ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

« Διοίκηση Επιχειρήσεων – Μάνατζμεντ Τουρισμού (MBA – Tourism Management*)* »

ΤΙΤΛΟΣ ΕΡΓΑΣΙΑΣ

«ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ,ΑΠΟΚΕΝΤΡΩΣΗ ΚΑΙ ΧΡΗΣΗ ΤΗΣ BLOCKCHAIN ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΟ ΣΥΓΧΡΟΝΟ ΟΙΚΟΝΟΜΙΚΟ ΠΕΡΙΒΑΛΛΟΝ»

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΦΙΛΙΠΠΑΣ ΝΙΚΟΛΑΟΣ

ΜΠΡΑΤΣΙΑΚΟΣ ΝΙΚΟΛΑΟΣ

ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ: ΔΕΜΤ1623

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών,του Πανεπιστημίου Πειραιώς,στη **Διοίκηση Επιχειρήσεων : Μάνατζμεντ Τουρισμού – (MBA-Tourism Management)»** με τίτλο :

«Κρυπτονομίσματα,αποκέντρωση και χρήση της Blockchain τεχνολογίας στο σύγχρονο οικονομικό περιβάλλον» έχει συγγραφεί από εμένα προσωπικά και στο σύνολο της.Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών,στην Ελλάδα ή στο εξωτερικό,ούτε είναι εργασία ή τμήμα εργασίας ακαδημαικού ή επαγγελματικού χαρακτήρα. Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας,αναφέρονται στο σύνολό τους,κάνοντας πλήρη αναφορά στους συγγραφείς,τον εκδοτικό οίκο ή το περιοδικό,συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.Παράβαση της ανωτέρω ακαδημαικής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Υπογραφή Μεταπτυχιακού Φοιτητή Ονοματεπωνυμο:

Νικόλαος Μπρατσιάτος

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας,θα ήθελα αρχικά να αναφερθώ στην δυνατότητα που μου δόθηκε να ερευνήσω ένα τόσο σημαντικό κομμάτι της τεχνολογίας και συνάμα της οικονομίας.Η περίοδος ενασχόλησης μου στον τομέα του Blockchain,με σκοπό την εκπόνηση της παρακάτω εργασίας,αποτελεί αδιαμφισβήτητα μια απ' τις πιο ενδιαφέρουσες περιόδους της ζωής μου.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Νικόλαο Φίλιππα, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση και τη συνεχή του υποστήριξη .Τέλος,θα ήθελα να ευχαριστήσω,από καρδιάς,τους γονείς μου Ιωάννη και Αλεξάνδρα για την υποστήριξη τους.

Περίληψη

Η θεωρία των αποκεντρωμένων κρυπτονομισμάτων (π.χ. Bitcoin και Altcoins) έχει αποκτήσει γρήγορα αναγνώριση. Ενώ η τεχνολογία του Bitcoin έχει μελετηθεί εκτενώς, πιστεύουμε ότι η έννοια του blockchain παρέχει μια νέα προοπτική για την ήδη υπάρχουσα βιβλιογραφία, εξετάζοντας τις διάφορες εφαρμογές της υποκείμενης τεχνολογίας σε ένα κοινωνικοοικονομικό περιβάλλον. Το Blockchain αντιπροσωπεύει μια νέα εφαρμογή στην κρυπτογραφία και την τεχνολογία της πληροφορίας. Οι ερευνητές συμφωνούν ότι η τεχνολογία Blockchain έχει ορισμένα χαρακτηριστικά που εφαρμόζονται σωστά στο χρηματοπιστωτικό τομέα. Στην παρούσα εργασία διεξήχθη μια αντιπροσωπευτική βιβλιογραφική επισκόπηση των σημερινών θεμάτων στην έρευνα blockchain,συζητήθηκαν κάποιες μελλοντικές επιπτώσεις και δόθηκαν κάποιες συστάσεις προς μελλοντική εφαρμογή. Λαμβάνοντας υπόψη το εύρος των ανοιχτών ερωτημάτων, δείξαμε πού η έρευνα μπορεί να επωφεληθεί από τις πολυεπιστημονικές συνεργασίες και τις υπάρχουσες πηγές δεδομένων ως σημεία εκκίνησης για εμπειρικές έρευνες με βάση το blockchain

Λέξεις κλειδιά: Κρυπτονομίσματα, blockchain

Abstract

The theory of decentralized cryptocurrencies (eg Bitcoin and Altcoins) has gained rapid recognition. While Bitcoin technology has been extensively studied, we believe that the concept of blockchain provides a new perspective for existing literature by looking at the different applications of the underlying technology in a socio-economic environment. Blockchain represents a new application in cryptography and information technology. The researchers agree that Blockchain technology has some features that are well applied in the financial sector. A representative bibliographic review of current issues in blockchain research was conducted in this paper and some future impacts were discussed and some recommendations were made for future implementation. Taking into account the breadth of open questions, we have shown where research can benefit from multidisciplinary collaborations and existing data sources as starting points for empirical research based on the blockchain

Key words: Cryptocurrency, blockchain

Πίνακας Περιεχομένων

ΠΕΡΙΛΗΨΗ ..... **IV**
ABSTRACT ..... **V**
ΕΙΣΑΓΩΓΗ **6**
ΚΕΦΑΛΑΙΟ 1. ΕΞΕΛΙΞΗ ΝΟΜΙΣΜΑΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗ ΧΡΗΜΑΤΟΣ **10**
1.1 Συστήματα πληρωμών 10
1.2 Νομισματικές πολιτικές 12
1.3 Κεντροποίηση 13
1.4. Κατηγοριοποίηση χρημάτων 14
1.5. Οι ρόλοι των χρημάτων 15
1.6. Αποεκντροποιημένη Τραπεζική: νομισματική τεχνοκρατία στην ψηφιακή εποχή 18
1.6.1. Κανόνες Τραπεζικής 18
1.6.2 Η τεχνοκρατία μέσω της αποκεντρωμένης Τραπεζικής 23
ΚΕΦΑΛΑΙΟ 2. ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ **25**
2.1. Εισαγωγή 25
2.2. Τι είναι ένα κρυπτονόμισμα 30
2.3. Κρυπτονομίσματα απο την κεντροποίηση στην αποκεντροποίηση 32
2.4. Bitcoin 33
2.4.1 Εξέλιξη και αποδοχή 36
2.4.2 Ο ρόλος του χρήματος και η ρύθμιση 38
2.4.3 Κατηγοριοποίηση 39
2.4.4 Επένδυση 40
2.5. Άλλα κρυπτονομίσματα 40
2.5.5 Διαφοροποίηση απο τα παραστατικά χρήματα 43
2.6. Πλεονεκτήματα και μειονεκτήματα κρυπτονομισμάτων 47
ΚΕΦΑΛΑΙΟ 3. ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN **49**
2.1 Οι βασικές έννοιες του blockchain 50
2.1.1. Συμμετέχοντες 54
2.1.2 Επικύρωση και συναίνεση 55
2.2 Αρχιτεκτονική δομή του blockchain 57
2.2.1 Block 57
2.2.2 Ψηφιακή Υπογραφή 58
2.2.3 Αποκεντρωμένο Δίκτυο 58
2.3. Εφαρμογή του blockchain 59
2.3.1 Οικονομικές εφαρμογές 59
2.3.2 Μη-οικονομικές εφαρμογές 61
2.4 Προκλήσεις χρήσης του blockchain 62
2.5 Εφαρμογές με χρήση blockchain 64
2.5.1. Οικονομικές εφαρμογές 65
2.5.2. Επαλήθευση ακεραιότητας 67
2.5.3 Διακυβέρνηση 69

2.5.4 Διαχείριση υπηρεσιών υγείας 71
2.5.5 Επιχειρηματικές και βιομηχανικές εφαρμογές 72
2.5.6. Διαχείριση αλυσίδας εφοδιασμού 72
2.5.7. Ενεργειακός τομέας 73
ΚΕΦΑΛΑΙΟ 4. ΣΥΜΠΕΡΑΣΜΑΤΑ 75
ΒΙΒΛΙΟΓΡΑΦΙΑ 77

ΕΙΣΑΓΩΓΗ

Σχεδόν μια δεκαετία πριν, ο άγνωστος άνθρωπος / ομάδα πίσω από τον Bitcoin, Satoshi Nakamoto, περιγράφει πώς η τεχνολογία blockchain, μια κατανεμημένη δομή που συνδέεται με ομότιμους χρήστες, θα μπορούσε να χρησιμοποιηθεί για να λυθεί το πρόβλημα της διατήρησης της σειράς συναλλαγών και για να το πρόβλημα των διπλών δαπανών (double spending) (Nakamoto, 2008). Το Bitcoin δίνει εντολές για συναλλαγές και τις ομαδοποιεί σε μια δομή περιορισμένου μεγέθους που ονομάζεται μπλοκ που μοιράζονται την ίδια χρονική σήμανση. Οι κόμβοι του δικτύου (miners) είναι υπεύθυνοι για τη σύνδεση των μπλοκ μεταξύ τους σε χρονολογική σειρά, με κάθε μπλοκ που περιέχει το hash του προηγούμενου μπλοκ να δημιουργήσει ένα blockchain (Crosby et al., 2016). Έτσι, η δομή του blockchain καταφέρνει να περιέχει ένα ισχυρό και ελέγξιμο μητρώο όλων των συναλλαγών.

Τα blockchain εισήγαγαν σοβαρές διαταραχές στις παραδοσιακές επιχειρησιακές διαδικασίες, καθώς οι εφαρμογές και οι συναλλαγές, οι οποίες χρειάζονταν κεντρικές αρχιτεκτονικές ή αξιόπιστα τρίτα μέρη για την επαλήθευση τους, μπορούν τώρα να λειτουργούν με αποκεντρωμένο τρόπο με το ίδιο επίπεδο βεβαιότητας. Τα εγγενή χαρακτηριστικά της αρχιτεκτονικής και του σχεδιασμού των blockchain παρέχουν ιδιότητες όπως η διαφάνεια, η ευρωστία και η ασφάλεια (Greenspan, 2015; Christidis & Devetsikiotis, 2016). Ένα blockchain μπορεί να θεωρηθεί μια κατανεμημένη βάση δεδομένων που είναι οργανωμένη ως κατάλογος των εντοπισμένων μπλοκ, όπου τα δεσμευμένα μπλοκ είναι αμετάβλητα. Μπορούμε να διαπιστώσουμε ότι αυτό είναι ιδανικό στον τραπεζικό τομέα, καθώς οι τράπεζες μπορούν να συνεργάζονται με το ίδιο blockchain και να προωθούν τις συναλλαγές των πελατών τους. Με αυτόν τον τρόπο, πέρα από τη διαφάνεια, το blockchain διευκολύνει τον έλεγχο των συναλλαγών. Οι εταιρείες επενδύουν στην τεχνολογία αυτή καθώς βλέπουν το δυναμικό αποκεντρωμένης αποκατάστασης και ελαχιστοποίησης του κόστους των συναλλαγών καθώς καθίστανται εγγενώς ασφαλέστεροι, διαφανέστεροι και σε ορισμένες περιπτώσεις πιο γρήγοροι. Ως εκ τούτου, blockchain δεν είναι μόνο μια διαφημιστική εκστρατεία.

Ο αριθμός των κρυπτονομισμάτων δείχνει τη σημασία του blockchain, που υπερβαίνει σήμερα το 1900 και αυξάνεται (CoinMarketCap, 2017). Αυτός ο ρυθμός

ανάπτυξης θα μπορούσε σύντομα να δημιουργήσει προβλήματα διαλειτουργικότητας λόγω της ανομοιογένειας των εφαρμογών κρυπτονομισμάτων (Tschorsch & Scheuermann, 2016; Haferkorn &. Quintana Diaz, 2017). Επιπλέον, το τοπίο εξελίσσεται ταχέως, καθώς το blockchain χρησιμοποιείται σε άλλους τομείς πέρα από τα κρυπτονομίσματα, με τις έξυπνες συμβάσεις (Smart Contracts/ SCs) να διαδραματίζουν κεντρικό ρόλο. Οι έξυπνες συμβάσεις που ορίστηκαν το 1994 από την Szabo ως ένα πρωτόκολλο υπολογιστικής συναλλαγής που εκτελεί τους όρους μιας σύμβασης, μας επιτρέπουν να μετατρέψουμε τις συμβατικές ρήτρες σε ενσωματωμένο κώδικα (Zhao, Fan & Yan, 2016) ελαχιστοποιώντας έτσι την εξωτερική συμμετοχή και τους κινδύνους. Επομένως, μια έξυπνη σύμβαση είναι μια συμφωνία μεταξύ των μερών τα οποία, αν και δεν εμπιστεύονται ο ένας τον άλλον, οι συμφωνημένοι όροι εφαρμόζονται αυτομάτως. Επομένως, στο πλαίσιο του πλαισίου των μπλοκ αλυσίδων, οι έξυπνες συμβάσεις είναι σενάρια που εκτελούνται με αποκεντρωμένο τρόπο και αποθηκεύονται στο blockchain (Christidis & Devetsikiotis, 2016) χωρίς να στηρίζονται σε καμία αξιόπιστη αρχή. Συγκεκριμένα, συστήματα βασισμένα σε blockchain που υποστηρίζουν έξυπνες συμβάσεις επιτρέπουν πιο σύνθετες διαδικασίες και αλληλεπιδράσεις, ώστε να δημιουργήσουν ένα νέο πρότυπο με πρακτικά απεριόριστες εφαρμογές.

Ως αποτέλεσμα, η τεχνολογία blockchain καθίσταται ολοένα και πιο σχετική (Zhao, Fan & Yan, 2016). Σχεδόν 1.000 (33%) στελέχη της C-suite δηλώνουν ότι σκέφτονται ή έχουν ήδη ασχοληθεί ενεργά με μπλοκ αλυσίδες (IBM, 2017). Οι ερευνητές και οι προγραμματιστές γνωρίζουν ήδη τις δυνατότητες της νέας τεχνολογίας και διερευνούν διάφορες εφαρμογές σε μια μεγάλη γκάμα τομέων (Christidis & Devetsikiotis, 2016). Με βάση το συγκεκριμένο κοινό, μπορούν να διακριθούν τρεις γενιές blockchain (Zhao, Fan & Yan, 2016): Blockchain 1.0 που περιλαμβάνει εφαρμογές που επιτρέπουν ψηφιακές συναλλαγές κρυπτονομισμάτων. blockchain 2.0 που περιλαμβάνει SC και ένα σύνολο εφαρμογών που εκτείνονται πέρα από τις συναλλαγές κρυπτογράφησης και blockchain 3.0 που περιλαμβάνει εφαρμογές σε περιοχές πέρα από τις προηγούμενες δύο εκδόσεις, όπως η υγεία, η επιστήμη και η διακυβέρνηση.

Ενώ υπάρχουν αρκετές αναθεωρήσεις σχετικά με την τεχνολογία blockchain (Tama et al., 2017), υποστηρίζουμε ότι οι τελευταίες τεχνολογίες εφαρμογών που έχουν ενεργοποιηθεί με blockchain έχουν περιορισμένη προσοχή. Ακόμη, οι εφαρμογές των blockchain δεν καλύπτονται πλήρως ούτε εφαρμόζονται. Υπάρχουν πράγματι μερικές ανασκοπήσεις που επικεντρώνονται στον ιδιαίτερο ρόλο του blockchain, συμπεριλαμβανομένης της ανάπτυξης αποκεντρωμένων εφαρμογών και εφαρμογών

δεδομένων για το Διαδίκτυο των πραγμάτων (IoT) (Christidis & Devetsikiotis, 2016; Karafiloski & Mishev, 2017) και η διαχείριση μεγάλων δεδομένων με αποκεντρωμένο τρόπο (Karafiloski & Mishev, 2017). Άλλες αξιολογήσεις επικεντρώνονται στα ζητήματα ασφάλειας του blockchain (Khan & Salah, 2017) και στις δυνατότητές του να επιτρέπουν την εμπιστοσύνη και την αποκέντρωση στα συστήματα υπηρεσιών (Seebacher & Schuritz, 2017) και τις πλατφόρμες P2P (Hawlitschek, Notheisen, & Teubner, 2018). Ορισμένες τεχνικές πτυχές του σχεδίου blockchain όπως το πρωτόκολλο συναίνεσης (Sankar, Sindhu & Sethumadhavan, 2018), οι ευπάθειες των έξυπνων συμβάσεων (Atzei, Bartoletti, & Cimoli, 2017) και άλλα τεχνικά χαρακτηριστικά, όπως το μέγεθος και το εύρος ζώνης, η χρηστικότητα, η ακεραιότητα των δεδομένων και η δυνατότητα κλιμάκωσης έχουν επίσης μελετηθεί σε (Yli-Huumo et al., 2016; Koteska, Karafilovski & Mishev, 2017). Επιπλέον, υπάρχουν και άλλες έρευνες (Koteska, Karafilovski & Mishev, 2017; Bonneau et al., 2015; Tsukerman, 2015) οι οποίες επικεντρώνονται περισσότερο στη νομισματική πλευρά των blockchain και στην προσφερόμενη ασφάλεια και ιδιωτικότητα.

Είναι προφανές ότι η βιβλιογραφία στερείται συγκεκριμένης και συστηματικής ανασκόπησης των σύγχρονων εφαρμογών που είναι πλέον διαθέσιμες στο πλαίσιο ενός blockchain, ενός περιορισμού που ήταν ο κύριος οδηγός για τη διεξαγωγή αυτής της έρευνας. Συγκεκριμένα, προσπαθούμε να το αντιμετωπίσουμε απαντώντας στις ακόλουθες τρεις ερωτήσεις: (i) Πώς αναπτύσσονται οι εφαρμογές που βασίζονται σε blockchain με την πάροδο του χρόνου; (ii) Πόσο ορισμένοι τεχνικοί περιορισμοί της αρχιτεκτονικής blockchain επηρεάζουν τις διαδικασίες / διαδικασίες σε συγκεκριμένους τομείς; Ποιοι είναι αυτοί οι περιορισμοί; (iii) Ποια είναι η καταλληλότητα της τεχνολογίας blockchain σε διάφορους τομείς και θεματικές περιοχές;

Η δουλειά μας συμβάλλει στην πλήρη κατανόηση των χαρακτηριστικών του blockchain και παρέχει ένα στιγμιότυπο των τρεχουσών εφαρμογών με δυνατότητα blockchain σε διάφορους τομείς. Με βάση μια θεωρητικής προσέγγιση, υπογραμμίζουμε το αυξανόμενο ενδιαφέρον από την ακαδημαϊκή κοινότητα και εντοπίζουμε τρία βασικά ερευνητικά ρεύματα: (i) ταξινόμηση του εύρους των εφαρμογών που βασίζονται σε blockchain σε μια μεγάλη ποικιλία τομέων (ii) καταλληλότητα του blockchain τεχνολογία για τη δημιουργία αξίας σε αυτούς τους τομείς λαμβάνοντας υπόψη τους διάφορους περιορισμούς που παρουσιάζει αυτή η τεχνολογία και iii) καθοδηγώντας τους ερευνητές παρέχοντας έναν χάρτη με πολλά υποσχόμενα ερευνητικά μέσα, προκλήσεις και ευκαιρίες για τις οποίες απαιτείται περαιτέρω έρευνα. Αξίζει να σημειωθεί ότι αυτή η ανασκόπηση δεν

μπορεί με κανένα τρόπο να θεωρηθεί απόλυτη δεδομένου ότι η τεχνολογία blockchain αναπτύσσεται συνεχώς με πολύ γρήγορους ρυθμούς.

ΚΕΦΑΛΑΙΟ 1. ΕΞΕΛΙΞΗ ΝΟΜΙΣΜΑΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗ ΧΡΗΜΑΤΟΣ

Ο ορισμός των χρημάτων δεν ήταν ποτέ εύκολος στόχος, ειδικά λόγω των διαφορετικών μορφών που έχει πάρει το χρήμα σε όλη την ιστορία. Επομένως, οι οικονομολόγοι θα χαρακτηρίζουν μάλλον τα χρήματα όχι για το τι είναι, αλλά για τις λειτουργίες που εκτελούν. Αυτές οι λειτουργίες είναι τρεις:

1. Μέσο ανταλλαγής: τα χρήματα χρησιμοποιούνται για την εμπορία αγαθών και την πληρωμή των υποχρεώσεων, ως μια πολύ πιο βολική εναλλακτική λύση για την ανταλλαγή.
2. Λογιστική μονάδα: τα χρήματα είναι ο αριθμός που χρησιμοποιείται για τη μέτρηση των αξιών και των τιμών.
3. Απόθεμα αξίας: τα χρήματα μπορούν να αποθηκευτούν και να διατηρήσουν την αξία τους.

Αυτά τα χαρακτηριστικά είναι θεμελιώδη για να θεωρηθούν τέτοια τα χρήματα, ωστόσο, δεν απαιτούν συγκεκριμένη μορφή: οτιδήποτε έχει αυτά τα χαρακτηριστικά είναι χρήμα. Έτσι, όπως αναφέρθηκε προηγουμένως, κατά τη διάρκεια των δεκαετιών τα χρήματα άλλαξαν τη μορφή τους πολλές φορές.

1.1 Συστήματα πληρωμών

Καθ 'όλη την διάρκεια της ιστορίας, διάφορα νομισματικά συστήματα προέκυψαν υπό την επίδραση της πρακτικής ζήτησης και των εξελίξεων στις νομισματικές πολιτικές. Αρχικά, η πρακτική ανάγκη για χρήματα, ένα κοινώς αποδεκτό μέσο ανταλλαγής, προέκυψε από την ανταλλαγή. Η εξέλιξη αυτή δόθηκε από τον Karl Menger (1892) και εξήγησε ότι σε πολλές περιπτώσεις δεν είναι δυνατή η άμεση ανταλλαγή βασικών εμπορευμάτων, διότι ορισμένα αγαθά είναι αδιαίρετα και επομένως η διαδικασία αντιστοίχισης της προσφοράς και της ζήτησης είναι κουραστική, με αποτέλεσμα το κόστος αναζήτησης. Αυτή η πρακτική

ανάγκη έχει ως αποτέλεσμα μια φυσική σύγκλιση προς έναν ή περιορισμένο αριθμό ευρέως αποδεκτών προϊόντων που θα χρησιμοποιηθούν στις συναλλαγές. Ο Menger εξηγεί ότι αυτή η διαδικασία έχει οδηγήσει στη χρήση του χρυσού και του αργύρου ως χρήματος, καθώς και ως μονάδα λογιστικής σε προηγμένους πολιτισμούς. Η εξήγησή του περιλαμβάνει επίσης την άποψη ότι δεν έχει ληφθεί ενιαία συλλογική απόφαση για την επίτευξη του παρατηρούμενου αποτελέσματος. Για να εξοικονομήσει περαιτέρω το κόστος που συνεπάγεται η ανταλλαγή χρημάτων μέσω χρημάτων, η εμφάνιση νομισμάτων έχει παρατηρηθεί σε ένα μη ρυθμισμένο ανταγωνιστικό περιβάλλον (White, 1984). Η πρακτική ανάγκη για εύκολη επαλήθευση της αξίας των κερμάτων ικανοποιήθηκε με εμπορικά σήματα που μπόρεσαν να οικοδομήσουν εμπιστοσύνη μεταξύ των εμπόρων μειώνοντας το κόστος εξακρίβωσης της γνησιότητας στην εμπορική διαδικασία και τελικά οδηγώντας στην κυβέρνηση να μονοπωλεί τη λειτουργία νομισμάτων (White, 1984). Η επόμενη εξέλιξη με τα νομισματικά συστήματα ήταν η εισαγωγή τραπεζικών υποχρεώσεων που οδήγησαν σε ένα διατραπεζικό σύστημα εκκαθάρισης (White, 1984). Σε μια απλοποιημένη θεώρηση, η μετάβαση από το σύστημα αυτό στο σημερινό σύστημα χρηματικών ταμείων διεξάγεται με δύο βήματα: 1) αντικαθιστώντας τα είδη με εξαγοραζόμενες υποχρεώσεις που εκδίδονται από κεντρική τράπεζα που έχει δημιουργηθεί από την κυβέρνηση, 2) αναστέλλοντας τη δυνατότητα αποπληρωμής της ευθύνης των κεντρικών τραπεζών (White, 1984). Ως εκ τούτου, τα χρήματα μη οικιακής χρήσης χωρίς εγγενή αξία έχουν αξία ανταλλαγής (White, 1984).

Σε ένα έγγραφο που εξετάζει την τραπεζική στη θεωρία της οικονομίας, ο Eugene Fama περιγράφει τη βασική λειτουργία των τραπεζών ως τη διατήρηση ενός συστήματος λογαριασμών στο οποίο πραγματοποιούνται μεταβιβάσεις περιουσιακών στοιχείων με λογιστικές εγγραφές (Fama, 1980). Συνεχίζει να περιγράφει ότι ένα αποτελεσματικό καθαρό λογιστικό σύστημα ανταλλαγής θα είχε ένα καθαρό ονομαστικό αγαθό ή μονάδα λογιστικής που θα παίρνει το ρόλο του αριθμητικού στοιχείου. Η άποψη της Fama είναι ανεξάρτητη από το φυσικό μέσο ή την έννοια του χρήματος καθώς μόνο οι αριθμητικές ή σχετικές τιμές πρέπει να προσδιοριστούν. Ο Fama καταλήγει σε ένα φουτουριστικό σενάριο στο οποίο ο όρος «χρήματα» ξεχνιέται και η κυβέρνηση αποφασίζει να εισαγάγει ένα καθαρό ονομαστικό αγαθό, μια «μονάδα» χωρίς φυσική αναπαράσταση ή εγγενή χρησιμότητα που αποφέρει μηδενικό επιτόκιο. Το σενάριο περιγράφει την πρόκληση της καθιέρωσης λειτουργιών προσφοράς και ζήτησης για τη "μονάδα" που καθορίζει τη σχετική αξία του σε άλλα αγαθά. Η προτεινόμενη λύση του Fama είναι να δημιουργήσει ζήτηση για "μονάδες" επιβάλλοντας αποθεματικό. Μεταξύ άλλων, ο Lawrence White (1984) συζητά το σύστημα του Fama ως

δυνητικό ανταγωνιστικό σύστημα πληρωμών και περιγράφει τις απαραίτητες προϋποθέσεις ώστε ένα τέτοιο νέο σύστημα να μπορεί να αντικαταστήσει το τότε σύστημα. Η ανάλυση του White καταλήγει στο συμπέρασμα ότι μια αντικατάσταση είναι δυνατή αν οι συναλλαγές που διεξάγονται στο δεύτερο χρήμα αυξάνονται σε σχετική σημασία ή επειδή τα πρώτα χρήματα βιώνουν μια εξωγενώς προκαλούμενη συνεχιζόμενη μείωση της αγοραστικής δύναμης. Δηλώνει επίσης ότι η ευκολία των εμπόρων στον τότε κόσμο είναι αυτό που υπαγορεύει το χρηματικό χρήμα και τη λογιστική μονάδα. Το σύστημα που περιγράφεται από τον Fama ταιριάζει αρκετά καλά με το Bitcoin, στο οποίο το αριθμητικό δεν είναι συνδεδεμένο με τον φυσικό κόσμο, το επιτόκιο είναι μηδενικό και είναι δύσκολο να καθορίσουμε την αξία του σε σχέση με άλλα αγαθά. Μια σαφής διαφορά είναι ότι το σύστημα της Fama εισάγεται από την κυβέρνηση, ενώ το Bitcoin εισήχθη από έναν ιδιώτη.

1.2 Νομισματικές πολιτικές

Η ανάπτυξη των νομισματικών συστημάτων είχε ως αποτέλεσμα το ελεγχόμενο από την κυβέρνηση μονοπώλιο της προσφοράς χρήματος. Η βέλτιστη νομισματική πολιτική αποτελούσε πάντοτε αντικείμενο συζήτησης και συνεχίζει να εγείρει αντιφατικές απόψεις μεταξύ ακαδημαϊκών και εμπειρογνωμόνων. Για να μπορεί ένα νομισματικό σύστημα να λειτουργεί σωστά, η παροχή χρημάτων πρέπει να ελέγχεται με τον κατάλληλο τρόπο. Ο Μίλτον Φρίντμαν έχει δημοσιεύσει βιβλία και έρευνες για τις νομισματικές πολιτικές και στις συζητήσεις του αναδεικνύει ότι ο ρητός κυβερνητικός έλεγχος της προσφοράς χρήματος μπορεί να οδηγήσει σε ανεύθυνες κυβερνητικές ενέργειες (Friedman, 1948). Προτείνει ότι ο κίνδυνος αυτός θα μπορούσε να αποφευχθεί με τη μετάβαση σε ένα "μεταλλικό νόμισμα" και την εξάλειψη "κάθε κρατικού ελέγχου της ποσότητας των χρημάτων", γεγονός που θα ενθάρρυνε έναν «ισορροπημένο πραγματικό προϋπολογισμό». Όντας οι δανειστές της τελευταίας λύσης, οι κεντρικές τράπεζες έχουν αποκτήσει μια μοναδική οικονομική θέση. Εάν οι κυβερνήσεις που επηρεάζουν τις κεντρικές τράπεζες επιλέγονται μέσω μιας διαδικασίας ελεύθερης δημοκρατίας με ειλικρινείς υπεύθυνους λήψης αποφάσεων, θεωρητικά τα τελικά αποτελέσματα θα πρέπει να είναι ένα εύλογα λειτουργικό σύστημα. Ωστόσο, τα προβλήματα που αντιμετωπίζει το σύστημα αυτό δείχνουν ότι υπάρχουν ελαττώματα που έχουν και θα καταστρατηγηθούν. Ενώ το κόστος εξακρίβωσης των στοιχείων χρήματος που αναφέρθηκε νωρίτερα μπορεί να μειωθεί με την εμπιστοσύνη και τη φήμη μιας κυβέρνησης, η Friedman βλέπει έναν αντιτιθέμενο παράγοντα να εξετάσει, την

κατάχρηση εξουσίας που μπορεί να καταστρέψει αυτή την εμπιστοσύνη. Θα μπορούσε κανείς να υποδείξει ότι αυτή η ρύθμιση δημιουργεί σοβαρό ηθικό κίνδυνο. Μια από τις επιλογές νομισματικής πολιτικής που πρότεινε ο Friedman είναι ο κανόνας k-percent, που υπαγορεύει ότι η προσφορά χρήματος πρέπει να αυξηθεί με σταθερό ρυθμό ανεξάρτητα από τους οικονομικούς κύκλους (Friedman & Schwartz, 2008). Αυτή η πολιτική έχει ορισμένες ομοιότητες με το σύστημα Bitcoin, στο οποίο η ποσότητα χρημάτων αυξάνεται με προκαθορισμένο ρυθμό.

1.3 Κεντροποίηση

Μια καθοριστική πτυχή ενός νομισματικού συστήματος είναι ο βαθμός κεντροποίησης του. Υπάρχουν διαφορετικές απόψεις σχετικά με τον βέλτιστο βαθμό κεντροποίησης ενός νομισματικού συστήματος, αλλά η ιστορική εξέλιξη ήταν προς ένα πιο ρυθμισμένο και συγκεντρωτικό σύστημα. Θα μπορούσαμε να εντοπίσουμε το πρώτο σαφές σημάδι του σημερινού συστήματος στο έτος 1844, όταν το Κοινοβούλιο του Ηνωμένου Βασιλείου ψήφισε το νόμο του Bank Charter Act (1844) περιορίζοντας την έκδοση χαρτονομισμάτων και τελικά δίνοντας στην Τράπεζα της Αγγλίας αποκλειστική εξουσία έκδοσης χρημάτων. Αυτή η αμφιλεγόμενη πράξη τροφοδότησε τη συζήτηση μεταξύ της βρετανικής τραπεζικής σχολής και της σχολής νομισμάτων και θεωρήθηκε νίκη για τη σχολή συναλλάγματος που ισχυρίστηκε ότι η Τράπεζα της Αγγλίας θα μπορούσε να σταθεροποιήσει την οικονομία ελέγχοντας τις τιμές μέσω του ελέγχου του κυκλοφορούντος νομίσματος (Skaggs, 1999) . Η αναπόφευκτη πρόοδος προς την συγκέντρωση των αποθεμάτων επικρίθηκε από τον Walter Bagehot (1878) ο οποίος ισχυρίστηκε ότι αυτό το είδος συγκέντρωσης δεν ήταν καλή ιδέα και ήταν ενάντια στο φυσικό σύστημα κάθε τράπεζας που κρατούσε δικά της αποθέματα.

Ο Lawrence White (1983) γράφει για αυτή την «πυραμίδα των αποθεμάτων» και συζητά για τον ελεύθερο τραπεζικό τομέα στη Σκωτία για έναν αιώνα πριν από το νόμο του 1844. Κατά τη διάρκεια αυτού του χρόνου ο ελεύθερος ανταγωνισμός οδήγησε σε ένα λειτουργικό σύστημα που δεν απαιτούσε μια κεντρική τράπεζα, κεντρικό κέντρο εκκαθάρισης. Σύμφωνα με τον White, υπάρχουν δύο λόγοι για τους οποίους το ίδιο δεν ήταν δυνατό στις Ηνωμένες Πολιτείες που ονομάζεται ελεύθερη τραπεζική κατά τον 19ο αιώνα. Πρώτον, οι διαπεριφερειακοί τραπεζικοί περιορισμοί μείωσαν την κυκλοφορία αξιόπιστων τραπεζικών χαρτονομισμάτων και, δεύτερον, οι απαιτήσεις για κατοχή κρατικών ομολόγων

από τις τράπεζες κατέληξαν σε διαφοροποίηση των τραπεζικών περιουσιακών στοιχείων. Ενώ το σημερινό σύστημα έχει αναμφίβολα καταφέρει να διευκολύνει την οικονομική ανάπτυξη σε πολλά μέρη του κόσμου, υπάρχει συνεχής συζήτηση για τον βέλτιστο βαθμό συγκέντρωσης. Υπάρχει το ιστορικό παράδειγμα της επιτυχούς ελεύθερης τραπεζικής στη Σκωτία, που δείχνει ότι ίσως ο ελεύθερος ανταγωνισμός σε τραπεζικά και νομισματικά συστήματα θα μπορούσε να είναι επωφελής. Το όφελος του ανταγωνισμού γενικά είναι ότι πρόκειται για μια διαδικασία ανακάλυψης (Hayek, 2002). Ως εκ τούτου, η παρέμβαση της κυβέρνησης στη διαδικασία ανταγωνισμού χρημάτων και νομισματικών συστημάτων μπορεί να θεωρηθεί ύποπτος τρόπος για τον ορισμό συστημάτων που έχουν εξαιρετικά σημαντικό αντίκτυπο στην καθημερινή ζωή όλων των πολιτών. Αυτό μπορεί να θεωρηθεί ως θυσία βέλτιστης απόδοσης για χάρη του κεντρικού ελέγχου.

