



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΚΑΙΟ ΤΟΥ BLOCKCHAIN

Χρυσάνθη-Νεκταρία Γεωργάκη

Μεσολόγγι 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΚΑΙΟ ΤΟΥ BLOCKCHAIN

Χρυσάνθη-Νεκταρία Γεωργάκη

Επιβλέπων καθηγητής

Αντώνιος Μανιάτης

Μεσολόγγι 2020

UNIVERSITY OF PATRAS

SCHOOL OF ECONOMICS & BUSINESS

DEPARTMENT OF MANAGEMENT SCIENCE AND
TECHNOLOGY

**FORMER DEPARTMENT OF BUSINESS
ADMINISTRATION AT MESSOLONGHI**

THESIS

BLOCKCHAIN LAW

Chrysanthi-Nektaria Georgaki

Messolonghi 2020

ΕΥΧΑΡΙΣΤΙΕΣ

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου , κύριο Αντώνη Μανιάτη για την καθοδήγηση και τις ουσιώδεις συμβουλές που μου πρόσφερε καθ' όλη την διάρκεια της πτυχιακής μου εργασίας. Επίσης θα ήθελα ειλικρινά να ευχαριστήσω θερμά την οικογένεια μου για την συνεχή υποστήριξη τους και όλους αυτούς που ήταν δίπλα μου σε αυτή την προσπάθεια και έρευνα.

Πνευματικά δικαιώματα

Copyright © Πανεπιστήμιο Πατρών. Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1988 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον.

Χρυσάνθη-Νεκταρία Γεωργάκη, 2020

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Πανεπιστημίου Πατρών δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΠΕΡΙΛΗΨΗ

Ο ενθουσιασμός ο οποίος έχει δημιουργηθεί τα τελευταία χρόνια γύρω από το blockchain είναι πολύ μεγάλος. Η τεχνολογία αυτή γεννήθηκε όπως όλοι γνωρίζουμε στο διαδίκτυο. Έτσι σε λιγότερο από μια δεκαετία, η αρχική «λευκή βίβλος» του Bitcoin μετατράπηκε σε ένα πλούσιο, λειτουργικό, οικοσύστημα τεχνολογίας από τη βάση προς τα πάνω, από μια ταχέως αναπτυσσόμενη ομάδα τεχνολόγων, επενδυτών και επιχειρηματιών. Οι καινοτομίες που έρχονται διαρκώς στην επιφάνεια και συγκεκριμένα, η τεχνολογία αλυσίδας συστοιχιών (Blockchain) ενδέχεται να προκαλέσουν μεγάλες αλλαγές στον τρόπο λειτουργίας του παραδοσιακού χρηματοοικονομικού συστήματος και γενικότερα του τρόπου παροχής των υπηρεσιών. Ο κόσμος των “Fintech” (*Financial Technologies*) λοιπόν, εξελίσσεται διαρκώς καθοδηγούμενος από τις εκάστοτε τεχνολογικές αλλαγές, οι οποίες υπόσχονται να επιφέρουν μείωση του κόστους και του χρόνου ολοκλήρωσης των χρηματοοικονομικών συναλλαγών, την αλλαγή στις προσδοκίες των καταναλωτών που επιθυμούν τη ψηφιοποίηση του τρόπου παροχής των υπηρεσιών τους, τη διαθεσιμότητα κεφαλαίων προς επένδυση στις νέες τεχνολογίες που έχουν ως αντικείμενο τον χρηματοοικονομικό τομέα και τέλος, την αυξανόμενη υποστήριξη από τα κράτη και τις ρυθμιστικές αρχές προς την εφαρμογή των αλλαγών αυτών.

Η τεχνολογία blockchain προσπαθεί να οικοδομήσει μια αποκεντρωμένη, διαμεσολαβημένη και κατανεμημένη τεχνολογία, η οποία επιτρέπει αποκεντρωμένους, διαμεσολαβημένους και κατανεμημένους τρόπους κοινωνικού συντονισμού με έναν κατά κύριο λόγο αποκεντρωμένο, διαμεσολαβημένο και κατανεμημένο τρόπο. Αυτή η συνάφεια μεταξύ του σχεδιασμού της τεχνολογίας, του τρόπου ανάπτυξής της και των δηλωμένων στόχων της είναι το ισχυρότερο επιχείρημα υπέρ της σοβαρής αντιμετώπισης της τεχνολογίας blockchain. Εξηγεί γιατί, παρά όλες τις πιθανές παγίδες, το έργο της αξιολόγησης του κοινωνικού, οικονομικού και πολιτικού αντίκτυπου της τεχνολογίας πρέπει να αναληφθεί από τους ερευνητές.

Αντικείμενο της εργασίας αυτής είναι η μελέτη της τεχνολογίας blockchain με έμφαση στη νομοθεσία αυτής και στους νομικούς περιορισμούς που υπάρχουν προκειμένου η τεχνολογία αυτή να είναι τόσο επικερδής για τους επενδυτές αλλά και σύννομη.

Η εργασία αποτελείται από πέντε κεφάλαια κάθε ένα εκ των οποίων αντιμετωπίζει και από μια διαφορετική οπτική το υπό εξέταση θέμα. Ειδικότερα, στο πρώτο κεφάλαιο

γίνεται μια εισαγωγή στην έννοια των κρυπτονομισμάτων και στη τεχνολογία blockchain. Στη συνέχεια στο δεύτερο κεφάλαιο παρουσιάζεται το πώς γίνεται η παραγωγή κρυπτονομίσματος και η κοστολόγηση αυτού. Επίσης στο τρίτο κεφάλαιο της εργασίας παρουσιάζονται διάφορα νομικά ζητήματα σχετικά με την τεχνολογία blockchain και τις ιδιαιτερότητες που αυτή παρουσιάζει.

Στο τέταρτο κεφάλαιο αναλύονται οι έννοιες της ψηφιακής χρηματοδότησης, της ψηφιακής ένταξης και ακόμη οι έξυπνες συμβάσεις (smart contracts). Η επίδραση των νέων ψηφιακών τεχνολογιών στον χρηματοπιστωτικό τομέα είναι ιδιαίτερα ισχυρή και με τη βοήθεια τους μετασχηματίζεται όλο το οικονομικό σύστημα έτσι ώστε να αυξηθεί η πρόσβαση σε χρηματοοικονομικά προϊόντα και υπηρεσίες και να δοθεί ώθηση στην οικονομική ανάπτυξη των χωρών.

Τέλος, στο πέμπτο κεφάλαιο αναλύεται το δίκαιο του blockchain, το δίκαιο του «ξεπλύματος χρημάτων» καθώς και η διαδικασίες μέσω των οποίων κάποιοι χρήστες του διαδικτύου επιχειρούν να νομιμοποιήσουν χρήμα από παράνομες δραστηριότητες μέσω της τεχνολογίας αυτής.

Λέξεις Κλειδιά: blockchain, κρυπτονόμισμα, τεχνολογία, νομοθεσία, δίκαιο

ABSTRACT

The excitement that has been created around blockchain in recent years is very high. This technology was born as we all know on the internet. In less than a decade, Bitcoin's original "white paper" has been transformed into a rich, functional, bottom-up technology ecosystem by a rapidly growing team of technologists, investors and entrepreneurs.

The innovations that are constantly coming to the surface, and in particular, the blockchain technology (Blockchain) may cause major changes in the way the traditional financial system works and in the way services are provided in general. The world of "Fintech" (Financial Technologies) is constantly evolving, guided by the current technological changes, which promise to reduce the cost and completion time of financial transactions, the change in the expectations of consumers who want to digitize the way of delivery the availability of funds to invest in new technologies in the financial sector and, finally, the growing support from states and regulators for the implementation of these changes.

Blockchain technology seeks to build a decentralized, mediated, and distributed technology that enables decentralized, mediated, and distributed ways of social coordination in a predominantly decentralized, mediated, and distributed manner. This connection between the design of the technology, the way it is developed and its stated goals is the strongest argument in favor of taking blockchain technology seriously. It explains why, despite all the potential pitfalls, the task of assessing the social, economic and political impact of technology must be undertaken by researchers.

The object of this work is the study of blockchain technology with emphasis on its legislation and the legal restrictions that exist in order for this technology to be both profitable for investors and legal.

The work consists of five chapters, each of which deals with the subject in question from a different perspective. In particular, the first chapter introduces the concept of cryptocurrencies and blockchain technology. Then in the second chapter is presented how the production of cryptocurrency and its costing is done. Also in the third chapter

of the work are presented various legal issues related to blockchain technology and its peculiarities.

The fourth chapter analyzes the concepts of digital financing, digital inclusion and even smart contracts. The impact of new digital technologies on the financial sector is particularly strong and with their help the whole economic system is being transformed in order to increase access to financial products and services and to boost the economic development of countries.

Finally, the fifth chapter analyzes the law of blockchain, the law of "money laundering" as well as the procedures through which some internet users try to launder money from illegal activities through this technology.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

| | |
|---|----|
| ΠΕΡΙΛΗΨΗ..... | 6 |
| ΕΙΣΑΓΩΓΗ..... | 12 |
| ΚΕΦΑΛΑΙΟ 1ο: ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN | 13 |
| 1.1 Έννοια - ορισμός | 13 |
| 1.2 Η χρησιμότητα των κρυπτονομισμάτων | 14 |
| 1.3 Η λειτουργία των κρυπτονομισμάτων | 17 |
| 1.4 Ζητήματα ασφάλειας και κίνδυνοι από τη χρήση κρυπτονομισμάτων | 19 |
| 1.5 Η δημιουργία του Bitcoin..... | 22 |
| 1.6 Οι λόγοι της διεύρυνσης της χρήσης του Bitcoin | 23 |
| 1.7 Η μελλοντική εξέλιξη των κρυπτονομισμάτων..... | 26 |
| ΚΕΦΑΛΑΙΟ 2ο: Η ΠΑΡΑΓΩΓΗ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΟΣ ΚΑΙ Η ΚΟΣΤΟΛΟΓΗΣΗ ΑΥΤΟΥ | 29 |
| 2.1 Η χρήση του κρυπτονομίσματος | 29 |
| 2.2 Τρόποι απόκτησης του κρυπτονομίσματος | 40 |
| 2.3 Η παραγωγή του κρυπτονομίσματος..... | 41 |
| 2.4 Το κόστος της παραγωγής του κρυπτονομίσματος | 48 |
| ΚΕΦΑΛΑΙΟ 3ο: ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN | 50 |
| 3.1 Η τεχνολογία blockchain | 50 |
| 3.2 Νομικοί περιορισμοί..... | 52 |
| 3.3 Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων (GDPR) και πως συνδέεται με το blockchain | 54 |
| 3.3.1 Τι ορίζονται ως προσωπικά δεδομένα..... | 54 |

| | |
|--|----|
| 3.3.2 Οι αρχές του GDPR..... | 55 |
| 3.3.3 Τα δικαιώματα των χρηστών του διαδικτύου με το GDPR | 56 |
| 3.3.4 Οι προκλήσεις σχετικά με το GDPR και οι καινοτομίες του κανονισμού..... | 57 |
| 3.3.4.1 Η ασφάλεια των προσωπικών δεδομένων..... | 57 |
| 3.3.4.2 Το δικαίωμα της διαγραφής δεδομένων | 58 |
| 3.3.4.3 Οι βασικές καινοτομίες του Κανονισμού..... | 58 |
| 3.4 Η νομοθεσία σχετικά με το GDPR (Νόμος 4624 / 2019) | 60 |
| ΚΕΦΑΛΑΙΟ 4: ΨΗΦΙΑΚΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗ , ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΕΝΤΑΞΗ ΚΑΙ ΕΞΥΠΝΕΣ ΣΥΜΒΑΣΕΙΣ..... | 63 |
| 4.1 Ψηφιακή χρηματοδότηση και ψηφιακά νομίσματα | 63 |
| 4.2 Η έννοια της χρηματοοικονομικής ένταξης | 64 |
| 4.3 Οι έξυπνες συμβάσεις (smart contracts)..... | 65 |
| 4.4 Λύσεις για την καλύτερη εφαρμογή των έξυπνων συμβάσεων | 69 |
| ΚΕΦΑΛΑΙΟ 5: ΤΟ ΔΙΚΑΙΟ ΤΟΥ BLOCKCHAIN ΚΑΙ ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΞΕΠΛΥΜΑΤΟΣ ΧΡΗΜΑΤΩΝ..... | 71 |
| 5.1 Οι ρυθμίσεις του Blockchain..... | 71 |
| 5.2 Το δίκαιο του Blockchain..... | 75 |
| 5.3 Ξέπλυμα χρήματος μέσω της χρήσης της τεχνολογίας Blockchain..... | 78 |
| 5.4 Το δίκαιο του Blockchain σε σύγκριση με το δίκαιο του διαδικτύου..... | 80 |
| ΣΥΜΠΕΡΑΣΜΑΤΑ..... | 82 |
| ΒΙΒΛΙΟΓΡΑΦΙΑ..... | 84 |

ΕΙΣΑΓΩΓΗ

Αντικείμενο της εργασίας αυτής είναι η μελέτη της τεχνολογίας blockchain με έμφαση στη νομοθεσία αυτής και στους νομικούς περιορισμούς που υπάρχουν προκειμένου η τεχνολογία αυτή να είναι τόσο επικερδής για τους επενδυτές αλλά και σύννομη.

Ξεκινώντας τη μελέτη του θέματος αξίζει να τονιστεί ότι τα blockchains είναι διαμεσολαβημένα και διακρατικά δίκτυα, συχνά βασίζονται σε πρωτόκολλα λογισμικού ανοιχτού κώδικα. Δεύτερον, είναι ανθεκτικά σε παραβιάσεις, λόγω της κατακερματισμένης φύσης τους, των μηχανισμών συναίνεσης που χρησιμοποιούνται και της χρήσης κατακερματισμού. Τρίτον, η τεχνολογία blockchain είναι διαφανής - υπό την έννοια ότι τα δεδομένα συναλλαγών είναι αυθεντικά και ορατά - και τα δεδομένα που περιέχουν δεν είναι αξιόπιστα (λόγω της χρήσης κρυπτογραφίας δημόσιου-ιδιωτικού κλειδιού). Τέταρτον, τα συστήματα blockchain χαρακτηρίζονται από ψευδώνυμο, καθώς επιτρέπουν στα συμβαλλόμενα μέρη να συμμετέχουν στο σύστημα χωρίς να αποκαλύπτουν την ταυτότητά τους. Πέμπτον, τα blockchain έχουν συγκεκριμένα κίνητρα και δομές κόστους, π.χ. αποκλεισμός ανταμοιβών και εξόρυξης εξόδων που ενθαρρύνουν και αποζημιώνουν τα μέρη που διατηρούν ένα δίκτυο που βασίζεται σε blockchain. Ένα έκτο μοναδικό χαρακτηριστικό είναι η ανάπτυξη μηχανισμών συναίνεσης για τον συντονισμό της κοινωνικής δραστηριότητας προς μια συμφωνία για την κατάσταση των πραγμάτων στο σύστημα. Έβδομο, και σε βαθύτερο επίπεδο, τα blockchains επιτρέπουν έναν συγκεκριμένο τύπο «αυτονομίας»: διευκολύνουν την εκτέλεση κώδικα λογισμικού που είναι εντελώς ανεξάρτητος από οποιοδήποτε μέρος.

Ο συνδυασμός αυτών των χαρακτηριστικών οδηγεί στην παρατήρηση ότι τα blockchain έχουν διπλή φύση, που σημαίνει ότι έχουν τη δυνατότητα να χρησιμοποιηθούν για νόμιμους και παράνομους σκοπούς.

Η εργασία αυτή αποτελείται από 5 κεφάλαια κάθε ένα εκ των οποίων μελετάει και από μια διαφορετική οπτική το συγκεκριμένο θέμα.

ΚΕΦΑΛΑΙΟ 1ο: ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

1.1 Έννοια - ορισμός

Το κρυπτονόμισμα είναι μια μέθοδος πληρωμής που υπάρχει μόνο σε ηλεκτρονική μορφή και δεν είναι απτή. Το κρυπτονόμισμα μπορεί να μεταφερθεί μεταξύ φορέων ή χρηστών με τη βοήθεια τεχνολογίας όπως οι υπολογιστές, τα smartphones και το Διαδίκτυο. Παρόλο που είναι παρόμοιο με τα φυσικά νομίσματα, το κρυπτονόμισμα επιτρέπει τη μεταφορά χωρίς περιθώρια ιδιοκτησίας καθώς και τις στιγμιαίες συναλλαγές. Τα κρυπτονομίσματα μπορούν να χρησιμοποιηθούν για την αγορά αγαθών και υπηρεσιών, αλλά μπορούν επίσης να περιοριστούν σε ορισμένες διαδικτυακές κοινότητες όπως ένα gaming ή κοινωνικά δίκτυα. Το κρυπτονόμισμα είναι επίσης γνωστό ως ψηφιακό χρήμα και cybercash¹.

Το κρυπτονόμισμα έχει επί του παρόντος μόνο περιορισμένη βάση χρηστών και το κανονιστικό πλαίσιο καθώς και οι φορολογικές επεξεργασίες των ψηφιακών νομισμάτων εξακολουθούν να εξελίσσονται. Η υποδομή που απαιτείται για τη στήριξη του κρυπτονομίσματος εξακολουθεί να καθορίζεται και να αναπτύσσεται. Οι κρυπτοεμβολές και τα εικονικά νομίσματα είναι κατηγορίες κρυπτονομισμάτων. Δεδομένου ότι οι πληρωμές πραγματοποιούνται απευθείας μεταξύ πληρωτών και δικαιούχων, τα κρυπτονομίσματα μπορούν να εξαλείψουν τους μεσάζοντες, να επεξεργαστούν τα βήματα και τις δαπάνες που συνδέονται με την υποδομή, σε αντίθεση με τις παραδοσιακές μεθόδους πληρωμής, οι οποίες δεν μπορούν να παρακάμψουν τις τράπεζες ή τους εκκαθαριστικούς οίκους. Μπορεί επίσης να βοηθήσει στην απλούστερη και πιο διαφανή ροή των κεφαλαίων.

¹ Grinberg R., (2012), Bitcoin: An innovative alternative digital currency, Hein Online

Υπάρχουν πολλά οφέλη που συνδέονται με τα κρυπτονομίσματα, όπως η δυνατότητα εύκολης πραγματοποίησης πληρωμών εγκαίρως και χαμηλότερου κόστους συναλλαγής. Ένας άλλος τρόπος με τον οποίο τα ψηφιακά νομίσματα μπορούν να βοηθήσουν την οργάνωση είναι η εξάλειψη / μείωση των κινδύνων έκθεσης χρησιμοποιώντας αυτά ως νόμισμα μεταφοράς.

Προς το παρόν, τα κρυπτονομίσματα δεν γίνονται δεκτά από τις τράπεζες και ως εκ τούτου δεν μπορούν να κερδιστούν από τους ιδιώτες ή τους οργανισμούς. Υπάρχουν επίσης κίνδυνοι που συνδέονται με τα ψηφιακά νομίσματα, όπως η ασφάλεια, η αστάθεια των νομισμάτων και ο προσδιορισμός των δικαιούχων πληρωμών. Ορισμένοι τομείς αβεβαιότητας, όπως η συμμόρφωση με τους κανονισμούς και η αναγνώριση των πελατών μαζί με τον κίνδυνο, περιορίζουν την αποδοχή των ψηφιακών νομισμάτων στον κλάδο των πληρωμών.

1.2 Η χρησιμότητα των κρυπτονομισμάτων

Για τους περισσότερους ανθρώπους, τα κρυπτονομίσματα θεωρούνται συνήθως επενδύσεις υψηλού κινδύνου. Εντούτοις, αυτό που χάνεται εν μέσω της δημοσιότητας και της κερδοσκοπίας είναι ότι τα περισσότερα αποκεντρωμένα κρυπτονομίσματα, όπως το bitcoin, δημιουργήθηκαν για να κάνουν κάτι και έτσι έχουν ένα ευρύ φάσμα ισχυρών περιπτώσεων χρήσης. Παρακάτω παρουσιάζονται οι σημαντικότερες χρήσεις των κρυπτονομισμάτων και η χρησιμότητα αυτών στη καθημερινότητα².

