

# Το κρυπτονόμισμα Bitcoin θα είναι το νόμισμα της νέας ψηφιακής εποχής;



Των Κ.Κ. Νικολάου Φίλιππα,  
Καθηγητή Χρηματοοικονομικής  
του Τμήματος Ο.Δ.Ε.  
του Πανεπιστημίου Πειραιώς



Μάριου Ρούκη,  
Υποψήφιου Διδάκτορος  
του Τμήματος Ο.Δ.Ε.  
του Πανεπιστημίου Πειραιώς



Στο άρθρο αυτό επιχειρείται για πρώτη φορά στην Ελλάδα η ολοκληρωμένη παρουσίαση του κρυπτονομίσματος Bitcoin, εντοπίζοντας τα βασικά χαρακτηριστικά του, αλλά και άγνωστες πτυχές του, όπως τη διαδικασία της εξόρυξης. Στη συνέχεια παρουσιάζεται η διαχρονική πορεία του, αλλά και τα κυριότερα γεγονότα που επηρέασαν και διαμόρφωσαν την τιμή του. Παρά τις προφανείς αδυναμίες του, όλες οι μελέτες συγκλίνουν ότι μέχρι το 2025 τα παραδοσιακά νομίσματα θα υποχωρήσουν και τα ψηφιακά νομίσματα θα κυριαρχήσουν.

## I. Εισαγωγή

Τα κρυπτονομίσματα είναι μια μορφή ηλεκτρονικού χρήματος που χρησιμοποιούνται περιορισμένα μέχρι στιγμής ως μέσο συναλλαγών, αλλά φαίνεται ότι θα αποτελέσουν το κυρίαρχο νόμισμα στην μελλοντική παγκόσμια ψηφιακή οικονομία.

Τα κρυπτονομίσματα έχουν παρόμοιες ιδιότητες με τα παραδοσιακά νομίσματα, αλλά διαφοροποιούνται επειδή χρησιμοποιούν κρυπτογραφία για την κωδικοποίηση και απόκρυψη πληροφοριών.<sup>1</sup> Κρυπτογραφία είναι το διεπιστημονικό γνωστικό πεδίο το οποίο ασχολείται με τεχνικές κρυπτογράφησης και αποκρυπτογράφησης δεδομένων. Η κρυπτογράφηση δεδομένων γίνεται με χρήση των μαθηματικών και είναι μια πολύ σημαντική λειτουργία αφού χάρη σε αυτή διατηρείται το προσωπικό απόρρητο του κάθε χρήστη και αποφεύγονται οι ηλεκτρονικές κλοπές από επιθέσεις των hackers.

Η χρησιμοποίηση κρυπτονομισμάτων στοιχίζει λιγότερο από τα παραδοσιακά νομίσματα, ενισχύει και τονώνει τη διαφάνεια των συναλλαγών<sup>2</sup> (αφού τα πάντα είναι δημόσια και διαθέσιμα στην αλυσίδα των blocks) και έχουν σχεδιαστεί να αντιστέκονται στη διαχρονική μείωση της αξίας τους από το πληθωρισμό. Είναι δύσκολο να πλαστογραφηθούν, είναι άυλα και πιο -δημοκρατικά- για τους πολίτες επειδή είναι αποκεντροποιημένα, με την έννοια ότι δεν ελέγχονται από κάποια κυβέρνηση ή κεντρική τράπεζα.

Ο τρόπος παραγωγής και διανομής κρυπτονομισμάτων θα αναλυθεί στη συνέχεια του άρθρου όπου θα επικεντρωθούμε κυρίως στο κρυπτονόμισμα Bitcoin που είναι το πρώτο κρυπτονόμισμα στην ιστορία.

Πολλοί ισχυρίζονται ότι η θεωρητική βάση των κρυπτονομισμάτων (μεταξύ άλλων και η Κεντρική Ευρωπαϊκή Τράπεζα, Οκτώβριος 2012)<sup>3</sup> έχει τις ρίζες της στον Αυστριακό οικονομολόγο F. A. Hayek. Στο βιβλίο του, με τίτλο: Denationalisation of Money, (1976), ο συγγραφέας οραματίστηκε ένα νομισματικό σύστημα που δεν θα ελέγχεται από κάποια κυβέρνηση και τα νομίσματα που θα εκδίδονται από τις κεντρικές τράπεζες, θα συνυπάρχουν μαζί με άλλα που θα εκδίδονται από ιδιώτες.

Οι γρήγοροι ρυθμοί εξέλιξης της τεχνολογίας, η παγκοσμιοποίηση, καθώς και η εύκολη πρόσβαση των ανθρώπων στο Internet, έχουν δημιουργήσει πλέον τις προϋποθέσεις ώστε το όραμα του F.A. Hayek να υλοποιηθεί σύντομα.

Το Bitcoin είναι μία πρωτοποριακή μορφή κρυπτονομίσματος το οποίο προτάθηκε από τον Satoshi Nakamoto σε ένα άρθρο που δημοσίευσε το Νοέμβριο του 2008

και άρχισε να συναλλάσσεται ηλεκτρονικά από τον Ιανουάριο του 2009. Ο Nakamoto δεν έχει αποκαλύψει τη ταυτότητα του μέχρι σήμερα και μπορεί να είναι ένα άτομο ή μια ομάδα ατόμων με αυτό το ψευδώνυμο.

Το Bitcoin ανήκει στην κατηγορία των κρυπτονομισμάτων και είναι το πρώτο αποκεντρωμένο δίκτυο πληρωμής, όπου όλοι οι χρήστες που συμμετέχουν σε αυτό είναι ίσοι μεταξύ τους, από την άποψη ότι δεν υπάρχει κάποια συγκεκριμένη ιεραρχία και η επικοινωνία των χρηστών γίνεται άμεσα, χωρίς διαμεσολάβηση τρίτων.

Το Bitcoin όπως και όλα τα άλλα κρυπτονομίσματα, είναι ένα άυλο ψηφιακό νόμισμα που υπάρχει μόνο στο Internet. Οποιοσδήποτε χρήστης που έχει πρόσβαση στο Internet, μπορεί να δημιουργήσει το δικό του ψηφιακό Bitcoin πορτοφόλι σε κάποιο Bitcoin ανταλλακτήριο. Ο χρήστης πληκτρολογεί το ποσό των χρημάτων που επιθυμεί να κάνει Bitcoin και αυτά στη συνέχεια κατατίθενται στο ανταλλακτήριο. Ανάλογα με το ποσό των χρημάτων που κατάθεσε ο χρήστης, το ανταλλακτήριο καταγράφει τη συναλλαγή στο ψηφιακό του πορτοφόλι. Το ψηφιακό πορτοφόλι του κάθε χρήστη είναι μοναδικό και μπορεί να έχει πρόσβαση σε αυτό μόνο όποιος γνωρίζει τους κωδικούς εισόδου για το συγκεκριμένο πορτοφόλι. Ο κάθε χρήστης μπορεί να στέλνει ή να λαμβάνει bitcoins μέσω του ψηφιακού του πορτοφολιού και επιλεγμένα καταστήματα (από καφετέριες μέχρι μεσιτικά γραφεία για αγορές ακινήτων) επιτρέπουν τις αγορές αγαθών με χρήση Bitcoin εισάγοντας απλά τη κωδικοποιημένη διεύθυνση του ψηφιακού πορτοφολιού του παραλήπτη.

Η αποκεντροποιημένη φύση του Bitcoin καθιστά τις κυβερνήσεις ανήμπορες να ελέγξουν τα ψηφιακά Bitcoin πορτοφόλια και όπως έχει δείξει η ιστορία, δεν είναι λίγες οι φορές που το Bitcoin έχει αποτελέσει διέξοδο για τη μαύρη αγορά, αλλά και για παράνομες εμπορικές δραστηριότητες. (π.χ. η διαδικτυακή μαύρη αγορά γνωστή ως Silk Road)

Μαύρη αγορά ή παραοικονομία, θεωρείται η οικονομική δραστηριότητα που κάνουν κάποιοι με παράνομο τρόπο, όπως για παράδειγμα η δημιουργία, πώληση και εμπορία προϊόντων και υπηρεσιών χωρίς αυτά να ελέγ-

1. Αξιοσημείωτο είναι πως δυο πρωτοπόροι της κρυπτογραφίας, ο Whitfield Diffie και ο Martin Hellman, βραβεύτηκαν τη 1η Μαρτίου του 2016 με το φετινό βραβείο Νόμπελ της Πληροφορικής (βραβείο Τούρινγκ).