1.4. Κατηγοριοποίηση χρημάτων

Ένας τρόπος να συνοψίσουμε την ανάπτυξη των νομισματικών συστημάτων είναι να τονίσουμε συγκεκριμένα παραδείγματα και την πορεία ανάπτυξης. Αυτό μπορεί να γίνει επιλέγοντας τρία διαφορετικά συστήματα που διαφέρουν θεμελιωδώς μεταξύ τους. Αυτή η ενότητα θα εξετάσει τρία συστήματα, συγκρίνοντας τις δύο ιδιότητές τους: μέτρηση του πλούτου και της αριθμητικής φυσικής αξίας. Πρώτον, υπάρχουν κονδύλια βασικών εμπορευμάτων που είναι περιορισμένα σε ποσότητα και συνεπώς αντιπροσωπεύουν ένα απόλυτο μέτρο πλούτου μέσα στο σύστημα. Ο αριθμητής σε αυτό το σύστημα είναι μια μονάδα φυσικού αγαθού. Δεύτερον, υπάρχουν χρήματα με δυνατότητα εξαγοράς τα οποία έχουν κυβερνητικό αριθμό μετρητών (Friedman & Schwartz, 2008). Αν και ο αριθμητικός είναι συνδεδεμένος με ένα φυσικό αγαθό, η ποσότητα των χρημάτων ελέγχεται κεντρικά με κρατική επιρροή, με αποτέλεσμα ένα σχετικό μέτρο πλούτου. Τρίτον, υπάρχουν αμετακίνητα χρήματα που έχουν εκδοθεί από την κυβέρνηση. Αυτό είναι παρόμοιο με το δεύτερο σύστημα, ωστόσο, δεν υπάρχει σύνδεση με ένα φυσικό αγαθό. Αυτή η αναπτυξιακή πορεία μπορεί να συνεχιστεί με τη συμπερίληψη μιας τέταρτης κατηγορίας, αποκεντρωμένης κρυπτογράφησης, δηλαδή των Bitcoin και των κρυπτονομισμάτων. Αυτό το τέταρτο σύστημα έχει ένα αριθμητικό στοιχείο που προκύπτει από το ίδιο το σύστημα και δεν συνδέεται με ένα φυσικό αγαθό. Η ποσότητα των χρημάτων είναι αυστηρά περιορισμένη, έτσι ώστε μέσα στο σύστημα, το μέτρο του πλούτου είναι απόλυτο.

Όσον αφορά την ποσότητα του χρήματος, αυτό το τέταρτο σύστημα μπορεί να προταθεί ότι αντιπροσωπεύει ένα βήμα προς τα πίσω στην ανάπτυξη. Ωστόσο, το παραστατικό χρηματικό ποσό είναι ακόμα μια σχετικά νέα ιδέα, έτσι ώστε κάποια από τα πλεονεκτήματα και τα μειονεκτήματά του να μην είναι ακόμα γνωστά και επομένως η ανάπτυξη αυτή θα ήταν δύσκολο να αξιολογηθεί πλήρως. Αν ένα αριθμητικό στοιχείο είναι συνδεδεμένο με ένα φυσικό αγαθό, η φυσική του αξία είναι απόλυτη. Μια σχετική φυσική αξία ενός αριθμητικού στοιχείου μπορεί να είναι δύσκολο να εφαρμοστεί με τρόπο που δημιουργεί εμπιστοσύνη, ωστόσο, μπορεί να οδηγήσει σε καλύτερη γενική αποδοτικότητα. Εάν οι μονάδες του νομισματικού συστήματος αντιπροσωπεύουν μόνο ένα σχετικό μέτρο του πλούτου μέσα στο σύστημα, αποθαρρύνεται η μακροπρόθεσμη εξοικονόμηση των μονάδων. Ένα απόλυτο μέτρο του πλούτου διασφαλίζει μια ορισμένη αγοραστική δύναμη μέσα στο σύστημα και μετά από μια μακρά περίοδο κράτησης. Το μέτρο του πλούτου αντιπροσωπεύει τη φύση της προσφοράς χρήματος στο σύστημα.

1.5. Οι ρόλοι των χρημάτων

Σύμφωνα με τον Scitovsky (1969), τα χρήματα εξυπηρετούν τρεις λειτουργίες: μία μονάδα λογαριασμού, ένα μέσο ανταλλαγής και ένα απόθεμα αξίας. Ενώ οι δύο πρώτες από αυτές συζητήθηκαν στις προηγούμενες ενότητες, η τελευταία από τις τρεις είναι επίσης μια σημαντική λειτουργία. Λόγω της αστάθειας των τιμών του, το Bitcoin έχει επικριθεί ευρέως για τα κακά χαρακτηριστικά του ως αποθήκη αξίας, ωστόσο, είναι σημαντικό να σημειωθεί ότι το σύστημα απαιτεί μια περίοδο αποπληθωρισμού για να κερδίσει αξία. Θα μπορούσε κανείς να υποδείξει ότι αυτή η διαδικασία θα συνεχιστεί έως ότου το σύστημα βρει τον ρόλο του και τα επίπεδα ζήτησης μακριά. Ενώ η Bitcoin διέρχεται μια ισχυρή αποπληθωριστική διαδικασία, είναι δύσκολο να πούμε αν θα υπάρξει μια ισοπέδωση της ζήτησης. Συγκριτικά, μπορούμε να δούμε πώς το δολάριο ΗΠΑ έχει αποδώσει ως αποθήκη αξίας. Δεδομένου ότι ο χρυσός έχει χαρακτηριστικά ασφαλείας (Baur & Lucey, 2010; Coudert & Raymond, 2011), μπορεί να θεωρηθεί αξιόπιστο μακροπρόθεσμο μέτρο αξίας. Επομένως, η αξία του δολαρίου σε χρυσό είναι ένα εύλογο μέτρο για το πόσο καλά το δολάριο ΗΠΑ έχει επιτελέσει ως αποθήκη αξίας. Το Σχήμα 1 δείχνει την τιμή των 1000USD σε χρυσό από τις αρχές του 1976. Σύμφωνα με το μέτρο αυτό, το δολάριο ΗΠΑ δεν ήταν πολύ αξιόπιστο κατάστημα αξίας. Η πρόσφατη εξέλιξη ήταν τέτοια που μετά το έτος 2000, το δολάριο ΗΠΑ έχασε περίπου τα τρία τέταρτα της αξίας του που μετράται σε χρυσό. Είναι επίσης καλό να σημειωθεί ότι το

γράφημα αποκλείει την προηγούμενη περίοδο των 4,5 ετών αμέσως μετά το σοκ Nixon, κατά τη διάρκεια του οποίου το δολάριο έχασε τα δύο τρίτα της αξίας του που μετράται σε χρυσό.

Σχήμα 1. USD σε χρυσό βάση στοιχείων από το World Gold Council, http://www.gold.org/investment/statistics/gold_price_chart/

Ο ρόλος του Bitcoin είναι επί του παρόντος πολύ μικρός όσον αφορά τον οικονομικό του αντίκτυπο. Ωστόσο, αντιπροσωπεύει μια εντελώς νέα γενεά χρηματοπιστωτικών μέσων που επιτρέπουν μια νέα προσέγγιση στα νομισματικά συστήματα και τη νομισματική πολιτική. Ποτέ πριν δεν ήταν δυνατό για δύο άτομα να διεξάγουν επαληθεύσιμες συναλλαγές χωρίς μεσάζοντα. Αυτή η πρόοδος έχει λύσει το πρόβλημα στο οποίο μια ομάδα ατόμων δεν είναι σίγουρη για την αξιοπιστία μιας άλλης ομάδας, μπορεί να καταλήξει ανώνυμα σε συλλογική απόφαση (Lamport, Shostak and Pease, 1982). Παρόλο που οι Lamport et al. (1982) συζητούν τον χειρισμό της αποτυχίας ενός στοιχείου σε ένα σύστημα ηλεκτρονικών υπολογιστών, το σύστημα Bitcoin μπορεί να θεωρηθεί ότι επιλύει αυτό το πρόβλημα στον τομέα των δικτύων υπολογιστών και της διαμεσολάβησης των συναλλαγών. Όταν αντικατοπτρίζεται στις ιστορικές προκλήσεις των νομισματικών συστημάτων, μπορεί να φανεί ότι το σύστημα Bitcoin εξαλείφει το κόστος αναζήτησης και το κόστος ταυτότητας. Αξίζει να σημειωθεί ότι ακόμη και η χρήση χαρτονομισμάτων σε δολάρια ή ευρώ προκαλεί κόστος ελέγχου ταυτότητας επειδή υπάρχουν πλαστά τραπεζογραμμάτια σε κυκλοφορία. Τελικά αυτό οδηγεί στην ανάγκη για εξοπλισμό και μεθόδους πιστοποίησης κατά την αντιμετώπιση μεγάλων χρηματικών ποσών. Το κόστος αυθεντικοποίησης έχει επίσης αντίκτυπο στον τρόπο κατανόησης και προσέγγισης της εμπιστοσύνης σε ένα νομισματικό σύστημα.

Κάποιος μπορεί να χωρίσει την εμπιστοσύνη σε ένα νομισματικό σύστημα σε δύο μέρη. Πρώτον, υπάρχει εμπιστοσύνη στα χρήματα και στην αγοραστική τους δύναμη. Δεύτερον, υπάρχει εμπιστοσύνη στη λειτουργικότητα του συστήματος και της συναλλαγής. Η εμπιστοσύνη στην αγοραστική δύναμη του bitcoin είναι χαμηλή λόγω της αστάθειας των τιμών και της νομικής του θέσης. Ωστόσο, η αστάθεια των τιμών μπορεί να υποστηριχθεί ότι αποτελεί μέρος της φάσης ανάπτυξης και εισαγωγής του Bitcoin, υποδηλώνοντας ότι, όταν η bitcoin έχει βρει τη θέση της στην οικονομία ως μέθοδο πληρωμής και ως εναλλακτικό χρήμα, η αστάθεια των τιμών της θα μειωθεί σε ένα βολικότερο επίπεδο (Koteska, Karafilovski & Mishev 2017).. Μια άλλη προοπτική για την αγοραστική δύναμη του bitcoin είναι η νομική του θέση. Ενώ αυτό συζητείται και συζητείται συνεχώς, είναι ασφαλές να πούμε ότι δεν είναι προς το συμφέρον των κυβερνήσεων και των κεντρικών τραπεζών να εγκαταλείψουν τον έλεγχο των αποφάσεων νομισματικής πολιτικής. Αυτό οδηγεί στο συμπέρασμα ότι το bitcoin δεν είναι πιθανόν να γίνει αποδεκτό ως άμεσος τρόπος πληρωμής για τους φόρους. Με αυτή την υπόθεση, ακόμη και αν η χρήση bitcoins αυξάνεται, έτσι ώστε τα άτομα και οι επιχειρήσεις θα έχουν όλο και περισσότερα από το εισόδημα και τις δαπάνες τους σε bitcoin, τελικά φορολογικές υποχρεώσεις θα πρέπει να πληρούνται με παραστατικό νόμισμα. Αυτό θα αναγκάσει τους νόμιμους χρήστες bitcoin να εξαρτώνται από τις ανταλλαγές bitcoin-παραστατικού νομίσματος και επομένως ευάλωτοι στην κρατική παρέμβαση. Αυτός είναι ο λόγος για τον οποίο η νομική θέση του Bitcoin είναι καθοριστικής σημασίας για την αποδοχή του, παρόλο που η τεχνολογική εκτέλεση του βασικού συστήματος είναι πολύ ανθεκτική στις εξωγενείς αυτές παρεμβάσεις.

Το δεύτερο μέρος της εμπιστοσύνης, που αφορά λειτουργικότητα συστήματος και συναλλαγών, είναι πολύπλοκο στην περίπτωση του Bitcoin. Το σύστημα μπορεί να χρησιμοποιηθεί με τρόπο που επιτρέπει σε δύο μέρη να διεξάγουν μια συναλλαγή χωρίς εμπιστοσύνη σε άλλες οντότητες. Ο χρήστης χρειάζεται μόνο να εμπιστευτεί την ασφάλεια του δικτύου που βασίζεται στην υπόθεση ότι ένας μεμονωμένος ηθοποιός δεν θα αποκτήσει τον πλειοψηφικό έλεγχο του δικτύου Bitcoin που μετράται σε υπολογιστική ισχύ, το ρυθμό κατακερματισμού (Koteska, Karafilovski & Mishev 2017). Αυτός ο τρόπος χρήσης είναι ο βέλτιστος όσον αφορά την εμπιστοσύνη στο σύστημα και τη λειτουργικότητα συναλλαγών επειδή το κατανεμημένο δίκτυο μπορεί να θεωρηθεί ως κατανεμημένο σύστημα εμπιστοσύνης όπου ο μηχανισμός εκκαθάρισης bitcoin έχει αποδειχθεί πολύ ισχυρός. Έχοντας δηλώσει αυτό, στην πράξη, οι χρήστες που ενδιαφέρονται για bitcoin μόνο ως χρήματα δεν θα θέλουν πιθανώς να ασχοληθούν με την εξόρυξη bitcoin και τη διαχείριση της

ασφάλειας των πορτοφολιών. Θα χρησιμοποιούν κατά πάσα πιθανότητα τρίτους φορείς παροχής υπηρεσιών για την αγορά bitcoins μέσω ανταλλαγής και διαχείρισης ψηφιακών πορτοφολιών. Η εμπιστοσύνη προς αυτά τα τρίτα μέρη είναι συγκρίσιμη με το σημερινό νομισματικό σύστημα στο οποίο εμπιστεύονται οι τράπεζες. Ωστόσο, η διαφορά είναι ότι πολλοί πάροχοι υπηρεσιών Bitcoin στερούνται την πολυπλοκότητα και τη φήμη που θα τους καθιστούσε αξιόπιστους. Το πιο πρόσφατο και ίσως το σημαντικότερο παράδειγμα μιας αναξιόπιστης ανταλλαγής bitcoin είναι η χρεοκοπία του Mt.Gox τον Φεβρουάριο του 2014 (Takemoto & Knight, 2014). Ενώ η εμπιστοσύνη του συστήματος έχει καλές βάσεις και δυνατότητες βασισμένες στο βασικό σύστημα Bitcoin, η σύντομη ιστορία του δείχνει ότι υπάρχει μεγάλη απόσταση για το Bitcoin και ιδιαίτερα για τους παρόχους υπηρεσιών να αξιοποιήσουν πλήρως αυτό το δυναμικό στην πράξη. Σε ένα μελλοντικό σενάριο με ευρύτερη αποδοχή bitcoin, ο ελεύθερος ανταγωνισμός θα πρέπει να προάγει τις αξιόπιστες υπηρεσίες και να εξαλείψει τις δυσλειτουργίες των υπηρεσιών. Το αν η διαδικασία του ελεύθερου ανταγωνισμού είναι υπερβολικά δαπανηρή για τους επισφαλείς καταναλωτές είναι ένα άλλο θέμα συζήτησης σχετικά με τον κρατικό έλεγχο και τη ρύθμιση.

Λαμβάνοντας υπόψη την περιγραφή του Fama (1980) της κύριας λειτουργίας της τραπεζικής που είναι η διαχείριση των λογιστικών εγγραφών και του προβλεπόμενου ανταγωνιστικού νομισματικού της συστήματος, φαίνεται ότι κατά κάποιον τρόπο η Bitcoin συναντά τα ιδανικά του διάσημου οικονομολόγου. Σε συνδυασμό με τα επιχειρήματα που παρουσιάστηκαν για τον ελεύθερο ανταγωνισμό των χρημάτων και των τραπεζών, θα μπορούσε κανείς να υποδείξει ότι το Bitcoin θα μπορούσε ενδεχομένως να εξελιχθεί σε σημαντικό συμπλήρωμα των σημερινών συστημάτων. Ο ρόλος που μπορεί να επιτύχει το Bitcoin εξαρτάται από τρεις κύριους παράγοντες. Οι δύο τελευταίες βασίζονται στα επιχειρήματα του White (1984) σχετικά με τα ανταγωνιστικά συστήματα πληρωμών. Πρώτον, η Bitcoin πρέπει να αποκτήσει νομική θέση, στην οποία επιτρέπεται να είναι ανταγωνιστής ως χρήμα και σύστημα πληρωμών. Δεύτερον, οι συναλλαγές Bitcoin πρέπει να αποκτήσουν μεγαλύτερη σημασία, είτε ως μέθοδο πληρωμής είτε μέσω άλλων εφαρμογών. Τρίτον, πρέπει να υπάρξουν κάποιες κρίσεις με το επικρατούμενο σύστημα που επιδεινώνει την αγοραστική δύναμη των παραστατικών νομισμάτων.

1.6. Αποεκντροποιημένη Τραπεζική: νομισματική τεχνοκρατία στην ψηφιακή εποχή

1.6.1. Κανόνες Τραπεζικής

Το επιχείρημα ότι οι κεντρικές τράπεζες πρέπει να διέπονται από κανόνες, και όχι να επιτυγχάνουν ένα σύνολο στόχων, ανεξάρτητα από το ποια είναι η πιθανότητα, έχει μεγάλη υποστήριξη. Αν οι συμμετέχοντες στην αγορά κρίνουν εσφαλμένα τον τρόπο με τον οποίο θα αλλάξουν τα επιτόκια ή αν η κεντρική τράπεζα εκπλήξει την αγορά μεταβάλλοντας τιμές αντίθετες προς τις προσδοκίες, οι διακυμάνσεις της αγοράς θα μπορούσαν να αυξηθούν. Αυτό ισχύει τόσο για το πόσο συχνά όσο και για το πόσο αλλάζουν τα επιτόκια. Στην πραγματικότητα, η εμπειρική έρευνα έχει δείξει ότι η υπερβολική συσσώρευση με τα επιτόκια μπορεί να προκαλέσει αρνητικά οικονομικά αποτελέσματα (Kydland & Prescott, 1977).

Στις Ηνωμένες Πολιτείες, οι Δημοκρατικοί έχουν εισαγάγει αριθμό λογαριασμών που θα απαιτούσαν από το Ομοσπονδιακό Αποθεματικό να ακολουθήσει έναν «κανόνα». Πρόσφατα, ο Jeb Hensarling (2014), ο οποίος είναι επικεφαλής της επιτροπής οικονομικών που επιβλέπει την Ομοσπονδιακή Τράπεζα των ΗΠΑ, εξέφρασε ανησυχίες το μέγεθος της ελευθερίας που υπάρχει για τον καθορισμό των ποσοστών και τις απρόβλεπτες συνέπειες που μπορεί να προκαλέσει. παρότρυνε τους κεντρικούς τραπεζίτες να ακολουθήσουν ένα απλό σύνολο ρητών κανόνων. Σχετικά με την εκστρατεία εκστρατείας, ο υποψήφιος πρόεδρος Ted Cruz εξέφρασε την επιθυμία του να εφαρμόσει έναν ρητό κανόνα νομισματικής πολιτικής σε μια σειρά προεδρικών συζητήσεων το 2015 και το 2016.

Οι πολιτικές ομάδες προβληματισμού έχουν επίσης εκφράσει την υποστήριξή τους για μια νομισματική πολιτική βασισμένη σε κανόνες. Τον Φεβρουάριο του 2015, το Ίδρυμα Heritage σχολίασε ότι ένας ρητός κανόνας νομισματικής πολιτικής «θα βελτιώσει σημαντικά τη διαφάνεια και την προβλεψιμότητα». Από πολιτική άποψη, η προσέγγιση επιτρέπει στους φορείς χάραξης πολιτικής να αξιολογούν τη συνοχή της Τράπεζας με την αυθεντική νομισματική πολιτική ή με άλλη σχετική νομοθεσία (Walsh, 2015). Σύμφωνα με τον Walsh, αυτό το στυλ μπορεί να αντιπαραβληθεί με μια πιο χαλαρή προσέγγιση βασισμένη σε στόχους, όπως η σύγχρονη στόχευση του πληθωρισμού, όπου οι κεντρικοί τραπεζίτες αξιολογούνται ως προς το πόσο ικανοποιημένοι επιτυγχάνονται οι στόχοι πολιτικής, αφήνοντας πολύ περιθώρια ευελιξίας και δημιουργικότητας για την επίτευξη αυτών στόχους. Οι ακαδημαϊκοί (π.χ. Taylor & Williams, 2010) συμφωνούν ότι η απλή λήψη αποφάσεων βασισμένη σε κανόνες είναι μια ισχυρή μέθοδος εφαρμογής της νομισματικής πολιτικής και επισημαίνουν στοιχεία που αποδεικνύουν ότι η ιστορική εμπειρία έχει δείξει ότι ένα σύνολο απλών κανόνων λειτουργεί καλά στον πραγματικό κόσμο. Οι μελέτες του Taylor & Williams δείχνουν ότι οι σχετικές μακροοικονομικές επιδόσεις ήταν καλύτερες όταν οι αποφάσεις των

κεντρικών τραπεζών περιγράφηκαν από κανόνες και ισχυρίστηκαν ότι οι κανόνες αυτοί δεν υπονομεύονται από χρηματοπιστωτικές κρίσεις. Οι κεντρικοί τραπεζίτες έχουν επί του παρόντος αρκετή διακριτική ευχέρεια ως προς τον τρόπο καθορισμού και εφαρμογής πολιτικής. Προβλήματα τείνουν να προκύψουν όταν η αβεβαιότητα που περιβάλλει αυτές τις αποφάσεις (π.χ. για τον καθορισμό των επιτοκίων) προκαλεί αστάθεια στις χρηματοπιστωτικές αγορές (Deshmukh et al., 1983). Αν οι συμμετέχοντες στην αγορά κρίνουν εσφαλμένα πώς και πότε θα αλλάξουν τα επιτόκια ή αν η κεντρική τράπεζα εκπλήξει την αγορά μεταβάλλοντας ποσοστά αντίθετα από τις επικρατούσες προσδοκίες, θα μπορούσε να αυξηθεί το ενδεχόμενο αρνητικής μεταβλητότητας. Ο Kydland & Prescott (1977) υποδεικνύουν ότι η εντολή να ακολουθεί ένα αυστηρό σύνολο κανόνων θα μπορούσε να χρησιμεύσει για τη μείωση της οικονομικής αβεβαιότητας.

Μπορεί να υποστηριχθεί ότι οι σύγχρονες οικονομίες είναι πολύ μεγάλες και υπερβολικά πολύπλοκες ώστε οι κεντρικές τράπεζες να αποκλίνουν από ένα βασικό σύνολο κανόνων (Walsh, 2015). Πώς μπορεί να αναμένεται από τις κεντρικές τράπεζες να διαχειριστούν με επιτυχία την οικονομική σταθερότητα μέσω χειρισμών που μπορούν να προκαλέσουν απρόβλεπτα αποτελέσματα με απρόβλεπτες συνέπειες; Ο διάσημος οικονομολόγος Ludwig Von Mises (1953) ισχυρίστηκε ότι οι κεντρικές τράπεζες προκαλούν στην πραγματικότητα οικονομική αστάθεια προκαλώντας μια μη βιώσιμη επέκταση των τραπεζικών πιστώσεων. Ο F.A Hayek, φοιτητής του Mises, αντιλήφθηκε την ανάγκη οι κεντρικές τράπεζες να ρυθμίσουν τη νομισματική πολιτική ως είδος αναγκαίου κακού, ώστε να μην καταρρεύσει ένα εντελώς ξεκάθαρο νομισματικό σύστημα (White, 1999). Πιο πρόσφατα, ο πρώην Πρόεδρος της Ομοσπονδιακής Τράπεζας, Ben Bernanke (2000), περιέγραψε εκτενώς το πώς η πολιτική των κεντρικών τραπεζών επιδείνωσε τη Μεγάλη Ύφεση του 1929, αυξάνοντας λανθασμένα τα επιτόκια, αντί να ακολουθούν τους θεσπισθέντες κανόνες, γεγονός που θα τους είχε αναγκάσει να ενεργήσουν αντίθετα.

Η πολιτική επιρροή ή άλλες εξωτερικές πιέσεις δεν μπορούν με κανέναν τρόπο να επηρεάσουν την απόλυτη έλλειψη ενός αλγορίθμου. Οι εκλεγμένοι αξιωματούχοι αντιμετωπίζουν συχνά κίνητρα για να ευνοήσουν πολιτικές που προωθούν βραχυπρόθεσμα κέρδη στην παραγωγή και την απασχόληση και οι ψηφοφόροι είναι πιθανόν να θυμούνται μια πρόσφατη περίοδο οικονομικής ανάπτυξης και όχι να εξετάζουν τον επιζήμιο μακροπρόθεσμο πληθωρισμό ή αστάθεια που θα μπορούσαν να επιφέρουν οι πολιτικές στο μέλλον. Μια κεντρική τράπεζα πρέπει να είναι πρόθυμη και ικανή να κάνει αντιλαϊκές αποφάσεις και να αναλάβει δράσεις που ένας πολιτικός δεν θα μπορούσε. Για παράδειγμα,

μια κυβέρνηση μπορεί να επιδιώξει μια πολιτική υψηλού πληθωρισμού, προκειμένου να επιτύχει νομισματική χρηματοδότηση των ελλειμμάτων. Μια τέτοια πολιτική ήταν συχνά ο προάγγελος της κατάρρευσης των εθνικών οικονομιών, από την Αργεντινή και τη Ζιμπάμπουε στη Βαϊμάρη της Γερμανίας και στην Ουγγαρία (Minsky, 2015).

Τα κίνητρα για την εξόφληση του χρέους με τον πληθωρισμό είναι δελεαστικά. Εάν μια κυβέρνηση οφείλει π.χ. ένα εκατομμύριο δολάρια την ημέρα σε σταθερές πληρωμές τόκων προς τους πιστωτές, θα ήταν πολύ πιο εύκολο αν το ονομαστικό ένα εκατομμύριο δολάρια είχε γίνει για να αντιπροσωπεύσει σημαντικά μικρότερη αγοραστική δύναμη. Ο πληθωρισμός προκαλεί πτώση της αξίας ενός νομίσματος και αυτό θα ήταν ελκυστικό για τις κυβερνητικές υποχρεώσεις εκτός ελέγχου. Μια ανεξάρτητη κεντρική τράπεζα δεν θα επηρεάζεται από το μέγεθος ενός εθνικού χρέους και μπορεί να μην συμφωνεί με την ελκυστικότητα της υποτίμησης του νομίσματος μέσω του πληθωρισμού. Μια αυτόνομη νομισματική αρχή με εντολή για σταθερό στόχο πληθωρισμού χρησιμεύει ως μηχανισμός ασφάλειας.

Βεβαίως, το επιχείρημα για την ανεξαρτησία δεν είναι καινούργιο: ένας από τους ιδρυτές της σύγχρονης οικονομίας, ο Ντέιβιντ Ρικάρντο (1849), κατηγόρησε την τράπεζα της Αγγλίας, η οποία ήταν ήδη πάνω από εκατό ετών εκείνη την εποχή, ότι τάσσεται υπέρ των ιδιοτροπιών του θρόνου. Ο Ρικάρντο πρότεινε μια κεντρική τράπεζα να είναι ανεξάρτητη από την πολιτική πίεση με τρεις σημαντικούς τρόπους: με τη δύναμη να δημιουργεί χρήματα χωρισμένα από την εξουσία για να αποφασίσει πώς να τα ξοδέψει. με την αποτροπή μιας κεντρικής τράπεζας από τη χρηματοδότηση του προϋπολογισμού του κράτους και με εξωτερική ευθύνη για τη λήψη αποφάσεων. Με βάση τον Ricardo, το άρθρο 130 της Συνθήκης του Μάαστριχτ του 1992 καθιέρωσε την τρέχουσα βάση για την ανεξαρτησία της κεντρικής τράπεζας για την Ευρώπη και από τότε έχει αντιγραφεί στην πράξη από μεγάλο μέρος του ανεπτυγμένου κόσμου (Lastra, 2012).

Σε αυτήν την ψηφιακή εποχή, μπορεί η τεχνολογία αιχμής να επιτρέπει τη συνετή λειτουργία των αποφάσεων της νομισματικής πολιτικής - και να φέρει μαζί της τις δυνατότητες μακρο-σταθερότητας που φέρνει σε ορισμένες αγορές κάποιο επίπεδο βεβαιότητας; Τα ψηφιακά συστήματα νομισμάτων σήμερα είναι προφανή παραδείγματα τεχνολογίας που θα μπορούσαν ενδεχομένως να λειτουργήσουν ως τεχνοκρατική νομισματική αρχή. Αυτά είναι γνωστά γενικά ως «cryptocurrencies», εξαιτίας του ονόματος της διαδικασίας κρυπτογράφησης που τα διευκολύνει, με το πιο καθιερωμένο και ευρέως χρησιμοποιούμενο Bitcoin.

Για λόγους απλούστευσης, μπορούμε να πούμε ότι η σημερινή τεχνολογία - και συγκεκριμένα η τεχνολογία blockchain - μπορεί πράγματι να παράγει ένα τέτοιο αποτέλεσμα. Συγχρόνως, δεν υποστηρίζεται ότι ένα ψηφιακό νόμισμα είναι το ιδανικό πρωτόκολλο για την εφαρμογή μιας πολιτικής των κεντρικών τραπεζών που βασίζεται σε κανόνες. Αντίθετα, ένα σύστημα βασισμένο σε τεχνολογίες βασισμένο σε τεχνολογίες μπορεί να υπάρχει στο πλαίσιο ενός αποκεντρωμένου ψηφιακού νομισματικού συστήματος βασισμένου σε blockchain, έστω και αν το πλαίσιο αυτό αποδεικνύεται κατώτερο από την παραδοσιακή κεντρική τραπεζική χρηματοδότηση από άποψη αποδοτικότητας στον πραγματικό κόσμο. Θα πρέπει να καταστεί σαφές ότι η τεχνολογία, από μόνη της, είναι κατά πάσα πιθανότητα ανεπαρκής για την προώθηση της σταθερότητας, δεδομένου ότι αποτελεί ένα σύνολο ρητών κανόνων. Οι αλγοριθμικές επιχειρήσεις εμπορίας πιστεύεται σε μεγάλο βαθμό συνέβαλαν στην πρόσφατη εκτοξεύσεις της μεταβλητότητας της αγοράς συμπεριλαμβανομένων των «flash crashes» (Kirilenko, et al. 2015). Εναλλακτικά, οι υποστηρικτές του αλγοριθμικού εμπορίου αναφέρουν ότι η τεχνολογία αυξάνει την αποτελεσματικότητα της αγοράς και τη ρευστότητα (Boehmer, et al., 2014). χρειάζεται περισσότερη εμπειρική εργασία για την επίλυση αυτής της αναδυόμενης συζήτησης. Ανεξαρτήτως, θα πρέπει να υπάρχουν τόσο θετικά όσο και αρνητικά για οποιαδήποτε τεχνολογική παρέμβαση - συμπεριλαμβανομένης της χρήσης κρυπτονομισμάτων- και η μείωση των πιθανών αρνητικών συνεπειών θα πρέπει να είναι πρωταρχικής σημασίας. Φυσικά, πολλοί από τους αλγορίθμους που χρησιμοποιούνται κρατούνται μυστικοί και ιδιόκτητοι, οπότε δεν είναι σαφές εάν οι αποτυχίες που προκαλούνται από τέτοια συστήματα είναι αποτέλεσμα της ίδιας της τεχνολογίας ή των ανθρώπινων ατελειών στον κώδικα. Οποιαδήποτε αλγοριθμική προσέγγιση της κεντρικής τράπεζας πρέπει να είναι τόσο ισχυρή όσο και διαφανής, ώστε να είναι εύκολο να εντοπιστούν και να διορθωθούν τυχόν τεχνικά σφάλματα. Οι περισσότερες υλοποιήσεις blockchain είναι ευτυχείς να βασίζονται σε κώδικα λογισμικού ανοικτού κώδικα και να διαθέτουν έναν πλήρως ορατό και ελεγμένο κατάλογο συναλλαγών.

Σκοπός της παρούσας εργασίας είναι να παράσχει μια προοπτική για το πώς ένα ψηφιακό νόμισμα βασισμένο σε blockchain θα μπορούσε να λειτουργήσει ως ανεξάρτητη νομισματική αρχή ακολουθώντας τις αρχές, αναλαμβάνοντας μερικούς από τους ρόλους που παίζουν τώρα οι κεντρικές τράπεζες. Το Bitcoin σχεδιάστηκε για να είναι ένα παγκόσμιο νομισματικό σύστημα και παρόλα αυτά δεν υπάρχει λίγη βιβλιογραφία για τη χρήση του ως τέτοιο (Selgin, 2015).

1.6.2 Η τεχνοκρατία μέσω της αποκεντρωμένης Τραπεζικής

Όπως περιγράφεται παραπάνω, μια κεντρική τράπεζα πρέπει να εφαρμόζει αποτελεσματικά τη νομισματική πολιτική, να εποπτεύει την επίλυση των συναλλαγών και να λειτουργεί ως δανειστής ύστατης λύσης. Υποστήριξα ότι ένα σύστημα ψηφιακού νομίσματος μπορεί πράγματι να εκπληρώσει τους πρώτους δύο ρόλους. Μια κεντρική τράπεζα μπορεί να αφήνει τη νομισματική πολιτική "καθημερινά" στα χέρια ενός αυτοματοποιημένου συστήματος κανόνων που διέπεται από ένα καθεστώς ψηφιακού νομίσματος και να επεμβαίνει υποθετικά μόνο εάν και πότε θα προέκυπτε μια κρίση.

Στο πλαίσιο του τελευταίου επεισοδίου της ελληνικής τραπεζικής κρίσης, ο πρώην υπουργός Οικονομικών Γιάννης Βαρουφάκης υποστήριξε ότι η χώρα του θα μπορούσε να υιοθετήσει το Bitcoin (ή κάποιο παρόμοιο σύστημα) για να λειτουργήσει ως νόμισμα γέφυρας σε μια νέα δραχμή αν η Ελλάδα πράγματι εγκατέλειπε το ευρώ (Mason, 2015). Ο Βαρουφάκης επεσήμανε πολλές αδυναμίες του ίδιου του Bitcoin ως πρακτικό μακροπρόθεσμο υποκατάστατο του νομισματικού συστήματος ενός έθνους - όπως το δυναμικό του να είναι αποπληθωριστικό και η ανικανότητά του να αντιδράσει στις εξωτερικές δυνάμεις (Varoufakis, 2014). Εντούτοις, ανέφερε ότι η τεχνολογία Bitcoin, αν είναι κατάλληλα προσαρμοσμένη, μπορεί να χρησιμοποιηθεί αποδοτικά στην ευρωζώνη ως όπλο κατά του αποπληθωρισμού και ως μέσο παροχής της απαιτούμενης ευελιξίας για να υπογραμμίσουμε τα δημοσιονομικά. Μια τέτοια τεχνολογία μπορεί να βασιστεί σε ένα κατανεμημένο δίκτυο, έτσι ώστε κανένα άτομο ή οργάνωση να μην έχει αποκλειστικό έλεγχο επί του συστήματος και παρόλα αυτά μπορεί να παραμείνει εξαιρετικά σταθερό και ανθεκτικό χωρίς ένα μόνο σημείο αποτυχίας. Παρόλο που θα καταστεί εμφανές ότι η Bitcoin με την σημερινή της μορφή είναι πιθανώς μια κακή επιλογή για να λειτουργήσει ως σημαντικό παγκόσμιο αποθεματικό νόμισμα, ένα σύστημα που βασίζεται στην βασική τεχνολογία του - το blockchain - μπορεί στην πραγματικότητα να είναι μια βιώσιμη στρατηγική.

Η Τράπεζα της Αγγλίας, η κεντρική τράπεζα της Βρετανίας, διεξήγαγε έρευνα που βρίσκει σαφή μακροοικονομικά οφέλη για την εφαρμογή ενός ψηφιακού νομίσματος που υποστηρίζεται από την κεντρική τράπεζα ("CBDC"), βασισμένο στην τεχνολογία blockchain (Barrdear & Kumhof, 2016). Θεωρούν ότι ένα τέτοιο νόμισμα που βασίζεται ανταγωνίζεται τις τραπεζικές καταθέσεις ως μέσο ανταλλαγής θα μπορούσε να αυξήσει μόνιμα το ΑΕΠ μιας χώρας κατά 3% λόγω των μειώσεων των πραγματικών επιτοκίων, των φόρων και του

κόστους συναλλαγής. Υποστηρίζουν επίσης ότι ένα νομισματικό σύστημα κρυπτογράφησης θα συμβάλει αποφασιστικά στη σταθεροποίηση του επιχειρηματικού κύκλου.