1. Μεταφορές χρημάτων με χαμηλό κόστος συναλλαγής

Το πιο γνωστό όφελος των κρυπτονομισμάτων είναι η ικανότητά τους να στέλνουν και να δέχονται πληρωμές με χαμηλό κόστος και με μεγάλη ταχύτητα. Για παράδειγμα, μια συναλλαγή σε κρυπτονομίσμα ύψους 99 εκατομμυρίων δολαρίων χρειάζεται μόλις λίγα λεπτά για να επεξεργαστεί και να κοστίζει στον αποστολέα μόνο λίγα cents σε τέλη συναλλαγών. Εάν η μεταφορά χρημάτων είχε περάσει από ενδιάμεσο χρηματοπιστωτικό

² Kaplanov N., (2012), Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, Heinonline

οργανισμό, τα τέλη θα ήταν πολύ, πολύ υψηλότερα και η μεταφορά θα είχε διαρκέσει αρκετές ημέρες ή και περισσότερο εάν πρόκειται για διασυνοριακή συναλλαγή.

2. Ένας τραπεζικός λογαριασμός χωρίς κίνδυνο απώλειας χρημάτων

Παρόλο που πολλοί άνθρωποι δεν γνωρίζουν ότι ο τραπεζικός τους λογαριασμός και τα περιουσιακά τους στοιχεία θα μπορούσαν να παγώσουν, η πραγματικότητα είναι ότι αυτό συμβαίνει συχνότερα από ό, τι συνειδητοποιούν οι άνθρωποι ειδικά σε περιπτώσεις φοροδιαφυγής. Δεν είναι άλλωστε λίγες οι περιπτώσεις που σήμερα η ΑΑΔΕ προχωρεί αυτόματα σε κατασχέσεις τραπεζικών λογαριασμών για χρέη των ιδιωτών απέναντι στο δημόσιο.

Εδώ μπαίνει στο παιχνίδι μία από τις πιο μοναδικές και ισχυρές χρήσεις των κρυπτονομισμάτων. Τα κρυπτονομίσματα, όπως το bitcoin, λειτουργούν ως εναλλακτικός τραπεζικός λογαριασμός ή για να είμαστε περισσότερο αληθείς ως ένα πορτοφόλι που έχει πρόσβαση μόνο το άτομο με τα ιδιωτικά κλειδιά στο πορτοφόλι. Ως εκ τούτου, κανένα προσωπικό πορτοφόλι δεν μπορεί ποτέ να παγώσει από τις αρχές και αυτό δίχως αμφιβολία είναι ένα μεγάλο πλεονέκτημα³.

3. Επενδύσεις σε καινοτόμες νεοσύστατες επιχειρήσεις

Η εμφάνιση της συγκέντρωσης χρημάτων μέσω κρυπτονομισμάτων έχει επιτρέψει σε οποιονδήποτε με σύνδεση στο διαδίκτυο να γίνει επενδυτής σε καινοτόμες τεχνολογικές καινοτομίες πρώιμης φάσης, ενώ ταυτόχρονα παρέχει νέες επιχειρηματικές εκκινήσεις με πολύ αναγκαία κεφάλαια εκκίνησης.

Οι αρχικές προσφορές νομισμάτων αποτελούν μια νέα μορφή συλλογής κεφαλαίων που παρέχει στις νεοσύστατες επιχειρήσεις την ευκαιρία να αντλήσουν κεφάλαια με την πώληση ενός ψηφιακού επενδύσεων που δημιουργήθηκε πρόσφατα στους πρώτους υποστηρικτές του έργου, σε αντάλλαγμα για καθιερωμένες κρυπτοσυχνότητες όπως Bitcoin (BTC) κτλ.

4. Η πραγματοποίηση ιδιωτικών συναλλαγών

³ Yermak D., (2015), Is Bitcoin a real currency? An economic appraisal, Elsevier

Υπάρχουν διάφορα εξατομικευμένα κρυπτονομίσματα τα οποία επιτρέπουν στους χρήστες να κάνουν ανώνυμες οικονομικές συναλλαγές.

Αυτό σημαίνει ότι τα άτομα μπορούν να κάνουν μεταφορές χρημάτων χωρίς να χρειάζεται να εξηγήσουν σε μια τράπεζα γιατί στέλνουν ένα μεγάλο χρηματικό ποσό, ποιες είναι οι πηγές των κεφαλαίων στις οποίες την αποστέλλουν, πράγμα που μπορεί να καθυστερήσει τη συναλλαγή και να συνεπάγεται άσκοπα γραφειοκρατικές διαδικασίες.

5. Πληρωμές για τη δημοσίευση περιεχομένου σε blogs / sites κτλ

Διάφορες σελίδες και πλατφόρμες κοινωνικών μέσων ενημέρωσης, blogs δίνουν τη δυνατότητα στους ιδιοκτήτες να λαμβάνουν οικονομικές ανταμοιβές με τη μορφή κρυπτονομισμάτων για την απόσπαση περιεχομένου και την επιμέλεια του blog με την προώθηση περιεχομένου υψηλής ποιότητας.

6. Τα κρυπτονομίσματα δίνουν τη δυνατότητα στους πελάτες να τα χρησιμοποιούν

Λόγω της εκρηκτικής ανάπτυξης των κρυπτονομισμάτων τα τελευταία εννέα χρόνια, είναι πλέον δυνατόν να ταξιδέψουμε τον κόσμο με χρήση των νομισμάτων αυτών.

Σήμερα διάφορα εγκατεστημένα ταξιδιωτικά πρακτορεία δέχονται το bitcoin ως τρόπο πληρωμής για την κράτηση πτήσεων, ενοικιάσεις αυτοκινήτων και ξενοδοχεία και για όσους προτιμούν να παραμείνουν σε διαμέρισμα όταν ταξιδεύουν, μπορούν να κλείσουν καταλύματα χρησιμοποιώντας διάφορα κρυπτονομίσματα.

Επίσης η ανάπτυξη της αγοράς ATM bitcoin σημαίνει επίσης ότι οι ταξιδιώτες είναι πλέον σε θέση να μετατρέψουν τα κρυπτονομίσματα σε τοπικό νόμισμα στις περισσότερες μεγάλες πόλεις σε όλο τον κόσμο⁴.

7. Αγορά πολύτιμων αγαθών και ακριβών προϊόντων.

Τέλος, με τη χρήση των κρυπτονομισμάτων οι καταναλωτές μπορούν να αγοράζουν αγαθά ακριβής αξίας όπως πολύτιμους λίθους, ακριβά αυτοκίνητα, έργα τέχνης κτλ χωρίς να χρειάζεται να υποβάλλονται σε έλεγχο πόθεν έσχες για τις αγορές αυτές.

⁴ Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber

1.3 Η λειτουργία των κρυπτονομισμάτων

Η χρήση ενός ψηφιακού νομίσματος είναι σχεδόν ισοδύναμη με τη χρήση του PayPal ή μιας χρεωστικής κάρτας, με εξαίρεση τους αριθμούς στην οθόνη που αντιπροσωπεύουν το κρυπτονόμισμα αντί για ένα παραδοσιακό νόμισμα όπως το δολάριο ή το ευρώ κτλ. Το μόνο που χρειάζεται ένας νέος χρήστης είναι να δημιουργήσει έναν λογαριασμό δηλαδή ένα ηλεκτρονικό πορτοφόλι στο οποίο να «αποθηκεύει» να ψηφιακά του χρήματα. Με το ηλεκτρονικό πορτοφόλι οι χρήστες μπορούν να αγοράσουν, να πουλήσουν, να στείλουν, να λάβουν και να αποθηκεύσουν ψηφιακά νομίσματα.

Για να χρησιμοποιήσουμε ένα κρυπτονόμισμα, δεν χρειάζεται να κατανοήσουμε απόλυτα τη λειτουργία του η οποία και είναι παρόμοια με τη λειτουργία του νομισματικού συστήματος για τη χρήση χρεωστικής / πιστωτικής κάρτας. Ωστόσο, εάν θέλετε να κατανοήσετε τη λειτουργία του κρυπτονομίσματος, πρέπει να κατανοήσετε την έννοια του κρυπτονομίσματος, την έννοια του blockchain το οποίο είναι το δημόσιο βιβλίο των συναλλαγών και της τεχνολογίας όσο και την έννοια της κρυπτογράφησης. Μετά από όλα, η κρυπτογράφηση είναι ένα κρυπτονόμισμα, όπου οι συναλλαγές καταγράφονται σε ένα δημόσιο ψηφιακό βιβλίο που ονομάζεται blockchain, και κάθε διαδικασία εξασφαλίζεται με κρυπτογραφία⁵.

Το κρυπτονόμισμα λειτουργεί λίγο πολύ σαν τραπεζική πίστωση σε χρεωστική κάρτα. Και στις δύο περιπτώσεις, ένα πολύπλοκο σύστημα που εκδίδει συναλλαγές λειτουργεί πίσω από τα παρασκήνια για να επιτρέπει στους ανθρώπους να στέλνουν και να λαμβάνουν νόμισμα ηλεκτρονικά. Ομοίως, όπως συμβαίνει και με τις τραπεζικές συναλλαγές, οι ηλεκτρονικές πλατφόρμες μπορούν να χρησιμοποιηθούν για τη διαχείριση λογαριασμών και την μετακίνηση υπολοίπων. Η κύρια διαφορά ανάμεσα στο κρυπτονόμισμα και την τραπεζική πίστωση είναι ότι αντί για τις τράπεζες και τις κυβερνήσεις που εκδίδουν το νόμισμα και τη διατήρηση βιβλίων, αυτό το κάνει ένας αλγόριθμος.

⁵ Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber

Οι συναλλαγές με τη χρήση του κρυπτονομίσματος αποστέλλονται μεταξύ χρηστών χρησιμοποιώντας λογισμικό που ονομάζεται πορτοφόλια κρυπτογράφησης. Το άτομο που δημιουργεί τη συναλλαγή χρησιμοποιεί το λογισμικό πορτοφολιού για να μεταφέρει τα υπόλοιπα από έναν λογαριασμό σε άλλο. Για να μεταφέρει ο χρήστης τα χρήματα, απαιτείται η γνώση ενός κωδικού πρόσβασης που σχετίζεται με τον λογαριασμό. Οι συναλλαγές που πραγματοποιούνται μεταξύ των χρηστών είναι κρυπτογραφημένες και στη συνέχεια μεταδίδονται στο δίκτυο κρυπτογράφησης και περιμένουν να προστεθούν στο δημόσιο βιβλίο. Στη συνέχεια, οι συναλλαγές καταγράφονται στο δημόσιο βιβλίο μέσω μιας διαδικασίας που ονομάζεται εξόρυξη κεφαλαίου. Τα ποσά των συναλλαγών είναι δημόσια, αλλά ο χρήστης που έστειλε τη συναλλαγή είναι κρυπτογραφημένος είναι δηλαδή ανώνυμος. Κάθε συναλλαγή οδηγεί πίσω σε ένα μοναδικό σύνολο κλειδιών. Όποιος κατέχει ένα σύνολο κλειδιών, κατέχει το ποσό κρυπτογράφησης που συνδέεται με αυτά τα κλειδιά.

Το blockchain είναι σαν ένα αποκεντρωμένο τραπεζικό βιβλίο, και στις δύο περιπτώσεις το βιβλίο είναι ένα αρχείο συναλλαγών και υπολοίπων. Όταν πραγματοποιείται συναλλαγή με κρυπτογράφηση, αυτή η συναλλαγή αποστέλλεται σε όλους τους χρήστες που φιλοξενούν ένα αντίγραφο του blockchain. Συγκεκριμένοι τύποι χρηστών που ονομάζονται miners στη συνέχεια προσπαθούν να λύσουν ένα κρυπτογραφικό πάζλ το οποίο τους επιτρέπει να προσθέσουν ένα πακέτο συναλλαγών στο βιβλίο. Μερικές φορές οι miners συγκεντρώνουν την ισχύ των υπολογιστών και μοιράζονται τα νέα νομίσματα. Ο αλγόριθμος βασίζεται στη συναίνεση. Εάν η πλειονότητα των χρηστών που προσπαθούν να λύσουν το πάζλ υποβάλλουν όλα τα ίδια δεδομένα συναλλαγής, τότε επιβεβαιώνει ότι οι συναλλαγές είναι σωστές. Επιπλέον, η ασφάλεια του blockchain βασίζεται στην κρυπτογραφία. Κάθε μπλοκ συνδέεται με τα δεδομένα του τελευταίου μπλοκ μέσω μονόδρομων κρυπτογραφικών κωδικών που ονομάζονται hashes οι οποίοι έχουν σχεδιαστεί για να καταστήσουν πολύ δύσκολη την παραβίαση του blockchain⁶.

Οι χρήστες που χρησιμοποιούν το λογισμικό και το υλικό που αποσκοπούν στην επιβεβαίωση των συναλλαγών στο ψηφιακό βιβλίο είναι οι ανθρακωρύχοι με

⁶ Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate

κρυπτογράφηση. Η επίλυση των κρυπτογραφικών πάζλ μέσω του λογισμικού για την προσθήκη συναλλαγών στο βιβλίο με την ελπίδα να κερδίσουμε τα κέρματα ως ανταμοιβή. Αυτή είναι με λίγα λόγια η έννοια της εξόρυξης.

Τα πλήκτρα που μετακινούν ισορροπία γύρω από το blockchain χρησιμοποιούν έναν τύπο μονόδρομης κρυπτογράφησης που ονομάζεται κρυπτογραφία δημόσιου κλειδιού. Οι hashes δηλαδή οι μονόδρομοι κρυπτογραφικοί κώδικες που συνδέουν τα μπλοκ στο blockchain χρησιμοποιούν παρόμοιο τύπο κρυπτογραφίας. Εν τω μεταξύ, τα δεδομένα συναλλαγών που αποστέλλονται και αποθηκεύονται στο blockchain είναι ένας τύπος μίας κρυπτογραφίας που δείχνει τα δεδομένα αλλά δεν περιέχει όλα τα αρχικά δεδομένα. Το κλειδί για την κατανόηση αυτών των επιπέδων κρυπτογράφησης που εξασφαλίζουν ένα σύστημα όπως το Bitcoin βρίσκεται σε κρυπτογραφικές λειτουργίες μονής κατεύθυνσης. Η βασική ιδέα είναι ότι η κρυπτογράφηση χρησιμοποιεί έναν τύπο κρυπτογραφίας που είναι εύκολο να υπολογιστεί με έναν τρόπο, αλλά είναι δύσκολο να υπολογιστεί ο άλλος τρόπος χωρίς ένα «κλειδί». Μπορούμε να το σκεφτούμε για να το κάνουμε περισσότερο παραστατικό ότι είναι εύκολο να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης αν βρίσκεστε στον ηλεκτρονικό σας τραπεζικό λογαριασμό, αλλά είναι πολύ δύσκολο για τους άλλους να μαντέψουν έναν ισχυρό κωδικό πρόσβασης μετά τη δημιουργία του⁷.

1.4 Ζητήματα ασφάλειας και κίνδυνοι από τη χρήση κρυπτονομισμάτων

Είναι γεγονός ότι τα τελευταία χρόνια τα ψηφιακά νομίσματα έχουν κερδίσει μια σημαντική θέση στις προτιμήσεις των επενδυτών εξαιτίας των μεγάλων πλεονεκτημάτων που αυτά έχουν. Παρ' όλα αυτά, υπάρχουν ορισμένοι βασικοί κίνδυνοι που πλήττουν τα κρυπτονομίσματα και εμποδίζουν την υιοθέτηση και τη σταθερότητα της αγοράς

⁷ Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate

ευρύτερα. Στη συνέχεια παρουσιάζονται παραδείγματα βασικών κινδύνων που θέτουν σε κίνδυνο και αμφιβολία τα κρυπτονομίσματα και εμποδίζουν την πρόοδο της αγοράς.

1. Η εύκολη είσοδος και περιορισμένη έξοδος από την αγορά

Είναι αλήθεια ότι η εμφάνιση των κρυπτονομισμάτων έχει εκδημοκρατίσει πολλές πτυχές χρηματοδότησης. Αυτό το μειωμένο εμπόδιο στην είσοδο δημιουργεί μια ευρεία είσοδο και μια πολύ δύσκολο έξοδο μπορεί να οδηγήσει σε παράπλευρες ζημιές καθώς οι άνθρωποι βιάζονται να βγουν από την αγορά. Η έξοδος μπορεί να αποκλειστεί λόγω των τεχνολογικών περιορισμών, της μη μετατρεψιμότητας του νομίσματος και των λίγων αντισυμβαλλομένων με τους οποίους θα διαπραγματευτεί ο χρήστης. Ενώ η κατηγορία των κρυπτονομισμάτων γενικά δεν συνδέεται με την παραδοσιακή οικονομία, όλα συσχετίζονται με τη παραδοσιακή αγορά, γεγονός που μπορεί να δημιουργήσει πανικό σε ολόκληρο το σύστημα.

2. Τα κρυπτονομίσματα είναι άυλα, μη ρευστοποιήσιμα και ανασφάλιστα

Το αληθινό θαύμα των κρυπτονομισμάτων, όπως το bitcoin, είναι ότι το ζήτημα της διπλής μέτρησης επιλύεται χωρίς κανένα ενδιάμεσο, όπως η τράπεζα. Αυτό το χαρακτηριστικό που καταγράφεται από την έννοια της ψηφιακής ιδιαιτερότητας, όπου μπορεί να υπάρξει μόνο μία περίπτωση ενός περιουσιακού στοιχείου, είναι ισχυρή και ένας από τους πρωταρχικούς λόγους για τους οποίους αυτή η κατηγορία των κρυπτονομισμάτων έχει αναπτυχθεί. Ωστόσο, η άυλη και μη ρευστοποιήσιμη φύση των κρυπτονομισμάτων εμποδίζει τη δυνατότητα μετατροπής τους και την ασφάλειά τους. Πράγματι, παρά τις αναφορές αύξησης του ενδιαφέροντος των ασφαλίσεων στον κλάδο, η πλειοψηφία των νομισμάτων είναι είτε ανασφάλιστα είτε δεν είναι ασφαλισμένα με τα σημερινά πρότυπα. Δεν υπάρχει επομένως ασφαλιστική κάλυψη καταθέσεων για αυτή την κατηγορία περιουσιακών στοιχείων, η οποία μπορεί να συμβάλει στη διεύρυνση της ασφάλειας των επενδυτών⁸.

3. Η εύκολη παραπληροφόρηση

Ενώ κανένας επενδυτής δεν είναι διατεθειμένος να χάσει καμία ποσότητα χρημάτων, ανεξάρτητα από το ονομαστικό ποσό όμως τα κρυπτονομίσματα είναι ιδιαίτερα επιρρεπή

⁸ Gans J., Halaburda H., (2015), Some economics of private digital currency, Nber

στην κοινωνική μηχανική και τους κινδύνους παραπληροφόρησης. Οι αφελείς επενδυτές επομένως, όπως και στην αναλογική οικονομία, μπορούν να γίνουν εύκολα θύματα εκβιασμού στον κυβερνοχώρο, χειραγώγησης της αγοράς, απάτης και άλλων επενδυτικών κινδύνων.

4. Η φύλαξη και ο έλεγχος

Παρά την άυλη και αόρατη φύση των κρυπτονομισμάτων ένα από τα μεγαλύτερα ζητήματα που μαστίζουν την αγορά είναι η φροντίδα, η επιμέλεια και ο έλεγχος αυτής. Σε αντίθεση με τη φυσική ασφάλεια του παραδοσιακού τραπεζικού τομέα, πραγματοποιείται ένας πραγματικός πόλεμος προτύπων μεταξύ των εταιρειών των ψηφιακών νομισμάτων σχετικά με το ποιος παρέχει τα υψηλότερα πρότυπα προστασίας επενδυτών και ασφάλειας περιουσιακών στοιχείων. Ο αριθμός των καταθετών υψηλού προφίλ και υψηλής αξίας υποδηλώνει ότι αυτή η λίστα με τις καλύτερες πρακτικές ασφαλείας είναι σε διαρκή εξέλιξη.

5. Οι κίνδυνοι στο διαδίκτυο

Όπως συμβαίνει με τις απειλές στο διαδίκτυο είναι δεδομένο ότι το κρυπτονόμισμα ως ένα μη φυσικό και από περιουσιακό στοιχείο εκτίθεται σε διαδικτυακούς κινδύνους. Αν και πρέπει να σημειωθεί εδώ ότι υπάρχει μεγάλη ασφάλεια σχετικά με τα ψηφιακά νομίσματα κανείς δε μπορεί να εγγυηθεί στους επενδυτές απόλυτα ότι τα ηλεκτρονικά τους χρήματα είναι απόλυτα ασφαλή.