2. Yermack, D., 2013. Is Bitcoin a Real Currency? An Economic Appraisal. Technical Report. National Bureau of Economic Research.

3. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>



χονται και να φορολογούνται από το κράτος. Το παγκόσμιο Α.Ε.Π. σήμερα υπολογίζεται στα 76 περίπου τρισεκατομμύρια δολάρια και η παγκόσμια μαύρη αγορά γύρω στα 10 τρισεκατομμύρια δολάρια αποτελώντας τη τρίτη μεγαλύτερη οικονομία παγκοσμίως μετά από την οικονομία της Αμερικής και της Κίνας.<sup>4</sup> Ως εκ τούτου, οι δυνατότητες ανάπτυξης του Bitcoin και μόνο από την μαύρη αγορά είναι τεράστιες αφού η κεφαλαιοποίησή του είναι μόλις 7 δισεκατομμύρια δολάρια.

Η αξία του Bitcoin καθορίζεται αποκλειστικά από τους νόμους της προσφοράς και της ζήτησης και της αποδοχής του ή μη απ' τους συναλλασσόμενους.

Το 2015 αποτέλεσε τη χρονιά όπου τα επιχειρηματικά κεφάλαια και η Wall Street πίστεψαν στην τεχνολογία που χρησιμοποιεί το Bitcoin, τη λεγόμενη τεχνολογία των blocks. Εταιρείες όπως η Goldman Sachs, η American Express, το χρηματιστήριο του Nasdaq καθώς και η Kleiner Perkins, επένδυσαν στο τομέα της τεχνολογίας των blocks επιχειρηματικά κεφάλαια περίπου αξίας 314 εκατομμυρίων δολαρίων. Το ενδιαφέρον της Wall Street για το Bitcoin επιβεβαιώνεται από το γεγονός ότι το 2015 δημιουργήθηκε στο Χρηματιστήριο της Νέας Υόρκης, δείκτης για την πορεία του Bitcoin (NYXBT).

Επιπλέον, δημιουργήθηκε το Bitcoin Investment trust (GBTC), του οποίου οι μετοχές μπορούν να επενδυθούν και να διακρατηθούν σε διάφορους συνταξιοδοτικούς λογαριασμούς (όπως IRA, Roth IRA, κτλ.). Τα αδέρφια Winklevoss ίδρυσαν ένα πλήρως πιστοποιημένο Bitcoin ανταλλακτήριο (το λεγόμενο Gemini) και έχουν δημιουργηθεί ETFs σε Bitcoin τα οποία μπορούν να προσελκύσουν ιδρύματα και συνταξιοδοτικά προγράμματα, όπου δεν μπορούν (ή δεν θέλουν) να αγοράσουν το κρυπτονόμισμα κατευθείαν, αλλά επιθυμούν την έμμεση επένδυση σε αυτό.<sup>5</sup>

Αξιοσημείωτο είναι επίσης ότι αρκετές εταιρείες προσφέρουν πλέον Bitcoin χρεωστικές κάρτες. Πιο συγκεκριμένα η εταιρεία BitPay αποτελεί φορέα παροχής υπηρεσιών για πληρωμές σε Bitcoin και προσφέρει μια

Bitcoin χρεωστική κάρτα η οποία εκδίδεται από την Metropolitan Commercial Bank και είναι διαθέσιμη για τις 50 πολιτείες των ΗΠΑ.

Η Bitcoin χρεωστική κάρτα λειτουργεί όπως όλες οι άλλες χρεωστικές κάρτες (debit cards) με την διαφορά ότι τα χρήματα του χρήστη της, αντλούνται απ' το ψηφιακό πορτοφόλι του Bitcoin και όχι από κάποιο τραπεζικό του λογαριασμό. Η κάρτα αυτή είναι αποδεκτή για πληρωμές σε όλους τους φορείς που δέχονται Visa και αναλήψεις χρημάτων μπορούν να πραγματοποιηθούν από οποιοδήποτε ATM.

## II. Η ιστορία του Bitcoin

Τον Ιανουάριο του 2009 δημιουργήθηκε το πρώτο block (genesis block) της αλυσίδας των blocks και η πρώτη συναλλαγή με Bitcoin πραγματοποιήθηκε στις 12

Ιανουαρίου του 2009 στο block 170, από τον δημιουργό του Bitcoin, Satoshi Nakamoto στον προγραμματιστή H. Finney ο οποίος ήταν από τους πρώτους χρήστες του Bitcoin.

Το πρώτο χρόνο το Bitcoin συναλλασσόταν αποκλειστικά από άτομο σε άτομο χωρίς τη διαμεσολάβηση ανταλλακτηρίων και στις 5 Οκτωβρίου του 2009

η New Liberty Standard δημοσιεύει τη πρώτη συναλλαγματική ισοτιμία δολαρίου σε Bitcoin η οποία ήταν 1\$ ίσο με 1.309 BTC.

Τον Ιούλιο του 2010 δημιουργήθηκε ένα από τα πρώτα ανταλλακτήρια Bitcoin το οποίο λεγόταν Mt.Gox και στη συνέχεια δημιουργήθηκαν και άλλα ιδιωτικά Bitcoin ανταλλακτήρια, όμως το Mt.Gox ήταν το κυρίαρχο, αφού το 2013 εκτελούσε το 70% όλων των συναλλαγών Bitcoin. Στα τέλη του 2013 προέκυψαν προβλήματα αναλήψεων κεφαλαίων από τους πελάτες του Mt.Gox και το τέλος του ανταλλακτηρίου ήρθε το Φεβρουάριο του 2014 όταν έκλεισε την ιστοσελίδα του και χρεοκόπησε μη μπορώντας να ανακτήσει 744.408 bitcoins που είχε χάσει από μια επίθεση που δέχθηκε στο σύστημα ασφαλείας του από hacker. Το γεγονός αυτό καθώς και άλλα θέματα ασφαλείας που παρατηρήθηκαν σε άλλα ανταλλακτήρια από επιθέσεις hackers, είχαν σαν αποτέλεσμα να προκαλέσουν μια σημαντική πτώση στη τιμή του Bitcoin στα τέλη του 2013. (Βλέπε Διάγραμμα 1)



4. <http://www.forbes.com/sites/benzingainsights/2011/11/07/rise-of-the-shadow-economy-second-largest-economy-in-the-world/#fcc51115d38f>

5. <http://www.forbes.com/sites/laurashin/2015/12/11/should-you-invest-in-bitcoin-10-arguments-in-favor-as-of-december-2015/#1081b60d540e>

Το Bitcoin δεν είναι το μόνο κρυπτονόμισμα. Τον Αύγουστο του 2015 κατεγράφησαν πάνω από 600 κρυπτονόμισμα με τα πιο γνωστά μέσα σε αυτά το Ethereum, το Ripple και το Litecoin. Το Bitcoin είναι με διαφορά το πιο γνωστό και με την υψηλότερη κεφαλαιοποίηση. Το Ethereum είναι δεύτερο με κεφαλαιοποίηση γύρω στα 750 εκατομμύρια δολάρια και το Ripple τρίτο με συνολική κεφαλαιοποίηση 200 εκατομμύρια δολάρια.

### III. Χαρακτηριστικά του Bitcoin

Το Bitcoin έχει ιδιαίτερο ενδιαφέρον γιατί παρουσιάζει πολλά πλεονεκτήματα όπου το καθιστούν ξεχωριστό, καινοτόμο και ιδανικό για τις αγορές και τις ανάγκες της μελλοντικής ψηφιακής παγκόσμιας οικονομίας.

Η μεγάλη καινοτομία του Bitcoin είναι ότι δεν ελέγχεται από κάποια κυβέρνηση ή κεντρική τράπεζα, οπότε δίνεται η ευκαιρία στους χρήστες του να διαμορφώσουν τους δικούς τους δημοκρατικούς όρους συναλλαγών. Οι χρήστες μπορούν να στείλουν ή να λάβουν οποιοδήποτε ποσό, σε οποιοδήποτε ψηφιακό πορτοφόλι Bitcoin, οποιαδήποτε στιγμή, αλλά με το πάτημα λίγων κουμπιών από τον υπολογιστή τους ή το κινητό τους.