ΚΕΦΑΛΑΙΟ 2. ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

2.1. Εισαγωγή

Την τελευταία δεκαετία, ο Bitcoin και οι κρυπτοεπιχειρήσεις γενικότερα, εισέβαλαν στις σκηνές των χρηματοπιστωτικών αγορών και σύντομα έγιναν ένα από τα πιο συζητημένα και αμφιλεγόμενα θέματα με το οποίο ασχολείται η επιστημονική κοινότητα. Το Bitcoin, το κρυπτογραφικό νόμισμα που δημιούργησε ο Satoshi Nakamoto το 2009, δημιούργησε ένα καινοτόμο φαινόμενο, που είναι ακόμα πλούσιο σε ανεξερεύνητες δυνατότητες. Αυτά τα αποκεντρωμένα νομίσματα μπορεί να αντιπροσωπεύουν την εναλλακτική λύση, την απάντηση στα πολυάριθμα ανεπίλυτα προβλήματα που προκλήθηκαν από την τελευταία οικονομική κρίση. Είναι πολύ νωρίς για να επιβεβαιωθεί αν αυτό συμβαίνει ή όχι: τα κρυπτονομίσματα είναι ακόμα σε νηπιακό στάδιο και, εκτός από το Bitcoin, μόνο λίγα από αυτά αξίζουν προσοχής. Οι πληροφορίες σχετικά με αυτά είναι διασκορπιστικές και συγκεχυμένες και συχνά προκαλούν σύγχυση, συνιστώντας ένα σοβαρό περιορισμό για την κατανόησή τους και τη διάδοσή τους στο ευρύ κοινό, το οποίο συχνά αντιδρά με δυσαρέσκεια και αμφιβολίες για τα πολλά θέματα που θέτουν τα κρυπτονομίσματα (Li & Wang, 2017). Για το λόγο αυτό, αυτό στόχος είναι να αποσαφηνιστεί το θέμα, ιδίως για το Bitcoin, προσπαθώντας να εξηγήσει τη λειτουργία του και τις επιπτώσεις του, ιδίως σε μια νομισματική πολιτική. Προτού γίνει αυτό, είναι απαραίτητο να ορισθεί η έννοια του χρήματος. Αυτό ήταν πάντα ένα δύσκολο έργο για τους οικονομολόγους, οι οποίοι, αντί να ορίσουν χρήματα για αυτό που είναι, εξέτασαν τη βασική τους λειτουργία: τα χρήματα είναι μέσο ανταλλαγής και μια λογιστική μονάδα. Αυτός ο λειτουργικός ορισμός καθιστά σαφές γιατί κατά τη διάρκεια της ιστορίας τα χρήματα έχουν πάρει διάφορες μορφές: από τα βοοειδή, το πρώτο μέσο ανταλλαγής μετά από καθαρό εμπόδιο, στα κοχύλια, στα πρώτα παραδείγματα μεταλλικών νομισμάτων. Τα κέρματα πολύτιμων μετάλλων, τα οποία έχουν επίσης μια εγγενή αξία, ήταν στο προσκήνιο για πολλούς αιώνες, μέχρι την έκδοση των πρώτων τραπεζογραμματίων. Στην αρχή, αυτά τα τραπεζογραμμάτια δεν συνδέονταν με την αξία κάποιου προϊόντος, οδηγώντας σε πολλές περιπτώσεις σε κατάχρηση της εκπομπής και της χρήσης τους (Li & Wang, 2017). Το 1816, όμως, η Αγγλία άρχισε να χρησιμοποιεί το χρυσό ως εφεδρικό εμπόρευμα για χαρτονομίσματα. Αυτό σηματοδότησε την αρχή του επονομαζόμενου Χρυσού Προτύπου. Παρά τους δύο Παγκόσμιους Πολέμους και τη Μεγάλη

Ύφεση που έδειξαν τις αδυναμίες ενός τέτοιου συστήματος, το Χρυσό Πρότυπο συνέχισε να ζει. Η διεθνής νομισματική συμφωνία του Bretton Woods το κράτησε, αν και χωρίς άμεση μετατρεψιμότητα για όλα τα νομίσματα: μόνο τα δολάρια θα μπορούσαν να ανταλλάσσονται με πραγματικό χρυσό. Αυτή η κατάσταση έγινε σύντομα μη βιώσιμη και επομένως εγκαταλείφθηκε. Με το τέλος της μετατρεψιμότητας των τραπεζογραμματίων σε χρυσό ή άλλα εμπορεύματα, έχει αρχίσει η εποχή των παραστατικών χρημάτων (fiat money). Τα παραστατικά χρήματα δεν έχουν εγγενή αξία, αλλά η αξία τους είναι εγγυημένη από την κυβέρνηση ή την κεντρική τράπεζα, η οποία την εκδίδει: ο νόμος εγγυάται και επιτρέπει τη χρήση του. Ωστόσο, η εισαγωγή του Διαδικτύου και του World Wide Web, καθώς και η απίστευτη διάδοσή του, άλλαξαν τους κανόνες και επέκτειναν το τοπίο των ποικιλιών χρήματος (Bailis & Song, 2017). Συγκεκριμένα, έχουν προκύψει τα εικονικά νομίσματα. Είναι βασικά ιδιωτικά χρήματα, αλλά με ψηφιακό χαρακτήρα: δεν έχουν φυσική οντότητα, γεννιούνται, αποθηκεύονται και χρησιμοποιούνται σε ηλεκτρονικούς υπολογιστές και άλλες ηλεκτρονικές συσκευές (smartphones, tablets κ.λπ.), επομένως αναμένεται να αποκτήσουν πάντα μεγαλύτερη σημασία καθώς αναπτύσσονται συνεχώς πιο προηγμένες τεχνολογίες. Για μερικά χρόνια ο μόνος τύπος εικονικού χρήματος ήταν ο τύπος που χρησιμοποιήθηκε σε online εφαρμογές MMORPG. Πρόκειται για παιχνίδια με βάση το πρόγραμμα περιήγησης στο web, στα οποία πολλοί παίκτες αλληλεπιδρούν μεταξύ τους online. Αυτός ο τύπος παιχνιδιών περιλαμβάνει τη δημιουργία ενός εικονικού κόσμου, συνήθως φανταστικού ή sci-fi, στον οποίο κάθε παίκτης δημιουργεί το δικό του avatar και συμμετέχει σε μια ιστορία. Στη συνέχεια, άλλες πραγματικότητες του ιστού, όπως το Facebook και το Amazon, εξέδωσαν τα δικά τους ψηφιακά νομίσματα, τα οποία θα μπορούσαν να χρησιμοποιηθούν για την αγορά περιεχομένου στο διαδίκτυο (Bailis & Song, 2017). Τα τελευταία χρόνια, ωστόσο, εμφανίστηκε ένας νέος τύπος εικονικών νομισμάτων, τα κρυπτονομίσματα. Τα κρυπτονομίσματα είναι εικονικά νομίσματα που εκμεταλλεύονται την κρυπτογραφία. Τα πρωτόκολλα κρυπτογραφικών νομισμάτων εξαρτώνται σε μεγάλο βαθμό από κρυπτογραφικές τεχνικές σε όλα τα στάδια της συναλλαγής. Μπορούν να χρησιμοποιηθούν για την αγορά οτιδήποτε, εφόσον τα μέρη που συμμετέχουν στη συναλλαγή αποδέχονται το συγκεκριμένο κρυπτογραφικό νόμισμα. Το πρώτο κρυπτονόμισμα που δημιουργήθηκε ποτέ είναι το Bitcoin. Προς το σκοπό του δημιουργού του, Satoshi Nakamoto, το Bitcoin θα πρέπει να είναι μια μαθηματική απάντηση στην ανάγκη εκτέλεσης ανώνυμων, ασφαλών και άμεσων ηλεκτρονικών πληρωμών (Nakamoto 2008). Ακόμη και αν εξακολουθούν να υπάρχουν, το φαινόμενο των εικονικών νομισμάτων, οι αλληλεπιδράσεις τους με τις

πραγματικές οικονομίες και τις συνέπειες, μελετώνται από ακαδημαϊκούς, κυρίως υπό μικροοικονομική άποψη. Η μακροοικονομική ανάλυση, αντιθέτως, είναι ακριβώς στην αρχή, με μερικές μελέτες να θέτουν ερωτήματα σχετικά με το ρόλο των παραδοσιακών χρημάτων και των κεντρικών τραπεζών, τώρα που τα εικονικά νομίσματα και τα κρυπτογραφικά νομίσματα ειδικότερα βρίσκονται στο προσκήνιο (Bailis & Song, 2017)..

Η σημασία των ψηφιακών νομισμάτων για το νομισματικό σύστημα αρχίζει να αναγνωρίζεται ακόμη και από τις κεντρικές τράπεζες. Το 2012, η ΕΚΤ δημοσίευσε μια ανασκόπηση για το τι αποκαλούν συστήματα εικονικών νομισμάτων, αναφέροντας ως παραδείγματα την υπόθεση Bitcoin και την υπόθεση Linden Dollars. Προσπαθούν να καθορίσουν μια αυστηρή προσέγγιση για τη μελέτη αυτού του φαινομένου, υπογραμμίζοντας τους κινδύνους που ενέχουν τα συστήματα εικονικών νομισμάτων (πώς ένα συγκεκριμένο εικονικό νόμισμα αλληλεπιδρά μέσα στην κοινότητα στην οποία ανήκει και, τελικά, στον πραγματικό κόσμο) στο νομισματικό σύστημα από την άποψη της σταθερότητας των τιμών, της χρηματοπιστωτικής σταθερότητας, της σταθερότητας του συστήματος πληρωμών (ECB 2012). Πριν εξετάσουμε το Bitcoin ως σχήμα εικονικού νομίσματος, πρέπει να εξηγηθούν τα χαρακτηριστικά του και ο μηχανισμός λειτουργίας του. Το Bitcoin είναι ένα ηλεκτρονικό σύστημα πληρωμών, το οποίο επιτρέπει απευθείας συναλλαγή μεταξύ δύο ατόμων. Στην πραγματικότητα, το σύστημα Bitcoin είναι αποκεντρωμένο, πράγμα που σημαίνει ότι δεν υπάρχει κεντρική τράπεζα ή αρχή, η οποία να τον ελέγχει και να εγγυάται τη σταθερότητά του. Όλες οι συναλλαγές, αντίθετα, βασίζονται σε ένα δίκτυο peer-to-peer, του οποίου η ακεραιότητα διατηρείται από τους κόμβους που ανήκουν σε αυτόν. Το Bitcoin ορίζεται ως ένα κρυπτογραφικό νόμισμα, δεδομένου ότι η κρυπτογραφία χρησιμοποιείται έντονα για την ενεργοποίηση κάθε συναλλαγής (Subramanian & Chino, 2016). Όταν μιλάμε για συναλλαγές Bitcoin, δεν μπορούμε να τις θεωρήσουμε ως παραδοσιακές συναλλαγές νομισμάτων: αντιπροσωπεύουν συμμετοχές σε ένα παγκόσμιο ψηφιακό βιβλίο. Επομένως, ας υποθέσουμε ότι ένα συμβαλλόμενο μέρος θέλει να μεταφέρει κάποια Bitcoin σε μια άλλη, πρέπει να καθορίσει την ποσότητα κερμάτων που εμπλέκονται στη συναλλαγή και να εφαρμόσει μια ψηφιακή υπογραφή στη λειτουργία, έτσι ώστε η ψηφιακή της ταυτότητα να είναι συνδεδεμένη με τη συναλλαγή (Meiklejohn et al., 2016). Είναι σημαντικό να υπογραμμίσουμε ότι οι ταυτότητες στο δίκτυο Bitcoin δεν είναι πραγματικές φυσικές ταυτότητες, είναι αριθμοί που λειτουργούν ως ψευδώνυμο για τον πραγματικό άνθρωπο πίσω από τη συναλλαγή, εξασφαλίζοντας έτσι ένα υψηλό επίπεδο ιδιωτικότητας. Μόλις καθοριστούν τα στοιχεία των συναλλαγών, μεταδίδονται σε ολόκληρο το σύστημα. Είναι

αυτή η δημόσια αποκάλυψη σε όλους τους κόμβους που εγγυάται την φερεγγυότητα της επιχείρησης στο παραλήπτη. Ωστόσο, ο τελευταίος εξακολουθεί να αντιμετωπίζει ένα πρόβλημα: πώς μπορεί να είναι σίγουρος ότι τα Bitcoin που έχουν ληφθεί δεν έχουν ήδη δαπανηθεί; Το φαινόμενο αυτό, γνωστό ως διπλή δαπάνη, είναι, στην πραγματικότητα, ένα από τα κύρια προβλήματα που πλήττουν τις ηλεκτρονικές συναλλαγές. Η κύρια καινοτομία του συστήματος Bitcoin έγκειται ακριβώς στον τρόπο που αντιμετωπίζει τις διπλές δαπάνες (Meiklejohn et al., 2016). Υπάρχουν ορισμένοι κόμβοι στο δίκτυο, γνωστοί ως miners, των οποίων η αποστολή είναι απαραίτητη για την επιβίωση και τη συντήρηση του ίδιου του δικτύου: συγκεντρώνουν όλες τις συναλλαγές που σημειώθηκαν εντός συγκεκριμένης χρονικής περιόδου σε αυτό που ονομάζεται μπλοκ συναλλαγής (Li & Wang, 2017).. Με αυτόν τον τρόπο, δίνουν ένα είδος πιστοποιητικού γνησιότητας σε κάθε συναλλαγή, επιτρέποντας σε όλους τους κόμβους να αναγνωρίζουν κάθε μπλοκ ως έγκυρο. Αυτή η απόδειξη του μηχανισμού εργασίας είναι η καρδιά της αποκεντρωμένης φύσης του συστήματος Bitcoin και ελέγχει την προσφορά χρήματος, αφού οι ανθρακωρύχοι ανταμείβονται με ολοκαίνουργιο Bitcoin για κάθε μπλοκ που δημιουργούν και μερικοί προαιρετικοί χρήστες τελών μπορούν να αποφασίσουν να τους πληρώσουν ως περαιτέρω κίνητρο για τη δραστηριότητά τους. Τέλος, η προσφορά χρήματος είναι περιορισμένη (Meiklejohn et al., 2016): το 2140 το συνολικό ποσό του Bitcoin αναμένεται να φθάσει τα 21 εκατομμύρια. Το Bitcoin δεν είναι το τέλειο νόμισμα, αλλά δείχνει κάποιους συγκεκριμένους περιορισμούς, δημιουργώντας ανησυχίες τόσο στους χρήστες όσο και στους επικριτές του. Οι κύριες ανησυχίες είναι η ασφάλεια πρωτοκόλλων, η εμπλοκή κυρίως πλαστογραφίας και η πιθανότητα κλοπών, τόσο σε επίπεδο δικτύου όσο και σε επίπεδο υλικού, καθώς και σε θέματα δεοντολογίας και ιδεολογίας σχετικά με τη χρήση Bitcoin.

Η πραγματική συμβατότητα του κινήτρου του συστήματος εξόρυξης είναι μία από τις μεγαλύτερες ανησυχίες, αλλά υπάρχουν ισχυρά επιχειρήματα για την υποστήριξή του. Η υπόθεση του MtGox είναι υποδειγματική για να συζητήσει θέματα ασφάλειας. Το MtGox ήταν μια από τις σημαντικότερες πλατφόρμες ανταλλαγής Bitcoin, με χιλιάδες χρήστες. Τον Φεβρουάριο του 2014, κήρυξε πτώχευση εξαιτίας ενός σφάλματος, το οποίο οδήγησε σε τεράστια κλοπή της Bitcoin από τους λογαριασμούς της. Ωστόσο, η αποτυχία του MtGox δεν πρέπει να θεωρείται ως αποτυχία του ίδιου του πρωτοκόλλου Bitcoin. Το εν λόγω σφάλμα, το σφάλμα ευπάθειας συναλλαγής, είναι γνωστό από το 2011 και μπορεί να καταστεί ακίνδυνο με το λογισμικό, το οποίο αναφέρει με ακρίβεια τα υπόλοιπα και τις συναλλαγές. Πράγματι, άλλες ανταλλαγές Bitcoin μπορούν να το διαχειριστούν τέλεια (Meiklejohn et al.,

2016). Μια άλλη περίπτωση που προκαλεί ανησυχίες σχετικά με αυτό το κρυπτογραφικό νόμισμα είναι η περίπτωση του Silk Road. Ο Silk Road ήταν μια ηλεκτρονική αγορά για παράνομα προϊόντα, ειδικά για τα ναρκωτικά. Ορίστηκε πράγματι ως ο «ηλεκτρονικός τρόπος για τα ναρκωτικά». Επέτρεψε στη Bitcoin ως τον μόνο μέσο πληρωμής της, λόγω της ανωνυμίας των συναλλαγών και για χρόνια οι αρχές δεν είχαν ιδέα πώς να την κλείσουν (Li & Wang, 2017).. Στις 2 Οκτωβρίου 2013, το FBI κατόρθωσε να κλείσει τον παράνομο δικτυακό τόπο και να συλλάβει τον ιδρυτή του Ulbrich, Silk Road, σε κοινή επιχείρηση με το τμήμα IRS Criminal Investigation Division, την ICE Homeland Security Investigation και την Drug Enforcement Administration. Ωστόσο, στις 6 Νοεμβρίου 2013 άνοιξε μια νέα ιστοσελίδα, το Silk Road 2.0 για επιχειρηματικούς σκοπούς, με στόχο να είναι άμεσος διάδοχος του προηγούμενου έργου. Αυτό, δυστυχώς, δεν είναι το μόνο παράδειγμα τέτοιου είδους παράνομων ηλεκτρονικών αγορών, οι οποίες μπορούν να παραμείνουν στην επιχείρηση χάρη στο Bitcoin ή σε άλλα κρυπτογραφικά νομίσματα. Φαίνεται ότι αυτή η τάση θα αυξηθεί μόνο εάν οι κυβερνήσεις και οι αρχές δεν λάβουν τις σωστές προφυλάξεις και αντίμετρα. Ωστόσο, η απαγόρευση του Bitcoin ή των εικονικών νομισμάτων γενικότερα δεν είναι το σωστό βήμα προς αυτήν την κατεύθυνση. Αντίθετα, μια λογική αφετηρία προσπαθεί να κατανοήσει καλύτερα τις συνέπειες και τις δυνατότητες των ψηφιακών νομισμάτων και να σχεδιάσει έναν τρόπο ενσωμάτωσής τους στις πραγματικότητές μας, για παράδειγμα καθορίζοντας σαφείς κανόνες για τη φορολογία και άλλα νομικά ζητήματα που τους αφορούν. Σε αυτό το σημείο, αφού συζητηθεί το κύριο χαρακτηριστικό και οι συνέπειες, το Bitcoin μπορεί να αναλυθεί στο πλαίσιο των συστημάτων εικονικών νομισμάτων. Ειδικότερα, μπορεί να αξιολογηθεί η επίδρασή της στη σταθερότητα των τιμών, στη χρηματοπιστωτική σταθερότητα και στη σταθερότητα του συστήματος πληρωμών. Από σήμερα, η Bitcoin δεν αποτελεί απειλή για τη σταθερότητα των τιμών (Tymoigne, 2015). Το μέγεθος του φαινομένου εξακολουθεί να είναι περιορισμένο. Ωστόσο, η συνάφεια της αυξάνεται καθημερινά, επομένως ο αντίκτυπος του Bitcoin σε αυτές τις πτυχές που συζητήθηκαν παραπάνω μπορεί να αλλάξει εντελώς στο μέλλον. Για το λόγο αυτό, οι νομισματικές αρχές πρέπει να είναι έτοιμες να αντιμετωπίσουν ένα τέτοιο περιστατικό, παρακολουθώντας την εξέλιξη του κρυπτογραφικού νομίσματος, προκειμένου να συνεχίσουν να εκτελούν τα καθήκοντά τους με τον καλύτερο δυνατό τρόπο. Το ίδιο συμπέρασμα μπορεί να συναχθεί για τη χρηματοπιστωτική σταθερότητα. Ωστόσο, το βάρος του Bitcoin στις χρηματοπιστωτικές αγορές αυξάνεται και υπάρχουν πτυχές του κρυπτογραφικού νομίσματος, οι οποίες θα μπορούσαν πράγματι να αποτελέσουν απειλή, αν δεν αντιμετωπιστούν με τον

σωστό τρόπο. Για παράδειγμα, δεν υπάρχει ακόμη πιστωτικό σύστημα που να σχετίζεται με την Bitcoin, αλλά εάν αρχίσουν να ξεπεράσουν τα δάνεια και τα χρέη στο Bitcoin, τότε η διασύνδεση των κρυπτονομισμάτων με το χρηματοπιστωτικό σύστημα θα γίνει πιο περίπλοκη και επικίνδυνη (Tymoigne, 2015). Τέλος, το Bitcoin εξακολουθεί να είναι ένα ασταθές σύστημα πληρωμών, στο οποίο οι χρήστες φέρουν όλους τους κινδύνους που σχετίζονται με τις συναλλαγές. Εάν ο αριθμός των ατόμων που καταφεύγουν στο Bitcoin για συναλλαγές λιανικής αυξάνεται, τότε οι κεντρικές τράπεζες πρέπει να υιοθετήσουν ορισμένα μέτρα για την προστασία του παραδοσιακού συστήματος πληρωμών από την αστάθεια που προκαλείται από την εικονική πληρωμή. Σήμερα, το Bitcoin, ως σύστημα πληρωμών, δεν μπορεί να θεωρηθεί πραγματική απειλή, αλλά αυτό δεν σημαίνει ότι θα μπορούσε να γίνει κάτι τέτοιο στο εγγύς μέλλον. Το κύριο πρόβλημα του Bitcoin ως εικονικού νομίσματος, ως νέος παίκτης στη νομισματική και χρηματοοικονομική σκηνή, είναι η έλλειψη ρύθμισης (Tymoigne, 2015). Οι κυβερνήσεις και οι αρχές έχουν πολλά προβλήματα όταν ασχολούνται με το Bitcoin, κυρίως επειδή δεν ξέρουν πώς να το ορίσουν και τη σχέση τους με τα πραγματικά νομίσματα. Ακόμα, ο χρόνος είναι αυστηρός: το Bitcoin, και τα κρυπτονομίσματα γενικότερα, έχουν γίνει μια ευρέως διαδεδομένη πραγματικότητα, η οποία δεν μπορεί πλέον να αγνοηθεί. Οι κυβερνήσεις και οι αρχές πρέπει να καθορίσουν κάποιες σαφείς κατευθυντήριες γραμμές για να επιτρέψουν μια πιο συνειδητή και υπεύθυνη χρήση των εικονικών νομισμάτων.

2.2. Τι είναι ένα κρυπτονόμισμα

Ένα κρυπτονόμισμα είναι ένα ψηφιακό ή εικονικό νόμισμα που χρησιμοποιεί την κρυπτογραφία για την ασφάλεια. Ένα καθοριστικό χαρακτηριστικό ενός κρυπτονομισμάτων, αναμφισβήτητα είναι η οργανική του φύση καθώς δεν εκδίδεται από καμία κεντρική αρχή, καθιστώντας την θεωρητικά άνομη στην κρατική παρέμβαση ή χειραγώγηση.

Όσο πιο λεπτομερής είναι ο ορισμός μας για το κρυπτονόμισμα τόσο καλύτερα μπορούμε να κατανοήσουμε τον κρυπτογραφικό χώρο. Τα κρυπτονομίσματα μπορούν να ταξινομηθούν σε τέσσερις μεγάλες κατηγορίες (Subramanian & Chino, 2016):

1. Κουπόνια νομισμάτων (Currency tokens): Το νόμισμα J είναι ένα τέλειο παράδειγμα. Ένα συμβολικό επισυνάπτεται επισήμως στο ιαπωνικό γιεν που αναπτύσσεται επί του παρόντος.

2. Κουπόνια χρησιμότητας (Utility tokens): Το Ethereum είναι ένα καλό παράδειγμα χρησιμότητας. Το Ethereum είναι μια αποκεντρωμένη πλατφόρμα που εκτελεί έξυπνες συμβάσεις.
3. Κουπόνια συμμετοχής (Membership tokens): Το Storj είναι ένα καλό παράδειγμα για ένα κουπόνι συμμετοχ΄ης. Είναι μια αποκεντρωμένη πλατφόρμα αποθήκευσης cloud που επιτρέπει σε οποιονδήποτε να νοικιάσει τον χώρο του σκληρού δίσκου σε αδράνεια και να κερδίσει έσοδα με αυτόν τον τρόπο. Οι τελικοί χρήστες μπορούν να χρησιμοποιήσουν το Storj για να αποθηκεύσουν τα αρχεία τους σε ανταγωνιστικές τιμές και μέσα σε ένα δίκτυο p2p που είναι ασφαλές από downtime server, λογοκρισία και hacks.
4. Κουπόνια ασφαλείας (Security tokens): Το TaaS αποτελεί καλό παράδειγμα για την τελευταία κατηγορία: Είναι ένα επενδυτικό ταμείο που έχει σχεδιαστεί για να επενδύσει σε αγορές μπλοκ.

Το κρυπτονόμισμα είναι ένα σχετικά νέο φαινόμενο και τεχνολογία βασισμένη στην κρυπτογραφία, η οποία ξεκίνησε με την Bitcoin το 2009. Το ψηφιακό νόμισμα, Bitcoin, δημιουργήθηκε από τον Satoshi Nakamoto και ήταν το πρώτο κρυπτονόμισμα που διατέθηκε στην αγορά το 2009. Ο Satoshi Nakamoto είχε κουραστεί από τις τράπεζες και τις χρηματοπιστωτικές κρίσεις που ξεκίνησαν και αποφάσισε να δημιουργήσει ένα νόμισμα που οι χώρες δεν μπορούν να ελέγξουν. Έχει επεκταθεί και αναπτύσσεται τα τελευταία χρόνια και μπορεί, λόγω της πρόσφατης νέας δημοτικότητας και της επέκτασης της αγοράς, να αποκτηθεί με πολλά διαφορετικά σχήματα και μορφές. Από τη συγγραφή της παρούσας εργασίας έχουν καταχωρηθεί πάνω από 1600 διαφορετικά κρυπτονομίσματα (CoinMarketCap, 2017). Παρόλο που υπάρχει ένας μεγάλος αριθμός διαφορετικών κρυπτονομισμάτων που διατίθενται με διαφορετικούς στοχευμένους τομείς εφαρμογών και χρήσεις, πολλά από αυτά μπορούν να θεωρηθούν ως εξαιρετικά ασταθή και έχουν αποκαλύψει πιθανά ή χαμηλά ποσοστά υιοθέτησης της αγοράς. Η εργασία αυτή θα περιορίσει τη μελέτη εστιάζοντας στις πιο συνηθισμένα και δημοφιλή κρυπτονομίσματα από την κεφαλαιοποίηση της αγοράς. Αυτό περιλαμβάνει κρυπτονομίσματα όπως Bitcoin, Ethereum, Ripple, Bitcoin Cash και Litecoin. Το κοινό στοιχείο κρυπτονομισμάτων βρίσκεται στο δημόσιο αρχείο καταχωρήσεων (public ledger) του που αναφέρεται συχνά ως η "αλυσίδα μπλοκ", μια σύνδεση μεταξύ των μελών του δικτύου και η χρήση του ψηφιακού κρυπτονομίσματος του δικτύου (Tymoigne, 2015).

2.3. Κρυπτονομίσματα απο την κεντροποίηση στην αποκεντροποίηση

Το κύριο μειονέκτημα του παραδοσιακού συστήματος πληρωμών με κυμαινόμενο επιτόκιο είναι τα υψηλά τέλη συναλλαγών με μακρά περίοδο διακανονισμού, η οποία οδήγησε τους ανθρώπους σε εναλλακτικά νομίσματα που επιτρέπουν μικρότερο χρόνο διεκπεραίωσης (peer-to-peer-P2P) χωρίς μεσάζοντες, με αποτέλεσμα μια ακμάζουσα αγορά για ψηφιακά νομίσματα που έχουν χαμηλότερο κίνδυνο διακανονισμού. Πριν από τη δημιουργία των κρυπτονομισμάτων, υπήρχαν πολλοί άλλοι τύποι ψηφιακών νομισμάτων. Το πιο συνηθισμένο παράδειγμα είναι ένα ψηφιακό νόμισμα που δημιουργήθηκε από ένα ίδρυμα και πραγματοποιήθηκε σε πλατφόρμα. Αυτά τα νομίσματα μπορεί να είναι πόντοι πιστότητας/αφοσίωσης (loyalty points) που δημιουργούνται από εταιρείες ή ψηφιακά κέρματα που ορίζονται από πλατφόρμες με βάση το Διαδίκτυο. Τα ιδρύματα ή οι νομικές οντότητες ελέγχουν τη δημιουργία, τη συναλλαγή, τη λογιστική και την επαλήθευση των ψηφιακών νομισμάτων (Tymoigne, 2015).

Με άλλα λόγια, αυτά τα ψηφιακά νομίσματα που βασίζονται σε πλατφόρμες είναι κεντροποιημένες (centralized). Ένα αξιοσημείωτο παράδειγμα είναι οι πόντοι αφοσίωσης των εταιρειών ηλεκτρονικού εμπορίου όπως το Rakuten και το iHerb, τα οποία λειτουργούν σαν μετρητά στην πλατφόρμα. Το Q-coin, που εισήχθη από την κινεζική κοινωνική πλατφόρμα Tencent, μπορεί να αγοραστεί χρησιμοποιώντας το Renminbi και μπορεί να χρησιμοποιηθεί για να αγοράσει κάποιος υπηρεσίες στο Tencent. Το World of Warcraft Gold είναι ένα παιχνίδι που μπορεί να κερδηθεί μόνο μέσω της ολοκλήρωσης των δραστηριοτήτων εντός του παιχνιδιού και δεν μπορεί να αγοραστεί ή να ανταλλαγεί σε νομίσματα fiat (Gendal & Halaburda, 2016).

Αυτά τα κεντρικά ψηφιακά νομίσματα διεκπεραιώνονται σε μια συγκεκριμένη πλατφόρμα και έχουν σχεδιαστεί για να υποστηρίζουν την επιχειρηματική δραστηριότητα των ιδρυμάτων που τα εκδίδουν. Είναι δύσκολο να τα χρησιμοποιηθούν ως υποκατάστατο χρημάτων, επειδή αυτά τα κενροποιημένα (centralized) ψηφιακά νομίσματα δεν αποτελούν νόμιμο χρήμα. Ως εκ τούτου, τα αποκεντρωμένα ψηφιακά νομίσματα φαίνεται να αποτελούν πιθανή αντικατάσταση για τα χρήματα με την επιφύλαξη ότι δεν απαιτείται κεντρική αρχή για την επαλήθευση των συναλλαγών. Ωστόσο, εξακολουθούν να υπάρχουν πολλά εμπόδια που πρέπει να αντιμετωπιστούν χωρίς τη χρήση μιας ενδιάμεσης ή κεντρικής αρχής. Ένα κύριο εμπόδιο είναι το πρόβλημα των διπλών δαπανών: Είναι δυνατόν να ξοδέψετε το ίδιο

ψηφιακό νόμισμα περισσότερες από μία φορές (Meiklejohn et al., 2016). Το πρόβλημα αυτό έχει παραμείνει άλυτο για μεγάλο χρονικό διάστημα, αποθαρρύνοντας την επικράτηση των αποκεντρωμένων κερμάτων. Για να διασφαλιστεί ότι κάθε συναλλαγή αντικατοπτρίζεται με ακρίβεια στο υπόλοιπο του λογαριασμού για τα ψηφιακά νομίσματα για να αποφευχθεί η διπλή δαπάνη, υπάρχει ανάγκη για ένα έμπιστο σύστημα χωρίς κεντρική αρχή.

Η πρώτη κρυπτογράφηση, eCash, ήταν ένα συγκεντρωτικό σύστημα που ανήκει στην DigiCash, Inc. και αργότερα στην eCash Technologies. Παρόλο που καταργήθηκε στα τέλη της δεκαετίας του 1990, me τα κρυπτογραφικά πρωτόκολλα που χρησιμοποιούσαν αποφεύγονταν διπλές δαπάνες. Μια τυφλή υπογραφή χρησιμοποιήθηκε για την προστασία της ιδιωτικής ζωής των χρηστών και χρησίμευσε ως μια καλή έμπνευση για την περαιτέρω ανάπτυξη. Λίγο μετά την ανακάλυψη των πρωτοκόλλων κρυπτογράφησης, το ψηφιακό χρυσό νόμισμα έγινε δημοφιλές, μεταξύ των οποίων το πιο χρησιμοποιημένο ήταν το e-Gold. Ήταν το πρώτο επιτυχημένο σύστημα μικροπληρωμών στο διαδίκτυο και οδήγησε σε πολλές καινοτομίες, καθιστώντας τις συναλλαγές περισσότερο προσβάσιμες και ασφαλέστερες. Ωστόσο, η αποτυχία αντιμετώπισης των ζητημάτων συμμόρφωσης οδήγησε τελικά στην εκκαθάρισή της το 2008, παρά το γεγονός ότι ο ετήσιος όγκος συναλλαγών υπερβαίνει τα 2 δισ. Δολάρια (Lam & Lee, 2015).

Η παγκόσμια χρηματοπιστωτική κρίση το 2008, σε συνδυασμό με την έλλειψη εμπιστοσύνης στο χρηματοπιστωτικό σύστημα, προκάλεσε έντονο ενδιαφέρον για τα κρυπτονομίσματα. Μια πρωτοποριακή ιδέα του Satoshi Nakamoto κυκλοφόρησε ηλεκτρονικά το 2008. Στην έρευνα αυτή εισήγαγαν ένα ψηφιακό νόμισμα που είναι ευρέως γνωστό ως bitcoin. Το Bitcoin χρησιμοποιεί το blockchain ως το «δημόσιο κατάλογο» για όλες τις συναλλαγές και ένα πρόγραμμα που ονομάζεται PoW για να αποφευχθεί η ανάγκη μιας έμπιστης αρχής ή ενός κεντρικού διακομιστή για συναλλαγές χρονικής σήμανσης (Nakamoto, 2008). Επειδή το blockchain είναι ένας ανοιχτός και κατανεμημένος λογαριασμός που καταγράφει όλες τις συναλλαγές με έναν επαληθεύσιμο και μόνιμο τρόπο, επιλύει το πρόβλημα των διπλών δαπανών.