6. Τεχνολογικοί Κίνδυνοι

Έχουν υπάρξει πολλές αναφορές σχετικά με την υπολογιστική πολυπλοκότητα και διάφορους άλλους κινδύνους των κρυπτονομισμάτων. Αυτή η υπολογιστική πολυπλοκότητα μπορεί επίσης να λειτουργήσει αντίστροφα και να δημιουργήσει δυνητικούς κινδύνους για την κατηγορία στοιχείων ενεργητικού υπό την προϋπόθεση ότι τα σύνθετα συστήματα αποτυγχάνουν με περίπλοκο τρόπο. Για το σκοπό αυτό, οι επενδυτές πρέπει να προσέχουν τους τεχνολογικούς κινδύνους και τις ψευδείς υποσχέσεις αποκέντρωσης που γίνονται σε πολλά έργα⁹.

⁹ Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate

Τέλος όμως πρέπει να σημειωθεί ότι ακριβώς επειδή υπάρχουν κίνδυνοι στην αγορά των κρυπτονομισμάτων, υπάρχουν και ανταμοιβές. Η κατανόηση των δυνητικών κινδύνων της αγοράς μπορεί να συμβάλει στη βελτίωση των μακροπρόθεσμων προοπτικών των κρυπτονομισμάτων και στη διεύρυνση της υιοθέτησής τους πέρα από τους κινδύνους που υπάρχουν στην αγορά αυτή.

1.5 Η δημιουργία του Bitcoin

Τα τελευταία χρόνια η έννοια του Bitcoin είναι ολοένα και περισσότερο διαδεδομένη όμως οι περισσότεροι άνθρωποι δεν είναι σίγουροι τι είναι ή πώς λειτουργεί και γιατί ολοένα και περισσότεροι ξεκίνησαν να το χρησιμοποιούν στην καθημερινότητά τους. Ο λόγος είναι απλός. Μέχρι το 2009 τα χρήματα θα μπορούσαν να εκδοθούν μόνο από τα ακόλουθα τρία όργανα: τις κεντρικές τράπεζες μέσω της εκτύπωσης χρημάτων, από τα πιστωτικά ιδρύματα μέσω της δημιουργίας χρημάτων μέσω δανείων ή μέσω των ιδρυμάτων με άδεια ηλεκτρονικού χρήματος μέσω της έκδοσης ηλεκτρονικού χρήματος. Το κοινό σημείο σε όλες τις περιπτώσεις, η έκδοση των χρημάτων πραγματοποιούνταν μέσα σε ένα εξαιρετικά ρυθμισμένο πλαίσιο. Ακόμη και σήμερα ο τραπεζικός κλάδος είναι ο πιο ρυθμιζόμενος τομέας στη γη, καθώς εκπληρώνει έναν διπλό ρόλο, να εκδίδει δάνεια στους δανειολήπτες και να συγκεντρώνει ταυτόχρονα τα οφειλόμενα ποσά.

Αυτό άλλαξε τον Ιανουάριο του 2009, όταν εξορύσσεται το πρώτο bitcoin μέσα σε μια μη ρυθμισμένη αγορά και σε ένα αποκεντρωμένο περιβάλλον. Το Bitcoin ήταν το πρώτο νόμισμα που εφευρέθηκε το 2008 από τον Satoshi Nakamoto μαζί με την τεχνολογία blockchain¹⁰.

Σήμερα χρησιμοποιούμε τη λέξη κρυπτονομίσματα για όλες τις ψηφιακές μορφές πληρωμής, οι οποίες εκδίδονται από ένα δίκτυο υπολογιστών (peer-to-peer: δίκτυο P2P) μετά την επίλυση σύνθετων μαθηματικών εξισώσεων, αντί να δημιουργούνται από τα παραδοσιακά αδειοδοτημένα όργανα εντός μιας ρυθμιζόμενης αγοράς. Αυτές οι

¹⁰ Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., (2012). Evaluating User Privacy in Bitcoin

μαθηματικές εξισώσεις ονομάζονται ως κρυπτογραφία, οι οποίες ονομάστηκαν εμφανίστηκαν μετά τον Δεύτερο Παγκόσμιο Πόλεμο, καθώς υπήρχε ανάγκη για ασφαλή επικοινωνία για προφανείς λόγους. Επί του παρόντος υπάρχουν περισσότερες από 1000 κρυπτοσυχνότητες και το bitcoin είναι το πιο γνωστό από όλα αυτά.

Η ραχοκοκαλιά του bitcoin είναι η τεχνολογία blockchain, η οποία είναι βασικά κρυπτογραφημένη βάση δεδομένων συναλλαγών (ημερολόγιο), που μοιράζεται μεταξύ όλων των συμμετεχόντων σε ένα δημόσιο δίκτυο και επομένως επαληθεύεται και από τους χρήστες. Η διαφορά μεταξύ του υφιστάμενου συστήματος και της τεχνολογίας blockchain είναι ότι δεν απαιτεί υπερβολικά ρυθμιζόμενες οντότητες τρίτων όπως οι τράπεζες και ο χρήστης να διατηρεί πολλά βιβλία παράλληλα, αλλά μόνο ένα, επομένως η απαίτηση της τεχνολογίας της πληροφορίας είναι επίσης χαμηλότερη και όλοι οι συμμετέχοντες στο δίκτυο μπορούν να έχουν πρόσβαση σε αυτό οποιαδήποτε στιγμή. Κατά συνέπεια, εφαρμόζεται αυστηρότερος έλεγχος αφήνοντας λιγότερες ευκαιρίες για χειραγώγηση των δεδομένων. Επίσης δεν απαιτείται ειδική υποδομή για να κρατήσει το σύστημα σε λειτουργία, αλλά αντί αυτού οι χρήστες του δικτύου είναι ουσιαστικά οι ίδιοι η υποδομή αυτή. Αυτό σημαίνει ότι δεν πρέπει να υπάρχουν εξωτερικές οντότητες που συμμετέχουν στη ροή των συναλλαγών, αλλά το ίδιο το δίκτυο πληροί όλες τις απαραίτητες λειτουργίες τις ίδιες υπηρεσίες, που ήταν διαθέσιμες μόνο με εξειδικευμένα ιδρύματα στο παρελθόν.

1.6 Οι λόγοι της διεύρυνσης της χρήσης του Bitcoin

Η δημοτικότητα του κρυπτονομίσματος και της τεχνολογίας blockchain απορρέει από τις ιδιαιτερότητές του στον χρηματοπιστωτικό τομέα. Η διατήρηση μιας μόνο κοινής βάσης δεδομένων μπορεί να μην είναι τόσο ενδιαφέρουσα ή μοναδική ιδέα, αλλά τα δικά της πλεονεκτήματα την καθιστούν πραγματικά ανταγωνιστική ως προς παραδοσιακές τραπεζικές υπηρεσίες για τους παρακάτω λόγους¹¹:

¹¹ Antonopoulos, A.M.,(2014). Mastering Bitcoin, Jstor

1. Χαμηλότερο κόστος. Δεδομένου ότι οι συναλλαγές πραγματοποιούνται μέσω κοινόχρηστου και δημόσιου δικτύου, δεν απαιτεί, συνεπώς, ειδική υποδομή πληροφορικής από μια κεντρική οντότητα ενώ και το κόστος των τελών επεξεργασίας και συντήρησης είναι επίσης περιορισμένο. Βασικά ο καθένας μπορεί να είναι ένα μέλος του δικτύου blockchain με έναν υπολογιστή. Τότε εξαρτάται από τις προτιμήσεις του χρήστη πότε και πόση ικανότητα είναι διατεθειμένη να διαθέσει για εξόρυξη κρυπτονομισμάτων. Το κίνητρο πίσω από αυτή τη διαδικασία είναι απλό: Το άτομο το οποίο αναλαμβάνει την εξόρυξη του κρυπτονομίσματος (miner) ορίζει τον υπολογισμό, τις ικανότητες κρυπτογράφησης και τις λεπτομέρειες των συναλλαγών, οι οποίες αποθηκεύονται αργότερα στο κοινό ημερολόγιο, το οποίο είναι ευρύτερα γνωστό ως blockchain και λαμβάνει bitcoins ως πληρωμή για τις υπηρεσίες αυτές. Κατά συνέπεια, εξαλείφονται επίσης τα συνολικά έξοδα συναλλαγής.

2. Χαμηλότερος κίνδυνος απάτης και μεγαλύτερης ασφάλειας. Δεδομένου ότι η βάση δεδομένων των συναλλαγών (ημερολόγιο) μοιράζεται μεταξύ όλων των συμμετεχόντων στο δίκτυο, χωρίς τρίτους παρόχους (όπως οι τράπεζες) συμμετέχουν στη ροή των συναλλαγών επεξεργασίας, αφήνοντας λιγότερο χώρο για δόλιες δραστηριότητες. Είναι δύσκολο, αλλά δεν είναι αδύνατο να αλλάξουμε το βιβλίο, καθώς είναι πιστοποιημένο από όλα τα μέλη του δικτύου και είναι μόνο εγκεκριμένο, αν ταιριάζει με το 51% των χρηστών. Το βιβλίο είναι από μπλοκ, τα οποία είναι βασικά παρτίδες κρυπτογραφημένες συναλλαγές με όλες τις λεπτομέρειες τους. Αυτά τα μπλοκ αποθηκεύονται μετά το ένα με το άλλο κατά χρονολογική σειρά και να είναι σε θέση να προσθέσει ένα νέο μπλοκ στην αλυσίδα από το κρυπτογραφημένο στάδιο που πρέπει να είναι το ίδιο για τουλάχιστον το 51% των miners.

3. Παρέχει ανωνυμία. Υπάρχει μια γενική πεποίθηση για bitcoin, ότι οι χρήστες τους μπορούν να ξεκινήσουν τη συναλλαγή τους σε ένα πλήρως ανώνυμο περιβάλλον, αλλά αυτή είναι μόνο η μισή αλήθεια. Πράγματι όλες οι συναλλαγές και οι λεπτομέρειες τους είναι κρυπτογραφημένες και υπάρχουν διάφορες δυνατότητες οι οποίες όμως θα χρειαστεί καιρός για να την αποκωδικοποιηθούν, αλλά εξακολουθεί να υπάρχει η

βιβλιοθήκη και είναι διαθέσιμη στο κοινό και μοιράζονται μεταξύ όλων των συμμετεχόντων¹².

Για να αυξηθεί η πολυπλοκότητα, το σύστημα δεν μεταφέρει bitcoins από έναν αποστολέα σε έναν δέκτη, αλλά συνδυάζει διάφορες συναλλαγές πολλών αποστολέων και προς τα εμπρός σε πολλούς δέκτες, γεγονός που καθιστά ακόμη πιο δύσκολη την παρακολούθηση σε περίπτωση αποκρυπτογράφησης. Είναι επίσης αλήθεια ότι αντί των ονομάτων ή των προσωπικών λεπτομερειών που χρησιμοποιεί το σύστημα παράγει διευθύνσεις για τους χρήστες, αλλά σε περίπτωση που κάποιος μπορεί να τις συνδέσει τις απευθύνει σε ταυτότητες ανθρώπων, τότε όλες οι πληρωμές τους, θα πρέπει να αποστέλλονται ή που έχουν ληφθεί, μπορούν να εντοπιστούν, δεδομένου ότι η καθυστέρηση της συναλλαγής είναι δημόσια προσβάσιμη για τον οποιονδήποτε.

4. Αυξημένη ακρίβεια των συναλλαγών. Από τότε που καταγράφονται τα μπλοκ συναλλαγών στη βάση δεδομένων και είναι πιστοποιημένα από τα μέλη του δικτύου, των οποίων η συναίνεση δίνεται. Το 51% ή περισσότερο απαιτείται για την έγκριση ενός νέου μπλοκ, επομένως οι πιθανότητες ανακρίβειας είναι σημαντικά χαμηλότερες. Φυσικά αυτό δεν εγγυάται 100% ακρίβεια, επειδή η απορριπτική θεωρία εξακολουθεί να ισχύει και για την τεχνολογία blockchain και θα μπορούσε να ανοίξει θεωρητικές πόρτες για χειραγώγηση, αλλά σημαίνει επίσης ότι οι κίνδυνοι των διακανονισμών είναι επίσης χαμηλότεροι και οι συναλλαγές φθάνουν στους δικαιούχους τους με πολύ μεγαλύτερες πιθανότητες από ό, τι πριν.

5. Αποκεντρωμένη χρήση. Αυτή μπορεί να είναι μία από τις σημαντικότερες ιδιαιτερότητες του blockchain δεδομένου ότι το ίδιο το σύστημα βασίζεται σε ένα δίκτυο χρηστών από ομότιμους χρήστες και όχι μόνο σε συγκεκριμένα χρηματοπιστωτικά ιδρύματα όπως τα έχουμε στην παραδοσιακή τραπεζική δομή. Βασικά λέει ότι υπάρχει ένα νομισματικό σύστημα που παρέχει παγκόσμια κάλυψη για τα προϊόντα και τις υπηρεσίες τους και ακόμα δεν υπάρχει κάτι τέτοιο όπως το Bitcoin που θα μπορούσε να χρεοκοπήσει. Η κρίση του 2008 υπογράμμισε πόσο εύθραυστη ήταν η κρίση στο κεντρικό τραπεζικό σύστημα και ότι μερικά γεγονότα ενεργοποίησης μπορούν να ξεκινήσουν το ντόμινο τα οποία μπορούν να ωθήσουν τις τράπεζες σε αφερεγγυότητα.

¹² Antonopoulos, A.M.,(2014). Mastering Bitcoin, Jstor

Ένα από τα κύρια πλεονεκτήματα της ύπαρξης της αποκεντρωμένης φύσης είναι ότι εξαλείφει το ρευστό και τον πιστωτικό κίνδυνο και μειώνει τον συστημικό κίνδυνο¹³.

6. Ταχύτητα πραγματοποίησης συναλλαγών: Βέβαια υπάρχουν και λύσεις για πληρωμές στην παραδοσιακή τραπεζική που χρειάζονται μόνο δευτερόλεπτα για επεξεργασία, όπως η άμεση μεταφορά πίστωσης σε SEPA δίκτυο, αλλά έχει τους περιορισμούς της. Σε περίπτωση που σήμερα θέλουμε να ξεκινήσουμε μια διεθνής μεταφορά από μια τράπεζα σε άλλη, μπορεί να χρειαστούν αρκετές ημέρες για να φτάσει κανείς δικαιούχος. Αν κοιτάξουμε πίσω από τις κουρτίνες, μπορούμε εύκολα να εντοπίσουμε τα μεγάλα εμπόδια με την τρέχουσα ρύθμιση: κεντρικό τραπεζικό σύστημα με αρκετές ενδιάμεσες τράπεζες επιβραδύνοντας τη ροή των χρημάτων, η οποία επεξεργάζεται μόνο μερικές παρτίδες συναλλαγών κάθε ορισμένες ώρες και δεν λειτουργεί κατά τις αργίες, κλπ. Με το δίκτυο blockchain ο χρήστης μπορεί βασικά να ξεκινήσει μια άμεση πληρωμή σε οποιονδήποτε σε ολόκληρο τον κόσμο, δεδομένου ότι η εκκαθάριση του τμήματος των συναλλαγών πραγματοποιείται 24 ώρες το εικοσιτετράωρο.

1.7 Η μελλοντική εξέλιξη των κρυπτονομισμάτων

Το μέλλον των Bitcoin ή άλλων πλατφορμών ψηφιακών νομισμάτων μπορεί να διαταράξει δυνητικά την παραδοσιακή ή την κληρονομιά των οικονομικών συστημάτων. Απελευθερώνει αποτελεσματικά τις νομισματικές συναλλαγές από τον τραπεζικό τομέα και τη νομισματική αρχή και αντί αυτού δημιουργεί εμπιστοσύνη χρησιμοποιώντας μόνο τεχνολογία. Μπορεί να παρέχει πρόσβαση σε χρηματοπιστωτικές υπηρεσίες προς τις μη και κάτω τραπεζικές, επιτρέπουν εξαιρετικά χαμηλού κόστους μεταφορές χρημάτων και εμβασμάτων πέρα από τα κρατικά σύνορα, και χρησιμεύουν ως αποθήκη αξίας έναντι των εθνικών νομισμάτων¹⁴.

¹³ European Central Bank, (ECB), (2015), Virtual currency schemes –a further analysis

¹⁴ Mullan, P., (2014), The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations. U.S.A.: Palgrave Macmillan US

Ωστόσο, οι διακυμάνσεις των τιμών του bitcoin έναντι των εθνικών νομισμάτων, όπως το δολάριο ΗΠΑ, το ευρώ ή το κινεζικό γιουάν, είναι εξαιρετικά ευμετάβλητες τα τελευταία χρόνια. Αυτή η ακραία μεταβλητότητα των τιμών παράγει πολύ θόρυβο που κάνει δύσκολη την ανάλυση. Ευτυχώς, υπάρχει μια ενεργή και αρκετά ρευστοποιημένη αγορά για διάφορα ζευγάρια συναλλαγών altcoin-bitcoin, ένα altcoin είναι ένα από τα πολλά εναλλακτικά ψηφιακά νομίσματα βασισμένα στον αρχικό κώδικα bitcoin ανοικτού κώδικα. Εξετάζοντας το συγγενικό όνομα τις τιμές και την κατάργηση των συναλλαγματικών ισοτιμιών εξωτερικού δολαρίου, ευρώ, γιουάν κλπ., μεγάλο μέρος της αστάθειας του θορύβου και των τιμών μπορεί να είναι γεγονός που καθιστά μια καλύτερη ανάλυση των δεδομένων. Συγκρίνοντας τον τρόπο με τον οποίο οι παραλλαγές σε αρκετά κοινά χαρακτηριστικά των κρυπτοσυχνοτήτων επηρεάζει τις σχετικές τιμές τους με το bitcoin, μπορούν να εντοπιστούν παράγοντες που επηρεάζουν τον σχηματισμό αξιών.

Η αρχική τεχνολογία blockchain έχει φέρει πολλές νέες πτυχές στο πώς σκεφτόμαστε τα χρήματα σήμερα, αλλά επειδή είναι ένας νέος τρόπος τραπεζικής, ο οποίος δεν έχει ακόμη ωριμάσει, εξακολουθεί να περιλαμβάνει αρκετές αδυναμίες ή ευκαιρίες ανάπτυξης. Η τεχνολογία με τα μέσα της έχει δημιουργήσει έδαφος για την εφεύρεση και την παροχή εναλλακτικών κερμάτων ή λύσεις για πρόσθετα χαρακτηριστικά ή κενά ασφαλείας. Επί του παρόντος, υπάρχουν πάνω από 1000 εναλλακτικοί τύποι κερμάτων και 18 από αυτούς έχουν ήδη μεγαλύτερο όγκο χρηματοδότησης από 1 δισ. δολάρια¹⁵.

Σε αυτό το σημείο όλοι γνωρίζουμε, ότι bitcoin ήταν το πρώτο κρυπτονόμισμα που έχει ξεκινήσει ποτέ και έχει τους περισσότερους χρήστες και την κεφαλαιοποίηση της αγοράς από σήμερα, αλλά το 2009, όταν τέθηκε σε λειτουργία, υπήρχαν ορισμένοι περιορισμοί στον κώδικα για την πρόληψη μελλοντικών καταχρήσεων. Ένας από αυτούς τους περιορισμούς ήταν το μέγεθος ενός μπλοκ. Αρχικά ήταν 1 Mbyte, το οποίο έχει ρυθμιστεί για να προστατεύσει το δίκτυο από την υπερφόρτιση μέσω ανεπιθύμητης αλληλογραφίας ή επιθέσεων και αποχωρήσεων. Πιθανότατα, ακόμη και ο δημιουργός του blockchain δεν περίμενε μια τέτοια δημοτικότητα για την τεχνολογία, καθώς ήδη από το 2015 ένα μπλοκ περιλάμβανε 600 Kbytes δεδομένων.

