Τμήμα Μηχανικών Η/Υ και Πληροφορικής

Κοινωνικές και Νομικές Πλευρές της Τεχνολογίας

Το Bitcoin ως ψηφιακό νόμισμα, και άλλες εφαρμογές των κατανεμημένων κρυπτο-οικονομιών

Παναγόπουλος Παναγιώτης ΑΜ: 4622

Ημερομηνία υποβολής: 12/06/2015

Περιεχόμενα

1 Πρόλογος

Το Bitcoin έγινε η πρώτη κατανεμημένη κρυπτο-οικονομία το 2009, παρουσιάζοντας μία νέα τεχνολογία στον χώρο των κατανεμημένων συστημάτων και των ψηφιακών οικονομιών, ένα μηχανισμό συμφωνίας σε κατανεμημένα περιβάλλοντα (decentralized consensus mechanism). Αυτή η εφεύρεση, η οποία αποτελεί την καρδιά του Bitcoin, δημιούργησε, τα χρόνια που ακολούθησαν, ένα κύμα από καινοτομίες στις ψηφιακές οικονομίες, στα κατανεμημένα συστήματα, στα συστήματα ηλεκτρονικής ψηφοφορίας, και τις συμβάσεις (contracts).

Σε αυτό το κείμενο παρουσιάζονται τα κύρια χαρακτηριστικά των κατανεμημένων κρυπτρο-οικονομιών και παρουσιάζονται οι προοπτικές αποδοχής κάποιου κρυπτο-νομίσματος ως ψηφιακό νόμισμα παγκόσμιας εμβέλειας, έχοντας ως σημείο αναφοράς το Bitcoin. Επίσης γίνεται αναφορά και σε άλλες εφαρμογές που μπορεί να υποστηρίξει αυτή η τεχνολογία, όπως αυτές έχουν προταθεί από την κοινότητα.

2 Ψηφιακές οικονομίες

Ως ψηφιακή οικονομία, ή ψηφιακό νόμισμα, ορίζεται μία οικονομία η οποία διαθέτει ιδιότητες παρόμοιες με μία φυσική/υλική οικονομία, ωστόσο επιτρέπει την πραγματοποίηση συναλλαγών άμεσα, μεταξύ οποιωνδήποτε σημείων βρίσκονται στην περιοχή κάλυψης του μέσου που χρησιμοποιείται. Οι εικονικές οικονομίες και οι κρυπτο-οικονομίες είναι κατηγορίες ψηφιακών οικονομιών.

Οι εικονικές οικονομίες, ή εικονικά νομίσματα, ορίζονται ως οικονομίες οι οποίες δεν προορίζονται για χρήση στον πραγματικό κόσμο, αλλά περιορίζονται σε εικονικά περιβάλλοντα. Δηλαδή τα εικονικά νομίσματα δεν βασίζονται στην φυσική πραγματικότητα και δεν μπορούν να χρησιμοποιηθούν ως αντιπροσωπευτικά περιουσιακών στοιχείων. Ως αποτέλεσμα αυτού οι εικονικές οικονομίες συναντώνται κυρίως σε παιχνίδια στο διαδίκτυο και υπόκεινται στον έλεγχο των δημιουργών του ψηφιακού κόσμου.

Οι κρυπτο-οικονομίες είναι ψηφιακές οικονομίες οι οποίες χρησιμοποιούν κρυπτογραφικά σχήματα για την ασφάλεια των συναλλαγών και τον έλεγχο της δημιουργίας νέων μονάδων αξίας.

Το bitcoin είναι η πρώτη κατανεμημένη κρυπτο-οικονομία. Προτάθηκε ως ένα ομότιμο (peer-to-peer) ηλεκτρονικό σύστημα πληρωμών το 2008 σε δημοσίευση με τίτλο “Bitcoin: A Peer-to-Peer Electronic Cash System” [1], την οποία ο συγγραφέας υπογράφει με το ψευδώνυμο Satoshi Nakamoto. Το 2009 δημοσιεύεται η πρώτη έκδοση του συστήματος ως λογισμικό ανοιχτού κώδικα, ο συγγραφέας του οποίου υπογράφει πάλι με το ψευδώνυμο Satoshi Nakamoto.

3 Γιατί κρυπτογραφικά σχήματα;

Η χρήση κρυπτογραφικών σχημάτων για την δημιουργία ψηφιακών νομισμάτων δεν είναι κάτι νέο. Το Bitcoin δεν είναι η πρώτη κρυπτο-οικονομία, αλλά η πρώτη

κατανεμημένη κρυπτο-οικονομία. Η ανάγκη για βιώσιμο ψηφιακό χρήμα είναι στενά συνδεδεμένη με την ανάπτυξη στον τομέα της κρυπτογραφίας. Αυτή η σχέση γίνεται ξεκάθαρη αν αναλογιστούμε τις βασικές προκλήσεις που εμφανίζονται όταν χρησιμοποιούνται bits για να την αναπαράσταση αξίας η οποία μπορεί να ανταλλάσσεται για αγαθά και υπηρεσίες.

Δύο βασικά ερωτήματα που δημιουργούνται σε οποιονδήποτε είναι πρόθυμος να δεχτεί ψηφιακά χρήματα είναι τα ακόλουθα:

- μπορώ να είμαι σίγουρος πως τα χρήματα είναι αυθεντικά και όχι πλαστά;
- μπορώ να είμαι σίγουρος πως κανείς άλλος δεν έχει την δυνατότητα να ισχυριστεί πως τα χρήματα ανήκουν στον ίδιο και όχι σε εμένα; (το γνωστό ως “double-spend” πρόβλημα)

Όσο αφορά τις παραδοσιακές οικονομίες στις οποίες χρησιμοποιούνται κέρματα και χαρτονομίσματα, το πρώτο πρόβλημα αντιμετωπίζεται χρησιμοποιώντας όλο και πιο εξειδικευμένα υλικά και τεχνικές εκτύπωσης. Τα φυσικά χρήματα αντιμετωπίζουν αποτελεσματικά το double-spend πρόβλημα εύκολα διότι το ίδιο χαρτονόμισμα δεν μπορεί να βρίσκεται σε δύο μέρη ταυτόχρονα. Ωστόσο, τα παραδοσιακά χρήματα συχνά αποθηκεύονται και μεταφέρονται ψηφιακά. Σε αυτές τις περιπτώσεις τα παραπάνω δύο προβλήματα αντιμετωπίζονται δρομολογώντας όλες τις συναλλαγές μέσω κεντρικών αρχών οι οποίες έχουν την δυνατότητα να διατηρούν μία συνολική εικόνα των χρημάτων σε κυκλοφορία. Για ψηφιακές οικονομίες οι οποίες δεν μπορούν να αναπτύξουν και να διατηρήσουν μία τόσο ισχυρά κεντρικοποιημένη δομή παραμένοντας ταυτόχρονα αποδοτικές, η κρυπτογραφία παρέχει την βάση της εμπιστοσύνης στη γνησιότητα του ισχυρισμού κάποιου χρήστη για ιδιοκτησία αξίας.

Πιο συγκεκριμένα, κρυπτογραφικές ψηφιακές υπογραφές παρέχουν την δυνατότητα σε ένα χρήστη να υπογράψει ένα ψηφιακό περιουσιακό στοιχείο ή μία συναλλαγή, παραχωρώντας την ιδιοκτησία σε κάποιον άλλον. Με την κατάλληλη αρχιτεκτονική, οι κρυπτογραφικές ψηφιακές υπογραφές, μπορούν επίσης να αντιμετωπίσουν το double-spend πρόβλημα.

Όταν η κρυπτογραφία άρχισε να γίνεται περισσότερο προσβάσιμη και κατανοητή στα τέλη του 1980, αρκετοί ερευνητές άρχισαν να χρησιμοποιούν κρυπτογραφικά σχήματα για να χτίσουν ψηφιακές οικονομίες. Αυτές οι πρώιμες ψηφιακές οικονομίες χρησιμοποιούσαν ψηφιακά χρήματα, τα οποία συνήθως υποστηρίζονταν από κάποια εθνική οικονομία ή από πολύτιμα μέταλλα όπως ο χρυσός και το ασήμι.