2.4. Bitcoin

Ο Satoshi Nakamoto, ο δημιουργός του Bitcoin, ορίζει ένα ηλεκτρονικό νόμισμα ως μια αλυσίδα ψηφιακών υπογραφών. Βασικά αυτό σημαίνει ότι κάθε νόμισμα έχει ψηφιακό

κλειδί. Όταν πραγματοποιείται μια συναλλαγή, ο συναλλασσόμενος πραγματοποιεί μια ψηφιακή υπογραφή της προηγούμενης συναλλαγής. Η συναλλαγή χρειάζεται επίσης το δημόσιο κλειδί του δέκτη. Η υπογραφή και το δημόσιο κλειδί προστίθενται στη συνέχεια στο τέλος του νομίσματος. (Satoshi Nakamoto, 2008)

Ένα πρόβλημα που προκύπτει από τις συναλλαγές είναι η πιθανότητα διπλών δαπανών, για παράδειγμα, ότι οι ιδιοκτήτες προσπαθούν να διπλασιάσουν το νόμισμα. Αυτό μπορεί να λυθεί με την εμφάνιση ολόκληρου του ιστορικού των συναλλαγών όλων των κερμάτων και ενός δικτύου συμμετεχόντων, οι οποίοι μπορούν να συμφωνήσουν σχετικά με το ενιαίο ιστορικό των εντολών και με ποια σειρά παραλαμβάνονται. Αυτό καθιστά το σύστημα συναλλαγών προστατευτικό και επίσης πολύ ασφαλέστερο από τα τρέχοντα νομίσματα, γιατί αν κάποιος θέλει να εισέλθει στο σύστημα Bitcoin χρειάζεται την πλειοψηφία της δύναμης υπολογισμού (CPU) στον κόσμο, η οποία είναι σχεδόν αδύνατη, με ακόμη περισσότερους miners που εισέρχονται στην αγορά κάθε μέρα. Επίσης, οι κανονικοί υπολογιστές στην αγορά δεν έχουν τη δύναμη υπολογισμού που χρειάζεται το σύστημα, γι 'αυτό και οι miners έχουν ειδικούς υπολογιστές ειδικά κατασκευασμένους για Bitcoins mining (Nakamoto, 2008).

Η παραπάνω εικόνα καταδεικνύει την ιδιωτικότητα που ασκείται από το παραδοσιακό τραπεζικό μοντέλο και το νέο μοντέλο προστασίας της ιδιωτικής ζωής. Το παραδοσιακό τραπεζικό μοντέλο επιτυγχάνει τον στόχο της προστασίας της ιδιωτικής ζωής, περιορίζοντας την πρόσβαση σε όλα τα εμπλεκόμενα μέρη. Για παράδειγμα, στο χρηματιστήριο ανακοινώνουν όλες τις συναλλαγές (χρόνο και μέγεθος συναλλαγών) χωρίς να λένε ποιοι είναι οι συμβαλλόμενοι. Αλλά οι πληροφορίες είναι εντός των χρηματοπιστωτικών εταιρειών, πράγμα που σημαίνει ότι μπορείτε να μάθετε ποιος πραγματικά αγόρασε εάν κάποιος έχει τη σωστή πρόσβαση. Το νέο μοντέλο απορρήτου δίνει στο κοινό όλες τις συναλλαγές (δημόσια κλειδιά), χωρίς να λέει ποια είναι τα μέρη. Και είναι αδύνατο να ανακαλύψετε ποιος μεταβίβασε τα χρήματα και σε ποιους, είναι δυνατή μόνο η απόκτηση των δημόσιων κλειδιών. Τα δημόσια κλειδιά δεν μπορούν να συνδεθούν με ένα συγκεκριμένο άτομο. Εάν το ίδιο πρόσωπο διεξάγει πολλαπλές συναλλαγές με το ίδιο κλειδί, υπάρχει ελάχιστη πιθανότητα να εκθέσει τον εαυτό του, γι 'αυτό και ο Nakamoto συνιστά προσθήκη στην ασφάλεια της ιδιωτικής ζωής δημιουργώντας ένα νέο ζευγάρι κλειδιών για κάθε συναλλαγή (Nakamoto, 2008).

Σύμφωνα με τη Meiklejon et al (2016), το Bitcoin είναι ένα καθαρά ηλεκτρονικό εικονικό νόμισμα, χωρίς να υπονομεύεται ούτε από φυσικά προϊόντα ούτε από κυρίαρχη

υποχρέωση. Αντίθετα, βασίζεται σε ένα συνδυασμό κρυπτογραφικής προστασίας και ενός πρωτοκόλλου ομότιμου-ομότιμου για τον εντοπισμό των οικισμών. Ως εκ τούτου, η Bitcoin έχει την αόριστη ιδιότητα ότι ενώ η ιδιοκτησία των χρημάτων είναι σιωπηρώς ανώνυμη, η ροή της είναι παγκοσμίως ορατή. Οι παραπάνω συγγραφείς, οι Meiklejon et al (2016, σελ. 87) εξηγούν ότι ένα bitcoin μπορεί να θεωρηθεί ως μια αλυσίδα συναλλαγών από έναν ιδιοκτήτη στο επόμενο, όπου οι ιδιοκτήτες αναγνωρίζονται από ένα δημόσιο κλειδί από εδώ και έξω, μια διεύθυνση που χρησιμεύει ως ψευδώνυμο. δηλαδή οι χρήστες μπορούν να χρησιμοποιήσουν οποιοδήποτε αριθμό διευθύνσεων και η δραστηριότητά τους χρησιμοποιώντας ένα σύνολο διευθύνσεων δεν συνδέεται εγγενώς με τη δραστηριότητά τους χρησιμοποιώντας ένα άλλο σύνολο ή με την πραγματική ταυτότητά τους.

Το Bitcoin είναι το κύριο κρυπτονομίσμα στην αγορά, με σχεδόν επταπλάσια κεφαλαιοποίηση της αγοράς, σε σχέση με το κρυπτονομίσματα, το Ethereum. Αυτό συνδυάζεται με το γεγονός ότι οι περισσότερες κρυπτοεπιχειρήσεις βασίζονται γύρω από την τεχνολογία ίδρυσης που εισήγαγε το Bitcoin, καθιστά σημαντικό για τις μελλοντικές συζητήσεις ότι το Bitcoin είναι κατανοητό σωστά τόσο ως τεχνολογία όσο και ως βασικός παίκτης στην αγορά κρυπτογράφησης (Coin Market Cap, 2017).

Τα Cryptocurrencies, όπως το Bitcoin, δημιουργούνται από την εξόρυξη (dta mining), πράγμα που σημαίνει ότι οι υπολογιστές επιλύουν δύσκολους αλγόριθμους και παίρνουν ως ανταμοιβή ένα ορισμένο ποσό νομισμάτων. Το όλο δίκτυο Bitcoin, όπου εξορύσσονται νέα νομίσματα και αποστέλλονται συναλλαγές, διατηρείται από μια τεράστια δεξαμενή υπολογιστών που επιλύει δύσκολους αλγόριθμους. Αυτό σημαίνει ότι δεν θα υπήρχαν Bitcoins χωρίς το δίκτυο υπολογιστών και δεν θα μπορούσαν να δημιουργηθούν περισσότερα Bitcoins εκτός του δικτύου υπολογιστών. Το ψηφιακό νόμισμα Bitcoin βασικά λειτουργεί με τον ίδιο τρόπο όπως ένα κανονικό νόμισμα, έχει την πλειοψηφία του νόμισμα στο Διαδίκτυο και με το νόμισμα μπορείτε να αγοράσετε διαφορετικά είδη ή υπηρεσίες. Ο κύριος λόγος για τη δημιουργία του Bitcoin ήταν να εξαλείψει το αξιόπιστο τρίτο μέρος στις συναλλαγές, γεγονός που συνεπάγεται κόστος μεταξύ του. Ο στόχος ήταν να επιτευχθεί ένα κρυπτονόμισμα, όπου ένα άτομο θα μπορούσε να μεταφέρει το νόμισμα σε άλλο πρόσωπο οπουδήποτε στον κόσμο χωρίς υψηλά έξοδα συναλλαγών και χωρίς να παρακολουθεί τη συναλλαγή ένα τρίτο μέρος (Li & Wang, 2017).

Τα κρυπτονομίσματα είναι κατασκευασμένα έτσι ώστε κανείς να μην επιταχύνει την ποσότητα κρυπτογραφημένων χρημάτων στην αγορά, επειδή έχει τις μεταβλητές της που καθορίζουν πόσα κέρματα μπορούν να εξορύσσονται ή με άλλο τρόπο απελευθερώνονται.

Αυτό σημαίνει ότι κανείς δεν μπορεί πραγματικά να ελέγξει το νόμισμα. Όμως, επειδή η αξία των κρυπτονομισμάτων βασίζεται στην προσφορά και την ζήτηση, μπορεί να αυξηθεί ή να μειωθεί δραστικά εάν ξαφνικά αγοραστεί ή πωληθεί τεράστιο ποσό του νομίσματος. Η απότομη αύξηση της ζήτησης του Bitcoin και η αργή ταχύτητα με την οποία εξορύσσονται τα νέα Bitcoins οδηγούν σε τεράστια αύξηση αξίας τον Ιανουάριο 2012 από 10 USD σε 100 USD τον Μάρτιο του 2012. Στη συνέχεια, ο Bitcoin αυξήθηκε από 100 USD σε 1000 USD μεταξύ Μαρτίου και τον Δεκέμβριο του 2012. Από τότε το νόμισμα έχει υποστεί πολλές επικρίσεις, γεγονός που είναι προς το παρόν (24 Ιανουαρίου 2014) εκτιμώμενο σε περίπου 570 δολάρια ανά Bitcoin (Li & Wang, 2017).

2.4.1 Εξέλιξη και αποδοχή

Ανάλογα με την προοπτική, η σημασία του Bitcoin μπορεί να φανεί πολύ διαφορετική. Όπως αναφέρθηκε προηγουμένως, η τεχνολογική πτυχή είναι σαφώς σημαντική. Ο Michael (2013) διερευνά τις τεχνολογίες του μέλλοντος και παρουσιάζει το Bitcoin ως μία από τις τρεις τεχνολογίες που θα αμφισβητήσουν τις αρχές. Οι άλλες δύο είναι η Κοινή χρήση αρχείων και η εκτύπωση 3D. Ωστόσο, δεν υπάρχει αμφιβολία ότι η τρέχουσα κατάσταση του Bitcoin είναι ακόμα αβέβαιη και είναι εύκολο να υποστηρίξουμε ότι θα είναι δύσκολο για την τεχνολογία να αποκτήσει ευρύτερη αποδοχή. Ο Evans-Pughe (2012) υποστηρίζει ότι η φιλικότητα προς το χρήστη του Bitcoin εμποδίζει την αποδοχή του, περιγράφοντας την τρέχουσα φάση ανάπτυξης ως το Διαδίκτυο χωρίς το πρόγραμμα περιήγησης στο Web. Παρόλο που το Διαδίκτυο και οι ηλεκτρονικές υπηρεσίες έχουν αναπτυχθεί σημαντικά από τις πρώτες μέρες του Διαδικτύου, για κάποιο λόγο οι τεχνολογικοί κολοσσοί δεν κατάφεραν να αναλάβουν τον τραπεζικό κλάδο. Ο Valentine (2012) εξετάζει το γεγονός ότι στη δεκαετία του 1990 η Microsoft και το Yahoo αναμενόταν να αποεπενδύσουν τις τράπεζες. Ωστόσο, είναι σαφές ότι αυτό δεν συνέβη και οι τράπεζες μπόρεσαν να λειτουργήσουν ουσιαστικά με τον ίδιο τρόπο όπως και πριν. Σύμφωνα με τον Valentine, οι τράπεζες αξιοποίησαν την εμπιστοσύνη της πελατειακής βάσης. Υποστηρίζει ότι αυτή η εμπιστοσύνη και η μεγαλύτερη ευκολία που απαιτείται από μια νέα υπηρεσία εξηγούν από κοινού γιατί η διαχείριση των προσωπικών οικονομικών δεν έχει δει την υιοθέτηση μεγάλης κλίμακας που είχε προβλεφθεί στη δεκαετία του 1990. Ίσως το Bitcoin θα μπορέσει να προωθήσει αυτήν την εξέλιξη.

Η αποδοχή του Bitcoin αυξάνεται συνεχώς καθώς όλο και περισσότεροι έμποροι το δέχονται ως τρόπο πληρωμής, είτε απευθείας είτε μέσω τρίτου παρόχου υπηρεσιών. Ορισμένες μικρές περιοχές, όπως το Kreuzberg στη Γερμανία, έχουν ένα πολύ υψηλό επίπεδο αποδοχής, αλλά η αστάθεια της συναλλαγματικής ισοτιμίας του bitcoin αποτελεί πρόκληση για την αξιοπιστία του σε ευρύτερη κλίμακα (Neroth, 2013). Σύμφωνα με τους επαγγελματίες του χρηματοπιστωτικού τομέα, η έλλειψη ρευστότητας, η ανύπαρκτη τυποποιημένη αγορά, η ανικανότητα αντιστάθμισης των κινδύνων, η έλλειψη ασφάλειας και η έλλειψη ρύθμισης της αγοράς είναι οι άλλοι σημαντικοί λόγοι για να αποφευχθεί η συμμετοχή στο Bitcoin (Stark, 2013). Προς το παρόν, τα bitcoins φαίνονται απλά πολύ επικίνδυνα. Ωστόσο, μια άλλη προοπτική του Luther (2013) τονίζει το σκεπτικισμό προς το σημερινό χρηματοπιστωτικό σύστημα και την αβεβαιότητα της μελλοντικής αγοραστικής δύναμης των υφιστάμενων χρημάτων. Στο άρθρο του ο Luther αναζητά λόγους για τους οποίους το Bitcoin δεν έχει κερδίσει ευρύτερη αποδοχή και διαπιστώνει ότι οι επιπτώσεις στο δίκτυο και το κόστος αλλαγής πρέπει να είναι οι κύριοι λόγοι γι 'αυτό. Δηλώνει ακόμη ότι τα κρυπτονομίσματα όπως το Bitcoin δεν θα επιτύχουν ευρεία αποδοχή χωρίς σημαντική νομισματική αστάθεια ή κυβερνητική υποστήριξη. Ένα παράδειγμα νομισματικής αστάθειας που προκαλεί στους καταναλωτές τη χρήση ενός συστήματος χωρίς επίσημη έγκριση είναι η περίπτωση του ελβετικού δηναρίου στο Ιράκ (Grinberg, 2011). Σε αυτή την περίπτωση, αναμφισβήτητα σημαντική νομισματική αστάθεια ήταν ο λόγος για τον οποίο οι καταναλωτές χρησιμοποίησαν χρήματα που εγκαταλείφθηκαν επισήμως και δεν είχαν καμία εγγενή αξία. Από την άλλη πλευρά, είναι καλό να θυμόμαστε ότι στην περίπτωση του Ελβετικού Δηναρίου, ήταν το προηγούμενο σύστημα που οι άνθρωποι ήταν πρόθυμοι να χρησιμοποιήσουν, καθιστώντας τη μετάβαση σε Bitcoin διαφορετική στην περίπτωση της νομισματικής αστάθειας. Είναι ενδιαφέρον ότι μπορεί κανείς να συγκρίνει την αποδοχή του Bitcoin σε προηγούμενα παρόμοια συστήματα και να παρατηρήσει ότι ήταν πραγματικά πολύ επιτυχημένη. Οι Barber et al. (2012) χρησιμοποιούν αυτήν την προοπτική και συγκρίνουν το Bitcoin με άλλα συστήματα ηλεκτρονικών χρημάτων. Βρίσκουν πολλούς τρόπους με τους οποίους το Bitcoin φαίνεται να είναι ανώτερο από τα προηγούμενα συστήματα, αλλά ο πιο κρίσιμος παράγοντας φαίνεται να είναι ο επιτυχημένος σχεδιασμός κινήτρων για συμμετοχή στο δίκτυο Bitcoin. Κατά την αξιολόγηση του μακροπρόθεσμου δυναμικού του Bitcoin, η έρευνα εξετάζει επίσης προσεκτικά τις αδυναμίες και τα μειονεκτήματα του συστήματος και καταλήγει στο συμπέρασμα ότι, εάν εφαρμοστεί σωστά, ο σχεδιασμός θα μπορούσε να υποστηρίξει ένα ισχυρό αποκεντρωμένο νόμισμα.

Ο Cedillo (2013) παρουσιάζει μια άλλη ενδιαφέρουσα προοπτική της νομισματικής ανάπτυξης και περιγράφει τον τρόπο με τον οποίο η σκιώδης τραπεζική βιομηχανία παρουσίασε πολλές οικονομικές καινοτομίες τις οποίες ο υπόλοιπος οικονομικός κόσμος τις αποδέχθηκε αργότερα. Η συζήτησή του αναφέρει επίσης ότι ακόμη και η Ευρωπαϊκή Κεντρική Τράπεζα έχει αναγνωρίσει ότι το ρυθμιστικό της πλαίσιο υστερεί από τεχνολογικές εξελίξεις κατά έτη. Μπορεί κάποιος να χαρακτηρίσει το Bitcoin ως μέρος της σκιώδους τραπεζικής επειδή είναι ένα νομισματικό σύστημα που λειτουργεί εκτός του επίσημου χρηματοπιστωτικού συστήματος. Από αυτή την άποψη, το Bitcoin θα μπορούσε να αντιπροσωπεύει μια τέτοια καινοτομία που ο επίσημος χρηματοπιστωτικός κόσμος θα αγκαλιάσει με τη μία ή την άλλη μορφή στο μέλλον.

2.4.2 Ο ρόλος του χρήματος και η ρύθμιση

Ο Lemieux (2013) εξετάζει πώς η ευρεία αποδοχή του Bitcoin δεν είναι προς το συμφέρον των κυβερνήσεων. Θα οδηγούσε σε απώλεια ελέγχου που καθιστά δύσκολη ή και αδύνατη την εκτέλεση της νομισματικής πολιτικής. Αυτό θα μπορούσε να αλλάξει θεμελιωδώς τον τρόπο χρηματοδότησης των κρατών. Σύμφωνα με τον Lemieux, είναι πολύ αβέβαιο αν το ρυθμιστικό κράτος επιτρέπει στην Bitcoin να αναπτυχθεί περαιτέρω. Δηλώνει ακόμη ότι το ρυθμιστικό κράτος θα μπορούσε απλώς να μην συμφωνήσει με αυτό το πείραμα. Αν και η τεχνολογική «θανάτωση» του δικτύου Bitcoin είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η ρύθμιση μπορεί να χρησιμοποιηθεί για να επηρεάσει τις πύλες μεταξύ παραστατικών νομισμάτων (fiat) και bitcoins (Varriale, 2013). Μια πιο φουτουριστική περιγραφή της ρύθμισης Bitcoin δίνεται από τον Plassaras (2013), ο οποίος αντιλαμβάνεται πώς το ΔΝΤ θα μπορούσε ενδεχομένως να επιτρέψει σε ένα μέλος για χρήση εικονικών νομισμάτων όπως το Bitcoin να συλλέξει ένα απόθεμα bitcoins για απορρόφηση ζημιών με αναντιστοιχία λήξης για τη σταθεροποίηση των συναλλαγματικών ισοτιμιών. Η έρευνα αναφέρει ότι η συμμετοχή του ΔΝΤ θα ήταν ένας τρόπος αποφυγής των αρνητικών επιπτώσεων μιας μελλοντικής κερδοσκοπικής επίθεσης στα νομίσματα fiat που πραγματοποιούνται από κατόχους bitcoin. Ο Plassaras (2013) δεν εκτιμά ποια θα είναι η αγοραία αξία των bitcoins για να είναι δυνατή μια τέτοια επίθεση. Αν και η συμμετοχή του ΔΝΤ θα μπορούσε θεωρητικά να σταθεροποιήσει τις συναλλαγματικές ισοτιμίες, η συγκέντρωση επαρκούς αποθέματος στην πράξη θα ήταν προβληματική.

2.4.3 Κατηγοριοποίηση

Λόγω των νέων χαρακτηριστικών του, είναι πολύ δύσκολο να κατηγοριοποιηθεί το Bitcoin. Παρόλο που έχει κάποια χαρακτηριστικά του χρήματος, του εμπορεύματος και ακόμη και του αποθέματος, δεν υπάρχει άμεση σχέση με καμία από αυτές τις παραδοσιακές κατηγορίες. Ο Toma (2012) περιγράφει το Bitcoin απλώς ως σύστημα ηλεκτρονικού χρήματος το οποίο μπορεί να χρησιμοποιηθεί και για κινητές πληρωμές. Ο Yermack (2013) αναφέρεται στη κατηγοριοποίηση του Bitcoin ως νομίσματος, δηλώνοντας ότι το Bitcoin φαίνεται να συμπεριφέρεται περισσότερο σαν μια κερδοσκοπική επένδυση παρά σαν ένα νόμισμα. Το επιχείρημα αυτό βασίζεται στην μεταβλητότητα του bitcoin και στο γεγονός ότι οι ημερήσιες συναλλαγματικές ισοτιμίες του bitcoin παρουσιάζουν ουσιαστικά μηδενική συσχέτιση με τα νομίσματα fiat. Επίσης, είναι διαθέσιμες πιο εξελιγμένες προσπάθειες κατηγοριοποίησης κρυπτονομισμάτων. Η Wells (2011) προτείνει πέντε κατηγορίες για συστήματα ψηφιακού νομίσματος:

1. Barter Exchange Software Systems
2. Non-Bank Digital Currency Payment Systems
3. Digital Precious Metal Systems
4. Online Value Transfer Software Systems,
5. Online Stored Value Transaction Software Systems

Σύμφωνα με την Wells, το Bitcoin ανήκει στην κατηγορία των ηλεκτρονικών συστημάτων λογισμικού μεταφοράς αξίας (Online Value Transfer Software Systems,). Ενώ η Wells επικεντρώνεται αποκλειστικά σε συστήματα ψηφιακών νομισμάτων, οι Bergstra και Leeuw (2013) υιοθετούν μια γενικότερη προοπτική και μιλάνε για τα πληροφοριακά χρήματα. Πιο συγκεκριμένα, κατηγοριοποιούν το Bitcoin ως αποκλειστικά πληροφοριακό χρήμα (Exclusively Informational Money/EXIM), επειδή τα πληροφοριακά νομίσματα ενός EXIM μπορούν να βρίσκονται υπό τον έλεγχο κάποιου αλλά δεν ανήκουν σε κανέναν. Ο Selgin (2013) εξετάζει την ιστορική εξέλιξη των νομισματικών συστημάτων και κατηγοριοποιεί το Bitcoin ως συνθετικό χρηματικό προϊόν. Σύμφωνα με τον Selgin (2013) τα

συνθετικά χρήματα σε βασικά προϊόντα δεν πρέπει να υποστηρίζονται ούτε από την ιδιότητα του νόμιμου ούτε από την είσπραξη δημόσιων πληρωμών, αν και αυτά τα χαρακτηριστικά θα μπορούσαν βέβαια να συμβάλουν στην σταθερότητα της αξίας και της αγοραστικής δύναμής του.

2.4.4 Επένδυση

Ως επένδυση, το bitcoin είναι ένα μέσο υψηλής μεταβλητότητας και υψηλού κινδύνου. Για να κατανοήσουμε καλύτερα αυτόν τον κίνδυνο, θα ήταν σημαντικό να κατανοήσουμε τους παράγοντες της μεταβλητότητας αυτής και τον τρόπο με τον οποίο θα μπορούσαν να χρησιμοποιηθούν τα bitcoins στα επενδυτικά χαρτοφυλάκια. Με βάση τα στοιχεία των Hommes et al. (2008), Husler et al. (2013) εξετάζει την εμφάνιση φουσκών (bubbles) που παρουσιάζουν ταχύτερη από την εκθετική ανάπτυξη. Η φούσκα και η συντριβή του Bitcoin τον Απρίλιο του 2013 αναφέρονται ως ένα τέτοιο παράδειγμα. Η μελέτη χρησιμοποιεί ένα εργαστηριακό πείραμα μάθησης-πρόβλεψης με ανθρώπους και καταλήγει στο συμπέρασμα ότι αυτοί οι τύποι υπερ-εκθετικών φουσκών μπορεί να εμφανιστούν σε μια τέτοια ρύθμιση. Στην πραγματικότητα, ένα κοινό χαρακτηριστικό τέτοιων φουσκών είναι ότι οι τιμές είναι μόνο χαλαρά συνδεδεμένες με τα θεμελιώδη στοιχεία. Η μελέτη αυτή βοηθάει στην κατανόηση του τρόπου με τον οποίο οι δραματικές διακυμάνσεις των τιμών ήταν δυνατές επειδή το bitcoin είναι εντελώς αποσυνδεδεμένο από τα θεμελιώδη στοιχεία. Μια άλλη ενδιαφέρουσα μελέτη για τους οδηγούς της τιμής bitcoin είναι ην έρευνα του Kristoufek (2013), ο οποίος εξετάζει τη σύνδεση των δεδομένων της Google Trends και της δραστηριότητας Wikipedia με την τιμή του bitcoin. Οι Briere et al. (2013) σε μελέτη με το bitcoins ως μέρος ενός χαρτοφυλακίου επενδύσεων με τη διεξαγωγή δοκιμών κάλυψης για την αξιολόγηση της χρηστικότητας του bitcoin σε ένα διαφοροποιημένο χαρτοφυλάκιο. Το χαρτοφυλάκιο των παραδειγμάτων τους περιλαμβάνει παγκόσμιες μετοχές, ομόλογα, νομίσματα, εμπορεύματα, αμοιβαία κεφάλαια κινδύνου και ακίνητα. Η μελέτη διαπιστώνει ότι η ενσωμάτωση των bitcoins στο χαρτοφυλάκιο προσφέρει σημαντικά οφέλη διαφοροποίησης όσον αφορά τις συμφωνίες μεσαίας διακύμανσης.

2.5. Άλλα κρυπτονομίσματα

Μετά το λανσάρισμα του Bitcoin το 2009, πάνω από 300 εναλλακτικά νομίσματα, ή altcoins, έχουν αναδειχθεί για να οδηγήσουν το κύμα ενθουσιασμού που περιβάλλει αυτή τη νέα τεχνολογία. Ενώ οι περισσότεροι από αυτούς είναι εντελώς ερασιτεχνικά, χωρίς παγκόσμιες φιλοδοξίες, μερικοί έχουν επωφεληθεί από την αυξημένη προσοχή των επενδυτών και ακόμη και την υιοθέτηση από τους καταναλωτές. Στη συνέχεια, θα παρουσιασθούν οι έξι κορυφαίοι τύπου altcoin (Bradbury, 2013) και την τρέχουσα αγοραία αξία τους με βάση στοιχεία που καλύπτουν 306 νομίσματα από 704 αγορές, από το coinmarketcap.com.

- Litecoin (LTC). Κατώτατο όριο αγοράς: 308,265,259$. Πρώτη εξόρυξη στις 7 Δεκεμβρίου 2011. Το όνομα litecoin θεωρείται ως η κύρια εναλλακτική λύση για το bitcoin και είναι πράγματι το νόμισμα με την υψηλότερη κεφαλαιοποίηση της αγοράς μετά το bitcoin, αλλά η αξία της προσφοράς είναι 24 φορές μικρότερη από την εκτιμώμενη τιμή 7,294,753,289 για την BTC. Η επιτυχία του είναι μια πρόωρη απόδειξη ενός σχεδόν πανομοιότυπου νομίσματος που είναι σε θέση να διεισδύσει στην αγορά παρά τα πλεονεκτήματα του δικτύου του ήδη καθιερωμένου πρωτοπόρου και ηγέτη (The Genesis Block, 2014). Το Litecoin σχεδιάστηκε ως σχεδόν πανομοιότυπο με το bitcoin, αλλά με λίγες τεχνικές και νομισματικές διαφορές: χρησιμοποιεί διαφορετική απόδειξη του αλγορίθμου εργασίας (scrypt σε αντίθεση με το SHA bitcoin), που επιλέχθηκε ειδικά έτσι ώστε οι μέσοι miners να είναι σε θέση να κερδίσουν νόμισμα με απλούς υπολογιστές; το πρωτόκολλο LTC στοχεύει σε χαμηλότερο μέσο χρόνο αποκλεισμού (2,5 λεπτά έναντι 10 για το BTC). Επιπλέον, η τελική της προσφορά, αν και επίσης περιορισμένη, είναι 84 εκατομμύρια, σε σύγκριση με τα 21 εκατομμύρια της BTC (Stacke, 2013).
- Peercoin (PPCoin). Κατώτατο όριο αγοράς 47.215.407 δολαρίων. Το Peercoin διακρίνεται σημαντικά από τα αντι-πληθωριστικά ιδεώδη των κρυπτονομισμάτων, χωρίς να έχει όριο στην ποσότητα των κερμάτων που μπορούν να δημιουργηθούν. Με τη χρήση της απόδειξης συμμετοχής, μια εναλλακτική λύση στο μηχανισμό απόδειξης εργασίας που χρησιμοποιείται από το bitcoin, ο αλγόριθμος Peercoin παράγει αυτόματα περισσότερα κέρματα με βάση τις εκμεταλλεύσεις που έχει ήδη ένα άτομο, διατηρώντας έτσι ένα ετήσιο ποσοστό πληθωρισμού 1%. Σύμφωνα με τον κατασκευαστή Sunny King, ένα ψευδώνυμο που μοιάζει με αυτό του Satoshi Nakatomo, αυτό έχει σκοπό να επιτύχει μακροπρόθεσμη ενεργειακή αποδοτικότητα εξόρυξης και μεγαλύτερη ανταγωνιστικότητα κόστους στην επεξεργασία πληρωμών. Ο σταθερός, μη

περιορισμένος ρυθμός ανάπτυξης για την προσφορά χρήματος θα αμβλύνει τις ανησυχίες ότι τα κρυπτονομίσματα θα μπορούσαν να προκαλέσουν μια αποπληθωριστική σπείρα (Krugman, 2011) εάν η υιοθεσία γίνει ευρέως διαδεδομένη.

- Namecoin. Κατώτατο όριο αγοράς: $ 20.381.687. Το Namecoin είναι ένα τυπικό παράδειγμα ενός bitcoin copycat. Δύσκολα μπορεί να υποστηριχθεί ότι αυτό το altcoin έχει σημαντικές διαφορές σε σχέση με τον ηγέτη της αγοράς. Το Namecoin είναι κατασκευασμένο ως τροποποιημένη έκδοση του λογισμικού bitcoin και έχει την ίδια πολυπλοκότητα εξόρυξης. Επιπλέον, το νόμισμα λειτουργεί σε συγχωνευμένη βάση εξόρυξης με το bitcoin και οι πελάτες μπορούν να διαμορφωθούν για να ελέγξουν και τα δύο blockchains κατά την εκτέλεση εργασιών αποδείξεων εργασίας. Σχεδιασμένο για να επιτρέπει στους χρήστες να αποθηκεύουν και να μεταδίδουν κρυπτογραφικά ζεύγη κλειδιών και τιμών, σε ένα εντελώς αποκεντρωμένο σύστημα ονομάτων τομέα, το altcoin έχει χάσει μια σειρά θέσεων στην κατάταξη της κατάταξης στην αγορά μετά τον εντοπισμό ενός τεχνικού προβλήματος στα τέλη του 2013.
- Worldcoin. Κατώτατο όριο αγοράς: 1.328.414 δολάρια. Ο στόχος για την Worldcoin από την έναρξή του είναι να μετατραπεί σε παγκόσμιο κρυπτονόμισμα για εμπόρους, καταναλωτές και εμβάσματα, με έναν από τους ταχύτερους χρόνους επιβεβαίωσης για συναλλαγές, 60 δευτερόλεπτα (Bradbury, 2013). Το 2013, το Worldcoin και οι συνεργάτες της feathercoin και phenixcoin προσπάθησαν να ενώσουν τις δυνάμεις τους για τη δημιουργία μιας κοινής πλατφόρμας προώθησης, των United Open Currencies Solutions (UNOCS), που θα αυξήσουν την προβολή τους στην αγορά και τις πιθανότητές τους να ανταγωνίζονται τα καθιερωμένα κρυπτονομίσματα
- Feathercoin. Κατώτατο όριο αγοράς: 2,896,844 δολάρια. Το Feathercoin ήταν επίσης σχετικός νεοεισερχόμενος στην αγορά, ο οποίος εγκαινιάστηκε τον Απρίλιο του 2013. Ως απόκριση σε μια επίθεση κατά 51% που επιχειρήθηκε στο altcoin, διαθέτει ένα καινοτόμο χαρακτηριστικό που ενσωματώνεται στον κώδικα πελάτη και ονομάζεται προηγμένος έλεγχος σημείου ελέγχου, το blockchain. Επιπλέον, το feathercoin επωφελείται από τη δική του αγορά τύπου eBay και τη δυνατότητα τοποθέτησης μεταδεδομένων στην αλυσίδα μπλοκ, που θα βοηθούσε στη μετάδοση αρχείων (Bradbury, 2013).
- Dogecoin. Κατώτατο όριο αγοράς: 30.142.049 δολάρια. Πρώτη εξόρυξη Δεκ..6, 2013. Το Dogecoin είναι η πιο πρόσφατη άφιξη σε αυτόν τον κατάλογο επιλογών altcoin, εναλλακτικών κρυπτονομισμάτων και ξεκίνησε ως ένας τρόπος γελοιοποίησης του

φαινομένου κρυπτονομισμάτων υιοθετώντας το διάσημο μωρό "doge" στο διαδίκτυο και μια εικόνα του Shiba Inu ως έμβλημα του. Αξίζει να σημειωθεί ότι το altcoin γρήγορα εμφανίστηκε ως ένας από τους κορυφαίους υποψήφιους, δημιουργώντας μια ισχυρή κοινότητα Reddit και υπερέχοντας στο παιχνίδι μάρκετινγκ, κυρίως με την αγορά διαφημιστικού χώρου στα οχήματα NASCAR. Ωστόσο, η Dogecoin όχι μόνο δημιουργεί ένα συγκριτικό πλεονέκτημα στο μάρκετινγκ, αλλά έχει ελκυστικά τεχνολογικά χαρακτηριστικά που την κάνουν να ξεχωρίζει από την ομάδα altcoin: τα περισσότερα νομίσματα σε κυκλοφορία (άνω των 28 δισεκατομμυρίων), το υψηλότερο μέσο όρο συναλλαγών και την υψηλότερη ανταμοιβή εξόρυξης (κάθε μπλοκ περιέχει 526,226 dogecoins).

2.5.5 Διαφοροποίηση απο τα παραστατικά χρήματα

Υπάρχουν ορισμένες θεμελιώδεις διαφορές μεταξύ των νομισμάτων bitcoin και των παραστατικών νομισμάτων. Υπάρχουν πολλές διαφορετικές απόψεις για αυτές τις διαφορές. Οι σημαντικότερες διαφορές μεταξύ παραστατικών νομισμάτων και bitcoin θα συζητηθούν σε αυτό το κομμάτι της εργασίας.

Τέλη συναλλαγής

Με τα παραστατικά νομίσματα είναι δυνατή η συναλλαγή με άλλους απευθείας και χωρίς τέλη συναλλαγής. Ωστόσο, αυτό είναι δυνατό μόνο όταν γίνεται φυσικά. Κάποιος θα πρέπει να πάει στο άλλο συμβαλλόμενο μέρος και να παραδώσει τους λογαριασμούς ή τα χρήματα αυτοπροσώπως. Δεδομένου ότι αυτό είναι εξαιρετικά μη πρακτικό και επιβάλλει κόστος ευκαιρίας, ένας κοινός τρόπος διαπραγμάτευσης των χρημάτων είναι μέσω του Διαδικτύου. Τα παραστατικά νομίσματα απαιτούν μεσάζοντες για τέτοιου είδους συναλλαγές. Αυτοί οι διαμεσολαβητές μπορούν να χρεώνουν έξοδα για αυτήν την υπηρεσία. Αυτά τα τέλη μπορεί να αυξηθούν εάν οι συναλλαγές συμβαίνουν μεταξύ διαφορετικών τραπεζών και άλλων χωρών / νομισμάτων (Kim, 2015).

