδύσεις σε τεχνολογίες του χρηματοπιστωτικού τομέα (Dietz και άλλοι 2016)

Ιδιαίτερη έμφαση δίνεται στο τομέα των πληρωμών. Αν και η παροχή υπηρεσιών διαδικτυακών πληρωμών υπάρχει από το 1998, όταν δηλαδή ιδρύθηκε η εταιρεία Paypal, Δέκα χρόνια μετά, αρκετές εταιρίες, μεταξύ των οποίων είναι και τεχνολογικοί κολοσσοί, όπως η Google, η Samsung, το Facebook και η Apple, εισέρχονται στην παροχή υπηρεσιών πληρωμής και συναλλαγών δημιουργώντας δικές τους εφαρμογές όπως το Facebook Pay, το Apple Pay, το Samsung Pay και το Google Wallet (Liu, 2015), δίνοντας έτσι τη δυνατότητα επίτευξης συναλλαγών μέσω των κινητών συσκευών. Χαρακτηριστική είναι και η συμβολή της M-Pesa και Alipay, κυρίως σε αγορές αναπτυσσόμενων χωρών. Σημαντικό ρόλο, για την ανάπτυξη των πληρωμών μέσω κινητών συσκευών, έπαιξε η ευρεία χρήση αυτών, καθώς σύμφωνα με την Παγκόσμια Ένωση Τηλεπικοινωνίας, το 97% των ανθρώπων το 2015 κατείχε κινητό τηλέφωνο. Αξιοσημείωτο είναι ότι, σε 16 αγορές της Αφρικής, οι λογαριασμοί μέσω κινητών συσκευών είναι περισσότεροι από τους τραπεζικούς λογαριασμούς (Menat, 2016).

Παράλληλα καθώς το ποσοστό το ποσοστό του πληθυσμού που έχει πρόσβαση σε προϊόντα δανεισμού είναι 20% (Menat, 2016) και η χρηματοπιστωτική κρίση έχει επηρεάσει αρνητικά την προσφορά των δανείων (Gonzalez 2016), λόγω κεφαλαιακών ρυθμιστικών περιορισμών που επιβάλλονται στα χρηματοπιστωτικά ιδρύματα, άρχισαν

να εμφανίζονται μία σειρά . Ο διαδικτυακός δανεισμός peer-to-peer (p2p) είναι μία εναλλακτική υπηρεσία δανεισμού, που φέρνει σε επαφή τους δανειζόμενους και τους δανειστές μέσω ψηφιακών πλατφορμών. Η συγκεκριμένη υπηρεσία δίνει την δυνατότητα πρόσβασης σε δάνεια με καλύτερες συνθήκες, σε σχέση με τα παραδοσιακά χρηματοπιστωτικά ιδρύματα, ενώ, από την πλευρά του δανειστή, λειτουργεί ως μια μορφή επένδυσης ενώ οι εταιρίες που παρέχουν τις πλατφόρμες έχουν οικονομικό όφελος από τις επιτυχημένες συναλλαγές. Οι πρώτες ψηφιακές πλατφόρμες p2p δανεισμού εμφανίστηκαν ήταν η Zopa και η Prosper, το 2006 στο Ηνωμένο Βασίλειο και το 2007 στις Ηνωμένες Πολιτείες αντίστοιχα (Hulme και Wright, 2006). Η διαδικασία που επιτυγχάνονται οι συναλλαγές είναι μια μορφή δημοπρασίας, όπου οι δανειστές θέτουν ένα αρχικό επιτόκιο και οι δανειζόμενοι κάνουν προσφορές.

2.3.1 Η τεχνολογία του blockchain ως Fintech

Στις τεχνολογίες της κατηγορίας Fintech 3.0 εντάσσεται και η τεχνολογία του blockchain. Οπως θα αναλυθεί στο επόμενο κεφάλαιο ο Nakamoto (2009) δημιούργησε μία πλατφόρμα που επιτρέπει την επίτευξη συναλλαγών, αντικαθιστώντας την εμπιστοσύνη μεταξύ των συναλλασσόμενων με κρυπτογραφία δημιουργώντας μία πλατφόρμα συναλλαγών και ένα εικονικό νόμισμα το Bitcoin για την επίτευξη των συναλλαγών εντός της πλατφόρμας. Το έντονο ενδιαφέρον της αγοράς για το Bitcoin, πυροδότησε μια σειρά νέων εγχειρημάτων που χρησιμοποιούν το blockchain για την δημιουργία πλατφορμών που επιτρέπουν τις p2p συναλλαγές. Σύμφωνα με στοιχεία του CoinMarketCap, το 2018 η συνολική κεφαλαιοποίηση 1587 κρυπτονομισμάτων ανέρχεται στα 256 δισεκατομμύρια. Παράλληλα, τα έξυπνα συμβόλαια, χαρακτηριστικό ορισμένων πλατφορμών όπως της πλταφόρμας Ethereum που αναλύεται στο επόμενο κεφάλαιο, επιτρέπουν την δημιουργία νέων μορφών συμβολαίων εντός των πλατφορμών. Το συγκεκριμένο χαρακτηριστικό δίνει την δυνατότητα συναλλαγών περιουσιακών στοιχείων μέσα από την αποτύπωση του ιδιοκτησιακού καθεστώτος στα έξυπνα συμβόλαια.

Η Swan (2014) διαχωρίζει την τεχνολογία του blockchain σε τρείς βασικές κατηγορίες:

- Blockchain 1.0: p2p συναλλαγές εικονικών νομισμάτων (Swan 2014: 1-8).

- Blockchain 2.0: συναλλαγές περιουσιακών στοιχείων, συμβόλαια μεσεγγύησης, συμβόλαια πολλαπλών υπογραφών και υπηρεσιών χρηματοπιστωτικών ιδρυμάτων (όπως μετοχές, ιδιωτικά επενδυτικά κεφάλαια, ομόλογα, δάνεια, crowdfunding, αμοιβαία κεφάλαια κ.α). (Swan, 2014: 9-27)
- Blockchain 3.0: εφαρμογές της τεχνολογίας πέρα από αυτές των χρηματοοικονομικών και των επιχειρήσεων, σε κλάδους όπως αυτός της υγείας και σε διαδικασίες σχετικές με την διακυβέρνηση (διαδικασίες ψηφοφοριών) (Swan, 2014: 27-64).

Σε ότι αφορά την εφαρμογή των υπαρχόντων χρηματοπιστωτικών ιδρυμάτων, η Ένωση Ευρωπαϊκών Τραπεζών (2015) θεωρεί ότι οι εφαρμογές της τεχνολογίας στον χρηματοπιστωτικό τομέα είναι δυνατό να αυξήσουν την ταχύτητα των διαδικασιών μειώνοντας την πολυπλοκότητά και το κόστος τους. Παράλληλα αναφέρει ότι είναι δυνατή η ενσωμάτωσή της στο υπάρχον πληροφοριακό σύστημα και περιουσιακά στοιχεία (όπως μετοχές, νομίσματα, ομόλογα κλπ). Οι αναφορές της επικεντρώνονται στις διαδικασίες συναλλαγών συναλλαγμάτων και εμβασμάτων, στην ανταλλαγή εγγράφων και σε υπηρεσίες σχετικές με συναλλαγές περιουσιακών στοιχείων θεωρώντας ότι με την χρήση της τεχνολογίας η διεκπεραίωση των συναλλαγών μπορεί να γίνει σε πραγματικό χρόνο. Μία πιθανή εφαρμογή της τεχνολογίας πρόκειται να αναδιαμορφώσει τις διαδικασίες των χρηματοπιστωτικών ιδρυμάτων, αυτοματοποιώντας ορισμένες από αυτές. Παράλληλα κρίνεται απαραίτητη η συμμετοχή ενός ελάχιστου αριθμού συμμετεχόντων για την επίτευξη της δια λειτουργικότητας του συστήματος. Επιπλέον, η ύπαρξη ενός ρυθμιστικού πλαισίου που θα δίνει σαφείς κατευθύνσεις προς τους συμμετέχοντες ενώ παράλληλα δεν θα περιορίζει την υιοθέτηση της καινοτομίας είναι καταλυτικός παράγοντας για την δημιουργία εφαρμογών σε μία σε μία blockchain πλατφόρμα.

Ο Peters και Panayi (2016) κάνουν ξεχωριστή αναφορά πιθανές εφαρμογές της τεχνολογίας σε εμπορικές τράπεζες μειώνοντας την πολυπλοκότητα των διαδικασιών σε ότι αφορά τα τραπεζικά δάνεια, την έκδοση ομολόγων και την έκδοση μετοχών. Οι Mills και άλλοι (2016) αναφέρουν ότι η εφαρμογή της τεχνολογία του blockchain στα χρηματοπιστωτικά ιδρύματα μπορεί μειώσει την πολυπλοκότητα των διαδικασιών (κυρίως σε πολυμερής διασυνοριακές συναλλαγές), μείωση της ταχύτητας των διαδικασιών για την μεταφορά κεφαλαίων και περιουσιακών στοιχείων, αύξηση της διαφάνειας και αμεταβλητότητας των διεκπεραιωμένων συναλλαγών, αύξηση της

ανθεκτικότητας του δικτύου μέσα από μία διαχείριση ενός κατανεμημένου δικτύου δεδομένων και μείωση του ρίσκου σε επίπεδο διαδικασιών και χρηματοπιστωτικού ρίσκου. Τέλος κάνουν αναφορά σε πιθανά προβλήματα που μπορεί να αντιμετωπίσουν τα χρηματοπιστωτικά ιδρύματα από την υιοθέτηση της τεχνολογίας, δεδομένου του πρώιμου σταδίου στο οποίο βρίσκεται, σχετικά με δυσκολίες στην εφαρμογή και την σύνδεση με τα υπάρχοντα πληροφοριακά συστήματα αλλά και νέα ζητήματα όπως την ανάγκη για νέα ρυθμιστικά πλαίσια και εποπτεία παρά την αυτοματοποίηση των διαδικασιών και την διαχείριση του ρίσκου λόγω των νέων προκλήσεων που δημιουργούνται από την εφαρμογή της τεχνολογίας.

2.4 Συμπεράσματα

Σε αυτό το κεφάλαιο κατηγοριοποιήθηκε η καινοτομία σε 4 βασικές κατηγορίες (σε επίπεδο διαδικασιών, σε επίπεδο προϊόντος, σε οργανωτικό επίπεδο και στο μάρκετινγκ). Ένα από τα βασικότερα κίνητρα για την καινοτομία των επιχειρήσεων είναι απαραίτητη για την επιβίωσή και την μεγέθυνση τους μακροπρόθεσμα. Παράλληλα, η οργανωσιακή δυσκαμψία, το κόστος και η έλλειψη εξειδικευμένου προσωπικού μπορεί να αποτελέσουν εμπόδια για την καινοτομία. Ωστόσο οι επιχειρήσεις δεν είναι απαραίτητο να καινοτομούν εσωτερικά. Εξίσου σημαντική είναι η διαδικασία υιοθέτησης καινοτομιών, κάτι που ωστόσο απαιτεί την αναγνώριση των νέων αναγκών της αγοράς και των πλεονεκτημάτων από την υιοθέτηση της. Τέλος, αναλύεται η έννοια του Fintech σε τρεις κατηγορίες και παρουσιάζεται η τεχνολογία του blockchain ως μια τεχνολογία που ανήκει σε αυτή την κατηγορία, καθώς δημιουργεί νέες πλατφόρμες p2p συναλλαγών αντικαθιστώντας την εμπιστοσύνη μεταξύ των συναλλασσόμενων με τεχνικές κρυπτογραφίας ενώ παράλληλα αναφέρονται πιθανές εφαρμογές της στον χρηματοπιστωτικό τομέα για την μείωση του κόστους και της πολυπλοκότητας στην διεκπεραίωση των συναλλαγών, την αύξηση της ταχύτητας στην επίτευξή τους και τα πιθανά ζητήματα που δημιουργούνται από την υιοθέτηση της.

Κεφάλαιο 3: Η τεχνολογία του Blockchain

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο δίνεται ο ορισμός του blockchain και τα βασικά δομικά στοιχεία της τεχνολογίας μέσα από τις δυο μελέτες περιπτώσεις Bitcoin και Ethereum. Στην συνέχεια κατηγοριοποιείται παρουσιάζοντας την τρίτη μελέτη περίπτωσης που αφορά την εταιρεία Ripple και τις «δομές» blockchain Hyperldger Fabric, Corda και Qurorum.

3.2 Ορισμός του Blockchain και η ιστορική αναδρομή της τεχνολογίας

Η Swan (2015) ορίζει το blockchain ως ένα κατανεμημένο συνεχές κατάστιχο στο οποίο καταγράφονται οι συναλλαγές, μία βάση δεδομένων διαμοιρασμένη σε όλους τους κόμβους του δικτύου που ανανεώνεται από τους miners, παρακολουθείται από τον καθένα χωρίς να ελέγχεται από κανένα. Είναι σαν ένα τεράστιο διαδραστικό υπολογιστικό φύλλο που ο καθένας έχει πρόσβαση ενώ παράλληλα μπορεί να το ανανεώσει και να επικυρώσει ότι τα κεφάλαια που χρησιμοποιούνται στις ψηφιακές συναλλαγές είναι μοναδικά. Ο Mougayar (2016) δίνει τρεις διαφορετικές ερμηνείες· τεχνικά πρόκειται για μια υποστηρικτική βάση δεδομένων που περιέχει ένα κατανεμημένο κατάστιχο που μπορεί να ελεγχθεί από τον καθένα, από επιχειρηματικής σκοπιάς πρόκειται για ένα δίκτυο ανταλλαγών για την επίτευξη συναλλαγών, αξίας, περιουσιακών στοιχείων μεταξύ ισότιμων, μέσα στο δίκτυο δρώντων χωρίς την ύπαρξη ενδιάμεσων και από νομικής σκοπιάς πρόκειται για ένα μέσο επικύρωσης συναλλαγών που αντικαθιστά την ανάγκη για την ύπαρξη ενός έμπιστου φορέα. Αν και η δημιουργία του blockchain αναφέρθηκε το 2009 από τον Satoshi Nakamoto στο άρθρο του “Bitcoin: A Peer-to-Peer Electronic Cash System” (η ανάλυσή του θα γίνει στην συνέχεια) ο οποίος το χρησιμοποίησε για την επικύρωση των συναλλαγών η ιδέα της χρονικής αποτύπωσης για την δημιουργία της πνευματικής ιδιοκτησίας αποτυπώθηκε στο 1991 από τους Haber και Stornetta.

Βλέποντας ότι η ψηφιοποίηση κειμένων, ηχητικών και οπτικοακουστικών αρχείων επιτρέπει την εύκολη μετατροπή τους, αναγνώρισαν την ανάγκη για δημιουργία ενός μέσου χρονικής αποτύπωσης των αρχείων για την προστασία των πνευματικών δικαιωμάτων των δημιουργών τους. Η διαδικασία χρονικής αποτύπωσης

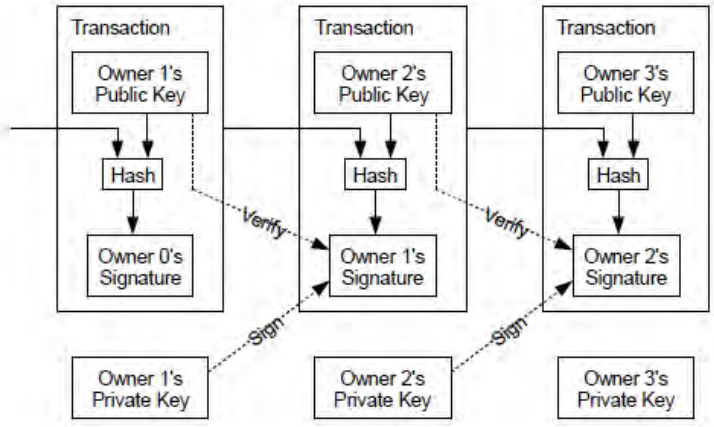
θα πρέπει να διέπεται από δύο αρχές. Η πρώτη αφορά την δυνατότητα της αποτύπωσης των δεδομένων χωρίς να στηρίζεται στα χαρακτηριστικά του μέσου που εμφανίζονται τα δεδομένα έτσι ώστε ακόμη και μία μικρή αλλαγή να είναι εμφανής. Η δεύτερη αφορά την ημερομηνία και την ώρα της αποτύπωσης η οποία θα πρέπει να είναι αδύνατο να διαφέρει από την πραγματική. Για την ανάλυση τους χρησιμοποίησαν ως παράδειγμα μία περίπτωση κατανεμημένο δικτύου χρηστών/εταιριών. Εξηγώντας ότι μια λύση στην οποία μια υπηρεσία χρονικής αποτύπωσης δέχεται από τους χρήστες τα δεδομένα, τα αποτυπώνει χρονικά και τα αποθηκεύει δημιουργεί προβλήματα ιδιωτικότητας, ταχύτητας στην αποστολή, χώρου αποθήκευσης, σφάλματων στην αποθήκευση αλλά και εμπιστοσύνης πρότειναν δύο διαφορετικές λύσεις.

Και στις δύο περιπτώσεις πρότειναν την χρήση κρυπτογραφίας και συγκεκριμένα την χρήση συναρτήσεων κατακερματισμού οι οποίες συμπιέζουν τις γραμμές του κώδικα (bit-strings) με αυθαίρετο μέγεθος σε γραμμές κώδικα με ορισμένο μέγεθος l (h : {0,1}*→ {0,1}^l). Για τις συγκεκριμένες συναρτήσεις ισχύει ότι είναι εύκολο να υπολογιστούν, να επιλεχθεί μία από αυτές τυχαία και ότι είναι υπολογιστικά αδύνατο να δεδομένου ότι δίνεται μία εξ αυτών των συναρτήσεων και ένα ζευγάρι κώδικα «bit-string» x,x’ να ικανοποιείται η συνάρτηση h(x)=h(x’). Η διαδικασία αυτή γίνεται με τις συναρτήσεις κατακερματισμού μίας κατεύθυνσης και με τη χρήση της ψηφιακής υπογραφής. Με αυτό τον τρόπο δεν απαιτείται ολόκληρη η αποθήκευση του αρχείου αλλά μόνο η παραπάνω πληροφορία. Για την δημιουργία μιας αλληλουχίας στην αποθήκευση των πληροφοριών προτείνει για κάθε νέα προσπάθεια νέας χρονικής αποτύπωσης, την προσθήκη του κώδικα της προηγούμενης χρονικής αποτύπωσης. Με αυτό τον τρόπο δημιουργεί ένα αρχείο καταγραφών με χρονολογική σειρά. Με την χρήση του κατακερματισμένου κωδικού μπορεί κάποιος να επιβεβαιώσει τον χρόνο δημιουργίας του ψηφιακού αρχείου ελέγχοντας τα δεδομένα της αλυσίδας. Η σύνδεσης της κάθε χρονική αποτύπωσης με την προηγούμενη κάνει αδύνατη την αλλαγή των δεδομένων, καθώς η παραμικρή αλλαγή στα δεδομένα μιας χρονικής αποτύπωσης θα αλλάξει πλήρως το αποτέλεσμα της συνάρτησης κατακερματισμού και κατά συνέπεια όλης της αλυσίδας. Η διαφορά έγκειται στον τρόπο αποθήκευσης της ημερομηνίας και ώρας. Στην πρώτη περίπτωση, οι χρήστες στέλνουν τα κρυπτογραφημένα αρχεία στέλνονται σε μία υπηρεσία χρονικής αποτύπωσης, στη συνέχεια η υπηρεσία τα συνδέει με την υπόλοιπη αλυσίδα και τα αποστέλλει σε όλους τους χρήστες. Στη δεύτερη περίπτωση, οι ίδιοι χρήστες

αποτυπώνουν χρονικά τα αρχεία. Η επιλογή του χρήστη γίνεται μέσω μιας ψευδοτυχαίας γεννήτριας η οποία χρησιμοποιεί το κρυπτογραφημένο αρχείο για την επιλογή του. Με αυτό τον τρόπο είναι αδύνατο να προβλεφθεί ποιος θα χρήστης θα πραγματοποιήσει την αποτύπωση. Οι δύο περιπτώσεις περιέχουν διαδικασία αυτή απαιτεί και την ύπαρξη μιας ψηφιακής υπογραφής του χρήστη η οποία χρησιμοποιείται από το σύστημα χρονικής αποτύπωσης για την αναγνώρισή του χρήστη. Η ψηφιακή υπογραφή είναι ένας αλγόριθμος για τα συμβαλλόμενα μέλη, με το οποίο ο χρήστης υπογράφει μοναδικά τα αρχεία (Haber και Stornetta, 1991).

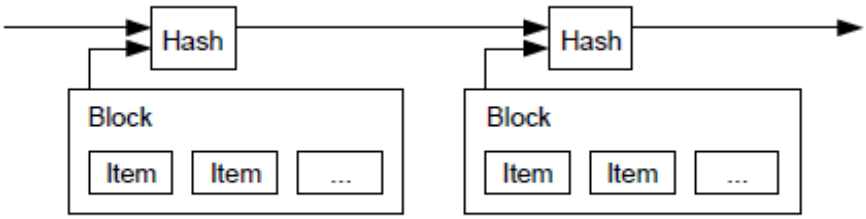
3.3 Η περίπτωση του Bitcoin

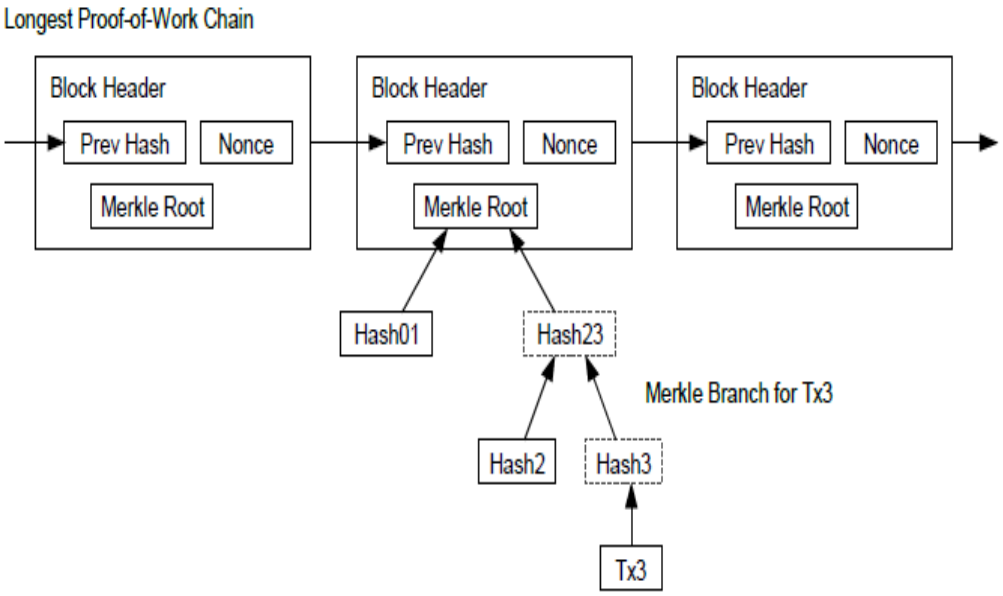
Ο Satoshi Nakamoto το 2009 παρατηρώντας ότι οι συναλλαγές μέσω Διαδικτύου στηρίζονται σχεδόν αποκλειστικά στα χρηματοπιστωτικά ιδρύματα για την επίτευξη ηλεκτρονικών πληρωμών σχεδίασε ένα μοντέλο συναλλαγών το οποίο δεν βασίζονταν σε ένα τρίτο έμπιστο πρόσωπο για την επίτευξή τους. Σε αυτό το μοντέλο αντικατέστησε την εμπιστοσύνη με κρυπτογραφία. Συγκεκριμένα περιέγραψε το ηλεκτρονικό νόμισμα ως μία αλυσίδα ψηφιακών υπογραφών. Κάθε συναλλαγή απαιτούσε την υπογραφή του ιδιοκτήτη του νομίσματος στον προηγούμενο κατακερματισμένο κωδικό (hash) και το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης με αυτό τον τρόπο θα μπορούσε να ελέγξει την υπογραφή του ιδιοκτήτη για να ελέγξει την αλυσίδα ιδιοκτησίας. Για την αποφυγή της χρήσης του νομίσματος περισσότερες από μία φορές (double-spending) πρότεινε την δημιουργία μιας βάσης χρονικού αποτυπώματος όπως αυτή στην περίπτωση των Haber και Stornetta η οποία θα ανακοινώνεται δημόσια και οι συμμετέχοντες θα συμφωνούν και θα αποδέχονται μία χρονική σειρά.



Σχήμα 3.1: Οι διαδικασία των συναλλαγών στο Bitcoin (Nakamoto, 2008)

Επιπλέον πρότεινε την δημιουργία μιας ομάδας συναλλαγών (blocks) που θα περιέχουν πάνω από μία συναλλαγές για την μείωση των πόρων που απαιτούνται για την κρυπτογράφησή τους. Μέσα σε κάθε ομάδα θα συμπυκνώνονται οι μεμονωμένες συναλλαγές με την μέθοδο Merkle tree και θα δίνεται ένας τίτλος σε αυτή. Ο τίτλος κάθε ομάδας θα περιέχει τον τίτλο του προηγούμενου και ούτω καθεξής δημιουργώντας έτσι μια σύνδεση μεταξύ τους. Για την μετατροπή του σε μία peer-to-peer βάση απαιτείται η ένα σύστημα απόδειξης της εργασίας κρυπτογράφησης. Το σύστημα αυτό υλοποιείται προσθέτοντας σε κάθε block ένα ψευδοτυχαίο αριθμό ο οποίος όταν κρυπτογραφηθεί δίνει ως αποτέλεσμα ένα συγκεκριμένο αριθμό 0 bit στην αρχή του. Αυτό επιτυγχάνεται μέσα από την χρήση επεξεργαστή CPU (διαδικασία trial and error) και η επεξεργαστική ισχύ που απαιτείται είναι εκθετική ως προς τον αριθμό των 0 bits που απαιτούνται. Με αυτό τον τρόπο παραμένει σταθερός ο αριθμός των blocks που παράγονται κατά μέσο όρο από το σύστημα. Για την επεξεργαστική ισχύ και τον ηλεκτρισμό που χρησιμοποιούν οι miners των ομάδων αποδίδεται σε αυτούς ένα νέο νόμισμα και παράλληλα το κόστος συναλλαγής. Για την αλλαγή μίας συναλλαγής απαιτείται ο επανάληψη της διαδικασίας στο block που βρίσκεται αλλά και στα μετέπειτα blocks. Ακόμα και αν κάποιος είναι σε θέση να έχει μεγαλύτερη υπολογιστική ισχύ από όλο το υπόλοιπο σύστημα θα ήταν πιο κερδοφόρο για τον ίδιο η επικύρωση νέων blocks. Αυτό αποθαρρύνει τους συμμετέχοντες από την προσπάθεια για εξαπάτηση ή αλλοίωση της αλυσίδας.





Σχήμα 3.2 και 3.3: Η διαδικασία αποθήκευσης στο Bitcoin (Nakamoto, 2008)

3.4 Τα δομικά στοιχεία της Τεχνολογίας του Blockchain

Μέσα από την ανάλυση του whitepaper του Bitcoin διακρίνονται τρείς τεχνολογίες από τις οποίες αποτελείται η τεχνολογία του Blockchain. Η πρώτη είναι τα peer to peer δίκτυα, η δεύτερη κρυπτογραφία για την αποθήκευση των δεδομένων και η τρίτη το σύστημα συναίνεσης το οποίο χρησιμοποιείται για την επέκταση blockchain. Για την βαθύτερη κατανόηση της τεχνολογίας του blockchain θα αναλυθούν τα τρία βασικά στοιχεία που το απαρτίζουν.

3.4.1 Peer-to-peer δίκτυα

Η αρχιτεκτονική δικτύωσης peer-to-peer είναι η βάση για την λειτουργία των αποκεντρωμένων υπολογιστών. Οι (Ανδρουτσέλης-Θεοτόκης και Σπινέλλης, 2004) θεωρούν ότι τα χαρακτηριστικά των peer-to-peer αρχιτεκτονικών είναι δύο. Το πρώτο χαρακτηριστικό είναι ο απευθείας διαμοιρασμός υπολογιστικών πόρων μεταξύ των χρηστών χωρίς να απαιτείται η ύπαρξη ενδιάμεσου κεντρικού διακομιστή. Κεντρικοί διακομιστές μπορεί να υπάρχουν για την διεκπεραίωση συγκεκριμένων λειτουργιών όπως την στήριξη του συστήματος, την προσθήκη νέων κόμβων/χρηστών, διάφορες διαδικασίες σχετικές με την κρυπτογράφηση των δεδομένων αλλά ακόμη και για την επίτευξη της βασικής λειτουργίας του συστήματος. Στην περίπτωση που της έλλειψης ενός κεντρικού διακομιστή, τις παραπάνω λειτουργίες αναλαμβάνουν οι χρήστες/κόμβοι του. Το δεύτερο χαρακτηριστικό των συγκεκριμένων αρχιτεκτονικών

αναφέρεται στην δυνατότητα του συστήματος να διαχειρίζεται την αστάθεια και την μεταβλητή συνδεσιμότητα ως κάτι συνηθισμένο. Συγκεκριμένα έχει την δυνατότητα να προσαρμόζεται αυτόματα σε σφάλματα της συνδεσιμότητας του δικτύου και των υπολογιστών όπως και στην παροδικότητα των κόμβων. Η ιδιότητα του να μπορεί να αντιμετωπίζει τα σφάλματα και να οργανώνεται αυτόματα του επιτρέπουν να διατηρεί την συνδεσιμότητα μέσα στο δίκτυο όπως και την απόδοσή του. Οι δύο περιπτώσεις που αναφέρθηκαν αποτελούν ουσιαστικά και τις δύο βασικές κατηγορίες, τα δομημένα και τα αδόμητα peer-to-peer δίκτυα.

Η διαφορετικότητα των δικτύων που βασίζονται στην αρχιτεκτονική peer-to-peer καθιστά δύσκολη την ύπαρξη ενός ορισμού που να καλύπτει το σύνολο αυτών. Ο Shirky (2000) ορίζει ως peer-to-peer «μία σειρά εφαρμογών η οποία εκμεταλλεύεται μια σειρά πόρων όπως η αποθήκευση, η επεξεργαστικοί ισχύ, οι πληροφορίες και η ανθρώπινη παρουσία που βρίσκονται μέσα στο Διαδίκτυο». Οι Ανδρουτσέλης-Θεοτόκη και Σπινέλλης (2004) θεώρησαν ότι ο συγκεκριμένος ορισμός δεν καλύπτει όλο το φάσμα των p2p συστημάτων και ορίσαν ως peer-to-peer «τα κατανεμημένα συστήματα τα οποία αποτελούνται από διασυνδεδεμένους κόμβους ικανούς να οργανώνονται αυτόνομα σε διαδικτυακές τοπολογίες με στόχο τον διαμοιρασμό πόρων, ικανών να προσαρμόζονται στα σφάλματα, και στον παροδικό αριθμό των κόμβων ενώ παράλληλα διατηρούν την συνδεσιμότητα και την απόδοσή τους χωρίς να απαιτούν την ύπαρξή ή την στήριξη ενός κεντρικού διακομιστή ή μίας κεντρικής αρχής.

