



**Κρυπτονόμισμα : Ένα αναδυόμενο εργαλείο οικονομικής ελευθερίας**

Ο Χάγιεκ αναφέρει στο *Constitution of Liberty* ότι ένας από τους πιο αποτελεσματικούς τρόπους για την διασφάλιση της ατομικής ελευθερίας είναι να υπάρχουν θεσμοί οι οποίοι θα απαγορεύουν τους περιορισμούς σε οποιαδήποτε χρηματική συναλλαγή. Ο δημιουργός (ή οι δημιουργοί) του bitcoin ίσως είχαν παρόμοιες σκέψεις όταν έγραφαν τον κώδικα για το λογισμικό τους.

**Ανταγωνισμός νομισμάτων: η εφαρμογή της θεωρίας του Χάγιεκ.**

**1) Τι είναι το κρυπτονόμισμα**

Η λέξη κρυπτονόμισμα (cryptocurrency) περιγράφηκε πρώτη φορά το 1998 από τον Wei Dai στη λίστα αλληλογραφίας των cypherpunks, υποστηρίζοντας την ιδέα μιας νέας μορφής χρήματος η οποία κάνει χρήση κρυπτογραφίας για να ελέγξει τη δημιουργία και τις συναλλαγές του, παρά μια κεντρική αρχή. 10 χρόνια αργότερα ο Satoshi Nakamoto θα δημοσιεύσει στην ίδια λίστα αλληλογραφίας τις πρώτες προδιαγραφές του bitcoin στο περίφημο πλέον white paper που λίγο αργότερα κατατέθηκε και δημόσια. Αυτό που πιστεύω πως ήθελε(αν) να πετύχει στο εγχείρημα του ήταν η δημιουργία ενός χρηματικού εργαλείου το οποίο θα είναι πολύ **ανθεκτικό στη λογοκρισία**, δηλαδή, ότι θα είναι απαραβίαστο από τρίτους, και διαθέσιμο σε οποιονδήποτε έχει πρόσβαση στο διαδίκτυο.

Το bitcoin έχει πλέον επικρατήσει ως το πρώτο κρυπτονόμισμα σε αξία και αναγνωρισιμότητα, όχι όμως μέσω ανταγωνισμού, αλλά κυρίως επειδή ήταν το πρώτο που κατάφερε να υπερβεί προβλήματα που είχαν αντιμετωπίσει προηγούμενες προσπάθειες, και επίσης λόγω της χρονικής περιόδου που δημιουργήθηκε, στα τέλη του Οκτωβρίου του 2008. Από τότε η κοινότητα του bitcoin μεγάλωσε εκθετικά, με πολλούς προγραμματιστές που ασχολούνται με το bitcoin.

Για την λειτουργία του, το bitcoin χρησιμοποιεί ένα αποκεντρωμένο δίκτυο υπολογιστών, οι οποίοι επαληθεύουν μέσω μαθηματικών πράξεων τις συναλλαγές που ζητούν οι χρήστες του. Το δίκτυο αυτό ελέγχεται από τους ίδιους τους χρήστες καθώς λειτουργεί με βάση consensus, δηλαδή, δεν μπορεί κάποιος προγραμματιστής να εξαναγκάσει καμία αλλαγή στο πρωτόκολλο, διότι όλοι οι χρήστες είναι ελεύθεροι να ελέγξουν τον ανοικτό κώδικα του και να επιλέξουν την έκδοση του λογισμικού που χρησιμοποιούν. Για να διατηρηθεί η συμβατότητα, όλοι οι χρήστες πρέπει να χρησιμοποιούν το λογισμικό που υπακούει στους ίδιους κανόνες.