Οι προοπτικές του Bitcoin είναι πραγματικά τεράστιες. Σύμφωνα με πρόσφατα στατιστικά στοιχεία της GSMA Intelligence (2014), οι ενεργές συσκευές κινητών είναι περισσότερες πλέον από το πληθυσμό της ανθρωπότητας. Επιπρόσθετα σημειώνεται ότι δύο δισεκατομμύρια έφηβοι μπορούν να αποκτήσουν πρόσβαση στο παγκόσμιο χρηματοοικονομικό σύστημα με τη χρήση του Bitcoin μέσω των smartphone κινητών τους, παρά τους κινδύνους που μπορεί αυτό να ελλοχεύει. Ένα άλλο πλεονέκτημα είναι ότι το κόστος των συναλλαγών με bitcoins είναι πάρα πολύ μικρό και σε ορισμένες περιπτώσεις μηδενικό. Με την χρήση του Bitcoin ξεπερνιέται το εμπόδιο των διακρατικών ελέγχων κεφαλαίων, αφού ο κάθε χρήστης μπορεί να αντλήσει οποιοδήποτε χρηματικό ποσό επιθυμεί από το ψηφιακό του πορτοφόλι και τα εμβάσματα γίνονται πιο εύκολα, με χαμηλό κόστος προμηθειών και πιο γρήγορα από ποτέ.

Να σημειωθεί ότι οι Bitcoin συναλλαγές είναι ασφαλείς, αλλά μη αναστρέψιμες. Οι χρήστες του Bitcoin έχουν τον πλήρη έλεγχο του ψηφιακού τους πορτοφολιού και καμία κυβέρνηση δεν μπορεί να τους το «παγώσει». Για

αυτό το λόγο το Bitcoin είναι ιδιαίτερα γνωστό στις μαύρες αγορές για μεταφορά μαύρου χρήματος και αγορά παράνομων αγαθών, καθώς οι συναλλαγές μπορούν να διεξαχθούν χωρίς να συνδέονται με προσωπικές πληροφορίες των συμμετεχόντων.

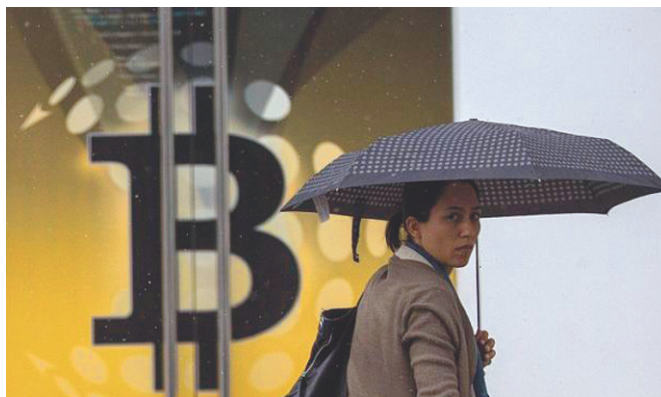
Όπως προαναφέρθηκε το Bitcoin είναι ανεξάρτητο από οποιαδήποτε κυβέρνηση ή κεντρική τράπεζα. Στο δίκτυο του Bitcoin δεν υπάρχει κάποιος κεντρικός διαχειριστής υπεύθυνος για ολόκληρο το δίκτυο, αλλά ο κάθε χρήστης είναι ίσος ως προς τους άλλους με την έννοια ότι τα δεδομένα των συναλλαγών είναι κοινά για όλους. Τα μαθηματικά φροντίζουν για την λειτουργία και την ασφάλεια όλου του δικτύου, όπως εξηγείται παρακάτω στη διαδικασία της εξόρυξης.

Το Bitcoin χρησιμοποιεί λογισμικό ανοικτού κώδικα με την έννοια ότι ο κώδικας που χρησιμοποιείται, είναι δημόσιος και επιτρέπεται σε οποιοδήποτε προγραμματιστή που έχει σχετική τεχνογνωσία, να τον τροποποιήσει (open source). Οι προγραμματιστές δεν μπορούν να εξα-

ναγκάσουν καμία αλλαγή στο πρωτόκολλο Bitcoin, όμως μπορούν να προτείνουν μια νέα καλύτερη έκδοση του λογισμικού αν το κρίνουν απαραίτητο και οι χρήστες είναι ελεύθεροι να επιλέξουν την έκδοση του λογισμικού που θα χρησιμοποιούν.

Το Bitcoin δεν είναι ανώνυμο και η ανωνυμία δεν είχε συμπεριληφθεί σαν ένας από του στόχους κατά τη σχεδίαση του (S. Nakamoto, no date). Συχνά υπάρχει η λανθασμένη αντίληψη ότι το Bitcoin είναι ανώνυμο επειδή είναι εφικτό να στείλει ή να λάβει κάποιος bitcoins χωρίς να χρειαστεί να δώσει κάποια πληροφορία πιστοποίησης, παρά μόνο τον κωδικοποιημένο αριθμό του ψηφιακού πορτοφολιού του. Ωστόσο αν θέλει κάποιος να πετύχει πλήρη μορφή ανωνυμίας, υπάρχουν ιστοσελίδες που το προσφέρουν αυτό, αλλά η διαδικασία αυτή εγκυμονεί κινδύνους να χάσουμε τα Bitcoin μας επειδή πρέπει να τα εμπιστευτούμε σε τρίτους, χρησιμοποιώντας τα λεγόμενα Mixing Services. Όπως θα δούμε παρακάτω στη διαδικασία της εξόρυξης, η διαφάνεια είναι επίσης ένα από τα χαρακτηριστικά του Bitcoin.

Άρα μπορούμε να ισχυρισθούμε ότι το Bitcoin είναι ένα νόμισμα που χρησιμοποιεί ψευδώνυμα και ο καθένας μας μπορεί να έχει το δικό του ψηφιακό πορτοφόλι χωρίς να χρειάζεται να δώσει προσωπικές πληροφορίες ταυτοποίησης.





## Η διαδικασία της εξόρυξης

Οι συναλλαγές που πραγματοποιούνται στο Bitcoin δίκτυο καταγράφονται περίπου ανά 10 λεπτά, σε μια ψηφιακή λίστα που ονομάζεται block. Το λογιστικό βιβλίο (ledger), που έχει καταγεγραμμένες όλες τις συναλλαγές που έχουν γίνει από τη πρώτη μέρα δημιουργίας του Bitcoin, είναι μια μεγάλη λίστα από πολλά blocks που συνδέονται μεταξύ τους και ονομάζεται η αλυσίδα των blocks (block chain).

Περίπου ανά 10 λεπτά δημιουργείται ένα νέο block που έχει αποθηκευμένες νέες πληροφορίες εκκρεμών συναλλαγών και προστίθεται στο τέλος της αλυσίδας των blocks. Η αλυσίδα των blocks ανανεώνεται συνεχώς με τις νέες ενημερώσεις των ολοκληρωμένων συναλλαγών και είναι σε ψηφιακή μορφή δημόσια για όλους τους χρήστες στο δίκτυο του Bitcoin. Αξίζει να σημειωθεί ότι οποιοσδήποτε χρησιμοποιεί το δίκτυο του bitcoin, μπορεί να δει οποιαδήποτε συναλλαγή που έχει πραγματοποιηθεί στο παρελθόν όπως και το ποσόν των bitcoins που κατέχει ο κάθε χρήστης. Όπως έχει ήδη αναφερθεί, τα προσωπικά στοιχεία του κάθε χρήστη δε φαίνονται παρά μόνο μια κωδικοποιημένη αλφαριθμητική ακολουθία που τον αντιπροσωπεύει. Για τον λόγο αυτό λέμε ότι το Bitcoin είναι ψευδώνυμο και όχι ανώνυμο.

Τα αρχεία είναι όλα ψηφιακά και πρέπει να είμαστε σίγουροι για την αυθεντικότητά τους και πως δεν έχουν τροποποιηθεί σκοπίμως από κάποιους για εξαπάτηση. Η διασφάλιση της αυθεντικότητας του λογιστικού βιβλίου που έχει καταγεγραμμένες όλες τις συναλλαγές στην ιστορία του Bitcoin, γίνεται μέσω της εξόρυξης (mining).