Η εφαρμογή αυτών των συστημάτων μπορεί να διαχωριστεί δύο κατηγορίες σύμφωνα με τους Ανδρουτσέλη-Θεοτόκη και Σπινέλλη (2004). Η πρώτη κατηγορία αφορά συστήματα ανταλλαγής αρχείων. Τέτοια συστήματα επιτυγχάνουν την απλή μεταφορά αρχείων μέσα στο δίκτυο και επιτρέπουν την αναζήτηση αρχείων. Η ασφάλεια, η διαθεσιμότητα των αρχείων και η ανθεκτικότητα των συστημάτων δεν είναι κύριο μέλημα τους. Τα συγκεκριμένα συστήματα ευθύνονται κατά κύριο λόγο για την αύξηση της δημοσιότητας των peer-to-peer τεχνολογιών. Η δεύτερη κατηγορία αφορά συστήματα δημοσίευσης περιεχομένου και δημοσίευσης αρχείων. Αυτά τα συστήματα στοχεύουν στην δημιουργία ενός κατανεμημένου μέσου αποθήκευσης, μέσα από το οποίο οι χρήστες μπορούν να δημοσιεύσουν να αποθηκεύσουν και να διανέμουν τα αρχεία. Η πρόσβαση στα αρχεία γίνεται ελεγχόμενα και ο στόχος αυτών των συστημάτων είναι η ασφάλεια και η ανθεκτικότητα. Παράλληλα στοχεύουν στην

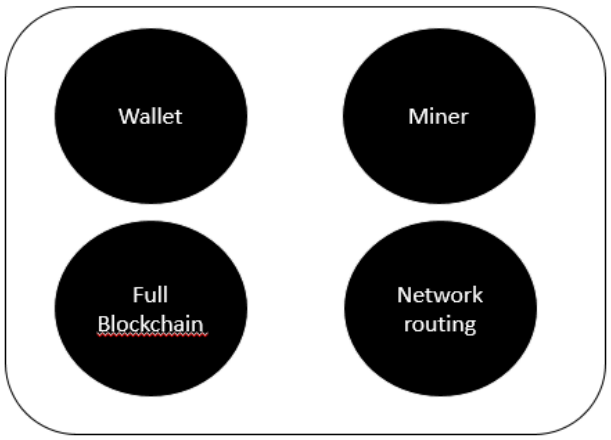
ενσωμάτωση διατάξεων που αφορούν την αξιοπιστία, την ανωνυμία και την αντίσταση λογοκρισία αλλά και την συνεχή διαχείριση των αρχείων.

Χαρακτηριστικό παράδειγμα ενός p2p συστήματος για μεταφορά αρχείων είναι το Napster. Πρόκειται για μία πλατφόρμα p2p που επέτρεπε στους χρήστες τον διαμοιρασμό τραγουδιών η οποία δημιουργήθηκε στα τέλη του ΄90. Η εύκολη πρόσβαση σε ένα πολύ μεγάλο αριθμό αρχείων μουσικής χωρίς αντίτιμο την έκανε διάσημη φτάνοντας μέχρι και 80 εκατομμύρια εγγεγραμμένους χρήστες. Ωστόσο τα προβλήματα πνευματικής ιδιοκτησίας που αντιμετώπιζε, σε ότι αφορά την μεταφορά διανομή των μουσικών αρχείων, το οδήγησαν σε οριστική παύση λειτουργίας το 2001 (Harris,2018)

3.4.1.1 Το p2p δίκτυο του Bitcoin

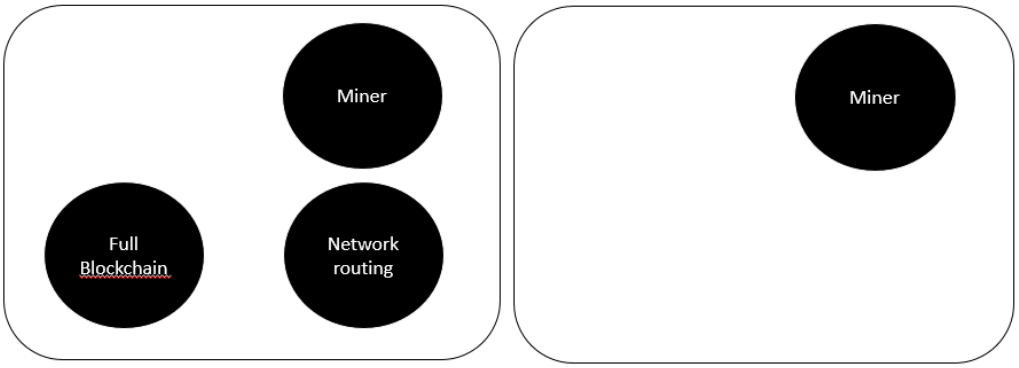
Στην περίπτωση του Bitcoin, οι κόμβοι του δικτύου, παρόλο που θεωρούνται ίσοι, μπορούν να έχουν διαφορετικές ρόλους αναλόγως με την λειτουργικότητά τους. Ένας κόμβος μπορεί να εμπεριέχει 4 στοιχεία, το πορτοφόλι (πρόκειται για «θήκη» των δύο κλειδιών του χρήστη και εξηγούνται στην επόμενη κατηγορία), την λειτουργία του mining, την λειτουργία της δρομολόγησης του δικτύου (network routing) και την αλυσίδα του blockchain. Η λειτουργικότητά τους διαφέρει ανάλογα με τον αριθμό των στοιχείων που διαθέτουν (Αντωνόπουλος, 2016).

Το πορτοφόλι είναι μία «θήκη» για το δημόσιο και το ιδιωτικό κλειδί του κάθε χρήστη. Η λειτουργία του mining είναι μία διαδικασία που χρησιμοποιείται για την αποθήκευση των νέων συναλλαγών στο blockchain και την παραγωγή νέων νομισμάτων και αναφέρεται στην επεξεργαστική ισχύ των κόμβων. Η λειτουργία της δρομολόγησης (network routing) αναφέρεται ουσιαστικά στην δυνατότητα των κόμβων να επικυρώνουν και να διαδίδουν τις νέες συναλλαγές και block στους υπόλοιπους κόμβους. Ως αλυσίδα του blockchain (full blockchain) αναφέρεται σε όλες τις επιτυχημένες συναλλαγές που έχουν γίνει από την αρχή του δικτύου και έχουν αποθηκευτεί σε αυτό (Αντωνόπουλος, 2016).



Σχήμα 3.4: Βασικός κόμβος στο Bitcoin (Αντωνόπουλος 2016)

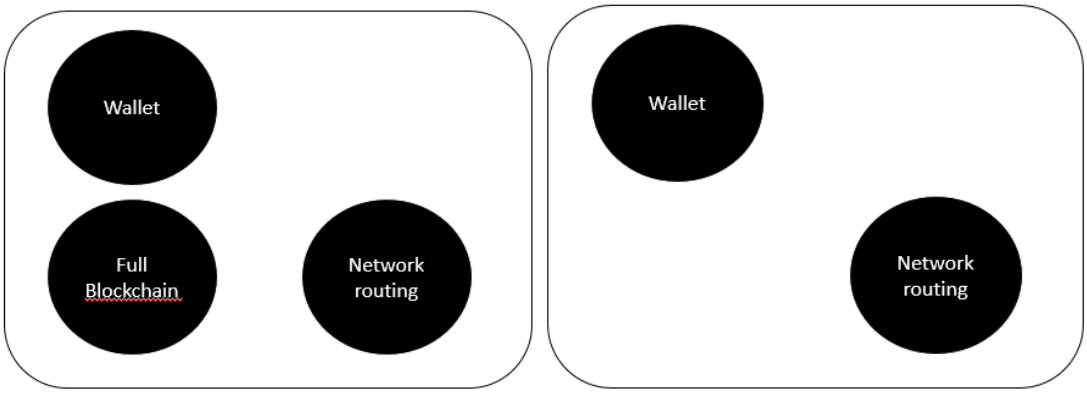
Ένας πλήρης κόμβος εμπεριέχει και τα 4 στοιχεία. Ο κάθε χρήστης/κόμβος του δικτύου δεν απαιτείται να έχει και τις τέσσερις παρακάτω λειτουργίες. Ένας miner θα πρέπει να έχει τουλάχιστον τις τρείς λειτουργίες, της δρομολόγησης, του mining και ολόκληρη την αλυσίδα. Ωστόσο υπάρχουν και περιπτώσεις που οι miners λειτουργούν σε ομάδες (pools), ενώνοντας δηλαδή την υπολογιστική ισχύ τους. Σε αυτές τις περιπτώσεις δεν απαιτείται από τους κόμβους των miner μόνο η λειτουργία του mining δηλαδή η επεξεργαστική ισχύ τους (Αντωνόπουλος, 2016).



Σχήμα 3.5: Κόμβοι επικύρωσης στο Bitcoin (Αντωνόπουλος 2016)

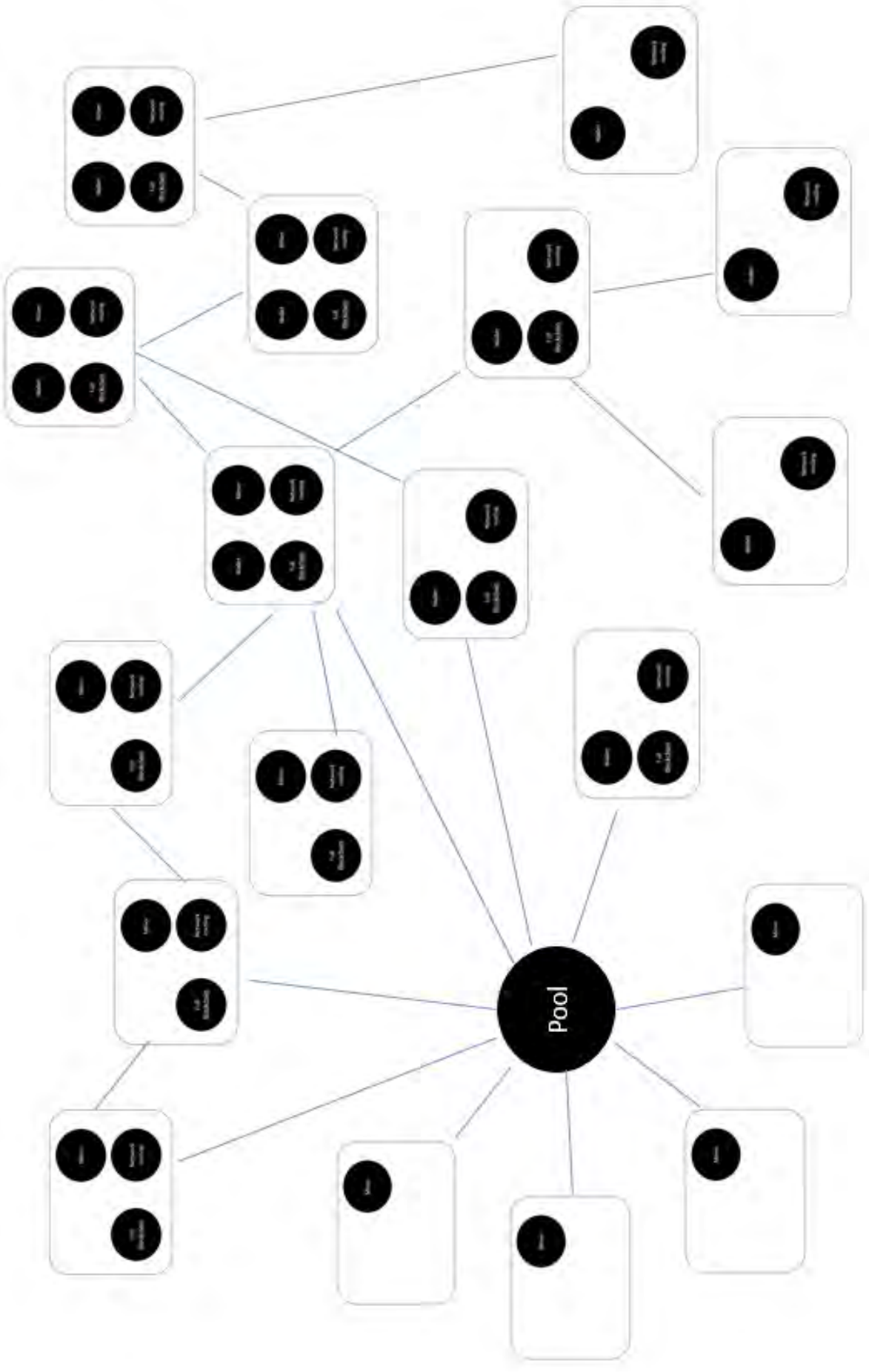
Ένας χρήστης ενός πορτοφολιού μπορεί να εμπεριέχει το πορτοφόλι, την αλυσίδα του blockchain και την λειτουργία της δρομολόγησης. Ωστόσο οι περιορισμένοι πόροι σε ότι αφορά την αποθήκευση (τα smartphones είναι ένα χαρακτηριστικό παράδειγμα) καθιστά αδύνατη την ύπαρξη ολόκληρης της αλυσίδας του blockchain. Σε αυτές τις περιπτώσεις χρησιμοποιείται η τεχνολογία SPV (simplified payment verification) η οποία επιτρέπει στους συγκεκριμένους χρήστες-κόμβους να είναι σε θέση να κάνουν συναλλαγές. Πρόκειται για μία διαδικασία που

επιτρέπει στους χρήστες να χρησιμοποιούν το πορτοφόλι τους έχοντας αποθηκεύσει μόνο τις επικεφαλίδες των block της αλυσίδας (Αντωνόπουλος, 2016).



Σχήμα 3.6: Οι μορφές πορτφολιών στο Bitcoin (Αντωνόπουλος, 2016)

Στο παρακάτω σχήμα φαίνεται πως λειτουργεί το p2p δίκτυο του Bitcoin. Στο σχήμα φαίνονται οι κόμβοι χρήστες που αναλύθηκαν παραπάνω.



Σχήμα 3.7: Το δίκτυο του Bitcoin (Αντωνόπουλος, 2016)

Καθώς αναφερόμαστε σε ένα σύστημα p2p απαιτείται η συνεχής επικοινωνία και ενημέρωση των κόμβων είναι απαραίτητη. Ο Nakamoto 2009 έθεσε τους εξής κανόνες για την λειτουργία του δικτύου:

1. Οι νέες συναλλαγές μεταδίδονται σε όλους τους κόμβους
2. Κάθε κόμβος συλλέγει τις νέες σε ένα block
3. Κάθε κόμβος δουλεύει για την λύση ενός προβλήματος γνωστό ως proof-of-work
4. Όταν ένας κόμβος βρίσκει ένα proof of work το μεταδίδει και στους υπόλοιπους κόμβους
5. Οι κόμβοι δέχονται ένα block μόνο όταν όλες οι συναλλαγές μέσα σε αυτό είναι έγκυρες
6. Οι κόμβοι εκφράζουν την αποδοχή τους στο block με την χρήση της κατακερματισμένης ακολουθίας του (hash) μέσα στο νέο block ως το hash του προηγούμενου block.

3.4.2 Κρυπτογραφία

Ως κρυπτογραφία ορίζεται από τους Menezes, van Oorschot και Vanstone (1996:19-20) ως η μελέτη των μαθηματικών τεχνικών που σχετίζονται με τις πτυχές της ασφάλειας πληροφοριών όπως η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η ταυτοποίηση των προσώπων και η ταυτοποίηση της προέλευσης των δεδομένων. Η κρυπτογραφία δεν είναι μόνο ένα μέσο παροχής ασφάλειας των πληροφοριών αλλά ένα σύνολο τεχνικών. Οι κύριοι στόχοι της κρυπτογραφίας είναι η εμπιστευτικότητα/ ιδιωτικότητα, η ακεραιότητα των δεδομένων, η πιστοποίηση και η αδυναμία της απάρνησης.

Ως εμπιστευτικότητα ορίζει την υπηρεσία που χρησιμοποιείται για την προστασία των δεδομένων, δίνοντας πρόσβασης μόνο σε όσους έχουν εξουσιοδοτηθεί. Με αυτό τον τρόπο επιτυγχάνεται και η ιδιωτικότητα.

Η ακεραιότητα των δεδομένων είναι μία υπηρεσία που αντιμετωπίζει την μη εξουσιοδοτημένη αλλαγή των δεδομένων. Για να επιτευχθεί η ακεραιότητα πρέπει να είναι δυνατή η αναγνώριση της χειραγώγησης των δεδομένων (διαδικασίες όπως η διαγραφή, η προσθήκη ή η αλλαγή των δεδομένων) από μη εξουσιοδοτημένα πρόσωπα.

Η πιστοποίηση ορίζεται η υπηρεσία που σχετίζεται με την αναγνώριση των δρώντων και των πληροφοριών που ανταλλάσσουν. Σε μία συνομιλία οι συμμετέχοντες επιθυμούν πρέπει να είναι σε θέση να αναγνωρίσουν αμφότεροι τον συνομιλητή τους αλλά και τα χαρακτηριστικά των πληροφοριών (όπως η πηγή, η ημερομηνία και η ώρα αποστολής) που ανταλλάσσουν κατά την διάρκεια της επικοινωνίας.

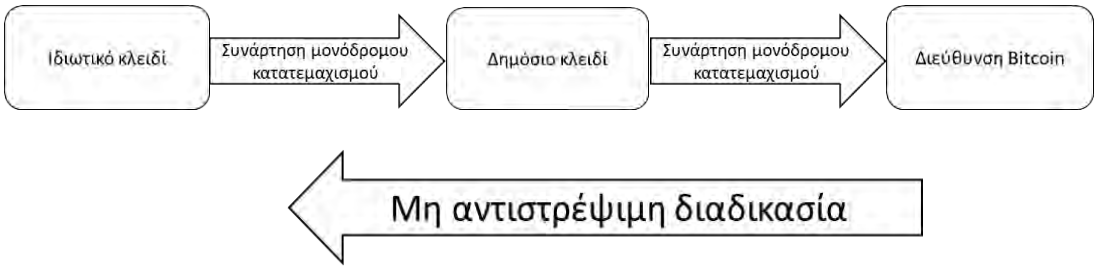
Η αδυναμία της απάρνησης (non-repudiation) είναι μία υπηρεσία που αποτρέπει μία οντότητα από την άρνηση μιας προηγούμενης δέσμευσης. Για παράδειγμα, σε μία αγοροπωλησία, όταν μία πλευρά δώσει την συγκατάθεσή στην αγορά ενός προϊόντος και στην συνέχεια αρνηθεί την δήλωσή της, για την επίλυση του ζητήματος απαιτείται ένας τρίτος έμπιστος συμβαλλόμενο μέρος.

3.4.2.1 Η κρυπτογραφία στο Bitcoin

3.4.2.1.1 Η διαδικασία διαχείρισης της ιδιοκτησίας

Σύμφωνα με τον Αντωνόπουλο (2016) το Bitcoin χρησιμοποιεί την κρυπτογραφία για την διαχείριση της ιδιοκτησίας των νομισμάτων μέσα στο σύστημά του. Αυτό επιτυγχάνεται με την διαδικασία κρυπτογράφησης δημόσιου κλειδιού. Πρόκειται για μία διαδικασία που ανακαλύφθηκε από τους Diffie και Hellman το 1976. Η διαδικασία εμπεριέχει την ύπαρξη δύο κλειδιών. Το πρώτο είναι το ιδιωτικό κλειδί το οποίο είναι και το προσωπικό κλειδί του χρήστη και λειτουργεί ως ένα κλειδί αποκρυπτογράφησης. Το δεύτερο είναι το δημόσιο κλειδί το οποίο είναι παράγωγο του ιδιωτικού και μπορεί να δοθεί σε άλλους χρήστες για την αποδοχή νομισμάτων. Η διαδικασία παραγωγής του δημόσιου κλειδιού είναι τέτοια που είναι αδύνατο, γνωρίζοντας το δημόσιο κλειδί, να βρεθεί το ιδιωτικό κλειδί ενώ η αντίστροφη διαδικασία είναι εφικτή (με συναρτήσεις μονόδρομου κατακερματισμού) (Diffie & Hellman, 1976). Παράλληλα το ιδιωτικό κλειδί είναι αυτό που παράγει και την ψηφιακή υπογραφή η οποία χρησιμοποιείται για την διεκπεραίωση των συναλλαγών. Η ψηφιακή υπογραφή διαμορφώνεται με την χρήση των στοιχείων της συναλλαγής και το ιδιωτικό κλειδί του αποστολέα. Επομένως σε κάθε συναλλαγή παράγεται διαφορετική υπογραφή. Ωστόσο, ο καθένας που έχει τα στοιχεία της συναλλαγής και το δημόσιο κλειδί μπορεί να ελέγξει αν η συναλλαγή έγινε από το συγκεκριμένο χρήστη. Από το δημόσιο κλειδί του κάθε χρήστη είναι δυνατό να παραχθεί και η διεύθυνση bitcoin του κάθε χρήστη. Ουσιαστικά λειτουργεί όπως και το δημόσιο κλειδί, χρησιμοποιείται δηλαδή για την αποδοχή νομισμάτων. Η δημιουργία του

βασίζεται σε συναρτήσεις μονόδρομου κατακερματισμού όπως και στην παραγωγή δημόσιου κλειδιού, προσθέτοντας μεγαλύτερη ασφάλεια στον χρήστη.



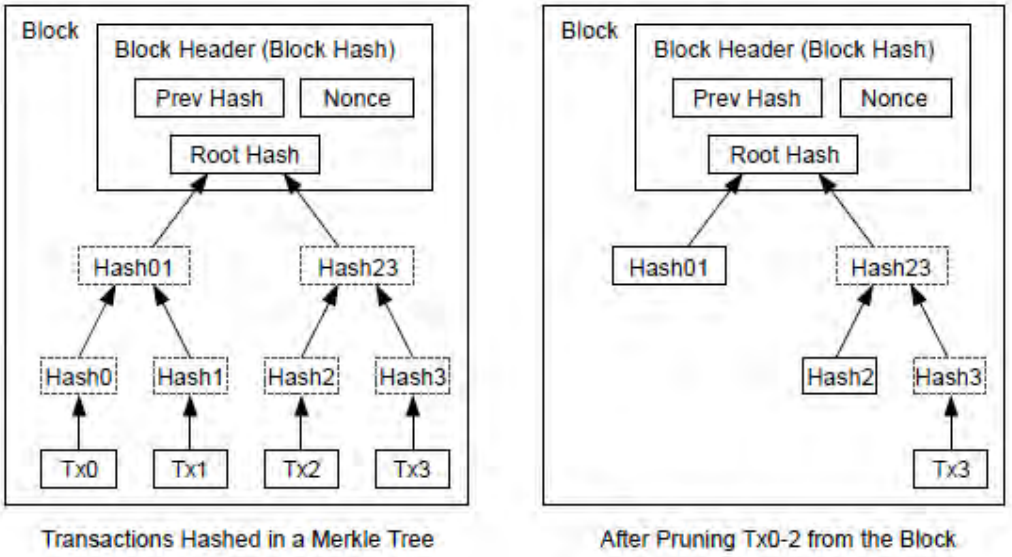
Σχήμα 3.8: Δημόσιο και ιδιωτικό κλειδί (Αντωνόπουλος, 2016)

Η παραπάνω διαδικασία δεν αναφέρεται στην αποθήκευση των στοιχείων στο blockchain αλλά στον τρόπο μεταφοράς των νομισμάτων μέσα σε αυτό, διαδικασία άρρηκτα συνδεδεμένη με το blockchain του bitcoin. Τα συγκεκριμένα κλειδιά δημιουργούνται και αποθηκεύονται σε βάσεις εκτός του blockchain, γνωστά και ως πορτοφόλια (Αντωνόπουλος, 2016). Ουσιαστικά τα πορτοφόλια είναι μία «θήκη» για το δημόσιο και το ιδιωτικό κλειδί του κάθε χρήστη. Υπάρχουν 5 βασικά είδη πορτοφολιών (Bitcoin Magazine, 2015). Το πρώτο είναι σε μορφή εφαρμογής και εγκαθίσταται κανονικά στο υπολογιστή σε μορφή προγράμματος. Το δεύτερο είναι το διαδικτυακό πορτοφόλι το οποίο διατίθεται από τα ανταλλακτήρια, σημεία που μπορεί κανείς να αγοράσει εικονικά νομίσματα όπως το Bitcoin. Το τρίτο είναι το πορτοφόλι για mobile συσκευές, εφαρμογές δηλαδή οι οποίες χρησιμοποιούν την τεχνολογία SPV. Το τέταρτο είδος είναι το πορτοφόλι σε μορφή συσκευής (hardware) ενώ τέλος το πέμπτο είδος είναι σε φυσική μορφή και εκτυπώνεται σε χαρτί. Οι τρεις πρώτες κατηγορίες αφορούν πορτοφόλια συνδεδεμένα στο διαδίκτυο ενώ οι δύο τελευταίες αφορούν περιπτώσεις πορτοφολιών που δεν συνδέονται άμεσα με αυτό.

3.4.2.1.2 Η διαδικασία αποθήκευσης των συναλλαγών

Ένα block αποτελείται από τρία βασικά στοιχεία, την επικεφαλίδα, τις συναλλαγές που αποθηκεύονται μέσα σε αυτό και ένα ψευδοτυχαίο αριθμό (nonce). Όπως αναφέρει ο Satoshi Nakamoto (2009) για τον περιορισμό του αποθηκευτικού χώρου που απαιτείται για την αποθήκευση των συναλλαγών χρησιμοποιείται η διαδικασία Merkle-tree. Πρόκειται για μία διαδικασία κατά την οποία χρησιμοποιούνται συναρτήσεις μονόδρομου κατακερματισμού (one way hash

functions) για την μείωση του χώρου που απαιτούν τα καταγεγραμμένα στοιχεία (Merkle 1980). Οι συναρτήσεις μονόδρομου κατακερματισμού χρησιμοποιούνται σε όλες τις συναλλαγές με αποτέλεσμα την μείωση των πληροφοριών που αποθηκεύονται σε μία κατακερματισμένη ακολουθία που θεωρείται η ρίζα κάθε κατακερματισμένης ακολουθίας των συναλλαγών (root hash).



Σχήμα 3.8: Η διαδικασία Merkle Tree (Nakamoto, 2008)

Η επικεφαλίδα του block αποτελείται από μία σειρά στοιχείων. Η συγκεκριμένη ακολουθία αποτελείται διαμορφώνεται από μία σειρά κατακερματισμένων ακολουθιών. Συγκεκριμένα η επικεφαλίδα του κάθε block περιέχει το την έκδοση του πρωτόκολλου που χρησιμοποιήθηκε την ακολουθία του προηγούμενου block την ακολουθία του root hash που αποθηκεύεται μέσα στο συγκεκριμένο block, την ημερομηνία που αποθηκεύεται, μία ακολουθία που ορίζει την δυσκολία της διαδικασίας mining στο συγκεκριμένο block και τον ψευδοτυχαίο αριθμό (nonce). Τα παραπάνω στοιχεία χρησιμοποιούνται για την δημιουργία της κατακερματισμένης ακολουθίας του κάθε block. Με την συμπλήρωση όλων των στοιχείων η επικεφαλίδα του block είναι έτοιμη για να περάσει στην διαδικασία του mining. Η συγκεκριμένη ακολουθία της επικεφαλίδας του block δεν αποθηκεύεται απευθείας στο block αλλά υπολογίζεται σε κάθε κόμβο ξεχωριστά (Αντωνόπουλος, 2016).

3.4.2.2 Η σύστημα συναίνεσης (consensus) και η διαδικασία του Mining

Για την αποθήκευση των δεδομένων και την δημιουργία νέων blocks στο p2p δίκτυο ο Nakamoto χρησιμοποίησε ένα σύστημα απόδειξης της εργασίας (Proof of

work) παρόμοιο με αυτό το Hashcash. Το Hashcash είναι ένας μηχανισμός ο οποίος δημιουργήθηκε από τον Adam Back (2002) και εφαρμόστηκε το 1997 ως μία μέθοδος ελέγχου της αλόγιστης χρήσης των ψηφιακών πόρων (χαρακτηριστικό παράδειγμα είναι τα email). Πρόκειται για μία διαδικασία που απαιτεί την υπολογιστική ισχύ ενός επεξεργαστή για να υπολογίσει ένα «κουπόνι» (token), παράγωγο τον συναρτήσεων κόστους που χρησιμοποιούνται. Ο κάθε κόμβος χρήστης που συμμετέχει πρέπει να χρησιμοποιήσει τις συναρτήσεις κόστους για να παράγει το token το οποίο χρησιμοποιείται για την συμμετοχή του σε ένα πρωτόκολλο με ένα διακομιστή. Ο διακομιστής ελέγχει την αξία του ειδικού νομίσματος μέσω συναρτήσεων αξιολόγησης και συνεχίζει στην διαδικασία του πρωτοκόλλου μόνο όταν το αξία του νομίσματος είναι η κατάλληλη. Οι συναρτήσεις παραμετροποιούνται ανάλογα με μέγεθος της εργασίας που δαπανά ο χρήστης για την παραγωγή του token (Back 2002).

Οι συναρτήσεις κόστους διαχωρίζονται σε διαδραστικές και μη. Με τις διαδραστικές συναρτήσεις κόστους ο διακομιστής θέτει ένα πρόβλημα στον χρήστη προς επίλυση. Αντίθετα στις μη διαδραστικές ο χρήστης/κόμβος επιλέγει την συνάρτηση κόστους. Η συνάρτηση κόστους του Hashcash είναι μία μη διαδραστική συνάρτηση απεριορίστου πιθανού κόστους (unbounded probabilistic cost), δεν μπορεί να υπολογιστεί εξαρχής δηλαδή ο χρόνος υπολογισμού του token. Παράλληλα ορίζεται ως trap-door free, δηλαδή ο διακομιστής δεν έχει πλεονέκτημα στην παραγωγή νομισμάτων. Τέλος χαρακτηρίζεται ως δημόσια ελέγξιμός, δηλαδή μπορεί ο καθένας να ελέγξει ότι η διαδικασία παραγωγής έγινε. Για την αποτροπή της χρήσης των νομισμάτων σε πάνω από ένα διακομιστή, το κάθε token έχει αξία μόνο στο διακομιστή που παράχθηκε (Back 2002).

Καθώς η συνάρτηση Hashcash δημιουργήθηκε για την αποτροπή της αλόγιστης χρήσης των ψηφιακών πόρων όπως τα emails, είναι αδύνατη η χρήση διαδραστικών συναρτήσεων καθώς είναι αδύνατη η συνεχής επικοινωνία μεταξύ του χρήστη και του διακομιστή. Ωστόσο, υπάρχει και η περίπτωση του διαδραστικού πρωτοκόλλου Hashcash που έχει ο ως στόχο την αποφυγή της χρήση των πόρων του διακομιστή μόνο από ένα κόμβο/χρήστη. Η μέθοδος αυτή είναι γνωστή ως επίθεση άρνησης εξυπηρέτησης (DoS attack) (Back, 2002).