¹⁵ Mullan, P., (2014), *The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations*. U.S.A.: Palgrave Macmillan US

Αυτό σήμαινε ότι το 60% της χωρητικότητας του blockchain έχει ήδη εξαντληθεί και το 2006 περίπτωση που θα είχε αυξηθεί πάνω από 1 Mbyte, οι χρήστες θα έπρεπε να περιμένει πολύ περισσότερο τους χρόνους επεξεργασίας των συναλλαγών, καθιστώντας το δίκτυο λιγότερο ανταγωνιστικό έναντι των παραδοσιακών μέσων πληρωμής¹⁶.

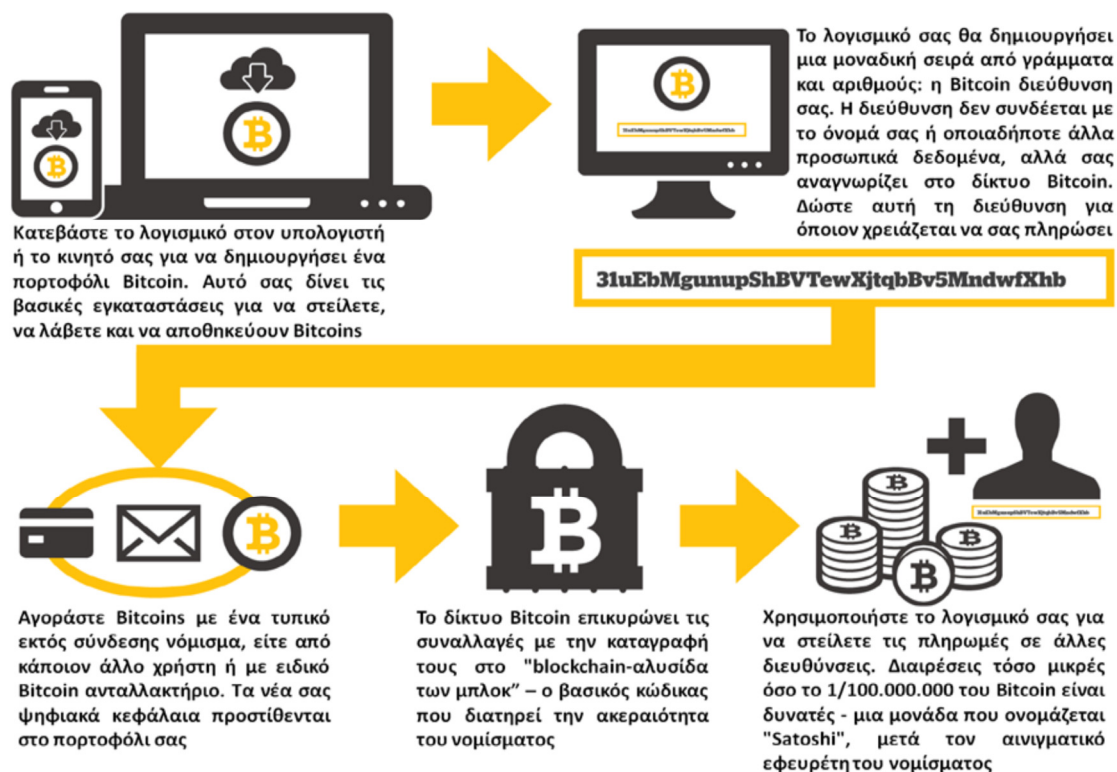
Ένα νόμισμα έχει τρεις λειτουργίες. Πρώτον, χρησιμεύει ως μέσο πληρωμής, με τη μορφή χαρτονομισμάτων και κερμάτων. Δεύτερον, χρησιμεύει ως λογιστική μονάδα που χρησιμοποιείται για να εκφράσει τις τιμές, την εξοικονόμηση, υποθήκες. Τρίτον, συμβάλλει στη διατήρηση της αξίας αποταμίευσης. Θεωρητικά, μπορεί να ειπωθεί ότι το Bitcoin πληροί τους τρεις ρόλους ενός νομίσματος, αλλά στην πράξη αυτό δεν συμβαίνει. Ο ρόλος του ως μέσου πληρωμών προϋποθέτει ότι υπάρχει ευρεία αποδοχή για το νόμισμα στην κοινωνία, αλλιώς είναι δύσκολο να το χρησιμοποιήσει κανείς για να κάνει τις πληρωμές. Σε πολλές χώρες, δεν υπάρχει τέτοια ευρεία αποδοχή και οι δυνατότητες χρήσης Bitcoin ως μέσο πληρωμής, επομένως, είναι πολύ περιορισμένη στην πράξη. Ομοίως, είναι ασυνήθιστο οι τιμές να εκφράζονται σε Bitcoin, αν και αυτό συμβαίνει. Επομένως, δεν μπορεί να λεχθεί ότι το Bitcoin χρησιμεύει ως γενικώς αποδεκτή λογιστική μονάδα. Τέλος, η υψηλή μεταβλητότητα της συναλλαγματικής ισοτιμίας Bitcoin το καθιστά ακατάλληλο για τη διατήρηση της αξίας, επειδή η αγοραστική δύναμη του μπορεί πολύ γρήγορα να μειωθεί και ένα μεγάλο μέρος της αξίας τότε χάνεται. Μια άλλη διαφορά μεταξύ του Bitcoin και των παραδοσιακών εθνικών νομισμάτων, είναι ότι τα τελευταία απολαμβάνουν ειδικό νομικό καθεστώς στη χώρα έκδοσής τους.

¹⁶ Mullan, P., (2014), *The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations*. U.S.A.: Palgrave Macmillan US

ΚΕΦΑΛΑΙΟ 2^ο: Η ΠΑΡΑΓΩΓΗ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΟΣ ΚΑΙ Η ΚΟΣΤΟΛΟΓΗΣΗ ΑΥΤΟΥ

2.1 Η χρήση του κρυπτονομίσματος

Ένα ψηφιακό νόμισμα που έχει εξέχουσα θέση και ξεχωρίζει των υπολοίπων είναι το Bitcoin (BTC), το οποίο αποτελεί πρωτοπόρο αποκεντρωμένο κρυπτονόμισμα και το συντριπτικό μέγεθος των υπολοίπων είναι παραλλαγές του και είχαν να κάνουν με τις ίδιες καινοτομίες που εισήγαγε αυτό, μεταβάλλοντας ορισμένες παραμέτρους στους αλγόριθμους. Το BTC είναι ένα νόμισμα σε ένα σύστημα ηλεκτρονικών συναλλαγών που βασίζεται στα πρωτόκολλα της κρυπτογράφησης και εμπεριέχει ψηφιακές υπογραφές για να δίνει τον πλήρη έλεγχο της ιδιοκτησίας. Οι συναλλαγές γίνονται μεταξύ των δύο μερών σε ένα δίκτυο διαμοιρασμού (peer-to-peer), χωρίς να εμπλέκονται τρίτα χρηματοπιστωτικά ιδρύματα για τον έλεγχο και πιστοποίηση της συναλλαγής. Ο ρόλος των τρίτων φορέων αντικαθίσταται από τους χρήστες του δικτύου που μοιράζονται τους πόρους των υπολογιστών τους, από όπου παράγονται τα BTCs (mining) και μπορούν να αποθηκευτούν ψηφιακά. Εφόσον επαληθευτούν και καταγραφούν οι συναλλαγές (miners) στην αλυσίδα των μπλοκ (blockchain) που περιέχουν όλες τις συναλλαγές που έχουν προηγηθεί και ακολουθούν το κάθε νόμισμα, γίνονται αποδεκτές από το εκάστοτε μέλος του δικτύου. Έτσι η διαδικασία αυτή δεν έχει να κάνει με την διττή πληρωμή με το ίδιο νόμισμα, διότι δεν θα γίνει δεκτή από την κοινότητα, η οποία έχει την μεγαλύτερη υπολογιστική ισχύ. Τα μέλη που έχουν αποχωρήσει και ξαναμπεί στο δίκτυο αποδέχονται την υπάρχουσα επαληθευμένη και καταγεγραμμένη blockchain. Στη παρακάτω εικόνα φαίνονται οι ενέργειες που πρέπει να γίνουν για να χρησιμοποιηθεί το Bitcoin.

Εικόνα 1**ΠΩΣ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΣΕΤΕ BITCOINS**

Πηγή: www.aatcomment.org

Στη συνέχεια στην εικόνα 2 φαίνονται τα στάδια της συναλλαγής κρυπτονομισμάτων που γίνονται μεταξύ δύο ατόμων, τα οποία στη συνέχεια αναλύονται ανά στάδιο.

Εικόνα 2

Πως λειτουργεί μία συναλλαγή με Bitcoin

Ο Bob, σε διαδικτυακός έμπορος, αποφασίζει να αρχίσει να δέχεται bitcoins ως πληρωμή. Η Alice, ένας αγοραστής, έχει bitcoins και θέλει να αγοράσει εμπορεύματα από τον Bob.

ΠΟΡΤΟΦΟΛΙΑ ΚΑΙ ΔΙΕΥΘΥΝΣΕΙΣ

Και ο Bob και η Alice έχουν "πορτοφόλια" στην ηλεκτρονική τους υπολογιστική μηχανή.

Το πορτοφόλιο είναι αρχίον που κρύβουν πληροφορίες σε κωδικούς διευθύνσεις Bitcoin.

Μία διευθύνση είναι μία σειρά από γράμματα και νούμερα, όπως:

```
1KJLmNp
KdVcH
43WqEzYb
1CwDxH
```

ΔΗΜΙΟΥΡΓΗΣΗ ΜΙΑΣ ΚΑΡΙΟΥΡΠΙΑ ΔΙΕΥΘΥΝΣΗΣ

Ο Bob δημιουργεί μια κωδικόφιλη διεύθυνση για την Alice για να στείλει εκεί την πληρωμή της.

Κάθε διευθύνση έχει το δικό της υπολογιστικό κλειδί.

ΥΠΟΒΑΛΛΟΝΤΑΙ ΜΙΑ ΠΛΗΡΩΜΗ

Όταν ο Bob δημιουργεί μία κωδικόφιλη διεύθυνση, αυτό που πραγματικά κάνει είναι να παράγει ένα ζεύγος κρυπτογραφικών κλειδιών, αποτελείται από ένα ιδιωτικό κλειδί και ένα δημόσιο κλειδί. Εάν υπογράψεις ένα μήνυμα με ένα ιδιωτικό κλειδί (που μόνο σου γνωρίζεις), μπορεί να επαληθευτεί χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί (που είναι γνωστό σε όλους). Η νέα διεύθυνση Bitcoin του Bob αντιπροσωπεύει ένα μοναδικό δημόσιο κλειδί και το αντιστοιχείονόμοιο ιδιωτικό κλειδί είναι αποθηκευμένο στο πορτοφόλι του. Το δημόσιο κλειδί απεμπνέεται αποκρίματα να επαληθεύσει ότι ένα μήνυμα που υπογράφεται από το ιδιωτικό κλειδί είναι άψευδο.

Ο Gary, ο Sarah και ο Steve είναι αθλητικοί Bitcoin.

Οι υπολογιστές τους εφοδιάζουν τις συναλλαγές τα τελευταία 10 λεπτά σε ένα νέο κωδικό συναλλαγής.

ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΣΥΝΑΛΛΑΓΗΣ

Οι υπολογιστές εφόρμη υπολογίζουν όλες τις συναλλαγές που έχουν συσταθεί για την υπολογιστική κρυπτογραφική συνάρτηση συναλλαγών.

Οι υπολογιστές εφόρμη υπολογίζουν όλες τις συναλλαγές που έχουν συσταθεί για την υπολογιστική κρυπτογραφική συνάρτηση συναλλαγών.

ΕΠΑΛΗΘΕΥΣΗ ΣΥΝΑΛΛΑΓΗΣ

Όσο γρήγορα ο κωδικός η μεταφορά της Alice στον Bob θαφύεται τόσο από άλλους, που πρόκειται συναλλαγής. Όπως θέλει να πραγματοποιήσει το εμπόριο, θα πρέπει να επαληθεύσει τη δουλειά που έκανε ο Gary, Sarah και Steve, απεμπνέοντας αποκρίματα για επαλήθευση επαλήθευση κωδικών, στη συνέχεια, επαληθεύονται την εργασία όλων των μελών της ομάδας. Ένα τέτοιο κομμάτι είναι σχεδόν αδύνατο.

Κρυπτογραφικοί Καταχωρημένοι

Οι λειτουργίες κρυπτογραφικών καταχωρημένων μετατρέπουν μια συλλογή δεδομένων σε ένα αλφαριθμητικό σειρά με ένα σταθερό μήκος και αποκάλυψη της καταχωρημένου. Ακόμη και μικρές αλλαγές στα αρχικά δεδομένα αλλάζει δραματικά την προκύπτουσα της καταχωρημένου. Και είναι αδύνατο αδύνατο να προβλεφθεί ποιο αρχικό σύνολο δεδομένων θα δημιουργήσει μια οριστική καταχωρημένου.

Η Alice είναι των κωδικών: 6666 9999 8888 (36 χαρακτήρες)

Η Alice είναι των κωδικών: 6666 8888 8888...

Η Alice είναι των κωδικών: 6666 6666 8888...

Νόμος για να δημιουργήσει διαφορετικές της καταχωρημένου από τα ίδια δεδομένα, το Bitcoin χρησιμοποιεί "hashes". Ένα hash είναι σειρά από χαρακτήρες αριθμούς που προστίθεται στα δεδομένα πριν τον καταχωρημένου. Αλλάζοντας την ποσότητα, μια ελαφρώς διαφορετική της καταχωρημένου.

Εάν μπορεί επαληθεύσει με "hashes" συλλογή κωδικών είναι με βάση καλύτερα λειτουργία με διεύθυνση) που κωδικός 30 κωδικούς (σε κωδικούς από 4 κωδικούς 2018) (και 20 κωδικούς) για 15 μήνες που επαληθεύονται, σε μια περίπτωση, η Gary και Steve διαβάζουν διαφορετικά συλλογικά του δικού με σειρά τα κωδικούς Bitcoin.

ΕΠΑΛΗΘΕΥΣΗ ΣΥΝΑΛΛΑΓΗΣ

Όσο γρήγορα ο κωδικός η μεταφορά της Alice στον Bob θαφύεται τόσο από άλλους, που πρόκειται συναλλαγής. Όπως θέλει να πραγματοποιήσει το εμπόριο, θα πρέπει να επαληθεύσει τη δουλειά που έκανε ο Gary, Sarah και Steve, απεμπνέοντας αποκρίματα για επαλήθευση επαλήθευση κωδικών, στη συνέχεια, επαληθεύονται την εργασία όλων των μελών της ομάδας. Ένα τέτοιο κομμάτι είναι σχεδόν αδύνατο.

Πηγή: Palacio, 2012

Έστω ότι ο Νίκος είναι έμπορος ο οποίος δέχεται Bitcoins και η Μαρία θέλει να πραγματοποιήσει αγορά στέλνοντάς του BTCs. Με εγκατεστημένες τις αντίστοιχες εφαρμογές του κρυπτονομίσματος στα τηλέφωνα, τις ταμπλέτες ή τους ηλεκτρονικούς υπολογιστές τους, έχουν και οι δύο πρόσβαση στα πορτοφόλια και τις διευθύνσεις τους.

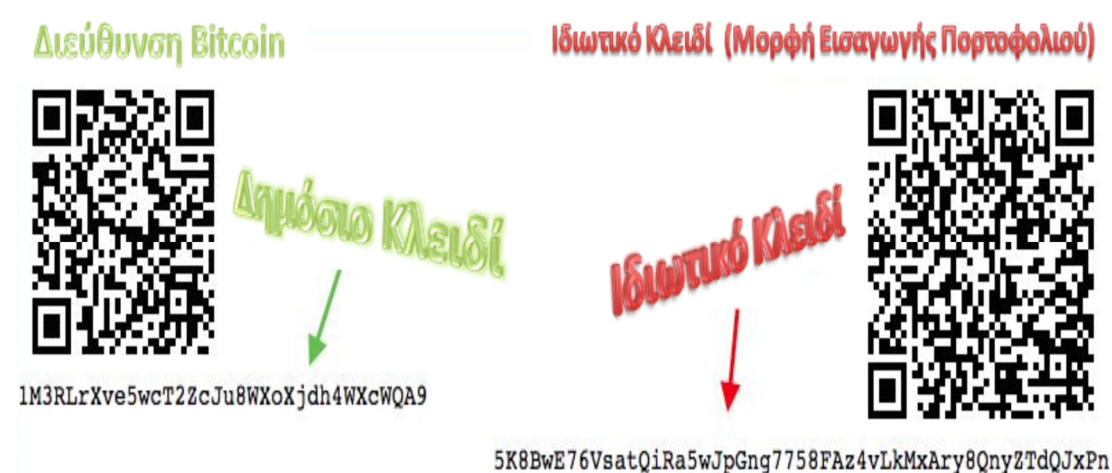
Εικόνα 3



Πηγή: Palacio, 2012

Όταν δημιουργείται μία διεύθυνση γεννιέται ένα ζευγάρι από κρυπτογραφημένα κλειδιά, το δημόσιο και το ιδιωτικό.

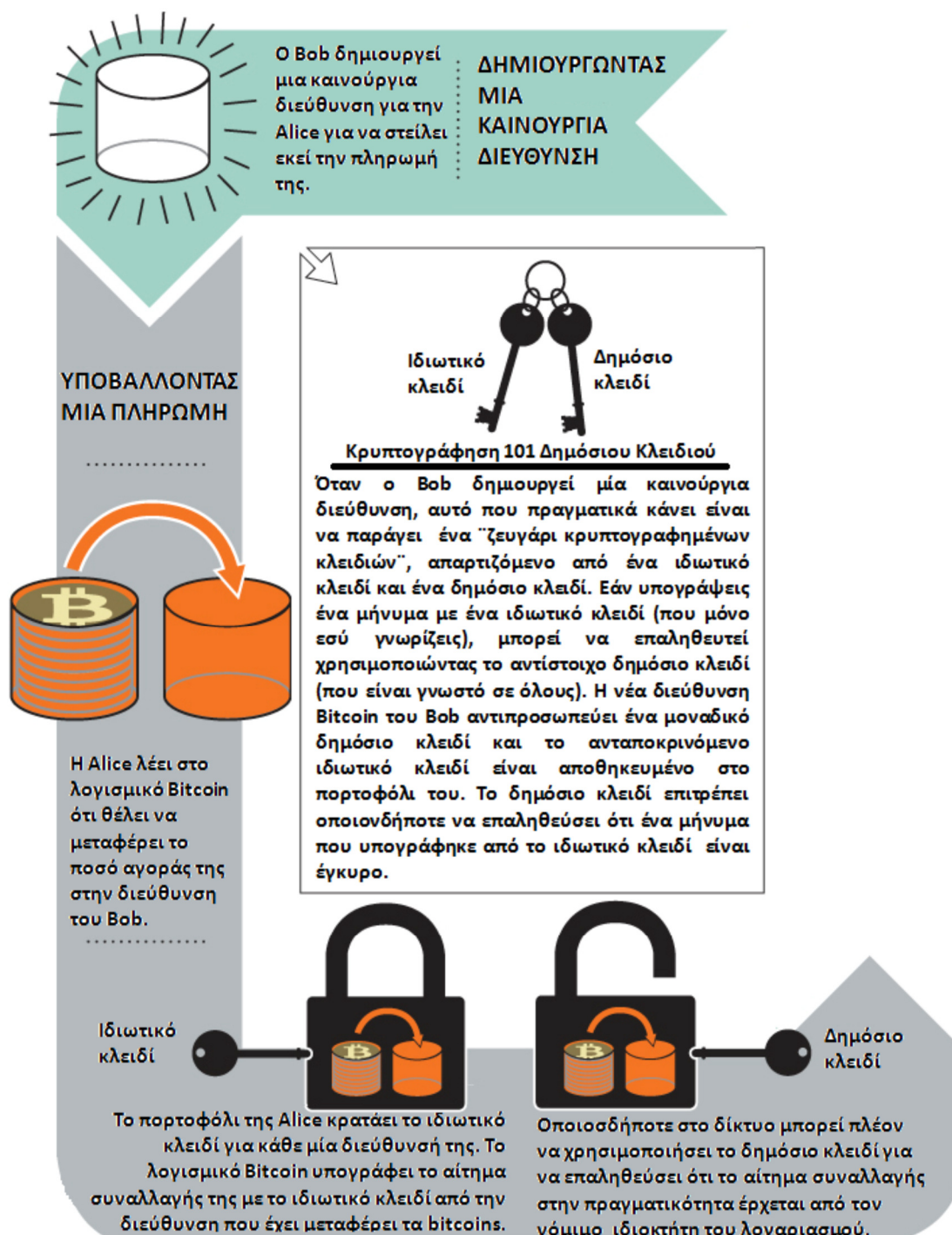
Εικόνα 4



Πηγή: Beigel, 2015

Η Μαρία, έχοντας πρόσβαση στο πορτοφόλι της, χρησιμοποιεί ένα από τα ιδιωτικά της κλειδιά με το οποίο υπογράφεται η συναλλαγή που θέλει να κάνει, καθώς και μία ή περισσότερες διευθύνσεις (δημόσια κλειδιά) του Νίκου όπου θα στείλει τα BTC. Το κάθε ιδιωτικό κλειδί αντιστοιχεί σε μια διεύθυνση από το πορτοφόλι, η οποία αναλογεί σε ένα ποσό BTC.