Αν και αυτές οι ψηφιακές οικονομίες λειτούργησαν, ή αρχιτεκτονική τους ήταν κεντρικοποιημένη, και αυτό είχε ως αποτέλεσμα να είναι εύκολος στόχος επίθεσης από κυβερνήσεις, άλλες ανταγωνιστικές οικονομίες, αλλά και hackers. Αντίθετα μία κατανεμημένη ψηφιακή οικονομία είναι ανθεκτική απέναντι σε θεμιτές και αθέμιτες παρεμβάσεις, διότι ως κατανεμημένο σύστημα δεν διαθέτει κάποιο μοναδικό σημείο επίθεσης. Η επιβίωσή της εξαρτάται από την πρόθεση των χρηστών να την αποδέχονται και να την χρησιμοποιούν.

Το Bitcoin είναι ένα τέτοιο σύστημα, πλήρως κατανεμημένο, και απαλλαγμένο από κεντρικές αρχές ή σημεία ελέγχου τα οποία μπορούν να δεχτούν επίθεση ή να αλλοιωθούν με κακόβουλο τρόπο.

Το Bitcoin αντιπροσωπεύει δεκαετίες έρευνας στον τομέα της κρυπτογραφίας και των κατανεμημένων συστημάτων, και συνδυάζει 4 καινοτομίες με μοναδικό και ισχυρό συνδυασμό:

- ένα κατανεμημένο, ομότιμο (peer-to-peer) δίκτυο
- ένα δημόσιο αρχείο με όλες τις συναλλαγές (blockchain)
- ένα κατανεμημένο, μαθηματικό και ντετερμινιστικό μηχανισμό έκδοσης νέων νομισμάτων
- ένα κατανεμημένο μηχανισμό επικύρωσης των συναλλαγών

4 Τι είναι το Bitcoin;

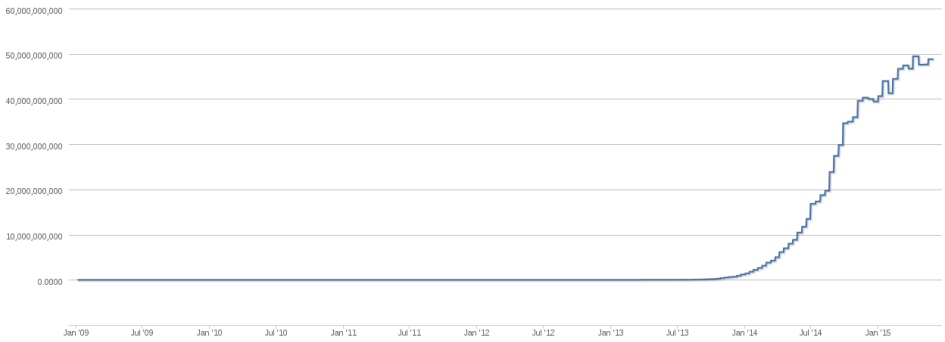
Πιο συγκεκριμένα, το Bitcoin είναι μία συλλογή εννοιών και τεχνολογιών οι οποίες διαμορφώνουν την βάση ενός οικοσυστήματος ψηφιακού χρήματος. Νομισματικές μονάδες, οι οποίες ονομάζονται bitcoins, χρησιμοποιούνται για να αποθηκεύουν και να μεταφέρουν αξία μεταξύ των συμμετεχόντων στο bitcoin δίκτυο. Οι χρήστες επικοινωνούν μεταξύ τους χρησιμοποιώντας το bitcoin πρωτόκολλο κυρίως χρησιμοποιώντας ως μέσο το internet, αν και είναι δυνατόν να χρησιμοποιηθούν επίσης και άλλα δίκτυα μεταφοράς. Η στοίβα του bitcoin πρωτοκόλλου, η οποία προσφέρεται ως κώδικας ανοιχτού λογισμικού, μπορεί να εκτελεστεί σε πληθώρα συσκευών, συμπεριλαμβανομένων των laptops και των smartphones, καθιστώντας την τεχνολογία εύκολα προσβάσιμη.

Οι χρήστες μπορούν να μεταφέρουν bitcoins δια μέσω του δικτύου και να πραγματοποιήσουν οποιαδήποτε ενέργεια μπορεί να πραγματοποιηθεί με τα συμβατικά νομίσματα, όπως την αγορά και πώληση αγαθών, την αποστολή χρημάτων σε άτομα και οργανισμούς, ή την παροχή πίστωσης. Τα bitcoins μπορούν να αγοράζονται, να πωλούνται, και να ανταλλάζονται με άλλα νομίσματα.

Αντίθετα με τις παραδοσιακές μορφές χρήματος, το Bitcoin είναι εξ ολοκλήρου ψηφιακό. Δεν υπάρχουν φυσικά νομίσματα, αλλά ούτε και ψηφιακά νομίσματα. Τα νομίσματα “υπονοούνται” στις συναλλαγές οι οποίες μεταφέρουν αξία από τον αποστολέα στον παραλήπτη. Οι bitcoin χρήστες διαθέτουν κλειδιά τα οποία τους δίνουν την δυνατότητα να αποδείξουν την ιδιοκτησία των συναλλαγών στο bitcoin δίκτυο, ξεκλειδώνοντας την αξία ώστε να την ξοδέψουν (μεταφέρουν) σε κάποιο άλλο χρήστη. Αυτά τα κλειδιά συνήθως αποθηκεύονται σε ένα ψηφιακό πορτοφόλι στον υπολογιστή κάθε χρήστη. Η κατοχή του κλειδιού το οποίο ξεκλειδώνει μία συναλλαγή είναι το μόνο προαπαιτούμενο για την δαπάνη κάποιων bitcoins, εναποθέτοντας τον έλεγχο εξ ολοκλήρου στον τελικό χρήστη.

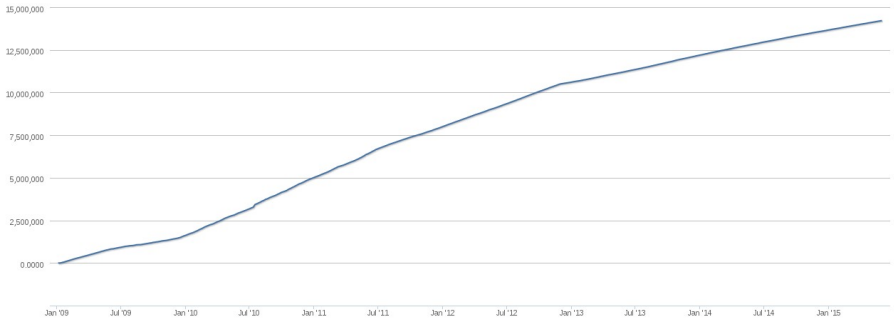
Το Bitcoin είναι ένα κατανεμημένο, ομότιμο (peer to peer) σύστημα. Ως ένα τέτοιο σύστημα δεν διαθέτει κεντρικό εξυπηρετητή ή κάποιο σημείο ελέγχου. Τα bitcoins δημιουργούνται μέσω μιας διαδικασίας η οποία ονομάζεται εξόρυξη, και η οποία περιλαμβάνει ανταγωνισμό για την εύρεση λύσεων σε ένα μαθηματικό πρόβλημα, καθώς επεξεργάζονται οι bitcoin συναλλαγές. Κάθε ένας ο οποίος συμμετέχει στο bitcoin δίκτυο, δηλαδή οποιοσδήποτε χρησιμοποιεί κάποια συσκευή που εκτελεί την

πλήρη στοίβα του bitcoin πρωτοκόλλου, μπορεί να πραγματοποιεί εξόρυξη, χρησιμοποιώντας την υπολογιστική ισχύ του υπολογιστή του για να επικυρώσει και να καταχωρήσει συναλλαγές. Κάθε 10 λεπτά, κατά μέσο όρο, κάποιος είναι σε θέση να επικυρώσει τις συναλλαγές των περασμένων 10 λεπτών και αμείβεται με ολοκαίνουργια bitcoins. Ουσιαστικά, η διαδικασία της εξόρυξης αποκεντρώνει τις λειτουργίες έκδοσης και εκκαθάρισης νομισμάτων, και με αυτό τον τρόπο αντικαθιστά την ανάγκη για μία κεντρική τράπεζα με αυτόν τον καθολικό διαγωνισμό.