Μέσα στο δίκτυο Bitcoin όλες οι συναλλαγές γίνονται απευθείας απο το ένα μέρος στο άλλο μέρος. Για να πραγματοποιηθεί μια συναλλαγή, είναι απαραίτητο μόνο αυτή η συναλλαγή να επιβεβαιωθεί και να υιοθετηθεί σε ένα μπλοκ. Για να δοθεί κίνητρο στους miners να υιοθετήσουν μια συναλλαγή σε ένα μπλοκ, μια προμήθεια συναλλαγής είναι

προαιρετική. Κάποιος θα μπορούσε να επιλέξει να συμπεριλάβει μια χρέωση με τη συναλλαγή τους για να επιταχύνει τη συναλλαγή καθώς οι miners είναι σε θέση να επιλέξουν τις συναλλαγές που θα υιοθετήσουν στο μπλοκ τους. Μια συναλλαγή με ένα τέλος συναλλαγής είναι πολύ πιθανότερο να υιοθετηθεί στην αλυσίδα μπλοκ σε σύγκριση με μια συναλλαγή χωρίς τέλος συναλλαγής (Grimbergen, 2011). Η κοινότητα Bitcoin συμφώνησε σε μια τυπική χρέωση συναλλαγής 0,0001 BTC η οποία από τον Μάιο του 2015 είναι περίπου 0,002 δολάρια (Andresen, 2013). Αυτό κάνει τις συναλλαγές Bitcoin σημαντικά λιγότερο δαπανηρές από τις ηλεκτρονικές συναλλαγές με τα παραστατικά νομίσματα. Για παράδειγμα, στις ΗΠΑ, το μέσο τέλος συναλλαγής που καταβάλλεται σε μετρητά σε εγχώριο τραπεζικό λογαριασμό είναι $ 27,50 και σε ξένο τραπεζικό λογαριασμό $ 47,50 (Kim, 2015). Εάν τα ίδια ποσά χρημάτων αποστέλλονται σε bitcoin αυτό το τέλος συναλλαγής θα ήταν 0,002 δολάρια, ανεξάρτητα από το πού και ποιο ποσό χρημάτων.

Ψευδώνυμο

Πολλοί έχουν διατυπώσει τον ισχυρισμό ότι ο Bitcoin είναι εντελώς ανώνυμος. Αυτό δεν ισχύει, το Bitcoin είναι ένα «ψευδώνυμο» δίκτυο όπου κάθε χρήστης λειτουργεί κάτω από ένα ή πολλά ψευδώνυμα. Αυτό το ψευδώνυμο είναι το δημόσιο κλειδί (Reid & Harrigan, 2012). Αυτό κάνει το Bitcoin πιο ανώνυμο από τις πιστωτικές ή χρεωστικές κάρτες, αλλά το καθιστά λιγότερο ιδιωτικό. Αυτή η ιδιωτικότητα διακυβεύεται λόγω της δημοσιότητας της αλυσίδας μπλοκ. Όλοι μπορούν να δουν κάθε συναλλαγή στην αλυσίδα μπλοκ, οπότε αν ένα ψευδώνυμο συνδέεται με ένα πραγματικό πρόσωπο, κάθε συναλλαγή που έκανε το άτομο με το ψευδώνυμο είναι δημόσια. Υπάρχουν πολλές υπηρεσίες όπως το σκοτεινό πορτοφόλι που δημιουργούν ένα νέο ψευδώνυμο για κάθε συναλλαγή που πραγματοποιείται στο bitcoin. Χωρίς αυτή την υπηρεσία, η Bitcoin πέφτει κάπου ανάμεσα στις πιστωτικές και χρεωστικές κάρτες και τις συναλλαγές σε μετρητά που είναι εντελώς ανώνυμες και ιδιωτικές (Coindesk, 2015).

Θεωρούμε ότι η αύξηση της ανωνυμίας είναι μια βελτίωση για τις ηλεκτρονικές πληρωμές. Και όχι μόνο αυτό είναι μια βελτίωση προς τα θεμελιώδη ανθρώπινα δικαιώματα. το δικαίωμα στην ιδιωτική ζωή. Ωστόσο, δημιουργεί πολλές προκλήσεις όσον αφορά τη ρύθμιση και τη φορολογία, που εξετάζονται στο επόμενο τμήμα.

Κανονισμοί και φορολογία

Είναι αδύνατο να ρυθμιστεί το ίδιο το πρωτόκολλο Bitcoin, καθώς είναι ένα δίκτυο από ομότιμους χρήστες, όπου η κυβέρνηση δεν μπορεί να παρεμβαίνει. Επιπλέον, η χρήση ψευδωνύμων καθιστά αδύνατο να προσδιοριστεί ποιο πρόσωπο κάνει την συναλλαγή. Αυτά

τα χαρακτηριστικά του Bitcoin κάνουν τα bitcoins ένα δημοφιλές μέσο ανταλλαγής για παράνομη δραστηριότητα. Το Bitcoin διευκόλυνε την ανώνυμη αγορά του λεγόμενου «Silk road» που χρησιμοποιήθηκε για την ανταλλαγή παράνομων λαθρεμπόρων για bitcoins. Μέχρι το κλείσιμο, πάνω από 1,2 εκατομμύρια δολάρια σε bitcoins άλλαξε τα χέρια σε αυτή την αγορά (Christin, 2012). Μετά το κλείσιμό της το 2013, δημιουργήθηκαν πολλές άλλες ανώνυμες αγορές για τη διευκόλυνση της παράνομης δραστηριότητας. Επιπλέον, ο ψευδώνυμος χαρακτήρας του Bitcoin επιτρέπει τη χρήση του για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες.

Το Bitcoin έχει απαγορευτεί από την Ισλανδία, τη Βολιβία και τον Ισημερινό για τους λόγους αυτούς (Bitlegal, 2015). Ωστόσο, το επιχείρημα ότι το Bitcoin πρέπει να απαγορευθεί λόγω αυτών των λόγων είναι εξαιρετικά αμφισβητήσιμο, καθώς τα παραστατικά νομίσματα χρησιμοποιούνται σε πολύ μεγαλύτερη κλίμακα για αυτούς τους τύπους δραστηριοτήτων (Havocscope, 2015). Οι πιο ανεπτυγμένες δημοκρατίες είναι ανοικτές στον Bitcoin και αναπτύσσουν κανονισμούς και νόμους για τη χρήση κρυπτονομισμάτων. Λιγότερο ανοικτές χώρες όπως η Κίνα και η Ρωσία έχουν αμφιλεγόμενη άποψη για τη χρήση του Bitcoin (Bitlegal, 2015).

Η φορολογία είναι ένα άλλο πρόβλημα για τις κυβερνήσεις. Το Bitcoin προσφέρει τη δυνατότητα να αποφύγει κάποιος τη φορολογία λόγω της ψευδώνυμης φύσης του (Marian, 2013). Σε πολλές χώρες δεν υπάρχουν σαφείς φορολογικοί νόμοι για τα κρυπτονομίσματα. Ορισμένες κυβερνήσεις έχουν θεσπίσει φορολογικούς κανονισμούς για κρυπτονομίσματα, ωστόσο, τα περιουσιακά στοιχεία πρέπει να αναφέρονται οικειοθελώς από τον φορολογούμενο. Για παράδειγμα, το 2015 η ολλανδική κυβέρνηση προσέθεσε την επιλογή της δήλωσης περιουσιακών στοιχείων σε «εικονικά νομίσματα» (Belastingdienst, 2015). Με μια μικρή πιθανότητα να συλληφθούν για φοροδιαφυγή όταν δεν αναφέρουν αυτά τα περιουσιακά στοιχεία, είναι πολύ πιθανό ότι πολλοί άνθρωποι επέλεξαν να μην αναφέρουν αυτά τα περιουσιακά στοιχεία.

Ένας πιθανός τρόπος ρύθμισης και φορολόγησης του Bitcoin θα ήταν να προσδιοριστούν τα άτομα πίσω από κάθε δημόσιο κλειδί. Αυτό θα μπορούσε να γίνει με τη ρύθμιση των εταιρειών που παρέχουν υπηρεσίες για χρήστες Bitcoin (Gruber, 2013). Ένα πρώτο βήμα προς αυτό το είδος ρύθμισης έχει γίνει στις ΗΠΑ. Το 2014, το Τμήμα Χρηματοπιστωτικών Υπηρεσιών του κράτους της Νέας Υόρκης πρότεινε μια άδεια με την ονομασία «BitLicense». Μια προτεινόμενη άδεια που θα πρέπει να έχει κάθε εταιρεία αν θέλει να συμμετάσχει σε οποιαδήποτε «επιχειρηματική δραστηριότητα σε εικονικό

νόμισμα». Σκοπός αυτής της άδειας είναι η ρύθμιση όλων των επιχειρήσεων που επιθυμούν να εξυπηρετήσουν σε εικονικά νομίσματα (Department of Financial services,, 2014).

Το BitLicense έχει πάρει μεγάλη αντίσταση από την κοινότητα Bitcoin, και συγκεκριμένα για λόγους προστασίας της ιδιωτικής ζωής. Οι εταιρείες που λαμβάνουν ένα BitLicense ενδέχεται να αναγκαστούν να συλλέξουν στοιχεία ταυτοποίησης σχετικά με τους κατόχους λογαριασμών και τους τελικούς χρήστες, συμπεριλαμβανομένου του πλήρους ονόματος και της φυσικής διεύθυνσης (Department of Financial services,, 2014). Στόχος των ρυθμιστικών αρχών είναι να έχουν πληροφορίες σχετικά με την εταιρεία για να αποτρέψουν οποιαδήποτε παράνομη δραστηριότητα. Ωστόσο, ως αποτέλεσμα αυτού, οι ρυθμιστικές αρχές θα έχουν όλο το ιστορικό συναλλαγών του κάθε χρήστη αυτής της εταιρείας, ακόμη και αν αυτές οι συναλλαγές δεν είχαν καμία σχέση με αυτήν την εταιρεία. Αυτό οφείλεται στην πλήρη διαφάνεια της αλυσίδας μπλοκ.

Πιστεύω ότι ο κανονισμός και η φορολογία μπορεί να είναι ένα σημαντικό σημείο αντίστασης έναντι της πλήρους υιοθέτησής του ως νομίσματος. Υπάρχει η άποψή ότι το μεγαλύτερο πρόβλημα είναι ότι δεν υπάρχει πραγματικό μέσο όσον αφορά την προστασία της ιδιωτικής ζωής. Ο σχεδιασμός της αλυσίδας μπλοκ είναι τέτοιος ώστε, αν οι χρήστες πίσω από τα ψευδώνυμα γίνουν γνωστοί χάνονται όλα τα προσωπικά δεδομένα. Οι κυβερνήσεις θέλουν πλήρη διαφάνεια, ενώ οι χρήστες του Bitcoin θέλουν την ιδιωτικότητα. Αυτή η σύγκρουση συμφερόντων μπορεί να είναι πολύ δύσκολο να επιλυθεί.

Προσφορά χρημάτων

Σε ένα κεντρικό νομισματικό σύστημα, η προσφορά χρήματος ρυθμίζεται από τις κεντρικές τράπεζες, όπως η Ευρωπαϊκή Κεντρική Τράπεζα και η Federal Reserve. Με αυτή τη νομισματική πολιτική μπορούν να επιτύχουν ορισμένους στόχους όπως η σταθερότητα των τιμών, η οικονομική ανάπτυξη και η σταθερότητα των επιτοκίων (Woodford, 2005). Σε ένα αποκεντρωμένο σύστημα, η πολιτική εφοδιασμού πρέπει να καθοριστεί εκ των προτέρων. Με το Bitcoin, η προμήθεια bitcoins ρυθμίζεται και καθορίζεται από το λογισμικό και εκτελείται από τους miners που λαμβάνουν νέα bitcoins ως ανταμοιβή για την εξόρυξη συναλλαγών (Nakamoto, 2008). Η πεπερασμένη προσφορά του Bitcoin καθορίζεται σε 21 εκατομμύρια bitcoins. Το πρώτο μπλοκ εξήχθη το 2009 από τον Satoshi Nakamoto και περιείχε 50 bitcoins. Έκτοτε, περίπου κάθε 10 λεπτά εξορύσσεται ένα μπλοκ. Το πρωτόκολλο Bitcoin είναι κωδικοποιημένο για να μειώσει κατά το ήμισυ την ανταμοιβή bitcoin ανά μπλοκ κάθε 4 χρόνια. Το τελευταίο bitcoin πρόκειται να εξορυχθεί το 2140.

2.6. Πλεονεκτήματα και μειονεκτήματα κρυπτονομισμάτων

Τα κρυπτονομίσματα γενικότερα και το bitcoin ειδικότερα ήρθαν έξω από τον ακαδημαϊκό χώρο. Ωστόσο, η εισαγωγή της ακαδημαϊκής κοινότητας σε αυτόν τον οικονομικό νομισματικό τομέα ήταν πολύ σημαντική. Επιπλέον, δεδομένου ότι η αγορά κρυπτονομισμάτων εξελίσσεται με τεράστια ταχύτητα και υπάρχει μια σημαντική δόση σύγχυσης για το τι συμβαίνει, η ακαδημαϊκή έρευνα στον τομέα αυτό πρέπει να ληφθεί με επιφυλάξεις και προσοχή. Παρά τα γεγονότα αυτά, η ακαδημαϊκή έρευνα σχετικά με τα κρυπτονομίσματα συνέβαλε στην έκθεση των περιορισμών και των παγίδων του συστήματος των πληρωμών, αλλά και στην πρόταση τρόπων αντιμετώπισης αυτών (Bailis & Song, 2017). Οι παραπάνω συγγραφείς ισχυρίζονται ότι τα τρία κύρια πλεονεκτήματα των κρυπτονομισμάτων είναι η ανωνυμία, η ιδιωτικότητα και η εμπιστευτικότητα. Ωστόσο, το πιο σημαντικό χαρακτηριστικό του συστήματος πληρωμών μέσω κρυπτονομισμάτων είναι η διαφάνεια. Ο λόγος που υπ΄άρχει αυτή η άποψη είναι ότι η διαφάνεια είναι το κλειδί για την επιτυχία του συστήματος κρυπτονομισμάτων είναι το γεγονός ότι σε αυτό το σύστημα, σε αντίθεση με το συμβατικό τραπεζικό σύστημα πληρωμών όπου ο πελάτης έχει πληροφορίες μόνο για δικό του λογαριασμό. Ενώ στο σύστημα κρυπτογράφησης των πληρωμών, όλοι μέσα στο σύστημα μπορούν να δουν τις οικονομικές συναλλαγές όλων των άλλων συμμετεχόντων, κάνοντας έτσι το σύστημα εξαιρετικά διαφανές. Ως εκ τούτου, αν και δεν υποστηρίζεται από μια κυρίαρχη αρχή, το υψηλό επίπεδο διαφάνειας καθιστά τα κρυπτονομίσματα αποδεκτά για τους χρήστες τους. Ωστόσο, ορισμένοι συγγραφείς, όπως ο Camoron (2016) ισχυρίζονται ότι είναι πολύ απίθανο οι κυβερνήσεις να επιτρέψουν τη χρήση κρυπτονομισμάτων με τον τρόπο που λειτουργούν επί του παρόντος. Αντίθετα, ο συγγραφέας ισχυρίζεται ότι οι περισσότερες κυβερνήσεις είναι σε θέση να αποτρέψουν την ενσωμάτωση των κρυπτονομισμάτων μέσα στα σημερινά επίσημα χρηματοπιστωτικά ιδρύματα. Όσον αφορά τις συναλλαγματικές ισοτιμίες των κρυπτονομισμάτων έναντι παραδοσιακών νομισμάτων, όπως το δολάριο ΗΠΑ, παρά τη μεγάλη δημοσιότητα, η θεωρητική κατανόηση είναι περιορισμένη όσον αφορά την αξία των κρυπτονομισμάτων που βασίζονται σε blockchain. Από αυτή την άποψη, οι Li & Wang (2017) διεξήγαγαν μια εμπειρική μελέτη βασισμένη στη θεωρία του προσδιορισμού της συναλλαγματικής ισοτιμίας Bitcoin (έναντι του δολαρίου ΗΠΑ), λαμβάνοντας υπόψη τόσο τους τεχνολογικούς όσο και

τους οικονομικούς παράγοντες. Σύμφωνα με τους προαναφερθέντες συντάκτες, βραχυπρόθεσμα, η συναλλαγματική ισοτιμία Bitcoin προσαρμόζεται στις μεταβολές των οικονομικών μεγεθών και των συνθηκών της αγοράς. Η μακροπρόθεσμη συναλλαγματική ισοτιμία Bitcoin είναι πιο ευαίσθητη στα βασικά οικονομικά μεγέθη και λιγότερο ευαίσθητη στους τεχνολογικούς παράγοντες. Οι τελευταίοι συγγραφείς ισχυρίζονται επιπλέον ότι έχουν εντοπίσει σημαντικό αντίκτυπο της τεχνολογίας εξόρυξης και τη μειωμένη σημασία της δυσκολίας εξόρυξης στον καθορισμό της τιμής ανταλλαγής Bitcoin.

Μερικοί συγγραφείς, όπως ο Smalley (2017), έθεσαν το ζήτημα των κρυπτονομισμάτων και του φόρου, υποστηρίζοντας ότι πρέπει να γίνουν περισσότερα σε αυτή την πτυχή, αφού η φορολόγηση των συναλλαγών κρυπτονομισμάτων δεν έχει ακόμη ρυθμιστεί επίσημα. Τέλος, η Vora (2015) ισχυρίζεται ότι τα κρυπτονομίσματα και οι παραλλαγές των εικονικών νομισμάτων είναι μια ευπρόσδεκτη εξέλιξη, θα προσφέρουν ανταγωνισμό στις υπάρχουσες μορφές χρημάτων και κυβερνητική ρύθμιση, θα παράσχουν εναλλακτικούς τρόπους στους οικονομικούς παράγοντες για τις συναλλαγές τους και η καινοτόμος ύπαρξή τους να ενθαρρυνθούν έτσι ώστε τα ευεργετικά τους χαρακτηριστικά να ξεπεράσουν κάθε επιβλαβή αποτελέσματα.

ΚΕΦΑΛΑΙΟ 3. ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

Οι κατάλογοι (lodgers) έχουν χρησιμοποιηθεί από τις κοινωνίες για εκατοντάδες χρόνια για να παρακολουθούν τους οικονομικούς πόρους. Οι κατάλογοι χρησιμοποιούνται από ιδιώτες, επιχειρήσεις και κυβερνήσεις, για την καταγραφή συναλλαγών και την τρέχουσα κατάσταση λογαριασμών. Οι εμπορικές τράπεζες χρησιμοποιούν ψηφιακά μητρώα για να τηρούν ακριβή αρχεία σχετικά με την κατάσταση των λογαριασμών του καταθέτη τους. Μεγάλη προσπάθεια και πόροι αφιερώνονται στην εξασφάλιση αυτών των βιβλίων και πολλαπλά αντίγραφα φυλάσσονται σε χωριστά μέρη ανά πάσα στιγμή. Εάν μια τράπεζα θα χάσει όλα τα βιβλία της, οι συνέπειες θα είναι καταστροφικές. Όλα τα βιβλία έχουν ορισμένα κοινά χαρακτηριστικά. καταγράφουν συναλλαγές, εμφανίζουν την τρέχουσα κατάσταση λογαριασμών και πρέπει να ενημερώνονται τακτικά (Edwards, 2013).

Ο όρος "κατανεμημένος κατάλογος" χρησιμοποιείται για να περιγράψει ένα σύστημα καταλόγων όπου πολλαπλά αντίγραφα του ίδιου καταλόγου φυλάσσονται σε ξεχωριστές θέσεις. Ο λόγος για τη διατήρηση ενός κατανεμημένου καταλόγου είναι να μειωθούν οι κίνδυνοι - και οι πιθανές αρνητικές συνέπειες - των οικονομικών αρχείων που κρατούνται να κλαπούν, να καταστρέφονται ή να δρουν με δόλο. Η απώλεια ενός καταλόγου δεν θα οδηγήσει σε καταστροφή αν διατηρηθούν επιπλέον αντίγραφα. Όλοι οι κατανεμημένοι κατάλογοι πρέπει να διαθέτουν ένα σύστημα που να επιτρέπει τη συναίνεση σχετικά με την πραγματική κατάσταση των λογαριασμών του. Σε περίπτωση που οι κατανεμημένοι κατάλογοι μιας εταιρείας ή ενός οργανισμού δεν είναι όλα πανομοιότυποι, πρέπει να υπάρχει ένας κανόνας συναίνεσης για να προσδιοριστεί ποια έκδοση του καταλόγου πρέπει να γίνει αποδεκτή ως σωστή (Mills & Wang, 2016).

Στα τέλη του 20ου αιώνα, η ψηφιακή τεχνολογία μετασχημάτισε το μέσο του καταλόγου από χαρτί σε δυαδική μορφή. Παρόλα αυτά, ένας κατάλογος που διατηρείται σε μια σύγχρονη σχεσιακή βάση δεδομένων είναι ουσιαστικά συγκεντρωμένο, αν και μπορεί να αναπαραχθεί και να αναζητηθεί ευκολότερα από τα παλαιότερα βιβλία που διατηρούνται σε φυσική μορφή (Egilsson & Valfells, 2017). Στο πιο βασικό επίπεδο, ένα blockchain είναι απλώς ένα λογιστικό σύστημα - ένας κατάλογος. Το blockchain είναι ένας κατανεμημένος ψηφιακός κατάλογος που καταγράφει τις συναλλαγές όπου ανταλλάσσονται αξίες. Με τον όρο κατανεμημένο σημαίνει ότι υπάρχουν πολλαπλά αντίγραφα του καταλόγου. Ο κατάλογος διανέμεται μεταξύ πολλών συμμετεχόντων, που ονομάζονται κόμβοι, σε δίκτυο

Peer-to-Peer (P2P). Οι κόμβοι είναι το ισοδύναμο διακομιστών στο παραπάνω παράδειγμα. Οι κόμβοι εκτελούν τρεις κύριους τύπους λειτουργιών. (Tapscott & Tapscott, 2016), καθώς και την αποστολή και την αναμετάδοση των συναλλαγών, την ενημέρωση του blockchain με νέα μπλοκ συναλλαγών (consensus) και μπλοκ συναλλαγών αναμετάδοσης. Στην συνέχεια του κεφαλαίου παρουσιάζονται οι βασικές έννοιες του blockchain καθώς και να δοθούν κάποιες βασικές εφαρμογές του όπως αυτές έχουν καταγραφεί από διάφορες έρευνες ανά τον κόσμο.

2.1 Οι βασικές έννοιες του blockchain

Η τεχνολογία blockchain τέθηκε στη ζωή με το ψευδώνυμο Satoshi Nakamoto (The Economist, 2015). Ο Nakamoto, ο οποίος είναι ο εφευρέτης του Bitcoin Cryptocurrency, δημοσίευσε το 2008 τη μελέτη " Bitcoin: A Peer-to-Peer Electronic Cash System ". Ο συγγραφέας αυτής της μελέτης είναι ακόμα άγνωστος σήμερα, αλλά πιστεύεται ότι είναι ένας χάκερ ή μια ομάδα χάκερ (Trautman & Harrell, 2016). Αναμφισβήτητα, το bitcoin ήταν ο πρώτοw αποκεντρωμένοw δημόσιος κατάλογος (public ledger) του κόσμου και σήμερα έχει αποκτήσει παγκόσμια θέση σε όλο τον κόσμο (Pilkington, 2015). Ωστόσο, η επιτυχία του bitcoin προέρχεται από την κρυπτογραφική τεχνολογία που την υποκρύπτει, δηλαδή την τεχνολογία blockchain (Pilkington, 2015). Αυτή η τεχνολογία έχει γίνει πρόσφατα ένα καυτό θέμα για τους ερευνητές και έχει υποστηριχθεί ότι είναι ένα ακόμη πιο ανανεωτικό φαινόμενο από το bitcoin.

Το blockchain είναι ένα χαρακτηριστικό ενός κατανεμημένου καταλόγου (distributed ledger,), που σημαίνει ότι δεν ελέγχεται από κανέναν ηθοποιό, αλλά διατηρείται από διάφορους συμμετέχοντες (The Economist, 2015). Αυτό επιτρέπει στους ανθρώπους που δεν γνωρίζουν ή έχουν εμπιστοσύνη ο ένας στον άλλο για να σχηματίσουν ένα αξιόπιστο κατάλογο, όπου καταγράφονται οι πληροφορίες (The Economist, 2015). Οποιεσδήποτε άυλες πληροφορίες, όπως δικαιώματα ιδιοκτησίας και συναλλαγές εικονικού νομίσματος, μπορούν να αποθηκευτούν σε αυτές τις μπλοκ αλυσίδες. Οι πληροφορίες είναι διαθέσιμες σε όλους και είναι απαραβίαστες, γεγονός που επιτρέπει στο blockchain να είναι ένα διαφανές μηχάνημα που δημιουργεί και διατηρεί την αλήθεια (The Economist, 2015). Οι τρεις βασικές ιδιότητες του blockchain είναι ότι είναι ένας κοινός, αξιόπιστος και δημόσιος κατάλογος (The Economist, 2015).

Η βασική ιδέα της τεχνολογίας blockchain είναι συνεπώς το γεγονός ότι είναι προσβάσιμο για όλους, αλλά εξακολουθεί να ελέγχεται ή να κατέχεται από κανέναν μεμονωμένο χρήστη. Είναι με τη βοήθεια και τη συνεργασία των συμμετεχόντων του δικτύου που τηρούν τον κατάλογο σύμφωνα με την παρούσα στιγμή. Οι συμμετέχοντες ενισχύουν και συνεχίζουν τη δέσμευση ακολουθώντας αυστηρούς κανόνες και τη γενική συμφωνία, πράγμα που σημαίνει ότι οι συμμετέχοντες συμφωνούν για τον τρόπο ενημέρωσης της αλυσίδας. (The Economist, 2016b) Η συμφωνία αυτή ονομάζεται «μηχανισμός συναίνεσης» (The Economist, 2015).

Η τεχνολογία λειτουργεί μέσω ενός δικτύου peer-to-peer, το οποίο βασίζεται σε χιλιάδες κόμβους, π.χ. υπολογιστές παγκοσμίως (The Economist, 2015). Οι κόμβοι μπορούν να έρχονται και να φεύγουν όπως θέλουν στο δίκτυο (Nakamoto, 2008). Νέα μπλοκ γεννιούνται μέσω μιας διαδικασίας που ονομάζεται εξόρυξη από εξειδικευμένους κόμβους, ή με άλλα λόγια από miners. Αυτοί οι miners λειτουργούν ανώνυμα εργαζόμενοι από κοινού και προσπαθώντας να λύσουν μαθηματικά παζλ, τα οποία δημιουργούν νέα μπλοκ στο blockchain. Αυτή η δημιουργία δεν είναι τόσο απλή όσο μπορεί να ακούγεται. Χρειάζονται αρκετά βήματα για να επιτευχθεί και να επιβεβαιωθεί ένα νέο μπλοκ. Σε συναλλαγές νομισμάτων, πολλοί ανθρακωρύχοι επαληθεύουν τις συναλλαγές και επιβλέπουν ότι όλα είναι εντάξει και ότι το άτομο που πραγματοποιεί τη συναλλαγή έχει πραγματικά τα χρήματα που επιθυμεί να δαπανήσει. Εάν πρόκειται για έγκυρη συναλλαγή, οι miners επιβεβαιώνουν την αλλαγή. Στη συνέχεια, παρόμοιες συναλλαγές είναι σε μια χρονολογική σειρά που συσσωρεύεται στο ίδιο μπλοκ, το οποίο μακροπρόθεσμα αποτελεί μια αλυσίδα μπλοκ. (The Economist, 2015) Η αλυσίδα περιέχει όλες τις αποδεκτές συναλλαγές που συνέβησαν από τη γέννηση του blockchain (Peters & Panayi, 2015) και οι πληροφορίες είναι διαθέσιμες σε όλους ανά πάσα στιγμή. Οι Peters και Panayi (2015) αναφέρθηκαν στο blockchain ως χρονολογικός κατάλογος ή μια βάση δεδομένων στην οποία οι συναλλαγές καταγράφονται από ένα δίκτυο που αποτελείται από υπολογιστές.

Κάθε συναλλαγή έχει έναν κωδικό ταυτοποίησης, γνωστός ως hash, ο οποίος περιέχει την αρχική πληροφορία της συναλλαγής (The Economist, 2015). Οι τιμές κατακερματισμού των συναλλαγών που συνοδεύονται μαζί σε ένα μπλοκ, συνδυάζονται σε ένα σύστημα που ονομάζεται «Merkle Tree» . Αυτή η συνδυασμένη τιμή κατακερματισμού τοποθετείται στην κεφαλίδα ενός νέου μπλοκ επιπλέον με κάποιες άλλες πληροφορίες, όπως το hash του προηγούμενου μπλοκ και ένα timestamp. Το προηγούμενο hash στο νέο μπλοκ εξασφαλίζει

ότι τα μπλοκ δεν παραβιάζονται και εμποδίζει την εξαπάτηση (The Economist, 2015) Από την άλλη, η χρονική σήμανση αποδεικνύει ότι τα δεδομένα υπήρχαν (Nakamoto, 2008).

Στη συνέχεια η κεφαλίδα γίνεται μέρος ενός μαθηματικού παζλ, το οποίο οι miners επιλύουν χειριζόμενοι έναν ορισμένο αριθμό που ονομάζεται «nonce» (The Economist, 2015). Οι miners περνούν τρισεκατομμύρια πιθανές λύσεις για να λύσουν το παζλ και όταν βρεθεί η σωστή λύση, ο miners που το βρίσκει, το ανακοινώνει στους άλλους στο δίκτυο (Nakamoto, 2008). Οι άλλοι miners ελέγχουν τη λύση και αν είναι σωστό το επιβεβαιώνουν και ενημερώνουν αντίστοιχα το μπλοκ (The Economist, 2015). Αυτή είναι η ομορφιά του blockchain - το παζλ είναι δύσκολο να λυθεί, αλλά είναι απλό να το ελέγξεις. Ο κατακερματισμός της επικεφαλίδας είναι η συμβολοσειρά αναγνώρισης του νεοαποκτηθέντος μπλοκ, ο οποίος είναι τώρα μέρος του blockchai (The Economist, 2015)

Σε αντάλλαγμα για την εξόρυξη νέων μπλοκ και τη διατήρηση του blockchain, οι miners λαμβάνουν τις ανταμοιβές ενός ορισμένου αριθμού νεοαποκτηθέντων bitcoins (The Economist, 2016b). Τον Οκτώβριο του 2015, το ποσό ήταν 25 bitcoins ανά εξόρυξη μπλοκ, που αντιστοιχεί σε 7.500 δολάρια (Böhme et al., 2015; The Economist, 2015). Αυτό είναι το κίνητρο γιατί οι miners είναι πρόθυμοι να ενημερώσουν τα blockchains επιλύοντας δύσκολα παζλ. Η πληρωμή μπορεί επίσης να αναβληθεί έως ότου εξαντληθούν ορισμένοι όγκοι (The Economist, 2015). Αυτό εξασφαλίζει ότι οι miners διατηρούν πιο αποτελεσματικά το blockchain. Η αναβολή γίνεται με έξυπνες συμβάσεις, οι οποίες εξηγούνται σε επόμενη ενότητα (The Economist, 2015) Ένα εναλλακτικό σύστημα επιβράβευσης προσθέτει τις αμοιβές στις συναλλαγές (Böhme et al., 2015). Το 2014, το 97% των συναλλαγών περιελάμβανε ένα τέλος συναλλαγής, το οποίο είναι σήμερα χαμηλότερο από το 0,1% της συναλλακτικής αξίας. Αυτό το σύστημα ανταμοιβής είναι απαραίτητο, δεδομένου ότι αποτελεί επαρκές κίνητρο για τους miners να συνεχίσουν να διατηρούν τις μπλοκ αλυσίδες όταν εξορύσσονται τα τελευταία bitcoins και δεν μπορούν να ληφθούν άλλα bitcoins ως ανταμοιβή. Αυτά τα τέλη συναλλαγών είναι οριακά σε σύγκριση με το παραδοσιακό κόστος συναλλαγής, αλλά τείνουν να αυξάνονται όταν εξορύσσονται τα τελευταία bitcoins (Böhme et al., 2015)

Τα blockchain μπορούν να κατηγοριοποιηθούν σε διαφορετικές υποκατηγορίες ανάλογα με το αν απαιτείται η εξουσιοδότηση για τους κόμβους δικτύου ως επαληθευτές και εάν η πρόσβαση στα δεδομένα blockchain είναι δημόσια ή ιδιωτική (Peters & Panayi, 2016). Η πρώτη κατηγοριοποίηση είναι αν η διαδικασία επαλήθευσης και συναίνεσης είναι επιτρεπτή ή μη:

1. Προσβάσιμα blockchains, ο καθένας μπορεί να δημιουργήσει έναν κόμβο, να συνδεθεί στο δίκτυο και να συμμετάσχει στη διαδικασία επαλήθευσης.
2. Μη προσβάσιμα blockchains, στις οποίες τα δικαιώματα εκμετάλλευσης μεταβιβάζονται από κεντρική αρχή ή κοινοπραξία.

Η δεύτερη κατηγοριοποίηση είναι αν ο κατάλογος είναι δημόσιος ή ιδιωτικός:

1. Τα δημόσια blockchains είναι blockchains όπου ο καθένας μπορεί να αποκτήσει ένα αντίγραφο του καταλόγου και της έναρξης συναλλαγών.
2. Τα ιδιωτικά blockchains είναι blockchains όπου η άδεια περιορίζεται στους χρήστες μέσα σε μια οργάνωση ή οντότητα.

Στις δημόσιες blockchains, οποιοσδήποτε μπορεί να συμμετάσχει συνδέοντας σε έναν ή περισσότερους κόμβους και μεταδίδοντας μια συναλλαγή. Όταν ένας χρήστης πραγματοποιεί μια συναλλαγή, κάθε κόμβος παραλαβής μεταδίδει τη συναλλαγή στις συνδέσεις του μέχρις ότου τελικά όλοι οι κόμβοι έχουν ένα αντίγραφο της συναλλαγής. Δημιουργούνται νέα μπλοκ όταν μερικοί ή όλοι οι κόμβοι συναρμολογούν τις συναλλαγές σε μπλοκ συναλλαγής με χρονική σήμανση, οι οποίες στη συνέχεια μεταδίδονται μέσω του δικτύου. Η συναίνεση καθιερώνεται όταν όλοι οι κόμβοι, ή μια πλειοψηφία των κόμβων, έχουν λάβει ένα έγκυρο μπλοκ συναλλαγών το οποίο προσαρτάται στα προηγούμενα μπλοκ του blockchain. Κάθε νέο μπλοκ είναι ψηφιακά υπογεγραμμένο και περιλαμβάνει την υπογραφή του προηγούμενου μπλοκ. Οι συνδεδεμένες ψηφιακές υπογραφές εγγυώνται την ακεραιότητα των συναλλαγών που είναι καταχωρημένες στο blockchain και δεν υπάρχει ανάγκη διατήρησης ενός κεντρικού αντιγράφου (Egilsson & Valfells, 2017).