Όλες οι συναλλαγές που έχει επεξεργαστεί το δίκτυο καταγράφονται σε ένα μοιρασμένο δημόσιο λογιστικό βιβλίο, το επονομαζόμενο blockchain. Το blockchain επιτρέπει στον χρήστη να εξακριβώνει την αυθεντικότητα της κάθε συναλλαγής, καθώς αυτές προστατεύονται από ψηφιακές υπογραφές για τον κάθε χρήστη. Επιπλέον δίνεται η δυνατότητα και κυρίως, το κίνητρο, σε οποιονδήποτε χρήστη να επεξεργαστεί συναλλαγές που χρησιμοποιούν την υπολογιστική ισχύ εξειδικευμένου εξοπλισμού και να κερδίζει ανταμοιβή για την υπηρεσία αυτή, αυτό είναι το λεγόμενο mining (εξόρυξη). Το mining εκτός του να εξακριβώνει συναλλαγές και να εκδίδει νέο νόμισμα, συμβάλλει και στην ασφάλεια του δικτύου. Όσο μεγαλύτερη υπολογιστική δύναμη έχει συνολικά το δίκτυο, τόσο λιγότερο ευάλωτο είναι σε επιθέσεις και κακόβουλους χειρισμούς. \*\*\*Το δίκτυο, αρχικά αποτελούμενο από απλούς προσωπικούς υπολογιστές χρηστών μεγάλωσε και μεγαλώνει ακόμα με ταχύτατους ρυθμούς δίνοντας ώθηση σε μια πολύ ανταγωνιστική αγορά εξειδικευμένου εξοπλισμού και την ανάπτυξη μεγάλων "ορυχείων" όπως αυτά που βλέπετε στις φωτογραφίες. \*\*\* Αυτή τη στιγμή, το δίκτυο του bitcoin έχει την μεγαλύτερη συνδυασμένη υπολογιστική δύναμη από τα 500 μεγαλύτερα supercomputers του πλανήτη αν τα βάλουμε όλα μαζί. \*\*\* Αυτή η υπολογιστική δύναμη είναι που εξασφαλίζει το δίκτυο μέσω της διαδικασίας που λέγεται proof of work, η οποία ουσιαστικά αποδεικνύει ότι χρησιμοποιήθηκαν φυσικοί πόροι οι οποίοι μέσω ενός αλγόριθμου μετατράπηκαν σε ένα κομμάτι δεδομένων. Το proof of work έχει την ιδιότητα να είναι χρονοβόρο και δαπανηρό για την δημιουργία του, αλλά είναι εύκολα επαληθεύσιμο από το υπόλοιπο δίκτυο. Το κόστος της εξασφάλισης του δικτύου λοιπόν αντικατοπτρίζεται στο ποσό που δαπανάται ετήσια για το ηλεκτρικό ρεύμα που χρειάζονται τα "ορυχεία" για να λειτουργήσουν, το οποίο εκτιμάται σε μερικές εκατοντάδες εκατομμύρια δολάρια. Για να επιτεθεί κάποιος στο δίκτυο λοιπόν, θα πρέπει να δαπανήσει επίσης εκατοντάδες εκατομμύρια δολάρια.

## 2) **Αλλά κρυπτονομίσματα**

\*\*\*Λόγω της ανοικτής φύσης του λογισμικού του bitcoin (open source), επιτράπη σε πολλούς προγραμματιστές να πειραματιστούν με τον κώδικα και να τον τροποποιήσουν (forking) φτιάχνοντας έτσι νέα κρυπτονομίσματα, τα οποία περιέχουν βελτιώσεις ή/και προσθήκες όπως πιο γρήγορες συναλλαγές, μεγαλύτερη ανωνυμία κ.ά. Τα περισσότερα από αυτά τα νομίσματα έχουν βέβαια κακό τέλος, καθώς οποιοσδήποτε με βασικές γνώσεις προγραμματισμού μπορεί πολύ εύκολα να φτιάξει ένα καινούργιο νόμισμα. Αυτό οδήγησε σε μια έκρηξη δημιουργίας νέων κρυπτονομισμάτων, ειδικά την μετά τα τέλη 2013, όπου το bitcoin άρχισε να αποκτά

ιδιαίτερη προβολή λόγω της ραγδαίας αύξησης της τιμής του. Τα λίγα κρυπτονομίσματα που είχαν ουσιαστικές αλλαγές και χρήσιμες καινοτομίες διέπρεψαν και ανέβηκαν σε αξία και όσα είχαν άχρηστες ή καθαρά κερδοσκοπικές για τους δημιουργούς τους λειτουργίες αργά ή γρήγορα εξαφανίσθηκαν. Μέσω αυτής της διαδικασίας δημιουργήθηκε μια παγκόσμια, πολύ ανταγωνιστική και πλήρως ελεύθερη αγορά όπου το κάθε κρυπτονόμισμα ψάχνει τρόπους και μεθόδους για να ελκύσει επενδυτές και χρήστες.