Η εξόρυξη διασφαλίζει την εγκυρότητα των πληροφοριών των συναλλαγών και τη δημιουργία νέων Bitcoin, διαδικασία που συμβάλλει ταυτόχρονα και στην αύξηση της ρευστότητας του νομίσματος αυτού.

Οποιοσδήποτε χρήστης με ψηφιακό πορτοφόλι Bitcoin μπορεί εθελοντικά, χωρίς να είναι απαραίτητο, να λάβει μέρος στη διαδικασία της εξόρυξης. Στη περίπτωση αυτή ο χρήστης θα ονομάζεται εξορύχος (miner).

Μέσω της εξόρυξης οι πληροφορίες των συναλλαγών που βρίσκονται σε ένα block, κωδικοποιούνται καθώς μετατρέπονται σε ένα αλφαριθμητικό αποτέλεσμα με τη χρήση κρυπτογραφίας. Το αλφαριθμητικό αποτέλεσμα λέγεται hash και αυτή είναι η μορφή με την οποία οι πληροφορίες αποθηκεύονται στο block. Οι hashes είναι

μοναδικές και εύκολα δημιουργήσιμες από τους υπολογιστές ανεξάρτητα από το μέγεθος των πληροφοριών. Η hash του κάθε block συνδέεται με τη hash του προηγούμενου block έτσι ώστε να υπάρχει ενημέρωση του υπολοίπου στα ψηφιακά πορτοφόλια που συμμετέχουν σε κάποια συναλλαγή. Όταν κάποιος προσπαθήσει να τροποποιήσει μια υπάρχουσα hash (δηλαδή να εξαπατήσει σε κάποια συναλλαγή), η τροποποιημένη μη-αληθής hash εντοπίζεται από τους εξορύχους (miners) και τόσο το block με τη πλαστή hash, όσο και τα επακόλουθα blocks που συνδέονται με αυτό ακυρώνονται.

Το μόνο που πρέπει να κάνουν οι εξορύχιοι για να συμμετάσχουν στη διαδικασία της εξόρυξης, είναι να επιτρέπουν εκούσια στο δίκτυο του Bitcoin να χρησιμοποιεί τη κεντρική μονάδα επεξεργασίας (CPU) του υπολογιστή τους για την επίλυση σύνθετων προβλημάτων μαθηματικής κρυπτογραφίας προκειμένου να γίνεται επιβεβαίωση των Bitcoin συναλλαγών που είναι σε εξέ-

λιξη. Οι εξορύχιοι επιλέγουν αν ο υπολογιστής τους θα κάνει εξόρυξη αποκλειστικά «μόνος» του ή σε συνεργασία με άλλους υπολογιστές άλλων εξορύχων. Ο εξορύχος σε αυτή την περίπτωση επιλέγει σε ποια ομάδα υπολογιστών θα βάλει τον υπολογιστή του να

κάνει εξόρυξη και η κάθε μια από αυτές τις ομάδες υπολογιστών ονομάζεται πισίνα εξόρυξης (mining pool). Οι υπολογιστές των εξορύχων που βρίσκονται στην ίδια πισίνα εξόρυξης, μοιράζονται μαζί τα αποτελέσματά τους για τα μαθηματικά προβλήματα κρυπτογραφίας προκειμένου να δημιουργούν επιτυχώς και γρήγορα hashes, συνεπώς και καινούρια blocks.

Οπότε η απάντηση στο εύλογο ερώτημα: Πως ελέγχονται όλες οι συναλλαγές μέσα στο δίκτυο του Bitcoin; είναι πως οι υπολογιστές των εξορύχων φροντίζουν για αυτό!

Σύμφωνα με τους κανόνες που διέπουν την εξόρυξη, ο αριθμός των νέων bitcoins που δημιουργούνται υποδιπλασιάζεται ανά 4 χρόνια. Το καλοκαίρι του 2016 στις 23 Ιουλίου θα γίνει ο δεύτερος υποδιπλασιασμός. Πιο συγκεκριμένα, όταν ξεκίνησε η κυκλοφορία του Bitcoin, 50 νέα Bitcoin δημιουργούνταν ανά 10 λεπτά μέσω της εξόρυξης από τους εξορύχους. Σήμερα δημιουργούνται 25 νέα bitcoin ανά 10 λεπτά και στις 23 Ιουλίου του 2016 θα πέσει ο αριθμός των νέων bitcoins που θα δημιουργούνται στα 12,5 ανά 10 λεπτά. Η δημιουργία νέων bitcoins θα σταματήσει το 2140 όπου θα έχουν παραχθεί





21 εκατομμύρια bitcoin. Αυτή τη στιγμή είναι σε κυκλοφορία πάνω από 15 εκατομμύρια bitcoin.

Με αυτό το τρόπο το Bitcoin καταφέρνει να αντιμετωπίσει το πρόβλημα της πιθανής μείωσης της διαχρονικής αξίας του νομίσματος. Πρέπει να σημειωθεί ότι ένα από τα βασικά μειονεκτήματα των παραστατικών χρημάτων είναι ότι οι κεντρικές τράπεζες, στα πλαίσια της νομισματικής τους πολιτικής, μπορούν να τυπώσουν όσα νέα χρήματα επιθυμούν και αν τυπώσουν πολλά, οι νόμοι της προσφοράς και της ζήτησης βεβαιώνουν ότι η πραγματική αξία του νομίσματός τους θα μειωθεί και πολλές φορές με δραματικό τρόπο.

Σύμφωνα με μια έρευνα του 2011 σε 775 παραστατικά χρήματα από το DollarDaze.org, ο μέσος όρος ζωής για ένα παραστατικό νόμισμα, πριν αντικατασταθεί λόγω του εκμηδενισμού της αξίας του, είναι 27 χρόνια.

Οι κύριοι λόγοι αποτυχίας των παραστατικών χρημάτων φαίνεται να είναι ο υπερπληθωρισμός, οι πόλεμοι και φυσικά η τάση των κεντρικών τραπεζών να εκδίδουν ανεξέλεγκτα πολλές φορές, όσα χρήματα θέλουν. Το πιο επιτυχημένο παραστατικό χρήμα στο χρόνο είναι η αγγλική λίρα η οποία έχει καταφέρει να επιβιώσει για 323 χρόνια, έχοντας όμως χάσει από το 1694 όπου δημιουργήθηκε το 99,5% της πραγματικής της αξίας.

Τελικά η εξόρυξη είναι ένας διαγωνισμός, μια λοταρία θα μπορούσαμε να πούμε, όπου είναι τυχαίο ποιος εξορύχος θα επιβεβαιώσει κάποια συναλλαγή. Οι υπολογιστές των τυχαία επιλεγμένων εξορύχων που θα συμβάλουν στην έγκριση μιας συναλλαγής, θα ανταμειβο-

νται με ένα μέρος από τα νέα bitcoins που θα δημιουργούνται ανάλογα με την ποσοστιαία συμβολή τους στην επίλυση των μαθηματικών προβλημάτων κρυπτογραφίας. Έτσι όπως είναι σχεδιασμένο το πρωτόκολλο του Bitcoin αυτή τη στιγμή, μετά από το 2140 θα έχουν παραχθεί όλα τα Bitcoin και οι εξορύχοι θα παίρνουν αποκλειστικά σαν ανταμοιβή το ποσοστό προμήθειας από τις συναλλαγές που εγκρίνουν.

Ο Satoshi Nakamoto θέσπισε τους κανόνες που αφορούν το Bitcoin με τέτοιο τρόπο ώστε να το προσομοιάσει με το χρυσό. Υπάρχουν περιορισμένα αποθέματα χρυσού στο κόσμο και για κάθε γραμμάριο χρυσού που γίνεται εξόρυξη τόσο δυσκολότερο είναι να εξορυχθεί ο υπολειπόμενος. Αντίστοιχα ο μέγιστος αριθμός bitcoin που θα υπάρξει είναι 21 εκατομμύρια το 2140 και όσο περνάει ο χρόνος η εξόρυξη νέων bitcoins από τους χρήστες, θα γίνεται όλο και πιο πολύ ανταγωνιστική και όπως εξηγείται παρακάτω λιγότερο επικερδής. Εξαιτίας αυτής της περιορισμένης παραγωγής, ένας από τους λόγους που ο χρυσός έχει καταφέρει να διατηρήσει την αξία του για πολλά χρόνια είναι τα περιορισμένα του αποθέματα και οι υποστηρικτές των ψηφιακών νομισμάτων ευελπιστούν ότι το ίδιο θα συμβεί και με το Bitcoin.