σχήμα. 1: η δυσκολία της υπολογιστικής διαδικασίας στην εξόρυξη
πηγή: blockchain.info

Το bitcoin πρωτόκολλο περιλαμβάνει ενσωματωμένους αλγορίθμους οι οποίοι ρυθμίζουν την λειτουργία της εξόρυξης σε όλο το δίκτυο. Η δυσκολία της υπολογιστικής διαδικασίας που πρέπει να εκτελέσουν οι χρήστες οι οποίοι συμμετέχουν στην εξόρυξη ρυθμίζεται δυναμικά, έτσι ώστε, κατά μέσο όρο κάποιος να επιτυγχάνει κάθε 10 λεπτά, άσχετα από τον αριθμό των συμμετεχόντων και των επεξεργαστών που εργάζονται κάθε στιγμή. Επίσης, το πρωτόκολλο, μειώνει στο μισό το ρυθμό με τον οποίο δημιουργούνται νέα bitcoins κάθε 4 χρόνια, και με αυτό τον τρόπο βάζει ένα άνω όριο στο συνολικό αριθμό των bitcoins που θα δημιουργηθούν περιορίζοντάς τα στα 21 εκατομμύρια. Συνέπεια αυτού είναι πως ο αριθμός των bitcoins τα οποία κυκλοφορούν ακολουθεί μία εύκολα προβλέψιμη καμπύλη η οποία αγγίζει τα 21 εκατομμύρια το έτος 2140. Λόγω του φθίνοντος ρυθμού έκδοσης, μακροπρόθεσμα, η bitcoin οικονομία είναι αποπληθωριστική. Επιπλέον, στην bitcoin οικονομία δεν μπορεί να υπάρξει πληθωρισμός ως αποτέλεσμα της έκδοσης νέων νομισμάτων πάνω από τον προκαθορισμένο ρυθμό έκδοσης.



σχήμα. 2: το σύνολο των bitcoins σε κυκλοφορία
πηγή: blockchain.info

Bitcoin είναι το όνομα ενός νομίσματος, ενός πρωτοκόλλου, ενός δικτύου, και ενός καινοτόμου κατανεμημένου υπολογιστικού σχήματος. Η bitcoin οικονομία είναι μόνο μία από τις εφαρμογές που μπορεί να υποστηρίξει αυτό το σχήμα. Το Bitcoin μπορεί να χαρακτηριστεί ως το “internet του χρήματος”, δηλαδή ένα δίκτυο για την μετάδοσή της αξίας και την προστασία της ιδιοκτησίας ψηφιακών περιουσιακών στοιχείων μέσω κατανεμημένου υπολογισμού.

5 Κλειδιά / πορτοφόλι

5.1 Ο έλεγχος στον τελικό χρήστη

Αν και σκοπός αυτού του κειμένου δεν είναι να πραγματοποιηθεί λεπτομερής αναφορά στα τεχνικά χαρακτηριστικά του Bitcoin, σε αυτό το σημείο αξίζει να γίνει μία εξαίρεση, διότι το σύστημα των κλειδιών επιτρέπει πολλές από τις ενδιαφέρουσες ιδιότητες του bitcoin, και γενικά των κρυπτο-οικονομιών, και αποτελεί ένα από τα χαρακτηριστικά τα οποία ισχυροποιούν τον τελικό χρήστη παρέχοντάς του τον απόλυτο έλεγχο των χρημάτων του.

Η ιδιοκτησία στο bitcoin δίκτυο καθορίζεται μέσω των ψηφιακών κλειδιών, των bitcoin διευθύνσεων, και των ψηφιακών υπογραφών. Τα ψηφιακά κλειδιά δεν αποθηκεύονται στο δίκτυο, αλλά δημιουργούνται και αποθηκεύονται από τους χρήστες σε ένα αρχείο, ή μία απλή βάση δεδομένων, το οποίο αποτελεί αυτό που ονομάζεται ψηφιακό bitcoin πορτοφόλι. Τα ψηφιακά κλειδιά στο πορτοφόλι ενός χρήστη είναι απόλυτα ανεξάρτητα από το bitcoin δίκτυο και μπορούν να παραχθούν και να διαχειριστούν από το λογισμικό του πορτοφολιού του χρήστη χωρίς να χρειάζεται αναφορά στο δημόσιο αρχείο συναλλαγών (blockchain), ή πρόσβαση στο διαδίκτυο. Τα κλειδιά επιτρέπουν πολλές από τις ενδιαφέρουσες ιδιότητες του Bitcoin, και γενικά των κρυπτο-οικονομιών, συμπεριλαμβανομένου του κατανεμημένου ελέγχου και εμπιστοσύνης, της βεβαίωσης της ιδιοκτησίας, και του κρυπτογραφικού μοντέλου ασφαλείας.

Το Bitcoin χρησιμοποιεί τεχνολογία κρυπτογραφίας δημοσίου κλειδιού (public key cryptography). Συγκεκριμένα χρησιμοποιεί πολλαπλασιασμό ελλειπτικής καμπύλης (elliptic curve multiplication), ως βάση της κρυπτογραφίας δημοσίου κλειδιού. Το ιδιωτικό κλειδί είναι ένας τυχαίος δυαδικός αριθμός μήκους 256 bits. Χαρακτηριστικά

μπορείς να δημιουργήσεις ένα ιδιωτικό κλειδί ρίχνοντας απλά ένα νόμισμα 256 φορές. Για την ακρίβεια για να είναι αυτός ο αριθμός ένα έγκυρο ιδιωτικό κλειδί πρέπει απλά να βρίσκεται στο διάστημα μεταξύ 1 και n-1, όπου n είναι μία σταθερά η οποία ορίζεται στο πρότυπο ελλειπτικής καμπύλης secp256k1 το χρησιμοποιείται στο bitcoin. Το ιδιωτικό κλειδί χρησιμοποιείται στην δημιουργία ψηφιακών υπογραφών οι οποίες απαιτούνται για την μετάθεση της ιδιοκτησίας των χρημάτων σε μία συναλλαγή. Μία ψηφιακή υπογραφή μπορεί να επαληθευτεί χρησιμοποιώντας το δημόσιο κλειδί, χωρίς να χρειάζεται να αποκαλυφθεί το ιδιωτικό κλειδί. Το δημόσιο κλειδί παράγεται από το ιδιωτικό χρησιμοποιώντας πολλαπλασιασμό ελλειπτικής κρυπτογραφίας. Σύμφωνα με αυτή την διαδικασία, ένα ιδιωτικό κλειδί μπορεί να παράξει ένα δημόσιο, αλλά από ένα δημόσιο κλειδί δεν μπορεί να υπολογιστεί το ιδιωτικό. Μία bitcoin διεύθυνση παράγεται από το δημόσιο κλειδί, χρησιμοποιώντας μία one-way συνάρτηση.

Όταν ξοδεύονται bitcoins, ο κάτοχος των bitcoins παρέχει το δημόσιο κλειδί του και μία ψηφιακή υπογραφή (διαφορετική κάθε φορά, η οποία όμως παράγεται από το ίδιο ιδιωτικό κλειδί) σε μία συναλλαγή όπου μεταθέτει την ιδιοκτησία των bitcoins σε κάποια άλλη bitcoin διεύθυνση. Όπως αναφέρθηκε πιο πάνω οποιοσδήποτε μπορεί να επαληθεύσει την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί.