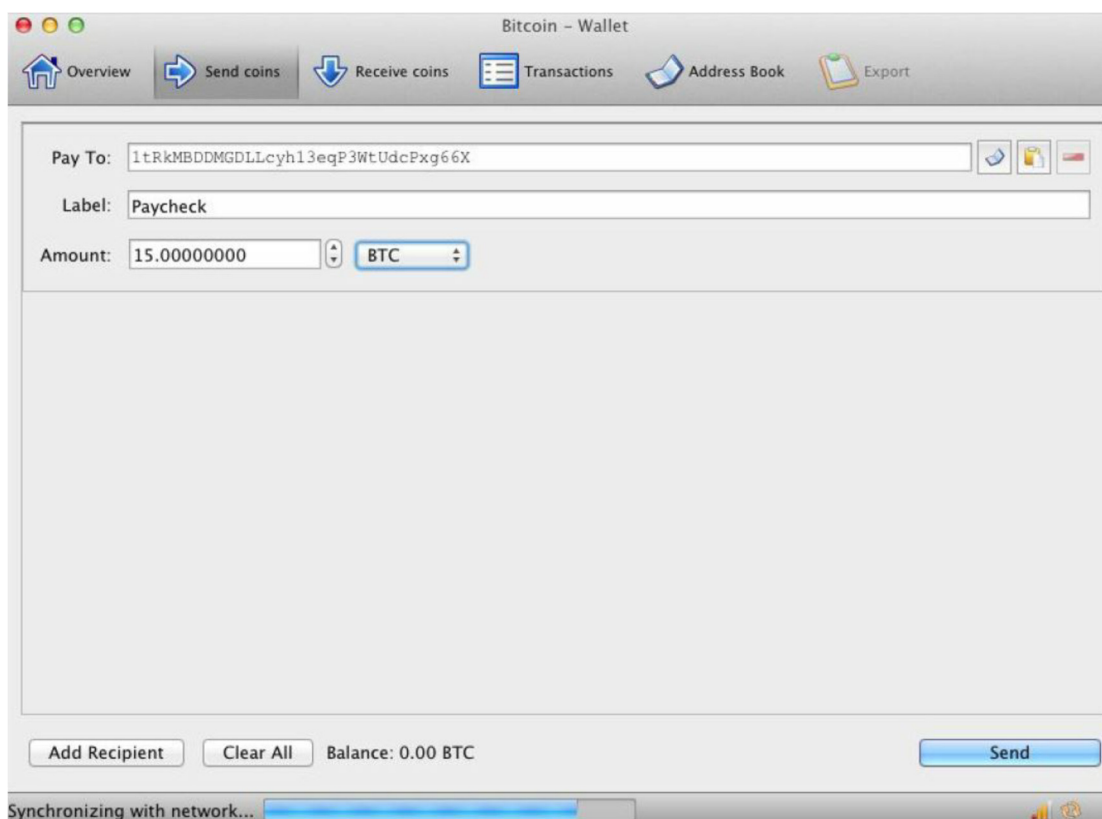
Εικόνα 5



Πηγή: Palacio, 2012

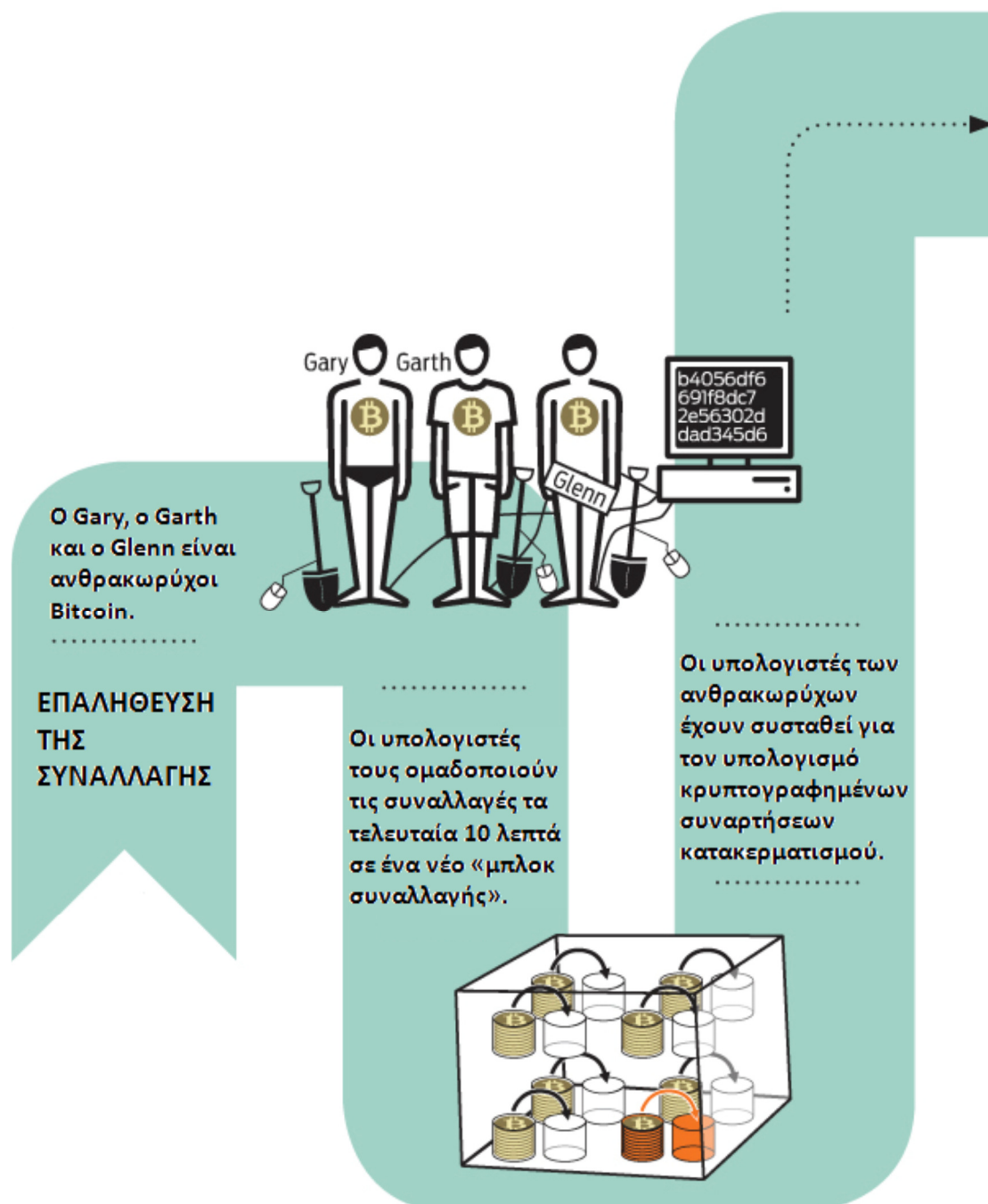
Η Μαρία προσθέτει το δημόσιο κλειδί που αποτελεί τη διεύθυνση προορισμού και το ποσό που θέλει να στείλει στα αντίστοιχα κενά συμπλήρωσης της καρτέλας του λογισμικού και το αποστέλλει, περιμένοντας την επιβεβαίωση από το δίκτυο BTC (επίλυση προβλήματος από miners).

Εικόνα 6



Πηγή: Clark, 2013

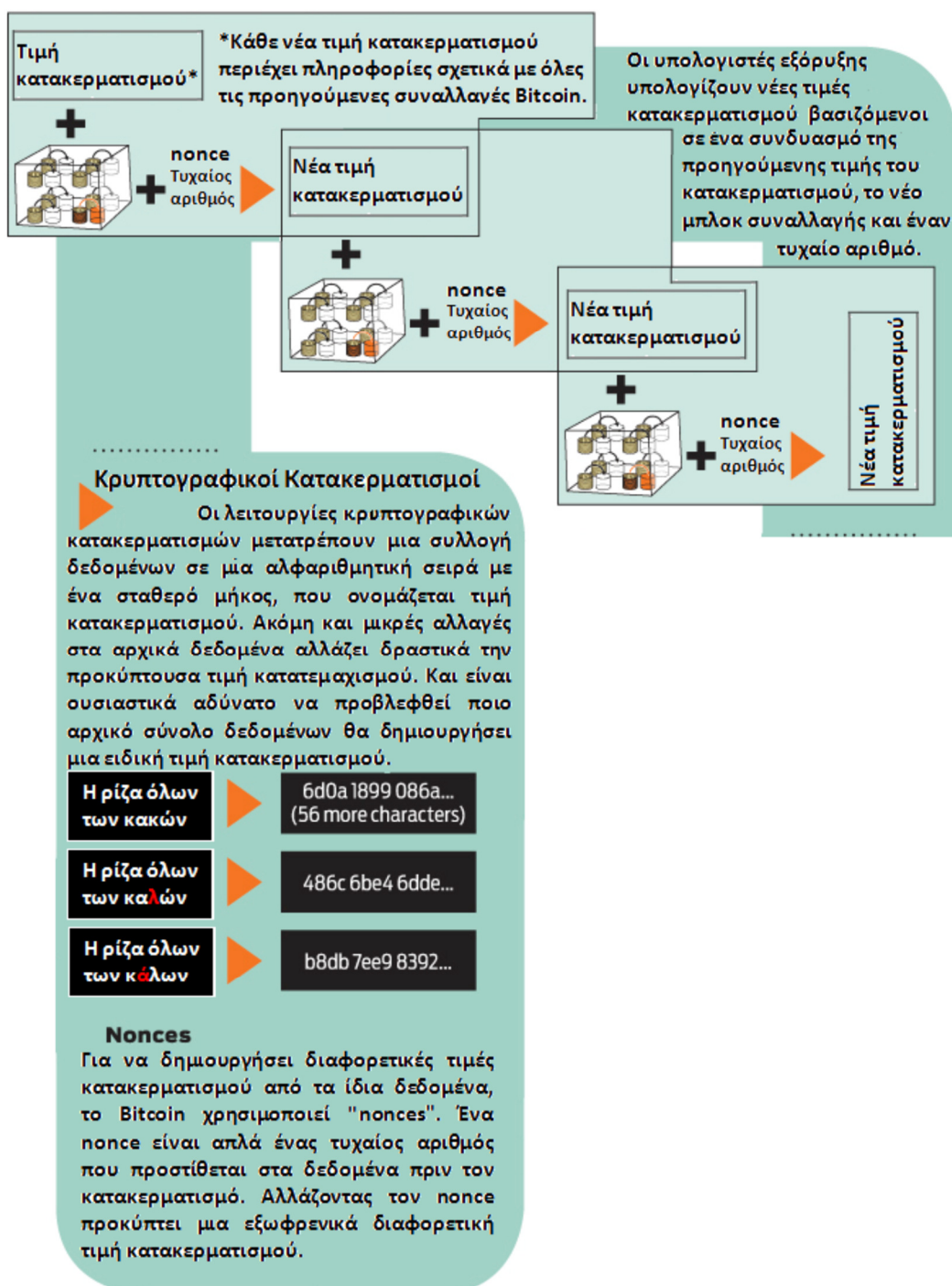
Το αντίστοιχο δημόσιο κλειδί που αποτελεί ζεύγος του ιδιωτικού και το οποίο είναι γνωστό σε όλους τους χρήστες του δικτύου, χρησιμοποιείται για την επαλήθευση της νόμιμης συναλλαγής. Ανά δέκα λεπτά, δημιουργείται ένα μπλοκ με όλες τις ανεπιβεβαίωτες συναλλαγές που δεν υπάρχουν σε άλλο μπλοκ. Οι ανθρακωρύχοι (miners) είναι αυτοί οι οποίοι με την υπολογιστική ισχύ των ηλεκτρονικών υπολογιστών τους προσπαθούν να υπολογίσουν τις κρυπτογραφημένες συναρτήσεις κατακερματισμού.

Εικόνα 7

Πηγή: Palacio, 2012

Με τον κατακερματισμό (hash) των δεδομένων προκύπτει μια αλφαριθμητική σειρά συγκεκριμένου μήκους, όπου σε κάθε πρωτότερη από το hash αλλαγή δεδομένων δίνει διαφορετικό αποτέλεσμα. Μετά από κάθε κατακερματισμό είναι ουσιαστικά αδύνατο να προβλεφτούν τα αρχικά δεδομένα που έδωσαν τη συγκεκριμένη τιμή. Το σύστημα του κρυπτονομίσματος προσθέτει ένα τυχαίο αριθμό (nonce) στα δεδομένα πριν το hash ώστε μετά να υπάρξει διαφορετικό αποτέλεσμα, το οποίο περιλαμβάνει πληροφορίες των προηγούμενων συναλλαγών του BTC. Η διαδικασία επαναλαμβάνεται για τις επόμενες συναλλαγές με νέα τιμή κατακερματισμού.

Εικόνα 8



Πηγή: Palacio, 2012

Το σύστημα του κρυπτονομίσματος απαιτεί η αλφαριθμητική σειρά που προκύπτει μετά τον κατακερματισμό, να έχει μπροστά ένα συγκεκριμένο αριθμό μηδενικών, κάτι το οποίο επιτυγχάνεται με μοναδικό συνδυασμό των αρχικών δεδομένων και του nonce πριν το hash.

Εικόνα 9


Η ρίζα όλων
των κακών ???

▶

0000 0000
0000 ...

Η δημιουργία κατακερματισμών είναι υπολογιστικά ασήμαντη, αλλά το σύστημα Bitcoin απαιτεί η νέα τιμή κατακερματισμού να έχει μια συγκεκριμένη μορφή, συγκεκριμένα, θα πρέπει να ξεκινάει με έναν ορισμένο αριθμό μηδενικών.

Οι ανθρακωρύχοι δεν έχουν τρόπο να προβλέψουν ποιο nonce θα παράγει μία κατακερματισμένη



τιμή με τον απαιτούμενο αριθμό των αρχικών μηδενικών. Έτσι, είναι αναγκασμένοι να δημιουργήσουν πολλούς κατακερματισμούς με διαφορετικές nonces μέχρι να συμβεί μετά αυτό που λειτουργεί.

Ανάλογα με την επιλογή του nonce έχουμε και έναν συγκεκριμένο αριθμό μηδενικών μετά το hash.


Εικόνα 10

| nonce | hash |
|-----------|---|
| 0 | 5c56c2883435b38aeba0e69fb2e0e3db3b22448d3e17b903d774dd5650796f76 |
| 1 | 28902a23a194dee94141d1b70102accd85fc2c1ead0901ba0e41ade90d38a08e |
| 2 | 729577af82250aaf9e44f70a72814cf56c16d430a878bf52fdaceeb7b4bd37f4 |
| 3 | 8491452381016cf80562ff489e492e00331de3553178c73c5169574000f1ed1c |
| 39 | 03fd5fff1048668cd3cde4f3fb5bde1ff306d26a4630f420c78df1e504e24f3c7 |
| 990 | 0001e3a4583f4c6d81251e8d9901dbe0df74d7144300d7c03cab15eca04bd4bb |
| 52117 | 0000642411733cd63264d3bedc046a5364ff3c77d2b37ca298ad8f1b5a9f05ba |
| 1813152 | 00000c94a85b5c06c9b06ace1ba7c7f759e795715f399c9c1b1b7f5d387a319f |
| 19745650 | 000000cdccf49f13f5c3f14a2c12a56ae60e900c5e65bfe1cc24f038f0668a6c |
| 243989801 | 0000000ce99e2a00633ca958a16e17f30085a54f04667a5492db49bcae15d190 |
| 856192328 | 0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50 |

Οι miners επιδιώκουν να βρουν το συνδυασμό γι' αυτό και γίνονται πολλά hash με συνδυασμούς nonce έως ότου βρεθεί το σωστό από κάποιον μέσα σε 10 λεπτά, όπου και δημιουργείται το μπλοκ που χρονοσημαίνεται στην blockchain και επιβραβεύεται ο miner με 25 BTC (2015). Η επιβράβευση υποδιπλασιάζεται ανά 210.000 μπλοκ, περίπου κάθε 4 χρόνια. Μετά από την επαλήθευση των συναλλαγών η ίδια διαδικασία συνεχίζεται με την χρήση του καινούργιου πλέον μπλοκ για την δημιουργία του επόμενου.

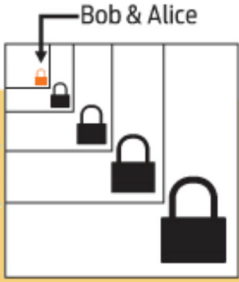
Εικόνα 10

Κάθε μπλοκ περιλαμβάνει μία "coinbase" συναλλαγή (είσοδος bitcoins με χρήση αυθαίρετων δεδομένων ως διεύθυνση) που πληρώνει 50 bitcoins (με υποδιαίρεση κάθε 4 χρόνια-τώρα (2015) είναι 25 bitcoins) για τη νίκη του ανθρακωρύχου, σε αυτή την περίπτωση, ο Gary. Μια νέα διεύθυνση δημιουργείται στο πορτοφόλι του Gary με υπόλοιπο τα νεόκοπα bitcoins.



ΕΠΑΛΗΘΕΥΣΗ ΣΥΝΑΛΛΑΓΩΝ

Όσο περνά ο καιρός, η μεταφορά της Alice στον Bob θάβεται κάτω από άλλες, πιο πρόσφατες συναλλαγές. Όποιος θέλει να τροποποιήσει τα στοιχεία, θα πρέπει να επαναλάβει τη δουλειά που έκανε ο Gary, επειδή τυχόν αλλαγές απαιτούν μια εντελώς διαφορετική επιτυχία πορσε-και, στη συνέχεια, επαναλαμβάνει την εργασία όλων των μετέπειτα ανθρακωρύχων. Ένα τέτοιο κατόρθωμα είναι σχεδόν αδύνατο.



Πηγή: Palacio, 2012

2.2 Τρόποι απόκτησης του κρυπτονομίσματος

Στην έκθεση που έγινε από την Ευρωπαϊκή Κεντρική Τράπεζα έγινε γνωστό πως υπάρχουν πέντε τρόποι προκειμένου να αποκτηθεί το κρυπτονόμισμα και είναι μέσω της αγοράς τους, της ανταμοιβής για ενεργό συμμετοχή των ενδιαφερομένων σε διάφορες δραστηριότητες, την εξόρυξη αυτών, την λήψη τους ως πληρωμή και ως δωρεά.

Υπάρχουν διάφορες διαδικτυακές υπηρεσίες που πουλάνε κρυπτονομίσματα (Bitstamp), και παρέχουν υπηρεσίες πορτοφολιού για τις συναλλαγές τους (Electrum) φέρνουν σε επαφή αγοραστές και πωλητές κρυπτονομισμάτων (Localbitcoins), μετατρέπουν τις πληρωμές εμπόρων από κρυπτονόμισμα σε παραστατικό χρήμα (Coincorner), κάνουν αγοραπωλησίες κρυπτονομισμάτων (Bitbargain), αποθηκεύουν και ασφαλίζουν τα κρυπτονομίσματα των κατόχων (Xapo), καθώς και άλλες που παρέχουν συνδυασμούς των προηγούμενων υπηρεσιών (Coinbase, Bitpay).