Το χρονικό διάστημα μεταξύ των νέων μπλοκ που δημιουργούνται ονομάζεται "χρόνος δημιουργίας μπλοκ". Ο χρόνος δημιουργίας του μπλοκ καθορίζεται από τους κύριους προγραμματιστές κάθε ξεχωριστού blockchain, ανάλογα με το τι κρίνουν κατάλληλο. Θα πρέπει να δημιουργηθούν αρκετά νέα τμήματα αρκετά συχνά ώστε να διασφαλιστεί ότι ο κατάλογος είναι επαρκώς ενημερωμένο. Για να επιτευχθεί ο επιθυμητός χρόνος δημιουργίας μπλοκ, ο αλγόριθμος του blockchain ρυθμίζει τη δυσκολία δημιουργίας ενός μπλοκ, προς τα πάνω ή προς τα κάτω, ανάλογα με την ποσότητα εξόρυξης που εμφανίζεται στο δίκτυο. Η αλλαγή της δυσκολίας δημιουργίας μπλοκ είναι μια διαδικασία που είναι πιο γνωστή ως "προσαρμογή του ρυθμού κατακερματισμού". Για παράδειγμα, στη blockachain Bitcoin, ο χρόνος δημιουργίας μπλοκ είναι 10 λεπτά. Αυτό σημαίνει ότι, κατά μέσο όρο, δημιουργείται ένα νέο μπλοκ κάθε 10 λεπτά.

Στο blockchain, ο κατάλογος μοιράζεται με όλους τους συμμετέχοντες, καθιστώντας το ένα αποκεντρωμένο, κατανεμημένο κατάλογο. Αντί να έχουμε μία κεντρική αρχή που να καταγράφει τις συναλλαγές, ο καθένας έχει ένα αντίγραφο του ίδιου ημερολογίου και ο λογαριασμός όλων ενημερώνεται τακτικά.

2.1.1. Συμμετέχοντες

Υπάρχουν τρεις τύποι συμμετεχόντων σε οποιοδήποτε σύστημα blockchain: καταναλωτές / χρήστες, miners και βασικοί προγραμματιστές.

1) Οι καταναλωτές είναι οι καθημερινοί χρήστες των κρυπτονομισμάτων. Είναι άνθρωποι που κατέχουν και διαμεσολαβούν τα κρυπτονομίσματα για διάφορους λόγους. Αυτοί οι λόγοι μπορούν να περιλαμβάνουν την κερδοσκοπική διαπραγμάτευση, την αποθήκευση πλούτου, την αγορά αγαθών και υπηρεσιών κλπ. Για να ξεκινήσει μια συναλλαγή, ένας χρήστης μπορεί είτε να δημιουργήσει έναν νέο κόμβο που συνδέεται άμεσα στο δίκτυο blockchain και εκπέμπει μια συναλλαγή είτε εκτελεί τη συναλλαγή μέσω μιας ανταλλαγής μεσάζοντος όπως το Coinbase.
2) Οι miners αποτελούν την καρδιά του blockchain και εκτελούν το καθήκον της ενημέρωσης του καταλόγου, μια διαδικασία που συνήθως αναφέρεται ως δημιουργία συναίνεσης ή την επικύρωση μπλοκ. Οι miners ανταγωνίζονται ενεργά μεταξύ τους για να χτίσουν επιτυχώς το επόμενο μπλοκ που θα προστεθεί στην αλυσίδα. Όταν είναι επιτυχείς, οι ανθρακωρύχοι που είναι υπεύθυνοι για τη δημιουργία του νεώτερου μπλοκ στο blockchain λαμβάνουν μια μορφή νομισματικής αποζημίωσης που ονομάζεται "ανταμοιβή μπλοκ". Η ανταμοιβή είναι η πληρωμή που λαμβάνουν οι miners για τις προσπάθειές τους να διατηρήσουν το blockchain (Carlsten & Kalodner, 2016). Η ανταμοιβή του μπλοκ είναι το άθροισμα των τελών συναλλαγής που καταβάλλονται από τους "καταναλωτές" και μιας νέας προσφοράς νομίσματος που εκδίδεται κάθε φορά που δημιουργείται ένα νέο μπλοκ. Οι miners λειτουργούν καθαρά κερδοσκοπικά και θα παράσχουν μόνο υπηρεσίες συναίνεσης (δηλαδή εξόρυξη), εάν έχει οικονομικό νόημα να το πράξουν. Οι αναλογίες των τελών συναλλαγών και της νέας προσφοράς στην ανταμοιβή του μπλοκ εξαρτώνται από το κρυπτονόμισμα που εξορύσσεται. Ορισμένοι έχουν χαμηλές χρεώσεις συναλλαγών

και υψηλό ποσοστό προσφοράς ή το αντίστροφο, ανάλογα με το τι αποφασίζουν οι κύριοι προγραμματιστές, είναι κατάλληλο για κάθε αντίστοιχο blockchain. Το σύστημα ανταμοιβής - ή η δομή κινήτρων - υποτίθεται ότι εξασφαλίζει οικονομικό κίνητρο για τους miners να συνεχίσουν να συμβάλλουν στην ενημέρωση του βιβλίου.

3) Η βασική ομάδα ανάπτυξης είναι υπεύθυνη για να διασφαλίσει ότι οι δομές κινήτρων των ανθρακωρύχων είναι κατάλληλα ευθυγραμμισμένες με το συνολικό σύστημα. Είναι υπεύθυνοι για τον καθορισμό της συγκεκριμένης δυσκολίας αλγορίθμου μέσα στο πρωτόκολλο μέσω του "κατακερματισμού". Με την προσαρμογή του ποσοστού κατακερματισμού, οι προγραμματιστές μπορούν να επηρεάσουν έμμεσα την προσφορά των miners για να ταιριάζουν με την επικρατούσα ζήτηση για υπηρεσίες εξόρυξης. Γενικά, ο ρυθμός κατακερματισμού αναπροσαρμόζεται αυτόματα από έναν αλγόριθμο, ανάλογα με το πόσο γρήγορα η ομάδα ανάπτυξης ιδρύματος θέλει τα μπλοκ να επικυρωθούν και έτσι να δημιουργηθούν, αυτό είναι γνωστό ως "χρόνος δημιουργίας μπλοκ". Ο χρόνος δημιουργίας μπλοκ είναι ο απαιτούμενος χρόνος, κατά μέσο όρο, για τη δημιουργία νέων μπλοκ (Bonneau, 2015).

2.1.2 Επικύρωση και συναίνεση

Όπως αναφέρθηκε προηγουμένως, όλα οι κατανεμημένοι κατάλογοι απαιτούν την επικύρωση των συναλλαγών, μετά την οποία πρέπει να καθοριστεί συναίνεση. Ωστόσο, τα blockchains συνδυάζουν επαλήθευση και συναίνεση σε μια διαδικασία γνωστή ως εξόρυξη (εξόρυξη = επαλήθευση συναλλαγών + συναίνεση). Οι διαφορετικές blockchain χρησιμοποιούν διαφορετικούς μηχανισμούς συναίνεσης. Ορισμένες blockchain, όπως το blockchain Bitcoin, είναι δημόσιες. αυτό σημαίνει ότι ο καθένας μπορεί να αγοράσει εξοπλισμό, να συνδεθεί στο δίκτυο και να ξεκινήσει "εξόρυξη". Άλλοι, ωστόσο, απαιτούν από τους συμμετέχοντες στη διαδικασία συναίνεσης να εκπληρώσουν ορισμένες προκαθορισμένες απαιτήσεις που ορίζονται από τους ιδρυτές.

1) Απόδειξη εργασίας: Η αρχική blockchain, η blockchain Bitcoin, χρησιμοποιεί μια διαδικασία που ονομάζεται Proof-of-Work (PoW) για να επικυρώσει τις συναλλαγές και να δημιουργήσει νέα μπλοκ. Το PoW προοριζόταν αρχικά ως οικονομικό μέτρο για την αποτροπή των κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) και άλλων παραβιάσεων υπηρεσιών, όπως το spam, σε ένα δίκτυο. Αυτό επιτυγχάνεται

απαιτώντας την εκτέλεση ορισμένων εργασιών από τον αιτούντα υπηρεσία, οι οποίες συνήθως απαιτούν χρόνο επεξεργασίας από έναν υπολογιστή. Για παράδειγμα, στο blockchain Bitcoin το "έργο" είναι να υπολογίσετε ένα έγκυρο διπλό hash SHA256. Το "έργο" που υποχρεούται να εκτελέσει ο αιτούμενος υπηρεσία απαιτεί τη δαπάνη κεφαλαίων υψηλής έντασης πόρων, όπως είναι η ισχύς επεξεργασίας, γεγονός που αυξάνει το κόστος ευκαιρίας για τη συμμετοχή σε δόλια ή ανήθικη συμπεριφορά. Ωστόσο, αυτό παρουσιάζει μια συρρίκνωση μεταξύ της ασφάλειας των δεδομένων και της σπατάλης κεφαλαίων. Ως εκ τούτου, η εργασία δεν πρέπει να είναι ούτε πολύ σκληρή ούτε πολύ εύκολη. Εάν η απαιτούμενη εργασία είναι πολύ δύσκολη, δημιουργεί αναποτελεσματικότητα, δεδομένου ότι η εργασία θα μπορούσε να είναι ευκολότερη και να αποφέρει τα ίδια αποτελέσματα. Ωστόσο, εάν το απαιτούμενο έργο είναι πολύ εύκολο, το σύστημα δεν εξυπηρετεί το σκοπό του, με αποτέλεσμα την ανεπαρκή χρήση των πόρων. Επί του παρόντος, όλες οι δημόσιες blockchain βασίζονται σε κάποια μορφή επαλήθευσης απόδειξης και κάποιου είδους διαδικασία συναίνεσης. Ωστόσο, το κύριο πρόβλημα με το PoW είναι ότι πρόκειται για μια διαδικασία εξαιρετικά εντατικής κατανάλωσης ενέργειας. Έχουν διατυπωθεί πολλές πιθανές λύσεις που αποσκοπούν στη μείωση των ενεργειακών απαιτήσεων για τη διατήρηση της ομάδας μπλοκ. Η πιο ελπιδοφόρα αντικατάσταση του PoW είναι η έννοια της απόδειξης συμμετοχής ή Proof-of-Stake (Peters & Panayi, 2016).

2) Απόδειξη συμμετοχής: Το Proof-of-Stake (PoS) είναι ένας αλγόριθμος για την επίτευξη κατανεμημένης συναίνεσης στα δίκτυα blockchain. Η PoS έχει προταθεί ως πιθανή αντικατάσταση της PoW και αποσκοπεί στην επίλυση του προβλήματος της αναποτελεσματικής χρήσης των κεφαλαιακών πόρων, όπως η υπολογιστική ισχύς και η ενέργεια. Η βασική ιδέα του Proof-of-Stake είναι να διαθέσει προνόμια εξόρυξης με βάση το πόσα "πονταρίσματα" ένα μέλος έχει στο δίκτυο. Έχουν προταθεί πολλές διαφορετικές εκδόσεις της απόδειξης απόδειξης και αν και οι απόψεις μπορεί να διαφέρουν ως προς τον τρόπο επίτευξης της βέλτιστης εφαρμογής, η βασική αρχή παραμένει η ίδια. Η απλούστερη έκδοση του Proof-of-Stake μεταβιβάζει τα δικαιώματα εξόρυξης βασισμένα στην ιδιοκτησία του φυσικού ψηφιακού νομίσματος του blockchain. Έχουν προταθεί πολλές διαφορετικές εκδοχές του συστήματος PoS, όπου τα δικαιώματα εξόρυξης εξαρτώνται όχι μόνο από την κυριότητα του νομίσματος αλλά και από άλλους παράγοντες. Τέτοιοι παράγοντες περιλαμβάνουν τη συχνότητα των συναλλαγών και το πόσο χρονικό διάστημα ένα μέλος είναι μέλος του

δικτύου (Vasin, 2014). Μέχρι στιγμής, κανείς δεν έχει δημιουργήσει με επιτυχία ένα σύστημα το οποίο βασίζεται πλήρως στο PoS. Ωστόσο, οι περισσότεροι εμπειρογνώμονες της βιομηχανίας συμφωνούν ότι είναι μόνο θέμα χρόνου πριν από την πρώτη επιτυχημένη blockchain PoS να δει το φως της ημέρας. Εάν είναι επιτυχής, η PoS θα μπορούσε να μειώσει σημαντικά την ποσότητα ενέργειας που απαιτείται για τη διατήρηση δικτύων blockchain και, ενώ όλα τα άλλα είναι ίσα, δημιουργούν πίεση προς τα κάτω στις τιμές ηλεκτρικής ενέργειας.

Το πρώτο blockchain που κέρδισε ευρεία χρήση και προσοχή είναι το Bitcoin. Ξεκίνησε ως έργο ανοιχτού κώδικα τον Ιανουάριο του 2009, το Bitcoin σχεδιάστηκε ως δίκτυο ηλεκτρονικών πληρωμών ομότιμων χρηστών. Υπάρχουν τώρα δεκάδες δημόσιες blockchain που χρησιμοποιούνται παγκοσμίως. Επί του παρόντος, τα Bitcoin, Ethereum και Ripple είναι τα πιο πολύτιμα μπλοκ με βάση την αξία των αντίστοιχων ενσωματωμένων κρυπτονομισμάτων. Εκτός από τις blockchain κρυπτονομισμάτων, αναδύονται νέοι τύποι blockchain οι οποίοι σχεδιάζονται πρωτίστως ως πλατφόρμες συναλλαγών. Από πολλές απόψεις, το Bitcoin χρησιμεύει ως πρότυπο με το οποίο συγκρίνονται σχεδόν όλα τα άλλα έργα blockchain, ανεξάρτητα από το αν είναι ανοιχτού κώδικα ή ιδιόκτητα (Egilsson & Valfells, 2017).

2.2 Αρχιτεκτονική δομή του blockchain

Αυτή η ενότητα περιγράφει τη βασική αρχιτεκτονική του blockchain ως κατανεμημένο κατάλογο. Ωστόσο, τα στοιχεία της αρχιτεκτονικής μπορεί να διαφέρουν ανάλογα με τους τύπους blockchain που χρησιμοποιούνται. Για παράδειγμα, ο μηχανισμός συναίνεσης μπορεί να είναι διαφορετικός για το Bitcoin και το Hyper Ledger.

2.2.1 Block

Το blochcain διευκολύνει ένα ιδιαίτερα κατανεμημένο κατάλογο για την καταγραφή συναλλαγών, την κατανομή τους σε έναν συγκεκριμένο κόμβο σε ένα δίκτυο και την παραγγελία τους εγκαίρως. Τα δεδομένα καταγράφονται διαρκώς στο δίκτυο μέσω αρχείων που ονομάζονται μπλοκ. Ένα μπλοκ είναι μια καταγραφή μερικών ή όλων των πιο πρόσφατων συναλλαγών που δεν έχουν ακόμη καταγραφεί σε προηγούμενα μπλοκ. Ο

κατάλογος των παρελθουσών συναλλαγών ονομάζεται blockchain, καθώς είναι μια blockchain (Matthew, Sören & John, 2016).

Ένα μπλοκ αποτελείται από κεφαλίδα (block header) και το block body (Aztori, 2015). Η κεφαλίδα του μπλοκ αποτελείται από τρία σύνολα μεταδεδομένων μπλοκ. Πρώτον, υπάρχει μια αναφορά σε ένα προηγούμενο hash μπλοκ, το οποίο συνδέει αυτό το μπλοκ με το προηγούμενο μπλοκ στο blockchain. Το δεύτερο σύνολο μεταδεδομένων, δηλαδή η δυσκολία, η χρονική σήμανση και το nonce, στην περίπτωση του bitcoin, σχετίζονται με τον ανταγωνισμό εξόρυξης. Το τελευταίο κομμάτι των μεταδεδομένων είναι η ρίζα δέντρου Merkle, μια δομή δεδομένων που χρησιμοποιείται για την αποτελεσματική σύνοψη όλων των συναλλαγών στο μπλοκ (Zeng et al., 2018). Το σώμα του μπλοκ περιλαμβάνει μια καταγραφή όλων των συναλλαγών που χωρίζονται σε είσοδο και έξοδο.

2.2.2 Ψηφιακή Υπογραφή

Η δημιουργία μιας συναλλαγής στο blockchain απαιτεί ψηφιακή υπογραφή για τον έλεγχο ταυτότητας της συναλλαγής. Μια τυπική ψηφιακή υπογραφή περιλαμβάνει δύο φάσεις: τη φάση υπογραφής και τη φάση επαλήθευσης. Για παράδειγμα, όταν ο χρήστης "Alice" θέλει να υπογράψει μια συναλλαγή, δημιουργεί πρώτα μια τιμή κατακερματισμού που προέρχεται από τη συναλλαγή. Έπειτα κρυπτογραφεί αυτή την τιμή κατακερματισμού χρησιμοποιώντας το ιδιωτικό της κλειδί (εμπιστευτικό σε αυτήν) και στέλνει σε έναν άλλο χρήστη "Bob" την κρυπτογραφημένη κατακερματισμό με τα αρχικά δεδομένα (δηλ. Τη συναλλαγή). Ο Bob ελέγχει την ληφθείσα συναλλαγή μέσω της σύγκρισης του αποκρυπτογραφημένου κατακερματισμού (χρησιμοποιώντας το δημόσιο κλειδί της Alice) και την τιμή κατακερματισμού που προέρχεται από τα ληφθέντα δεδομένα με την ίδια λειτουργία κατακερματισμού με την Alice's (Zeng et al., 2018).

2.2.3 Αποκεντρωμένο Δίκτυο

Οι αλληλεπιδράσεις μεταξύ του χρήστη στο blockchain χρησιμοποιούν κατά κύριο λόγο ένα αποκεντρωμένο δίκτυο στο οποίο κάθε χρήστης αντιπροσωπεύει έναν κόμβο στον οποίο είναι εγκατεστημένο ένα client blockchain. Όταν ένας χρήστης πραγματοποιεί συναλλαγή με άλλο χρήστη ή όταν ένας κόμβος λαμβάνει δεδομένα από άλλο κόμβο, επαληθεύει την αυθεντικότητα των δεδομένων. Στη συνέχεια μεταδίδει τα επικυρωμένα δεδομένα σε κάθε άλλο κόμβο που είναι συνδεδεμένος με αυτήν (Zeng et al., 2018). Μέσα σε

ένα τέτοιο μηχανισμό, τα δεδομένα διαδίδονται σε όλο το δίκτυο. Το όφελος από τη χρήση αυτού του μηχανισμού είναι η ελαχιστοποίηση της συγκέντρωσης του ανθρώπινου παράγοντα και η μεταστροφή της εμπιστοσύνης από τους ανθρώπινους παράγοντες μιας κεντρικής οργάνωσης σε έναν κώδικα ανοικτού κώδικα (Aztori, 2015).

2.3. Εφαρμογή του blockchain

Η εφαρμογή του blockchain θα έχει μετασχηματιστική επίδραση σε ορισμένες εφαρμογές για περιπτώσεις χρήσης. Το πρώτο blockchain, το bitcoin, αναπτύχθηκε για να ενισχύσει το σύστημα για τις χρηματοπιστωτικές εφαρμογές, λόγω της διαφάνειας του ως αποτέλεσμα της αποκεντρωμένης αρχής του. Αργότερα, αναπτύχθηκαν πιο ποικίλες χρήσεις του blockchain για οικονομικές εφαρμογές, όπως έξυπνες συμβάσεις, ασφάλειες και crowdfunding. Επιπλέον, καθώς πολλοί άνθρωποι ενδιαφέρονται για αυτή τη νέα τεχνολογία, η εφαρμογή του blockchain αναπτύσσεται επίσης ευρέως για τις μη χρηματοπιστωτικές υπηρεσίες όπως τα συστήματα ψηφοφορίας για κυβερνητικές υποθέσεις. Από την άποψη αυτή, θα μπορούσαμε να διαιρέσουμε τη χρήση του blockchain σε δύο τομείς: χρηματοπιστωτικές και μη χρηματοπιστωτικές υπηρεσίες (Zeng et al., 2018).

2.3.1 Οικονομικές εφαρμογές

Ψηφιακό Σύστημα Πληρωμών

Αυτή είναι βασικά η βασική λειτουργία του bitcoin ως ψηφιακού νομίσματος. Η γέννηση του bitcoin προκάλεσε μια εξέλιξη και διακοπή των συμβατικών συστημάτων πληρωμών που διαχειρίζονται οι τράπεζες ή άλλοι χρηματοπιστωτικοί οργανισμοί. Ένα σύστημα ψηφιακού νομίσματος ενσωματώνει τόσο ένα νέο σύστημα αποκεντρωμένων πληρωμών όσο και ένα νέο νόμισμα. Όλα τα προγράμματα παρουσιάζουν έναν ευδιάκριτο κατάλογο, ο οποίος μοιράζεται σε ένα υπολογιστικό δίκτυο. Ένα καθοριστικό χαρακτηριστικό του κάθε ψηφιακού νομίσματος είναι η διαδικασία με την οποία οι χρήστες του συμφωνούν για αλλαγές στον κατάλογο του (δηλαδή, στις οποίες οι συναλλαγές γίνονται αποδεκτές ως έγκυρες) (Zeng et al., 2018).

Έξυπνη σύμβαση

Βασικά, μια έξυπνη σύμβαση (smart contract) είναι μια εφαρμογή ηλεκτρονικού υπολογιστή που μπορεί να εκτελέσει αυτόματα εμπορικές συναλλαγές και συμφωνίες. Επιβάλλει επίσης τις υποχρεώσεις όλων των μερών σε μια σύμβαση χωρίς την πρόσθετη δαπάνη ενός μεσάζοντα (Vandervort, Gaucas & Jacques, 2015). Μια έξυπνη σύμβαση προσφέρει επίσης ένα μέσο για τους ιδιοκτήτες περιουσιακών στοιχείων να συγκεντρώνουν τους πόρους τους και να δημιουργούν μια επιχείρηση στο blockchain, όπου το συμβόλαιο κωδικοποιείται στη σύμβαση, διευκρινίζοντας σαφώς και επιβάλλοντας τα δικαιώματα αυτών των ιδιοκτητών. Οι συμβάσεις εργασίας των συνδεδεμένων πρακτορείων θα μπορούσαν να καθορίσουν τα δικαιώματα λήψης αποφάσεων των διαχειριστών, κωδικοποιώντας τι μπορούσαν και δεν μπορούσαν να κάνουν με εταιρικούς πόρους χωρίς άδεια ιδιοκτησίας (Narayanan et al., 2016).

Ασφάλιση

Οποιοδήποτε πολύτιμο περιουσιακό στοιχείο ή περιουσία που είναι δύσκολο να αναπαραχθεί ή να καταστραφεί μπορεί να καταχωρηθεί σε blockchain. Μπορεί να επαληθεύσει την ιδιοκτησία και να εντοπίσει το ιστορικό συναλλαγών. Η Everledger είναι μια εταιρεία που δημιουργεί ένα μόνιμο κατάλογο με πιστοποιήσεις διαμαντιών. Τα χαρακτηριστικά που προσδιορίζουν με μοναδικό τρόπο το διαμάντι, όπως το ύψος, το πλάτος, το βάρος, το βάθος, το χρώμα κ.λπ., έχουν καταχωρηθεί στον κατάλογο (Narayanan et al., 2016).

Crowdfunding

Επί του παρόντος, ένας αυξανόμενος αριθμός νεοσύστατων επιχειρήσεων εφαρμόζει κρυπτονομίσματα και πρωτόκολλα blockchain ως μέσο για τη συγκέντρωση των επιχειρήσεων. Η ιδέα είναι να δοθεί η δυνατότητα στις πλατφόρμες crowdfunding που λειτουργούν με την τεχνολογία blockchain, καταργώντας την ανάγκη για έναν τρίτο μεσάζοντα όπως Kickstarter ή Indiegogo. Οι νεοσύστατες επιχειρήσεις στη συνέχεια συγκεντρώνουν κεφάλαια δημιουργώντας τα δικά τους ψηφιακά νομίσματα και πουλώντας "κρυπτογραφικές μετοχές" σε πρώιμους υποστηρικτές (Vasek, Thornton & Moore, 2014). Οι επενδυτές σε μια εκστρατεία crowdfunding λαμβάνουν νομίσματα που αντιπροσωπεύουν τα μερίδια των εταιρειών που υποστηρίζουν.

2.3.2 Μη-οικονομικές εφαρμογές

Υπηρεσίες αποκεντρωμένης διακυβέρνησης

Η συνηθέστερη χρήση του blockchain στις υπηρεσίες διακυβέρνησης έχει τη μορφή συμβολαιογράφου. Η εφαρμογή του blockchain στη συμβολαιογραφική πράξη διασφαλίζει την ιδιωτικότητα του εγγράφου, καθώς και εκείνων που ζητούν πιστοποίηση. Ακόμα και η κυβέρνηση της Εσθονίας, σε συνεργασία με την πρώτη εικονική χώρα με την τράπεζα, Bitnation, θα αρχίσει να προσφέρει μια δημόσια συμβολαιογραφική υπηρεσία στους ηλεκτρονικούς κατοίκους (Tapscott & Tapscott, 2016). Μια άλλη μορφή υπηρεσίας διακυβέρνησης που υιοθέτησε επίσης blockchain είναι το ηλεκτρονικό σύστημα ψηφοφορίας ή η ηλεκτρονική ψηφοφορία. Συνήθως, οι ψηφοφορίες καταγράφονται, διαχειρίζονται, υπολογίζονται και ελέγχονται από μια κεντρική αρχή. Η ηλεκτρονική ψηφοφορία με δυνατότητα blockchain (Blockchain-enabled e-voting/ BEV) επιτρέπει στους ψηφοφόρους να κάνουν αυτά τα καθήκοντα από μόνοι τους, επιτρέποντάς τους να κατέχουν ένα αντίγραφο των ψηφοφοριών. Το ιστορικό αρχείο δεν θα μπορούσε να αλλάξει, επειδή άλλοι ψηφοφόροι μπορούσαν να δουν ότι οι εγγραφές διαφέρουν από τις δικό τους. Οι παράνομες ψήφοι δεν μπορούσαν να προστεθούν, επειδή άλλοι ψηφοφόροι θα μπορούσαν να ελέγξουν εάν οι ψήφοι ήταν συμβατοί με τους κανόνες, ίσως επειδή είχαν ήδη ληφθεί υπόψη ή δεν είχαν συνδεθεί με έγκυρο αρχείο ψηφοφόρων (Zalan, 2018). Με τον τρόπο αυτό, η τεχνολογία blockchain θα μπορούσε να ενθαρρύνει τη διαφάνεια στα κυβερνητικά συστήματα.

Αποκεντρωμένη αποθήκευση

Αυτή η έννοια έχει εφαρμοστεί στις βιομηχανίες υγείας και μουσικής. Για τις εφαρμογές που σχετίζονται με την υγεία, το blockchain παρέχει μια δομή για την αποθήκευση δεδομένων υγείας ή ηλεκτρονικών ιατρικών αρχείων (EMRs) στο blockchain έτσι ώστε να μπορούν να αναλυθούν αλλά να παραμείνουν ιδιωτικά, με ενσωματωμένο οικονομικό επίπεδο για να αντισταθμιστεί η συμβολή και η χρήση των δεδομένων (Tapscott & Tapscott, 2017). Αξιοποιώντας την ψευδώνυμη ταυτότητα που κωδικοποιείται σε μια ψηφιακή διεύθυνση και τον εγγυημένο μηχανισμό προστασίας της ιδιωτικής ζωής, τα προσωπικά αρχεία υγείας θα μπορούσαν να κωδικοποιηθούν ως ψηφιακά περιουσιακά στοιχεία και να τεθούν στο blockchain ακριβώς όπως το ψηφιακό νόμισμα. Από την άλλη πλευρά, στη μουσική βιομηχανία το blockchain χρησιμοποιήθηκε για να διατηρήσει μια ολοκληρωμένη και ακριβή κατανεμημένη βάση δεδομένων των δικαιωμάτων ιδιοκτησίας μουσικής σε ένα δημόσιο κατάλογο. Εκτός από τις πληροφορίες σχετικά με τα δικαιώματα ιδιοκτησίας,

πραγματοποιήθηκε επίσης η κατανομή των δικαιωμάτων για κάθε εργασία, όπως καθορίστηκε με έξυπνες συμβάσεις (Tapscott & Tapscott, 2017).

Αποκεντρωμένο διαδίκτυο πραγμάτων (Internet of Things/IoT)

Η χρήση του Διαδικτύου παρουσιάζει επίσης μερικές μεγάλες προκλήσεις. Ένα από αυτά οφείλεται στο κεντρικό σύστημα που είναι γνωστό και ως πρότυπο πελάτη / διακομιστή. Ενώ αυτό το μοντέλο έχει συνδέσει συσκευές γενικής χρήσης για δεκαετίες και θα συνεχίσει να υποστηρίζει δίκτυα IoT μικρής κλίμακας όπως τις βλέπουμε σήμερα, δεν θα είναι σε θέση να ανταποκριθεί στις αυξανόμενες ανάγκες των τεράστιων οικοσυστημάτων του IoT του μέλλοντος. Οι υπάρχουσες λύσεις IoT είναι δαπανηρές λόγω της υψηλής υποδομής και του κόστους συντήρησης που συνδέεται με κεντρικά clouds, μεγάλες μονάδες διακομιστών και εξοπλισμό δικτύωσης (Ouaddah, Elkalam & Ouahman, 2017). Χρησιμοποιώντας ένα τυποποιημένο μοντέλο επικοινωνίας ομότιμης επικοινωνίας για να επεξεργαστεί τον αριθμό των συναλλαγών μεταξύ συσκευών, θα μειώσει σημαντικά το κόστος που συνδέεται με την εγκατάσταση και τη συντήρηση μεγάλων κεντρικών κέντρων δεδομένων και θα κατανείμει τις ανάγκες υπολογισμού και αποθήκευσης σε δισεκατομμύρια συσκευές που σχηματίζουν Δίκτυα IoT. Σε συνεργασία με τη Samsung, η IBM έχει αναπτύξει ADEPT (Autonomous Decentralized Peer To Peer Telemetry), μια πλατφόρμα που χρησιμοποιεί στοιχεία του υποκείμενου σχεδιασμού του bitcoin για να δημιουργήσει ένα κατανεμημένο δίκτυο συσκευών ή αποκεντρωμένο IoT (Ouaddah, Elkalam & Ouahman, 2017).

2.4 Προκλήσεις χρήσης του blockchain

Γενικότερα, υπάρχει αρκετός ενθουσιασμός γύρω από το blockchain και οι ευκαιρίες που προσφέρει για τις οικονομικές και τις μη χρηματοοικονομικές υπηρεσίες. Σε αντίθεση με την προσδοκία, το blockchain έχει επίσης κάποια μειονεκτήματα. Πολλές εργασίες πρέπει ακόμη να γίνουν σχετικά με τις εφαρμογές και τις συνέπειες του blockchain. Εδώ περιγράφονται διάφορες προκλήσεις που συνήθως προκύπτουν σε σχέση με τις δημόσιες blockchain.

Απόδοση

Όταν μια συναλλαγή είναι υπό επεξεργασία, ένα blockchain πρέπει να εκτελεί τις ίδιες εργασίες με μια τακτική βάση δεδομένων, αλλά φέρει και τρεις πρόσθετες επιβαρύνσεις (Zalan, 2018):

1. Επαλήθευση υπογραφής. Κάθε συναλλαγή blockchain πρέπει να υπογραφεί ψηφιακά χρησιμοποιώντας ένα δημόσιο-ιδιωτικό σύστημα κρυπτογραφίας. Η δημιουργία και η επαλήθευση αυτών των υπογραφών είναι πολύπλοκα από υπολογιστικής απόψεως. Αντιθέτως, σε συγκεντρωτικές βάσεις δεδομένων, μόλις δημιουργηθεί μια σύνδεση, δεν χρειάζεται να επαληθεύεται μεμονωμένα κάθε αίτημα που εισέρχεται.
2. Μηχανισμοί συναίνεσης. Σε μια κατανεμημένη βάση δεδομένων, όπως ένα blockchain, πρέπει να καταβληθεί προσπάθεια για να εξασφαλιστεί ότι οι κόμβοι στο δίκτυο θα καταλήξουν σε συναίνεση. Ανάλογα με τον μηχανισμό συναίνεσης, αυτό μπορεί να συνεπάγεται σημαντική εμπρός και πίσω επικοινωνία και / ή αντιμετώπιση των πιρουνιών και των συνεπακόλουθών τους επιστροφών. Παρόλο που είναι αλήθεια ότι οι συγκεντρωτικές βάσεις δεδομένων πρέπει επίσης να αντιμετωπίζουν συγκρουόμενες και αποδιοργανωμένες συναλλαγές, αυτές είναι πολύ λιγότερο πιθανές όταν οι συναλλαγές βρίσκονται σε ουρά και επεξεργάζονται σε μια ενιαία τοποθεσία.
3. Πλεονασμός. Δεν πρόκειται για την απόδοση ενός μεμονωμένου κόμβου, αλλά για το συνολικό ποσό του υπολογισμού που απαιτεί ένα blockchain. Ενώ οι συγκεντρωτικές βάσεις δεδομένων επεξεργάζονται μία φορά (ή δύο φορές), σε ένα blockchain, πρέπει να υποβάλλονται σε επεξεργασία ανεξάρτητα από κάθε κόμβο του δικτύου, πράγμα που σημαίνει ότι πολύ περισσότερα έργα γίνονται για να επιτευχθεί το ίδιο τελικό αποτέλεσμα.

Μπορεί επομένως να υποτεθεί ότι τα ζητήματα απόδοσης στο blockchain προκύπτουν ουσιαστικά από τη μετατόπιση του μηχανισμού από το κεντρικό σε αποκεντρωμένο. Αυτός ο νέος μηχανισμός εισάγει μεγαλύτερη πολυπλοκότητα στην επεξεργασία ηλεκτρονικών υπολογιστών, όπως η επαλήθευση υπογραφών, οι μηχανισμοί συναίνεσης και οι απολύσεις. Ως αποτέλεσμα, ο χρόνος επεξεργασίας μπορεί να είναι βραδύτερος από αυτόν για μια συμβατική κεντρική βάση δεδομένων.

Ευελιξία

Σε δημόσιο blockchain, η ευελιξία είναι ένα σημαντικό ζήτημα που οι προγραμματιστές ενθαρρύνονται να λύσουν ή να ελαχιστοποιήσουν. Το ζήτημα αυτό τίθεται συχνά στις τεχνικές συζητήσεις του πρωτοκόλλου Bitcoin. Δεδομένου ότι το bitcoin είναι ένα αυτορυθμιζόμενο σύστημα που λειτουργεί με την ανακάλυψη μπλοκ σε κατά προσέγγιση χρονικά διαστήματα, η υψηλότερη απόδοση συναλλαγής του καλύπτεται αποτελεσματικά

στο μέγιστο μέγεθος μπλοκ διαιρούμενο με το διάστημα μπλοκ (Tapscott & Tapscott, 2017). Ωστόσο, το κύριο εμπόδιο για την κλιμάκωση του blockchain είναι η τάση προς συγκέντρωση με ένα αυξανόμενο blockchain: όσο μεγαλύτερο το blockchain μεγαλώνει, τόσο μεγαλύτερες είναι οι απαιτήσεις για αποθήκευση, εύρος ζώνης και υπολογιστική ισχύ που πρέπει να δαπανώνται από τους "πλήρεις κόμβους" οδηγώντας σε κίνδυνο υψηλότερης συγκέντρωσης εάν το blockchain γίνει τόσο μεγάλο που μόνο λίγοι κόμβοι είναι σε θέση να επεξεργαστούν ένα μπλοκ (Tapscott & Tapscott, 2017).