5.2 Η ευθύνη στον τελικό χρήστη

Το κατανεμημένο μοντέλο ασφάλειας του bitcoin δικτύου μεταβιβάζει δύναμη στον τελικό χρήστη με την πληθώρα των δυνατοτήτων και της ελευθερίας που του παρέχει. Αυτήν η δύναμη όμως συνοδεύεται από την ευθύνη για την διατήρηση της μυστικότητας του ιδιωτικού κλειδιού κάθε bitcoin διεύθυνσης. Είναι προφανές πως για αρκετούς χρήστες αυτό δεν είναι εύκολο, ειδικά σε υπολογιστικές συσκευές γενικού σκοπού όπως είναι οι προσωπικοί υπολογιστές, τα smartphones ή τα tablets.

Στο bitcoin δίκτυο η κατοχή των κλειδιών τα οποία ξεκλειδώνουν (δίνουν την δυνατότητα να μεταφερθούν σε κάποιο άλλο άτομο - ξοδευτούν) τα bitcoins κάποιων διευθύνσεων, είναι το αντίστοιχο της κατοχής μετρητών ή μιας ποσότητας κάποιου πολύτιμου μετάλλου. Αν κλαπούν ή χαθούν, ο χρήστης δεν μπορεί να καταφύγει σε κάποια αρχή για να λάβει πίσω τον έλεγχο των bitcoins αυτών των διευθύνσεων, ακριβώς όπως όταν κάποιος χάνει μετρητά στο δρόμο. Χαρακτηριστικό παράδειγμα προς αποφυγή, είναι κάποιος να διατηρεί αποθηκευμένα όλα τα κλειδιά του σε ένα μόνο αποθηκευτικό μέσο, έστω σε ένα σκληρό δίσκο, και κάποια στιγμή ο σκληρός δίσκος να καταστραφεί. Αξίζει να σημειωθεί πως στο σενάριο όπου ένα κλειδί έχει απλά χαθεί, τα bitcoins της συγκεκριμένης διεύθυνσης θα παραμείνουν αξόδευτα. Ωστόσο ένα bitcoin πορτοφόλι που περιέχει ένα ή περισσότερα κλειδιά, είναι απλά ένα αρχείο, και ως τέτοιο μπορεί να αντιγραφεί. Έτσι είναι δυνατόν να δημιουργηθούν πολλαπλά αντίγραφα, και να αποθηκευτούν σε περισσότερα από ένα αποθηκευτικά μέσα. Επίσης μπορούν να δημιουργηθούν φυσικά αντίγραφα, εκτυπώνοντας τα κλειδιά σε χαρτί.

Η ασφάλεια του bitcoin δικτύου βασίζεται στον κατανεμημένο έλεγχο των κλειδιών από τους ιδιοκτήτες τους, και στην ανεξάρτητη επικύρωση των συναλλαγών από τους χρήστες που πραγματοποιούν την λειτουργία της εξόρυξης, τους miners. Ενέργειες όπως η απομάκρυνση του ελέγχου των κλειδιών από τους ιδιοκτήτες τους, καθώς και

η πραγματοποίηση συναλλαγών εκτός της δομής του δημόσιου αρχείου συναλλαγών (offblockchain transactions), βρίσκονται εκτός του bitcoin μοντέλου ασφάλειας, και θέτουν σε κίνδυνο τους λογαριασμούς των τελικών χρηστών. Για παράδειγμα, πολλοί από τους αρχικούς παρόχους υπηρεσιών συναλλάγματος (exchanges) αποθήκευαν τα κλειδιά των πελατών τους στους εξυπηρετητές τους και συγκέντρωναν τα κεφάλαια όλων των πελατών τους σε ένα μοναδικό πορτοφόλι. Με αυτό τον τρόπο αφαιρούσαν τον έλεγχο των κλειδιών από τους χρήστες και τον συγκέντρωναν σε ένα μοναδικό σύστημα. Επίσης κάποιοι πάροχοι στην προσπάθειά τους να αυξήσουν τον αριθμό διεκπεραίωσης των συναλλαγών, διατηρούσαν ένα ιδιωτικό αρχείο καταγραφής των συναλλαγών το οποίο κατά διαστήματα συγχρόνιζαν με το δημόσιο καθολικό αρχείο καταγραφής συναλλαγών του bitcoin δικτύου (blockchain), υπονομεύοντας και πάλι την διαφάνεια των συναλλαγών των πελατών τους. Πολλά από αυτά τα συστήματα, τα οποία επέλεξαν να κινηθούν εκτός του bitcoin μοντέλου ασφάλειας, παραβιάστηκαν επιφέροντας καταστροφικές συνέπειες για τους πελάτες τους.

6 Ασφάλεια

Ένα κατανεμημένο σύστημα, όπως το Bitcoin, μεταφέρει την ευθύνη και τον έλεγχο στον τελικό χρήστη. Μία bitcoin συναλλαγή επικυρώνει μόνο την μεταφορά μιας αξίας σε ένα παραλήπτη, και δεν είναι δυνατόν να τροποποιηθεί. Επίσης δεν αποκαλύπτει ιδιωτικές πληροφορίες, όπως οι ταυτότητες των συναλλασσομένων, και δεν μπορεί να χρησιμοποιηθεί για να την επικύρωση επιπλέον συναλλαγών. Έτσι η δικτυακή κίνηση στο bitcoin δίκτυο δεν χρειάζεται να είναι κρυπτογραφημένη ή να προστατεύεται από υποκλοπές. Για παράδειγμα μία bitcoin συναλλαγή μπορεί να γίνει broadcast δημόσια σε μη ασφαλή κανάλια όπως WIFI χωρίς κρυπτογράφηση, ή Bluetooth, χωρίς να υπονομεύεται η ασφάλεια του δικτύου ή των συναλλασσομένων.

Η βασική αρχή στο Bitcoin είναι ο αποκεντρωτισμός. Αντίθετα με ένα κεντρικοποιημένο μοντέλο, όπως μία παραδοσιακή τράπεζα ή ένα παραδοσιακό δίκτυο πληρωμών, το Bitcoin δεν στηρίζει την ασφάλειά του στον έλεγχο της πρόσβασης των εμπλεκομένων στο δίκτυο, και δεν βασίζεται στο να διατηρεί τους κακόβουλους χρήστες έξω από αυτό. Και αυτό διότι κανείς κακόβουλος δεν είναι σε θέση να πάρει τον έλεγχο του συστήματος ή καλύτερα του δικτύου, σε οποιοδήποτε σημείο του δικτύου και αν βρίσκεται.

Η ασφάλεια του bitcoin δικτύου βασίζεται στο σχήμα της απόδειξης της εργασίας (proof of work), και βασική προϋπόθεση για να παραμένει το σύστημα ασφαλές είναι οι μη κακόβουλοι κόμβοι του δικτύου να διατηρούν συνολικά περισσότερη υπολογιστική ισχύ από οποιαδήποτε άλλη ομάδα κακόβουλων κόμβων. Ωστόσο για να συμμετάσχει κάποιος στο δίκτυο του bitcoin και να πραγματοποιήσει εξόρυξη, χρειάζεται αρκετή ηλεκτρική ενέργεια, και το bitcoin είναι έτσι σχεδιασμένο ώστε να είναι πιο κερδοφόρο όταν συνεργάζεσαι με το σύστημα παρά όταν λειτουργείς κακόβουλα.