Θα πρέπει να τονιστεί ότι η εξόρυξη είναι η πιο σημαντική διαδικασία για το Bitcoin, αφού δημιουργούνται νέα bitcoins στην αγορά συμβάλλοντας στην ρευστότητα και στην ομαλή εκπλήρωση των συναλλαγών όλου του δικτύου.

Συνοπτικά καταγράφονται στον ακόλουθο **Πίνακα 1 τα πλεονεκτήματα και τα μειονεκτήματα του Bitcoin.**



## ΠΙΝΑΚΑΣ 1: ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ BITCOIN

### ΠΛΕΟΝΕΚΤΗΜΑΤΑ

- Χαμηλά (και σε ορισμένες περιπτώσεις μηδενικά) κόστη συναλλαγών.
- Έχει σχεδιαστεί έτσι ώστε να προστατεύονται οι χρήστες του Bitcoin από τον πληθωρισμό.
- Διαφάνεια στις πληροφορίες των συναλλαγών.
- Είναι ασφαλές εξαιτίας της προχωρημένης κρυπτογραφίας που χρησιμοποιεί. Κανένας hacker δεν έχει καταφέρει να επιτεθεί στο Bitcoin δίκτυο κατευθείαν. Όλες οι επιτυχείς επιθέσεις που έχουν γίνει από hackers, στοχεύουν τα ανταλλακτήρια και επιτυγχάνουν εξαιτίας της χαμηλής ασφάλειας των ανταλλακτηρίων. Οπότε η επιλογή του ανταλλακτηρίου που θα δημιουργήσουμε το ψηφιακό μας πορτοφόλι είναι ιδιαίτερα σημαντική.
- Η χρήση του Bitcoin είναι ελεύθερη για οποιονδήποτε άνθρωπο, ανεξάρτητα από την ηλικία του, το εισόδημα του και την τοποθεσία του.
- Είναι αδύνατον να επέμβουν τρίτοι (π.χ. Κυβερνήσεις) για να "παγώσουν" το ψηφιακό μας πορτοφόλι.
- Το Bitcoin δίκτυο είναι ψευδώνυμο. Οι πληρωμές με Bitcoin γίνονται χωρίς να χρειάζεται να δώσετε προσωπικές σας πληροφορίες. Είναι τόσο ιδιωτικό, όσο θέλει κάποιος να είναι.
- Εύκολη πρόσβαση στο ψηφιακό μας πορτοφόλι από οποιαδήποτε συσκευή συνδέεται στο Internet.
- Το Bitcoin δίκτυο είναι παγκόσμιος κλίμακας και λειτουργεί κάθε μέρα για όλο το εικοσιτετράωρο.
- Είναι εύκολα στη μεταφορά.
- Δεν υπάρχει γραφειοκρατία.
- Γρήγορος χρόνος συναλλαγών.
- Μπορείτε να βγάξετε τα δικά σας χρήματα σε Bitcoin μέσω της εξόρυξης.
- Δεν είναι δυνατή η πλαστογράφηση του.
- Μπορεί να χρησιμοποιηθεί για διαφοροποίηση χαρτοφυλακίων.
- Δεν υπάρχουν όρια στα ποσά των συναλλαγών. Ξεπερνούνται οι διακρατικοί περιορισμοί κεφαλαίων.
- Φιλικό ως προς το περιβάλλον. Δεν απαιτείται χρήση χαρτιού όπως στα χαρτονομίσματα.

### ΜΕΙΟΝΕΚΤΗΜΑΤΑ

- Έλλειψη ενημέρωσης τόσο για την ύπαρξη του Bitcoin, όσο και για τον τρόπο λειτουργίας του.
- Υψηλό ρίσκο επειδή μέχρι στιγμής οι τιμές του Bitcoin είναι πολύ ευμετάβλητες.
- Ακόμα αναπτύσσεται. Είναι ακόμα καινούριο και υπάρχει αβεβαιότητα για το μέλλον του επειδή επηρεάζεται αποκλειστικά από το νόμο της προσφοράς και ζήτησης.
- Αν καθούν τα Bitcoin κάποιου χρήστη, είτε επειδή έπεσε θύμα επιθέσεων από hackers, είτε επειδή έχασε τους κωδικούς εισόδου για το ψηφιακό του πορτοφόλι, δεν μπορεί να διεκδικήσει τα χρήματα του πίσω.
- Υπάρχει περιορισμένη αποδοχή του Bitcoin στην αγορά. Δεν είναι ευρέως αποδεκτό από πολλούς εμπόρους.
- Επιρρεπές στις κερδοσκοπικές φούσκες.
- Μη αναστρέψιμες συναλλαγές. Αν ο πωλητής ενός προϊόντος λάβει το ποσό σε Bitcoin που ζητάει και δεν αποστείλει το προϊόν στον αγοραστή, δεν γίνεται επιστροφή χρημάτων.
- Απαγορεύεται η χρήση του Bitcoin σε ορισμένες χώρες (όπως η Ταϊλάνδη). Προς το παρόν δεν υπάρχει κάποια νομοθεσία για τη χρήση του Bitcoin στην Ελλάδα.



## IV. Το Bitcoin ως επένδυση

Όταν ξεκίνησε η λειτουργία του ανταλλακτηρίου Mt.Gox στις 18/07/2010, το ένα Bitcoin ήταν ίσο με \$0,07 και στις 29/11/2013 καταγράφηκε η μέγιστη ιστορικά τιμή στα \$1.242. Ισοδύναμα, αν κάποιος είχε επενδύσει \$1.000 το 2010 σε Bitcoin και τα διακρατούσε, το Νοέμβριο του 2013 αυτά θα αξίζαν πάνω από 17 εκατομμύρια δολάρια.

Ο Weber (2014) επισημαίνει ότι το 70% από τα Bitcoin που ήταν σε κυκλοφορία μέχρι το 2014, βρίσκονταν σε αδρανείς λογαριασμούς. Το γεγονός αυτό επιβεβαιώνεται και από τον Yermack (2013) όπου σημειώνει ότι οι αγοραστές του Bitcoin, το χρησιμοποιούν κυρίως ως μια επένδυση παρά σαν ένα νόμισμα,

Σύμφωνα με πρόσφατη έρευνα από το CoinDesk, αυξάνονται σημαντικά οι ρυθμοί αφομοίωσης του Bitcoin ως μέσο συναλλαγών. Πράγματι, ο μέσος όρος του ημερήσιου αριθμού των συναλλαγών που γίνονταν με Bitcoin το 2014 ήταν 69.200, ενώ για το 2015 ο αριθμός αυξήθηκε στις 125.100.

Όπως έχουμε ήδη αναφέρει, όταν κάποιος χρήστης χάσει τους κωδικούς εισόδου για το ψηφιακό του πορτοφόλι χάνει και τη πρόσβαση στα bitcoins μέσα σε αυτό. Τα χαμένα bitcoins παραμένουν ακόμα στην αλυσίδα των blocks, μέχρι ο κάτοχος να εισάγει τους σωστούς κωδικούς για το ψηφιακό πορτοφόλι που αυτά ανήκουν. Συχνοί λόγοι απώλειας του κωδικού εισόδου είναι η αμέλεια και ο θάνατος του χρήστη χωρίς να γνωστοποιήσει το κωδικό εισόδου στους κληρονόμους του. Επίσης σε ορισμένες περιπτώσεις κάποιοι χρήστες αποθηκεύουν το κωδικό εισόδου τους στο σκληρό δίσκο του υπολογιστή χωρίς να τον απομνημονεύσουν και όταν προκύψει κάποιο τεχνικό πρόβλημα στο σκληρό δίσκο, χάνουν τη πρόσβαση στο ψηφιακό τους πορτοφόλι.

### Οι κίνδυνοι του Bitcoin

Ο τρόπος λειτουργίας του Bitcoin είναι πρωτότυπος και τόσο τα χαρακτηριστικά του, όσο και οι κίνδυνοι που συνδέονται με αυτό, είναι δύσκολο να γίνουν κατανοητά από τους μη-ειδικούς. Το γεγονός αυτό αποτελεί έναν από τους βασικούς λόγους που η χρήση του Bitcoin δεν

είναι γνωστή στο ευρύτερο κοινό.