Μυστικότητα

Το Blockchain μπορεί να διατηρήσει ένα ορισμένο επίπεδο ιδιωτικότητας μέσω του δημόσιου κλειδιού (διεύθυνση για κάθε οντότητα). ωστόσο, αποδεικνύεται ότι το blockchain δεν μπορεί να εγγυηθεί την ιδιωτική ζωή των συναλλαγών, καθώς οι τιμές όλων των συναλλαγών και τα υπόλοιπα για κάθε δημόσιο κλειδί (ψευδώνυμο) είναι δημόσια ορατά (Zyskind, Nathan & Pentland, 2015). Έτσι, ο δημόσιος χαρακτήρας του blockchain σημαίνει ότι τα ιδιωτικά δεδομένα θα ρέουν μέσα από κάθε πλήρες κόμβο πλήρως εκτεθειμένο. Το πορτοφόλι HD έχει ήδη αντιμετωπίσει αυτό το πρόβλημα. χρησιμοποιεί ένα εκτεταμένο δημόσιο κλειδί ως το μοναδικό ευρετήριο για τη συσχέτιση των συναλλαγών blockchain δίνοντας στους χρήστες τη δυνατότητα να παράγουν όσα δημόσια κλειδιά θέλουν. Στη συνέχεια, οι χρήστες μπορούν να επιλέξουν να προστατεύσουν την ιδιωτική τους ζωή, στέλνοντας τις πληρωμές τους σε πολλαπλές συναλλαγές χωρίς να απαιτείται ρητός συντονισμός μεταξύ του αποστολέα και του παραλήπτη (Zyskind, Nathan & Pentland, 2015).

Κατανάλωση ενέργειας

Η δημιουργία μπλοκ PoW σε ένα δημόσιο blockchain καταναλώνει ένα μεγάλο μέρος της υπολογιστικής ισχύος και με αυτό ένα μεγάλο ποσό ηλεκτρικής ενέργειας. Η υπολογιστική ισχύς χρησιμοποιείται μόνο για αυτή τη διαδικασία και τα αποτελέσματα δεν έχουν κανένα άλλο όφελος από ό, τι για χάρη του blockchain (Zyskind, Nathan & Pentland, 2015).

2.5 Εφαρμογές με χρήση blockchain

Στην συνέχεια παρουσιάζονται ευρήματα από έρευνες που αφορούν τη χρήση της blockchain τεχνολογίας σε διάφορους τομείς. Οι περισσότεροι συγγραφείς ταξινομούν τις εφαρμογές blockchain σε οικονομικές και μη οικονομικές (2), καθώς τα κρυπτονομίσματα αντιπροσωπεύουν ένα σημαντικό ποσοστό των υφιστάμενων δικτύων blockchain. Άλλοι τα ταξινομούν σύμφωνα με τις εκδοχές blockchain (δηλ. 1.0, 2.0 και 3.0) (Swan, 2015; Zhao,

Fan, & Yan, 2016). Σε αυτή την εργασία, προτείνουμε μια ταξινόμηση προσανατολισμένη στην εφαρμογή, παρόμοια με εκείνη που προτείνεται στους Zheng et al. (2018). Η προσέγγισή μας, ωστόσο, διαφέρει από άλλα παρόμοια έργα, διότι χρησιμοποιεί μια αυστηρή μεθοδολογία βασισμένη στη βιβλιογραφία, και έτσι ταιριάζει καλύτερα στις τρέχουσες εξελίξεις στο blockchain και απεικονίζει με μεγάλη πιστότητα τις μελλοντικές τάσεις blockchain. Για το λόγο αυτό, λαμβάνοντας υπόψη την πραγματική και επικείμενη ετερογένεια των λύσεων blockchain, παρουσιάζουμε μια πιο ολοκληρωμένη και εις βάθος ταξινόμηση των εφαρμογών που βασίζονται σε blockchain, το οποίο παρουσιάζεται στα ακόλουθα υποτμήματα.

2.5.1. Οικονομικές εφαρμογές

Επί του παρόντος, η τεχνολογία blockchain εφαρμόζεται σε ευρύ φάσμα οικονομικών τομέων, συμπεριλαμβανομένων των επιχειρηματικών υπηρεσιών, του διακανονισμού των χρηματοπιστωτικών περιουσιακών στοιχείων, των αγορών πρόβλεψης και των οικονομικών συναλλαγών (Haferkorn &. Quintana Diaz, 2015). Το Blockchain αναμένεται να διαδραματίσει ουσιαστικό ρόλο στη βιώσιμη ανάπτυξη της παγκόσμιας οικονομίας, προσφέροντας οφέλη στους καταναλωτές, στο σημερινό τραπεζικό σύστημα και σε ολόκληρη την κοινωνία εν γένει (Nguyen, 2016).

Το παγκόσμιο χρηματοπιστωτικό σύστημα διερευνά τρόπους για τη χρησιμοποίηση εφαρμογών με δυνατότητα blockchain για χρηματοοικονομικά περιουσιακά στοιχεία, όπως τίτλους, χρηματαγορά και συμβάσεις παραγώγων (Peters & Panayi, 2016; Fanning & Centers, 2016; Nijeholt, Oudejans& Erkin, 2017; Paech, 2017). Για παράδειγμα, η τεχνολογία blockchain προσφέρει μια τεράστια αλλαγή στις κεφαλαιαγορές και έναν αποτελεσματικότερο τρόπο για την εκτέλεση πράξεων όπως η συναλλαγή τίτλων και παραγώγων (56, 57), ψηφιακές πληρωμές (Papadopoulos, 2015; Beck et al., 2016; Min et al., 2016; Yamada et al., 2017; English & Nezhadian, 2017; Lundqvist, DeBlanche & Andersson, 2017; Gao et al., 2018) τα συστήματα διαχείρισης (Gazalo et al., 2017), γενικές τραπεζικές υπηρεσίες (Cocco, Pinna & Marchesi, 2017), χρηματοοικονομικό έλεγχο (Dai & Vasarhelyi, 2017) ή η πληρωμή και η ανταλλαγή κρυπτονομισμάτων (δηλαδή τα ηλεκτρονικά πορτοφόλια) (Cawrey, 2014; Rizzo, 2014). Συγκεκριμένα, μια σειρά από τις μεγαλύτερες τράπεζες του κόσμου, συμπεριλαμβανομένων των Barclays και Goldman Sachs, έχουν ενώσει τις δυνάμεις τους με την R3 προκειμένου να δημιουργήσουν ένα λειτουργικό πλαίσιο

για τη χρηματοπιστωτική αγορά (Crosby et al., 2016). Ένα άλλο παράδειγμα συνεργασίας με την τράπεζα είναι Global Payments Steering Group (GPSG) (Brittto et al., 2014), των οποίων τα μέλη περιλαμβάνουν μεταξύ άλλων τις εταιρείες Santander, Bank of America και UniCredit. Το κρυπτονόμισμα πίσω από το GPSG είναι το XRP, το οποίο δημιουργήθηκε από το Ripple (Brittto et al., 2014), το οποίο υλοποιεί μια διαλειτουργική και επεκτάσιμη υποδομή ανοιχτού κώδικα που επιτρέπει τις παγκόσμιες πληρωμές και ανταλλαγές νομισμάτων.

Τα συστήματα πρόβλεψης της αγοράς (PMS), τα οποία χρησιμεύουν ως φορείς παροχής πληροφοριών, είναι επίσης ένα συναρπαστικό πεδίο που μπορεί να έχει αντίκτυπο στις επιχειρήσεις και τα κρυπτονομίσματα. Οι εφαρμογές P2P βασισμένες σε Blockchain του PMS μπορούν να βρεθούν στο Viacoin (2014), ενός κώδικα κρυπτονομισμάτων που διαθέτει εξόρυξη Scrypt Merged, έναν τύπο PoW που επιτρέπει πολύ πιο γρήγορες συναλλαγές από το Bitcoin. Το Augur[1] (2014) είναι ένα αποκεντρωμένο PMS που επιτρέπει στους χρήστες να ανταλλάσσουν μετοχές πριν από την εμφάνιση ενός γεγονότος. Οι χρήστες ανταμείβονται για την σωστή πρόβλεψη μελλοντικών γεγονότων πραγματικού κόσμου. Τα Bitshares (2014) είναι ψηφιακά σύμβολα (tokens) αποθηκευμένα στο blockchain που αναφέρονται σε συγκεκριμένα περιουσιακά στοιχεία όπως νομίσματα ή προϊόντα. Οι κάτοχοι συμβόλων μπορούν να κερδίσουν τόκους σε προϊόντα της αγοράς, όπως ο χρυσός, το πετρέλαιο, το φυσικό αέριο και επίσης σε νομίσματα. Το BitShares 2.0[2] προσφέρει μια ποικιλία χρηματοπιστωτικών υπηρεσιών που περιλαμβάνουν συναλλαγές συναλλάγματος ή τραπεζικές συναλλαγές σε αποκεντρωμένη βάση με blockchain. Η πλατφόρμα Nasdaq-Citi (Pizzo, 2017) είναι μια πλατφόρμα που επιτρέπει λειτουργίες όπως διαχείριση σχέσεων και επενδύσεις για ιδιωτικές εταιρείες. Το Medici[3] (Ventures, 2012) σχεδιάστηκε στην πλατφόρμα blockchain 2.0 και χρησιμοποιεί το πρωτόκολλο αντισυμβαλλομένου, το οποίο εφαρμόζει τα χρηματοπιστωτικά μέσα ως έξυπνες συμβάσεις, για να δημιουργήσει μια νέα χρηματιστηριακή αγορά. Ένα άλλο παράδειγμα είναι η Coinsetter, μια πλατφόρμα διαπραγμάτευσης Forex που βασίζεται στο NYC για τα bitcoins (Coinsetter, 2012). Το Plasma (Poon & .Buterin, 2017) είναι ένα πλαίσιο έξυπνων συμβάσεων που επιτρέπει τη χρήση των έξυπνων συμβάσεων για τη διεκπεραίωση της οικονομικής δραστηριότητας.

[1] https://www.augur.net
[2] https://bitshares.org
[3] https://www.mediciventures.com

Άλλα οικονομικά προσανατολισμένα πεδία εφαρμοφής μπορεί να περιλαμβάνουν την επεξεργασία εμπορικών περιουσιακών στοιχείων και ζημιών, τα κοινοπρακτικά δάνεια που αφορούν μετατρέψιμα ομόλογα, την επαναχρηματοδότηση περιουσιακών στοιχείων και την εξωχρηματιστηριακή αγορά (Deloitte, 2016; F.R.Ltd, Banking on blockchain, 2016; Infosys Consulting, 2016; McWaters, Galaski & Chatterjee, 2016). Τέλος, η υιοθέτηση από το χρηματοπιστωτικό τομέα θα οδηγήσει τελικά σε εξοικονόμηση κόστους σε τομείς όπως η κεντρική αναφορά χρηματοδότησης, η συμμόρφωση, οι συγκεντρωτικές πράξεις και οι επιχειρηματικές δραστηριότητες (Accenture, 2017)

2.5.2. Επαλήθευση ακεραιότητας

Ένα από τα πιο αναδυόμενα πεδία που σχετίζονται με το blockchain είναι η επαλήθευση της ακεραιότητας (Bhowmik & Feng, 2017; Dupont, 2017; Xu et al., 2017; Jamthagen, & Hell, 2016). Οι εφαρμογές επαλήθευσης ακεραιότητας Blockchain αποθηκεύουν πληροφορίες και συναλλαγές που σχετίζονται με τη δημιουργία και τη διάρκεια ζωής προϊόντων ή υπηρεσιών. Οι πιθανές εφαρμογές είναι: i) η προέλευση και η παραποίηση, ii) η ασφάλιση, και (iii) η διαχείριση της πνευματικής ιδιοκτησίας (IP). Ένα υποσύνολο επαλήθευσης ακεραιότητας των εφαρμογών blockchain είναι εκείνα που προσανατολίζονται στην προστασία IP (De La Rosa et al., 2017). Όπως αναφέρεται στον Swan (2015), ο όρος ψηφιακή τέχνη αναφέρεται στην IP και όχι μόνο στα διαδικτυακά έργα τέχνης, επομένως οι τεχνολογίες blockchain μπορούν να θεωρηθούν ότι καλύπτουν όλα αυτά τα σενάρια (O'Dair & Beaven, 2017). Οι ώριμες λύσεις όπως το Mediachain[4] (Labs, 2016) χρησιμοποιούν το Bitchin blockchain για να συνδέσουν το ψηφιακό περιεχόμενο με τους δημιουργούς τους. Το Asscribe το χρησιμοποιεί για τη μεταφορά ψηφιακών στοιχείων ιδιοκτησίας και δανείων, ενώ το Mediachain προσπαθεί να αποθηκεύσει τα μεταδεδομένα στο blockchain για να επιτρέψει την ανάκτηση και την αναζήτηση μέσων. Οι προσεγγίσεις δημιουργίας εσόδων, όπως το Monegraph[5], επιτρέπουν την κατανομή των εσόδων στην αλυσίδα αξίας της διανομής μέσων για διαδικτυακές εκπομπές, βίντεο κλιπ και άλλα περιεχόμενα αδειοδοτημένου ή εμπορικού σήματος που έχουν προηγουμένως επαληθευτεί στο blockchain. Το Factom[6] είναι μια άλλη λύση blockchain για την αποθήκευση και

[4] http://www.mediachain.io
[5] https://monegraph.com
[6] https://www.factom.com

επικύρωση ψηφιακών στοιχείων. Το SilentNotary[7] είναι μια υπηρεσία βασισμένη σε blockchain για την επιβεβαίωση της ύπαρξης του γεγονότος, η οποία καταγράφεται σε ψηφιακή μορφή, όπως η επικοινωνία στο messenger, η εικόνα, το αρχείο βίντεο και το ηλεκτρονικό ταχυδρομείο. Το Kodakcoin[8] είναι μια νέα μέθοδος πληρωμής που χρησιμοποιείται για την απόκτηση φωτογραφιών και δικαιωμάτων εικόνας από την πλατφόρμα kodakOne, η οποία αποθηκεύει τα έργα των εγγεγραμμένων φωτογράφων. Ένα άλλο παράδειγμα της διαχείρισης ψηφιακών δικαιωμάτων των μέσων δικτύου βρίσκεται στους Xu et el. (2017). Οι Herbaut & Negru (2017) προτείνουν μια προσέγγιση που βασίζεται στον χρήστη και βοηθά στην απαραίτητη αναδιαμόρφωση του συστήματος παροχής περιεχομένου.

Το έργο που παρουσιάζεται από τους Kim & Laskowski (2016) περιγράφει μια οντολογία που αποθηκεύει και ερμηνεύει δεδομένα με αυτοματοποιημένο τρόπο, στο πλαίσιο της προέλευσης και της ακεραιότητας των δεδομένων. Οι συγγραφείς ισχυρίζονται ότι οι έξυπνες συμβάσεις σχετίζονται στενά με τις οντολογίες και ότι τέτοια συστήματα μπορούν να προσαρμοστούν ανάλογα με το θέμα. Οι λύσεις, όπως οι Everledger[9] και Blockverify[10], χρησιμοποιούν blockchain και έξυπνες συμβάσεις για την αποφυγή απάτης για τις τράπεζες και τις ασφαλίσεις και για την εισαγωγή διαφάνειας στις αλυσίδες εφοδιασμού, αντίστοιχα. Περαιτέρω παραδείγματα σχετικά με την ακεραιότητα των δεδομένων μπορούν να βρεθούν στους Xun et al. (2017), όπου οι συγγραφείς εφαρμόζουν τα σχετικά πρωτόκολλα και το επόμενο πρωτότυπο σύστημα πλαισίου βασισμένο σε blockchain για την υπηρεσία ακεραιότητας δεδομένων.

Η τεχνολογία Blockchain δέχεται πρόσφατα μια όλο και μεγαλύτερη προσοχή από τον ασφαλιστικό κλάδο σε διάφορους τομείς, συμπεριλαμβανομένων των πωλήσεων, των αναδοχών, της εξυπηρέτησης πελατών, της διεκπεραίωσης των απαιτήσεων, των πληρωμών, των μεταβιβάσεων περιουσιακών στοιχείων και της αντασφάλισης[11]. Για παράδειγμα, οι ασφαλιστές με έδρα την Ευρώπη έχουν ξεκινήσει πρόσφατα την πρωτοβουλία B3i-blockchain για να διερευνήσουν πώς μπορεί να χρησιμοποιηθεί το blockchain για την

[7] https://silentnotary.com
[8] https://www.kodak.com/kodakone/region/changeregion/?blitz=off&hash=
[9] https://www.everledger.io
[10] http://www.blockverify.io
[11] Cognizant, Blockchain: A Potential Game-Changer for Life Insurance., https://www.cognizant.com/whitepapers/blockchain-a-potential-game-changer-for-life-insurance-codex2484.pdf

ανάπτυξη διαδικασιών και προτύπων για τη χρήση σε ολόκληρο τον κλάδο και να επιταχυνθεί η αύξηση της αποδοτικότητας στον ασφαλιστικό τομέα. Οι έξυπνες συμβάσεις που ενεργοποιούνται μέσω του blockchain οδηγούν στην αυτοματοποίηση πολλών διαδικασιών στον ασφαλιστικό τομέα, με αποτέλεσμα να μειωθεί σημαντικά το κόστος, η αυξημένη απόδοση και η ταχύτητα επεξεργασίας. Οι πιθανές συνέπειες της τεχνολογίας blockchain για την ασφάλιση υγείας μπορεί να περιλαμβάνουν τη δημιουργία ασφαλέστερων χώρων αποθήκευσης δεδομένων ιατρικής και ευεξίας, την ενεργοποίηση ειδοποιήσεων για τη λήψη συνταγών ή τη διενέργεια τακτικών ιατρικών επισκέψεων ή διαγνωστικών εξετάσεων, τη διευκόλυνση των συνεχών αναθεωρήσεων και τιμών, για την καθιέρωση λιγότερης αυθαίρετης, πιο επικαιροποιημένης συγκέντρωσης κινδύνων και για την παροχή περισσότερης εξατομικευμένης κάλυψης (Xun et al., 2017).

2.5.3 Διακυβέρνηση

Οι κυβερνήσεις καθ 'όλη τη διάρκεια των ετών είναι επιφορτισμένες με τη διαχείριση και τη διατήρηση επίσημων αρχείων τόσο των πολιτών όσο και των επιχειρήσεων. Οι εφαρμογές blockchain μπορούν να αλλάξουν τον τρόπο λειτουργίας των κυβερνήσεων σε τοπικό ή κρατικό επίπεδο με τη διαμεσολάβηση των συναλλαγών και την τήρηση αρχείων (Reijers & O'Brolcha, 2016). Η υπευθυνότητα, η αυτοματοποίηση και η ασφάλεια που προσφέρει το blockchain για το χειρισμό δημόσιων αρχείων θα μπορούσε τελικά να εμποδίσει τη διαφθορά και να καταστήσει τις κυβερνητικές υπηρεσίες πιο αποτελεσματικές. Συγκεκριμένα, το blockchain θα μπορούσε να χρησιμεύσει ως ασφαλή πλατφόρμα επικοινωνίας για την ενσωμάτωση των φυσικών, κοινωνικών και επιχειρησιακών υποδομών σε ένα έξυπνο περιβάλλον πόλης (Ibba et al., 2017). Το blockchain της διακυβέρνησης στοχεύει στην παροχή των ίδιων υπηρεσιών που προσφέρονται από το κράτος και τις αντίστοιχες δημόσιες αρχές του με αποκεντρωμένο και αποτελεσματικό τρόπο διατηρώντας παράλληλα την ίδια ισχύ. Παραδείγματα τέτοιων υπηρεσιών περιλαμβάνουν εγγραφές ή νομικά έγγραφα, βεβαίωση, αναγνώριση, συμβάσεις γάμου, φόροι και ψηφοφορία (Swan, 2015). Τα Blockchains μπορούν επίσης να χρησιμοποιηθούν σε άλλες δημόσιες υπηρεσίες όπως η εγγραφή γάμου, η διαχείριση των διπλωμάτων ευρεσιτεχνίας και τα συστήματα φορολογίας εισοδήματος (Akins,Chapman & Gordon, 2015). Άλλα έργα επικεντρώνονται σε ιδέες όπως η αντιπροσωπευτική δημοκρατία, όπου οι αντιπρόσωποι (αντί των κοινοβουλευτικών εκπροσώπων) λαμβάνουν την εξουσία ψήφου (Swan, 2015). Ομοίως, η

Holacracy (Robertson, 2015) είναι μια προσαρμοσμένη πρακτική αυτοδιαχείρισης για οργανισμούς όπου η εξουσία και η λήψη αποφάσεων κατανέμονται σε ομάδες αυτο-οργάνωσης, αντί να βασίζονται σε ένα τυπικό ιεραρχικό περιβάλλον οργάνωσης.

Η ενσωμάτωση των ψηφιακών τεχνολογιών στην καθημερινή ζωή απαιτεί μηχανισμούς που μπορούν να προσδιορίσουν με ακρίβεια ποιοι είναι οι χρήστες (Lee, 2016) και πιστοποιούν τα βασικά χαρακτηριστικά τους όπως όνομα, διεύθυνση, πιστωτικό αρχείο, καθώς και άλλα προσωπικά χαρακτηριστικά (Lee 2016; Lemieux, 2016; , Leiding & Norta, 2017; Augot et al., 2017). Επομένως, η ψηφιακή ταυτότητα έχει γίνει ένα κρίσιμο μέτρο ασφάλειας (Rivera et al., 2017). Ο Paul Dunphy (2018) αναλύει τρεις αποκεντρωμένες προσεγγίσεις διαχείρισης ταυτότητας, δηλαδή uPort, ShoCard και Sovrin, και αξιολογούν τα οφέλη και τις αδυναμίες τους. Επιπλέον, σύμφωνα με τον Roberts (2017) το ένα έκτο του παγκόσμιου πληθυσμού δεν έχει τεκμηριωμένη απόδειξη της ύπαρξής του. Η κατάσταση αυτή αφορά τους μετανάστες και τους πρόσφυγες, καθώς οι χώρες τους συχνά αρνούνται να παραδώσουν τα έγγραφα εάν, για παράδειγμα, ανήκουν στην αντιπολίτευση. Ως εκ τούτου, το blockchain γίνεται ένα μέσο ενίσχυσης της ισότητας και των ευκαιριών για τους πολίτες παγκοσμίως. Για περισσότερα σχετικά με την ψηφιακή ταυτότητα και το blockchain, μπορεί κανείς να ανατρέξει στο (Rivera et al., 2017).

Η εμφάνιση του Διαδικτύου των πραγμάτων (IoA) (133), το οποίο καθιερώνει τη σύνδεση μεταξύ του ψηφιακού περιεχομένου (Internet) και των πραγματικών συμφωνιών, συμβάσεων ή κανονισμών, επιτρέπει την επόμενη γενιά του ψηφιακού εμπορίου. Συνεπώς, οι εφαρμογές blockchain που εφαρμόζουν έξυπνες συμβάσεις για την επαλήθευση πολλών τύπων πράξεων, όπως μεμονωμένες ιδιότητες, χρησιμοποιούνται για να δηλώσουν τις συμβατικές σχέσεις μεταξύ των φορέων του Διαδικτύου, όπως είναι οι εταιρείες ή τα άτομα (Governatori et al., 2018). Για παράδειγμα, το Pavilion.io[12] είναι μια εταιρεία βασισμένη σε blockchain που παρέχει μια διεπαφή επαλήθευσης που εξαλείφει την ανάγκη για αγοραστές ηλεκτρονικού εμπορίου να τοποθετήσουν εμπιστοσύνη σε πωλητές ή τρίτους παρόχους. Το Mattereum[13] είναι ένα έργο IoA για τη διαχείριση των νομικών δικαιωμάτων επί της φυσικής και της πνευματικής ιδιοκτησίας στο blockchain. Το Stampery[14] είναι μια εταιρεία πιστοποίησης που χρησιμοποιεί blockchain για να δημιουργήσει μια σφραγίδα email ή εγγράφων. Αυτό το σύστημα παρέχει αποδεικτικά στοιχεία για την ύπαρξη (PoE), απόδειξη

[12] http://www.pavilion.io
[13] https://www.mattereum.com
[14] https://stampery.com

ιδιοκτησίας (PoO), απόδειξη της ακεραιότητας (PoI) καθώς και απόδειξη παραλαβής αποθηκεύοντας τις πληροφορίες της συναλλαγής στο δημόσιο κατάλογο. Ομοίως, το Bitrate[15], το btcluck[16] και ο Chronobit[17] χρησιμοποιούν το blockchain για να πιστοποιήσουν με ασφάλεια και επαληθεύσιμα το περιεχόμενο των εγγράφων (Swan, 2015). Έτσι, μπορούμε να χρησιμοποιήσουμε τα παραπάνω συστήματα για να αποθηκεύουμε αποδείξεις συναλλαγών και πράξεων μεταξύ ιδιωτών ή / και εταιρειών. Από την άποψη αυτή, η αύξηση των ηλεκτρονικών συναλλαγών, όπως στο ηλεκτρονικό εμπόριο, προκάλεσε αύξηση των διαφορών. Λόγω της γενικευμένης φύσης των διαδικτυακών διαφορών, πρέπει να παρέχεται αποτελεσματική διαχείριση των συγκρούσεων, η οποία να υπερνικά τα διασυνοριακά και θεσμικά γενικά έξοδα. Οι παραπάνω μέθοδοι και έργα επιτρέπουν τη δημιουργία αποτελεσματικών μεθόδων επίλυσης διαφορών, καθώς οι πληροφορίες που αποθηκεύονται στο blockchain μπορούν να επαληθευτούν και να ελεγχθούν.

2.5.4 Διαχείριση υπηρεσιών υγείας

Η τεχνολογία Blockchain θα μπορούσε να διαδραματίσει κεντρικό ρόλο στον κλάδο της υγειονομικής περίθαλψης με διάφορες εφαρμογές σε τομείς όπως η διαχείριση της δημόσιας υγείας, τα διαχρονικά μητρώα υγειονομικής περίθαλψης, η αυτοματοποιημένη αξιολόγηση των καταστάσεων υγείας, η πρόσβαση σε ασθενείς μέσω διαδικτύου, η ανταλλαγή ιατρικών δεδομένων ασθενών, (Mettler, 2016; Peterson et al., 2016; Ahram et al, 2017; Al Omar et al., 2017). Ειδικότερα, η τεχνολογία blockchain θα μπορούσαν να επιλύσουν προβλήματα επιστημονικής αξιοπιστίας των ευρημάτων (έλλειψη δεδομένων, αλλαγή παραμέτρων και επιλεκτική δημοσίευση) σε κλινικές δοκιμές, καθώς και θέματα συγκατάθεσης από ασθενείς.

Η Electronic Healthcare Records (EHR) είναι ίσως η περιοχή με την υψηλότερη δυναμική ανάπτυξη (Angraal, Krumholz & Schulz, 2017; Hoy, 2017; Kuo, Kim, & OhnMachado, 2017). Το EHR περιλαμβάνει το σύντομο ιατρικό του ασθενούς, ως μέρος του ιατρικού του μητρώου, καθώς και δεδομένα, προβλέψεις και πληροφορίες οποιουδήποτε είδους σχετικά με τις συνθήκες και την κλινική πρόοδο ενός ασθενούς καθ 'όλη τη διάρκεια της θεραπείας. Ένα σύστημα blockchain για EHRs θα μπορούσε να θεωρηθεί ως ένα πρωτόκολλο μέσω του οποίου οι χρήστες μπορούν να έχουν πρόσβαση και να διατηρούν τα

[15] https://www.bitrates.com/wallet/blockchain
[16] https://btcluck.win
[17] https://chronobit.net

δεδομένα τους για την υγεία, τα οποία ταυτόχρονα εγγυώνται την ασφάλεια και την προστασία της ιδιωτικής ζωής (Kuo, Kim, & OhnMachado, 2017). Τα πλεονεκτήματα ενός συστήματος βασισμένου σε blockchain για EHRs είναι πολλαπλά: τα αρχεία αποθηκεύονται με κατανεμημένο τρόπο (είναι δημόσια και εύκολα επαληθεύσιμα σε μη συνδεδεμένες εταιρείες παροχής), δεν υπάρχει κεντρικός ιδιοκτήτης ή κόμβος για έναν χάκερ που να διεγείρει ή να παραβιάζει, τα δεδομένα ενημερώνονται και είναι πάντα διαθέσιμα ενώ τα δεδομένα από διαφορετικές πηγές συγκεντρώνονται σε ένα ενιαίο και ενοποιημένο χώρο αποθήκευσης δεδομένων (Kuo, Kim, & OhnMachado, 2017).

2.5.5 Επιχειρηματικές και βιομηχανικές εφαρμογές

Το Blockchain έχει τη δυνατότητα να αποτελέσει σημαντική πηγή καινοτομιών στις επιχειρήσεις και τη διαχείριση μέσω της βελτίωσης, βελτιστοποίησης και αυτοματοποίησης των επιχειρηματικών διαδικασιών (Tapscott & Tapscott, 2017; Ying, Jia & Du, 2017). Πολλά μοντέλα ηλεκτρονικού επιχειρείν που βασίζονται σε IoT και blockchain αναδύονται. Ένα παράδειγμα μπορεί να βρεθεί στον Zhang & Wen (2015) όπου οι συγγραφείς προτείνουν ένα επιχειρηματικό μοντέλο στο οποίο οι συναλλαγές μεταξύ συσκευών εκτελούνται χρησιμοποιώντας έξυπνες συμβάσεις σε μια κατανεμημένη βάση δεδομένων βασισμένη σε blockchain. Επιπλέον, οι συγγραφείς προτείνουν ένα σύστημα προστασίας της ιδιωτικής ζωής που χρησιμοποιεί ένα δίκτυο IoT και ένα blockchain για να αποδείξει την προέλευση της παραγωγής χωρίς την πιστοποίηση τρίτου μέρους.

Οι εφαρμογές Blockchain φαίνεται να προσφέρουν σημαντικές ευκαιρίες βελτίωσης της απόδοσης και εμπορευματοποίησης (White, 2017), βελτιώνοντας την αξιοπιστία του ηλεκτρονικού εμπορίου και επιτρέποντας στις εταιρείες IoT να βελτιστοποιήσουν τις λειτουργίες τους, εξοικονομώντας χρόνο και κόστος (White, 2017). Οι εφαρμογές με βάση το Blockchain θα μπορούσαν να λειτουργήσουν ως αποκεντρωμένα συστήματα διαχείρισης επιχειρησιακών διαδικασιών για πολλές επιχειρήσεις. Σε αυτές τις περιπτώσεις, κάθε παράμετρος της επιχειρησιακής διαδικασίας μπορεί να διατηρηθεί στο blockchain και η δρομολόγηση της ροής εργασίας θα μπορούσε να εκτελεστεί από τις SCs, ομαλοποιώντας και αυτοματοποιώντας τις διεργασίες και μειώνοντας το κόστος (Prybila et al., 2017).

2.5.6. Διαχείριση αλυσίδας εφοδιασμού

Η τεχνολογία Blockchain αναμένεται να αυξήσει τη διαφάνεια και την υπευθυνότητα στα δίκτυα αλυσίδων εφοδιασμού (Kshetri, 2017). Συγκεκριμένα, οι εφαρμογές που βασίζονται σε blockchain έχουν τη δυνατότητα να δημιουργήσουν εφαρμογές σε τρεις τομείς στις αλυσίδες εφοδιασμού: ορατότητα, βελτιστοποίηση και ζήτηση (Kshetri, 2017). Το Blockchain μπορεί να χρησιμοποιηθεί στην εφοδιαστική, να εντοπίσει προϊόντα παραποίησης / απομίμησης, να μειώσει την επεξεργασία φορτίου, να διευκολύνει την καταδίωξη της προέλευσης (Kennedy et al, 2017) και να επιτρέψει στους αγοραστές και τους πωλητές να πραγματοποιούν απευθείας συναλλαγές χωρίς χειρισμούς από μεσάζοντες (Subramanian & Chino, 2016). Επιπλέον, έχει αποδειχθεί ότι η χρήση εφαρμογών που βασίζονται σε blockchain στα δίκτυα αλυσίδων εφοδιασμού μπορεί να διασφαλίσει την ασφάλεια, να οδηγήσει σε πιο ισχυρούς μηχανισμούς διαχείρισης συμβάσεων μεταξύ της τρίτης και της τετάρτης εφοδιαστικής (3PL, 4PL) για την καταπολέμηση της ασυμμετρίας των πληροφοριών, την ενίσχυση των μηχανισμών παρακολούθησης και εξασφάλισης ιχνηλασιμότητας (Apte & Petrovsky, 2016), παροχή καλύτερης διαχείρισης πληροφοριών σε ολόκληρη την αλυσίδα εφοδιασμού (Turk & Klinc, 2016), ασφάλεια των τροφίμων (Ahmed & Broek, 2017). βελτιώνουν τη διαχείριση των αποθεμάτων και των επιδόσεων σε όλες τις σύνθετες αλυσίδες εφοδιασμού και, τέλος, προσφέρουν καλύτερη εξυπηρέτηση πελατών μέσω προηγμένων αναλύσεων δεδομένων (π.χ. κρυπτογραφημένων δεδομένων πελατών) και μπορεί να βελτιώσει τα έξυπνα συστήματα μεταφορών (Lei et al., 2017).

2.5.7. Ενεργειακός τομέας

Οι δυνητικές εφαρμογές του blockchain στον ενεργειακό τομέα είναι εκτεταμένες και μπορεί να έχουν τεράστιο αντίκτυπο τόσο σε διαδικασίες όσο και σε πλατφόρμες (Bilal et al., 2014). Για παράδειγμα, το blockchain μπορεί να μειώσει το κόστος και να επιτρέψει τη δημιουργία νέων επιχειρηματικών μοντέλων και αγορών, να διαχειριστεί καλύτερα την πολυπλοκότητα, την ασφάλεια των δεδομένων και την ιδιοκτησία κατά μήκος των δικτύων. Επιπλέον, μπορεί να ενισχύσει τη διαφάνεια και την εμπιστοσύνη του συστήματος της αγοράς ενέργειας, να εγγυηθεί την υπευθυνότητα, διατηρώντας παράλληλα τις απαιτήσεις απορρήτου, να ενισχύσει την άμεση ανταλλαγή μεταξύ ομότιμων χρηστών για να υποστηρίξει την ομαλή λειτουργία του δικτύου ηλεκτρικής ενέργειας. πλαίσιο για πιο αποτελεσματικές διαδικασίες χρέωσης χρησιμότητας και πράξεις ενεργειακών συναλλαγών (Bilal et al., 2014).Η τεχνολογία Blockchain μπορεί επίσης να χρησιμοποιηθεί για την

έκδοση πιστοποιητικών προέλευσης, ιδιαίτερα για την παραγωγή πράσινης ενέργειας και ανανεώσιμων πηγών ενέργειας (Patil et al., 2018), για την ανάπτυξη συστημάτων συναλλαγών ενέργειας από ομότιμους χρήστες (Sikorski, Haughton & Kraft, 2017) και για τη θέσπιση συστημάτων ενεργειακής διαχείρισης ηλεκτρικών οχημάτων (Knirsch et al., 2018). Αξίζει επίσης να αναφερθεί ότι το blockchain θεωρείται παράγοντας που επιτρέπει την αποκεντροποίηση του ενεργειακού τομέα διευκολύνοντας τη μετάβασή του σε πιο αποκεντρωμένες πηγές ενέργειας (Knirsch et al., 2018).