7 Ο ανοιχτός χαρακτήρας, και το διαδίκτυο του χρήματος

Το Bitcoin είναι ένα ανοιχτό δίκτυο για το οποίο μπορείς να δημιουργήσεις και να εφαρμόσεις άμεσα κάποια εφαρμογή χωρίς να χρειάζεται να πιστοποιήσεις την ταυτότητά σου δίκτυο και χωρίς να χρειάζεται να ζητήσεις άδεια από κάποιον. Το

bitcoin δίκτυο προσφέρει όλα αυτά που αντιπροσωπεύει η φράση “καινοτομία χωρίς άδεια” (innovation without permission). Δηλαδή παρέχει χώρο για την δημιουργία νέων υπηρεσιών πάνω στο πρωτόκολλο του Bitcoin, ακριβώς όπως το διαδίκτυο παρείχε, και συνεχίζει να παρέχει, την δυνατότητα σε οποιονδήποτε να χτίσει την εφαρμογή του πάνω στην στοίβα πρωτοκόλλων TCPI/IP. Αυτό είναι ένα πολύ σημαντικό χαρακτηριστικό, ίσως ένα τα σημαντικότερα, αν αναλογιστούμε τον αντίκτυπο που έχει το διαδίκτυο, και οι διάφορες υπηρεσίες που εμφανίζονται κατά καιρούς και παρέχονται μέσα από αυτό, στην ανθρώπινη πραγματικότητα.

Στο άλλο άκρο βρίσκεται το τραπεζικό σύστημα. Δεν είναι σε θέση ο οποιοσδήποτε να υλοποιήσει κάποια υπηρεσία πάνω στο δίκτυο της Visa για παράδειγμα, και αυτό διότι δεν είναι σε θέση ο οποιοσδήποτε να λάβει άδεια για να χρησιμοποιήσει τέτοια κλειστά δίκτυα. Φυσικά, αν συνέβαινε κάτι τέτοιο, θα κινδύνευε η ασφάλεια αυτών των δικτύων διότι στηρίζουν την ασφάλειά τους στον έλεγχο της πρόσβασης. Το Bitcoin, όπως αναφέρθηκε και πιο πάνω, δεν στηρίζει την ασφάλειά του στο να διατηρεί τους κακόβουλους χρήστες έξω από αυτό.

Μπορούμε να πούμε πως το Bitcoin εμφανίζεται ως άμεση απειλή για υπηρεσίες όπως το paypal. Το paypal είναι η πλέον δημοφιλής υπηρεσία η οποία χρησιμοποιείται για αγορές στο διαδίκτυο, και λειτουργεί πάνω στο υπάρχον τραπεζικό σύστημα, και αυτό έχει ως αποτέλεσμα να περιορίζεται η λειτουργικότητά του από αυτό. Η ταχύτητά του, η ασφάλειά του, τα “σύνορά” του, τα τέλη συναλλαγών, και οι πολιτικές χρήσης του, είναι η ταχύτητα, η ασφάλεια, τα “σύνορα”, τα τέλη συναλλαγών, και οι πολιτικές χρήσης, του υπάρχοντος τραπεζικού συστήματος.

Ωστόσο, σε ένα κόσμο όπου οι άνθρωποι πειραματίζονται και δημιουργούν, τα “ανοιχτά” συστήματα κερδίζουν, διότι επιτρέπουν την καινοτομία να ευδοκιμήσει στον μέγιστο βαθμό. Όταν έχεις αυτά τα δύο περιβάλλοντα να λειτουργούν το ένα δίπλα στο άλλο, ένα παραδοσιακό τραπεζικό περιβάλλον όπου τα πάντα απαιτούν έγκριση, και ένα σύστημα το οποίο είναι ανοιχτό στην ολότητά του όπου η καινοτομία μπορεί να εφαρμοστεί χωρίς άδεια, δεν είναι παρανοϊκά δύσκολο να φανταστείς σε ποιο από τα δύο είναι περισσότερο πιθανόν να συμβεί η επόμενη καινοτόμα υπηρεσία.

Σύμφωνα με τα παραπάνω το Bitcoin, και γενικά οι κατανεμημένες κρυπτο-οικονομίες και η blockchain τεχνολογία, μπορούμε να πούμε πως δικαιολογημένα χαρακτηρίζονται από κάποιους ως “το διαδίκτυο του χρήματος” (“the internet of money”).

8 Χρήση σε εγκληματικές ενέργειες

Το Bitcoin είναι γρήγορο, ασφαλές και δεν έχει σύνορα, ιδιότητες που το καθιστούν την τέλεια μορφή νομίσματος για το διαδίκτυο. Επίσης το Bitcoin, και γενικά οι κρυπτο-οικονομίες, δίνουν την δυνατότητα στους συναλλασσομένους για πλήρως ανώνυμες συναλλαγές αξιών. Στην πραγματικότητα, το Bitcoin και οι άλλες υπάρχουσες κρυπτο-οικονομίες, είναι ψευδο-ανώνυμες. Ωστόσο κανείς μπορεί εύκολα να επιτύχει ανώνυμες, μη ανιχνεύσιμες, συναλλαγές. Επίσης μέσω προσθηκών στο ήδη υπάρχον πρωτόκολλο, όπως αυτές που προτείνει το Zerocoin [3] για κατανεμημένο ξέπλυμα χρήματος, μία κρυπτο-οικονομία μπορεί να προσφέρει σε όλους τους χρήστες της πλήρης ανωνυμία.

Ένα τέτοιο χαρακτηριστικό είναι ιδιαίτερα επιθυμητό σε εγκληματικές δραστηριότητες. Χαρακτηριστικό είναι το παράδειγμα, της χρήσης του Bitcoin ως νομίσματος στο Silkroad, μία διαδικτυακή αγορά στο δίκτυο Tor στην οποία γίνονταν αγοραπωλησίες κυρίως ναρκωτικών και παράνομων υπηρεσιών. Από την άλλη όμως, ένα τέτοιο χαρακτηριστικό είναι ιδιαίτερα επιθυμητό και σε νόμιμες και κοινωνικά αποδεκτές δραστηριότητες, όπως για παράδειγμα είναι οι φιλανθρωπίες.

Το Bitcoin είναι μία τεχνολογία. Η τεχνολογία είναι ουδέτερη. Χαρακτηριστικά μπορούμε να παρομοιάσουμε την τεχνολογία με ένα σφυρί. Μπορείς να το χρησιμοποιήσεις για να χτίσεις ένα σπίτι, ή για να συνθλίψεις το κρανίο κάποιου. Το Bitcoin είναι μία νέα τεχνολογία, και ως νέα τεχνολογία, μία από τις πρώτες εφαρμογές της είναι συχνά στα χέρια εγκληματιών.

Οι εγκληματίες είναι μία από τις πρώτες ομάδες ατόμων που είναι διατεθειμένες να χρησιμοποιήσουν την τελευταία λέξη της τεχνολογίας, επειδή λειτουργούν σε ένα περιβάλλον το οποίο χαρακτηρίζεται από υψηλά κέρδη, αλλά και υψηλά επίπεδα ρίσκου. Σε ένα τέτοιο περιβάλλον υπάρχει τεράστιος ανταγωνισμός και το να πάρεις το ρίσκο να κάνεις χρήση κάποιας νέας, μη διαδεδομένης τεχνολογίας, αν αναλαμβάνεις ήδη αρκετά ρίσκα, δεν είναι κάτι σημαντικό. Αλλά αν η χρήση αυτής της νέας τεχνολογίας σε φέρει σε πλεονεκτική θέση έναντι των αντιπάλων και των ανταγωνιστών σου, τότε τα κέρδη σου είναι μεγάλα.

9 Νομικό πλαίσιο χρήσης (regulation)

Η δυνατότητα χρήσης των κρυπτο-οικονομιών σε εγκληματικές δραστηριότητες καθώς και σε περιπτώσεις που είναι επιθυμητή η παράκαμψη των περιορισμών, των “συνόρων”, και των τελών των συναλλαγών που επιβάλλει το υπάρχον τραπεζικό σύστημα, οδήγησε κάποιες χώρες στο να κηρύξουν παράνομη την χρήση του bitcoin, ως το δημοφιλέστερο εξ αυτών, άλλες να προχωρήσουν σε συζητήσεις ως προς την επιβολή κανόνων στην χρήση του, και τις περισσότερες να μην το αναγνωρίζουν ως ψηφιακό νόμισμα.