Στην περίπτωση του bitcoin αλλά και των περισσότερων δικτυών που χρησιμοποιούνε το blockchain, παρόλο που χρησιμοποιούνε το proof-of-work δεν

υπάρχει κεντρικός διακομιστής που να επιβεβαιώνει την διαδικασία. Η διαδικασία της καταγραφής στο κατανεμημένο δίκτυο γίνεται από τους ίδιους κόμβους που συμμετέχουν στην διαδικασία του mining όπως περιγράφεται στην ανάλυση του p2p δικτύου. Η επικύρωση γίνεται από όλους τους κόμβους/χρήστες που συμμετέχουν στο δίκτυο ελέγχοντας αν όλες οι συναλλαγές που περιέχονται στο νέο block είναι έγκυρες. Παράλληλα ελέγχουν την εγκυρότητα της διαδικασίας του proof-of-work.

Η διαδικασία του proof-of-work στο δίκτυο του bitcoin επιτυγχάνεται μέσα από τον υπολογισμό της κατακερματισμένης ακολουθίας (hash) του ψευδοτυχαίου αριθμού (nonce) που βρίσκεται μέσα σε κάθε block. Για τον υπολογισμό του ωστόσο σε κάθε περίπτωση ορίζεται ένας αριθμός μηδενικών bit με τον οποίο θα αρχίζει η κατακερματισμένη ακολουθίας. Ουσιαστικά, βάζει τους κόμβους που συμμετέχουν στην διαδικασία του mining να ανταγωνιστούν μεταξύ τους για το ποιος θα καταφέρει να λύσει πρώτος την συγκεκριμένη ακολουθία. Η διαδικασία αυτή δίνει την δυνατότητα να στο σύστημα να διατηρεί σταθερό τον αριθμό των παραγόμενων block σε 1 ανά 10 λεπτά κατά μέσο όρο. Η αύξηση των μηδενικών bit στην αρχή της ακολουθίας αυξάνει την εκθετικά την δυσκολία του υπολογισμού του (Nakamoto 2009).

Η διαδικασία του proof-of-work έχει υιοθετηθεί και από άλλα εγχειρήματα ή πλατφόρμες που χρησιμοποιούν το blockchain ως διαδικασία. Ένα από αυτά είναι το Ethereum που θα αναλυθεί στην συνέχεια. Ωστόσο δεν είναι το μόνο σύστημα που επιτρέπει την συναίνεσης μέσα σε μια υλοποίηση του blockchain. Στην συνέχεια θα αναλυθούν οι περιπτώσεις άλλων πλατφορμών με διαφορετικούς αλγόριθμους συναίνεσης.

3.4.3 Η έκδοση νέων Bitcoin και τα κόστη συναλλαγής

Οι miners για την επεξεργαστική ισχύ και την ενέργεια που καταναλώνουν τους απονέμονται τα νέα νομίσματα που παράγονται. Παράλληλα, από κάθε συναλλαγή, ο miner αποκομίζει και ένα αντίτιμο από τον εκκινητή της συναλλαγής. Η παραγωγή νομισμάτων μειώνεται κατά το ήμισυ κάθε 210,000 νέα blocks ή περίπου κάθε 4 χρόνια. Τα πρώτα 4 χρόνια της λειτουργίας του, για κάθε παραγωγή νέου block απονέμονταν στον miner 50 bitcoins. Στην συνέχεια από τον Νοέμβριο του 2012 το αντίτιμο για την δημιουργία ενός block μειώθηκε στα 25 bitcoins. Ο Αντωνόπουλος (2016: 214-215) αναφέρει επίσης ότι τα bitcoins που θα παραχθούν είναι σχεδόν

εικοσιένα εκατομμύρια ή 2,099,999,997,690,000 satoshis (υποδιαίρεση του bitcoin). Ακολουθώντας τον παραπάνω κανόνα υπολογίζεται ότι το τελευταίο bitcoin θα δημιουργηθεί περίπου το 2140 ή μετά από έξι εκατομμύρια εννιακόσιες τριάντα χιλιάδες block.

Γράφημα 3.1: Η προσφορά του Bitcoin (Αντωνόπουλος, 2016)

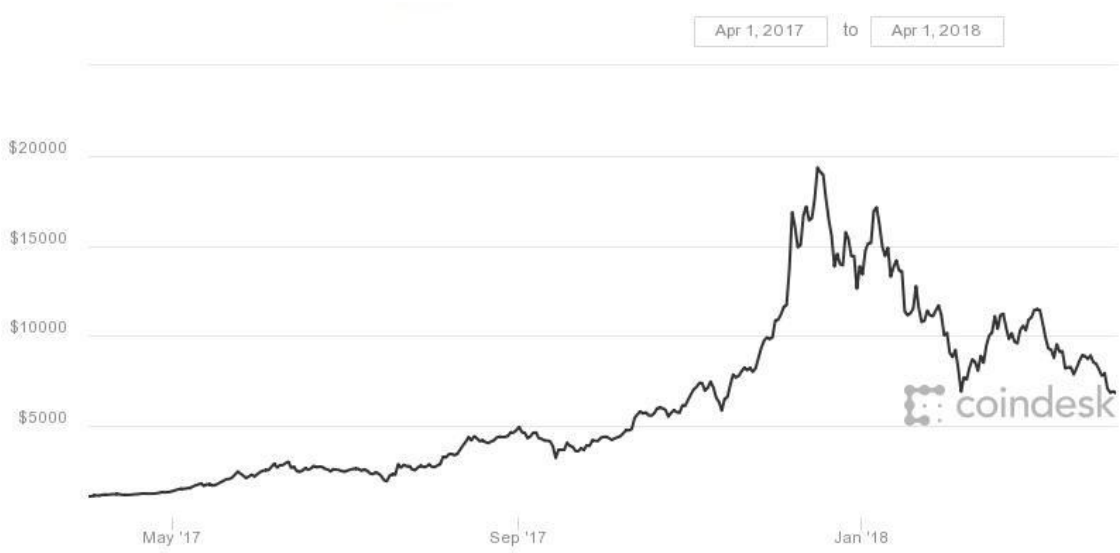
Ο πεπερασμένος αριθμός των bitcoin δημιουργεί μία καθορισμένη προσφορά χρήματος στο δίκτυο. Αντιθέτως, στα συμβατικά νομίσματα οι Κεντρικές τράπεζες είναι υπεύθυνες για την διαχείριση του πληθωρισμού, οι οποίες είναι σε θέση να «δημιουργήσουν» απεριόριστο αριθμό νέων νομισμάτων.

Ο Evans (2014) θεωρεί ότι οι blockchain πλατφόρμες λόγω της αδυναμίας καταστροφής των νομισμάτων όπως στην περίπτωση του bitcoin θα πρέπει να θεωρούνται μακράς διάρκειας περιουσιακά στοιχεία (long lived assets). Η Ευρωπαϊκή Κεντρική Τράπεζα (2015) ορίζει τα κρυτονομίσματα ως «εικονικά νομίσματα». Συγκεκριμένα, επισημαίνει ότι από οικονομικής σκοπιάς, ένα νόμισμα λειτουργεί ως μέσο συναλλαγής, ως μέσο αποθήκευσης αξίας και ως μέσο υπολογισμού του κόστους και αξίας αγαθών και υπηρεσιών. Ωστόσο η χαμηλή αποδοχή τους για την αγορά

προϊόντων και υπηρεσιών και η υψηλή αστάθεια στην αξία τους τα καθιστούν αναξιόπιστο μέσο υπολογισμού κόστους και αξίας προϊόντων.

Από νομικής σκοπιάς, χρήμα θεωρείται οτιδήποτε μπορεί να χρησιμοποιηθεί για ανταλλαγή αξίας. Ο όρος «νόμισμα» χρησιμοποιείται για χρήματα που έχουν εκδοθεί από Κεντρική Τράπεζα, όπως νομίσματα και τραπεζογραμμάτια. Στην περίπτωση των κρυπτονομισμάτων δεν ισχύει καμία από τις παραπάνω παραδοχές (ΕΚΤ, 2015).

Η αξία των εικονικών νομισμάτων αντικατοπτρίζεται από τις προσδοκίες για την αξία του στο μέλλον (Evans, 2014). Καθώς η χρήση τους περιορίζεται καθαρά σε επίπεδο συναλλαγών είναι δύσκολο να προβλεφθεί η αξία τους κάτι που έχει ως αποτέλεσμα έντονες διακυμάνσεις στην τιμή του. Παρόλο που οι διακυμάνσεις στην τιμή του δεν επηρεάζουν την διαδικασία ανταλλαγής και αποθήκευσης, καθιστούν δύσκολή την χρήση του ως συμβατικό νόμισμα λόγω της αστάθειας της συναλλαγματικής του αξίας (Evans 2014). Στο παρακάτω διάγραμμα φαίνεται οι διακυμάνσεις της τιμής του bitcoin από την 1η Απριλίου του 2017 εώς την 1η Απριλίου του 2018. Συγκεκριμένα η συναλλαγματική αξία του bitcoin την 25η Απριλίου του 2017 ήταν 1263,54$. Η αξία του έφτασε τα 19.343,04$ στις 16 Δεκεμβρίου του 2017. Σε διάστημα λίγο μεγαλύτερο των δύο μηνών και συγκεκριμένα στις 5 Φεβρουαρίου του 2017 η αξία του , έπεσε στα 6.914,26$ στην συνέχεια στις 5 Μαρτίου αξία του ανέρχονταν σε 11.432,98$ ενώ την 1η Απριλίου του 2018 η συναλλαγματική του αξία έπεσε στα 6.816,74$. Όπως είναι προφανές, η χρήση του ως νόμισμα θεωρείται εξαιρετικά δύσκολη λόγω των έντονων διακυμάνσεων. Οι αυξομειώσεις της συναλλαγματικής του αξίας δεν πτόησαν όμως αρκετές επιχειρήσεις από την αποδοχή εικονικών νομισμάτων (κατά κύριο λόγο του bitcoin). Μέσα σε αυτές συμπεριλαμβάνονται την εταιρία λογισμικού Microsoft (Vanian, 2018) και την γνωστή εταιρία ανάπτυξης παιχνιδιών και δημιουργό της πλατφόρμας Steam Valve, με την τελευταία ωστόσο να έχει αφαιρέσει το bitcoin ως μέσο συναλλαγών από τον Δεκέμβρη του 2017 (Dinkins, 2017).



Γράφημα 3.2: Το κόστος συναλλαγής στο Bitcoin (Coindesk, 2018)

Τα κόστη συναλλαγών είναι ένα ακόμη ζήτημα το οποίο θα πρέπει να αντιμετωπιστεί για την χρήση των εικονικών νομισμάτων ως συμβατικά. Στην περίπτωση του bitcoin από τον Απρίλη του 2017 εώς τον Απρίλη του 2018 παρατηρείται μία έντονη διακύμανση του μέσου κόστους συναλλαγής. Συγκεκριμένα την 25η Απριλίου του 2017 το μέσο κόστος συναλλαγής ήταν 1,059$. Στις 16 Δεκεμβρίου του 2017 το μέσο κόστος συναλλαγής είναι 26,893$ ενώ στις 22 του ίδιου μήνα άγγιξε τα 55,16$. Στις 5 Φεβρουαρίου 2018 έπεσε στα 6,193$ ενώ την 1η Απριλίου 2018 το μέσο κόστος κυμαίνονταν στα 0.925$. Παρατηρώντας τα δύο διαγράμματα φαίνεται ότι οι διακυμάνσεις του μέσου κόστους συναλλαγών ακολουθούν αυτές της τιμής του bitcoin.

Γράφημα 3.3: Κόστη συναλλαγής στο Bitcoin (Bitinfocharts, 2018)

3.4 Τα έξυπνα συμβόλαια

Ο Nick Szabo στις αρχές της δεκαετίας του ’90 παρατήρησε ότι οι ανθρώπινες κοινωνίες είναι δομημένες πάνω στην χρήση του χαρτιού. Στην καθημερινότητα τους οι άνθρωποι χρησιμοποιούν ως μέσο συναλλαγών (χρήματα, επιταγές κλπ) αλλά και ως μέσο επισημοποίησης των σχέσεων τους (γραπτοί νόμοι, κανόνες και φόρμες) το χαρτί. Το ίδιο ισχύει και σε επιχειρησιακό επίπεδο όπου το γραπτό συμβόλαιό θεωρείται ως βασικό μέσο επικύρωση συμφωνίας. Έχοντας περάσει σε μία εποχή όπου η επεξεργαστική ισχύς των υπολογιστών είναι ικανή να ανταπεξέλθει σε «απαιτητικούς» αλγόριθμους και τα δίκτυα ικανά να αποστέλλουν πιο γρήγορα και πιο περίπλοκα μηνύματα, είναι δυνατή η δημιουργία νέων πρωτόκολλων ικανών να αναδιαμορφώσουν το περιβάλλον και τα μέσα επίτευξης συμβάσεων (Szabo, 1997). Τα έξυπνα συμβόλαια είναι ένα παράδειγμα ενός τέτοιου πρωτόκολλου.

Η βασική ιδέα των έξυπνων συμβολαίων είναι η μετατροπή των συμβατικών ρητρών (όπως εγγυήσεις, δεσμεύσεις και δικαιώματα ιδιοκτησίας) σε κώδικα και η ενσωμάτωση τους στο υλικό και το λογισμικό που χρησιμοποιείται, πολλές φορές με τέτοιο τρόπο ώστε η αθέτηση της συμφωνίας να είναι αποτρεπτικά δαπανηρή για τον παραβάτη. Ο ίδιος ορίζει τα έξυπνα συμβόλαια ως ένα υπολογιστικό πρωτόκολλο συναλλαγών το οποίο είναι ικανό να εκτελεί τους όρους του συμβολαίου (Szabo, 1994). Οι γενικοί στόχοι ενός έξυπνου συμβολαίου είναι να ικανοποιηθούν οι κοινές συνθήκες του συμβολαίου (όπως οι όροι πληρωμής, οι δεσμεύσεις, η εμπιστευτικότητα αλλά και η επιβολή) περιορίζοντας τις πιθανότητες λαθών αλλά και της ανάγκης ύπαρξης εμπιστοσύνης μεταξύ των συμβαλλόμενων. Από οικονομικής άποψης συμβάλλουν στην μείωση των περιπτώσεων απάτης, και του κόστους από την παρακολούθηση και επιβολή των συμβολαίων.

Μία πρώιμη μορφή των έξυπνων συμβολαίων θα μπορούσε να θεωρηθεί το μηχάνημα αυτόματης πώλησης (δυνατότητα χρήσης από όποιο διαθέτει νομίσματα με μηχανισμούς προστασίας όπως το χρηματοκιβώτιο για την προστασία από επιθέσεις) αλλά και τεχνολογίες όπως τα μηχανήματα POS, οι πιστωτικές/χρεωστικές κάρτες και συστήματα ηλεκτρονικών συναλλαγών δεδομένων (Electronic data interchange) (Szabo, 1994). Ως συστήματα ηλεκτρονικών συναλλαγών δεδομένων ορίζονται τα δια-οργανωσιακά συστήματα συνεργασίας τα οποία επιτρέπουν στους συμμετέχοντες την ανταλλαγή δομημένων επιχειρησιακών πληροφοριών μεταξύ υπολογιστικών εφαρμογών (Swatman και Swatman, 1992).

3.5.1 Τα έξυπνα συμβόλαια και το blockchain – Η περίπτωση του Ethereum

Ο Nick Szabo (1998) ανέφερε στο «Secure Property Titles with Owner Authority» την δημιουργία μεταφερόμενων δικαιωμάτων ιδιοκτησίας μέσα σε ένα κατανεμημένο δίκτυο (ή όπως αναφέρει μέσω της τεχνολογίας επαναλαμβανόμενης βάσης δεδομένων) ωστόσο δεν υπήρχε κάποιο σύστημα αντιγραφόμενης βάσης δεδομένων στο οποίο θα μπορούσε να εφαρμοστεί. Αν και από το 2011 δημιουργήθηκαν τα πρώτα πρωτόκολλα που χρησιμοποιούσαν το blockchain του bitcoin για την δημιουργία εφαρμογών πάνω σε αυτό όπως το Namecoin, η γλώσσα προγραμματισμού script του Bitcoin δεν είναι Turing-complete με αποτέλεσμα να μην να καλύψει ένα μεγάλο εύρος εφαρμογών.

Ο Vitalik Buterin (2014) βλέποντας αυτή την τεχνική «αδυναμία» δημιούργησε ένα νέο πρωτόκολλο το Ethereum. Πρόκειται για ένα blockchain σύστημα το οποίο περιείχε μια νέα Turing complete γλώσσα προγραμματισμού (που μπορεί δηλαδή να εκτελέσει κάθε πιθανό υπολογιστικό πρόβλημα), την Solidity, που επιτρέπει την δημιουργία εφαρμογών μέσα στο blockchain. Τα έξυπνα συμβόλαια περιγράφονται από τον Buterin ως κρυπτογραφικα «κουτία» τα οποία περιέχουν αξία και «ξεκλειδώνονται» μόνο όταν ισχύουν οι συνθήκες του συμβολαίου.

3.5.2 Η ανάλυση του Ethereum

Στην περίπτωση του Ethereum ύπαρχουν δύο ήδη λογαριασμών. Η πρώτη αφορά τις περιπτώσεις των λογαριασμών που ελέγχονται από ιδιωτικά κλειδιά, δηλαδή από χρήστες, όπως και στην περίπτωση του Bitcoin. Η δεύτερη αφορά τους λογαριασμούς των συμβολαίων τα οποία διαχειρίζονται μέσα από τον κώδικα του συμβολαίου. Όπως αναφέρει ο Buterin (2014) ένας λογαριασμός του Ethereum μπορεί να περιέχει τα εξής 4 στοχεία:

1. Ένα αριθμό (nonce), που λειτουργεί ως μετρητής έτσι ώστε κάθε συναλλαγή να γίνεται μόνο μία φορά
2. Το ισοζύγιο του λογαριασμού σε ether
3. Ο κώδικας του συμβολαίου του λογαριασμού (αν υπάρχει)
4. Ο χώρος αποθήκευσης δεδομένων του λογαριασμού (άδειο εξ ορισμού)

Το εικονικό νόμισμα Ether λειτουργεί ως «καύσιμο» και χρησιμοποιείται ως αμοιβή για την επίτευξη των συναλλαγών όπως συμβαίνει και στην περίπτωση του Bitcoin. Η βασική του διαφορά με το bitcoin είναι πως μία συναλλαγή ή η δημιουργία

ενός νέου συμβολαίου μπορεί να γίνει όχι μόνο μέσω εξωτερικών λογαριασμών που διαχειρίζονται οι χρήστες αλλά και μέσω των εσωτερικών λογαριασμών των έξυπνων συμβολαίων. Επιπλέον, υπάρχει ξεχωριστή επιλογή, μία συναλλαγή μπορεί να περιέχει δεδομένα ενώ στην περίπτωση που ο αποδέκτης είναι λογαριασμός συμβολαίου, υπάρχει δυνατότητα απάντησης.

Τα δεδομένα που περιέχει μια συναλλαγή του Ethereum περιέχει τον αποδέκτη της συναλλαγής την ψηφιακή του υπογραφή για την αναγνώριση, το πόσο που θέλει ο αποστολέας να στείλει και δύο τιμές, το «STARTGAS» και το «GASPRICE». Για να αποφευχθεί η περίπτωση ατέρμονος κύκλου στο κώδικα, σε κάθε συναλλαγή απαιτείται ο ορισμός ενός ορίου σε ether για υπολογιστικά βήματα που απαιτούνται για την εκτέλεση του κώδικα του συμβολαίου που υπάρχει μέσα στην συναλλαγή αλλά και των πιθανών συναλλαγών που είναι πιθανό να γίνουν κατά την εκτέλεση του κώδικα. Το όριο αυτό είναι το «STARTGAS» και το «GASPRICE» είναι η ανταμοιβή σε ether που δίνεται στον miner για κάθε υπολογιστικό βήμα που εκτελεί. Αν κατά τη διάρκεια της συναλλαγής, ξεπεραστεί το όριο που είχε οριστεί από τον αποστολέα, η συναλλαγή ακυρώνεται, ο miner κρατάει την τιμή «STARTGAS» που έχει ορίσει σε ether ενώ αντίθετα στην περίπτωση που χρησιμοποιηθεί χαμηλότερο ποσό το υπόλοιπο επιστρέφεται στον αποστολέα.

Η διαδικασία που ακολουθείται για την επίτευξη μιας συναλλαγής είναι:

1. Έλεγχος της ορθότητας της συναλλαγής (δηλαδή ότι οι τιμές startgas και gasprice είναι σωστά ορισμένες) και η υπογραφή του αποστολέα είναι έγκυρη και ο μετρητής (nonce) ταιριάζει με αυτό του αποστολέα (αν όχι επιστρέφει σφάλμα)
2. Υπολογίζει το κόστος της συναλλαγής ως STARTGAS * GASPRICE(=X Ether), αφαιρεί την αμοιβή του miner από τον λογαριασμό του αποστολέα και στην συνέχεια αυξάνει τον μετρητή (αν δεν υπάρχει το πόσο που αντιστοιχεί στο κόστος επιστρέφει σφάλμα). Από το STARTGAS αφαιρεί ένα συγκεκριμένο ποσό για κάθε byte μέσα σε αυτή
3. Αποστολή του ποσού στον λογαριασμό του παραλήπτη. Αν δεν υπάρχει ο λογαριασμός, δημιουργείται ένας. Αν ο λογαριασμός του παραλήπτη είναι ένα έξυπνο συμβόλαιο, τότε τρέχει το έξυπνο συμβόλαιο μέχρι την ολοκλήρωσή του ή μέχρι να τελειώσει η τιμή STARTGAS.

4. Σε περίπτωση που η συναλλαγή δεν επιτευχθεί επειδή ο αποστολέας έχει θέσει μικρότερο ποσό ως κόστος συναλλαγής(=STARTGAS * GASPRICE) από το απαιτούμενο για την εκτέλεση του κώδικα τότε το ποσό της συναλλαγής παραμένει στο λογαριασμό του αποστολέα ενώ αντίθετα το ποσό που ορίζεται ως κόστος συναλλαγής μεταφέρεται στο λογαριασμό του miner.

Τα συμβόλαια εκτελούνται σε μία «εικονική» μηχανή του Ethereum (Ethereum Virtual Machine ή EVM). Το EVM αποτελείται από όλους τους χρήστες/κόμβους που συμμετέχουν στο Ethereum δηλαδή κάθε κόμβος έχει μία υλοποίηση του EVM. Βέβαια, όπως και στην περίπτωση του Bitcoin, σε ορισμένες περιπτώσεις οι πόροι των συσκευών που τρέχουν τους κόμβους είναι περιορισμένοι. Επομένως δεν συμμετέχουν στη διαδικασία της εκτέλεσης των συμβολαίων παρά μόνο αν συμμετέχουν στην διαδικασία του mining. Ως σύστημα συναίνεσης των κόμβων, χρησιμοποιείται και στην περίπτωση του Ethereum το Proof-of-Work όπως και στην περίπτωση του Bitcoin.

3.5.2.1 Αποκεντρωμένες εφαρμογές (Dapps) στην πλταφόρμα του Ethereum

Ως αποκεντρωμένες εφαρμογές θεωρούνται όλες οι εφαρμογές που χρησιμοποιούν τη μια blockchain πλατφόρμα για την σύνδεση των συναλλασσόμενων. Ο Buterin (2014) διαχωρίζει τις αποκεντρωμένες εφαρμογές σε τρεις κατηγορίες. Η πρώτη αφορά την διαχείριση και τις συναλλαγές νομισμάτων και γενικότερα χρηματοοικονομικών παράγωγων (μετοχές, ομόλογα, και αλλά συμβόλαια μελλοντικής εκπλήρωσης). Παράλληλα δίνει την δυνατότητα της δημιουργίας «υπό-νομισμάτων» (sub-currencies) γνωστά ως «κουπόνια» (tokens) τα οποία μπορεί να αποτυπώνουν ψηφιακά κάθε είδους περιουσιακό στοιχείο. Όπως αναφέρει ο ίδιος το Bitcoin θα μπορούσε να είναι μία εφαρμογή υλοποιημένη πάνω στην πλατφόρμα του Ethereum. Η δεύτερη κατηγορία αφορά συμβολαιακές σχέσεις που δεν είναι εγγενώς μονεταριστικές όπως συμβόλαια ιδιοκτησίας, συμβόλαια ενοικιάσεις κ.α.. Η τρίτη κατηγορία αφορά εφαρμογές που δεν σχετίζονται με τον χρηματοπιστωτικό τομέα όπως διαδικασίες ψηφοφορίας και διαδικασίες αποκεντρωμένης διοίκησης. Σε αυτή την κατηγορίας εντάσσονται οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (Decentralized Autonomous Organisations) (Buterin 2014).

3.5.2.2 Αρχική Προσφορά Κουπονιών (Initial Coin Offering)

Η αρχική δημόσια προσφορά κουπονιών είναι μια διαδικασία προπώλησης των κουπονιών των εφαρμογών σε blockchain πλατφόρμες. Με αυτό τον τρόπο βρίσκουν το κεφάλαιο για την χρηματοδότηση των εφαρμογών τους, προσφέροντας «κουπόνια» τα οποία επιτρέπουν την χρήση της εφαρμογής όταν αυτή ξεκινήσει την λειτουργία της. Η συγκεκριμένη διαδικασία θυμίζει αρκετά αυτή του crowdfunding. Το crowdfunding είναι μια υπηρεσία που έρχεται να καλύψει το «χρηματοδοτικό κενό» που δημιουργήθηκε μετά την κρίση και εμποδίζει τις μικρομεσαίες επιχειρήσεις και αρκετές start-up επιχειρήσεις να έχουν πρόσβαση σε χρηματοδότηση. Πρόκειται για μία καινοτόμο μέθοδο για τη χρηματοδότηση νέων επιχειρήσεων, επιτρέποντας στους επιχειρηματίες να ζητήσουν χρηματοδότησή από πολλούς ιδιώτες, για την δημιουργία προϊόντων ή την επίτευξη των επιχειρηματικών σχεδίων τους, με αντάλλαγμα τη προσφορά του προϊόντος όταν ολοκληρωθεί ή ενός ποσοστού ιδιοκτησίας. Τα είδη των επιχειρηματικών σχεδίων μπορεί να διαφέρει τόσο σε στόχους όσο και σε ένταση επένδυσης (Schwienbacher και Larralde, 2010).

3.5.2.3 Αποκεντρωμένοι Αυτόνομοι Οργανισμοί (Decentralized Autonomous Organisations)

Οι Αποκεντρωμένοι Αυτόνομοι Οργανισμοί είναι ψηφιακές οντότητες των οποίων οι λειτουργίες της καθορίζονται αποκεντρωμένα από τους χρήστες της μέσα μία από blockhain πλατφόρμα. Συγκεκριμένα οι χρήστες της πλατφόρμας έχουν την δυνατότητα, μέσω των «κουπονιών» που διαθέτουν, να καθορίσουν τις λειτουργίες του οργανισμού (Χρηστίδης και Δεβετσικιώτης, 2016).

Η πιο γνωστή περίπτωση DAO, είναι αυτή του «The DAO». Πρόκειται για μία εφαρμογή πάνω στην πλατφόρμα του Ethereum η οποία επέτρεπε στους κατόχους του DAO «κουπονιού» να ψηφίσουν που θα επενδυθούν τα κεφάλαια που συλλέχθηκαν από το την πώληση των «κουπονιών». Συγκεκριμένα, κατάφερε να συλλέξει 10.7 Eth (το νόμισμα του Ethereum) που αντιστοιχούσε εκείνη την περίοδο σε 120 εκατομμύρια δολάρια. Εφόσον η πλειοψηφία συμφωνούσε ως προς τη πρόταση της επένδυσης, μέσω των έξυπνων συμβολαίων, γίνονται οι απαραίτητες διαδικασίες για την επένδυση (Waters, 2016). Ωστόσο, ένα λάθος (bug) στο έξυπνο συμβόλαιο της εφαρμογής επέτρεψε σε κάποιον χρήστη/επιτιθέμενο να πάρει στην κατοχή του ένα μεγάλο ποσό Ether της εφαρμογής. Για να αντιμετωπιστεί η συγκεκριμένη κατάσταση αποφασίστηκε ύστερα από ψηφοφορία των κατόχων κρυπτονομισμάτων του Ethereum

να επιστραφούν τα χρήματα που χάθηκαν σε ένα λογαριασμό το έξυπνο συμβόλαιο του οποίου ο οποίος θα επέτρεπε μόνο στους πραγματικούς ιδιοκτήτες των «κουπονιών» DAO να πάρουν τα πόσο που είχαν επενδύσει πίσω σε κρυπτονομίσματα του Ethereum. Ωστόσο, η συγκεκριμένη διαδικασία βρήκε ένα μεγάλο ποσοστό της κοινότητας του Ethereum αντίθετη κάτι που οδήγησε στο διάσπαση του Ethereum blockchain σε δύο ενεργά blockchain, το Ethereum και το Ethereum Classic (Hertig, 2016). Η συγκεκριμένη διαδικασία ονομάζεται «Hard Fork».

3.5 Η Διακυβέρνηση των Blockchain δικτύων

Αν και η λειτουργία ενός Blockchain δικτύου δεν απαιτεί κάποια κεντρική διαχείριση ωστόσο η εξέλιξη και η συντήρηση και η διευθέτηση προβλημάτων του λογισμικού απαιτεί την συμμετοχή των ανθρώπινου παράγοντα. Στην περίπτωση του Bitcoin ο Satoshi Nakamoto παρέδωσε την διαχείριση του δικτύου στον προγραμματιστή Gavin Andersen. Αν και θεωρητικά η εξέλιξη εγχειρήματος, όπως σε όλα τα εγχειρήματα ανοιχτού κώδικα, στηρίζονται στο καθένα που θέλει να συμμετέχει στην εξέλιξή του. Ωστόσο μία ομάδα προγραμματιστών ορισμένη από τον Andersen πρέπει να αποδεχτεί αυτές τις αλλαγές για να ενσωματωθούν στην πλατφόρμα του Bitcoin. Οι συγκεκριμένοι προγραμματιστές ανήκουν στο Ίδρυμα του Bitcoin, ένα μη κερδοσκοπικό οργανισμό που στηρίζουν την λειτουργία του δικτύου. Το ίδιο ισχύει και για την περίπτωση του Ethereum με το Ethereum Foundation. Σε ότι αφορά τις αλλαγές στο δίκτυο, αυτές πρέπει να αποδεχθούν από τους κόμβους που συμμετέχουν στην διαδικασία του mining (Lehdonvirta, 2016). Σε αντίθετη περίπτωση, δηλαδή αν ένα ποσοστό δεν αποδεχτεί τις αλλαγές και συνεχίσει να λειτουργεί ως διαχωρισμένο δίκτυο δημιουργεί μία νέα πλατφόρμα blockchain. Η συγκεκριμένη διαδικασία ονομάζεται «hard fork». Στην περίπτωση του Bitcoin η συγκεκριμένη διαδικασία έχει συμβεί πολλές φορές δημιουργώντας νέα κρυπτονομίσματα με το πιο γνωστό από αυτά είναι το Bitcoin Cash. Όπως είναι προφανές, στην εξέλιξη των πρωτόκολλών των κρυπτονομισμάτων παίζουν σημαντικό ρόλο οι miners. Σύμφωνα με τους Hileman & Rauchs (2017) πάνω από το 51% miners θεωρούν ότι η επιρροή στην εξέλιξη των κρυπτονομισμάτων είναι υψηλή έως πολύ υψηλή.