Το Bitcoin είναι περιουσιακό στοιχείο, αλλά και δικτυο ταυτόχρονα. Οι κίνδυνοι που το επηρεάζουν είναι όχι μόνο αυτοί που επηρεάζουν τα περιουσιακά στοιχεία γενικά, αλλά και πιθανά τεχνικά προβλήματα που μπορεί να προκαλέσουν τη δυσλειτουργία (ίσως και την κατάρρευση) ολόκληρου του Bitcoin δικτύου.

Η αποκεντροποιημένη φύση του αποτελεί σημαντικό πλεονέκτημα, αλλά και ταυτόχρονα μειονέκτημά του. Πλεονέκτημα για όλους τους λόγους που έχουν προαναφερθεί, αλλά και μειονέκτημα από την άποψη ότι αν προκύψουν κάποια προβλήματα είναι δύσκολο να απαντηθούν τα ερωτήματα: Πως και ποιος θα τα επιλύσει ..αν φυσικά μπορούν να επιλυθούν;

Η αποδοχή του Bitcoin ως επίσημη μορφή νομίσματος είναι ακόμα υπό αμφισβήτηση και γι' αυτό επικρατεί θεσμική αβεβαιότητα γύρω από αυτό. Γενικά τα κρυπτονομίσματα έχουν υψηλό νομοθετικό ρίσκο (regulatory risk) επειδή οι κυβερνήσεις ίσως θεσπίσουν νόμους για να ελέγξουν, φορολογήσουν ή και να απαγορεύσουν τη χρήση τους. Δεν υπάρχει ομοιομορφία γύρω από το νομοθετικό πλαίσιο για το Bitcoin αφού είναι διαφορετικό από χώρα σε χώρα και σε ορισμένες χώρες δεν υπάρχει καν κάποιος νόμος για αυτό. Έμμεσα οι κυβερνήσεις μπορούν να επηρεάσουν το μέλλον του Bitcoin με την χρήση ευνοικών ή μη φορολογικών και άλλων ρυθμίσεων.

Οι μη αναστρέψιμες συναλλαγές, η ψευδώνυμη φύση του Bitcoin που προσφέρει κάποια μορφή ανωνυμίας, καθώς και η άμεση μεταβίβαση-ρευστοποίηση των κλεμμένων bitcoins ακόμα και μετά τη διαπίστωση της κλοπής, έχουν προσελκύσει το ενδιαφέρον των εγκληματιών και των hackers. Η κοινότητα του Bitcoin έχει υποχρέωση να συνεργαστεί με τις ανεξάρτητες και άλλες αρχές, για τη διατήρηση της καλής φήμης του, ώστε να μην γίνει η χρήση του συνώνυμη με την παραβατικότητα.

Αν κάποιος hacker αποκτήσει πρόσβαση στο ψηφιακό μας πορτοφόλι και κλέψει τα Bitcoin που βρίσκονται σε αυτό, δεν θα μπορούμε να τα ανακτήσουμε σε αντίθεση με τις τράπεζες όπου φροντίζουν την αποζημίωση των πελατών τους σε περίπτωση που πέσουν θύματα επιθέσεων από hackers.

Έναν άλλο προβληματισμό αποτελεί η αμοιβή που λαμβάνουν οι εξορύχιοι για τη συμμετοχή τους στη διαδικασία της εξορύξης. Η αμοιβή τους αποτελείται από τα νέα Bitcoin που κυκλοφορούν στην αγορά ανά 10 λεπτά καθώς και από τα κόστη των συναλλαγών που εγκρίνουν. Η αμοιβή από τη δημιουργία νέων Bitcoin μειώνεται συνεχώς επειδή όπως έχει ήδη αναφερθεί, σύμφωνα με το πρωτόκολλο ο ρυθμός των νέων Bitcoin που βγαί-

νουν στην αγορά υποδιπλασιάζεται ανά 4 χρόνια. Αν τα κόστη συναλλαγών αυξηθούν θα γίνει λιγότερο ελκυστική η χρήση του Bitcoin, ενώ αν δεν αυξηθούν, όλο και λιγότεροι εξορύχιοι θα βρίσκουν τη διαδικασία της εξορύξης δελεαστική στο μέλλον επειδή δεν θα μπορούν να καλύψουν τα κόστη τους (π.χ. το κόστος για το ηλεκτρικό ρεύμα). Κάτι τέτοιο θα μπορούσε να θέσει την ασφάλεια όλου του Bitcoin δικτύου σε ρίσκο αφού οι εξορύχιοι θα είναι όλο και λιγότεροι, το δικτυο δεν θα είναι πια αποκεντροποιημένο αλλά θα εξαρτάται αποκλειστικά στους λίγους εναπομείναντες εξορύχους και αυτό θα κάνει το δικτυο πιο επιρρεπής στις επιθέσεις από hackers.

Όπως έχουμε αναφέρει το Bitcoin αποτελεί και δικτυο, οπότε είναι σημαντικό να εξετάσουμε τη δομή του για να βγάλουμε συμπεράσματα για το πόσο εφικτή είναι διαχρονικά η ομαλή λειτουργία, αλλά και η επέκτασή του στο μέλλον. Το Bitcoin δικτυο χρησιμοποιεί λογισμικό ανοικτού κώδικα και προσφέρει ευελιξία στους προγραμματιστές να αντιμετωπίσουν πιθανά προβλήματα που ίσως προκύψουν, αλλά ήδη υπάρχουν κάποια που προβληματίζουν.

Ο όγκος των Bitcoin συναλλαγών αυξάνεται συνεχώς από χρονιά σε χρονιά και ένα δυνητικό πρόβλημα είναι η δυνατότητα κλιμάκωσης της χρήσης του Bitcoin. Το μέγεθος του κάθε block που δημιουργείται ανά 10 λεπτά, είναι σχεδιασμένο ώστε να μπορεί να εμπεριέχει δεδομένα χωρητικότητας μέχρι 1 MB. Αυτό επιτρέπει στο δικτυο να επεξεργάζονται μόλις 7 συναλλαγές το δευτερόλεπτο σε αντίθεση με το δικτυο της Visa το οποίο μπορεί να επεξεργάζεται μέχρι και 65.000 συναλλαγές το δευτερόλεπτο.<sup>6</sup>

Αν διατηρηθεί ίδιο το μέγεθος των blocks, θα προταθούν νέα υψηλότερα κόστη συναλλαγών και θα δίνεται μεγαλύτερο κίνητρο στους εξορύχους να συμμετάσχουν στην διαδικασία της εξορύξης. Τα υψηλότερα κόστη συναλλαγών θα αντιμετωπίσουν το παραπάνω πρόβλημα που αναφέραμε για τις αμοιβές των εξορύχων, αλλά ίσως τότε πολλοί χρήστες να βρίσκουν την αποστολή Bitcoin ακριβή. Από την άλλη μεριά, αν αυξηθεί το μέγεθος των blocks, θα χαθεί η αποκεντροποιημένη φύση του Bitcoin από μεγάλες εταιρείες τεχνολογίας (για τεχνικούς λόγους που δεν θα αναλύσουμε-running full nodes).