Όσον αφορά την Ευρώπη και την Ελλάδα, σύμφωνα με πρόσφατο έγγραφο της ευρωπαϊκής κεντρικής τράπεζας (ECB) τον Φεβρουάριο του 2015 [4], στο οποίο παρουσιάζεται μία ανάλυση των σχημάτων εικονικών οικονομιών, η πλειοψηφία των χωρών της Ευρώπης, σε γενικές γραμμές, δεν αναγνωρίζουν τα εικονικά νομίσματα ως πραγματικές οικονομίες και προς αυτήν την κατεύθυνση έχουν προχωρήσει στην έκδοση προειδοποιήσεων όσο αφορά τους κινδύνους κατά τη χρήση τους. Συγκεκριμένα η τράπεζα της Ελλάδος έχει εκδώσει προειδοποίηση στις 11/02/2014 με τίτλο “Ενημέρωση για την χρήση εικονικών νομισμάτων” [5], στην οποία παραπέμπει στην σχετική ανακοίνωση της Ευρωπαϊκής Αρχής Τραπεζών (EBA) με τίτλο “Προειδοποίηση προς τους καταναλωτές για τα εικονικά νομίσματα” και ημερομηνία 12/12/2013 [6]. Όσον αφορά το Bitcoin, αν και καμία ευρωπαϊκή χώρα δεν έχει χαρακτηρίσει την χρήση του Bitcoin παράνομη, κάποιες χώρες όπως η Γαλλία και το Λουξεμβούργο, απαιτούν την έκδοση κάποιου είδους άδειας για τις επιχειρήσεις.

Αξίζει να σημειωθεί πως σε όλα τα παραπάνω έγγραφα το Bitcoin και γενικά οι κρυπτο-οικονομίες δεν αντιμετωπίζονται ως ένα νέο είδος ψηφιακού χρήματος, αλλά

ως ένα ακόμα εικονικό νόμισμα. Για παράδειγμα το Bitcoin παρουσιάζεται ως το δημοφιλέστερο εικονικό νόμισμα. Επίσης ενώ παρουσιάζονται οι πιθανοί κίνδυνοι που έχει η χρήση των εικονικών νομισμάτων, η ανάλυση και η επιχειρηματολογία πραγματοποιείται κυρίως με αναφορές στα χαρακτηριστικά και τις δυνατότητες των κρυπτο-οικονομιών, χωρίς ωστόσο να αναφέρεται σε κανένα σημείο ο όρος “κρυπτο-οικονομία”.

Χαρακτηριστικά, η ευρωπαϊκή κεντρική τράπεζα το 2012 ορίζει ως εικονική οικονομία “ένα είδος μη πιστοποιημένου (unregulated) ψηφιακού χρήματος, το οποίο εκδίδεται και ελέγχεται από τους δημιουργούς του, και χρησιμοποιείται και είναι δεκτό μεταξύ των μελών μιας συγκεκριμένης εικονικής κοινότητας” [7]. Ορισμός ο οποίος άλλαξε με αντίστοιχο κείμενο της το 2015, καθορίζοντας ως εικονική οικονομία “οποιαδήποτε αντιπροσώπευση αξίας, η οποία δεν εκδίδεται από κάποια κεντρική τράπεζα, πιστωτικό οργανισμό ή οργανισμό e-money, και η οποία σε μερικές περιπτώσεις μπορεί να χρησιμοποιηθεί ως εναλλακτικό χρήμα.” [5] .

Αναφέρεται ωστόσο πως δεν μπορεί να αποκλειστεί το γεγονός, στο μέλλον να δημιουργηθεί μία παρόμοια μορφή νομίσματος, η οποία να είναι ασφαλέστερη, αποδοτικότερη, περισσότερο αξιόπιστη, και η οποία ίσως να είναι ικανή να ανταπεξέλθει στις προσδοκίες του υπάρχοντος τραπεζικού συστήματος.

10 Αποδοχή

Η αναγνώριση, στήριξη, ή η ρύθμιση με την μορφή της επιβολής κανόνων (regulation), παίζει σημαντικό ρόλο στην αποδοχή ενός νομίσματος. Ωστόσο, για να υπάρξει μαζική υιοθέτηση μιας νέας οικονομίας, ή καλύτερα ενός νέου νομίσματος, πρέπει να ικανοποιούνται κάποιες απαραίτητες συνθήκες:

- Το νέο νόμισμα πρέπει να έχει χρησιμότητα, ή καλύτερα, αξία. Για παράδειγμα, βασικό κίνητρο για να αρχίσει κάποιος να χρησιμοποιεί ένα νέο νόμισμα είναι αυτό να έχει μεγαλύτερη χρησιμότητα από αυτό ή αυτά που ήδη χρησιμοποιούνται.

- Η χρήση του πρέπει να είναι ανεμπόδιστη. Δηλαδή να μην υπάρχουν εμπόδια όπως νομικά, κοινωνικά, πολιτικά ή άλλου είδους πιέσεις, τα οποία να αντιτίθενται στην χρήση του. Για παράδειγμα, σε συγκεκριμένες γεωγραφικές περιοχές η χρήση του να συνοδεύεται με τον κίνδυνο νομικών, ηθικών, ή άλλου είδους κυρώσεων.

- Όσον αφορά τις ψηφιακά νομίσματα, θα πρέπει να είναι διαθέσιμη η τεχνολογία που απαιτείται για την χρήση του νομίσματος. Για παράδειγμα, σε γεωγραφικές περιοχές όπου δεν υπάρχει ηλεκτρική κάλυψη είναι σχεδόν απίθανο να ευδοκιμήσει μία ψηφιακή οικονομία.

Δηλαδή για να είναι σε θέση κάποιος να υιοθετήσει ένα νέο ψηφιακό νόμισμα θα πρέπει να έχει κίνητρα, να μην φοβάται τυχόν κυρώσεις και να διαθέτει την κατάλληλη τεχνολογία.

Με βάση τα παραπάνω αν και οι χώρες του ανεπτυγμένου κόσμου διαθέτουν αρκετές από τις απαραίτητες συνθήκες για να πραγματοποιηθεί αποδοχή ενός ψηφιακού ή εναλλακτικού νομίσματος, η χρησιμότητα δεν ικανοποιείται. Θα μπορούσε κάποιος να πει πως αύξηση των ατόμων που προσφέρουν αγαθά ή υπηρεσίες στο διαδίκτυο θα μπορούσε να δημιουργήσει την απαιτούμενη χρησιμότητα. Ωστόσο κάτι τέτοιο δεν φαίνεται να συμβαίνει.

Οπότε μπορούμε να πούμε πως οι χώρες του ανεπτυγμένου κόσμου φαίνεται πως θα είναι οι τελευταίες στις οποίες θα πραγματοποιηθεί αποδοχή του bitcoin ως ψηφιακό ή εναλλακτικό νόμισμα. Το bitcoin είναι περισσότερο ελκυστικό σε αυτούς που δεν έχουν πρόσβαση σε τραπεζικές υπηρεσίες (unbanked population) αλλά και αυτούς που δεν έχουν πρόσβαση στις διεθνείς αγορές. Η έλλειψη ενός συγκεκριμένου κεφαλαίου, οι έλλειψη εγγράφων, ή οι κανονισμοί λειτουργίας, είναι πιθανές αιτίες για την ύπαρξη τέτοιων πληθυσμών. Επίσης ένας μεγάλος πληθυσμός από οικονομικούς μετανάστες ανά τον κόσμο μπορεί να επωφεληθεί από τις χαμηλές τιμές των τελών μεταφοράς στο bitcoin δίκτυο, για να στέλνει χρήματα στις οικογένειές του σε άλλες χώρες.