Εκτός από την απόκτηση των ψηφιακών νομισμάτων μέσω διαδικτύου, μπορεί κάποιος να προμηθευτεί το κρυπτονόμισμα BTC μέσω ειδικών ATM, προσφάτως και στην

Ελλάδα, με δωρεάν άυλη χρεωστική κάρτα BTC (MasterCard) και πλαστική με χρέωση 20\$ Αμερικής που κυκλοφόρησε η εταιρία Xapo (xapo.com, 2015), ενώ υπάρχουν νομίσματα σε φυσική μορφή που αντιπροσωπεύουν το BTC, όπως το Casascius Bitcoin πριν απαγορευτεί η κυκλοφορία του και εκδίδονται σε περιορισμένο αριθμό συνήθως για συλλέκτες ή ως πρόταση για δώρο.

2.3 Η παραγωγή του κρυπτονομίσματος

Τα Clients είναι λογισμικά που χρησιμοποιούνται για το δίκτυο του κρυπτονομίσματος, κάποια εκ των οποίων περιέχουν και πορτοφόλια τα οποία ελέγχονται από τα λογισμικά και με την χρήση των διευθύνσεών τους γίνεται η συναλλαγή των κρυπτονομισμάτων. Το Bitcoin Core ή Bitcoin-Qt ή Satoshi Client είναι το αρχικό λογισμικό του BTC, το οποίο βρίσκεται υπό την επίβλεψη μιας ομάδας προγραμματιστών που έχουν αναλάβει την αναβάθμιση του για την σωστή λειτουργία του δικτύου. Το λογισμικό χρησιμοποιεί μια νέα διεύθυνση για κάθε συναλλαγή BTC που αναπαράγεται σε μια δεξαμενή κλειδιού με 100 νέες αχρησιμοποίητες διευθύνσεις και η οποία αναπληρώνεται μετά τη χρήση της. Κάθε φορά χρησιμοποιείται η πρώτη διεύθυνση που δημιουργήθηκε, ακολουθώντας την μέθοδο first-in-first-out (FIFO). Το Client αποθηκεύει όλη την blockchain στον υπολογιστή, όπου σήμερα ανέρχεται στα 60.71 GB και με τη σύνδεση στο σύστημα BTC ο υπολογιστής αποτελεί ένα κόμβο με τον οποίο γίνεται η επιβεβαίωση των συναλλαγών. Επίσης, η πρόσβαση στα BTC γίνεται μόνο από τον υπολογιστή που έχει εγκατεστημένο το λογισμικό και η κλωνοποίησή του σε άλλον υπολογιστή θα προκαλέσει σύγχυση λειτουργίας, αφού ο κάθε ένας θα παράγει τις δικές του διευθύνσεις. Είναι ένα ολοκληρωμένο λογισμικό το οποίο συνδέεται κατευθείαν στο δίκτυο του BTC, χωρίς τρίτους μεσάζοντες και χρησιμοποιείται και για mining. Τα Clients που συναντάμε σε κατηγορίες είναι τα εξής:

1. Full Client: είναι αυτόνομο λογισμικό, όπως το Bitcoin Core, το οποίο καταγράφει όλη την blockchain στον υπολογιστή και με την σύνδεση στο δίκτυο BTC και τη διαχείριση των πορτοφολιών του χρήστη κάνει την συναλλαγή, χωρίς τρίτους μεσάζοντες ως παρόχους υπηρεσιών ή διακομιστές.
2. Light Client: είναι αυτά τα οποία δεν χρειάζονται την πλήρη καταγραφή της blockchain στον υπολογιστή, είναι πιο εύχρηστα και γρήγορα, χρησιμοποιώντας

λιγότερους υπολογιστικούς πόρους, αφού μέσω άλλου διακομιστή γίνεται η επικύρωση της συναλλαγής και εισαγωγή στο δίκτυο του κρυπτονομίσματος. Τα λογισμικά αυτά έχουν την δυνατότητα να αποθηκεύουν τα πορτοφόλια του χρήστη.

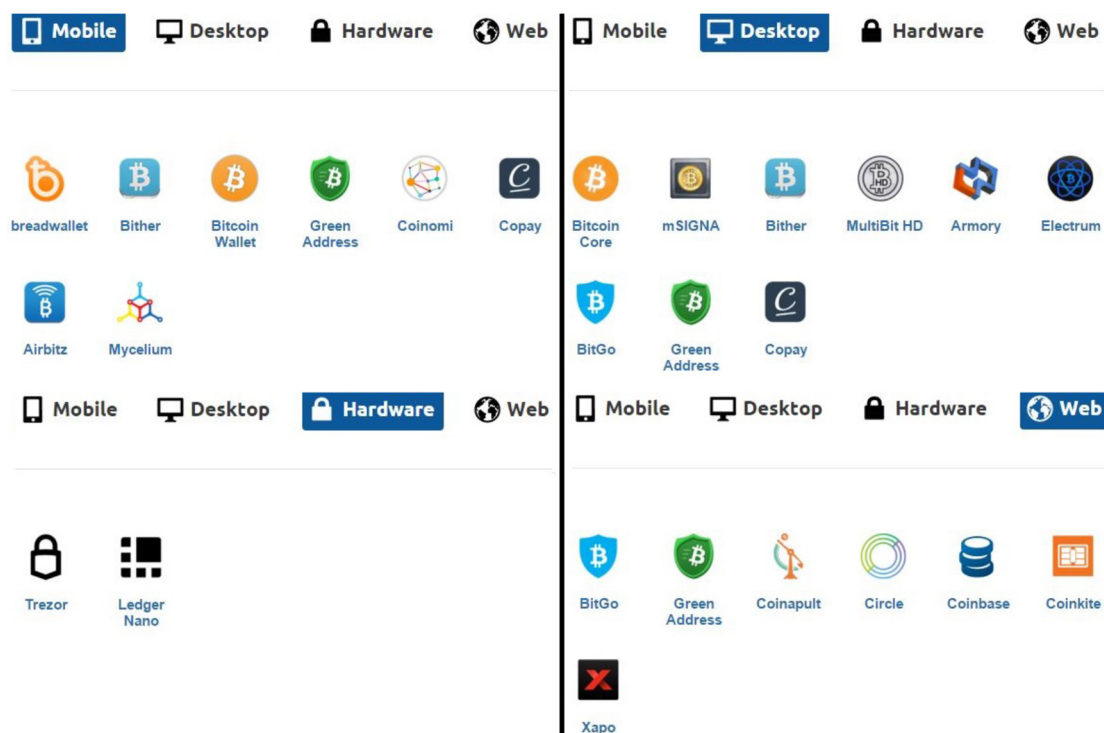
3. Web Client: βασίζονται εξολοκλήρου σε τρίτο διακομιστή, όπου αποθηκεύονται τα πορτοφόλια του χρήστη και με τον οποίο γίνονται οι συναλλαγές, ύστερα από είσοδο του μέσω ενός φυλλομετρητή.

4. Mobile Client: είναι λογισμικά για κινητές τηλεφωνικές συσκευές και ταμπλέτες και έχουν τα χαρακτηριστικά του ενός από τα τρία προαναφερόμενα τελευταία λογισμικά.

5. Mining Client: είναι ειδικά λογισμικά που εγκαθίστανται στον υπολογιστή για επεξεργασία και επιβεβαίωση των συναλλαγών στο peer-to-peer δίκτυο του κρυπτονομίσματος.

Υπάρχουν διάφορα πορτοφόλια όπως και Clients για επιλογή ανάλογα με τις ανάγκες των χρηστών.

Εικόνα 11



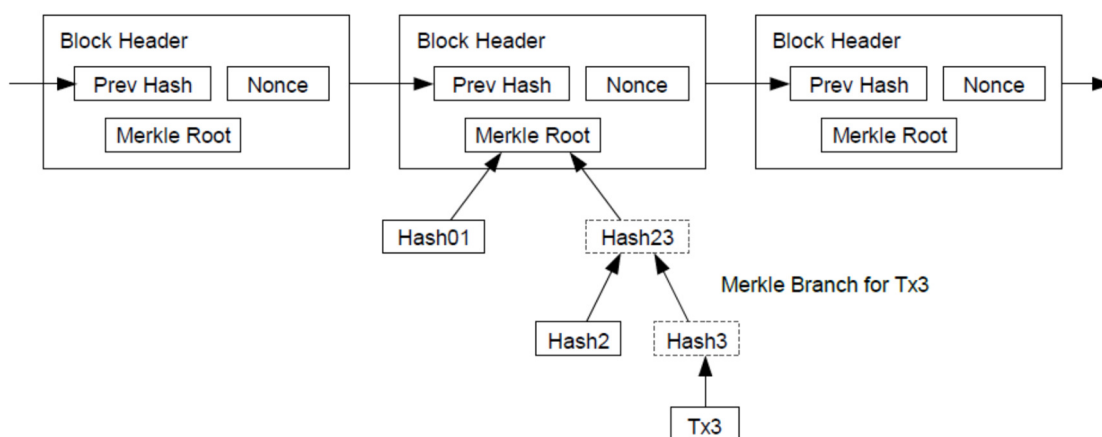
Τα είδη πορτοφολιών που συναντάμε είναι τα εξής:

1. Desktop wallet: είναι το πορτοφόλι που εγκαθίσταται σε υπολογιστές με διάφορα χαρακτηριστικά και «τρέχει» σε λειτουργικά Windows, Linux και Mac OSX. Κάποια από τα πορτοφόλια αυτά έχουν ιδιαίτερες λειτουργίες, όπως να συνδέονται άμεσα σε υπηρεσίες BTC, να έχουν αυξημένη ασφάλεια και να παρέχουν υψηλά επίπεδα ανωνυμίας με λειτουργίες mixing.
2. Mobile Wallet: είναι εφαρμογές για έξυπνες κινητές συσκευές τηλεφώνων και ταμπλέτων, δίνοντας τη δυνατότητα αποθήκευσης των ιδιωτικών κλειδιών και την πληρωμή μέσω της συσκευής. Λειτουργούν χρησιμοποιώντας SPV και το δίκτυο BTC με επαλήθευση πληρωμών, μέσω τρίτων διαμεσολαβητών, ώστε να μην χρειάζεται να «κατεβάζουν» ολόκληρη την blockchain. Κάποια έχουν επιπλέον χαρακτηριστικό πληρωμής την τεχνολογία NFC ή υποστηρίζουν smartwatches με λειτουργικό Android.
3. Paper wallet: είναι ένας φθηνός και εύκολος τρόπος αποθήκευσης των ιδιωτικών κλειδιών και διευθύνσεων με εκτύπωση σε χαρτί. Υπάρχουν υπηρεσίες πορτοφολιών που προσφέρονται από ιστοσελίδες, τα οποία παράγουν διευθύνσεις και κλειδιά σε εικόνα και με QR code προς διευκόλυνση του χρήστη.
4. Web Wallet: είναι πορτοφόλια που αποθηκεύουν τα ιδιωτικά κλειδιά σε υπολογιστές επιχειρήσεων συνδεδεμένους στο ιντερνέτ και κάποιες από τις επιχειρήσεις αυτές παρέχουν επιπλέον υπηρεσίες συγχρονισμού με τα mobile και desktop wallets. Υπάρχουν κάποια web wallets που επιτρέπουν την κρυπτογράφηση των ιδιωτικών κλειδιών πριν την αποθήκευση στον διακομιστή, ενώ άλλες την επιπρόσθετη αποθήκευση σε cold-storage μέσα.
(coindesk.com, 2015)
5. Cold-storage: είναι αποθήκες ιδιωτικών κλειδιών εκτός διαδικτυακής σύνδεσης και για την ύπαρξη συναλλαγής πρέπει να εισαχθούν σε πορτοφόλι εντός ή εκτός δικτύου. Τέτοιες αποθήκες είναι το paper wallet, οι εξωτερικοί σκληροί δίσκοι, τα usb flash drivers και BTC με φυσική υπόσταση, το hardware wallet και το offline wallet, το οποίο αποτελείται από συσκευή εκτός δικτύου (offline device) που έχει τα ιδιωτικά κλειδιά και στην οποία στέλνονται οι συναλλαγές για υπογραφή και έπειτα σε συνδεδεμένη συσκευή για την ολοκλήρωση της συναλλαγής.
6. Hardware wallet: είναι υλικό υπολογιστή που αποθηκεύονται τα ιδιωτικά κλειδιά για περισσότερη ασφάλεια και συμμετέχουν στην διαδικασία της συναλλαγής. Τα ιδιωτικά κλειδιά βρίσκονται πάντα στην συσκευή αυτή (hardware) και υπογράφεται η συναλλαγή,

συνήθως με πληκτρολόγηση ενός PIN από τα κουμπιά της συσκευής μέσα σε αυτήν, κατόπιν της σύνδεσης με το client wallet ή μέσω φυλλομετρητή σε κάποιο web wallet, όπου ο διακομιστής απλά διαβιβάζει την υπογεγραμμένη συναλλαγή. Οι συσκευές αυτές επιτρέπουν την δημιουργία αντιγράφου του ιδιωτικού κλειδιού σε κάποιο άλλο μέσο.

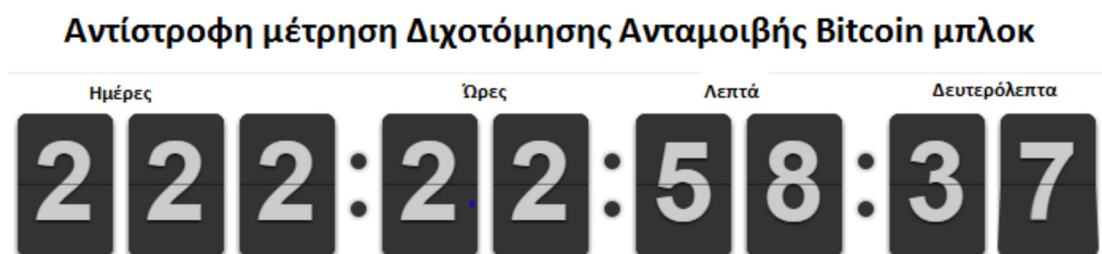
Από την στιγμή που θα παραχθεί η σωστή τιμή hash του Block Header από τον miner αναμεταδίδεται στο δίκτυο, ώστε να επιβεβαιωθεί από τους υπόλοιπους miners και να ενσωματωθεί το συγκεκριμένο καινούργιο μπλοκ στην blockchain για την έναρξη εύρεσης του επόμενου μπλοκ.

Εικόνα 12

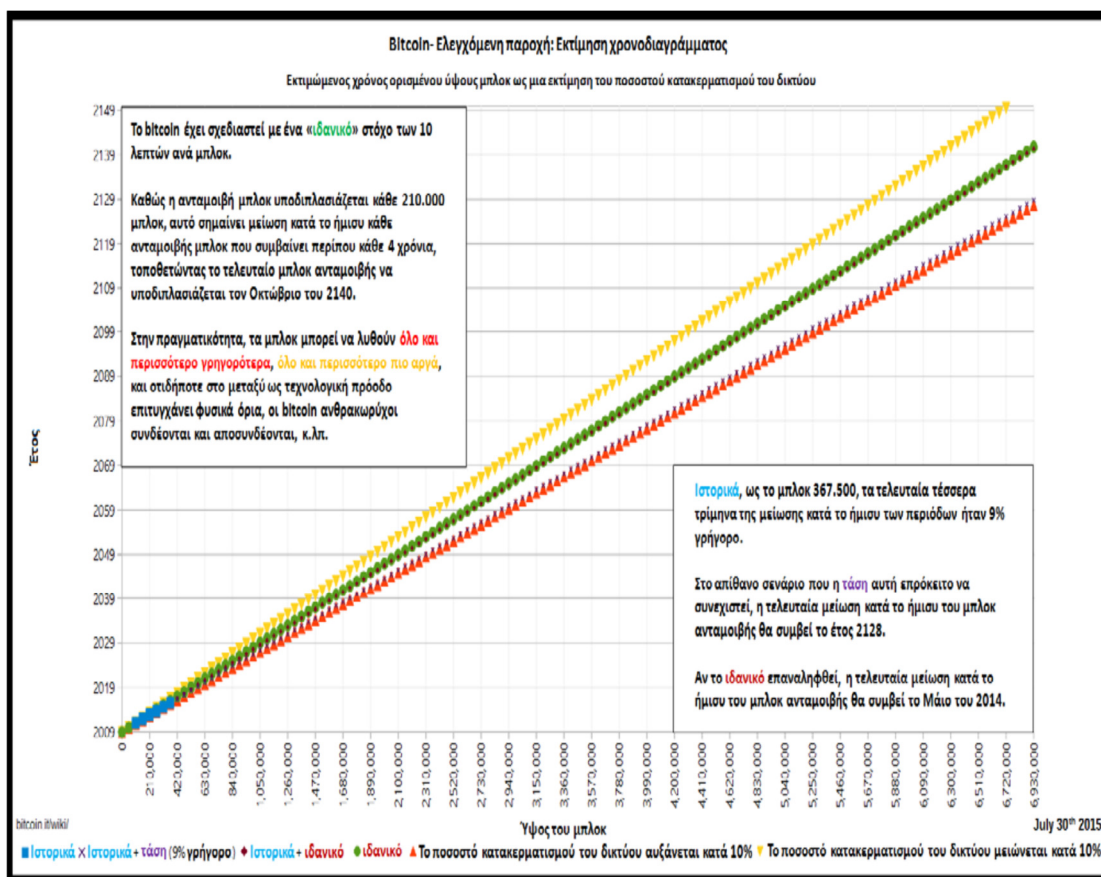


Η εύρεση του μπλοκ από κάποιον miner ξεκίνησε να επιβραβεύεται με 50 BTC, ενώ από το 2013 ανταμείβεται με 25 BTC έως και τον Ιούλιο του 2019, όπου υπολογίζεται ότι θα ξανά υποδιπλασιαστεί, κάτι το οποίο συμβαίνει κάθε φορά που δημιουργούνται 210.000 μπλοκ στην blockchain.

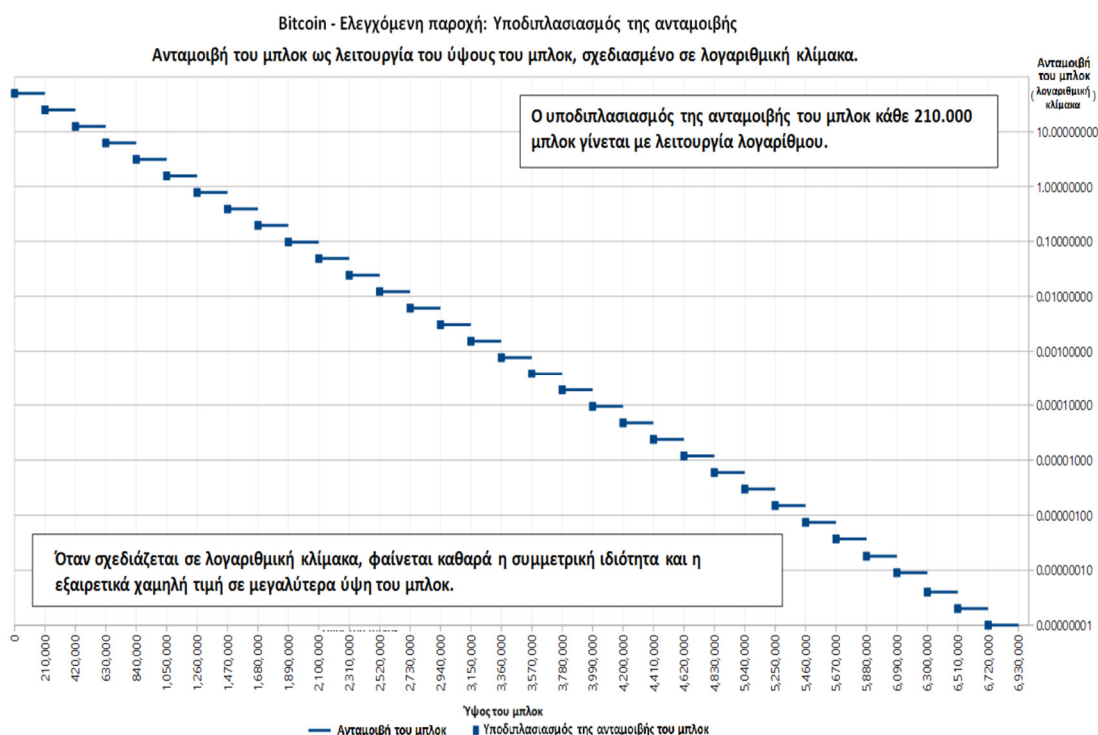
Εικόνα 13



Εικόνα 14



Εικόνα 15



Υπάρχουν διάφορες κατηγορίες hardware που χρησιμοποιούνται από τα λογισμικά εξόρυξης και είναι κατά ιστορική σειρά η CPU του υπολογιστή, η GPU της κάρτας γραφικών, τα ειδικά κατασκευασμένα κυκλώματα FPGA που μπορούν να ρυθμιστούν για εξόρυξη από τον miner και να εγκατασταθούν στον υπολογιστή, προσφέροντας καλύτερες αποδόσεις από τα προηγούμενα. Τέλος, χρησιμοποιούνται τα ολοκληρωμένα κυκλώματα ASICs που είναι σχεδιασμένα αποκλειστικά για mining, προσφέροντας χαμηλή ενεργειακή κατανάλωση και υψηλές ταχύτητες επεξεργασίας. Η χρήση των GPU αντί των CPU για mining επέφερε 50-100 περισσότερη ταχύτητα για το συγκεκριμένο σκοπό με μικρότερη κατανάλωση ρεύματος. Τα κυκλώματα FPGA μπορεί να μην αύξησαν την ταχύτητα όπως οι κάρτες γραφικών GPU, όμως μείωσαν αισθητά την κατανάλωση σε ρεύμα, όπου αν μία μέση κάρτα γραφικών κάνει 600 MegaHashes/sec με 400 watt, ένα μέτριο FPGA επιτυγχάνει 826 MegaHashes/sec με 80 watt. Αντιθέτως, ένα μέσο κυκλώματα ASIC αποδίδει 600 GigaHashes/sec με 350 watt¹⁷.