\*\*\*Αυτή η αγορά μετράει αυτή τη στιγμή κοντά στα 1000 διαφορετικά κρυπτονομίσματα σε κυκλοφορία με συνολική χρημ/κή αξία γύρω στα 8 δις. Ευρώ, εκ των οποίων τα 3 πρώτα αντιπροσωπεύουν το 93% με το bitcoin μόνο του να αντιπροσωπεύει το 78%. Στο Denationalisation of Money, ο Hayek αναφέρει ότι σε μια ελεύθερη αγορά νομισμάτων, η αγορά θα συγκλίνει προς έναν πολύ περιορισμένο αριθμό νομισμάτων, ή ακόμα και σε ένα, το οποίο και βλέπουμε να συμβαίνει εδώ και καιρό στην αγορά κρυπτονομισμάτων.

Τα πιο συνηθισμένα χαρακτηριστικά που έχω παρατηρήσει στα κρυπτονομίσματα που παρακολουθώ από το 2012 είναι τα εξής:

- Χωρίς κεντρική αρχή ελέγχου ή επιβεβαίωσης των συναλλαγών.
- Δυνατότητα χρήσης χωρίς να υποβάλλονται προσωπικά στοιχεία.
- Δυνατότητα χρήσης από οποιονδήποτε, οπουδήποτε
- Δυνατότητα αποστολής πολύ μικρών αλλά και πολύ μεγάλων συναλλαγών με πολύ μικρό κόστος
- Χρήση της τεχνολογίας Blockchain.
- Δυνατότητα συμμετοχής σε οποιονδήποτε στην έκδοση νομίσματος (mining).
- Περιορισμός και γνωστοποίηση του χρηματικού αποθέματος (money supply).

- Ανώνυμες ή/και μη ανιχνεύσιμες συναλλαγές.
- Χρήση ανοικτού κώδικα
- Προσπάθεια βελτίωσης σε κάποιο/πολλούς τομείς στον/στους οποίους υστερεί το bitcoin.

Σε τι υστερεί το bitcoin

- Αργές συναλλαγές για καθημερινή χρήση. (μέσος όρος ~10 λεπτά)
- Προσωρινό όριο 7 συναλλαγών το δευτερόλεπτο (πρόβλημα επεκτασιμότητας)
- Η άγνωστη ταυτότητα του δημιουργού του
- Ιστορικό χρήσης του νομίσματος για παράνομες αγορές/χρήσεις

### **Αξιοσημείωτα κρυπτονομίσματα:**

**Litecoin:** ένα από τα πρώτα κρυπτονομίσματα που κατάφεραν να κερδίσουν μεγάλο κοινό και επενδυτές, χάρη στις πολύ πιο γρήγορες συναλλαγές (2 λεπτά αντί για 10). Έχει συχνά αναφερθεί ως το "ασήμι" σε σχέση με το bitcoin που συχνά παρομοιάζεται με τον χρυσό.

Το **Ripple** εκτός από κρυπτονομίσμα είναι και μία ολοκληρωμένη πλατφόρμα συναλλαγών που έχει και αυτή ως βάση την τεχνολογία blockchain και το αποκεντρωμένο μοντέλο με την διαφορά ότι ο χρήστης έχει τη δυνατότητα να επιλέξει σε τι μορφή θα είναι τα κεφάλαια που θα διαχειρίζεται, έχοντας να επιλέξει ανάμεσα σε Ευρώ, Δολάρια, χρυσό, bitcoin και Ripple ανάμεσα σε άλλα.