Από την άλλη όμως το Bitcoin διαθέτει ως χαρακτηριστικό του την ουδετερότητα (neutrality). Χαρακτηριστικό το οποίο είναι ασυνήθιστο να υπάρχει σε νόμισμα. Ουδετερότητα σημαίνει πως ο καθένας είναι σε θέση να υιοθετήσει το νέο νόμισμα ανεξαρτήτου κουλτούρας, γλώσσας, θρησκείας, γεωγραφικής θέσης, πολιτικού ή οικονομικού συστήματος. Ένα άλλο παγκόσμιο σύστημα γνωστό για την ουδετερότητα του είναι το διαδίκτυο. Αξίζει να σημειωθεί πως στο διαδίκτυο η ουδετερότητα δεν αποτελεί απαραίτητο δομικό στοιχείο, ωστόσο υπάρχει. Η ουδετερότητα υπήρχε στα πρώτα στάδια της ανάπτυξης του διαδικτύου, και διατήρησε την αξία του διαδικτύου για αρκετό χρονικό διάστημα, ώστε αυτό να γίνει ευρέως κατανεμημένο, όπως στην μορφή που εμφανίζεται στις μέρες μας. Σήμερα η ουδετερότητα είναι αναπόσπαστο κομμάτι του συστήματος και κάθε επίθεση προς αυτό το χαρακτηριστικό αποτυγχάνει.

Η ενσωματωμένη ουδετερότητα του Bitcoin είναι μία συνθήκη η οποία θα μπορούσε να ενισχύσει την παγκόσμια αποδοχή του, ωστόσο αυτή δεν θα πραγματοποιηθεί αν δεν αντιμετωπιστούν κάποιες από της άλλες προϋποθέσεις. Για παράδειγμα η χρήση του Bitcoin χωρίς την συνεχή πρόσβαση στο δημόσιο αρχείο συναλλαγών (blockchain), ή η μεταφορά αξίας σε περιβάλλοντα με περιορισμένη ή μηδενική ηλεκτρική ή διαδικτυακή κάλυψη. Μία πιθανή λύση για την αποδοχή του Bitcoin σε περιβάλλοντα χωρίς ηλεκτρική κάλυψη, είναι η χρήση paper wallets ή κατάλληλων μεταλλικών νομισμάτων. Ακόμα σε περιοχές στις οποίες υπάρχει περιορισμένη διαδικτυακή κάλυψη, μπορούν να χρησιμοποιηθούν κινητά με ελάχιστες υπολογιστικές δυνατότητες τα οποία να επικοινωνούν μέσω γραπτών μηνυμάτων.

σχήμα. 3: αριθμός των συναλλαγών ανά ημέρα
πηγή: blockchain.info

11 Άλλες εφαρμογές

Το bitcoin έγινε η πρώτη κατανεμημένη κρυπτο-οικονομια το 2009, παρουσιάζοντας μία νέα τεχνολογία στον χώρο των κατανεμημένων συστημάτων και των ψηφιακών οικονομιών, τον μηχανισμό “decentralized consensus mechanism”. Αυτή η εφεύρεση, η οποία αποτελεί την καρδιά του bitcoin, δημιούργησε, τα χρόνια που ακολούθησαν, ένα κύμα από καινοτομίες στις ψηφιακές οικονομίες, στα κατανεμημένα συστήματα, στα συστήματα ηλεκτρονικής ψηφοφορίας, και τις συμβάσεις (contracts).

σχήμα. 4: το bitcoin project στο GitHub
πηγή: https://github.com/bitcoin/bitcoin

Το bitcoin υπάρχει ως κώδικας ανοιχτού λογισμικού, και έχει χρησιμοποιηθεί ως η βάση για πολλά άλλα projects. Η δημοφιλέστερη μορφή λογισμικού, που δημιουργείται με βάση τον κώδικα του bitcoin, είναι κάποια άλλη κρυπτο-οικονομία (alt coins). Το πιο γνωστό από τα εναλλακτικά κρυπτο-νομίσματα είναι το Litecoin. Το Litecoin χρησιμοποιει ως αλγόριθμο απόδειξης της εργασίας (proof of work), τον scrypt, ο οποίος σχεδιάστηκε αρχικά για να χρησιμοποιηθεί ως brute-force resistance τεχνική. Το Litecoin εκτός από τον scrypt υλοποιεί επίσης και ταχύτερη παραγωγή blocks, 2.5 λεπτά αντί των 10 λεπτών που υλοποιεί το bitcoin.

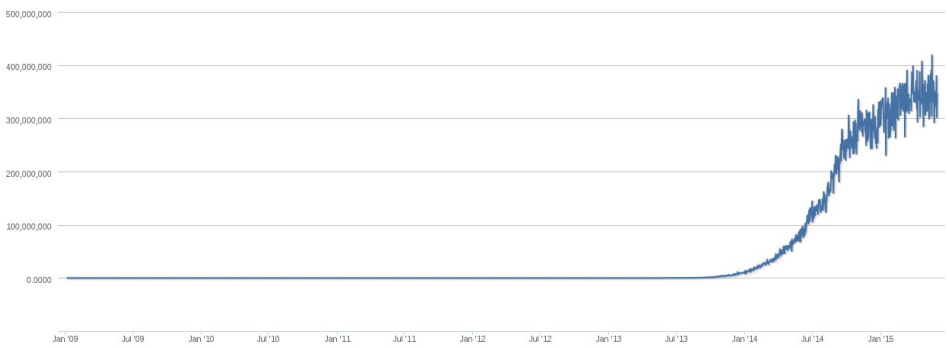
Εκτός από τις κρυπτο-οικονομίες, υπάρχει και ένα πλήθος πρωτοκόλλων τα οποία υλοποιούνται πάνω στην αλυσίδα των blocks του Bitcoin. Τέτοιες εφαρμογές χαρακτηρίζονται ως meta coins ή blockchain apps, διότι χρησιμοποιούν την αλυσίδα

των blocks του Bitcoin ως πλατφόρμα εφαρμογής. Χαρακτηριστικό παράδειγμα είναι τα colored coins, τα οποία αναθέτουν επιπλέον πληροφορίες σε bitcoin χρηματικά ποσά, ή πιο περιγραφικά, χρωματίζουν νομίσματα, επαναπροσδιορίζοντας με αυτό τον τρόπο τον σκοπό τους. Έτσι ένα χρωματισμένο νόμισμα εξυπηρετεί δύο σκοπούς. Από την μία είναι ένα νόμισμα με συγκεκριμένη αγοραστική δύναμη, και από την άλλη διαθέτει την αξία του "χρώματος" που του έχει δοθεί και η οποία καθορίζεται από τον σκοπό του "χρωματισμού".

Εκτός από τα alt coins τα οποία είναι παραλλαγές του bitcoin, και τα blockchain apps τα οποία είναι εφαρμογές που τρέχουν πάνω σε ήδη υπάρχουσες blockchains, υπάρχουν και εναλλακτικές blockchain υλοποιήσεις (alt chains). Τα alt chains υλοποιούν έναν αλγόριθμο συμφωνίας (consensus) και ένα κατανεμημένο αρχείο καταγραφής (distributed ledger), ως μία πλατφόρμα για συμβάσεις (contracts), name registration, και άλλες εφαρμογές. Παραδείγματα τέτοιων εφαρμογών είναι το Namecoin, το οποίο λειτουργεί κυρίως ως domain name υπηρεσία (DNS) για το .bit domain, το Bitmessage, το οποίο υλοποιεί μία κατανεμημένη υπηρεσία ανταλλαγής μηνυμάτων με ασφαλή τρόπο, και το Etherium, το οποίο μία Turing-complete πλατφόρμα για την σύναψη, επεξεργασία και εκτέλεση δυμβάσεων (contracts).Το Etherium καταγράφει τις συμβάσεις στην αλύσίδα των blocks σε μία χαμηλού επιπέδου, byte code-like, Turing-complete γλώσσα. Ουσιαστικά οι σύμβασεις είναι πρόγραμματα τα οποία τρέχουν σε κάθε κόμβο στο δίκτυο του Etherium, και συμπεριφέρονται ως κατανεμημένοι, αυτόνομοι software agents.