3.7 Ομάδες mining (Mining Pools)

Όπως αναλύθηκε στις προηγούμενες ενότητες η διαδικασία του Proof-of-Work απαιτεί τους υπολογιστικούς πόρους των κόμβων οι οποίοι πρέπει να υπολογίσουν το

«πρόβλημα» του proof-of-work. Για την αύξηση της ταχύτητας του υπολογισμού της κατακερματισμένης ακολουθίας, πολλοί κόμβοι «ενώνουν» τους υπολογιστικούς τους πόρους κάτι που αυξάνει την πιθανότητα επίλυσης του προβλήματός. Οι ομάδες αυτές ονομάζονται mining pools (Hileman & Rauchs 2017).

3.8 Ανταλλακτήρια εικονικών νομισμάτων (Cryptocurrency exchanges)

Τα ανταλλακτήρια είναι οργανισμοί που επιτρέπουν την μετατροπή των συμβατικών νομισμάτων σε κρυπτονομίσματα. Πρόκειται για εταιρίες που δεν συνδέονται άμεσα με την τεχνολογία του Blockchain αλλά για εταιρίες που λειτουργούν ως συνδετικοί κρίκοι για την συμμετοχή των χρηστών στο blockchain καθώς είναι ο μόνος νόμιμος τρόπος για την συμμετοχή νέων χρηστών σε blockchain πλατφόρμες όπως αυτές του Bitcoin και του Ethereum. Για την χρήση των υπηρεσιών των ανταλλακτηρίων απαιτείται, σε κάποιες περιπτώσεις, η διαδικασία αναγνώρισης των χρηστών «Know Your Customer» (KYC). Ένα από τα πιο γνωστά ανταλλακτήρια κρυπτονομισμάτων είναι το Coinbase.

3.9 Κατηγοριοποίηση της τεχνολογίας

Στις ενότητες περιγράφεται η τεχνολογία του κατανεμημένου κατάστιχου (ή αλλιώς γνωστού και ως τεχνολογίας του blockchain. Οι περιπτώσεις που μελετήθηκαν για την κατανόηση της τεχνολογίας ήταν αυτές του Bitcoin και του Ethereum. Οι δυο περιπτώσεις αφορούν p2p δίκτυα στα οποία ο καθένας μπορεί να συμμετέχει σε όλες τις 4 βασικές διαδικασίες του δικτύου που αναφέρει ο Αντωνόπουλος (2016), δηλαδή την αποθήκευση και την μεταφορά νομισμάτων (wallet), την διατήρηση ενός αντιγράφου του blockchain (full blockchain), την διαδικασία της προσθήκης νέων συναλλαγών (miner), και την διαδικασία μεταφοράς πληροφοριών μεταξύ των χρηστών/κόμβων (network routing). Η λειτουργία τους βασίζεται στους συμμετέχοντες χωρίς να περιορίζει την συμμετοχή στις παραπάνω διαδικασίες σε κάποια ομάδα χρηστών όπως και η εξέλιξή του πρωτόκολλού τους. Ωστόσο υπάρχουν διαφορετικές υλοποιήσεις οι οποίες χρησιμοποιούν τη συγκεκριμένη τεχνολογία δίνοντας διαφορετικά δικαιώματα σε κάθε χρήστη ή περιορίζουν τον αριθμό των συμμετεχόντων. Στην συνέχεια αναλύονται οι βασικές κατηγορίες της τεχνολογίας του blockchain.

3.9.1 Blockchain με ή χωρίς άδεια, Ιδιωτικό ή Δημόσιο (permissionless ή permissioned blockchain, private ή public)

Η διαφορετικές εφαρμογές της τεχνολογίας που αναφέρθηκαν διαχωρίζουν την τεχνολογία σε δύο κατηγορίες. Η πρώτη αφορά τις περιπτώσεις των εφαρμογών blockchain (ή κατανεμημένων κατάστιχών) που ο καθένας μπορεί να συμμετέχει σε όλες τις διεργασίες μέσα σε αυτό και παράλληλα να συμβάλλει στην εξέλιξη του αν το επιθυμεί (δεν έχουν δηλαδή συγκεκριμένο ιδιοκτήτη αλλά προωθούνται και στηρίζοναι από μη κερδοσκοπικά Ιδρύματα όπως το Bitcoin και το Ethereum Foundation) (Walport, 2015; Athanassiou, 2017). Η περίπτωση αυτή είναι γνωστή ως «μη αδειοδοτούμενα blockchain » (permissionless blockchain). Σε αυτή την κατηγορία ανήκουν το Bitcoin και το Ethereum.

Η δεύτερη περίπτωση αφορά εφαρμογές blockchain όπου οι χρήστες δεν έχουν τις ίδιες ιδιότητες μέσα στο δίκτυο. Στην περίπτωση του δικτύου του Ripple που θα αναλυθεί στην συνέχεια, οι κόμβοι που διαχειρίζονται την επικύρωση των συναλλαγών και την μεγέθυνση του κατανεμημένου κατάστιχου είναι συγκεκριμένοι και ορισμένοι από τους ιδιοκτήτες οι οποίοι είναι υπεύθυνοι για την εξέλιξη και την λειτουργία του. Οι συγκεκριμένες υλοποιήσεις όπου εφαρμόζουν αυτές τις πρακτικές είναι γνωστές ως αδείοδοτούμενα blockchain (permissioned blockhain) (Walport, 2015; Athanassiou, 2017). Ο Buterin (2015) τις διαχωρίζει ως blockchain κοινοπραξίας (consortium blockchains)

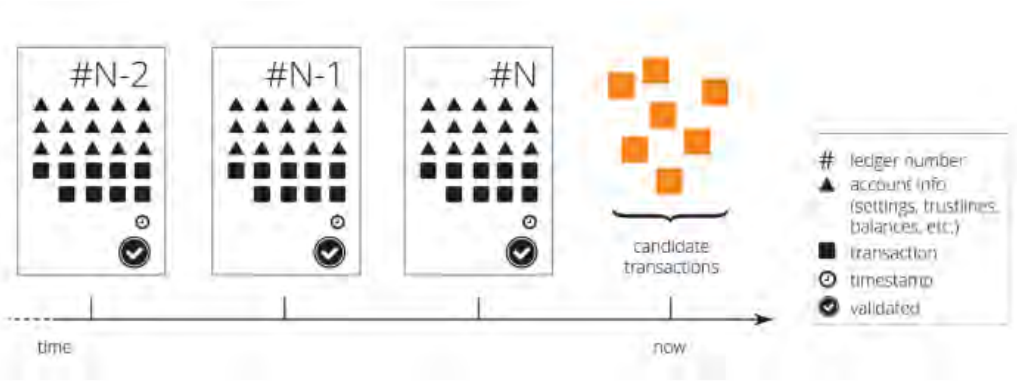
Το έντονο ενδιαφέρον αρκετών εταιριών (όπως η IBM) για την τεχνολογία του blockchain οδήγησε αρκετές από αυτές να αναπτύξουν δικές τους υλοποιήσεις κατανεμημένου κατάστιχου. Πρόκειται για «δομές» (frameworks), οι οποίες στοχεύουν στην υλοποίηση ιδιωτικών δικτύων. Τα συγκεκριμένα δίκτυα διαχειρίζονται αποκλειστικά από την επιχείρηση ή τις επιχειρήσεις που το υλοποιούν. Το ίδιο ισχύει και τις διαδικασίες επικύρωσης. Ωστόσο, η βασικότερη διαφορά με τις υλοποιήσεις στις δύο προηγούμενες υποκατηγορίες που αναφέρθηκαν, είναι ότι για την συμμετοχή στο δίκτυο είναι ελεγχόμενη από τον «ιδιοκτήτη» του δικτύου (Buterin, 2015). Η πιλοτική υλοποίηση Ubin ανήκει σε αυτή την κατηγορία ενώ οι δομές που χρησιμοποιούνται σε τέτοιες περιπτώσεις είναι το Corda της R3, το Hyperledger Fabric του Linux Foundation και το Quorum της J.P. Morgan.

3.9.1.1 Η περίπτωση της Ripple ως ένα public permissioned blockchain

Η Ripple είναι η πρώτη εταιρία που δημιούργησε αυτή τη κατηγορία του δικτύου δημιουργώντας ένα νέο επιχειρηματικό μοντέλο για την αξιοποίηση της τεχνολογίας του blockchain. Η Ripple παρέχει υπηρεσίες διακανονισμού σε συνεχή χρόνο (real time gross settlement) μέσα από μία κατανεμημένη πλατφόρμα πληρωμών. Το εικονικό νόμισμα της πλατφόρμας είναι το XRP (Schwartz et al, 2014). Πρόκειται για μία έτοιμη προς χρήση πλατφόρμα, δεν περιορίζει τον αριθμό των χρηστών ωστόσο οι διαδικασία επικύρωσης γίνεται μονό από εγκεκριμένους κόμβους.

Η Ripple επιτρέπει τις συναλλαγές, πέρα από το εικονικό νόμισμα XRP, οποιοδήποτε άλλου εικονικού ή συμβατικού νομίσματος μέσα στο δίκτυο της Ripple. Για να επιτευχθεί αυτό ορίζονται από το Ripple οργανισμοί (όπως χρηματοπιστωτικά ιδρύματα και πάροχοι υπηρεσιών πληρωμών) ως πύλες (gateways) για την έκδοση του αντίστοιχου ψηφιακού στοιχείου για την απεικόνισή τους μέσα στο δίκτυο. Για την συναλλαγές περιουσιακών στοιχειών πέρα του εικονικού νομίσματος XRP δημιουργούνται γραμμές εμπιστοσύνης (trust lines) μεταξύ των πυλών.

Η δομή ενός block (η εταιρία Ripple το ονομάζει ledger) στο δίκτυο του Ripple δεν διαφέρει ιδιαίτερα από αυτή των Bitcoin και Ethereum. Συγκεκριμένα ένα ledger αποτελείται από ένα αριθμό που λειτουργεί ως επικεφαλίδα μέσα στο δίκτυο, στοιχεία που αφορούν τους λογαριασμούς (όπως το υπόλοιπο), το σύνολο των συναλλαγών που περιέχει και την ώρα και ημερομηνία της χρονικής αποτύπωσης (Cohen και άλλοι, 2014).

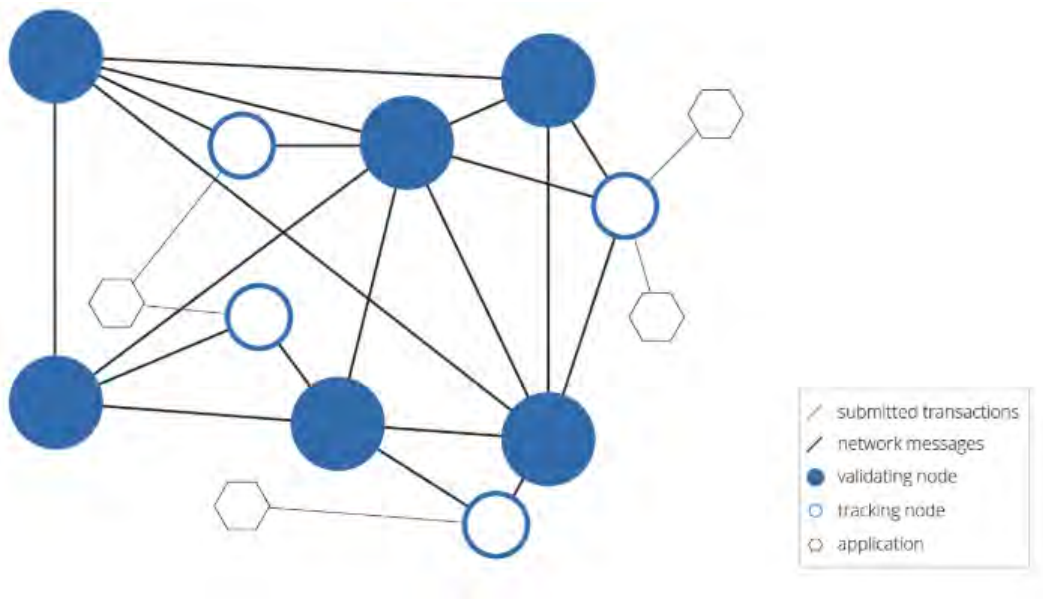


Σχήμα 3.9: Δομικά στοιχεία ενός block του Ripple (Cohen και άλλοι, 2014)

Η διαφορά έγκειται στον τρόπο που καταγράφονται οι συναλλαγές μέσα στο δίκτυο αλλά και στο σύστημα συναίνεσης που εφαρμόζεται και της επιτρέπει την

διεκπεραίωση των συναλλαγών μέσα σε 4 δευτερόλεπτα. Το δίκτυο της Ripple έχει τρία είδη συμμετεχόντων μέσα στο δίκτυο της. Η πρώτη κατηγορία είναι οι αποκεντρωμένοι εξυπηρετητές που ονομάζονται κόμβοι επικύρωσης και είναι υπεύθυνοι να δέχονται και προωθούν τις συναλλαγές. Η δεύτερη κατηγορία αφορά τους χρήστες που πραγματοποιούν τις συναλλαγές. Σε αυτή την κατηγορία ανήκουν τα ηλεκτρονικά πορτοφόλια, χρηματοπιστωτικά ιδρύματα που συνεργάζονται με την Ripple και διαδικτυακές πλατφόρμες συναλλαγών. Η τρίτη ομάδα συμμετεχόντων είναι οι κόμβοι παρακολούθησης. Πρόκειται για τους για «ενδιαμέσους» μεταξύ των κόμβων επικύρωσης και των χρηστών στέλνοντας τις νέες συναλλαγές από τους χρήστες στο κόμβους επικύρωσης. Οι κόμβοι παρακολούθησης είναι επιπλέον υπεύθυνοι για τις ίδιες διαδικασίες με αυτές των κόμβων επικύρωσης εκτός από την διαδικασία επικύρωσης, δηλαδή την προώθηση και την αναμετάδοση των συναλλαγών εκτός από την διαδικασία της επικύρωσης (Cohen et al, 2014). Για τους κόμβους επικύρωσης η Ripple έχει αναθέσει την λειτουργία τους σε πάνω από 50 ινστιτούτα και επιχειρήσεις. Σε αυτές συμπεριλαμβάνονται η Microsoft, το MIT, η CGI, η WorldLink, το Telindus-Proximus Group, η Swedish ISP, η Bahnhof και η AT TOKYO Corporation (del Castillo, 2017). Όπως γίνεται κατανοητό στην διαδικασία των επικυρώσεων δεν μπορεί να συμμετέχει ο καθένας, όπως συμβαίνει με τις περιπτώσεις των Bitcoin και Ethereum αλλά μόνο με την συγκατάθεση της Ripple.

Σημαντική παρατήρηση είναι ότι οι κόμβοι επικύρωσης δεν ανταμείβονται με νέα XRP. Η Ripple δημιούργησε 100 δισεκατομμύρια XRP από την αρχή της λειτουργίας της πλατφόρμας εκ των οποίων πλέον κατέχει 7,114,004,047. Στην αγορά βρίσκονται 39,178,259,468 και τα υπόλοιπα 53,700,000,024 η Ripple τα τοποθέτησε σε ένα κρυπτογραφικά προστατευμένο καταπιστευτικό λογαριασμό (escrow account). Με αυτό τον τρόπο, όπως αναφέρει η ίδια, επιτρέπει στους ενδιαφερόμενους να υπολογίζουν τη μέγιστη προσφορά μέσα στο δίκτυο (XRP Market Performance, 2018). Καθώς δεν υπάρχει οικονομικό κίνητρο κατά την διαδικασία επικύρωσης, δεν είναι σαφές ποιο είναι το κίνητρο των συγκεκριμένων κόμβων επικύρωσης για την συμμετοχή τους στο δίκτυο.



Σχήμα 3.10: Το δίκτυο του Ripple (Cohen και άλλοι, 2014)

Το σύστημα συναίνεσης διαφέρει από αυτά των δύο περιπτώσεων που αναλύθηκαν. Η βασική διαφορά είναι η αδυναμία συμμετοχής ως κόμβοι επικύρωσης χωρίς την συγκατάθεση της Ripple. Αν και η ύπαρξη εγκεκριμένων κόμβων επικύρωσης έρχεται σε αντίθεση με την αρχική ιδέα του Nakamoto (2009) για την δημιουργία μιας πλατφόρμας που δεν απαιτείται εμπιστοσύνη για την επίτευξη των συναλλαγών. Ωστόσο αυτό διευκολύνει αρκετά την επίτευξης συναίνεσης μεταξύ των κόμβων. Οι Schwartz κ.α (2014; Cohen κ.α., 2014) αναφέρουν ότι ο αλγόριθμος της συναίνεσης εφαρμόζεται κάθε λίγα δευτερόλεπτα σε κάθε κόμβο και περιγράφουν την διαδικασία στα εξής βήματα.

1. Κάθε κόμβος επικύρωσης και παρακολούθησης δέχεται ως σημείο εκκίνησης το τελευταίο ledger που έχει αποδεχτεί το δίκτυο. Κάθε κόμβος επικύρωσης και παρακολούθησης επεξεργάζεται μια ομάδα συναλλαγών ελέγχοντας την εγκυρότητά τους (σε αυτές μπορεί να περιέχονται νέες ή προηγούμενες συναλλαγές που έχουν απορριφθεί). Σε περίπτωση που είναι έγκυρες, τις μεταδίδει στους υπόλοιπους κόμβους ως υποψήφιο σετ.

2. Στην συνέχεια, κάθε κόμβος ελέγχει τις τελικές ομάδες που προτείνουν μόνο οι κόμβοι επικύρωσης. Οι συναλλαγές που έχουν το μεγαλύτερο αριθμό αποδοχών από το σύνολο των κόμβων περνάνε στην επόμενη φάση.

3. Οι συναλλαγές που προκρίθηκαν ελέγχονται από τους κόμβους επικύρωσης. Αν έχουν αποδοχή μεγαλύτερη του 80% εισάγονται στο νέο ledger το οποίο συνδέεται με τα υπόλοιπα και αποστέλλεται σε όλους τους κόμβους. Οι υπόλοιπες συναλλαγές που δεν προκρίθηκαν είτε απορρίπτονται είτε παραμένουν να ενταχθούν στο νέο ledger.

Για την αποφυγή της υπερβολικής μεγέθυνσης του blockchain και της κακόβουλης χρήσης του, η Ripple έχει θέσει ένα ελάχιστο ποσό που θα πρέπει να υπάρχει σε κάθε λογαριασμό για την δημιουργία και την χρήση του. Το ποσό ορίζεται στα 20 XRP (Reserves, 2018). Παράλληλα σε κάθε συναλλαγή υπάρχει ένα ποσό που δαπανά ο αποστολέας και ορίζεται ως κόστος συναλλαγής. Το ποσό ορίζεται στα 0.00001 XRP. Το ποσό αυτό δεν δίνεται ως αντίτιμο σε άλλους κόμβους αλλά καταστρέφεται (Transaction Cost, 2018).

3.9.2 Περιπτώσεις δομών private blockchain

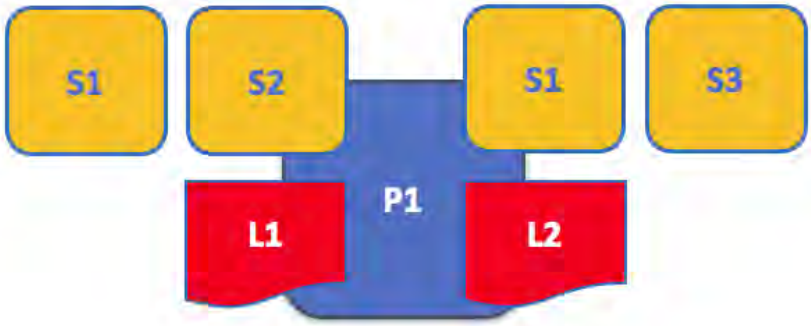
Σε αυτή την κατηγορία θα αναλυθούν οι δομές των τριών περιπτώσεων που προαναφέρθηκαν, δηλαδή του Hyperledger Fabric, του Corda και του Quorum.

3.9.2.1 Η περίπτωση του Hyperledger Fabric

Το ίδρυμα Linux τον Δεκέμβρη του 2015 δημιούργησε ένα διακλαδικό Blockchain πρόγραμμα ανοιχτού κώδικα. Σε αυτό το πρόγραμμα αναπτύσσονται διαφορετικές «δομές» (frameworks) βασισμένες στην τεχνολογία του Blockchain και τα αντίστοιχα εργαλεία για την χρήση τους. Συγκεκριμένα το πρόγραμμα, αποτελείται από 5 προσαρμοζόμενες «δομές» κατανεμημένου κατάστιχου (Indy, Fabric, Burrow, Iroha και Sawtooth) οι οποίες στοχεύουν στην κάλυψη των διαφορετικών αναγκών των επιχειρήσεων. Από αυτές η πιο διαδεδομένη είναι η Hyperleger Fabric. Στο πρόγραμμα συμμετέχουν διάφορες εταιρίες και χρηματοπιστωτικά ιδρύματα. Σε αυτές περιλαμβάνονται η IBM, η Intel, η J.P. Morgan, η Accenture, η Deutsche Bank και η American Express (Hyperledger, 2017).

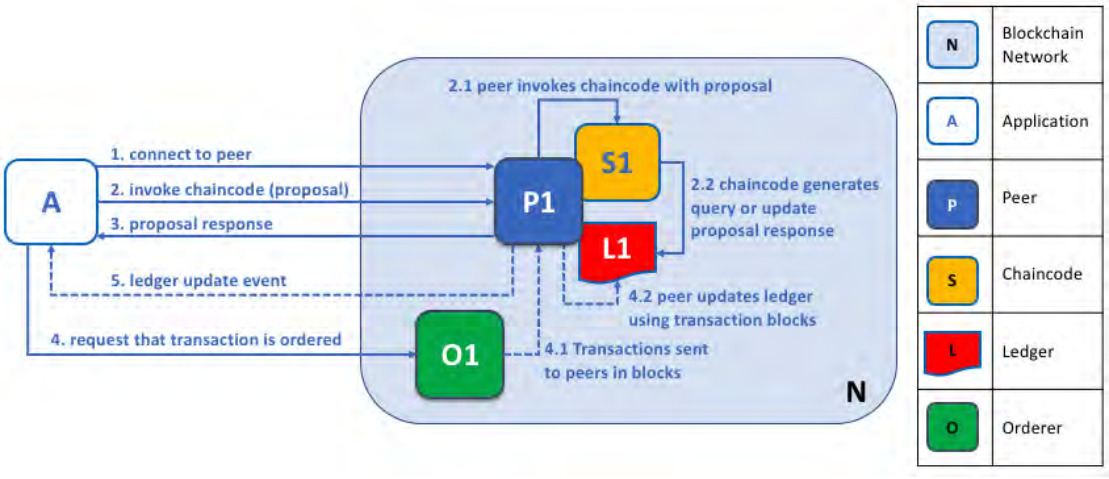
Το Hyperedger Fabric είναι μια πλατφόρμα που αναπτύχθηκε από την IBM και την Digital Asset. Η βασική διαφορά σε σχέση με τις πλατφόρμες που αναλύθηκαν είναι ότι η υλοποίηση τους γίνεται από τον οργανισμό ή τους οργανισμούς που το χρησιμοποιούν σε κάθε περίπτωση. Πρόκειται για μια «δομή» που υποστηρίζει την χρήση έξυπνων συμβολαίων (η ίδια το ονομάζει chaincode) και μπορεί να αναπαρασταθεί μέσα σε αυτό οποιαδήποτε μορφή υλικού ή άυλου περιουσιακού στοιχείου απεικονίζοντάς το με μία αυθαίρετη τιμή (Hyperleger Fabric, 2017).

Ένα δίκτυο βασισμένο στην αρχιτεκτονική του Hyperleger Fabric αποτελείται από κόμβους οι οποίοι χρησιμοποιούν τα έξυπνα συμβόλαια για την συμμετοχή τους στο κατανεμημένο κατάστιχο. Η βασική διαφορά, με τις υπόλοιπες κατανεμημένες πλατφόρμες είναι ότι ένας κόμβος μπορεί να διαθέτει, εκτός από διαφορετικά έξυπνα συμβόλαια (που περιγράφουν τις διαφορετικές συμβάσεις μεταξύ των κόμβων), διαφορετικά κατανεμημένα κατάστιχα για κάθε συμβόλαιο χωρίς βέβαια αυτό να είναι δεσμευτικό (Hyperleger Fabric, 2017). Επιπλέον για να μπορέσει κάποιος να συνδεθεί το δίκτυο απαιτείται πρώτα η συγκατάθεση του διαχειριστή του δικτύου.



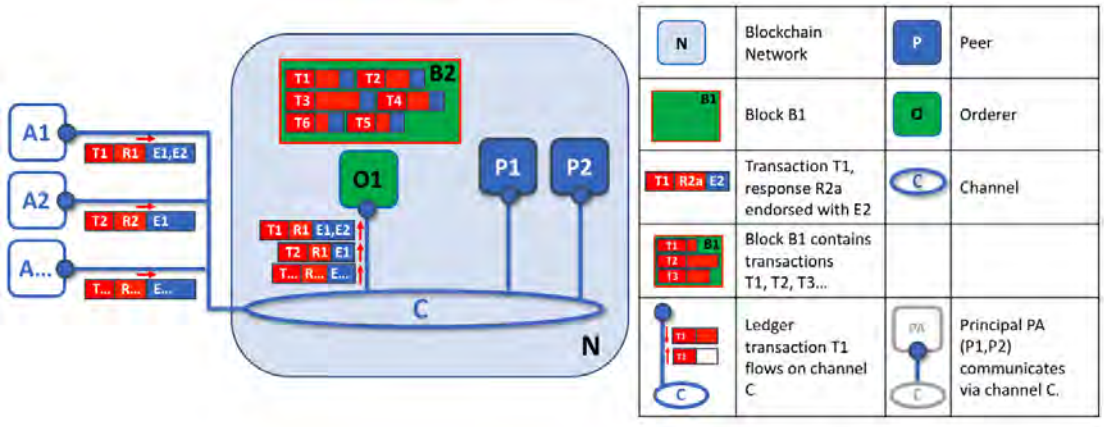
Σχήμα 3.10: Ο κόμβος στο Hyperledger Fabric (2015)

Μία εφαρμογή (την οποία χρησιμοποιεί ένας χρήστης για να συνδεθεί στο blockchain) πρέπει να είναι συνδεδεμένη με ένα κόμβο στο δίκτυο. Μέσα από την εφαρμογή μπορεί να ξεκινήσει μία «υποψήφια» νέα συναλλαγή, η οποία αποστέλλετε στον κανονικό βασικό κόμβο (peer) για να εκτελέσει το έξυπνο συμβόλαιο που αφορά την συγκεκριμένη συναλλαγή. Στην συνέχεια ενημερώνονται για το συγκεκριμένο συμβόλαιο οι ενδιαφερόμενοι βασικοί κόμβοι (endorsing peers). Εφόσον συμφωνούν και το υπογράψουν ψηφιακά αυτό αποστέλλεται πίσω στον χρήστη μέσω της εφαρμογής. Αυτό είναι το πρώτο στάδιο μίας συναλλαγής.



Σχήμα 3.11: Το πρώτο στάδιο της συναλλαγής στο Hyperledger Fabric (2017)

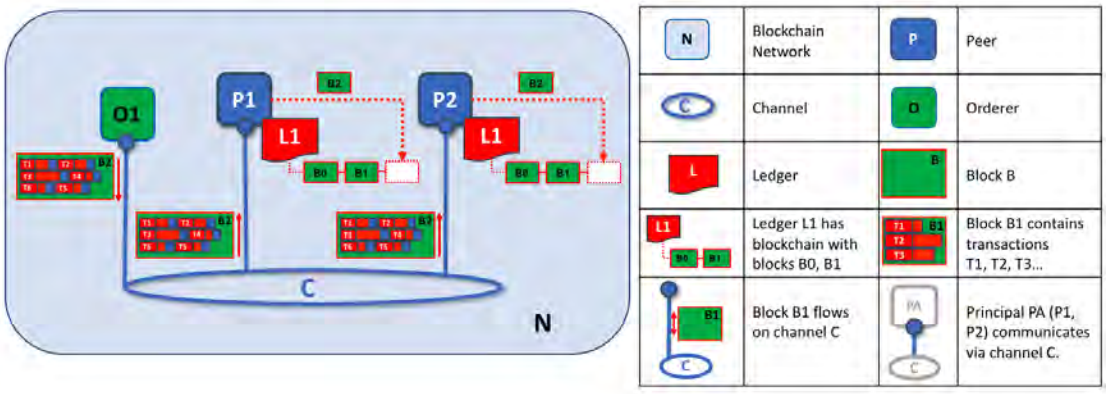
Το δεύτερο στάδιο της συναλλαγής περιλαμβάνει ένα άλλο είδος κόμβου ο οποίος λειτουργεί ως «ελεγκτής-ταξινομητής» (orderer) των συναλλαγών. Συγκεκριμένα είναι αυτός που δημιουργεί τα blocks, ελέγχει αν οι «υποψήφιες» νέες συναλλαγές παραβιάζουν κάποιους από τους όρους του συμβολαίου και μεταδίδει τα blocks στους κόμβους που συμμετέχουν στο συγκεκριμένο κατάστιχο που αφορά το έξυπνο συμβόλαιο που εκτελέστηκε. Αν και στην συγκεκριμένη περίπτωση ο «ελεγκτής» είναι ένας κόμβος, υπάρχει δυνατότητα εφαρμογής ενός κατανεμημένου συστήματος ελέγχου.



Σχήμα 3.12: Το δεύτερο στάδιο της συναλλαγής στο Hyperledger Fabric (2017)

Τέλος, το τρίτο στάδιο αφορά την αποδοχή των blocks από τους κόμβους που συμμετέχουν στο συγκεκριμένο κατάστιχο. Σε περίπτωση που αποδεχτούν τις νέες συναλλαγές τότε αυτές πραγματοποιούνται. Η διαφορά με τις υπόλοιπες πλατφόρμες

είναι ότι ακόμη και στην περίπτωση που δεν γίνει αποδεκτή μία συναλλαγή αυτή καταγράφεται στο blockchain.



Σχήμα 3.13: Το τρίτο στάδιο της συναλλαγής στο Hyperledger Fabric (2017)

3.9.2.2 Η περίπτωση του Corda

Το Corda είναι μια δομή (framework) που χρησιμοποιεί την τεχνολογία του Blockchain και των έξυπνων συμβολαίων. Αυτό σημαίνει ότι η υλοποίηση μπορεί να διαφέρει σε κάθε περίπτωση εφαρμογής. Σε κάθε περίπτωση ωστόσο υπάρχουν τρία βασικά είδη κόμβων.