Ο ψηφιακός κόσμος εγκυμονεί κινδύνους αυθεντικότητας των προϊόντων και υπηρεσιών που βρίσκονται σε αυτόν και αντίστοιχα στη περίπτωση του Bitcoin υπάρχουν πολλών ειδών απάτες, τόσο από κάποια ανταλλα-

6. <http://www.forbes.com/sites/laurashin/2015/12/28/should-you-invest-in-bitcoin-10-arguments-against-as-of-december-2015/#47ef8fe05466>



**ΔΙΑΓΡΑΜΜΑ 1: Η ΠΟΡΕΙΑ ΤΩΝ ΤΙΜΩΝ ΤΟΥ ΔΕΙΚΤΗ ΤΟΥ BITCOIN ΚΑΙ ΤΑ ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΓΕΓΟΝΟΤΑ ΠΟΥ ΤΟΝ ΕΠΗΡΕΑΣΑΝ**



\*Οι τιμές του δείκτη του Bitcoin υπολογίζονται ως ο μέσος όρος των ημεθικών τιμών ανταλλακτηρίου ανάμεσα σε XBP/USD και XBP/CNY (XBP=Bitcoin Price Index). Τα δεδομένα αντλήθηκαν από την ιστοσελίδα: [www.coindesk.com](http://www.coindesk.com)

**1) Το bail-in της Κύπρου – 25/03/2013**

Το Eurogroup, η Ευρωπαϊκή Επιτροπή, η Ευρωπαϊκή Κεντρική Τράπεζα και το Διεθνές Νομισματικό Ταμείο ελπίζουν ότι τα 10 δισ. ευρώ bail-out θα ενισχύσουν την εξασθενημένη Κυπριακή οικονομία. Ανάμεσα στους όρους για την Κυπριακή οικονομία είναι και μια υπερμεγέθης φορολόγηση και κούρεμα καταθέσεων από τους περισσότερους τραπεζικούς λογαριασμούς με πάνω από 100.000€. Αυτό αποτέλεσε σοβαρή ανησυχία όχι μόνο για τους πλούσιους Κύπριους αλλά και για πολλούς διεθνείς επενδυτές (κυρίως τους Ρώσους) γιατί η Κύπρος ήταν ένα από τα πιο δημοφιλή φορολογικά καταφύγια στον κόσμο. Πρωτού αρχίσουν να ισχύουν τα μέτρα του bail-in, πολλοί από αυτούς τους κατόχους λογαριασμών άρχισαν να αγοράζουν μαζικά Bitcoin οδηγώντας την τιμή του από \$80 σε πάνω από \$220.

**2) Ο αυξημένος όγκος συναλλαγών “έριξε” το Mt.Gox – 10/04/2013**

Αρχικά πίστευαν ότι ήταν μια διαδικτυακή επίθεση στο μεγαλύτερο ανταλλακτήριο bitcoin ώστε να καταστήσουν την υπηρεσία ανίκανη να δεχτεί τις εντολές των πελατών της (κατανεμημένη επίθεση άρνησης εξυπηρέτησης – DDoS attack), ενώ ο λόγος που οι συναλλαγές δεν εκπληρωνόντουσαν και καταβλήθηκαν οι εξυπηρετητές (servers) του Mt.Gox ήταν η μεγάλη εισοδηματική εμπορία (traders) εξαιτίας του bail-in της Κύπρου. Κερδοσκοπικές ανησυχίες για το πρόβλημα που παρουσίασε το Mt.Gox ανταλλακτήριο οδήγησαν σε ένα πανικό πωλητήματος οδηγώντας τις τιμές χαμηλά.

**3) Σύλληψη του Dread Pirate Roberts – 01/10/2013**

Το Αμερικανικό ομοσπονδιακό γραφείο έρευνας εντοπίζει τον ιδιοκτήτη της διαδικτυακής πλατφόρμας Silk Road (Ross Ulbricht) η οποία διακινούσε διαδικτυακά παράνομα ναρκωτικά. Το FBI συνέλαβε τελικά τον Ross Ulbricht για εμπόριο ναρκωτικών, hacking υπολογιστών και ξέπλυμα χρήματος. Έγινε στα 30.000 BTC που ήταν ιδιοκτησία του Silk Road και 144.000 BTC που ήταν ιδιοκτησία του Ross Ulbricht κατασχέθηκαν.

**4) Η κεντρική τράπεζα της Κίνας People’s Bank of China, εγκρίνει το Bitcoin – 20/11/2013**

Η είδηση αυτή αποτέλεσε μέσο ενεργοποίησης του Bitcoin στην αγορά της Κίνας και όχι μόνο, με τον όγκο

συναλλαγών στο ανταλλακτήριο BTC China να ανεβαίνει ραγδαία. Να σημειωθεί ότι η κεντρική τράπεζα της Κίνας People’s Bank of China είναι η δεύτερη παγκοσμίως κεντρική τράπεζα σε συνολικά περιουσιακά στοιχεία.

**5) Καταγράφεται η μεγαλύτερη ισοτιμία συναλλάγματος για το Bitcoin στο Mt.Gox ανταλλακτήριο, με το 1BTC να ισούται με 1.242USD – 29/11/2013**

Η αυξημένη αγορά Bitcoin από τη Κίνα οδήγηε σταθερά τις τιμές όλο και πιο ψηλά φτάνοντας τη κορυφή στις 29 Νοεμβρίου του 2013. Η ελευθερία που προσδίδει το Bitcoin για την μεταφορά χρημάτων πέρα των συνόρων μιας χώρας, έκαναν το Bitcoin ελκυστικό για τους Κινέζους πολίτες που αναζητούσαν μια εναλλακτική λύση για να αποφύγουν την διαρκή υποτίμηση που είχε υποστεί το επίσημο νόμισμα τους, Renminbi.

**6) Η Κινέζικη κυβέρνηση απαγορεύει στα χρηματοπιστωτικά ιδρύματα να χρησιμοποιούν το Bitcoin – 05/12/2013**

Η κεντρική τράπεζα People’s Bank of China ανακηρύσσει ότι η καινοτόμα εφεύρεση του Nakamoto δεν αποτελεί νόμισμα. Η αλλαγή πολιτικής απαγορεύει σε οποιοδήποτε χρηματοπιστωτικό ίδρυμα να κάνει οποιοδήποτε είδους συναλλαγές σε Bitcoin. Τις επόμενες εβδομάδες περισσότεροι περιορισμοί, πνίγουν σιγά σιγά τις Κινέζικες αγορές κρυπτονομισμάτων και οι τιμές τους αρχίζουν να πέφτουν δραματικά σε όλη την υφήλιο.

**7) Τα μεγαλύτερα ανταλλακτήρια προσβάλλονται από διαδικτυακές κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS attacks) – 07/02/2014**

Τα ανταλλακτήρια Mt.Gox, Bitstamp και BTC-e έπαυσαν τις συναλλαγές εξαιτίας μαζικών DDoS επιθέσεων. Το Mt.Gox ανταλλακτήριο έπαυσε τις συναλλαγές του πρώτο και είχε σαν αποτέλεσμα μια απότομη πτώση στη τιμή του Bitcoin.

**8) Το ανταλλακτήριο Mt.Gox κλείνει – 24/02/2014**

Μετά από την απότομη πτώση των αναλήψεων στις 6 Φεβρουαρίου του 2014, η ιστοσελίδα του Mt.Gox καταργείται χωρίς κάποιο επίσημο σχόλιο και έρευνες έδειξαν αργότερα ότι έλειπαν από την εταιρεία 744.000BTC. Το Mt.Gox ανταλλακτήριο ισχυρίζεται ότι ένας hacker ευθυνόταν για αυτή την απώλεια.

**9) Η Εσωτερική Υπηρεσία Εσόδων της Αμερικής ανακηρύσσει τη φορολόγηση του Bitcoin σαν ιδιοκτησία – 26/03/2014**

Το έγγραφο πολιτικής της Εσωτερικής Υπηρεσίας Εσόδων ανακηρύσσει τη φορολόγηση του Bitcoin σαν ιδιοκτησία (όχι σαν νόμισμα) και ως εκ τούτου ως υποκείμενο φορολόγησης εσόδων.

**10) Η πίσνα εξόρυξης Ghash.io μαζεύει το 51% σε δύναμη εξόρυξης – 13/06/2014**

Η πίσνα Ghash.io απέκτησε αρκετή δύναμη εξόρυξης (υπολογιστική δύναμη να παράγει hashes) και θα μπορούσε να επιτεθεί στο Bitcoin δίκτυο, δημιουργώντας προβλήματα αξιοπιστίας και λειτουργικότητας στο θεσμό του Bitcoin (DDoS attacks, double spending problem). Τελικά η Ghash.io δεν το έκανε και δήλωσε ξεκάθαρα ότι δεν θα συμμετάσχει ποτέ σε μια τέτοια διαδικτυακή επίθεση και υποχρέωσε κάποιους εξορύκτες να συμμετάσχουν σε άλλες πιάνες εξόρυξης, μειώνοντας με αυτό τον τρόπο την δύναμη εξόρυξης της στο 39,99% έτσι ώστε να λυθεί αυτό το πρόβλημα.