Το **MaidSafe** είναι μια προσπάθεια δημιουργίας ενός οικοσυστήματος όπου οι χρήστες έχουν τη δυνατότητα να διαθέσουν υπολογιστικούς πόρους (όπως αποθηκευτικό χώρο, υπολογιστική δύναμη, ευρηζωνηκότητα (bandwidth)) τους

οποίους δεν χρησιμοποιούν εις αντάλλαγμα πληρωμής από άλλους χρήστες οι οποίοι χρειάζονται αυτούς τους πόρους.

Το **Monero** έχει ως πρώτη προτεραιότητα την ιδιοκτητικότητα και την ανωνυμία. Χρησιμοποιώντας μια πολύ εξειδικευμένη ιδιότητα της κρυπτογραφίας (ring signatures), που καθιστά τις συναλλαγές σχεδόν απίθανο να ανιχνευθούν

Το **HayekGold** είναι ένα κρυπτονόμισμα που έχει ως βάση τον χρυσό και κάθε του μονάδα αντιστοιχεί στην αξία ενός γραμμαρίου χρυσού, ο οποίος είναι αποθηκευμένος σε χώρο της εταιρίας που εκδίδει νόμισμα μέσω της πλατφόρμας Counterparty.

Το **Ethereum** είναι το πιο γρήγορα αναπτυσσόμενο κρυπτονόμισμα τον τελευταίο καιρό και σίγουρα ότι πιο ενδιαφέρον έχουμε δει από τη δημιουργία του bitcoin και μετά. Πρόκειται περί μιας προγραμματιστικής πλατφόρμας η οποία συμπεριλαμβάνει μέσα της και το κρυπτονόμισμα Ether. Η πλατφόρμα έχει την δική της γλώσσα προγραμματισμού και επιτρέπει στους χρήστες να φτιάξουν εφαρμογές πάνω στο πρωτόκολλο, καθώς και να κάνει χρήση των λεγόμενων smart contracts, συμβόλαια, τα οποία εκτελούν αυτόματα ότι είναι προγραμματισμένα να κάνουν, από τις μεριές που το υπογράφουν. Είναι δύσκολο να εξηγήσει κανείς τι ακριβώς είναι το Ethereum λόγω του ότι είναι ένα τόσο νέο σύστημα που έχει απεριόριστες εφαρμογές οι οποίες δεν έχουν βρεθεί ακόμα αφού ακόμα και οι δημιουργοί του, που συμπεριλαμβάνουν γνωστές φυσιογνωμίες στον κόσμο της πληροφορικής, δυσκολεύονται να το περιγράψουν.

Παρ' όλες τις πολλές και αξιόλογες προσπάθειες, το Bitcoin συνεχίζει να επικρατεί στον τομέα, κυρίως χάρη στο αρκετά γνωστό πλέον όνομα που έχει κάνει και την αξιοπιστία που έχει δείξει σαν λογισμικό, και σαν δίκτυο.

\*\*\*Η μεταβλητότητα της τιμής του Bitcoin έχει περιοριστεί πάρα πολύ σε σχέση με το παρελθόν, με το 2015 να σημειώνεται ως η χρονιά με τη μικρότερη μεταβλητότητα στην ιστορία του νομίσματος. Το γεγονός αυτό το κάνει ακόμα πιο ελκυστικό ως μέσο αποθήκευσης αξίας σε σχέση με άλλα, πολύ μεταβλητά κρυπτονομίσματα και μη.

### 3) Χρήση

Οι έμποροι και οι επιχειρήσεις οι οποίοι δέχονται πληρωμές σε bitcoin, παρότι γίνονται όλο και περισσότεροι ανά τον κόσμο είναι λίγοι σε σχέση με το σύνολο. Αυτό όμως δεν σημαίνει ότι θα παραμείνει έτσι.