Η πρώτη κατηγορία κόμβων αφορά τις επιχειρήσεις τις οποίες χρησιμοποιούν το δίκτυο για την επίτευξη των συναλλαγών. Οι συγκεκριμένες έχουν την δυνατότητα χρήσης των έξυπνων συμβολαίων «CorDapps». Παράλληλα, κάθε κόμβος αποθηκεύει όλες τις συναλλαγές που συμμετέχει στο κατάστιχο «CordaVault» που διαθέτει αλλά και τις υποχρεώσεις προς τους άλλους κόμβους χωρίς να χρειάζεται να δημοσιεύει τις πληροφορίες των συναλλαγών σε μη εμπλεκόμενους κόμβους (Corda Docs,2017).

Η δεύτερη κατηγορία κόμβων αφορά τους κόμβους που παρέχουν την βεβαίωση της μοναδικότητας της συναλλαγής και την οριστικοποίηση της συναλλαγής. Η κόμβοι αυτοί ονομάζονται «συμβολαιογραφικοί» κόμβοι (Notary Nodes). Ο αριθμός των κόμβων, όπως και στην περίπτωση των «ελεγκτών» στο Hyperledger Fabric, διαφέρει σε κάθε περίπτωση ενώ μπορεί να επιτευχθεί και με την χρήση ενός κεντρικού κόμβου (Corda Docs,2017).

Τέλος, υπάρχει μία τρίτη κατηγορία κόμβων που λειτουργεί ως διαχειριστής των δημόσιων κλειδιών των οργανισμών που συμμετέχουν όπως και τις IP διευθύνσεις τους έτσι ώστε να γίνεται η ταυτοποίηση των οργανισμών και να επιτυγχάνεται η σύνδεση στο δίκτυο (Corda Docs, 2017).

3.9.2.3 Η περίπτωση του Quorum

Το Quorum χαρακτηρίζεται ως μία έκδοση της πλατφόρμας του Ethereum για επιχειρήσεις. Όπως και οι δύο προηγούμενες περιπτώσεις ιδιωτικών blockchain υποστηρίζει την χρήση των έξυπνων συμβολαίων. Παράλληλα, δίνει την δυνατότητα στους κόμβους που συμμετέχουν να δημιουργούν ιδιωτικές συναλλαγές στα συμβόλαια των οποίων έχουν πρόσβαση μόνο οι συμμετέχοντες. Ωστόσο το σύνολο των συναλλαγών αποθηκεύεται κρυπτογραφημένο σε ένα ενιαίο κατανεμημένο κατάστιχο σε όλους τους κόμβους (Quorum Whitepaper). Το πρωτόκολλο συναίνεσης που χρησιμοποιεί το Quorum είναι το πρωτόκολλο Raft. Ουσιαστικά, ορίζει ένα κόμβο ως «καθοδηγητή» ο οποίος είναι υπεύθυνος για την δημιουργία και την διάδοση των blocks ενώ οι υπόλοιποι κόμβοι αποδέχονται το νέο block. Ο καθοδηγητής ορίζεται μέσα από μία διαδικασία ψηφοφορίας για την δημιουργία κάθε νέου block. Παράλληλα για την υποστήριξη των ιδιωτικών συμβολαίων διαχωρίζει τα έξυπνα συμβόλαια σε ιδιωτικά και δημόσια σε κάθε κόμβο. Η διαφορά με τις δύο προηγούμενες περιπτώσεις ιδιωτικών blockchain είναι ότι δεν απαιτείται κάποιος τρίτος κόμβος (Orderer node και Notary Node) για τον επίτευξη των ιδιωτικών συμβολαίων. Αυτό το επιτυγχάνει με την υιοθέτηση του πρωτοκόλλου ασφαλείας του κρυπτονομίσματος Zcash, Zero-knowledge security layer (ZSL). Συγκεκριμένα δημιουργεί κατακερματισμένες ακολουθίες (hash values) του ισοζύγιού των συναλλασσόμενων, του ποσού της συναλλαγής και του τελικού ισοζυγίου που λειτουργούν ως αποδεικτικά στοιχεία χωρίς να αποκαλύπτονται τα στοιχεία των συναλλασσόμενων και των στοιχείων της συναλλαγής. Οι ακολουθίες ελέγχονται από τους υπόλοιπους κόμβους του δικτύου και εφόσον οι συναλλασσόμενοι τηρούν τα κριτήρια του ιδιωτικού συμβολαίου, η συναλλαγή πραγματοποιείται (Nielsen, 2017).

3.10 Συμπεράσματα

Σε αυτό κεφάλαια αναλυθήκαν οι τρεις μελέτες περίπτωσης του Bitcoin Ethereum και Ripple και οι «δομές» blockchain αρχιτεκτονικών Hyperledger Fabric, Quorum και Corda. Τα βασικά δομικά στοιχεία ενός blockchain δικτύου είναι p2p μορφή του, η κρυπτογραφία και ο αλγόριθμος συναίνεσης για την διεκπεραίωση των συναλλαγών. Σε αυτά εντάσσονται και τα έξυπνα συμβόλαια τα οποία δίνουν την δυνατότητα συναλλαγών περιουσιακών στοιχείων εντός των πλατφορμών. Παράλληλα αναλύθηκαν ο τρόπος παραγωγής νέων νομισμάτων στις τρεις πρώτες μελέτες περίπτωσης και το κόστος συναλλαγών. Ιδιαίτερη αναφορά γίνεται στην υψηλά κόστη

συναλλαγής του Bitcoin, στοιχείο που αποτρέπει την υιοθέτηση του σε επίπεδο μικροσυναλλαγών. Για την χρήση των συγκεκριμένων πλατοφρμών απαιτούνται υπηρεσίες που παρέχονται από τρίτες επιχειρήσεις για την αποθήκευση των νομισμάτων και την μετατροπή τους σε συμβατικά νομίσματα. Το σύστημα διακυβέρνησης διαφέρει σε κάθε κατηγορία καθώς στις περιπτώσεις του Bitcoin και του Ethereum η εξέλιξη της βασίζεται σε αντίστοιχές μη κυβερνητικές οργανώσεις (Ιδρυμα Bitcoin και Ethereum αντίστοιχα) για την εξέλιξή τους ενώ στην περίπτωση του Ripple έχουμε ένα νέο επιχειρηματικό μοντέλο. Τέλος στο επόμενο κεφάλαιο αναλύεται η εφαρμογή των δομών blockchain στο πιλοτικό εγχείρημα Ubin.

Κεφάλαιο 4: Το εγχείρημα Ubin και η συγκριτική ανάλυση

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο αναλύεται αρχικά οι δυο φάσεις του πιλοτικού εγχειρήματος Ubin της Κεντρικής Τράπεζας της Σιγκαπούρης. Στην συνεχεία αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα κάθε κατηγορίας blockchain (public pemissionless, public permissioned και private πλατφορμών), αξιολογείται το επίπεδο καινοτομίας σε κάθε περίπτωση και αναφέρονται τα συμπληρωματικά στοιχεία του ενεργητικού κάθε κατηγορίας.

4.2 Το Project Ubin

Το Project Ubin είναι ένα πιλοτικό εγχείρημα της Κεντρικής Τράπεζας της Σιγκαπούρης σε συνεργασία με την R3, μία εταιρία τεχνολογίας που προωθεί της τεχνολογίες του Blockchain και παράλληλα μια κοινοπραξία των μεγαλύτερων χρηματοπιστωτικών ιδρυμάτων στον κόσμο. Στόχος του συγκεκριμένου εγχειρήματος είναι η δημιουργία ενός πρωτότυπου (Proof-of-Concept) για την επίτευξη διατραπεζικών συναλλαγών με την χρήση της τεχνολογίας των κατανεμημένου κατάστιχου. Εκτός από την MAS και την R3 στο εγχείρημα συμμετέχουν παράλληλα και η Τράπεζα της Αμερικής Merrill Lynch, η Τράπεζα DBS, η HSBC, η J.P Morgan, η Mitsubishi UFJ Financial Group, η OCBC, η εταιρία Singapore Exchange, η Τράπεζα United Overseas και η εταιρεία πληροφοριακών συστημάτων BCS ως πάροχος της τεχνολογίας Ο στόχος του εγχειρήματος Ubin ήταν η δημιουργία ενός κατανεμημένου δίκτυο στο οποίο θα εκδίδεται ψηφιακά το Σιγκαπουριανό δολάριο και η αξιολόγηση των πιθανών προνομίων στο χρηματοπιστωτικό οικοσύστημα της Σιγκαπούρης (Deloitte, 2016).

Η MAS, ως Κεντρική Τράπεζα της Σιγκαπούρης λειτουργεί ως η Οικονομική Ρυθμιστική Αρχή. Συγκεκριμένα, λειτουργεί ως διαχειριστής και επιτηρητής πληρωμών, και συστημάτων clearing και settlement στην Σιγκαπούρη με κύριο στόχο την ασφάλεια και την αποτελεσματικότητα. Ένας από τους ρόλους της είναι να διαχειρίζεται το σύστημα ηλεκτρονικών πληρωμών και σύστημα λογιστικής εγγραφής, το New Mas Electronic Payment System (MEPS+). Το MEPS+ είναι ένα σύστημα ακαθάριστων διακανονισμών σε συνεχή χρόνο (Real Time Gross Settlement System) που υποστηρίζει την διατραπεζικές συναλλαγές κεφαλαίων μεγάλης αξίας και τον διακανονισμό Τίτλων της Κυβέρνησης της Σιγκαπούρης μεταξύ των συμμετεχόντων

στο MEPS+, με την προϋπόθεση της διαθεσιμότητας των κεφαλαίων και των τίτλων. Πρόκειται δηλαδή ότι η MEPS+ λειτουργεί ως σύστημα που επιτρέπει την μεταφορά αμετάκλητων και σε πραγματικό χρόνο των κεφαλαίων και τίτλων (Deloitte, 2016).

Τα βασικά χαρακτηριστικά του MEPS+ είναι:

1. Η χρήση μνημάτων μορφής SWIFT για την αύξηση της διαλειτουργικότητας
2. Η παραμετροποιημενή διαχείρισης αναμονής (queuing management) που παρέχει ρευστότητα και διαχείριση των διακανονισμών
3. Η αυτοματοποιημένη παροχή ρευστότητας εντός της ημέρας (κυρίως σε τράπεζες με χαμηλή ρευστότητα), που επιτρέπει την γρηγορότερη διεκπεραίωση των συναλλαγών.
4. Η αυτοματοποιημένη λύση στο πρόβλημα του αδιέξοδού (gridlock resolution). Συγκεκριμένα ανιχνεύονται τα gridlocks μεταξύ των συμμετεχόντων για να αποτραπεί ή να μειωθεί οι ουρές στις πληρωμές και να αυξηθεί η αποδοτικότητα της ροής των πληρωμών.

Το project Ubin είναι ένα εγχείρημα πολλών σταδίων. Στην πρώτη φάση του εγχειρήματος ο στόχος ήταν η δημιουργία ενός συστήματος MEPS+ το οποίο θα επιτρέπει την μεταφορά σε πραγματικό χρόνο και την έκδοση κεφαλαίων μέσα στο κατανεμημένο κατάστιχο. Αν και το MEPS+ στηρίζει τις εγχώριες συναλλαγές, στις περιπτώσεις διασυνοριακών συναλλαγών η αλληλεπίδραση με διεθνή συστήματα δημιουργεί τους εξής κινδύνους (Deloitte, 2016).

1. Κίνδυνος αλλαγής (Replacement risk)
2. Κίνδυνος Διακανονισμού (Settlement Risk)
3. Ανεπαρκή κεφαλαικά κόστη (Inefficient funding costs)
4. Κόστη συμφωνιών (Reconciliation costs)

Ο κύριος στόχος ολόκληρου του εγχειρήματος είναι η μείωση του ρίσκου και του κόστους για τις διασυνοριακές συναλλαγές και διακανονισμούς. Τα βασικά χαρακτηριστικά για την επίτευξη του στόχου μέσα από την χρήση του κατανεμημένου κατάστιχου είναι η διαλειτουργικότητα μεταξύ των διαφορετικών πλατφορμών blockchain, η επιλεκτική ταυτοποίηση των σχετικών ομάδων που συμμετέχουν, το επιθυμητό επίπεδο ιδιωτικότητας των συμμετεχόντων, την αποδεδειγμένη ικανότητα του συστήματος να ανταποκρίνεται κατάλληλα στην μεγέθυνση και την εξέλιξη των συστημάτων με την πάροδο του χρόνου (Deloitte, 2016).

4.2.1 Πρώτη φάση του Project Ubin

Στην πρώτη φάση του εγχειρήματος, δημιουργήθηκε ένα νέος λογαριασμός για κάθε τράπεζα ο οποίος ήταν συνδεδεμένος στο blockchain. Πριν γίνει η ανάλυση του συγκεκριμένου λογαριασμού κρίνεται σκόπιμη η ανάλυση των υπαρχόντων λογαριασμών των τραπεζών που βρίσκονται στο σύστημα MEPS+ (Deloitte, 2017).

1. Λογαριασμός CAS: Ο συγκεκριμένος λογαριασμός διατηρεί το υπόλοιπο της εκάστοτε τράπεζας κατά την διάρκεια της νύχτας, ενώ εκεί διατηρεί τα χρήματά της όταν δεν τα χρησιμοποίει σε διαδικασίες πληρωμών. Συνήθως, αυτός ο λογαριασμός διατηρείται στο χαμηλότερο δυνατό σημείο από πλευράς. Συγκεκριμένα, το διαθέσιμο υπόλοιπο μεταφέρεται στο λογαριασμό RTGS για τις συναλλαγές RTGS μεταξύ τραπεζών.
2. Λογαριασμός στο σύστημα διακανονισμού σε συνεχή χρόνο (Real time gross settlement): Ο Λογαριασμός RTGS χρησιμοποιείται για τις συναλλαγές μεταξύ τραπεζών. Ο συγκεκριμένος λογαριασμός χρεώνεται και πιστώνεται κατά την διάρκεια της μέρας, τις ώες λειτουργίας του MEPS+. Συνήθως χρηματοδοτείται από τον λογαριασμό CAS το πρωί και στέλνει πίσω το υπόλοιπό του κατά την διάρκεια της νύχτας. Στο εγχείρημα Ubin χρησιμοποιείται για την αποστολή κεφαλαίων στον λογαριασμό που είναι συνδεδεμένος με το κατανεμημένο κατάστιχο.
3. Λογαριασμός επιμέλειας γρήγορων και ασφαλών συναλλαγών (Fast and secure transfers cash custody account): Ο συγκεκριμένος λογαριασμός χρησιμοποιείται για τις διατραπεζικές συναλλαγές καθ’ όλη την διάρκεια της ημέρας. Τυπικά δεν χρηματοδοτείται ούτε αφαιρούνται τα κεφάλαιά του σε καθημερινή βάση. Ο συγκεκριμένος λογαριασμός δεν χρησιμοποιείται στο Ubin.
4. Λογαριασμός επιμέλειας κεφαλαίων στο κατανεμημένο κατάστιχο (Depository Receipt Cash Custody Account): Ο συγκεκριμένος λογαριασμός δημιουργήθηκε στα πλαίσια του εγχειρήματος και αντικαθιστά το λογαριασμό FAST. Το υπόλοιπο του αναδιαμορφώνεται ανάλογα με το ποσό σε ψηφιακό νόμισμα που κατέχει ο ιδιοκτήτης της λογαριασμού στη blockchain πλατφόρμα.

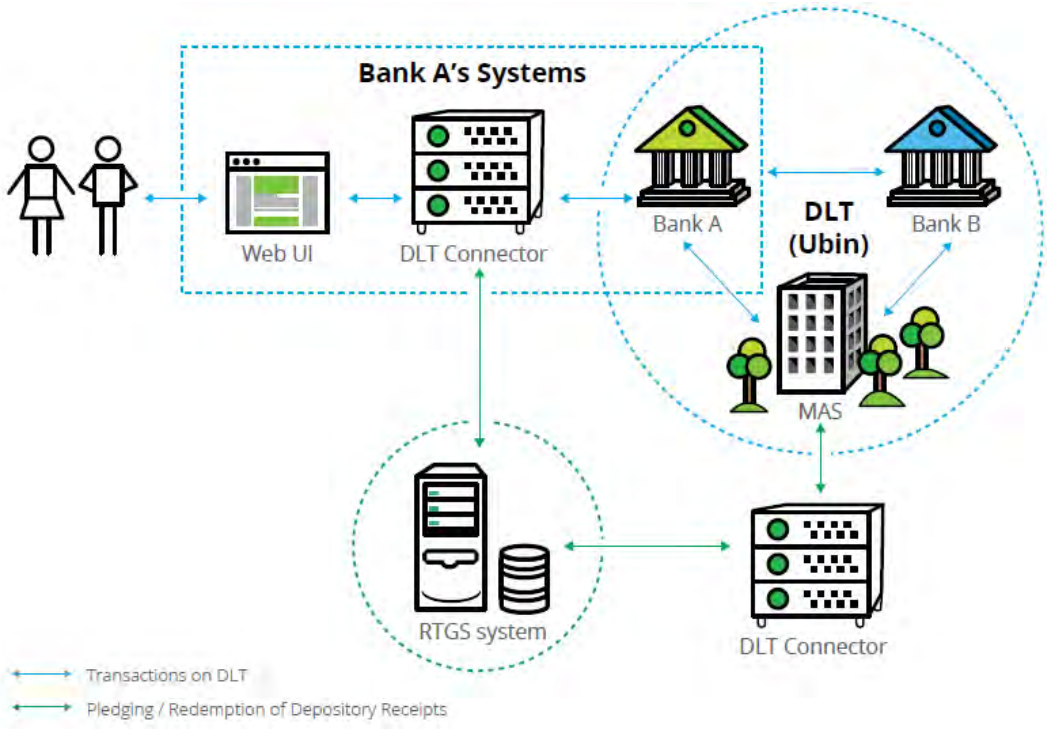
Τα χρηματοπιστωτικά ιδρύματα που συμμετέχουν έχουν στην κατοχή τους ένα ιδιωτικό λογαριασμό DR. Σε αυτό το λογαριασμό στέλνουν το οποίο χρηματοδοτείται από το λογαριασμό RTGS που κατέχουν. Το υπόλοιπο του λογαριασμού μετατρέπεται από την MAS σε ψηφιακό νόμισμα στο λογαριασμό της κάθε τράπεζας μέσα στο

blockchain και λειτουργεί ως εχέγγυο για την έκδοση των ψηφιακών νομισμάτων. Ωστόσο, κατά την διάρκεια της λειτουργίας της πλατφόρμας το υπόλοιπο στο λογαριασμό DR (λόγω των συναλλαγών μέσα στο κατανεμημένο κατάστιχο) μπορεί να μην αντικατοπτρίζει το ακριβές υπόλοιπο που έχει στην πλατφόρμα του blockchain. Ο συγχρονισμός των υπολοίπων των δύο λογαριασμών σε κάθε τράπεζα συμβαίνει στις περιπτώσεις που η τράπεζα αντιμετωπίζει προβλήματα ρευστότητας.

Οι τράπεζες μπορούν να μπορούν να αυξήσουν ή να μειώσουν το υπόλοιπο του λογαριασμού DR κατά την διάρκεια του ωραρίου λειτουργίας του MEPS+ ενώ μπορούν να διατηρούν υπόλοιπο στον συγκεκριμένο λογαριασμό καθ' όλη την διάρκεια της μέρας. Επίσης στο συγκεκριμένο λογαριασμό η προμήθεια είναι μηδενική σε αντίθεση με τους υπόλοιπους λογαριασμούς στο MEPS+. Τέλος, οι συναλλαγές εντός του κατανεμημένου κατάστιχου μπορούν να γίνονται καθ' όλη την διάρκεια της μέρας. Σε περίπτωση μεταφοράς του υπολοίπου από το DR στο RTGS λογαριασμό, το ψηφιακό νόμισμα στο πορτοφόλι του στο blockchain καταστρέφεται (Deloitte, 2016).

4.2.1.1 Η αρχιτεκτονική του δικτύου

Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική του δικτύου και τρόπος σύνδεσης των διαφορετικών τραπεζικών συστημάτων και των χρηστών μέσα στο δίκτυο καθώς και ο τρόπος αλληλεπίδρασης των συστημάτων για την επίτευξη συναλλαγών αλλά και την αυξομείωση του ποσού που βρίσκεται στο λογαριασμό DR του κάθε χρηματοπιστωτικού ιδρύματος. Η συγκεκριμένη πλατφόρμα είναι βασισμένη στην αρχιτεκτονική του Ethereum. Η MAS διαχειρίζεται δύο κόμβους εντός του blockchain ενώ άλλοι 8 κόμβοι βρίσκονται σε αντίστοιχο αριθμό τραπεζών/χρηστών. Το σύνολο των συναλλαγών είναι εμφανές μέσα στο δίκτυο (Deloitte, 2016).



Σχήμα 4.1: Η αρχιτεκτονική του δικτύου στο Project Ubin Phase 1 (Deloitte, 2017)

Η διαδικασία που θα πρέπει να ακολουθήσει ένα χρηματοπιστωτικό ίδρυμα για να μεταφέρει το υπόλοιπο στο λογαριασμό του εντός της πλατφόρμας είναι η εξής:

1. Στο ξεκίνημα της ημέρας γίνονται δύο διεργασίες

   a. Το κεφάλαιο που βρίσκεται ως πλεόνασμα στον λογαριασμό του χρήστη Α μεταφέρεται στο λογαριασμό RTGS

   b. Ο χρήστης Α στέλνει αίτημα στο σύστημα MEPS+ για την αποστολή κεφαλαίου από το λογαριασμό RTGS στο λογαριασμό του Blockchain λογαριασμό. Το ποσό θα σταλεί στο λογαριασμό του στο blockchain (xxxx0800). Για παράδειγμα θέλει να μεταφέρει 300 δολάρια. Η MAS ελέγχει αν υπάρχει το ανάλογο ποσό στον λογαριασμό RTGS για να μεταφέρει το ανάλογο πόσο στο λογαριασμό του Blockchain που λειτουργεί ως εχέγγυο για τα ψηφιακά νομίσματα που θα εκδοθούν στο πορτοφόλι του. Σημαντική παρατήρηση είναι ότι η μεταφορά από το RTGS στο Blockchain λογαριασμό γίνεται εικονικά, δηλαδή δηλώνεται το πόσο που επιθυμεί ο χρήστης να μεταφέρει στο πορτοφόλι του στην πλατφόρμα του Blockchain.

2. Η MAS εκδίδει το αντίστοιχο ποσό σε ψηφιακό νόμισμα στο πορτοφόλι του χρήστη με την χρήση ενός έξυπνου συμβολαίου. Η συνέχεια συμβαίνει εντός της blockchain πλατφόρμας.

3. Ο χρήστης Α θα κάνει συναλλαγές με άλλους συμμετέχοντες στη εντός του blockchain. Για παράδειγμα στέλνει 30 δολάρια Σιγκαπούρης στο χρήση Β.

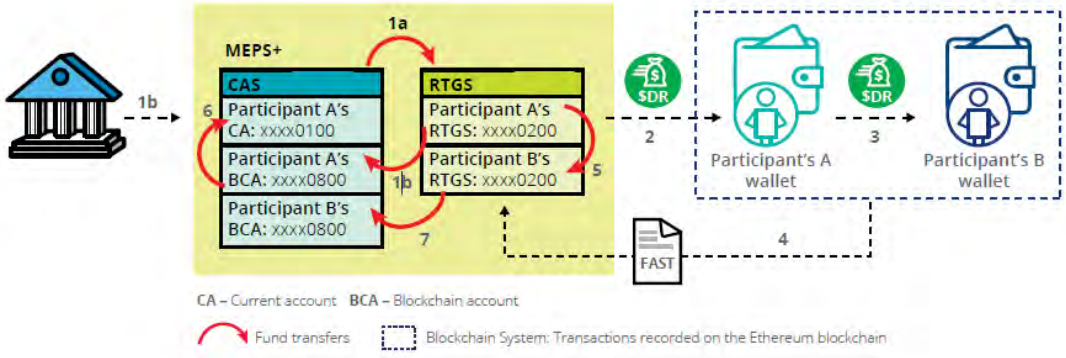
4. Στην περίπτωση αποστολής κεφαλαίου από τον Α στον Β το σύστημα του blockchain θα στείλει την πληροφορία στο σύστημα RTGS.

5. Θεωρώντας ότι υπάρχει το αντίστοιχο ποσό στον λογαριασμου RTGS του χρήστη Α, το ποσό των 30 δολαρίων θα χρεωθεί τον λογαριασμό του ενώ αντίστοιχα το ίδιο ποσό θα πιστωθεί στο RTGS λογαριασμό του Β. Αξίζει να σημειωθεί ότι μόνο το MEPS+ επιτρέπει την αποστολή κεφαλαίων.

6. Το ίδιο ποσό χρεώνεται στον blockchain λογαριασμό του χρήστη Α και πλέον το υπόλοιπο που έχει είναι 270.

7. Το ίδιο ποσό πιστώνεται στον blockchain λογαριασμό του χρήστη Β.

8. Στο τέλος της μέρας, το υπόλοιπο του blockchain λογαριασμού του χρήστη Α αναπροσαρμόζεται (Deloitte, 2016).



Σχήμα 4.2: Οι συναλλαγές στο Project Ubin Phase 1 (Deloitte, 2017)

4.2.1.2 Παρατηρήσεις για την πρώτη φάση του Project Ubin και μελλοντικοί στόχοι

Η πρώτη φάση του συγκεκριμένου εγχειρήματος θεωρείται επιτυχημένη καθώς κατάφερε να δημιουργήσει μία πλατφόρμα συναλλαγών χρησιμοποιώντας την τεχνολογία του blockchain και παράλληλα να την συνδέσει με το υπάρχον σύστημα MEPS+.

Στην πρώτη φάση του εγχειρήματος δεν παρατηρήθηκε πιστωτικός κίνδυνος καθώς το ψηφιακό νόμισμα εκδίδονταν σε κάθε περίπτωση από την Κεντρική Τράπεζα

που προηγουμένως είχε δεσμεύσει το αντίστοιχο ποσό. Ωστόσο απαιτείται η δημιουργία του αντίστοιχου νομικού πλαισίου που να επιβεβαιώνει ότι η συναλλαγές σε ψηφιακό νόμισμα είναι ισοδύναμες με τις συναλλαγές σε συμβατικό νόμισμα. Επιπλέουν οι τράπεζες χρηματοδοτούν καθημερινά τις αναμενόμενες πληρωμές τους σε μία ακαθάριστη βάση πληρωμών (gross basis), δεν υπάρχει κίνδυνος ρευστότητας στην πλατφόρμα του blockchain.

Παράλληλα, επιτεύχθηκε η απαγκίστρωση των συναλλαγών από σύστημα MEPS+. Ωστόσο τίθεται το ερώτημα κατά της ωριμότητας των τεχνολογιών και των εργαλείων που χρησιμοποιήθηκαν για την δημιουργία της πλατφόρμας καθώς αντιμετωπίσθηκαν αρκετές προκλήσεις κατά την διάρκεια της δημιουργίας. Σημαντικές παρατηρήσεις είναι επίσης η ανάγκη για συνεχή συγχρονισμό μεταξύ των κόμβων και η κρυπτογράφηση όλων των συναλλαγών για την προστασία της ιδιωτικότητας.

Οι μελλοντικοί στόχοι για τις επόμενες φάσεις του εγχειρήματος είναι οι εξής:

1. Η αντιμετώπιση των τεχνικών ζητημάτων λόγω της «ανωριμότητας» των τεχνολογιών (και πιθανώς η χρήση διαφορετικών αρχιτεκτονικών).
2. Η δημιουργία ενός δικτύου που για την διεκπεραίωση συναλλαγών τίτλων (Deliver versus Payment)
3. Η δημιουργία ενός δικτύου διασυνοριακών συναλλαγών (Payment versus Payment) μεταξύ της Σιγκαμπούρης, του Καναδα, του Χονγκ Κονγκ και πιθανώς και της Αυστραλίας, της Κίνας και της Ινδίας.
4. Η διεξαγωγή διεθνούς έρευνας για τις νομισματικές, ρυθμιστικές και νομικές επιπτώσεις των ψηφιακών νομισμάτων (με πρωταρχικό στόχο την συνεργασία με το αντίστοιχο εγχείρημα «Japser» που διεξάγεται στον Καναδά) (Deloitte, 2016).

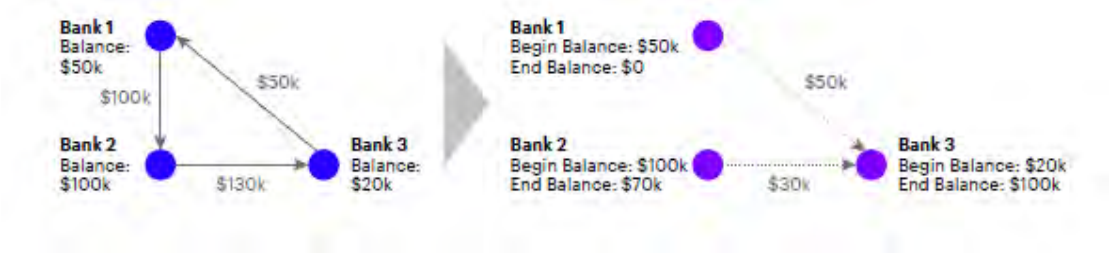
4.2.2 Δεύτερη φάση του Project Ubin

Στη δεύτερη φάση του Project Ubin, που διεξήχθη από την Νομισματική Αρχή της Σιγκαπούρης σε συνεργασία με την Ένωση Τραπεζών της Σιγκαπούρης, δόθηκε έμφαση στην δημιουργία ενός κατανεμημένου μηχανισμού προστασίας της ρευστότητας (Liquidity Saving Mechanism) και στην διατήρηση της ιδιωτικότητας μεταξύ των τραπεζικών συναλλαγών. Συγκεκριμένα δημιουργήσαν τρεις διαφορετικές πλατφόρμες κατανεμημένου κατάστιχου βασισμένες στις αρχιτεκτονικές toy Corda, του Hyperledger Fabric και του Quorum (Accenture, 2017).

Τα τρία πρωτότυπα αποδεικνύουν την δυνατότητα εκτέλεσης των βασικών λειτουργιών ενός συστήματος άμεσου διακανονισμού σε συνεχή χρόνο (RTGS), όπως η μεταφορά κεφαλαίων, ο μηχανισμός αναμονής (queuing mechanism) και η λύση του αδιεξόδου (gridlock resolution) σε διαφορετικές πλατφόρμες με διαφορετικές αρχιτεκτονικές ενώ αντιμετωπίζουν τα προβλήματα ενός κεντρικού συστήματος RTGS όπως την περίπτωση μοναδικού σημείου αποτυχίας (single point of failure). Παράλληλα, εκμεταλλεύεται τα βασικά πλεονεκτήματα ενός blockchain που είναι η ασφάλεια των πληροφοριών λόγω της κρυπτογράφησης και η αμεταβλητότητα των επικυρωμένων συναλλαγών (Accenture, 2017).