**11) Το ανταλλακτήριο Bitstamp δέχεται επίθεση από hackers – 04/01/2015**

Άγνωστοι hackers έκλεψαν 18.866 bitcoins αξίας περίπου 5,2 εκατομμυρίων δολαρίων από το Bitstamp ανταλλακτήριο. Το Bitstamp έκλεισε αμέσως για 8 μέρες όταν ανακαλύφτηκε το ρήγμα στην ασφάλεια του συστήματός του, για να ελεγχθούν τα συστήματά του και να ξαναφτιάσουν τη πλατφόρμα συναλλαγών. Η κλοπή αυτή ήταν ένα μικρό μέρος των αποθεμάτων του Bitstamp σε Bitcoin και κανένας λογαριασμός πελάτη δεν θίχτηκε από το γεγονός, αν και η ζημιά στη φήμη της εταιρείας και στην εμπιστοσύνη των πελατών ήταν μεγαλύτερη από τη χρηματική απώλεια σε Bitcoin.

**12) Η Ευρωπαϊκή Ένωση ανακηρύσσει ότι δεν θα υπάρχει ΦΠΑ στις συναλλαγές με Bitcoin – 22/10/2015**

Το Ευρωπαϊκό Δικαστήριο έκρινε ότι το συναλλάγμα σε Bitcoin και σε άλλα ψηφιακά νομίσματα, δεν θα φορολογείται με ΦΠΑ στην Ευρωπαϊκή Ένωση. Οι ενέργειες αυτές, κατατάσσουν το Bitcoin και τα άλλα κρυπτονομίσματα σε συναλλάγμα αντί για εμπόρευμα. Στην Αμερική σε αντίθεση, το Bitcoin κατατάσσεται και σαν συναλλάγμα και ως εμπόρευμα.

κτήρια που δεν επιστρέφουν τα χρήματα που έχουν καταθέσει οι επενδυτές σε αυτά, όσο και από διάφορες εταιρείες οι οποίες υπόσχονται υψηλές εγγυημένες αποδόσεις αν επενδύσετε τα Bitcoin σας σε αυτές. Οι εταιρείες αυτού του είδους λειτουργούν με βάση το σχήμα Πόντσι (Ponzi scheme) σύμφωνα με το οποίο οι παλαιότεροι επενδυτές πληρώνονται από τα κεφάλαια των μεταγενέστερων επενδυτών. Όταν δεν θα υπάρχουν νέοι επενδυτές το σχέδιο αποπληρωμής καταρρέει.

Όλοι οι παραπάνω κίνδυνοι, η πιθανή ανακάλυψη ενός καλύτερου ψηφιακού νομίσματος, καθώς και η υψηλή μεταβλητότητα των τιμών του Bitcoin, το καθιστούν ως μια από τις πιο ριψοκίνδυνες επενδύσεις που προσφέρει όμως ιδιαίτερα υψηλές αποδόσεις.

Σύμφωνα με το γραφείο χρηματοπιστωτικής προστασίας των καταναλωτών (Consumer Financial Protection Bureau), η τιμή του Bitcoin σημείωσε 61% πτώση μέσα σε μια μέρα του 2013, ενώ τα κακά νέα που ανακοινώθηκαν το 2014 για το ανταλλακτήριο Mt.Gox, προκάλεσαν πτώση της τιμής του Bitcoin γύρω στο 80% για λίγα μόλις δευτερόλεπτα.

Αναμφίβολα μιλάμε για ένα καινοτόμο κρυπτονόμισμα με πολλά πλεονεκτήματα, αλλά πριν αποφασίσετε να επενδύσετε σε αυτό πρέπει να λάβετε υπ όψιν σας τους ανωτέρω κινδύνους, ορισμένοι εκ των οποίων σύντομα θα εξαλειφθούν.

## V. Η διαχρονική πορεία του Bitcoin

Στο **Διάγραμμα 1** απεικονίζεται η πορεία των τιμών του δείκτη του Bitcoin (Bitcoin Price Index) για την περίοδο 18/07/2010 - 31/01/2016, καθώς και τα σημαντικότερα γεγονότα που τον επηρέασαν θετικά ή αρνητικά.

### REFERENCES

- Φίλιππας Ν., Ρούκας Μ., Πειραιάς 2016, Τιμητικός τόμος για τον ομότιμο Καθηγητή του Πανεπιστημίου Πειραιώς Οικονομού Γ.
- Dwyer G., 2015. The economics of Bitcoin and similar private digital currencies, Journal of Financial Stability, 17, 81-91
- Nakamoto S., no date. Bitcoin: A Peer-to-peer Electronic Cash System, Unpublished paper available at: <http://bitcoing.org/bitcoin.pdf>
- Pekas N., 2013, November. Country Rankings by Relative Bitcoin Adoption. <http://nikola.pekas.org/wpo/science-technology/bitcoin/comparison-of-bitcoin-adoption-rates-across-the-world-december-2013/>
- Yermack, D., 2013. Is Bitcoin a Real Currency? An Economic Appraisal. Technical Report. National Bureau of Economic Research.
- Weber, B., 2014. Bitcoin and the legitimacy crisis of money. Cambridge Journal of Economics, <http://dx.doi.org/10.1093/cje/beuo67>.

## VI. Συμπεράσματα

Παρά το γεγονός ότι υπάρχει ανησυχία για την μακροπρόθεσμη πορεία του Bitcoin, φαίνεται ότι την ίδια στιγμή η τεχνολογία που χρησιμοποιεί είναι η βάση του μέλλοντος για τα νομίσματα της νέας ψηφιακής εποχής.

Εξειδικευμένες εταιρείες χρηματοοικονομικών υπηρεσιών σχεδιάζουν να αφομοιώσουν τη τεχνολογία των blocks σαν ένα μητρώο για το ποιος κατέχει τι, αντί για μια σειρά από εσωτερικά λογιστικά βιβλία, το οποίο θα τους δώσει πιο αποτελεσματικές πρακτικές και εξοικονόμηση κόστους. Πιο συγκεκριμένα η ισπανική τράπεζα Santander υπολογίζει ότι η χρήση της τεχνολογίας των blocks θα μπορούσε να εξοικονομήσει στις τράπεζες μέχρι και 20 δισεκατομμύρια δολάρια το χρόνο έως το 2022.<sup>7</sup>

Η κυκλοφορία ψηφιακών νομισμάτων προσφέρει πολλά πλεονεκτήματα, αλλά θα μπορούσαμε να πούμε πως ακόμα είναι σε πειραματικό στάδιο καθώς υπάρχουν αρκετά προβλήματα που πρέπει να επιλυθούν. Για παράδειγμα, ο τρόπος λειτουργίας του Bitcoin δικτύου έχει βελτιωθεί σε αρκετούς τομείς αλλά χρειάζονται περαιτέρω αναβαθμίσεις, όπως επίσης ότι η ασφάλεια των ανταλλακτηρίων πρέπει να γίνει απόρθητη από τις επιθέσεις των hackers.

Οι αλυσίδες των blocks μπορούν να έχουν εναλλακτικές χρήσεις επειδή ικανοποιούν τα κριτήρια για την διατήρηση ενός αξιόπιστου μητρώου συναλλαγών, το οποίο είναι πολύ σημαντικό για συναλλαγές οποιουδήποτε είδους. Μια ιδέα για παράδειγμα είναι να φτιαχτούν φτηνές σε κόστος κατασκευής, απαραβίαστες και δημόσιες βάσεις δεδομένων π.χ. για τα υποθηκοφυλάκεια (η Ονδούρα και η Ελλάδα ενδιαφέρονται για αυτό).<sup>8</sup>

**Η blockchain τεχνολογία θα επιφέρει στους οργανισμούς που θα την χρησιμοποιήσουν, διαφάνεια, αξιοπιστία, και συνεχή επίβλεψη για την αυθεντικότητα των μητρώων συναλλαγών οποιουδήποτε είδους, με πολύ μικρότερο κόστος και αδιαμφισβήτητα μπορούμε να πούμε ότι μιλάμε για μια τεχνολογία όπου έχει την δυνατότητα να αλλάξει το τρόπο με τον οποίο οι άνθρωποι και οι επιχειρήσεις θα συνεργάζονται στο άμεσο μέλλον. Το bitcoin φαίνεται ότι ήρθε για να μείνει!**

7. <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

8. <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>.