11.1 GridCoin

Το πρόβλημα με το σχήμα απόδειξης της εργασίας (proof of work), όπως αυτό χρησιμοποιείται στο Bitcoin και σε πολλές άλλες κρυπτο-οικονομιες, βρίσκεται στο γεγονός πως είναι πολύ "σπάταλο". Το bitcoin δίκτυο χρησιμοποιεί τον αλγόριθμο sha-256 στο proof of work σχήμα του για την διατήρηση της ασφάλειας της αλυσίδας των blocks (blockchain). Κάποιος θα μπορούσε να ισχυριστεί πως τεράστια ποσά ενέργειας απαιτούνται για την πραγματοποίηση υπολογισμών οι οποίοι δεν παράγουν κάποια χρήσιμα αποτελέσματα, και υπάρχουν μόνο για να αποδεικνύουν πως οι miners έκαναν κάτι δαπανηρό.



σχήμα. 5: εκτιμώμενη υπολογιστική ισχύς στο bitcoin δίκτυο (hash rate)
πηγή: blockchain.info

Με βάση αυτό το σκεπτικό άτομα στον τομέα των κρυπτο-οικονομιων προσπάθησαν να εφεύρουν λιγότερο δαπανηρές εναλλακτικές, και σε αυτήν την κατεύθυνση έχουν δημιουργηθεί αρκετά διαφορετικά σχήματα. Αρκετά από αυτά ενώ υλοποιούν ένα proof of work σχήμα, επιδιώκουν να το χρησιμοποιούν ώστε να ωθούν τους χρήστες τους να πραγματοποιούν κάποιου είδους χρήσιμης εργασίας, αντί των άσκοπων υπολογισμών. Για παράδειγμα, το prime coin [8], απαιτεί από τους miners την αναζήτηση πρώτων αριθμών, μία εργασία η οποία είναι χρήσιμη στον τομέα των μαθηματικών. Ωστόσο, υπάρχουν και νέα σχήματα. Πιθανόν το πιο δημοφιλές από αυτά είναι το “proof of stake”, το οποίο απλά απαιτεί να διατηρείς στην κατοχή σου έναν αριθμό νομισμάτων (στοίχημα) σε αντίθεση με το proof of work σχήμα το οποίο απαιτεί να πραγματοποιείς ένα ποσοστό εργασίας. Η ιδέα πάνω στην οποία βασίζεται το proof of stake σχήμα, είναι πως οποιοσδήποτε διαθέτει αρκετά νομίσματα στην κατοχή ώστε να επιτεθεί αποτελεσματικά στο δίκτυο θα αποθαρρυνόταν διότι στην ουσία θα ήταν σαν να πραγματοποιούσε μία επίθεση στον εαυτό του. Και αυτό διότι η κατοχή ενός μεγάλου ποσού νομισμάτων ισοδυναμεί με ένα μεγάλο στοίχημα στην επιτυχία του δικτύου. Οπότε μία επίθεση στο δίκτυο θα ήταν κάτι δαπανηρό και ταυτόχρονα μη λογικό.

Ένα νόμισμα το οποίο υλοποιεί αυτό το σχήμα είναι το Gricoin [9]. Το Gridcoin είναι επίσης μία κατανεμημένη, ανοιχτού κώδικα, κρυπτο-οικονομία. Το Gridcoin παρέχει οφέλη στην ανθρωπότητα μέσω συνεισφορών στην υπολογιστική έρευνα. Είναι η μόνη κρυπτο-οικονομία η οποία ανταμείβει άτομα για την διάθεση των πόρων τους, με ένα ενεργειακά αποδοτικό τρόπο, χωρίς την ανάγκη για μία κεντρική αρχή που να διανέμει τις ανταμοιβές. Όπως αναφέρθηκε το Gridcoin βασίζεται στο proof of stake σχήμα, το οποίο είναι ενεργειακά αποδοτικό, και δίνει την δυνατότητα στους mires να διαθέτουν τους υπολογιστικούς τους πόρους σε επιστημονικούς υπολογισμούς, παρά να διασφαλίζουν την αλυσίδα των blocks (blockchain). Είναι το πρώτο blockchain πρωτόκολλο το οποίο παρέχει έναν αλγόριθμο εργασίας ο οποίος ανταμείβει, και αποδεικνύει κρυπτογραφικά, λύσεις σε BOINC εργασίες (Berkley Open Infrastructure for Network Computing) [10]. Το BOINC είναι ένα εθελοντικό υπολογιστικό πλέγμα (grid) ανοιχτού κώδικα το οποίο συνδυάζει την υπολογιστική ισχύ όλων των χρηστών του για επιστημονικούς ερευνητικούς σκοπούς. Είναι δωρεάν και εκμεταλλεύεται τους αχρησιμοποίητους υπολογιστικούς κύκλους επεξεργαστών και συστημάτων γραφικών,

για την ενίσχυση της ερευνητικής διαδικασίας στην αντιμετώπιση ασθενειών, στην εξερεύνηση των μυστηρίων του σύμπαντος, και άλλα.

Το Gridcoin αποζημιώνει τους miners για την συμμετοχή τους σε BOINC projects τα οποία ίσως οδηγήσουν σε ανακαλύψεις στην ιατρική, την βιολογία, τα μαθηματικά, την αστρονομία, και με αυτό τον τρόπο παρέχει πραγματικά οφέλη για την ανθρωπότητα.

Το Gridcoin διαφέρει από τις άλλες επιστημονικές κρυπτο-οικονομίες ως προς την δυνατότητά του να υποστηρίζει πολλά διαφορετικά επιστημονικά project, και περιορίζεται μόνο από το τι προωθείται αυτήν την στιγμή από το δίκτυο BOINC.

12 Επίλογος

Ο μηχανισμός συμφωνίας σε κατανεμημένα περιβάλλοντα, έχοντας ως δημοφιλή εφαρμογή του το Bitcoin, δείχνει πως είναι μία στιβαρή τεχνολογία, η οποία έχει να προσφέρει ενδιαφέρουσες εφαρμογές στο μέλλον. Καθώς η φρενίτιδα των εμπλεκομένων στις χρηματιστηριακές αγορές (stock markets) για τις κρυπτο-οικονομίες υποχωρεί, όπως άλλωστε δείχνει και η πρώτη των ισοτιμιών του Bitcoin, η τεχνολογία κερδίζει το χρόνο που χρειάζεται για να αναπτυχθεί και να ωριμάσει στην αντίληψη της κοινωνίας.

13 Αναφορές

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org. October 2008.

[2] Mastering Bitcoin Unlocking Digital Cryptocurrencies, Andreas M.Antonopoulos, O'Reilly Media, December 2014

[3] Zerocoin Project, http://zerocoin.org

[4] Virtual currency schemes – a further analysis, European Central Bank, February 2015, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

[5] Ενημέρωση για τη χρήση εικονικών νομισμάτων, Τράπεζα της Ελλάδος, 11/02/2014, http://www.bankofgreece.gr/Pages/el/Bank/News/Announcements/DispItem.aspx?Item_ID=4517&List_ID=1af869f3-57fb-4de6-b9ae-bdfd83c66c95&Filter_by=AN

[6] Προειδοποίηση προς τους καταναλωτές για τα εικονικά νομίσματα, European Banking Autority, 12/12/2013, http://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_EL_TRA_eg.pdf

[7] Virtual currency schemes, European Central Bank, 0ctober 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[8] Primecoin, http://primecoin.io/

[9] GridCoin, http://www.gridcoin.us/

[10] Berkley Open Infrastructure for Network Computing, https://boinc.berkeley.edu/