4.2.2.1 Η λύση του αδιεξόδου (gridlock resolution) και οι μηχανισμοί προστασία ρευστότητας (Liquidity Saving Mechanism)

Στις περιπτώσεις που οι τράπεζες αντιμετωπίζουν προβλήματα ρευστότητας με αποτέλεσμα να καθυστερούν την διεκπεραίωση των διατραπεζικών συναλλαγών και δημιουργούν μία σειρά αναμονής. Αντίστοιχα η καθυστέρηση της πληρωμής από την τράπεζα Α στην Β μπορεί να δημιουργήσει προβλήματα και στην ρευστότητα των υπόλοιπων τραπεζών ενώ συχνό φαινόμενο είναι η ανακύκλωση της ρευστότητας. Η περίπτωση αυτή ονομάζεται gridlock. Η λύση του έρχεται μέσα από το σύστημα διακανονισμού σε πραγματικό χρόνο το οποίο διαχειρίζεται η Κεντρική Τράπεζα. Όπως προαναφέρθηκε το ίδιο ισχύει και στην περίπτωση της Σιγκαπούρης. Ένας τρόπος επίλυσης του συγκεκριμένου προβλήματος είναι ο μηχανισμός προστασίας της ρευστότητας (Liquid Saving Mechanism). Στο σχήμα φαίνεται ένα απλό gridlock σενάριο στο οποίο συμμετέχουν 3 τράπεζες οι οποίες δεν έχουν την απαραίτητη ρευστότητα για να πραγματοποιήσουν τις τρείς συναλλαγές. Ο μηχανισμός LSM χρησιμοποιείται για την επίλυση του προβλήματος όπως φαίνεται στο σχήμα. Συνήθως σε αυτές τις περιπτώσεις ο συγκεκριμένος μηχανισμός εφαρμόζεται από την Κεντρική Τράπεζα η οποία έχει πληροφορίες για όλες τις οδηγίες πληρωμών μεταξύ των τραπεζών (Accenture, 2017).



Σχήμα 4.3: Το πρόβλημα gridlock (Accenture, 2017)

4.2.2.2 Οι στόχοι της δεύτερης φάσης του Project Ubin

Με την δημιουργία των τριών πρωτοτύπων γίνεται προσπάθεια αντιμετώπισης κάλυψης των εξής κριτηρίων:

1. Η ψηφιοποίηση των συναλλαγών RTGS με την χρήση του ψηφιακού νομίσματος

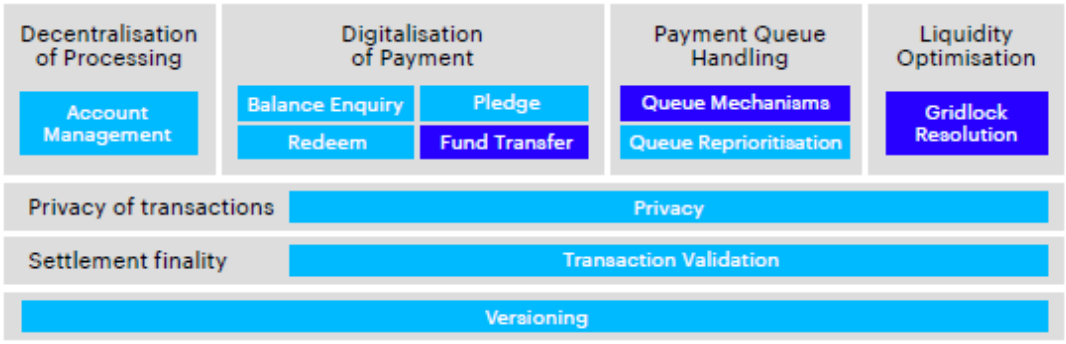
2. Η κατανεμημένη διαχείριση των διαδικασιών χωρίς να υπάρχει η περίπτωση μοναδικού σημείου αποτυχίας

3. Η διαχείριση της ουράς αναμονής των πληρωμών μέσα από την δημιουργία ενός συστήματος που θα επιτρέπει την ιεράρχηση, την διατήρηση και την ακύρωση των συναλλαγών.

4. Η ιδιωτικότητα των συναλλαγών αποτρέποντας τους μη συμμετέχοντες από την πρόσβαση στις πληροφορίες των συναλλαγών.

5. Η οριστικότητα των διακανονισμών των πληρωμών.

6. Η βελτίστοποίηση της ρευστότητας μέσα από την επίλυση των προβλημάτων gridlock.

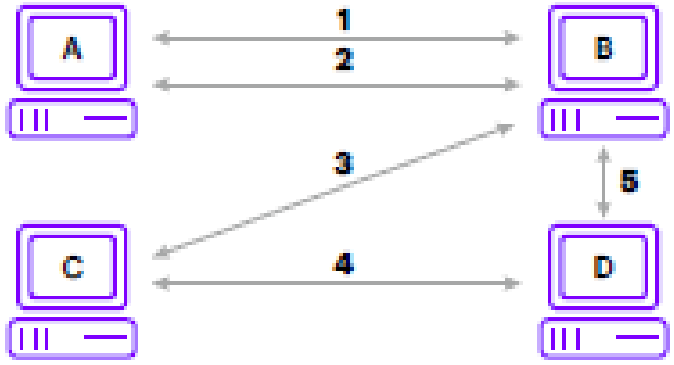


Σχήμα 4.4: Τα κριτήρια προς αντιμετώπιση στην δεύτερη φάση του Project Ubin (Accenture, 2017)

4.2.2.2 Η πλατφόρμα Corda

Η πλατφόρμα Corda είναι μία πλατφόρμα που χρησιμοποιεί την τεχνολογία του κατανεμημένου κατάστιχου και έχει σχεδιαστεί κυρίως για την εφαρμογή του σε χρηματοπιστωτικά ιδρύματα. Έχει σχεδιαστεί για την καταγραφή την διαχείριση και τον συγχρονισμό των συμφωνιών μεταξύ των συμμετεχόντων πάρεχοντάς τους ιδιωτικότητα στις συναλλαγές. Συγκεκριμένα, δεν αποστέλλει πληροφορίες σε όλους

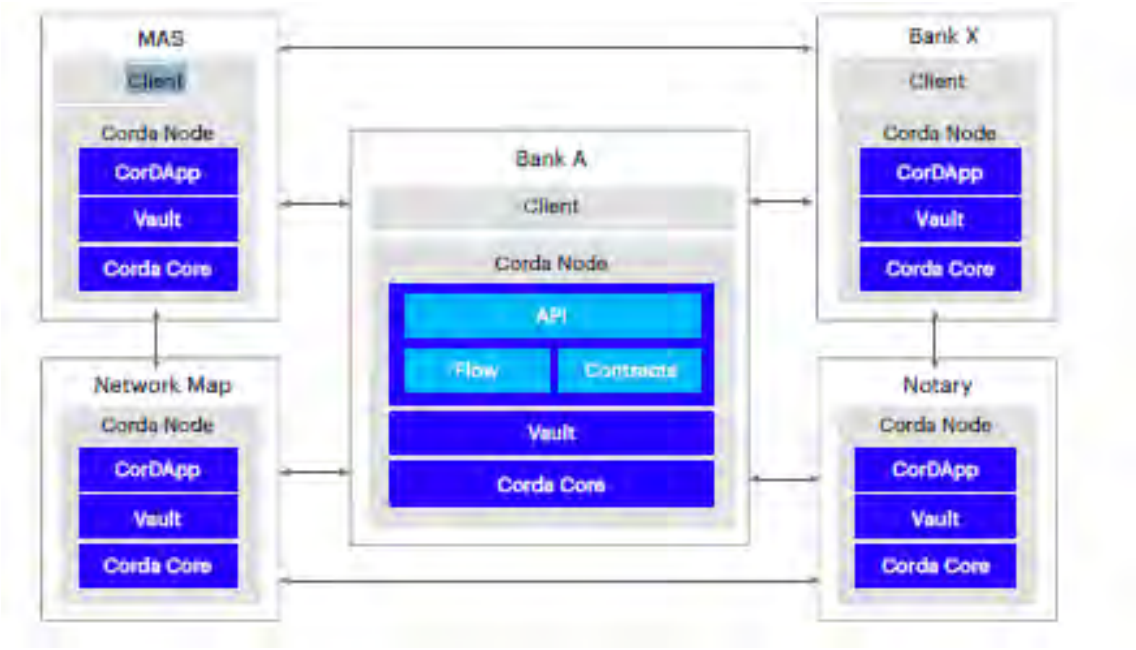
τους συμμετέχοντες αλλά σε όσους συμμετέχουν στην συναλλαγή. Όπως φαίνεται στο παρακάτω σχήμα, οι συναλλαγές των τεσσάρων κόμβων δεν είναι εμφανής σε όλους (Accenture, 2017).



Σχήμα 4.5: Το δίκτυο Corda (Accenture, 2017)

Οι κόμβοι του συστήματος είναι οι εξής:

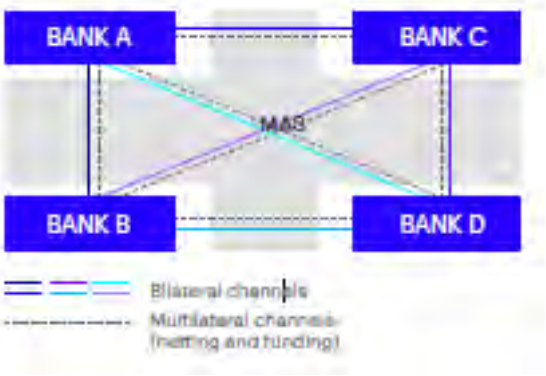
1. Οι βασικοί κόμβοι ενός συστήματος Corda είναι αυτοί των τραπεζών και της MAS οι οποίοι δημιουργούν τα έξυπνα συμβόλαια μέσα από το «CorDapp» και αποθηκεύουν τις συναλλαγές που έχουν επιτευχθεί αλλά και τις υπόλοιπες συναλλαγές που έχουν μπει στην αναμονή ως υποχρεώσεις προς τις άλλες τράπεζες.
2. Ο κόμβος που λειτουργεί ως «συμβολαιογράφος» (Notary node) και είναι αυτός που επιβεβαιώνει την ύπαρξη των ανάλογων κεφαλαίων στο υπόλοιπο της τράπεζας για την επίτευξη της συναλλαγής. Στην συγκεκριμένη περίπτωση είναι ένας ωστόσο δεν είναι απαραίτητο να είναι η MAS.
3. Τέλος υπάρχει ένας τρίτος κόμβος που λειτουργεί ως διαχειριστής των δημόσιων κλειδιών που χρησιμοποιούνται από τις τράπεζες και των διευθύνσεων IP για την ταυτοποίηση τους. Χαρακτηριστικό της συγκεκριμένης πλατφόρμας είναι η έκδοση νέου δημόσιου κλειδιού για κάθε νέα συναλλαγή για την διατήρηση της ανωνυμίας μέσα στο σύστημα.



Σχήμα 4.6 : Δομή του δικτύου Corda (Accenture,2017)

4.2.2.3 Η πλατφόρμα Hyperledger Fabric

Το Hyperledger Fabric είναι μία πλατφόρμα που χρησιμοποιεί την τεχνολογία του blockchain που υποστηρίζει την χρήση έξυπνων συμβολαίων. Επιτρέπει στους χρήστες να δημιουργούν «κανάλια» μεταξύ συγκεκριμένων συμμετεχόντων και να δημιουργούν ξεχωριστά κατάστιχα σε κάθε περίπτωση δίνοντας πληροφορίες μόνο στους συμμετέχοντες στηρίζοντας την ιδιωτικότητα των συναλλαγών. Οι συμμετέχοντες επικυρώνουν την συναλλαγή και στην συνέχεια ο κόμβος που λειτουργεί ως ταξινομητής στέλνει την πληροφορία στους υπόλοιπους κόμβους που συμμετέχουν στο συγκεκριμένο κανάλι για την έγκριση της συναλλαγής. Όπως φαίνεται στο παρακάτω σχήμα η τράπεζα Α έχει τρία διαφορετικά αμφίδρομα κανάλια με τα οποία συνδέεται με τις υπόλοιπες τράπεζες. Παράλληλα συμμετέχει σε δύο κανάλια για την μεταφορά κεφαλαίων (funding channel) και ένα κανάλι συμψηφισμού (netting channel) που λειτουργούν ως ένα πολυμερές κανάλι (multilateral channel) που αυξάνει τον έλεγχο και την ανιχνευσιμότητα των συναλλαγών μέσα στο δίκτυο (Accenture, 2017).

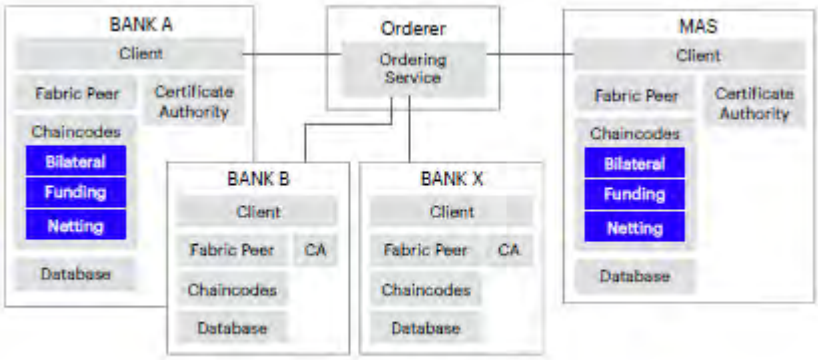


Σχήμα 4.7: Το δίκτυο Hyperledger Fabric (Accenture, 2017)

Στην συγκεκριμένη περίπτωση η MAS συμμετέχει και σε όλα τα κανάλια, δηλαδή και στα αμφίδρομα και στα πολυμερή κανάλια, για τον έλεγχο και όλων των συναλλαγών μέσα το δίκτυο. Η συμμετοχή της στα αμφίδρομα κανάλια έχει ως στόχο το διακανονισμό των διαδικασιών στο σενάριο του gridlock εφόσον βρεθεί λύση στο πρόβλημα (Accenture, 2017).

Οι βασικοί κόμβοι του δικτύου είναι οι εξής:

1. Ο κόμβος που λειτουργεί ως ταξινομητής - ελεγκτής των νεών συναλλαγών και είναι υπεύθυνος για την αποστολή των δεδομένών στο αντίστοιχο κανάλι.
2. Οι βασικοί κόμβοι δηλαδή οι τράπεζες και η MAS που δημιουργούν νέες συναλλαγές. Εντός των κόμβων υπάρχουν:
    - Το chaincode δηλαδή τα έξυπνα συμβόλαια που χρησιμοποιούνται για την δημιουργία και τον έλεγχο των συναλλαγών.
    - Ένα αρχείο που διαχειρίζεται τις ταυτότητες των υπόλοιπων τραπεζών έτσι ώστε να γίνεται η αναγνώριση. Το Hyperledger το ονομάζει Certificate Authority.
    - Ο αποδέκτης των νέων συναλλαγών που ονμάζεται Fabric Peer, ο οποίος δέχεται και επεξεργάζεται τις νέες συναλλαγές που δέχεται από τον Orderer.



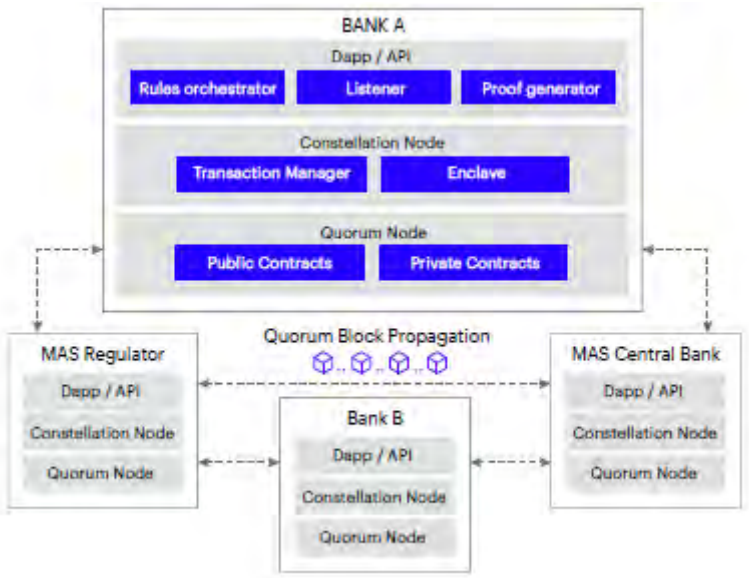
Σχήμα 4.8: Η δομή του Hyperledger Fabric (Accenture, 2017)

4.2.2.4 Η πλατφόρμα Quorum

Η πλατφόρμα Quorum είναι μία πλατφόρμα βασισμένη στην αρχιτεκτονική του Ethereum. Υιοθετεί το πρωτόκολλο Raft για την αποθήκευση των νέων συναλλαγών ενώ επιτρέπει στου κόμβους να δημιουργούν δύο κατάστιχα ένα δημόσιο και ένα ιδιωτικό στο οποίο αποθηκεύουν όλες τις συναλλαγές (Quorum constellation) για την ιδιωτικότητα των συναλλαγών. Τέλος για την διατήρηση της ιδιωτικότητας των συναλλασσόμενων κατά την μεταφορά των κεφαλαίων υιοθετεί το πρωτόκολλο Zero-knowledge security layer (ZSL) έτσι ώστε να επιτυγχάνεται η μεταφορά των κεφαλαίων χωρίς να αποκαλύπτονται τα στοιχεία των συναλλασόμενων. Σε αυτή την περίπτωση δεν χρειάζεται κάποια κεντρική αρχή για την επίτευξη των συναλλαγών επομένως μειώνεται ο κίνδυνος του σφάλματος ενός σημείου (single point of failure) (Accenture, 2017).

Τα βασική αρχιτεκτονική του δικτύου είναι η εξής:

1. Οι κόμβοι των τραπεζών που περιέχουν
    - Δύο κατάστιχα ένα ιδιωτικό (Constellation) και το δημόσιο κατάστιχο
    - Τα έξυπνα συμβόλαια
    - Το πρωτόκολλο ZSL που διασφαλίζει την ασφάλεια κατά την διάρκεια των μεταφορών κεφαλαίων
    - Τη Quorum αποκεντρωμένη εφαρμογή (Dapp) που είναι υπεύθυνη για την εκτέλεση των συμβολαίων



Σχήμα 4.9: Η δομή του δικτύου Qurum (Accenture, 2017)

4.2.2.5 Ο μηχανισμός αναμονής των πληρωμών

Όταν μία τράπεζα δημιουργεί μία νέα συναλλαγή αλλά δεν έχει τα απαραίτητα κεφάλαια για την δημιουργία τη διεκπεραίωσή της αυτή μπαίνει σε μία λίστα αναμονής έχοντας επίγνωση όλων των εισερχόμενων και εξερχόμενων πληρωμών. Όταν αποκτά την απαραίτητη ρευστότητα η συναλλαγές διεκπεραιώνονται βάση της σειράς που υπάρχει σε αυτή την λίστα. Ωστόσο, οι συναλλαγές χωρίζονται σε δύο κατηγορίες υψηλής προτεραιότητας και κανονικής προτεραιότητας. Όσες συναλλαγές χαρακτηρίζονται ως συναλλαγές υψηλής προτεραιότητας διεκπεραιώνονται πρώτες ενώ οι υπόλοιπες της κανονικής προτεραιότητας διεκπεραιώνονται βάσει της λίστας αναμονής. Τέλος, η κάθε τράπεζα έχει την δυνατότητα να αλλάξει την κατηγορία μίας συναλλαγής που δεν έχει διακπεραιωθεί ή να την ακυρώσει. Σε κάθε αρχιτεκτονική χρησιμοποιείται ένας διαφορετικός αλγόριθμος για την επίλυση του gridlock χωρίς παράλληλα να δημιουργεί έλλειμα σε κανένα από τους συμμετέχοντες (Accenture, 2017).

4.2.2.6 Συμπεράσματα και μελλοντικοί στόχοι της δεύτερης φάσης του Project Ubin

Τα συμπεράσματα της δεύτερης φάσης του εγχειρήματος Ubin δείχνουν ότι υπάρχει δυνατότητα χρήσης ενός συστήματος κατανεμημένου κατάστιχου για την αντικατάσταση του κεντρικού συστήματος RTGS που διαχειρίζεται η Κεντρική

Τράπεζα της Σιγκαπούρης. Ωστόσο, τίθενται κάποιες παρατηρήσεις που θα πρέπει να αναλυθούν περαιτέρω στις επόμενες φάσεις του εγχειρήματος (Accenture, 2017).

1. Η αντοχή του δικτύου για την και το επίπεδο ετοιμότητας των πάροχων υπηρεσιών «σύννεφου» (cloud services): Αν και θεωρητικά δεν δημιουργείται πρόβλημα σε περίπτωση που ένας κόμβος αντιμετωπίζει προβλήματα συνδεσιμότητας ή άλλα τεχνικά προβλήματα καθώς τα δεδομένα διαμοιράζονται σε όλους τους κόμβους κάτι που επιτρέπει την γρήγορη επαναφορά του στο σύστημα. Ωστόσο, απαιτείται περαιτέρω μελέτη για την αντοχή κατανεμημένων συστημάτων. Στο συγκεκριμένο εγχείρημα χρησιμοποιήθηκε οι υποδομές σύννεφου της Microsoft. Για την επίτευξη της λειτουργίας του συστήματος κρίθηκε απαραίτητη η ενίσχυση της λειτουργικότητας του σύννεφου σε θέματα σχετικά με την διαχείριση του περιβάλλοντος, την παρακολούθηση των διαδικασιών και την επαναφορά σε περίπτωση σφαλμάτων.

2. Με την προσθήκη ενός κατανεμημένου κατάστιχου στο σύστημα διακανονισμού συνεχής χρόνου επιτυγχάνεται η λειτουργία του καθ' όλη την διάρκεια της μέρας. Η συγκεκριμένη διαδικασία είναι ιδιαίτερα ωφέλιμη για τις περιπτώσεις των διασυνοριακών συναλλαγών όπου τα ωράρια λειτουργίας του συστήματος σε άλλες χώρες, όπως του Καναδά, είναι διαφορετικά. Παράλληλα το σύστημα επιτρέπει την επίτευξη διατραπεζικών συναλλαγών ακόμη και στις περιπτώσεις που κάποιοι χρήστες δεν είναι ενεργοί. Ωστόσο σε ένα σύστημα διακανονισμού σε συνεχή χρόνο που δεν λειτουργεί σε συγκεκριμένες ώρες πρέπει να διευθετηθούν θέματα όπως η μεταφορά κεφαλαίων των διεκπεραιωμένων συναλλαγών μέσα στο κατανεμημένο κατάστιχο πέρα από τις ώρες λειτουργίας (και σε άλλες περιπτώσεις όπως τις αργίες), τα κόστη συναλλαγής, και οι διαφορετικές καταληκτικές ώρες μεταξύ των τραπεζών.

3. Με την χρήση ενός αποκεντρωμένου μηχανισμού προστασίας της ρευστότητας που υιοθετήθηκε στην συγκεκριμένη φάση επιτεύχθηκε η λύση του προβλήματος gridlock. Σε αυτό το στάδιο αν και η συγκεκριμένη διαδικασία κρίνεται επιτυχημένη, σε πιθανή μεγέθυνση του συστήματος είναι πιθανή η αύξηση του χρόνου επίλυσης του προβλήματος. Αποτέλεσμα αυτής της καθυστέρησης είναι η καθυστέρηση των διακανονισμών.

4. Το επίπεδο χρηστικότητας μιας κατανεμημένης πλατφόρμας διαφέρει μεταξύ των χρηματοπιστωτικών ιδρυμάτων λόγω των διαφορετικού όγκου συναλλαγών σε κάθε περίπτωση. Επομένως τα κίνητρα για την εγκατάσταση και την χρήση ενός κόμβου σε κάποιες περιπτώσεις τραπεζών μπορεί να είναι μειωμένα. Επιπλέον το κόστος διατήρησης ενός κόμβου μπορεί να είναι ανασταλτικός παράγοντας για κάποιους από τους συμμετέχοντες. Στις επόμενες φάσεις θα εξεταστεί το ενδεχόμενο ενός συστήματος διακανονισμών σε συνεχή χρόνο με δύο κατηγορίες χρηστών, άμεσους και έμμεσους. Στην περίπτωση υλοποίηση μιας πλατφόρμας με δύο κατηγορίες χρηστών απαιτείται η υιοθέτηση πολιτικών και συμφωνιών σε επίπεδο υπηρεσιών (service level agreements) μεταξύ των συμμετεχόντων έτσι ώστε να μην δίνεται οικονομικό πλεονέκτημα στις μεγαλύτερες τράπεζες.

5. Στο κατανεμημένο σύστημα διακανονισμών σε συνεχή χρόνο κάθε τράπεζα είναι υπεύθυνη για την συντήρηση και την υποστήριξη των κόμβων, δηλαδή τον εξοπλισμό και το λογισμικό του κόμβου, για την διατήρηση της λειτουργικότητας και της σταθερότητας του συστήματος. Σε αυτά συμπεριλαμβάνονται μη λειτουργικά θέματα όπως θέματα ασφάλειας της πλατφόρμας και αναβαθμίσεις του λογισμικού ή του εξοπλισμού.

6. Με την δημιουργία ενός συστήματος διακανονισμού σε συνεχή χρόνο βασισμένο στην τεχνολογία του blockchain, ο ρόλος της Κεντρικής Τράπεζας ως διαχειριστής ενός κεντρικού του συστήματος πληρωμών δεν κρίνεται απαραίτητος καθώς οι διαδικασίες και τα δεδομένα αποστέλλονται στους συμμετέχοντες μέσα από το κατανεμημένο κατάστιχο. Η υιοθέτηση ενός κατανεμημένου συστήματος μειώνει το κόστος και τους πόρους που απαιτούνται για τις καθημερινές διαδικασίες. Ωστόσο δεν καταργείται ο ρόλος της ως «επόπτης» για την ασφάλεια και την αποτελεσματικότητα των συναλλαγών και των διακανονισμών. Συγκεκριμένα απαιτείται:

    - Ο έλεγχος της ρευστότητας του συστήματος.
    - Η διασφάλιση της σταθερότητας του συστήματος καθώς και πιθανές διορθώσεις ή αλλαγές στο λογισμικό και τον εξοπλισμό των κόμβων και η διαχείριση των συμμετεχόντων (όπως οδηγίες για την λειτουργία και την εισαγωγή νέων ή αφαίρεση κόμβων).

- Η έκδοση συμφωνιών σε επίπεδο υπηρεσιών μεταξύ των συμμετεχόντων μέσα στο δίκτυο.
- Η επίλυση πιθανών αντιπαραθέσεων εντός του δικτύου.

4.3 Χαρακτηριστικά των διαφορετικών κατηγοριών του Blockchain

Για την ανάλυση των βασικών χαρακτηριστικών γίνεται αναφορά των γενικών χαρακτηριστικών της τεχνολογίας του blockchain. Βάσει της ανάλυσης του Nakamoto (2008), ο διαμοιρασμός μίας **κοινής βάσης δεδομένων** αλλά και όλων των διαδικασιών σε αυτό είναι ίσως το πιο διακριτό χαρακτηριστικό ενός blockchain δικτύου, στοιχείο που ενισχύει την **διαφάνεια** ως προς την διεκπεραίωση των συναλλαγών μέσα στο δίκτυο. Παράλληλα η αδυναμία αλλαγής ή των δεδομένων δημιουργούν μια **αμετάβλητη** βάση δεδομένων.

4.3.1 Public Permissionless blockchain

4.3.1.1 Χαρακτηριστικά πλατφορμών public permissionless blockchain πλατφορμών

Ο Evans (2014) αναφέρει ότι όλες οι κατανεμημένες δημόσιες πλατφόρμες πληρωμών έχουν τα εξής χαρακτηριστικά:

1. Βασίζονται στο διαδίκτυο και συγκεκριμένα σε όσους θέλουν να διαθέσουν την επεξεργαστική ισχύ του υπολογιστή τους για την λειτουργία τους (χωρίς να υπάρχει περιορισμός ως προς την συμμετοχή) σε αντίθεση με άλλες πλατφόρμες που χρησιμοποιούν ιδιωτικά δίκτυα (όπως η Visa).

2. Έχουν ένα πρωτόκολλο το οποίο είναι απαραίτητο για την μεταφορά των νομισμάτων και την αποθήκευση τους στο blockchain το οποίο βασίζεται στην κρυπτογραφία (όπως έχει περιγραφεί στη δεύτερη ενότητα για την περίπτωση του bitcoin) δημιουργώντας ένα δίκτυο το οποίο . Παράλληλα συμβάλει στην επίτευξη συναίνεσης μέσα σε αυτό.

3. Περιέχουν τα εικονικά νομίσματα τα οποία χρησιμοποιούνται για την μεταφορά αξίας.

4. Υπάρχει ένα ανταποδοτικό σύστημα το οποίο ανταμείβει όσους συμμετέχουν στην αποθήκευση των συναλλαγών για την επεξεργαστική ισχύ και τους πόρους που δαπανούν.

5. Χρησιμοποιούν ένα ανοιχτού κώδικα λογισμικό επιτρέποντας δηλαδή την χρήση του και την συμμετοχή στην επεξεργασία του από τον καθένα.

6. Το σύστημα διακυβέρνησης που χρησιμοποιούν είναι παρόμοιο με αυτό του ανοιχτού κώδικα και βασίζεται κυρίως σε εθελοντές για την εξέλιξή του.

7. Επιπλέον σε αυτά μπορεί να προστεθεί η δυνατότητα της απόκρυψης των στοιχείων των χρηστών μέσω της κρυπτογραφίας και συγκεκριμένα της τεχνολογίας δημόσιου/ιδιωτικού κλειδιού. Η συγκεκριμένη τεχνολογία επιτρέπει την διατήρηση της ανωνυμίας μέσα στο δίκτυο, καθώς δεν υπάρχει κάποιος κεντρικός πάροχος που να ελέγχει και να ταυτοποιεί τους χρήστες των πλατφορμών. Παράλληλα η δυνατότητα χρήσης πολλαπλών κλειδιών δυσκολεύει ακόμη περισσότερο την ταυτοποίηση των χρηστών. Επομένως ενώ οι συναλλαγές είναι εμφανής στον καθένα, η ταυτοποίηση των χρηστών είναι πρακτικά αδύνατη.

4.3.1.2 Πλεονεκτήματα της χρήσης public permissionless blockchain πλατφορμών

Τα βασικό πλεονέκτημα μιας public permissionless blockchain είναι η ετοιμότητα ως προς την χρήση για την επίτευξη των συναλλαγών. Πρόκειται δηλαδή για έτοιμες πλατφόρμες στις οποίες ο χρήστης μπορεί να τις χρησιμοποιήσει εφόσον διαθέτει πορτοφόλι δηλαδή ένα δημόσιο και ένα ιδιωτικό κλειδί. Σε κάποιες περιπτώσεις το κόστος συναλλαγής μπορεί να είναι χαμηλό και η ταχύτητα των συναλλαγών αυξημένη σε σχέση με τους συμβατικούς τρόπους συναλλαγών.