Όπως αναφέρουν στο βιβλίο "Cryptocurrency" οι αρθρογράφοι της WSJ Paul Vigna και Michael Casey, η αληθινή δύναμη του bitcoin ίσως έγκειται στα 2.5 δισεκατομμύρια ενήλικες του κόσμου οι οποίοι δεν έχουν τραπεζικό λογαριασμό. 2.5 δισεκατομμύρια ενήλικες σημαίνει ότι συνολικά γύρω στα 5 δισεκατομμύρια άνθρωποι ανήκουν σε νοικοκυριά τα οποία είναι τελείως αποκομμένα από το χρηματοπιστωτικό σύστημα το οποίο εμάς μας θεωρεί δεδομένους. Οι άνθρωποι αυτοί δεν μπορούν να αρχίσουν έναν καταθετικό λογαριασμό. Δεν έχουν τρεχούμενο λογαριασμό. Μένουν σε μέρη όπου οι τράπεζες δεν θέλουν να πάνε, και γι' αυτό δεν μπορούν να συμμετάσχουν σε αυτό που ονομάζουμε παγκόσμια οικονομία. Οι τράπεζες δεν πάνε εκεί, είτε επειδή δεν υπάρχουν οι υποδομές ή η ασφάλεια που χρειάζεται για να ανοίξει κάποιο φυσικό κατάστημα, είτε επειδή τα κέρδη που θα αποφέρουν θα είναι πολύ μικρά για να δικαιολογήσουν το κόστος, αλλά κυρίως, δεν πάνε εκεί λόγω της έλλειψης ή ανυπαρξίας νομικών θεσμών και μη ανεπτυγμένων ιδιοκτησιακών τίτλων, κάτι το οποίο έχει γνωστοποιήσει και ο Hernando de Soto εδώ και αρκετό καιρό.

Το bitcoin, όπως ξέρουμε, δεν το νοιάζει ποιος είσαι. Δεν το ενδιαφέρει πόσο θέλει κανείς να ξοδέψει ή να αποταμιεύσει. Χρειάζεται μια ηλεκτρονική συσκευή και σύνδεση στο ίντερνετ, και άμεσα μπορεί κάποιος να λάβει ή να αποστείλει χρήματα οπουδήποτε. Η συμπερίληψη ενός τρίτου της ανθρωπότητας στο τραπεζικό σύστημα μπορεί να δημιουργήσει τεράστιες ευκαιρίες για την παγκόσμια οικονομία καθώς και στην καταπολέμηση της φτώχειας. Έχουμε ήδη δει τις τεράστιες επιπτώσεις της παγκοσμιοποίησης και της ψηφιοποίησης χωρίς να μετασχηματιστεί το χρηματοπιστωτικό σύστημα. Μπορεί αρκετοί στις πλούσιες χώρες που είδαν εργοστάσια να κλείνουν και άλλες δουλειές να γίνονται outsourced αλλά, σε μάκρο επίπεδο είναι δύσκολο να αγνοήσει κανείς τις θετικές επιπτώσεις της παγκοσμιοποίησης. Μεταξύ του 1990 και του 2010, το ποσοστό του πληθυσμού που ζει με λιγότερα από \$1.25 δολάρια τη μέρα μειώθηκε από το 43,1% στο 20,6%. Στο ίδιο διάστημα το προσδόκιμο ζωής ανέβηκε κατά 7 χρόνια και η παιδική θνησιμότητα έπεσε στο μισό. Όλο αυτό δεν έγινε από κάποια φιλανθρωπία των πλούσιων χωρών προς τις φτωχές, αλλά μέσω της ανάπτυξης της παγκόσμιας αγοράς.

Εννοείται πως το bitcoin δεν είναι το μόνο εργαλείο για την οικονομική ενσωμάτωση, αλλά σε ένα περιβάλλον όπου ένα κινητό τηλέφωνο με σύνδεση στο διαδίκτυο είναι πιο εύκολο να αποκτηθεί από ποτέ, ακόμα και σε απομακρυσμένες περιοχές της Αφρικής\*\*\*, μπορεί να αναδειχτεί ως ένα πάρα πολύ χρήσιμο εργαλείο. Η τεχνολογία είναι όλο και πιο εύκολα προσβάσιμη, καθώς η εφαρμογή Bitcoin γίνεται όλο και πιο εύκολη στη χρήση και τα smartphones γίνονται όλο και πιο φθηνά.