ΚΕΦΑΛΑΙΟ 4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Blockchain είναι μια ανατρεπτική καινοτομία η οποία μπορεί να φέρει επανάσταση στους οργανισμούς και να προσφέρει διάφορες εφαρμογές. Ξεκίνησε αρχικά το blockchain για τον χρηματοπιστωτικό τομέα αλλά τώρα οι ερευνητές, οι ακαδημαϊκοί και οι βιομηχανίες διερευνούν το blockchain για άλλες εφαρμογές σε διάφορους τομείς. Το Bitcoin ήταν η πρώτη εφαρμογή που χτίστηκε στο blockchain και διευκόλυνε τις μεταφορές χρημάτων και τις δραστηριότητες ηλεκτρονικού εμπορίου.

Το Blockchain είναι ένα αποκεντρωμένο, μόνιμο, διαφανές, αμετάβλητο, αξιόπιστο σύστημα λογιστικής συναλλαγών που υποστηρίζεται από αλγόριθμο εμπιστοσύνης και κατανεμημένου μηχανισμού συναίνεσης που επιτρέπει (α) ασφαλή ανταλλαγή πληροφοριών. β) μακροπρόθεσμη διατήρηση των ψηφιακών αρχείων · και (γ) επαλήθευση και επικύρωση των ψηφιακών συναλλαγών.

Τα προγράμματα Blockchain έχουν ξεκινήσει σε πολλές βιομηχανίες όπως η τράπεζα, η ασφάλιση, η αλυσίδα εφοδιασμού, η ανανεώσιμη ενέργεια, η ακίνητη περιουσία, η υγειονομική περίθαλψη και πολλά άλλα. Η αποκέντρωση και η αποδιαμεσολάβηση του blockchain οδηγούν σε πανταχού παρούσα εμπόριο. Το Blockchain είναι μια ελκυστική τεχνολογική λύση για: (α) την απόδειξη της ιδιοκτησίας, β) εμπορική ικανότητα, (γ) εμπιστοσύνη μεταξύ των χρηστών για συναλλαγές σε πραγματικό χρόνο, δ) αυξημένη αξιοπιστία και ε) ανθεκτικότητα σε εξωτερικές απειλές

Η βιβλιογραφία αναδεικνύει τα χαρακτηριστικά της τεχνολογίας που οδηγούν στην τεχνολογική κοινότητα: (α) αποδιαμεσολάβηση. (β) ανταλλαγή εμπιστοσύνης, (γ) αυξημένο έλεγχο από τον χρήστη των πληροφοριών, (δ) σταθερά, ασφαλή αποκεντρωμένα δίκτυα, (ε) διαφάνεια και είναι αμετάβλητο και στ) διατήρηση δεδομένων υψηλής ποιότητας και ακρίβειας και υπογραμμίζει επίσης τα τεχνολογικά χαρακτηριστικά που οδηγούν το blockchain μακριά από μια τεχνολογική κοινότητα: (α) ανεπίλυτες τεχνικές προκλήσεις. (β) μη ρυθμισμένο κανονιστικό περιβάλλον (γ) ανησυχίες στον τομέα της ασφάλειας στον κυβερνοχώρο και της ιδιωτικής ζωής , (δ) προκλήσεις για ευρεία υιοθεσία, (ε) απώλεια θέσεων εργασίας λόγω αυτοματοποίησης και (στ) μειωμένη υπευθυνότητα των επιχειρήσεων. Η βιβλιογραφία υποδεικνύει ότι υπάρχει μεγάλη πολυπλοκότητα στην υλοποίηση και στην κατοχή της εφαρμογής blockchain , όπως: (α) νομικές συνέπειες, (β)

κυριότητα μπλοκ, γ) λειτουργία blockchain, (δ) θέση του καταλόγου και (ε) έλεγχο των εγγραφών.

Η ταχεία ανάπτυξη του blockchain ως οικονομικής πλατφόρμας σε διαφορετικές βιομηχανίες και η τεράστια ζήτηση των χαρακτηριστικών και των τεχνολογικών λύσεων του δημιούργησαν την ανάγκη για ευρεία άποψη της χρήσης της τεχνολογίας στο πλαίσιο των επιχειρήσεων. Με την τεχνολογία blockchain να έχει τόσο μεγάλη απήχηση, βλέπουμε ήδη ευρεία υιοθέτηση. Καθώς σχεδόν κάθε βιομηχανία χρησιμοποιεί κάποιες ευέλικτες πρακτικές τήρησης αρχείων, δεν είναι παράλογο να περιμένουμε ότι αυτή η τεχνολογία θα εφαρμοστεί σε ένα ευρύ φάσμα εφαρμογών, μερικές από τις οποίες μνημονεύτηκαν στα προηγούμενα κεφάλαια, όπως η δυνατότητα για μια έξυπνη πόλη, ενώ άλλοι είτε βρίσκονται ακόμη σε εξέλιξη είτε δεν έχουν ακόμη ανακαλυφθεί. Όπως συμβαίνει με κάθε νέα τεχνολογία, οι βάσεις δεν είναι καλά κατανοητές και γι 'αυτό είναι δύσκολο να πούμε πόσο ευρέως θα υιοθετηθεί η τεχνολογία.

Η μελλοντική έρευνα θα πρέπει να εξελιχθεί σε αυτά τα θέματα και τις νέες εφαρμογές, καθώς και τα ποσοστά υιοθέτησης της τεχνολογίας. Για όσους προσαρμόζουν το blockchain, η περαιτέρω μελέτη θα μας έδινε τη δυνατότητα να δούμε πώς αυξάνεται (αν υπάρχει) η παραγωγικότητα. Οι μελέτες ενδέχεται επίσης να επικεντρωθούν σε φραγμούς ως προς το γιατί η τεχνολογία αυτή δεν έχει υιοθετηθεί καθώς και να διερευνήσει τις τάσεις της εμπιστοσύνης των καταναλωτών. Επιπλέον, καθώς η τεχνολογία αυξάνεται, οι μελλοντικές μελέτες ενδέχεται να βοηθήσουν στην εξάλειψη των προβλημάτων ασφαλείας που δεν ανακαλύφθηκαν αρχικά.

Με αυτό που ξεκίνησε ως κάποιος κώδικας που δημοσιεύτηκε από έναν ανώνυμο προγραμματιστή με στόχο τη δημιουργία μιας νέας πλατφόρμας νομισμάτων, το blockchain έχει αποκτήσει πλέον μεγάλη δημοτικότητα, με σχεδόν κάθε βιομηχανία από τη χρηματοδότηση και την υγειονομική περίθαλψη, μέχρι την εκπαίδευση και τον πολεοδομικό σχεδιασμό. Συμπερασματικά, η τεχνολογία blockchain φαίνεται όχι μόνο να βελτιώνει τα καθήκοντα των σημερινών βιομηχανιών αλλά και να διατηρεί τη δυνατότητα επανάστασης στα συστήματα που παρακολουθούν την ιστορία των αντικειμένων μέσω ενός πολύ βελτιωμένου, διαφανούς συστήματος καταλόγων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Accenture, (2017). Banking on blockchain. A value analysis for investment banks. Report.
2. Ahmed, S., Broek, NT. (2017). Food supply: Blockchain could boost food security,Nature. 550. (7674)43.
3. Ahram, T. Sargolzaei, A. Sargolzaei, S. Daniels, J. Amaba, B. (2017). Blockchain technology innovations, in: 2017 IEEE Technology and Engi- neering Management Society Conference, TEMSCON 2017, 137–141.
4. Akins, B.W., Chapman, JL., Gordon, JM. (2013). A Whole New World: Income Tax Considerations of the Bitcoin Economy, https://papers. ssrn.com/sol3/papers.cfm?abstract_id=2394738, 2013
5. Al Omar, A., Rahman, M. S. Basu, A. Kiyomoto, S. (2017). MediBchain: A blockchain based privacy preserving platform for healthcare data, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10658 LNCS, 534–543.
6. Andresen, G. (201). Bitcointalk.org. from https://bitcointalk.org/index.php?topic=219504.0
7. Angraal, S. Krumholz, HM., Schulz, WL., (2017). Blockchain technology: Applications in health care, Circulation: Cardiovascular Quality and Outcomes 10 (9).
8. Apte, S. Petrovsky, N. (2016). Will blockchain technology revolutionize excipient supply chain management?., Journal of Excipients and Food Chemicals 7 (3). 76–78.
9. Atzori, Marcella, Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (December 1, 2015). Available at SSRN: https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713
10. Augot, D. Chabanne, H. Chenevier, T. George, W. Lambert, L., (2017). A user-centric system for verified identities on the bitcoin blockchain, in: Lecture Notes

in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10436 LNCS, 390–407.

11. Augur, (2014). The augur project, https://augur.net/ .
12. Bagehot, W. (1878). Lombard street: a description of the money market.
13. Bailis, P. & Song, H. (2017). Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts; Hardware for Deep Learning. *Communications of the ACM,* 60(5), p. 48-51.
14. Bank Charter Act 1844 (7 & 8 Vict. c. 32). (1844). Bank of England http://www.bankofengland.co.uk/about/Documents/legislation/1844act.pdf
15. Barber, S., Boyen, X., Shi, E., Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. Financial Cryptography and Data Security, 399-414. Springer Berlin Heidelberg.
16. Barrdear, J, & Kumhof, M. (2016). The macroeconomics of central bank issued digital currencies. Bank of England Working Paper No. 605. London, England.
17. Baur, D. G. & Lucey, B. M. (2010). Is gold a hedge or a safe haven? an analysis of stocks, bonds and gold. Financial Review 45, 217-229.
18. Beck, R.,Stenum Czepluch, J., Lollike, N., Malone, S. (2016). Blockchain-Thegatewaytotrust-freecryptographictransactions,in:24th European Conference on Information Systems, ECIS 2016.
19. Belastingdienst. (2015). Belasting op overige bezitten. from Belastingdienst.nl: http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/vermogen_en_aanmerkelijk_belang/vermogen/wat_zijn_uw_bezittingen_en_schulden/uw_bezittin gen/overige_bezittingen/
20. Bergstra, J. A., de Leeuw, K. (2013). Bitcoin and beyond: exclusively informational monies. arXiv preprint arXiv:1304.4758.
21. Bernanke, B. (2000). Essays on the Great Depression. Princeton: Princeton University Press.
22. Bhowmik, D. T., Feng, T. (2017). The multimedia blockchain: A distributed and tamper-proof media transaction framework, in: International Conference on Digital Signal Processing, DSP.
23. Bilal, K. Malik, S. Khalid, O. Hameed, A. Alvarez, E. Wijaysekara, V. Irfan, R. Shrestha, S. Dwivedy, D. Ali, M. Shahid Khan, U. Abbas, A. Jalil, N. Khan, U

(2014). A taxonomy and survey on Green Data Center Networks, Future Generation Computer Systems 36. 189–208

24. Bitlegal. (2015, May 21). Bitlegal. Retrieved from Bitlegal.io: http://www.bitlegal.io
25. Bitshares, (2014). The bitshares project, https://bitshares.org/.
26. Boehmer, E., Fong, K. & Wu, JJ. (2014). International evidence on algorithmic trading. AFA 2013 San Diego Meetings Paper.
27. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, 29(2), 213-238.
28. Bonneau, J. (2015, November 3). How long does it take for a Bitcoin transaction to be confirmed? from https://coincenter.org/entry/how-long- does-it-take-for-a-bitcoin-transaction-to-be-confirmed
29. Bonneau, J., Miller, A. Clark, Narayanan, A.. Kroll, J.. Felten, E. (2015). Sok: Research perspectives and challenges for bitcoin and cryptocurrencies, in: Security and Privacy (SP) IEEE Symposium on, IEEE, 104–121, 2015.
30. Bradbury, D. (2013). Bitcoin's Best Competitors: The Top Altcoins of 2013. Coin Desk. http://www.coindesk.com/top-altcoins-2013/
31. Briere, M., Oosterlinck, K., Szafarz, A. (2013). Virtual currency, tangible return: portfolio diversification with bitcoins. Working Papers CEB, 13
32. Britto,A., Schwartz, D., Fugger, R. (2014). Ripple,https://ripple.com/.
33. Carlsten, M., Kalodner, H., Weinberg, S. M., & Narayanan, A. (2016, October). On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 154-167). ACM.
34. Cawrey, D. (2014). 37Coins Plans Worldwide Bitcoin Access with SMS-Based Wallet, http://www.coindesk.com/37coins-plansworldwide-bitcoin-access-sms-based-wallet/
35. Cedillo, I. (2013). The historical role of the European shadow banking system in the development and evolution of our monetary institutions. Available at SSRN 2220167.
36. Christidis, K. & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things, IEEE Access 4. 2292–2303.

37. Christin, N. (2012). Traveling the Silk Road: A measurement analysis. from https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf
38. Cocco, L, .Pinna, A., Marchesi, M (2017). Banking on blockchain: Costs savings thanks to the blockchain technology, Future Internet 9(3) 25.
39. Coindesk. (2015, April 10). State of Bitcoin Q1 2015. from Coindesk: http://www.coindesk.com/research/state-of-bitcoin-q1-2015/
40. CoinMarketCap (2017). Cryptocurrency Market Capitalizations, https://coinmarketcap.com/.
41. Coinsetter. (2012). NYC-basedForextradingplatformforBitcoin,www.coinsetter.com.
42. Coudert, V. & Raymond, H. (2011). Gold and financial assets: are there any safe havens in bear markets? Economics Bulletin 31, 1613-1622.
43. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain technology :Beyond bitcoin, Applied Innovation 2. 6–10.
44. Dai, J. & Vasarhelyi, M.A. (2017). Toward blockchain-based accounting and assurance, Journal of Information Systems 31(3) 5-21.
45. De La Rosa, JL., El-Fakdi, A., Torres, V., Amengual, X. (2017). Logo recognition by consensus for enabling blockchain implementations, in: Frontiers in Artificial Intelligence and Applications, vol. 300, 257-262.
46. Deloitte. (2016). Over the horizon. Blockchain and the future of financial infrastructure. Report
47. Department of Financial services. (2014). BitLicense . from http://www.dfs.ny.gov/: http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf
48. Deshmukh, S. D., Greenbaum, S. I., & Kanatas, G. (1983). Interest rate uncertainty and the financial intermediary's choice of exposure. The Journal of Finance, 38(1), 141-147.
49. Dupont, Q. (2017). Blockchain Identities: Notational Technologies for Control and Management of Abstracted Entities, Metaphilosophy 48 (5) 634-653.
50. Edwards, J. R. (2013). *A history of financial accounting (RLE Accounting)* (Vol. 29). Routledge.

51. Egilsson, J. H., & Valfells, S. (2017). *Blockchains and the future of financial services*. Retrieved from Monerium Website: http://monerium.com/content/monerium-report- web-2017-07.pdf
52. English, S.M., Nezhadian, E. (2017). Conditions of full disclosure: The blockchain remuneration model, in: Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017, 64–67.
53. European Central Bank. (2012). Virtual currency schemes. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
54. Evans-Pughe, C. (2012). From megabytes to megabucks. Engineering & Technology 7, 59-61.
55. F.R.Ltd, Banking on blockchain (2016). Charting the progress of distributed ledger technology in financial services.,Report.
56. Fama, E. F. (1980). Banking in the theory of finance. Journal of Monetary Economics 6, 39- 57.
57. Fanning, K., Centers, D.P. (2016). Blockchain and its coming impact on financial services, Journal of Corporate Accounting & Finance2 7(5) 53–57.
58. Friedman, M. (1948). A monetary and fiscal framework for economic stability. The American Economic Review 38, 245-264.
59. Friedman, M. & Schwartz, A. J. (2008). A monetary history of the United States, 1867-1960. Princeton University Press.
60. Gandal, N. & Halaburda, H. (2016). Can we predict the winner in a market with network effects? Competition in cryptocurrency market. *Games*, 7(3), p. 1-21.
61. Gao, F., Zhu, L. Shen, M., Sharif, K., Wan, Z., Ren, K. (2018). A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks, IEEE Network .
62. Gazali, HM., Hassan,R., Nor, RM, Rahman, H.M.M. (2017). Re-inventing PTPTN study loan with blockchain and smart contracts, in:ICIT2017 - 8th International Conference on Information Technology, Proceedings, 751–754.
63. Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R. .Sartor, G., .Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems, Artificial Intelligence and Law (2018) 1–33.
64. Greenspan, G., (2015). Ending the bitcoin vs blockchain debate, http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain- debate, 2015.

65. Grinberg, R. (2011). Bitcoin: an innovative alternative digital currency. Hastings Science & Technology Law Journal 4, 160.
66. Gruber, S. (2013). Trust, identity, and disclosure: Are Bitcoin exchanges the next virtual havens for money loaundering and tax evasion? rom http://www.quinnipiac.edu/: http://www.quinnipiac.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/Vol32_Issue1_2013_ Gruber.pdf
67. Haferkorn, M. &. Quintana Diaz, J. M . (2015). Seasonality and Interconnectivity Within Cryptocurrencies - An Analysis on the Basis of Bitcoin, Litecoin and Namecoin, Springer International Publishing, Cham, 106–120.
68. Havocscope. (2015). Havocscope Global Black Market Value. from Havocscope: http://www.havocscope.com/market-value/
69. Hawlitschek, F., Notheisen, B., Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, Electronic Commerce Research and Applications 29. 50–63.
70. Hayek, F. (2002). Competition as a discovery procedure. Quarterly Journal of Austrian Economics 5, 9-23.
71. Herbaut, N., Negru, N. (2017). A Model for Collaborative Blockchain-Based Video Delivery Relyingon Advanced Network Services Chains, IEEE Communications Magazine 55 (9). 70–76.
72. Hommes, C., Sonnemans, J., Tuinstra, J., van de Velden, H. (2008). Expectations and bubbles in asset pricing experiments. Journal of Economic Behavior & Organization 67, 116-133.
73. Hoy, MB. (2017). An Introduction to the Blockchain and Its Implications for Libraries and Medicine, Medical Reference Services Quarterly. 36(3).273–279.
74. Hüsler, A., Sornette, D., Hommes, C. H. (2013). Super-exponential bubbles in lab experiments: evidence for anchoring over-optimistic expectations on price. Journal of Economic Behavior & Organization 92, 304-316.
75. Ibba, S., Pinna, A., Seu, M., Pani, F. (2017). CitySense: Blockchain-oriented Smart Cities, in: ACM International Conference Proceeding Series, vol. Part F129907, 201
76. IBM. (2017). Three ways blockchain Explorers chart a new direction, https://www-935.ibm.com/services/studies/csuite/pdf/ GBE03835USEN-00.pdf

77. Infosys Consulting. (2016). Blockchain Technology and the Financial Services Market. State-of-the-Art Analysis., http://www.infosysconsultinginsights.com/wp-content/uploads/2016/10/InfosysConsulting_HHL_Blockchain.pdf.
78. Jamthagen, C., .Hell, M., (2016). Blockchain-Based Publishing Layer for the Keyless Signing Infrastructure, in:Proceedings-13th IEEE International Conference on Ubiquitous Intelligence and Computing, 374–381.
79. Karafiloski, E. & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review, in: Smart Technologies, IEEE EUROCON 2017-17th International Conference on, IEEE, 763–768.
80. Kennedy, ZC, .Stephenson, DE., Christ, JF, .Pope, TR., Arey, PW, Barrett, CA, Warner, MG. (2017) Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology, Journal of Materials Chemistry C 5 (37). 9570–9578.
81. Khan, M.A. & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82. 395 – 411.
82. Kim, .H.M. & Laskowski, M. (2016). Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance, http://arxiv.org/abs/1610.02922, 2016.
83. Kim, T. (2015). Comparing Wire Transfer Fees at the Top 10 U.S. Banks. Retrieved May 21, 2015, from Mybanktracker.com: http://www.mybanktracker.com/news/wire-transfer-fee- comparison-top-10-us-banks
84. Kirilenko, A., et al. (2015). The flash crash: The impact of high frequency trading on an electronic market. Available at SSRN 1686004.
85. Knirsch, F. Unterweger, A. Eibl, G. Engel, D. (2018). Privacy-preserving smart grid tariff decisions with blockchain-based smart contracts, in: Sustainable Cloud and Energy Services, Springer, 85–116
86. Koteska, B., Karafilovski, E., Mishev, E. (2017). Blockchain Implementation Quality Challenges: A Literature Review : Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia 11–13.
87. Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: quantifying the relationship between phenomena of the Internet era. Scientific reports 3, 3415.

88. Krugman, P. R. (2011). Golden Cyberfetters. The conscience of a liberal blog. http://krugman.blogs.nytimes.com/2011/09/07/goldencyberfetters/?_php=true&_type=blogs&_r=0
89. Kshetri, N. (2017). Blockchain's roles in strengthening cyber security and protecting privacy, Telecommunications Policy 41(10). 1027–1038.
90. Kuo,TT., Kim,HE., OhnMachado, L., (2017). Blockchain distributed ledger technologies for biomedical and healthcare applications, Journal of the American Medical Informatics Association 24 (6) 1211–1220.
91. Kydland, F. E., & Prescott, E. C. (1977). Rules rather than discretion: The inconsistency of optimal plans. The Journal of Political Economy, 473-491.
92. Labs, M. (2016). Building a more connected world for creators and audiences, http://www.mediachain.io/.
93. Lam, P.N. & Lee D.K.C. (2015). Introduction to Bitcoin." *Handbook of Digital Currency*, edited by D.K.C. Lee, pp. 5-30. San Diego: Elsevier
94. Lamport, L., Shostak, R., Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) 4, 382-401.
95. Lastra, R. M. (2012). The Evolution of the European Central Bank. Fordham International Law Journal, Spring.
96. Lee, J.H, (2016). BIDaaS: Blockchain Based ID As a Service, IEEE Access 6 2274–2278.
97. Lei, A. Cruickshank, H. Cao, Y. Asuquo, P. Ogah, C. Sun, Z. (2017). Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems, IEEE Internet of Things Journal. 4 (6). 1832–1843.
98. Leiding, B., Norta, A.. (2017). Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10646 LNCS, 181–196.
99. Lemieux, P. (2013). Who is Satoshi Nakamoto? Regulation 36, 14-15.
100. Lemieux, VL., (2016). Trusting records: is Blockchain technology the answer?, Records Management Journal 26(2) 110–139.

101. Li, X. & Wang, C.A (2017). The technology and economic determinant of cryptocurrency exchange rates: The case of Bitcoin. *Decision support system*, 95, p. 49-60.

102. Lundqvist, T., DeBlanche, A.M, Andersson, H.R. (2017). Thing-to-thing electricity micropayments using blockchain technology, in:GIoTS2017- Global Internet of Things Summit, Proceedings, 2017.

103. Luther, W. J. (2013). Cryptocurrencies, network effects, and switching costs. Available at SSRN 2295134 .

104. Marian, O. Y. (2013). Are Cryptocurrencies 'Super' Tax Havens? from http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1365&context=facultypub

105. Matthew, E, , Sören, A. & John. D. (2016). Block chain technologies & the semantic web: A framework for symbiotic development. Computer Science Conference for University of Bonn Students, J. Lehmann, H. Thakkar, L. Halilaj, and R. Asmat, Eds, pp. 47–6

106. McWaters, R. Galaski, R., Chatterjee, S. (2016). The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services, in: World Economic Forum, 2016.

107. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, Geoffrey, M. & Savage, S. (2016). A fistful of bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, 59(4), p. 86-93

108. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here, in: e-Health Networking, Applications and Services (Health- com), 2016 IEEE 18th International Conference on, IEEE, 1–3, 2016.

109. Michael, G. J. (2013). Anarchy and property rights in the virtual world: how disruptive technologies undermine the state and ensure that the virtual world remains a 'wild west'. Available at SSRN 2233374.

110. Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J. C., Badev, A. I., ... & Ellithorpe, M. (2016). Distributed ledger technology in payments, clearing, and settlement.

111. Min, X., Li, Q., Liu, L., Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size, in: Trust-com/BigDataSE/ISPA, 2016 IEEE, IEEE, 90–96, 2016.

112. N. Atzei, N., Bartoletti, M. Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK), in: International Conference on Principles of Security and Trust, Springer, 164–186.

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

114. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. *Princeton University Pre*

115. Neroth, P. (2013). Cyber currency - one way to bypass the euro? Engineering & Technology (17509637) 8, 18-18.

116. Nguyen, Q.K., (2016). Blockchain-A Financial Technology for Future Sustainable Development ,in: Proceedings-3rd International Conference on Green Technology and Sustainable Development, GTSD 2016, 51–54, 2016.

117. Nijeholt, H.L.A, J. Oudejans, J., Z. Erkin, Z. (2017). DecReg: A Framework for Preventing Double-Financing using Blockchain Technology, in: BCC 2017 - Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, co-located with ASIA CCS 2017, 29–34, 2017.

118. O'Dair, M. & Beaven, Z., (2017). The networked record industry: How blockchain technology could transform the record industry, Strategic Change 26 (5). 471–480.

119. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT, in: Advances in Intelligent Systems and Computing, vol. 520, 523–533

120. Paech, P.(2017). The governance of blockchain financial networks, Modern Law Review 80(6) 1073–111

121. Papadopoulos, G. (2015). Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies,153–172.

122. Patil, AS., Tama, BA. Park, Y. H. Rhee, K. (2018). A framework for blockchain based secure smart green house farming, in: Lecture Notes in Electrical Engineering, vol. 474, 1162–1167.

123. Paul Dunphy, F. (2018). A First Look at Identity Management Schemes on the Blockchain, To appear in IEEE Security and Privacy Magazine special issue on ”Blockchain Security and Privacy” in 2018 abs/1801.03294.

124. Peters, G. W., & Panayi, E. (2015). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. *Available at SSRN*.

125. Peters, GW.. Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, in: New Economic Windows, 239–278, 2016.

126. Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K. (2016). Ablockchain-basedapproachtohealthinformationexchangenetworks,in:Proc.NIST Workshop Blockchain Healthcare, vol. 1, 1–10,.

127. Pilkington, M. (2015). Blockchain technology: principles and applications. *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*.

128. Plassaras, N. A. (2013). Regulating digital currencies: bringing bitcoin within the reach of the IMF. Chicago Journal of International Law 14, 377-407

129. Poon, J. & Buterin, V. (2017). Plasma: Scalable Autonomous Smart Contracts, https://plasma.io/plasma.pdf.

130. Prybila, C., Schulte, S., Hochreiner, C. & and Weber, I. (2017). Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain. arXiv report 1706.04404. arXiv. https://arxiv.org/abs/1706.04404

131. Reid, F., & Harrigan, M. (2012). An Analysis of Anonymity in the Bitcoin System. University College Dublin.

132. Reijers, W. & O’Brolcha F. (2016). in, Haynes, P. Governance in Blockchain Technologies & Social Contract Theories, Ledger 134–151.

133. Ricardo, D. (1824), Plan for the Establishment of a National Bank, John Murray, London.

134. Rivera, R., Robledo, J.G., Larios,, V.M.. Avalos, J.M. (2017). How digital identity on blockchain can contribute in a smartcity environment, in:2017 International Smart Cities Conference (ISC2), 1–4.

135. Rizzo, P. (2014). How Kipochi Is Taking Bitcoin into Africa, http://www.coindesk.com/kipochi-taking-bitcoin-africa/.

136. Rizzo, P. (2017). Nasdaq and Citi Announce Pioneering Blockchain and Global Banking Integration, http://www.nasdaq.com/article/ nasdaq-and-citi-announce-pioneering-blockchain-and-global-banking-integration-cm792544, 2017.

137. Roberts, JJ. (2017). Microsoft and Accenture Unveil Global ID System for Refugees, http://fortune.com/2017/06/19/id2020- blockchain-microsoft/, 2017.

138. Robertson, BJ. (2015). Holacracy:The revolutionary management system that abolishes hierarchy, Penguin UK

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

140. Scitovsky, T. (1969). Money & the balance of payments. Vol. 81. Rand McNally.

141. Seebacher, S., R.Schuritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review, in: International Conference on Exploring Services Science, Springer, 12–23, 2017.

142. Selgin, G.. (2015). Synthetic commodity money. Journal of Financial Stability 17. 92-99.

143. Sikorski, JJ. Haughton, J., Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market, Applied Energy 195 (2017) 234–246.

144. Skaggs, N. T. (1999). Changing views: twentieth-century opinion on the banking school- currency school controversy. History of Political Economy 31, 361-391.

145. Smalley,C.V.(2017).Cryptocurrency and taxes.*Taxadviser*,p.1-3.

146. Stark, B. (2013). Is the corporate world ready for bitcoin? Risk Management 60, 6-9.

147. Subramanian, R. & Chino, T. (2016). The state of cryptocurrencies: Their issues and policy interactions. *Journal of International Technology & Information Management*, 24(3), p. 25-40.

148. Swan, M. (2015). Blockchain: Blue print for a new economy .O'ReillyMedia, Inc..

149. Takemoto, Y., Knight, S. (2014). Mt. Gox files for bankruptcy, hit with lawsuit. Reuters http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy- idUSBREA1R0FX20140228.

150. Tama, B.A., Kweka, B.J., Park, Y., Rhee, K.H. (2017) A critical review of blockchain and its current applications, in: Electrical Engineering and Computer Science (ICECOS), 2017 International Conference on, IEEE, 109–113, 2017.

151. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin.

152. Tapscott, D., Tapscott, A. (2017). How blockchain will change organizations. MIT Sloan Manag. Rev. 58(2), 10

153. Taylor, J. B. & Williams, J. (2010). Simple and robust rules for monetary policy. No. w15908. National Bureau of Economic Research.

154. The Economist. (2015, October 31). The trust machine. *The Economist*. Retrieved from https://www.economist.com/leaders/2015/10/31/the-trust-machine

155. The Genesis Block (2013). Bitcoin-Litecoin Ratio Returns to Historic Norm, Peercoin Climbs 200%. Tradeblock. http://tradeblock.com/research/bitcoin-litecoin-ratio-returns-historic-norm-peercoin-climbs-200/,

156. Toma, C. (2012). M-payments issues and concepts. Informatica Economica 16, 117-123.

157. Trautman, L. J., & Harrell, A. C. (2016). Bitcoin vs. Regulated Payment Systems: What Gives?. *Cardozo Law Review (forthcoming).*

158. Tschorsch, F. & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys Tutorials 18 (3) 2084–2123.

159. Tsukerman, M. (2015). The block is hot: A survey of the state of Bitcoin regulation and suggestions for the future, Berkeley Tech. LJ 30 1127.

160. Turk, Z., Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management, Procedia Engineering. 196. 638–645

161. Tymoigne (2015). Do Cryptocurrencies Such as Bitcoin Have a Future? No: As a Currency, Bitcoin Violates All The Rules of Finance. *Wall street journal – Eastern edition*, 265(49), p. 1-2.

162. Valentine, L. (2012). Payment innovations: are you in? American Bankers Association.ABA Banking Journal 104, 26-29,31-33.

163. Van de Velde, J. Scott, A., Sartorius, K., Dalton, I., Shepherd, B., Allchin, C., Dougherty, M., Ryan, P., Rennick, E. (2016). Blockchain in capital markets—The prize and the journey.

164. Vandervort, D., Gaucas, D., Jacques, R. (2015). Issues in Designing a Bitcoin-like Community Currency. In: Brenner M, Christin N, Johnson B, Rohloff K, editors. Financial Cryptography and Data Security. vol. 8976 of Lecture Notes in Computer Science. Springer Berlin Heidelberg. p. 78–91.

165. Varoufakis, Yanis (2014). BITCOIN: A flawed currency blueprint with a potentially useful application for the Eurozone. February 15, 2014. http://yanisvaroufakis.eu/2014/02/15/bitcoin-a-flawed-currency-blueprint-with- a-potentially-useful-application-for-the-eurozone/

166. Varriale, G. (2013). Bitcoin: how to regulate a virtual currency. International Financial Law Review from http://search.proquest.com/docview/1443818783?accountid=14541

167. Vasek, M., Thornton, M., & Moore, T. (2014, March). Empirical analysis of denial-of- service attacks in the Bitcoin ecosystem. In *International Conference on Financial Cryptography and Data Security* (pp. 57-71). Springer, Berlin, Heidelberg.

168. Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*.

169. Ventures, (M.). (2012). Medici,http://www.mediciventures.com/.

170. Viacoin. (2014). Viacoin Whitepaper, https://github.com/viacoin/documents/raw/master/whitepapers/Viacoin_whitepaper.pdf

171. Von Mises, L. (1953). The theory of money and credit. Ludwig von Mises Institute.

172. Vora, G. (2015). Cryptocurrencies: Are Disruptive Financial Innovations Here? *Modern Economy*, 6(7), p. 816-832.

173. Walsh, C. E. (2015). Goals and rules in central bank design (No. 5293). CESifo Group Munich.

174. Wells, C. J. (2011). Digital currency systems: emerging B2B e-commerce alternative during monetary crisis in the United States. Doctoral Dissertation, Aspen University.

175. White, G. (2017). Future Applications of Blockchain in Business and Management: a Delphi study' Strategic Change, vol 26, no. 5, pp. 439-451
176. White, L H. (1999). Why Didn't Hayek Favor Laissez Faire in Banking?. History of Political Economy 31.4; WIN: 753-769.
177. White, L. H. (1983). Competitive money, inside and out. Cato J. 3, 281.
178. White, L. H. (1984). Competitive payments systems and the unit of account. American Economic Review 74, 699.
179. Woodford, M. (2005). Interest and prices: Foundations of a theory of monetary policy. from Press.princeton.edu: http://press.princeton.edu/chapters/s7603.pdf
180. Wu, T., Liang, X. (2017). Exploration and practice of inter-bank application based on blockchain, in: ICCSE 2017 - 12th International Conference on Computer Science and Education, 219–224.
181. Xu, R., Zhang, L., Zhao, H., Peng, Y., (2017). Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology,in: Proceedings - 2017 IEEE 13th International Symposium on Autonomous Decentralized Systems, ISADS 2017, 128–133.
182. Xun, P. Zhu, P.-D., Hu, Y.-F., Cui, P.- Zhang, S.Y.. (2017). Command Disaggregation Attack and Mitigation in Industrial Internet of Things, Sensors 17 (10) 2408.
183. Yamada, Y., Nakajima, T., Sakamoto, M. (2017). Blockchain-LI: A study on implementing activity-based micro-pricing using cryptocurrency technologies, in: ACM International Conference Proceeding Series, 203–207.
184. Yermack, D. (2013). Is bitcoin a real currency? New York University Stern School of Business.
185. Ying, W., Jia, S., & Du, W. (2018). Digital enablement of blockchain: Evidence from HNA group. *Int J. Information Management, 39*, 1-4.
186. Yli-Huumo, J., Ko, D. S.Choi, S., Park, S., Smolander, K., (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review ,PloS one 11 (10)
187. Zalan, T. (2018). Born global on Blockchain. Rev. Int. Bus. Strat. 28(1), 19-34
188. Zhang, Y. JWen, J. (2015). An IoT electric business model based on the protocol of bitcoin, in: 2015 18th International Conference on Intelligence in Next Generation Networks, 184–191, doi:10.1109/ICIN.2015.7073830.

189. Zhao, J.L., Fan, J., Yan, j. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue, Financial Innovation 2 (1). 28.

190. Zhao, J.L.., Fan, S. & Yan, J., (2016). Overview of business innovations and research opportunities in block chain and introduction to the special issue, Financial Innovation 2 (1) 28.

191. Zheng, Z., Xie, S., Dai, H.N, Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services Vol.14 No.4, pp.352 - 375

192. Zyskind, G., Nathan, O., Pentland, A.S. (2015). Decentralizing privacy: Using blockchain to protect personal data, in: Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, 180–184.