4.3.1.3 Μειονεκτήματα της χρήσης public permssionless blockchain δικτύων

Τα μειονεκτήματα των public permssionless blockchain δικτύων είναι αρκετά όπως αναλύονται στις επόμενες παραγράφους. Τα βασικά προβλήματα μιας τέτοιας πλατφόρμας απορρέουν κατά κύριο λόγο με την έλλειψη κεντρικής αρχής, την έντονη εξάρτηση από τις τεχνολογίες της πληροφορίας και την ανωνυμία των χρηστών.

Η δημιουργία ενός δικτύου που η εμπιστοσύνη μεταξύ των συμμετεχόντων δεν είναι απαραίτητη έχει όμως και αρκετά μειονεκτήματα. Το πρωτόκολλο συναίνεσης Proof-of-Work που χρησιμοποιείται σε αυτές τις περιπτώσεις που αναλύθηκαν δημιουργεί προβλήματα στην μεγέθυνση του δικτύου και στην ταχύτητα των συναλλαγών. Στην περίπτωση του bitcoin παράγεται κατά μέσο όρο 1 block ανά 10 λεπτά. Παράλληλα ο αριθμός των συναλλαγών που επεξεργάζεται είναι περίπου 2 ανά δευτερόλεπτο. Το πρόβλημα είναι εμφανές αν συγκριθεί με το αριθμό διαχείρισης

συναλλαγών της Visa που υπολογίζεται περίπου στις 4000 συναλλαγές ανά δευτερόλεπτο.

Η συνεχής μεγέθυνση ενός public permissionless blockchain δημιουργεί έντονο ανταγωνισμό μεταξύ των κόμβων που διαχειρίζονται την διαδικασία της επικύρωσης (δηλαδή την διεργασία του mining). Παράλληλα, σε συνδυασμό με τον σταθερό μέσο αριθμό των παραγόμενων blocks, η διαδικασία του Proof-Of-Work (δηλαδή η επίλυση του προβλήματος που περιγράφεται στα προηγούμενα κεφάλαια) γίνεται ενεργειακά δαπανηρή. Συγκεκριμένα στην περίπτωση του Bitcoin, η ετησία κατανάλωση ενέργειας υπολογίζεται πλέον σε 24TWh που αντιστοιχεί στην ετήσια κατανάλωση ενέργειας ολόκληρης της Ιρλανδίας (Quartz, 2018).

Η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων (δηλαδή την αγορά και την ανταλλαγή τους) για τους χρήστες είναι ένα βασικό μειονέκτημα των public permssionless blockchain. Αυτό μπορεί να οδηγήσει σε παρανοήσεις και πιθανές ζημίες για τους χρήστες (ECB, 2015).

Η έλλειψη Κεντρικής Αρχής, που να ελέγχει τα κρυπτονομίσματα, όπως οι Κεντρικές Τράπεζες και το Διεθνές Νομισματικό Ταμείο που επιτηρούν τα χρηματοπιστωτικά ιδρύματα, δημιουργεί κινδύνους ως προς την χρήση τους. Η συνέχεια της λειτουργίας της μιας public permssionless blockchain πλατφόμας βασίζεται καθαρά στην ύπαρξη των κόμβων επικύρωσης (miners). Τα κίνητρά τους για την συνέχεια της προσφοράς των υπολογιστικών πόρων που διαθέτουν στο σύστημα βασίζεται μόνο στα οικονομικά κίνητρα (δηλαδή την παραγωγή νέων νομισμάτων και τα κόστη συναλλαγής που συλλέγουν από την συγκεκριμένη διαδικασία) που τους παρέχει το δίκτυο χωρίς να υπάρχει κάποιος δεσμευτικός όρος που να τους δεσμεύει να συνεχίσουν την διαδικασία. Συνεπώς υπάρχει πιθανότητα διακοπής της λειτουργίας ανά πάσα στιγμή αφήνοντας τους ιδιοκτήτες των κρυπτονομισμάτων με νομίσματα άνευ αξίας.

Η μείωση των miners μπορεί να επέλθει και από άλλες διαδικασίες όπως την διαδικασία του Hard-Fork. Η άγνοια του συστήματος για την υπολογιστική ισχύ που κατέχει ο κάθε κόμβος είναι ένα σημαντικό μειονέκτημα. Ο Satoshi Nakamoto (2008), όπως ανέλυσε στο White paper του Bitcoin,η διαδικασία του Proof-of-Work βασίζεται στην παραδοχή ότι το δίκτυο το μεγαλύτερο ποσοστό των κόμβων είναι «έντιμοι» (δηλαδή άνω του 50%). Αυτό σημαίνει ότι σε αντίθετη περίπτωση το δίκτυο αποκτά

μορφή ενός κεντρικού συστήματος όπου μία οντότητα ελέγχει το μεγαλύτερο ποσοστό των κόμβων. Στην συγκεκριμένη περίπτωση τις δίνεται η δυνατότητα να αποδέχεται και να απορρίπτει οποία συναλλαγή επιθυμεί ενώ έχει την δυνατότητα ακόμη και να αντιστρέψει προηγούμενες συναλλαγές. Η συγκεκριμένη διαδικασία ονομάζεται επίθεση του 51% (51% attack) (Shin, 2017; Peters, Panayi, Chappelle, 2016)

Η πιθανότητα χρεοκοπίας ή κλοπής νομισμάτων από ανταλλακτήρια κρυπτονομισμάτων είναι ένα υπαρκτό πρόβλημα σε αυτές τις πλατφόρμες μπορεί να οδηγήσει σε απώλεια των νομισμάτων των χρηστών τους. Καθώς τα περισσότερα ανταλλακτήρια δεν επιβλέπονται από κάποια ρυθμιστική αρχή είναι πολύ πιθανό η απώλεια αυτή να είναι μη αναστρέψιμη. Χαρακτηριστικά παραδείγματα τέτοιων περιπτώσεων είναι η χρεοκοπία του ανταλλακτηρίου Mt Gox τον Φεβρουάριο του 2014 που οδήγησε σε απώλεια χιλιάδων Bitcoin από τους χρήστες του ανταλλακτηρίου ενώ τον Ιανουάριο του 2015 κλάπηκαν 19.00 Bitcoin από το ανταλλακτηρίο Bitcoin (ECB, 2015).

Η έλλειψη Κεντρικής Αρχής, καθιστά αδύνατη την επίλυση την περιπτώσεων όπως η μη εγκεκριμένη από το χρήστη συναλλαγή, η μεταφορά λανθασμένου ποσού ή μεταφορά νομισμάτων σε λάθος χρήστη. Επιπλέον, η αδυναμία αναγνώρισης του παραλήπτη καθώς η συναλλαγές γίνονται μόνο με την χρήση της τεχνολογίας δημόσιων/ιδιωτικών κλειδιών οδηγούν σε μη αντιστρέψιμη απώλεια για τον αποστολέα (ECB, 2015; Peters και Panayi 2016; Peters, Panayi, Chappelle, 2016). Σε ότι αφορά τα έξυπνα συμβόλαια, η έλλειψη ρυθμιστικού πλαισίου ή Κεντρικής Αρχής που να ρυθμίζει την σύναψη συμβολαιακών σχέσεων δημιουργεί ερωτήματα ως προς την χρηστικότητά τους, ιδιαίτερα σε περιπτώσεις διαφωνιών μεταξύ των συναλλασσόμενων.

Αν και υπάρχει διαφάνεια ως προς τις συναλλαγές καθώς στο σύνολο τους αποθηκεύονται στην κατανεμημένη και αμετάβλητη βάση δεδομένων του blockchain ουσιαστικά σε αυτές αποθηκεύονται μόνο τα ψευδώνυμα δηλαδή των χρηστών (δηλαδή οι διευθύνσεις των πορτοφολιών τους) ενώ υπάρχει δυνατότητα χρήσης περισσότερων από ένα πορτοφολιών. Η αδυναμία σύνδεσης των χρηστών με τα ψευδώνυμα επιτρέπει την χρήση των συγκεκριμένων πλατφορμών για παράνομών και δόλιων διαδικασιών όπως αγοροπωλησίες παράνομών ουσιών και ξέπλυμα χρημάτων (Southurst, 2015; Peters, Panayi, 2016).

Η έντονη εξάρτηση των permissioned public blockchain πλατφορμών από τις τεχνολογίες της πληροφορικής και των δικτύων δημιουργούν είναι ένα μειονέκτημα των συγκεκριμένων πλατφορμών. Πιθανά τεχνικά προβλήματα στο δίκτυο ή περιπτώσεις κυβερνοεπιθέσεων είναι συχνό φαινόμενο. Επιπλέον, σε επίπεδο χρήστη η απώλεια των ιδιωτικών κλειδιών στα οποία αποθηκεύονται τα κρυπτονομίσματα μπορεί να οδηγήσει σε μη αντιστρέψιμη απώλειά τους (ECB, 2015; Peters, Panayi, Chappelle, 2016).

Ένα από τα βασικότερα προβλήματα των κρυπτονομισμάτων είναι έντονες αυξομειώσεις στην συναλλαγματική αξία των νομισμάτων. Όπως έχει ήδη αναλυθεί στο δεύτερο κεφάλαιο, η τιμή του Bitcoin (αλλά και γενικότερα στις περισσότερες περιπτώσεις κρυπτονομισμάτων) η συναλλαγματική τους αξία παρουσιάζει έντονες αυξομειώσεις. Συγκεκριμένα σε διάστημα λιγότερο των 2 μηνών (από 16 Δεκεμβρίου του 2017 μέχρι 5 Φεβρουαρίου του 2018) η συναλλαγματική του αξία έπεσε από τις 19.343,04$ στις 6.914,26$. Το ίδιο ισχύει και για τα κόστη συναλλαγής. Για την ίδια περίοδο παρατηρείται μία μείωση στο μέσο κόστος συναλλαγής από 26,893$ στα 6,193$.

Τέλος, η δυνατότητα εξερεύνησης και ελέγχου κάθε συναλλαγής μέσα στο δίκτυο είναι ένας περαιτέρω λόγος που αποτρέπει τα χρηματοπιστωτικά ιδρύματα την χρήση αυτής της κατηγορίας πλατφορμών για λόγους ιδιωτικότητας και προστασίας των συναλλαγών. Ο Peter και Panayi (2016) κάνουν αναφορά για την σημασία της διαθεσιμότητας, της ακεραιότητας και της ασφάλειας και της ιδιωτικότητα των δεδομένων σε εταιρίες και οργανισμούς. Η ιδωτικότητα των συναλλαγών δεν είναι ένα στοιχεία αυτής της κατηγορίας του blockchain, καθώς τα στοιχεία των συναλλαγών διαμοιράζονται σε όλους τους κόμβους του δικτύου, κάτι που θέτει σε κίνδυνο την ασφάλεια των πληροφοριών των συναλλαγών. Παράλληλα η διαθεσιμότητα των δεδομένων των συναλλαγών σε όλους τους κόμβους αυξάνει τον κίνδυνο ακεραιότητας των δεδομένων.

4.3.2 Public permissioned blockchain πλατφόρμες

4.3.2.1 Χαρακτηριστικά public permissioned blockchain πλατφορμών

Τα χαρακτηριστικά μιας public permissioned blockchain πλατφόρμας είναι τα εξής:

1. Η λειτουργία του βασίζεται σε ένα συγκεκριμένο διαχειριστή που είναι ο ιδιοκτήτης της (όπως αναλύθηκε στην περίπτωση του Ripple)

2. Βασίζεται, όπως και στην προηγούμενη κατηγορία, στην κρυπτογραφία για την μεταφορά, την αποθήκευση και την συναίνεση μεταξύ των κόμβων, υιοθετώντας ένα πρωτόκολλο το οποίο διαφέρει από το αντίστοιχο των permssionless πλατφορμών καθώς οι κόμβοι επικύρωσης είναι ορισμένοι από το ιδιοκτήτη.

3. Είναι πιθανή η χρήση εικονικών νομισμάτων για την μεταφορά αξίας αλλά όχι απαραίτητη.

4. Δεν υπάρχει ανταποδοτικό σύστημα σε όσους συμμετέχουν στην αποθήκευση και επικύρωση των συναλλαγών (τουλάχιστον όχι άμεσο όπως στην προηγουμενη περίπτωση).

5. Χρησιμοποιούν ένα λογισμικό το οποίο είναι ανοιχτού κώδικά και επιτρέπουν την συμμετοχή αλλά όχι την επικύρωση από τον καθένα.

6. Η διακυβέρνηση του συστήματος γίνεται από τον ιδιοκτήτη της πλατφόρμας.

7. Παρόλο που χρησιμοποιείται η τεχνολογία του δημόσιου/ιδιωτικού κλειδιού, η ανωνυμία είναι περιορισμένη γιατί οι πάροχοι των συγκεκριμένων κλειδιών για την συμμετοχή στο δίκτυο είναι ορισμένοι από τον ιδιοκτήτη και ακολουθούν τις διαδικασίες αναγνώρισης του πελάτη (Know your customer).

4.3.2.2 Πλεονεκτήματα χρήσης public permissioned blockchain πλατφορμών

Το βασικό πλεονέκτημα, όπως και στην προηγούμενη περίπτωση, είναι ότι πρόκειται για έτοιμες προς χρήση πλατφόρμες, που ωστόσο διεκπεραιώνουν τις συναλλαγές μέσα σε πολύ λίγα δευτερόλεπτα και με σχετικά χαμηλότερο κόστος σε σχέση με τις συμβατικές μεθόδους συναλλαγών, εφόσον ο χρήστης διαθέτει εφόσον διαθέτει πορτοφόλι δηλαδή ένα δημόσιο και ένα ιδιωτικό κλειδί. Παράλληλα επιτρέπει τις συναλλαγές εντός του δικτύου και άλλων νομισμάτων με την χρήση των πυλών (gateways) οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την έκδοση του ψηφιακού νομίσματος.

4.3.2.3 Μειονεκτήματα χρήσης public permissioned blockchain πλατφορμών

Τα μειονεκτήματα μιας public permissioned blockchain πλατφόρμας είναι αρκετά και έχουν να κάνουν κυρίως με την εμπιστοσύνη ως προς ιδιοκτήτη της συγκεκριμένης πλατφόρμας και την ασφάλεια των δεδομένων των συναλλαγών.

Η χρήση ενός εικονικού νομίσματός, για την επίτευξη των συναλλαγών, που δεν ελέγχεται από Κεντρική Αρχή και δεν υπόκειται σε κάποιο ρυθμιστικό πλαίσιο μπορεί να οδηγήσει σε καταστροφικές συνέπειες για τους χρήστες. Χαρακτηριστικά, οι αυξομειώσεις της συναλλαγματικής αξίας των νομισμάτων από πιθανή χειραγώγηση της αγοράς, αλλά και προβλήματα όπως η μη εγκεκριμένη αποστολή νομισμάτων ή η αποστολή εικονικών νομισμάτων σε λάθος χρήστη είναι αδύνατο να επιλυθούν λόγω της έλλειψης Κεντρικής Αρχής. Παράλληλα η δυσκολία ως προς την κατανόηση του τρόπου λειτουργίας και τη συμμετοχή σε πλατφόρμες κρυπτονομισμάτων ισχύει και σε αυτή την κατηγορία πλατφορμών.

Η πιθανότητα χρεωκοπίας ή κλοπής των εικονικών νομισμάτων, από ανταλλακτήρια που δεν διέπονται από κάποιο ρυθμιστικό πλαίσιο, υπάρχει και σε αυτή την περίπτωση όπως και η πιθανότητα απώλειας ή κλοπής των ιδιωτικών κλειδιών. Και στις δύο περιπτώσεις ο χρήστης οδηγείται σε μη αντιστρέψιμη απώλεια των εικονικών νομισμάτων. Επιπλέον χρήση των συγκεκριμένων πλατφορμών για συναλλαγές που σχετίζονται με παράνομες διαδικασίες είναι πιθανή και σε αυτή την περίπτωση. Αυτό συμβαίνει λόγω της αδυναμίας της ταυτοποίησης των χρηστών μέσα από την χρήση του δημόσιου/ιδιωτικού κλειδιού. Αν και πλατφόρμα του Ripple, που ανήκει στην συγκεκριμένη περίπτωση, δεν ενδείκνυται για τέτοιες χρήσεις (καθώς υπάρχουν άλλες πλατφόρμες της προηγούμενης κατηγορίας που διακρίνονται για την ανωνυμία των χρηστών τους) ο κίνδυνος είναι ορατός.

Καθώς ο ιδιοκτήτης της πλατφόρμας ορίζει συγκεκριμένου κόμβους για την επικύρωση των συναλλαγών, η λειτουργία και η σταθερότητα της πλατφόρμας είναι αρμοδιότητα του πάροχου. Επομένως τίθεται το θέμα της αξιοπιστίας ως προς πάροχο για την συνέχεια λειτουργίας του δικτύου. Αν και οι κόμβοι επικύρωσης δεν έχουν κάποιο οικονομικό κίνητρο όπως στην προηγούμενη περίπτωση, η «σύμβαση» για την λειτουργία των κόμβων επικύρωσης γίνεται με τον πάροχο της πλατφόρμας.

Τέλος, σε ότι αφορά την ακεραιότητα την ιδιωτικότητα των δεδομένων των συναλλαγών, στοιχείο που επιζητούν οι επιχειρήσεις και τα χρηματοπιστωτικά

ιδρύματα, το πρόβλημα συνεχίζει να υφίσταται όπως στην προηγούμενη περίπτωση καθώς τα δεδομένα αποστέλλονται σε όλους τους κόμβους επικύρωσης αλλά και στο ευρύ κοινό.

4.3.3 Private blockchain πλατφορμων

4.3.3.1 Χαρακτηριστικά private blockchain πλατφορμων

Τα χαρακτηριστικά μια private blockchain πλατφορμας είναι τα εξής:

1. Πρόκειται για «δομές» (frameworks) που εφαρμόζονται εντός ενός οργανισμού ή μεταξύ οργανισμών για την βελτίωση συγκεκριμένων διαδικασιών. Στην περίπτωση του εγχειρήματός Ubin ο αρχικός στόχος ήταν η δημιουργία μιας αποκεντρωμένης πλατφόρμας για την επίτευξη των διακανονισμών σε συνεχή χρόνο.

2. Χρησιμοποιείται και σε αυτή την περίπτωση πρωτόκολλα βασισμένα στην κρυπτογραφία για τις συναλλαγές και την επίτευξη συμφωνίας των συμμετεχόντων μέσα σε αυτό.

3. Δεν περιέχουν εικονικά νομίσματα όπως στις προηγούμενες κατηγορίες. Στην περίπτωση του Ubin δημιουργήθηκε ένα ψηφιακό νόμισμα που υπεύθυνη για την έκδοση του ήταν η Κεντρική Τράπεζα της Σιγκαπούρης και αντικατόπτριζε το συμβατικό νόμισμα.

4. Δεν υπάρχει ανταποδοτικό σύστημα για τους κόμβους επικύρωσης καθώς οι ίδιοι οι συμμετέχοντες αναλαμβάνουν την συγκεκριμένη διαδικασία.

5. Οι δομές που χρησιμοποιούν μπορεί να είναι ανοιχτού κώδικα, ωστόσο στις συγκεκριμένες υλοποιήσεις έχουν πρόσβαση μόνο οι συμμετέχοντες.

6. Η διακυβέρνηση του δικτύου γίνεται από τον χρήστη ή τους χρήστες που είναι υπεύθυνοι για την σταθερότητα και την εξέλιξή του.

7. Η χρήση κρυπτογραφίας για την ενίσχυση της ανωνυμίας δεν ισχύει σε αυτή την περίπτωση καθώς μιλάμε για ένα δίκτυο που δημιουργήθηκε από τους ίδιους τους χρήστες και δεν επιτρέπει την συμμέτοχη σε νέους χωρίς την έγκριση του διαχειριστή. Ωστόσο, ενδέχεται να χρησιμοποιηθεί για την ενίσχυση της ιδιωτικότητας των πληροφοριών των συναλλαγών (όπως συνέβη στην περίπτωση του εγχειρήματος Ubin, αποτρέποντας σε κάποιες περιπτώσεις τους μη συμμετέχοντες από τον έλεγχο των πληροφοριών των συναλλαγών).

4.3.3.2 Πλεονεκτήματα των private blockchain πλατφορμών

Η συγκεκριμένη κατηγορία αναφέρεται σε κλειστά δίκτυα, τα οποία έχουν ως στόχο να αντικαταστήσουν τα υπάρχοντα κεντρικά συστήματα των οργανισμών βελτιώνοντας πιθανά προβλήματα όπως σφάλματα που οφείλονται στην δομή ενός κεντρικού συστήματος, αυξάνοντας την διαλειτουργικότητα και την ταχύτητα των συναλλαγών. Επιπλέον, η ιδιωτικότητα και η ασφάλεια των πληροφοριών των συναλλαγών μεταξύ των συμμετεχόντων παραμένει σταθερή.

4.3.3.3 Μειονεκτήματα των private blockchain πλατφορμών

Τα μειονεκτήματα σε αυτή την περίπτωση πλατφορμών σχετίζονται κυρίως με την σύνδεση τους στο υπάρχον σύστημα των οργανισμών. Καθώς στις περισσότερες περιπτώσεις οι πλατφόρμες αυτές αντικαθιστούν κεντρικά συστήματα συγκεκριμένων διαδικασιών, όπως αναλύθηκε στο εγχείρημα Ubin, η προσαρμογή και η σύνδεση ενός κατανεμημένου δικτύου στα υπάρχοντα συστήματα μπορεί να παρουσιάσει αρκετές δυσκολίες. Συγκεκριμένα θα πρέπει να αναπτυχθεί ένα ρυθμιστικό πλαίσιο (όπως συμφωνίες σε επίπεδο παροχής υπηρεσιών μεταξύ των συμμετεχόντων και της Κεντρικής Τράπεζας της Σιγκαπούρης στο εγχείρημα Ubin) που να ορίζει τον τρόπο λειτουργίας της πλατφόρμας αλλά και την εγκυρότητα των συναλλαγών εντός αυτής. Επιπλέον η πιθανή μεγέθυνση ή τροποποίηση ενός κατανεμημένου δικτύου μπορεί να αυξήσει την πολυπλοκότητα των διαδικασιών. Σε αυτή την περίπτωση, η ταχύτητα των διαδικασιών μπορεί να μειωθεί αισθητά. Στην περίπτωση του Ubin το δίκτυο αποτελούταν από ένα περιορισμένο αριθμό τραπεζών (8 χρηματοπιστωτικά ιδρύματα), επιτρέποντας την διεκπεραίωση των συναλλαγών.

Για την λειτουργία και την χρήση ενός κατανεμημένου δικτύου οι οργανισμοί θα πρέπει να υιοθετήσουν νέες δεξιότητες σχετικές με το λογισμικό και τον εξοπλισμό που χρησιμοποιεί το κατανεμημένο δίκτυο. Συγκεκριμένα, απαιτούνται δεξιότητες σχετικές με τις τεχνολογίες πληροφοριών και με την κρυπτογραφία. Στην περίπτωση του εγχειρήματος Ubin, το ίδιο ισχύει και για την Κεντρική Τράπεζα της Σιγκαπούρης, η οποία είναι υπεύθυνη για την εύρυθμη λειτουργία και την εξέλιξη της πλατφόρμας. Παράλληλα, οι πάροχοι υπηρεσιών σύννεφου πρέπει να προσαρμόσουν τον εξοπλισμό τους για την εφαρμογή ενός κατανεμημένου δικτύου. Οι δομές σε αυτή την περίπτωση αναπτύσσονται από εταιρίες πληροφορικής ή εταιρίες συμβουλευτικής όπως η Accenture και η Deloitte. Επομένως, οι συγκεκριμένες εταιρίες πρέπει να αναπτύξουν

νέες δεξιότητες σχετικές με την δημιουργία δομών blockchain για κάθε περίπτωση εφαρμογής.

Τέλος σε ότι αφορά τους συμμετέχοντες, ανάπτυξη νέων δεξιοτήτων και το κόστος για την συμμετοχή σε ένα κατανεμημένο δίκτυο μπορεί να λειτουργήσει ως αντικίνητρο για την συμμετοχή τους σε αυτό. Ειδικότερα σε περιπτώσεις όπως του εγχειρήματος Ubin, η χρηστικότητα μιας private blockhain πλατφόρμας διαφέρει σε κάθε χρηματοπιστωτικό ίδρυμα με αποτέλεσμα η ανάπτυξη και η συμμετοχή τους κυρίως για μικρότερες επιχειρήσεις να θεωρείται ασύμφορη.

Στο παρακάτω πίνακα παρουσιάζονται τα κίνητρα και τα εμπόδια για την υιοθέτηση της blockchain τεχνολογίας στις τρεις κατηγορίες που αναλύθηκαν.

	Public permissionless blockchain		Public permissionless blockchain		Private blockchain	
Ζητήματα	Κίνητρα	Εμπόδια	Κίνητρα	Εμπόδια	Κίνητρα	Εμπόδια
Τεχνικά	• Έτοιμες προς χρήση πλατφόρμες • Αύξηση ταχύτητας διεκπεραίωσης των συναλλαγών (δυνατότητα)	• Χρήση τρίτων εφαρμογών για την συμμετοχή (πορτοφόλια, ανταλλακτήρια) • Μείωση ταχύτητας συναλλαγών λόγω μεγέθυνσης του δικτύου • Τεχνικά προβλήματα σχετικά με την σταθερότητα • Τεχνικές δυσκολίες για την χρήση τους από απλούς χρήστες	• Έτοιμες προς χρήση πλατφόρμες • Αυξημένη ταχύτητα και σταθερότητα σε σχέση με την προηγούμενη κατηγορία • Δυνατότητα συναλλαγών άλλων νομισμάτων	• Χρήση τρίτων εφαρμογών για την συμμετοχή (πορτοφόλια, ανταλλακτήρια) • Τεχνικά προβλήματα σχετικά με την σταθερότητα • Τεχνικές δυσκολίες για την χρήση τους από απλούς χρήστες	• Αύξηση ταχύτητας διεκπεραίωσης των συναλλαγών • Μείωση πιθανών προβλημάτων που δημιουργούνται στα υπάρχοντα κεντρικά συστήματα • Πιθανότητα αύξησης ταχύτητας των διασυνοριακών συναλλαγών	• Πρώιμο στάδιο της τεχνολογίας και των εργαλείων • Έλλειψη εξειδικευμένου προσωπικού στις επιχειρήσεις και στην αγορά • Προβλήματα σύνδεσης των υπαρχόντων συστημάτων με την νέα τεχνολογία • Πιθανά προβλήματα σε αλλαγές του δικτύου (μεγέθυνση, εξέλιξη)
Οικονομικά	• Δεν απαιτείται επιπλέον κόστος για την δημιουργία και εγκατάσταση • Χαμηλό κόστος διεκπεραίωσης συναλλαγών (δυνατότητα)	• Χειραγώγηση αγοράς • Ενεργειακά μη αποδοτική αρχιτεκτονική των μεγαλύτερων πλατφορμών • Υψηλό κόστος για την διεκπεραίωση μικρο-συναλλαγών	• Δεν απαιτείται επιπλέον κόστος για την δημιουργία και εγκατάσταση • Χαμηλό κόστος διεκπεραίωσης συναλλαγών (δυνατότητα)	• Χειραγώγηση αγοράς • Πιθανά ζητήματα αξιοπιστίας των συγκεκριμενών επιχειρήσεων	• Χαμηλό κόστος διεκπεραίωσης των συναλλαγών • Πιθανότητα μείωσης του κόστους των διασυνοριακών συναλλαγών	• Υψηλό κόστος δημιουργίας της πλατφόρμας • Υψηλό κόστος εγκατάστασης και λειτουργίας των κόμβων από τους συμμετέχοντες
Θεσμικά/ Νομικά	• Ιδιωτικότητα των συναλλαγών λόγω της ανωνυμίας • Νέες μορφές σύναψης συμβολαιακών σχέσεων	• Έλλειψη ρυθμιστικού πλαισίου • Έλλειψη Κεντρικής Αρχής • Συναλλαγές με δόλιο χαρακτήρα λόγω της ανωνυμίας • Προβλήματα ασφάλειας των δεδομένων των επιχειρήσεων	• Ιδιωτικότητα των συναλλαγών λόγω της ανωνυμίας • Νέες μορφές σύναψης συμβολαιακών σχέσων	• Έλλειψη ρυθμιστικού πλαισίου • Έλλειψη Κεντρικής Αρχής • Συναλλαγές με δόλιο χαρακτήρα λόγω της ανωνυμίας • Προβλήματα ασφάλειας των δεδομένων των επιχειρήσεων	• Αυξημένη ιδιωτικότητα των συναλλαγών • Νέες μορφές σύναψης συμβολαιακών σχέσεων	• Δημιουργία νέου ρυθμιστικού πλαισίου από τον διαχειριστή της πλατφόρμας (όπως συμφωνίες παροχής υπηρεσιών)

Πίνακας 4.10: Κινητρα και εμποδιά για την υιοθέτηση της τεχνολογίας του Blockchain (Ιδία επεξεργασία)

4.4 Η τεχνολογία του Blockchain ως καινοτομία

Βάσει των θεωριών της καινοτομίας που αναλύθηκαν στο πρώτο κεφάλαιο καταλήγουμε στο συμπέρασμα ότι τεχνολογία του blockchain είναι μία καινοτομία διαδικασιών καθώς επιτρέπει την επίτευξη συναλλαγών χωρίς την ύπαρξη κάποιου έμπιστου τρίτου προσώπου με την χρήση τεχνικών κρυπτογραφίας όπως ανέλυσε ο Nakamoto (2009). Η ύπαρξη διαφορετικών αρχιτεκτονικών σε κάθε κατηγορία υποδεικνύει σύμφωνα ότι δεν υπάρχει μέχρι στιγμής κάποιο κυρίαρχο μοντέλο σχεδιασμού. Στην συγκεκριμένη εργασία αναλύθηκαν εφτά διαφορετικές αρχιτεκτονικές εκ των οποίων οι τρείς «δομές» στην κατηγορία των private blockchain είναι αρθρωτές. Συμπερασματικά, βάσει της θεωρίας του Abernathy και Utterback (1978) βρισκόμαστε σε προπαραδειγματική φάση σε ότι αφορά την τεχνολογία και τις υλοποιήσεις της.

Στην περίπτωση των public permissionless blockchain οι πλατφόρμες που χρησιμοποιούν την τεχνολογία σε αυτή την περίπτωση προωθούνται και στηρίζονται από μη κερδοσκοπικούς οργανισμούς όπως το Ίδρυμα Bitcoin και το Ίδρυμα Ethereum. Σε αυτή την περίπτωση έχουμε καινοτομία σε επίπεδο οργανωσιακού μοντέλου καθώς δημιουργούνται νέοι μη κερδοσκοπικοί οργανισμοί που στηρίζουν τις πλατφόρμες των συναλλαγών. Οι συγκεκριμένες υπηρεσίες μέχρι την δημιουργία του Bitcoin παρέχονταν από επιχειρήσεις. Η έλλειψη περιορισμών σε ότι αφορά την χρήση των συγκεκριμένων πλατφορμών δίνει την δυνατότητα επίτευξης συναλλαγών από καταναλωτές που δεν είχαν πρόσβαση στους παραδοσιακούς παρόχους υπηρεσιών πληρωμών. Ωστόσο, βασισμένοι στην θεωρία του Christensen, δεν μιλάμε για μία ρηξικέλευθη καινοτομία νέας αγοράς. Οι ηλεκτρονικές πλατφόρμες συναλλαγών p2p με κεντρικό διαχειριστή υπάρχουν από τα τέλη της πρώτης δεκαετίας του 21^{ου} αιώνα όπως αναλύθηκε στο δεύτερο κεφάλαιο. Η βασική διαφορά των συμβατικών ηλεκτρονικών πλατφορμών όπως το Paypal, το Google wallet κλπ έγκειται στην διαδικασία επίτευξης και επικύρωσης των συναλλαγών. Επομένως σύμφωνα με την θεωρία του Christensen μιλάμε για μία ρηξικέλευθη καινοτομία χαμηλού επιπέδου.