Όπως κάθε άλλη μορφή χρήματος, το κρυπτονομισμα χρησιμοποιείται και έχει χρησιμοποιηθεί για νόμιμους όσο και για παράνομους σκοπούς. Το γεγονός αυτό ήταν και είναι ακόμα ένας λόγος για τους οποίους έχει αποκτήσει "κακό όνομα" για κάποιους. Όμως, ο σχεδιασμός της τεχνολογίας πίσω από το bitcoin θα μπορούσε να λειτουργήσει ως προστασία έναντι πολλών μορφών οικονομικού εγκλήματος. Λόγω της δημόσιας διαθεσιμότητας όλων των συναλλαγών, οι εγκληματολογικές έρευνες μπορούν να διεξαχθούν πολύ πιο εύκολα από ότι αν η συναλλαγή είχε γίνει με συμβατικά χρήματα. Μάλιστα, τα τελευταία χρόνια παρατηρείται ένα αρκετά

μεγάλο ενδιαφέρον εκ μέρους πολλών κεντρικών-και μη-τραπεζών οι οποίες λειτουργούν πιλοτικά προγράμματα, καθώς θέλουν να υιοθετήσουν την τεχνολογία blockchain.

\*\*\*Στην Ελλάδα, το ενδιαφέρον για το bitcoin και τα κρυπτονομίσματα εκδηλώθηκε ιδιαίτερα το 2015, την περίοδο που η κυβέρνηση ανήγγειλε τους περιορισμούς κεφαλαίου και το κλείσιμο των τραπεζών. Αρκετές εταιρίες σχετικές με το bitcoin δήλωσαν την προθυμία τους να επεκταθούν στην Ελλάδα από τότε αλλά απ' όσο γνωρίζω από αυτά λίγα γίνανε πράξη.

Τα μεγαλύτερα προβλήματα που αντιμετωπίζει το bitcoin στην πιο μαζική υιοθέτηση από το κοινό είναι τα εξής:

- Έλλειψη χρηστών, εμπόρων.

Το κυριότερο για να υπάρξει το απαιτούμενο "network effect" για την ανάπτυξη οποιαδήποτε τεχνολογίας ευρείας χρήσης.

- Έλλειψη νομοθεσίας.

Συνήθως είναι ανύπαρκτη. Το οποίο το καθιστά αποτρεπτικό για μεγάλους και "θεσμικούς" επενδυτές.

- Υψηλά μεταβλητές τιμές.

Αν και όπως είδαμε αυτό το πρόβλημα είναι σε σταδιακή ύφεση εδώ και αρκετό καιρό

Συνοπτικά, πιστεύω πως είναι μία τεχνολογία που βρίσκεται ακόμα στα αρχικά της στάδια, λίγος κόσμος ξέρει περί τίνος πρόκειται και είναι δύσκολο να γίνουν εικασίες για τι μπορεί να προκύψει, ιδιαίτερα αν projects σαν το Ethereum συνεχίσουν να κάνουν επιτυχίες. Τα κρυπτονομίσματα προσφέρουν έναν τρομακτικό αριθμό δυνατοτήτων τις οποίες ούτε τις φανταζόμασταν πριν μία δεκαετία ή ακόμα και πριν από 5 χρόνια. Ο ρυθμός ανάπτυξης είναι μεγάλος σε επίπεδο λογισμικού και καινοτομιών αλλά σίγουρα όχι τόσο μεγάλος σε επίπεδο υιοθεσίας από το κοινό. Ο περισσότερος κόσμος έχει μάθει πως τα χρήματα είναι κάτι το οποίο μόνο το κράτος μπορεί να εκδώσει και να ελέγξει, και γι' αυτό εκ πρώτης όψεως, δύσκολα θα πειστεί κανείς να μετατρέψει, εθελοντικά, τα "αληθινά" του χρήματα σε κάτι το οποίο δεν έχει καμία σχέση με αυτό που ήξερε μέχρι σήμερα.