Ο μεγάλος ανταγωνισμός στο mining είχε ως αποτέλεσμα οι ιδιώτες miners να μην μπορούν να ανταγωνιστούν τις επιχειρήσεις με τα πολύ πιο γρήγορα και τεχνολογικά εξελιγμένα μηχανήματα τους, ώστε να μην μπορούν για μεγάλο χρονικό διάστημα (μήνες ή και έτη) να εξορύξουν BTC. Η ανάγκη αντιμετώπισης του ανταγωνισμού οδήγησε κυρίως τους ιδιώτες miners σε συνεργασία μεταξύ τους και δημιουργία ομάδων mining pools, ενώνοντας την υπολογιστική ισχύ τους και μοιράζοντας τα κέρδη. Υπάρχουν διάφοροι τρόποι συμφωνίας μοιράσματος των κερδών, όπως ανάλογα με το διαμοιρασμό ισχύς (Pay-per-Share), τον τρόπο πληρωμής των κερδών (Eligius, μόνο μετά τη συγκέντρωση ενός ποσού π.χ. 400 BTC, για αποφυγή συχνών εξόδων συναλλαγής), το διαμοιρασμό ισχύς σε συνάρτηση με το χρόνο (Score), τη πληρωμή ανά μικρότερων ομάδων που χωρίζονται στο mining pool (Pay Per Last N Groups) κ.α.

Οι miners μπορούν να χρησιμοποιήσουν το Cloud mining, όπου επιχειρήσεις παροχής υπηρεσιών mining πουλάνε ισχύ εξόρυξης των hardware (GH/s, gigahash per second), που καθορίζει πόσο γρήγορη και κερδοφόρα είναι η εξόρυξη και είναι τοποθετημένα σε απομακρυσμένα κέντρα δεδομένων. Με αυτόν το τρόπο η εξόρυξη γίνεται μέσω cloud, χωρίς προβλήματα εγκατάστασης μηχανημάτων, συντήρησής τους, ενόχλησης από

¹⁷ Mullan, P., (2014), *The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations*. U.S.A.: Palgrave Macmillan US

θορύβους λειτουργίας, διάθεσης χώρου, σύνδεσης ιντερνέτ και κατανάλωσης ρεύματος. Ακόμη, παρέχονται υπηρεσίες αυτόματης μετατροπής των mining altcoins σε BTC ή LTC και δυνατότητα μεταπώλησης της ισχύς mining.

Διάφορες ιστοσελίδες (tradeblock.com, bitcoinx.com, coinwarz.com) παρέχουν στους miners πληροφορίες και υπολογίζουν την κερδοφορία και τον χρόνο απόσβεσης των εξόδων τους, εισάγοντας τις παραμέτρους που ζητούνται, όπως τιμές του hardware (κόστος, χρήση ισχύς, GH/s), τον αλγόριθμο, στατιστικά δυσκολίας εξόρυξης και ρυθμού αύξησής της, καθώς και διάφορα κόστη (ηλεκτρισμού, τέλη).

Το mining δεν είναι σημαντικό μόνο για την επιβράβευση και κερδοφορία των miners, αλλά για την κυκλοφορία νέων BTC στην αγορά και τη διαδικασία POW που γίνεται, ώστε να επιτευχθούν οι συναλλαγές και να ενσωματωθούν στην blockchain. Η συνεχής μείωση του ποσού της επιβράβευσης, κάθε φορά που προστίθενται 21.000 μπλοκ στην blockchain, επιφέρει μείωση της προσφοράς BTC και ίσως για κάποιους τη δημιουργία χρηματοπιστωτικής αστάθειας, λόγω ραγδαίας αύξησης της τιμής του. Οι miners αποτελούν ένα πολύ μεγάλο μέρος της προσφοράς του BTC στην αγορά και εκτός από τους ερασιτέχνες ιδιώτες, υπάρχουν επαγγελματίες που έχουν επιχειρήσεις εξόρυξης και κάνουν αποκλειστικά αυτή τη δουλειά. Η μείωση της επιβράβευσης είναι γνωστή πότε θα γίνει και υπάρχουν κερδοσκόποι που αποθηκεύουν BTCs και περιμένουν, μετά την υποδιαίρεση, την αύξηση της τιμής και την πώληση τους για αποκομιδή κέρδους. Από την άλλη πλευρά υποστηρίζεται ότι ο κύριος λόγος ύπαρξης της υποδιαίρεσης της προσφοράς είναι ο έλεγχος του πληθωρισμού και η αποφυγή της υποτίμησης της αξίας του BTC. Εάν παραλληλίσουμε το χρυσό με το BTC θα δούμε ότι με την πάροδο του χρόνου περιορίζεται η εξόρυξη χρυσού και είναι πιο δύσκολη, αφού τα αποθέματα ανά τον κόσμο είναι συγκεκριμένα και μειώνονται συνεχώς. Εντούτοις, ο χρυσός έχει διατηρήσει την αξία του για χιλιάδες χρόνια. Τέλος, θα πρέπει να υπολογίζεται και η επιρροή της τεχνολογικής εξέλιξης όπου ένας miner, ο οποίος έχει συγκεκριμένα έξοδα (ρεύμα, αβαρίες) και έσοδα, με τον πεπαλαιωμένο εξοπλισμό του θα δει να μειώνονται συνεχώς τα έσοδά του, έχοντας να αντιμετωπίσει την υποδιαίρεση της επιβράβευσης, αλλά και την είσοδο νέων miners με ποιο εξελιγμένο εξοπλισμό και καλύτερα

αποτελέσματα στο mining. Επομένως, ο εν λόγω miner ή θα πρέπει να αναβαθμίσει τα μηχανήματά του ή να αποχωρήσει εξαιτίας της ασύμφορης προσπάθειας του¹⁸.

2.4 Το κόστος της παραγωγής του κρυπτονομίσματος

Η παραγωγή (εξόρυξη) του κρυπτονομίσματος είναι μια δαπανηρή και σχετικά περίπλοκη διαδικασία η οποία συνίσταται να γίνεται από όσους έχουν την οικονομική δυνατότητα να την κάνουν. Το πιο σημαντικό στη διαδικασία αυτή είναι να υπάρχει ένας φθηνός πάροχος ηλεκτρικού ρεύματος καθώς είναι αρκετά δύσκολο κάποιος να βγάλει κέρδος από το κρυπτονόμισμα εάν πληρώνει ακριβά την ηλεκτρική ενέργεια. Αν μην ξεχνάμε άλλωστε ότι η εξόρυξη είναι μια ανταγωνιστική διαδικασία στην οποία οι χρήστες ανταγωνίζονται μεταξύ τους και μια από τις παραμέτρους έχει να κάνει και με τα χαμηλότερα έξοδα.

Οι δρόμοι που ανοίγονται στους εξορυκτές περιορίζονται καθημερινά. Τεχνικά, υπάρχουν 3 επιλογές: η αυτοτελής εξόρυξη, η συνεργατική εξόρυξη και η εξόρυξη νέφους. Η εξόρυξη νέφους είναι ένας εντυπωσιακός τρόπος για να λες ότι πληρώνεις κάποιον για να κάνει την εξόρυξη για λογαριασμό σου. Η αυτοτελής εξόρυξη απευθύνεται σε χρήστες που προτιμούν να κάνουν εικονικά αδύνατη υπερπροσπάθεια να λύσουν ένα μπλοκ χωρίς το πλεονέκτημα της τεράστιας δύναμης κατακερματισμού που αποκτά κάποιος όταν συμμετέχει σε μια ομάδα συνεργασίας.

Το επόμενο βήμα για την εξόρυξη έχει να κάνει με το κατέβασμα ενός λογισμικού εξόρυξης στον υπολογιστή. Ενδεικτικά προγράμματα είναι το CGminer και το BFGminer. Μετά τη λήψη του λογισμικού μπαίνουμε σε μια ομάδα δημιουργούμε έναν «εργάτη» δηλαδή έναν χρήστη ο οποίος θα μας βοηθήσει στην εξόρυξη και του δίνουμε ένα όνομα. Ύστερα αναζητούμε την IP της εξόρυξης του ιστότοπου η οποία και υπάρχει στη σελίδα της ομάδας. Στη συνέχεια ανοίγουμε ένα έγγραφο σε μορφή text στο σημειωματάριο και πληκτρολογούμε το παρακάτω κείμενο «cgminer – o stratum + tcp://

¹⁸ Mullan, P., (2014), The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations. U.S.A.: Palgrave Macmillan US

[το όνομα της ομάδας]:[τον αριθμό της θύρας IP] – u[το όνομα χρήστη].[όνομα «εργάτη»] –p [κωδικός χρήστη].

Στη συνέχεια αποθηκεύουμε το αρχείο αλλάζοντας όμως την επέκταση του και ονομαζόντας το StartMining.bat και το αποθηκεύουμε στον ίδιο φάκελο όπου έχει γίνει αποθήκευση και του CGMiner. Έτσι με την ολοκλήρωση της διαδικασίας επιλέγουμε το αρχείο και ο εξορυκτής θα αρχίσει να εξορρύσει αυτόματα κρυπτονομίσματα¹⁹.

¹⁹ Mullan, P., (2014), The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations. U.S.A.: Palgrave Macmillan US

ΚΕΦΑΛΑΙΟ 3^ο: ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

3.1 Η τεχνολογία blockchain

Το λογισμικό blockchain χρησιμοποιείται για συγχρονισμό των δεδομένων που αποθηκεύονται με κατακευματισμένο τρόπο μεταξύ των υπολογιστών που συμμετέχουν σε ένα συγκεκριμένο δίκτυο. Αυτό επιτρέπει πολλαπλές εγγραφές πανομοιότυπων δεδομένων. Η εμπιστοσύνη δημιουργείται επειδή όλοι οι κόμβοι στο δίκτυο ελέγχου, δίνουν τη συγκατάθεση τους για οποιεσδήποτε προσθήκες ή αλλαγές σε αυτό που έχει καταγραφεί. Το Blockchain μπορεί να χρησιμοποιηθεί για εγγραφή, διατήρηση, μεταφορά αξίας (μέσω κρυπτονομισμάτων) και έξυπνες συμβάσεις για αυτόματη εκτέλεση μιας συναλλαγής όταν πληρούνται οι προϋποθέσεις.

Μόλις αποθηκευτούν στο blockchain, τα δεδομένα δεν μπορούν να χειραγωγηθούν και είναι αμετάβλητα. Κάθε μπλοκ περιέχει μια μοναδική περίληψη του προηγούμενου μπλοκ με τη μορφή ασφαλούς τιμής κατακευματισμού. Επειδή κάθε μπλοκ είναι συνδεδεμένο, το χρονοδιάγραμμα, η σειρά και το περιεχόμενο των συναλλαγών δεν μπορεί να τροποποιηθεί και τα μπλοκ δεν μπορούν να αντικατασταθούν εκτός εάν όλοι οι κόμβοι συμφωνούν με την προτεινόμενη αλλαγή.

Ένα blockchain καταγράφει υλικά και άυλα περιουσιακά στοιχεία και υποχρεώσεις μεταξύ ενός δικτύου υπολογιστών που χρησιμοποιούν το ίδιο λογισμικό, αλγόριθμους και κρυπτογραφία διατηρεί τα αρχεία. Αυτά τα περιουσιακά στοιχεία και υποχρεώσεις μπορεί στη συνέχεια να μεταφερθούν μεταξύ των συμμετεχόντων με τη συγκατάθεση όλων των άλλων κόμβων²⁰.

²⁰ Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber

Ένα blockchain επιτρέπει στους συμμετέχοντες να μοιράζονται δεδομένα και κωδικούς χωρίς να χρειάζεται να λειτουργούν οι μεσάζοντες. Όλα τα μέρη μοιράζονται τα ίδια δεδομένα, τα οποία αναπαράγονται σε όλους τους κόμβους στο δίκτυο. Οι εγγραφές που περιλαμβάνονται στο blockchain είναι αμετάβλητες (ακόμη και αν είναι λάθος) και παρέχει μια αμετάβλητη, χρονική σήμανση ελέγχου.

Υπάρχουν δύο τύποι blockchain: χωρίς άδεια (στην οποία ο καθένας μπορεί να συμμετάσχει) και με άδεια (κατά την οποία ένας συμμετέχων πρέπει να εγκριθεί ώστε να συμμετάσχει). Αυτό μπορεί να είναι για την προστασία του απορρήτου ή των εμπορικών μυστικών των εμπλεκόμενων ή για να διασφαλιστεί η συμμόρφωση με τους κανονισμούς, όπως αυτοί που έχουν σχεδιαστεί για την πρόληψη της νομιμοποίησης των εσόδων από παράνομες δραστηριότητες.

Τα blockchain χωρίς άδεια είναι δημόσια. Οι συμμετέχοντες χρησιμοποιούν ψευδώνυμα για προστασία της ταυτότητά τους και δεν υπάρχει ταυτότητα ή πιστοποίηση των συμμετεχόντων. Επιτρέπεται τα blockchain να είναι ιδιωτικά και να προστατεύονται από έλεγχο πρόσβασης και (δυναμικά) διαφορετικά προνόμια ανάγνωσης και γραφής. Οι συμμετέχοντες είναι γνωστά, αναγνωρισμένα και επικυρωμένα άτομα και το δίκτυο μπορεί να ελέγχεται από έναν υπερ-χρήστη.

Ο έλεγχος ταυτότητας και η ταυτοποίηση χρησιμοποιούν πολύ ασφαλή κρυπτογραφία. Οι επιτρεπόμενες blockchains γενικά θεωρούνται πιο αξιόπιστες επειδή η αρχή της συναίνεσης λειτουργεί καλύτερα όσο υπάρχουν στο δίκτυο περισσότεροι συμμετέχοντες²¹.

Υπάρχουν διάφορες χρήσεις που ενεργοποιούνται από το λογισμικό blockchain. Σε αυτά περιλαμβάνονται: η κωδικοποίηση για την προστασία ευαίσθητων δεδομένων και η χρονική σήμανση λόγω του αμετάβλητου του blockchain. Έτσι λοιπόν αυτό χρησιμεύει ως κανάλι πληρωμών που επιτρέπει τη μεταφορά περιουσιακών στοιχείων και υποχρεώσεων και τη διευκόλυνση των έξυπνων συμβάσεων, το οποίο παρουσιάζει μεγάλο ενδιαφέρον για τους δικηγόρους.

²¹ Nofer M., (2017), Blockchain, Springer

Η τεχνολογία Blockchain έχει χρησιμοποιηθεί είτε για να καταστήσει τις διαδικασίες πιο αποτελεσματικές αντικαθιστώντας υπάρχοντα στοιχεία είτε για να παρέχει μια νέα υπηρεσία χρησιμοποιώντας το blockchain ως ραχοκοκαλιά. Το πιο προφανές παράδειγμα είναι τα κρυπτονομίσματα που συζητούνται πολύ. Ωστόσο, η χρήση του διερευνάται σε μια σειρά βιομηχανιών, όπως:

- Αεροπορικές εταιρείες (όπου οι έξυπνες συμβάσεις διευκολύνουν την εκκαθάριση μεταξύ αεροπορικών εταιρειών), πράκτορες εισιτηρίων και τράπεζες, εξόρυξη (για τη δημιουργία εικονικής αγοράς που βασίζεται σε blockchain),
- Μεταφορές
- Αγορά πετρελαίου και φυσικού αερίου (για την παρακολούθηση της χρηστής εταιρικής διακυβέρνησης θυγατρικών και χρηματοοικονομικών υπηρεσιών με διάφορους τρόπους, από την εκκαθάριση έως τα προγράμματα πιστότητας). Για παράδειγμα η ρωσική κεντρική τράπεζα ανέθεσε τη δημιουργία ενός εγκεκριμένου blockchain για τον τραπεζικό κλάδο για τη διευκόλυνση των συναλλαγών σε ένα αξιόπιστο περιβάλλον²².

3.2 Νομικοί περιορισμοί

Μεταξύ πολλών πιθανών εφαρμογών, θα μπορούσε κανείς να χρησιμοποιήσει μια λύση blockchain για την καταγραφή συμφωνιών μεταξύ δύο ή περισσότερων μερών ή για την καταγραφή μιας μονομερούς πράξης βάσει του ιδιωτικού δικαίου, για την εκτέλεση και δημοσίευση μιας απόφασης που υπόκειται στο δημόσιο δίκαιο, ως μια μοναδική πηγή αλήθειας (στο με άλλα λόγια, ως απόδειξη), για την εκτέλεση νομικής διαδικασίας ή απόφασης που υπόκειται σε διαφορετικούς τομείς δικαίου, για συμμόρφωση με φορολογικές υποχρεώσεις ή για χρήση ανασταλτικών ή / και λύσεων σε νομικές πράξεις²³.

²² Nofer M., (2017), Blockchain, Springer

²³ Werbach K., (2018), Trust, but verify: Why the blockchain needs the law, Hein online

Ανάλογα με την πρόθεση των μερών, περισσότερες από μία από αυτές τις νομικές εκδηλώσεις θα μπορούσαν να συνδυαστούν σε μια συγκεκριμένη λύση blockchain.

Οι συμμετέχοντες στο Blockchain πρέπει να γνωρίζουν τις νομικές συνέπειες της λύσης που χρησιμοποιούν, συμπεριλαμβανομένου του δημοσίου δικαίου, του ιδιωτικού δικαίου, του ποινικού δικαίου και του χρηματοοικονομικού και κανονιστικού δικαίου.

Στον τομέα ιδιωτικού δικαίου, υπάρχουν πολλά νομικά ζητήματα που πρέπει να ληφθούν υπόψη κατά τη χρήση έξυπνων συμβάσεων σε ένα blockchain. Στο προηγούμενο παράδειγμα, το ζήτημα της ευθύνης πρέπει να αντιμετωπιστεί εάν το συμβόλαιο έχει εσφαλμένα κωδικοποιηθεί έτσι ώστε να μην επιτυγχάνει την πρόθεση των μερών ή να γίνει λάθος ή σκόπιμο σφάλμα. Επιπλέον, τα μέρη θα πρέπει να συμφωνήσουν σχετικά με το εφαρμοστέο δίκαιο, τη δικαιοδοσία, τις γενικές αρχές ορθής διακυβέρνησης, την επίλυση διαφορών, το απόρρητο και τα μέσα ψηφιακής ταυτότητας. Είναι το συμβόλαιο διαθέσιμο γραπτώς, καθώς και ο κώδικας, ώστε τα μέρη να γνωρίζουν σε τι συμφωνούν; Μπορεί να προσδιοριστεί η ταυτότητα των μερών με επαρκή βεβαιότητα για να καταστεί έγκυρη η σύμβαση; Εάν αυτές οι προκλήσεις δεν αντιμετωπιστούν εκ των προτέρων, παρά τα μέρη που ενεργούν με καλή πίστη, μπορεί να διαπιστώσουν ότι δεν έχουν πραγματικά συμβόλαιο, και εάν προκύψουν προβλήματα, δεν έχουν συμφωνημένα μέσα για την επίλυσή τους²⁴.