Στην δεύτερη κατηγορία των public permissioned blockchain πλατφορμών, μέσα από την ανάλυση της περίπτωσης του Ripple, παρατηρείται καινοτομία σε επίπεδο επιχειρηματικού μοντέλου. Ουσιαστικά η εταιρία δημιούργησε ένα νέο

επιχειρηματικό μοντέλο για την εκμετάλλευση της τεχνολογίας. Αν και η συγκεκριμένη πλατφόρμα έχει το δικό της εικονικό νόμισμα, σε αντίθεση με τις προηγούμενες περιπτώσεις δίνεται η δυνατότητα συναλλαγών εντός της πλατφόρμας συμβατικών ή εικονικών νομισμάτων μέσα από συνεργαζόμενους πάροχους υπηρεσιών πληρωμών και χρηματοπιστωτικά ιδρύματα. Το συγκεκριμένο χαρακτηριστικό επιτρέπει τη σύνδεση των συστημάτων των χρηματοπιστωτικών ιδρυμάτων και των παροχών υπηρεσιών πληρωμών σε μία ενιαία κοινή πλατφόρμα βασισμένη στην τεχνολογία του blockchain. Η πρόταση αξίας του Ripple είναι η δυνατότητα ταχύτατων, ανιχνεύσιμων και χαμηλού κόστους πληρωμών σε παγκόσμιο επίπεδο με την χρήση της τεχνολογίας του blockchain. Η συγκεκριμένη περίπτωση εντάσσεται στην προηγούμενη κατηγορία p2p συναλλαγών.

Στην περίπτωση των private blockchain, μέσα από την ανάλυση που έγινε στο εγχείρημα Ubin παρατηρείται, οργανωσιακή καινοτομία καθώς δημιουργείται μία ενιαία πλατφόρμα για τις διατραπεζικές συναλλαγές, υπηρεσία που παρέχονταν από την Κεντρική Τράπεζα. Με την δημιουργία της πλατφόρμας, αλλάζει ο ρόλος της Κεντρικής Τράπεζας από κεντρικό πάροχο των υποδομών για την επίτευξη διατραπεζικών συναλλαγών σε επόπτη των διαδικασιών εντός κατανεμημένου δικτύου και υπεύθυνο για την εύρυθμη λειτουργεία του και την βελτίωση του δικτύου. Όπως και στις προηγούμενες κατηγορίες υπάρχει και εδώ καινοτομία διαδικασιών σε ότι αφορά τις διατραπεζικές συναλλαγές. Ως προς την έντασή της καινοτομίας σε αυτή την περίπτωση η χρήση της τεχνολογίας του blockchain δεν προκαλεί ρηξικέλευθη αλλά επαυξημένη καινοτομία καθώς μειώνει το κόστος, την πιθανότητα σφάλματος λόγω της έλλειψης ενός και διαχειριστή ενώ παράλληλα αυξάνει την ταχύτητα των διατραπεζικών συναλλαγών.

	Πλατφόρμες	Πεδίο καινοτομίας	Ένταση καινοτομίας
Blockchain *Καινοτομία διαδικασιών*	Public permissionless πλατφόρμες	Νέοι μη κερδοσκοπικοί οργανισμοί	Ρηξικέλευθη καινοτομία χαμηλού επιπέδου
	Public permissioned πλατφόρμες	Νέα επιχειρηματικά μοντέλα *Καινοτομία σε επίπεδο επιχειρηματικού μοντέλου*	Ρηξικέλευθη καινοτομία χαμηλού επιπέδου
	Private πλατφόρμες	Υπάρχουσες επιχειρήσεις *Οργανωσιακή καινοτομία*	Επαυξημένη καινοτομία

Πίνακας 4.11: Το blockchain ως καινοτομία σε κάθε κατηγορία (Ιδία επεξεργασία)

4.5 Τα συμπληρωματικά στοιχεία του ενεργητικού της τεχνολογίας του blockchain

Βάσει της θεωρίας του Teece (1996) τα συμπληρωματικά στοιχεία του ενεργητικού που απαιτεί η τεχνολογία του blockchain εντάσσονται σε δύο κατηγορίες σε άυλα και υλικά. Η πρώτη κατηγορία περιγράφει τις δεξιότητες και τις γνώσεις που απαιτούνται για την δημιουργία των αρχιτεκτονικών και του λογισμικού που απαιτείται για την δημιουργία μιας πλατφόρμας βασισμένη στην τεχνολογία του blockchain. Η δεύτερη κατηγορία αναφέρεται στον απαραίτητο εξοπλισμό που απαιτείται για την λειτουργία κάθε πλατφόρμας.

Για την περίπτωση των public permissionless blockchain για την αρχιτεκτονική και το λογισμικό του δικτύου υπεύθυνοι είναι οι μη κερδοσκοπικοί οργανισμοί σε κάθε δίκτυο. Ωστόσο καθώς σε αυτή την περίπτωση το λογισμικό είναι ανοιχτού κώδικα, είναι πιθανή και η συμβολή εθελοντών στην εξέλιξη της πλατφόρμας. Οι ικανότητες που απαιτούνται σε αυτή την περίπτωση σχετικές με τον κλάδο της πληροφορικής (μηχανικοί λογισμικών και μηχανικοί δικτύων) και της κρυπτογραφίας (μηχανικοί, πληροφορικάριοι ή ηλεκτρολόγοι μηχανικοί με εξειδίκευση στην κρυπτογράφηση δεδομένων). Για την επικύρωση και την αποθήκευση των συναλλαγών απαιτείται ο χώρος και η επεξεργαστική ισχύ των miners και γενικότερα των κόμβων αποθήκευσης. Για την αγορά εικονικών νομισμάτων οι χρήστες θα πρέπει να απευθυνθούνε στα ανταλλακτήρια εικονικών νομισμάτων. Τα ανταλλακτήρια, όπως έχει αναλυθεί είναι διαδικτυακές πλατφόρμες οι οποίες απαιτούν για την δημιουργία τους απαιτούνται δεξίοτητες σχετικές με τον κλάδο της πληροφορικής και της κρυπτογραφίας. Παράλληλα, απαιτείται ο αντίστοιχος εξοπλισμός, δηλαδή διακομιστές, για την αποθήκευση και την λειτουργία της. Τέλος, για την αποθήκευση των εικονικών νομισμάτων των χρηστών απαιτείται η χρήση πορτοφολιών δηλαδή ένα αποθετήριο του δημόσιου και του ιδιωτικού κλειδιού του χρήστη. Σε αυτή την περίπτωση τα συμπληρωματικά στοιχεία του ενεργητικού που απαιτούνται σε κάθε περίπτωση πορτοφολιού διαφέρουν. Συγκεκριμένα, στην περίπτωση των πορτοφολιών σε μορφή λογισμικού απαιτούνται δεξιότητες σχετικές με τον κλάδο της πληροφορικής και της κρυπτογραφίας. Στην περίπτωση που το πορτοφόλι είναι σε μορφή εξοπλισμού (όπως μονάδα usb) τότε απαιτούνται επιπλέον δεξιότητες σε ότι αφορά την δημιουργία του εξοπλισμού πέρα από την ανάπτυξη του λογισμικού.

Στην περίπτωση των public permissioned blockchain τα συμπληρωματικά περιουσιακα στοιχεία παρέχονται από τους ίδιους «παρόχους» με της κατηγορίας public permissionless blockchain πλατφορμών. Η μόνη διαφορά έγκειται στους κόμβους επικύρωσης, οι οποίοι ορίζονται από τον πάροχο της πλατφόρμας.

Στην περίπτωση των private blockchain πλατφορμών, οι αρχιτεκτονικές και το λογισμικό για την δημιουργία της πλατφόρμας παρέχονται είτε από εξειδικευμένες εταιρίες πληροφορικής πάνω στην συγκεκριμένη τεχνολογία (η BCS στην περίπτωση του Ubin) είτε από εταιρίες συμβουλευτικής όπως η Delloite και η Accenture (στο πρώτη και στην δεύτερη φάση του εγχειρήματος Ubin αντίστοιχα) που κατέχουν τις αντίστοιχες σε ικανότητες σχετικές με τους κλάδους της πληροφορικής και της κρυπτογραφίας. Καθώς μιλάμε για ένα κλειστό δίκτυο, η αποθήκευση και η επικύρωση των συναλλαγών καθώς και η χρήση της πλατφόρμας γίνονται από τους ίδιους τους συμμετέχοντες. Επομένως η αποθήκευση νομισμάτων γίνεται απευθείας στο κόμβο κάθε χρήστη, χωρίς να απαιτείται η χρήση πορτοφολιού ως υπηρεσία που παρέχεται από «τρίτους». Το ίδιο ισχύει και για την περίπτωση των ανταλλακτηρίων. Σε, ότι αφορά τις δεξιότητες, στην περίπτωση του Ubin, καθώς τα χρηματοπιστωτικά ιδρύματα και η Κεντρική Τράπεζα της Σιγκαπούρης είναι υπεύθυνα για την λειτουργία και την συντήρηση των κόμβων που χρησιμοποιούν, θα πρέπει να αποκτήσουν εξειδικευμένο προσωπικό με τα αντίστοιχες ικανότητες που προαναφέρθηκαν. Παράλληλα, οι πάροχοι υπηρεσιών σύννεφου θα πρέπει να αναδιαμορφώσουν τις υπηρεσίες τους έτσι ώστε να είναι δυνατή η εγκατάσταση των κόμβων ενός κλειστού δικτύου. Στην περίπτωση του Ubin, η Microsoft παρέχει αυτές τις υπηρεσίες σύννεφου έχοντας δημιουργήσει αντίστοιχα εργαλεία για την εγκατάσταση blockchain δικτύων.

Για την λειτουργία των πλατφορμών και στις τρεις κατηγορίες απαιτείται η χρήση η σύνδεσή τους διαδίκτυο. Επομένως, ως συμπληρωματικό στοιχείο του ενεργητικού θεωρείται και το διαδίκτυο που παρέχεται από τους εταιρίες παροχής διαδικτύου. Στον παρακάτω πίνακα απεικονίζονται όλα τα συμπληρωματικά στοιχεία του ενεργητικού που απαιτούνται για την λειτουργία μιας πλατφόρμας στο δίκτυο του blockchain σε κάθε κατηγορία.

		Public permissionless blockchain			Public permissioned blockchain			Private blockchain	
Συμπληρωματικά στοιχεία του ενεργητικού και βαθμός εξάρτησης	Πάροχοι	Υλικά	Άυλα	Πάροχοι	Υλικά	Άυλα	Πάροχοι	Υλικά	Άυλα
Αρχιτεκτονική του δικτύου	Μη κερδοσκοπικοί οργανισμοί και εθελοντές		Δεξιότητες στην πληροφορική και κρυπτογραφία (Λογισμικό) Εξειδικευμένα	Οι εταιρίες υπεύθυνες για την διαχείριση της πλατφόρμας		Δεξιότητες στην πληροφορική και κρυπτογραφία (Λογισμικό) Εξειδικευμένα	Εταιρίες πληροφορικής και εταιρίες συμβουλευτικής		Δεξιότητες στην πληροφορική και κρυπτογραφία Εξειδικευμένα
Αποθήκευση και Επικύρωση συναλλαγών	Ανεξάρτητα άτομα	Υπολογιστές και σκληροί δίσκοι Γενικά		Οργανισμοί ορισμένοι από την εταιρία διαχείρισης	Υπολογιστές και σκληροί δίσκοι Γενικά		Πάροχοι υπηρεσιών σύννεφου	Υπηρεσίες σύννεφου προσαρμοσμένες για την τεχνολογία Αμοιβαία εξειδικευμένα	
Αποθήκευση νομισμάτων χρηστών	Επιχειρήσεις παροχής πορτοφολιών		Δεξιότητες στην πληροφορική και κρυπτογραφία και στην δημιουργία του αντίστοιχου εξοπλισμού Εξειδικευμένα και Αμοιβαία εξειδικευμένα	Επιχειρήσεις παροχής πορτοφολιών		Δεξιότητες στην πληροφορική και κρυπτογραφία και στην δημιουργία του αντίστοιχου εξοπλισμού Εξειδικευμένα και Αμοιβαία εξειδικευμένα	-	-	-
Αγορά εικονικών νομισμάτων	Ανταλλακτήρια	Διακομιστές Γενικά	Δεξιότητες στην πληροφορική και κρυπτογραφία Εξειδικευμένα	Ανταλλακτήρια	Διακομιστές Γενικά	Δεξιότητες στην πληροφορική και κρυπτογραφία Εξειδικευμένα	-	-	-

Πίνακας 4.12: Συμπληρωματικά στοιχεία του ενεργητικού σε κάθε κατηγορία της blockchain τεχνολογίας (Ιδία επεξεργασία)

4.6 Συμπεράσματα

Σε αυτό το κεφάλαιο αναλύθηκαν το πιλοτικό εγχείρημα Ubin, μέσα από το οποίο δημιουργήθηκε μια πλατφόρμα διατραπεζικών συναλλαγών αντικαθιστώντας το υπάρχων κεντρικό σύστημα. Αν και η συγκεκριμένη υλοποίηση του εγχειρήματος κρίνεται επιτυχημένη, τίθενται ζητήματα των νέων δεξιοτήτων που πρέπει να αποκτήσουν οι τράπεζες, του κόστους που επωμίζονται για την λειτουργία και την συντήρησης του δικτύου και πρακτικών ζητημάτων που η Κεντρική Τράπεζα της Σιγκαπούρης που πρέπει να λύσει. Με την χρήση της πλατφόρμας αλλάζει ο ρόλος της Κεντρικής Τράπεζας από κεντρικό πάροχο του συστήματος διατραπεζικών συναλλαγών σε επόπτη του κατανεμημένου δικτύου και υπεύθυνο για την αναβάθμισή του. Στην συνέχεια αναλύθηκαν τα βασικά χαρακτηριστικά κάθε περίπτωσης, τα κίνητρα και τα εμπόδια από την υιοθέτησή τους και τα συμπληρωματικά στοιχεία του ενεργητικού για την εγκατάσταση, την λειτουργία και την χρήση τους. Συμπερασματικά το blockchain θεωρείται μία καινοτομία διαδικασιών. Στην περίπτωση των public permissionless blockchain η διακυβέρνηση γίνεται από μη κερδοσκοπικούς οργανισμούς κάτι που έρχεται σε αντίθεση με τις υπάρχοντα επιχειρηματικά μοντέλα p2p συναλλαγών. Στην περίπτωση των public permissioned blockchain πλατφορμών παρατηρείται ένα νέο επιχειρηματικό μοντέλο, αυτό του Ripple, το οποίο δημιουργείται για την εκμετάλλευση της τεχνολογίας. Και στις δύο περιπτώσεις η καινοτομία αξιολογείται ως ρηξικέλευθη καινοτομία χαμηλού επιπέδου σύμφωνα με την θεωρία του Christensen. Τέλος στην τρίτη κατηγορία των private blockchain, μέσα από την ανάλυση του εγχειρήματος Ubin, η blockchain τεχνολογία κατάφερε να μειώσει το κόστος των διατραπεζικών συναλλαγών δημιουργώντας μία πλατφόρμα που επιτρέπει τις διατραπεζικές συναλλαγές καθ’ όλη την διάρκεια της μέρας. Επομένως, σε αυτή την περίπτωση η καινοτομία χαρακτηρίζεται ως επαυξημένη καθώς βελτιώνει την συγκεκριμένη διαδικασία.

Κεφάλαιο 5: Συμπεράσματα και προτάσεις για μελλοντική ερευνα

5.1 Συμπεράσματα

Στην παρούσα διπλωματική μελετήθηκε η τεχνολογία του blockchain ως μία καινοτομία στο στάδιο των συναλλαγών μέσα από τις τρείς βασικές κατηγορίες που την απαρτίζουν ενώ παράλληλα αναλύθηκαν τα βασικά συμπληρωματικά στοιχεία του ενεργητικού για την κάθε περίπτωση. Στην ανάλυση χρησιμοποιήθηκαν τέσσερις μελέτες περιπτώσεις. Η περίπτωση του Bitcoin και του Ethereum ανήκουν στην κατηγορία των public permissionless blockchain πλατφορμών. Η εταιρεία Ripple ανήκει στην δεύτερη κατηγορία των public permissioned blockchain πλατφορμών. Τέλος το πιλοτικό εγχείρημα Ubin ανήκει στην τρίτη κατηγορία private blockchain πλατοφρμών. Οι διαφορετικές αρχιτεκτονικές των πλατφορμών αποδεικνύουν ότι δεν υπάρχει ένα κυρίαρχο μοντέλο σχεδίασης της τεχνολογίας. Επομένως βρισκόμαστε σε ένα προπαραδειγματικό στάδιο σε ότι αφορά την σχεδίαση των πλατφορμών.

Η έλλειψη Κεντρικής Αρχής που να καθορίζει την λειτουργία τους, η ανωνυμία, δυσκολία κατανόησης της λειτουργίας του χρήστη, η χειραγώγηση της αγοράς των νομισμάτων και η έλλειψή ρυθμιστικού πλαισίου είναι μερικά από τα εμπόδια για την υιοθέτηση των permissionless blockchain πλατφορμών. Στην δεύτερη κατηγορία των public permissionless blockchain πλατφορμών το βασικότερο ζήτημα είναι αυτό αξιοπιστίας ως προς τον πάροχο της υπηρεσίας καθώς σε αυτές τις περιπτώσεις η διαχείριση της πλατφόρμας γίνεται κεντρικά. Στην τρίτη κατηγορία των private blockchain πλατφορμών τα βασικότερα προβλήματα που θα πρέπει να αντιμετωπιστούν είναι αυτά της σύνδεσης με τα υπάρχοντα πληροφοριακά συστήματα, του κόστους για την δημιουργία και την συντήρηση των δικτύου και των κόμβων των συμμετεχόντων και των νέων δεξιοτήτων που θα πρέπει να αποκτήσουν τα χρηματοπιστωτικά ιδρύματα μέσα από την απόκτηση του εξειδικευμένου προσωπικού.

Η τεχνολογία του blockchain αξιολογήθηκε, ως μία καινοτομία διαδικασιών. Ως προς την έντασή της, στην πρώτη και στην δεύτερη κατηγορία χαρακτηρίζεται ως ριξικέλευθη καινοτομία χαμηλού βαθμού δημιουργώντας νέους μη κερδοσκοπικούς οργανισμούς και νέα επιχειρηματικά μοντέλα αντίστοιχα, ενώ στην τρίτη περίπτωση ως επαυξημένη καινοτομία καθώς βελτιώνει τις διαδικασίες των διατραπεζικών συναλλαγών. Τέλος τα συμπληρωματικά στοιχεία του ενεργητικού σε κάθε περίπτωση διαφέρουν. Στην πρώτη κατηγορία απαιτούνται κόμβοι επικύρωσης που παρέχονται

από τους miners, επιχειρήσεις παροχής πορτοφολιών και ανταλλακτήρια για την χρήση των πλατφορμών. Στην δεύτερη, καθώς οι κόμβοι επικύρωσης είναι ορισμένοι από τον πάροχο, απαιτούνται μόνο οι επιχειρήσεις παροχής πορτοφολιών και ανταλλακτήρια για την χρήση τους. Στην τρίτη κατηγορία των private permissioned blockchain απαιτούνται επιχειρήσεις με τεχνογνωσία για την δημιουργία και την εγκατάσταση του δικτύου και του αντίστοιχου εξοπλισμού όπως και εταιρείες παροχής υπηρεσιών σύννεφου.

Κλείνοντας, με την ολοκλήρωση της διπλωματικής εργασίας θεωρείται κρίσιμο να ένα βασικό ζήτημα. Καθώς η τεχνολογία του blockchain εξελίσσεται, για την επιτυχημένη εφαρμογή της απαιτούνται μία σειρά νέων δεξιοτήτων που πρέπει να αποκτηθούν από τις επιχειρήσεις. Πέρα από τις τεχνικές δεξιότητες που απαιτούνται για την υλοποίηση και εγκατάσταση των δικτύων, απαραίτητες είναι και οι ικανότητες σχετικές με την αναγνώριση των ωφελειών από την χρήση της συγκεκριμένης τεχνολογίας, των πλαισίων εφαρμογής της και του πιθανού ρίσκου που αναλαμβάνουν οι επιχειρήσεις σε κάθε περίπτωση. Οι συγκεκριμένες ικανότητες απαιτούν την πλήρη κατανόηση της τεχνολογίας και των αλλαγών που μπορεί να επιφέρει.

5.2 Προτάσεις για μελλοντική έρευνα

Λόγω του πρώιμου σταδίου της τεχνολογίας, οι εφαρμογές της τεχνολογίας είναι περιορισμένες. Αν και στην κατηγορία public permissionless blockchain πλατφορμών υπάρχουν ήδη αρκετά εγχειρήματα, στις άλλες δύο κατηγορίες οι εφαρμογές είναι περιορισμένες. Σε επόμενες μελέτες, θα μπορούσε να αναλυθεί ο τρόπος εφαρμογής της τεχνολογίας και σε άλλους κλάδους ή επιχειρήσεις για την μελέτη των συμπερασμάτων σε αυτές τις περιπτώσεις. Ακόμη και σε θεωρητικό επίπεδο, η βιβλιογραφία αυτή την στιγμή είναι γενική και περιορισμένη. Θα είχε επίσης ενδιαφέρον η ανάλυση των επόμενων φάσεων του εγχειρήματος Ubin καθώς και άλλων εγχειρημάτων Κεντρικών Τραπεζών όπως το εγχείρημα Jasper.

Βιβλιογραφία

Abernathy, W. J. (1978). Patterns of industrial innovation. *Technology review, 80(7)*, 40-47.

Accenture, Monatery Authority Of Singapore. (2017). Project Ubin Phase 2: Re-imagining Interbank Real Time Gross Settlement System Using Distributed Ledger Tecnhlogoies.

Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM computing surveys (CSUR), 36*(4), 335–371.

Angela S.M. Irwin and George Milad. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, 19*(4), 407-425.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media, Inc.

Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. *Geo. J. Int'l L., 47, 1271*.

Assink, M. (2006). Inhibitors of disruptive innovation capability: a conceptual model. *European Journal of Innovation Management, 9(2)*, 215-233.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Bitcoin Magazine. (2018). *What are bitcoin wallets?* Ανάκτηση από Bitcoin Magazine: https://bitcoinmagazine.com/guides/what-are-bitcoin-wallets/

Buterin, V. (2014). Ethereum White Paper. *Github Repository*.

Buterin, V. (2015). *On public and private blockchains*. Ανάκτηση από Ethereum Blog: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Castillo, M. d. (2017, July 17). *Ripple's Distributed Ledger Network Passes 50-Validator Milestone.* Ανάκτηση από Coindesk: https://www.coindesk.com/ripples-distributed-ledger-network-passes-50-validator-milestone/

Christensen, C. M., Anthony, S. D., & Roth, E. A. (2004). *Seeing what's next: Using the theories of innovation to predict industry change.* Using the theories of innovation to predict industry change.

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

Cohen, D., Schwartz, D., Britto, A. (2014). *The XRP Ledger Consensus Process.* Ανάκτηση από Ripple: https://ripple.com/build/xrp-ledger-consensus-process/

Damanpour, F. &. (2006). Research on innovation in organizations: Distinguishing innovation-generating from innovation-adopting organizations. . *Journal of engineering and technology management, 23(4)*, 269-291.

Delloitte, Monetary Authority of Singapore. (2016). Project Ubin: SGD on Distributed Ledger - Phase 1.

Dietz, M., Khanna, S.,Olanrewaju, T.,Rajgopal K. (2016, February). *Cutting through the noise around financial technology.* Ανάκτηση από Mckinsey: https://www.mckinsey.com/industries/financial-services/our-insights/cutting-through-the-noise-around-financial-technology

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 644-654.

Dinkins, D. (2017, December 7). *Steam Stops Accepting Bitcoin Payments Citing Extreme Volatility, Fees.* Ανάκτηση από Cointelegraph: https://cointelegraph.com/news/steam-stops-accepting-bitcoin-payments-citing-extreme-volatility-fees

Euro Banking Association. (2015). Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios. An exploration for transaction banking and payments professionals. *EBA Working Group on Electronic and Alternative Payments, 5*(11).

European Central Bank. (2015). Virtual currency schemes – a further analysis.

European Commission. (1996). *Green Paper on Innovation.* Luxemburg: European Commission.

Evans, D. (2014). Economic aspects of bitcoin and other decentralized public-ledger currency platforms.

Gonzalez, R. (2016). Lending (Capital) in 21st Century. Στο *Lending (Capital) in the 21st Century.The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries* (σσ. 25-27).

Haber S., Stonertta S. W. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology, 3*(2), 99-111.

Harris, M. (2018, February 26). *Napster history.* Ανάκτηση από Lifewire: https://www.lifewire.com/history-of-napster-2438592

Hertig, A. (2016). *What is a DAO?* Ανάκτηση από Coindesk: https://www.coindesk.com/information/what-is-a-dao-ethereum/

Hertig, A. (2017, December 11). *Ethereum's Two Ethereums Explained*. Ανάκτηση από Coindesk: https://www.coindesk.com/ethereum-classic-explained-blockchain/

Hileman, G., Rauchs, M. (2017). Global Cryptocurrency Benchmarking Study.

Hulme, M. K. (2006). Internet based social lending: Past, present and future. *Social Futures Observatory, 115.*

Hyperledger Fabric Model. (2017). Ανάκτηση από Hyperledger: https://hyperledger-fabric.readthedocs.io/en/release-1.1/fabric_model.htmlHy

Insights, M. (2015, June 25). *Survey Shows Americans Trust Technology Firms More Than Banks and Retailers*. Ανάκτηση από Medici: https://gomedici.com/survey-shows-americans-trust-technology-firms-more-than-banks-and-retailers/

Liu, J., Kauffman, R. J., & Ma, D. (2015). Competition, cooperation, and regulation: Understanding the evolution of the mobile payments technology ecosystem. *Electronic Commerce Research and Applications, 14(5)*, 372-391.

Menat, R. (2016). Why We're so Excited About FinTech. Στο *The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries*, (σσ. 10-12).

Menezes, A. J., Katz, J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium* (σσ. 122-122). IEEE.

Mills, D., Wang, K., Malone, B., Ravi A.,Marquardt J., Chen, Badev, A., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellirhorpe, M., Ng, W., Baird, M. (2016). Distributed ledger technology in payments, clearing, and settlement. *Finance and Economics Discussion Series, Washington: Board of Governors of the Federal Reserve System*.

Morgan, J. P. (2016). Quorum Whitepaper. *New York: JP Morgan Chase*.

Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.

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

Nielsen, P. M. (2017). ZSL Proof of Concept. *Github Repository*.

Oecd, Eurostat. (2005). Guidelines for Collecting and Interpreting Innovation Data.

Peters, G. W. (2016). Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective. *Journal of Banking Regulation, 17(4)*, 239-272.

Peters, G. W. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Στο *In Banking Beyond Banks and Money* (σσ. 239-278). Springer, Cham.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Στο *Banking Beyond Banks and Money* (σσ. 239-278). Springer, Cham.

Peters, G. W., Chapelle, A., & Panayi, E. (2016). pening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective. *Journal of Banking Regulation, 17(4)*, 239-272.

R3. (2018). *Corda docs*. Ανάκτηση από Corda R3: https://docs.corda.net

Raft-based consensus for Ethereum/Quorum 2017. (2017). Ανάκτηση από Github Repository: https://github.com/jpmorganchase/quorum/blob/master/raft/doc.md

Rathi, A. (2015). *Is it worth worrying about bitcoin's growing electricity use?* Ανάκτηση από Quartz: https://qz.com/1281850/bitcoins-energy-consumption-is-as-much-a-year-as-all-of-ireland-says-the-first-peer-reviewed-study-on-the-subject/

Ripple. (2015). *Reserves.* Ανάκτηση από Ripple: https://developers.ripple.com/reserves.html

Ripple. (2015). *Transaction Cost.* Ανάκτηση από Ripple: https://developers.ripple.com/transaction-cost.html

Ripple. (2018, May 6). *XRP Maket Performance.* Ανάκτηση από Ripple: https://ripple.com/xrp/market-performance/

Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*(5).

Schwienbacher, A. L. (2010). Crowdfunding of small entrepreneurial ventures. *HANDBOOK OF ENTREPRENEURIAL FINANCE*.

Shin, L. (2017, October 23). *Will This Battle For The Soul Of Bitcoin Destroy It?* Ανάκτηση από Forbes: https://www.forbes.com/sites/laurashin/2017/10/23/will-this-battle-for-the-soul-of-bitcoin-destroy-it/#16f973c03d3c

Southurst, J. (2014, December 3). *Australian Federal Investigators Look at Bitcoin's Organized Crime Role*. Ανάκτηση από Coindesk: https://www.coindesk.com/australian-federal-investigators-look-bitcoins-organized-crime-role/

Souto, J. E. (2015). Business model innovation and business concept innovation as the context of incremental innovation and radical innovation. *Tourism Management, 51*, 142-155.

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

Swatman, P. M., & Swatman, P. A. (1992). EDI system integration: A definition and literature survey. *The Information Society, 6*(9).

Szabo, N. (1994). Smart contracts. *Unpublished manuscript.*

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

Szabo, N. (1998). Secure Property Titles with Owner Authority.

Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research policy, 15(6)*, 285-305.

Teece, D. J. (2010). Business models, business strategy and innovation. Long range planning. *Long range planning, 43(2-3)*, 172-194.

The World Bank. (2018). *Commercial bank branches (per 100,000 adults)*. Ανάκτηση από International Monetary Fund, Financial Access Survey: https://data.worldbank.org/indicator/FB.CBK.BRCH.P5

Tidd, J. (. (2001). Innovation management in context: environment, organization and performance. *International Journal of Management Reviews, 3(3)*, 169-183.

Vanian, J. (2018, January 10). *Microsoft Welcomes Back Bitcoin.* Ανάκτηση από Fortune: http://fortune.com/2018/01/10/microsoft-bitcoin-temporary-halt/

Vili Lehdonvirta . (2016). Governance and Regulation. *UK Government Office for Science*, 41-45.

Walport, M. G. C. S. A. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*.

Waters, R. (2016, May 17). *Automated company raises equivalent of $120M in digital currency*. Ανάκτηση από CNBC: https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM, 58*(9), 104-113.