Από τη σκοπιά του δημοσίου δικαίου, υπάρχουν προφανώς κίνδυνοι ότι οι άδειες blockchain ίσως χρησιμοποιούνται για παράνομους σκοπούς όπως η νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για να επωφεληθούν από την ψευδώνυμη εμπλοκή για την αντιμετώπιση ζητημάτων δικαίου ανταγωνισμού. Οι συμμετέχοντες ενδέχεται να εκτίθενται στους minors που δημιουργούν νέα μπλοκ που ενεργούν ανεύθυνα ή δεν ενεργούν με καλή πίστη. Προς το παρόν δεν υπάρχουν συγκεκριμένα ένδικα μέσα κατά των διεφθαρμένων minors.

Δεδομένου ότι τα έξυπνα συμβόλαια εκτελούνται σε ένα blockchain, δεν μπορούν να χειραγωγηθούν μετά το συμβάν και, καθώς αυτο-εκτελούνται, η εκτέλεση δεν μπορεί να

²⁴ Rodrigues U., (2018), Law and the Blockchain, Hein online

αποφευχθεί. Εάν πληρείται η προϋπόθεση αυτή, τότε η συναλλαγή εκτελείται αυτόματα, ακόμη και αν τα μέρη έχουν βάσιμους λόγους να μην επιθυμούν πλέον να συμβαίνει.

3.3 Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων (GDPR) και πως συνδέεται με το blockchain

3.3.1 Τι ορίζονται ως προσωπικά δεδομένα

Σύμφωνα με τον κανονισμό 679 / 2016 του Ευρωπαϊκού Κοινοβουλίου οποιαδήποτε δεδομένα σχετίζονται άμεσα ή έμμεσα με ένα φυσικό πρόσωπο θεωρούνται ως προσωπικά δεδομένα. Παραδείγματα προσωπικών δεδομένων είναι το όνομα, η διεύθυνση, το κινητό και το σταθερό τηλέφωνο, η διεύθυνση ηλεκτρονικού ταχυδρομείου ή διεύθυνση IP, τα φυσικά, γενετικά ή βιομετρικά δεδομένα, ψυχικά, οικονομικά, πολιτιστικά ή κοινωνικά δεδομένα ενός φυσικού προσώπου. Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων απαγορεύεται σύμφωνα με το άρθρο 9 του κανονισμού. Επίσης η φυλετική καταγωγή, οι πολιτικές απόψεις, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα υγείας, σεξουαλική ζωή του ατόμου ή ο γενετήσιος προσανατολισμός μπορεί να θεωρηθούν ως ευαίσθητα δεδομένα²⁵.

Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή θεωρείται επεξεργασία προσωπικών δεδομένων.

²⁵ Πλατής Ε., (2018), Προσωπικά δεδομένα, εκδόσεις Παπαδόπουλος

3.3.2 Οι αρχές του GDPR

Στο άρθρο 5 του κανονισμού 679 / 2016 περιγράφονται οι βασικές αρχές στις οποίες οφείλουν να σέβονται οι επιχειρήσεις κατά την επεξεργασία των προσωπικών δεδομένων.

Οι πιο σημαντικές από αυτές τις αρχές του GDPR είναι οι εξής²⁶:

- Η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με νόμιμη, δίκαιη και διαφανή μέθοδο.
- Τα προσωπικά δεδομένα πρέπει να συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να μην γίνεται επεξεργασία που δεν είναι συμβατή με αυτούς τους σκοπούς.
- Η επεξεργασία των προσωπικών δεδομένων πρέπει να είναι επαρκής, σχετική και περιορισμένη για τους σκοπούς για τους οποίους συμβαίνει
- Τα προσωπικά δεδομένα πρέπει να διατηρούνται σε μορφή που επιτρέπει την αναγνώριση των υποκειμένων των δεδομένων μόνο για όσο χρόνο χρειάζεται
- Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που να εξασφαλίζεται και να προστατεύεται η μη εξουσιοδοτημένη ή παράνομη μεταποίηση αυτών
- Ο ελεγκτής είναι υπεύθυνος για την απόδειξη της συμμόρφωσης των δεδομένων με τον κανονισμό.
- Η νομιμότητα, η δικαιοσύνη και η διαφάνεια πρέπει να ισχύουν στο έπακρο και η επιχείρηση πρέπει να ορίσει ένα άτομο ως υπεύθυνο για τις μεθόδους επεξεργασίας δεδομένων. Επιπλέον, οι επιχειρήσεις οφείλουν να ενημερώσουν για το είδος των δεδομένων που υποβάλλονται σε επεξεργασία²⁷.

²⁶ Κυριαζόγλου I., (2019), Προστασία προσωπικών δεδομένων (GDPR Protection), εκδόσεις Φυλάτος

²⁷ Κυριαζόγλου I., (2019), Προστασία προσωπικών δεδομένων (GDPR Protection), εκδόσεις Φυλάτος

3.3.3 Τα δικαιώματα των χρηστών του διαδικτύου με το GDPR

Παρακάτω παρουσιάζονται τα σημαντικότερα δικαιώματα που αποκτούν οι πολίτες της ΕΕ με την εφαρμογή του κανονισμού για το GDPR.

1. Το δικαίωμα ενημέρωσης

Η επιχείρηση που διατηρεί προσωπικά στοιχεία πρέπει να δώσει πληροφορίες σε κάθε άτομο σχετικά με²⁸:

- Τα στοιχεία επικοινωνίας της εταιρείας
- Το σκοπό που η εταιρεία διατηρεί προσωπικά στοιχεία
- Εάν τα προσωπικά δεδομένα παραχωρούνται σε τρίτους και ποιοι είναι αυτοί
- Εάν διαβιβάζονται ή πρόκειται να διαβιβαστούν προσωπικά δεδομένα σε τρίτες χώρες και άλλα παρόμοια ζητήματα

2. Το δικαίωμα πρόσβασης

Ένα άτομο έχει το δικαίωμα πρόσβασης στις προσωπικές του πληροφορίες γεγονός που σημαίνει ότι ο ελεγκτής μητρώου οφείλει να ειδοποιήσει το φυσικό πρόσωπο εάν κάποιος άλλο άτομο ζητήσει να έχει πρόσβαση σε αυτά τα προσωπικά δεδομένα.

3. Το δικαίωμα διόρθωσης των σφαλμάτων

Ο κανονισμός GDPR παρέχει στα φυσικά πρόσωπα το δικαίωμα να απαιτούν διόρθωση για λανθασμένες πληροφορίες που περιέχονται στη βάση δεδομένων κάποιας επιχείρησης.

4. Το δικαίωμα της διαγραφής των δεδομένων

Ένα άτομο έχει το δικαίωμα να ζητήσει διαγραφή των προσωπικών πληροφοριών που αυτό είχε δώσει. Επιπλέον, ένα άτομο έχει επίσης το δικαίωμα να ακυρώσει τη συγκατάθεση που είχε δώσει για την επεξεργασία των δεδομένων.

²⁸ Κοτσαλής Λ., Μενουδάκος Κ., (2018), Γενικός κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR), εκδόσεις Νομική βιβλιοθήκη

5. Το δικαίωμα μεταφοράς των δεδομένων

Το δικαίωμα στη φορητότητα δεδομένων είναι επίσης μια νέα απαίτηση του GDPR. Ένα άτομο έχει επομένως δικαίωμα να πάρει όλες τις προσωπικές του πληροφορίες και στη συνέχεια να μεταφέρει αυτά τα δεδομένα σε άλλη επιχείρηση²⁹.

6. Το δικαίωμα ενημέρωσης για παραβιάσεις των δεδομένων

Μία ευθύνη για τις επιχειρήσεις είναι η ενημέρωση των εγγεγραμμένων προσώπων για παραβιάσεις στα δεδομένα και για τα δεδομένα τα οποία έχουν διαρρεύσει. Το δικαίωμα είναι σε ισχύ αν η παραβίαση προκαλεί μεγάλους κινδύνους για τα δικαιώματα και την ελευθερία του ατόμου. Οι προαναφερθέντες κίνδυνοι είναι για παράδειγμα: κλοπές ταυτότητας, απάτες πιστωτικών καρτών ή άλλες εγκληματικές δραστηριότητες. Η κοινοποίηση δεν είναι υποχρεωτική εάν οι πληροφορίες που διαχέονται με προσωπική ταυτότητα έχουν διαρρεύσει όμως τα κρυπτογραφημένα κλειδιά δεν διαρρεύσαν. Μια επιχείρηση μπορεί να χρησιμοποιήσει τα μέσα κοινωνικής δικτύωσης για την ενημέρωση σχετικά με την παραβίαση δεδομένων για την πληρέστερη ενημέρωση των πολιτών.

3.3.4 Οι προκλήσεις σχετικά με το GDPR και οι καινοτομίες του κανονισμού

3.3.4.1 Η ασφάλεια των προσωπικών δεδομένων

Το άρθρο 33 του κανονισμού σχετικά με το GDPR ορίζει ότι «Σε περίπτωση παραβίασης των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι εφικτό, το αργότερο εντός 72 ωρών από την ημερομηνία αυτή υποχρεούται να γνωστοποιήσει το γεγονός, να κοινοποιήσει την παραβίαση των προσωπικών δεδομένων στην εποπτική αρχή σύμφωνα με το άρθρο 55, εκτός εάν είναι πιθανό η παραβίαση προσωπικών δεδομένων να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στη περίπτωση αυτή η κοινοποίηση προς την

²⁹ Νόμος 4624 / 2019

εποπτική αρχή δεν γίνεται εντός 72 ωρών και θα πρέπει να συνοδεύεται από τους λόγους της καθυστέρησης³⁰».

3.3.4.2 Το δικαίωμα της διαγραφής δεδομένων

Επίσης σύμφωνα με το άρθρο 17 του GDPR « το άτομο που έχει συναινέσει στη παραχώρηση προσωπικών δεδομένων έχει το δικαίωμα να ζητήσει από την επιχείρηση τη διαγραφή των προσωπικών δεδομένων που τον αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο ελεγκτής έχει την υποχρέωση να διαγράψει τα προσωπικά δεδομένα. Το άρθρο 17 περιγράφει τα δικαιώματα του ατόμου να ζητήσει τη διαγραφή δεδομένων και οι εταιρείες πρέπει να τηρούν αυτό το αίτημα. Οι εταιρείες πρέπει να έχουν ένα μηχανισμό και διαδικασίες και να βεβαιώνουν το άτομο ότι τα αφαιρεθέντα δεδομένα δεν θα επανέλθουν στο μέλλον.

3.3.4.3 Οι βασικές καινοτομίες του Κανονισμού

Ι) Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την εποπτική αρχή (δηλ. την εκάστοτε αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) της επεξεργασίας, η οποία βάρυνε τους υπευθύνους επεξεργασίας και μόνο.

Την καταργούμενη αυτή υποχρέωση ο νέος ΓΚΠΔ αντικαθιστά με την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας όλων των δεδομένων προσωπικού χαρακτήρα, για τις οποίες είναι υπεύθυνοι, καθώς και με την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας (Βλ. άρθρο 30 του ΓΚΠΔ).

Ένας ικανοποιητικός τρόπος προετοιμασίας ήδη από σήμερα, τόσο για τους υπευθύνους, όσο και για τους εκτελούντες επεξεργασία, είναι α) η κατανόηση των ζητημάτων που ανακύπτουν από τον ΓΚΠΔ (awareness), β) η καταγραφή των δεδομένων (data

³⁰ Νόμος 4624 / 2019

inventory) και των διαδικασιών, συστημάτων και αρχείων (φυσικών και ψηφιακών) που τα περιέχουν (data mapping), γ) η ανάλυση της απόκλισης από την συμμόρφωση με τον ΓΚΠΔ (Gap Analysis), δ) ο σχεδιασμός (ή ανασχεδιασμός) των κατάλληλων πολιτικών ροών δεδομένων και των επεξεργασιών που διενεργούνται, ώστε ο φορέας να είναι σε θέση να παρακολουθεί και να δημιουργήσει σύστημα τήρησης αρχείων.

II) Εισάγεται η υποχρέωση του υπεύθυνου επεξεργασίας προς διενέργεια εκτίμησης αντικτύπου (Data protection impact assessment – DPIA) σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών. Ειδικότερα, ο υπεύθυνος επεξεργασίας υποχρεούται ρητά σε διενέργεια DPIA πριν από την κρίσιμη επεξεργασία κάθε φορά που ένα είδος επεξεργασίας, ιδίως με τη χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας αυτής, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. (Βλ. άρθρο 35 παρ. 1 ΓΚΠΔ).

III) Εισάγεται η υποχρέωση για κατηγορίες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία, να ορίσουν Υπεύθυνο Προστασίας Δεδομένων (Data Protection Officer-DPO) στη βάση συγκεκριμένων ποιοτικών κριτηρίων, που περιλαμβάνουν τη διενέργεια συγκεκριμένων τύπων επεξεργασιών. Επίσης ορίζονται οι περιπτώσεις υποχρεωτικού ορισμού DPO και παρέχεται η ευχέρεια όπως ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων ή εκτελούντων επεξεργασία, ορίσουν DPO και πέραν των περιπτώσεων του υποχρεωτικού ορισμού τούτου.

Η ύπαρξη και λειτουργία του DPO είναι εξαιρετικά σημαντική για τις εταιρείες διότι ουσιαστικά αυτός θα είναι το πρόσωπο που θα κατευθύνει τον οργανισμό προς την ολοκλήρωση και τήρηση ενός ικανού προγράμματος συμμόρφωσης με τον ΓΚΠΔ, θα διαχειριστεί τυχόν καταγγελίες και παραβάσεις και θα εκπροσωπήσει την εταιρεία στην εποπτική αρχή για κάθε σχετικό ζήτημα. Για το λόγο αυτό ακόμα και όταν δεν είναι υποχρεωτικός ο διορισμός DPO, θα ήταν ιδιαίτερα συμφέρον για κάθε εταιρεία να έχει εθελοντικά ορίσει έναν DPO. Ο ΓΚΠΔ δεν προβλέπει ειδικά κριτήρια ή πιστοποιήσεις για την επιλογή του DPO, θεωρεί όμως ότι θα πρέπει να είναι πρόσωπο με μεγάλη εμπειρία στη νομοθεσία των προσωπικών δεδομένων και τη διαχείριση τυχόν σχετικών παραβάσεων.

IV) Ενθαρρύνεται ιδιαίτερος η σύνταξη κωδίκων δεοντολογίας από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία προκειμένου να προσδιορίσουν την εφαρμογή του ΓΚΠΔ (αρθ. 40 ΓΚΠΔ), καθώς και η θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων, με σκοπό την απόδειξη συμμόρφωσης προς το ΓΚΠΔ (αρθ. 42). Σημειώνεται βέβαια, ότι αμφότερες οι περιπτώσεις αυτές δεν λειτουργούν ως απαλλακτικοί λόγοι ευθύνης.

3.4 Η νομοθεσία σχετικά με το GDPR (Νόμος 4624 / 2019)

Ο νόμος αυτός είναι ουσιαστικά η ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης - πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.

Βασικοί ορισμοί του νόμου αυτού είναι οι εξής³¹:

1. Δεδομένα προσωπικού χαρακτήρα: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.
2. Επεξεργασία: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση

³¹ Νόμος 4624 / 2019

πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

3. Υπεύθυνος επεξεργασίας : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

4. Εκτελών την επεξεργασία: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

5. Παραβίαση δεδομένων προσωπικού χαρακτήρα: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία³²

6. Εποπτική αρχή: ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος επιφορτισμένη με την παρακολούθηση της εφαρμογής του παρόντος κανονισμού, με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα στην Ένωση

7. Υπεύθυνος Προστασίας δεδομένων: Πρόκειται για τον άνθρωπο εκείνον ο οποίος θα ενημερώνει τους χρήστες των οποίων τα δεδομένα επεξεργάζεται η εταιρεία αλλά και θα είναι εκείνος ο οποίος έρχεται σε επικοινωνία με την Εποπτική Αρχή.

8. Φορέας Παρακολούθησης: Με την επιφύλαξη των καθηκόντων και των αρμοδιοτήτων της αρμόδιας εποπτικής αρχής σύμφωνα με τα άρθρα 57 και 58, η παρακολούθηση της συμμόρφωσης με κώδικα δεοντολογίας δυνάμει του άρθρου 40 μπορεί να διεξάγεται από φορέα που διαθέτει το ενδεδειγμένο επίπεδο εμπειρογνωμοσύνης σε σχέση με το

³² Νόμος 4624 / 2019

αντικείμενο του κώδικα και είναι διαπιστευμένος για τον σκοπό αυτόν από την αρμόδια εποπτική αρχή.

Τέλος, σε περίπτωση που η εποπτική αρχή αντιληφθεί μετά από καταγγελία την μη συμμόρφωση κάποια επιχείρησης σε σχέση με την κείμενη νομοθεσία επιβάλλει ποινές οι οποίες ανάλογα με τη σοβαρότητα της παράβασης.

ΚΕΦΑΛΑΙΟ 4: ΨΗΦΙΑΚΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗ , ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΕΝΤΑΞΗ ΚΑΙ ΕΞΥΠΝΕΣ ΣΥΜΒΑΣΕΙΣ

4.1 Ψηφιακή χρηματοδότηση και ψηφιακά νομίσματα

Το ψηφιακό νόμισμα είναι μια μορφή νομίσματος που διατίθεται μόνο σε ψηφιακή ή ηλεκτρονική μορφή και όχι σε φυσική μορφή. Ονομάζεται επίσης ψηφιακό χρήμα, ηλεκτρονικό χρήμα, ηλεκτρονικό νόμισμα ή μετρητά στον κυβερνοχώρο.

Τα ψηφιακά νομίσματα είναι άυλα και μπορούν να ανήκουν και να πραγματοποιούνται συναλλαγές μόνο με τη χρήση υπολογιστών ή ηλεκτρονικών πορτοφολιών συνδεδεμένων στο Διαδίκτυο ή τα καθορισμένα δίκτυα. Αντιθέτως, τα φυσικά νομίσματα, όπως τα τραπεζογραμμάτια και τα νομισματοκοπεία, είναι απτά και οι συναλλαγές είναι δυνατές μόνο από τους κατόχους τους που έχουν τη φυσική τους ιδιοκτησία³³.

Όπως κάθε τυπικό νόμισμα τα ψηφιακά νομίσματα μπορούν να χρησιμοποιηθούν για την αγορά αγαθών καθώς και για την πληρωμή υπηρεσιών, αν και μπορούν επίσης να βρουν περιορισμένη χρήση σε ορισμένες διαδικτυακές κοινότητες, όπως ιστότοπους τυχερών παιχνιδιών, πύλες τυχερών παιχνιδιών ή κοινωνικά δίκτυα.

Τα ψηφιακά νομίσματα έχουν όλες τις εγγενείς ιδιότητες όπως το φυσικό νόμισμα και επιτρέπουν στιγμιαίες συναλλαγές που μπορούν να εκτελούνται απρόσκοπτα για την πραγματοποίηση πληρωμών διασυνοριακά όταν συνδέονται με υποστηριζόμενες συσκευές και δίκτυα.

Τα ψηφιακά νομίσματα προσφέρουν πολλά πλεονεκτήματα. Καθώς οι πληρωμές σε ψηφιακά νομίσματα γίνονται απευθείας μεταξύ των συναλλασσόμενων μερών χωρίς την

³³ Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber

ανάγκη διαμεσολαβητών, οι συναλλαγές είναι συνήθως στιγμιαίες και χαμηλού κόστους. Αυτό είναι καλύτερο σε σύγκριση με τους παραδοσιακούς τρόπους πληρωμής που περιλαμβάνουν τράπεζες ή εκκαθαριστικά γραφεία. Οι ηλεκτρονικές συναλλαγές με ψηφιακό νόμισμα φέρνουν επίσης την απαραίτητη τήρηση αρχείων και διαφάνεια στις συναλλαγές.

4.2 Η έννοια της χρηματοοικονομικής ένταξης

Η χρηματοοικονομική ένταξη είναι ένα φαινόμενο όπου οι χρηματοπιστωτικές αγορές σε γειτονικές, περιφερειακές ή παγκόσμιες οικονομίες συνδέονται στενά μεταξύ τους για παράδειγμα, μέσω διασυνοριακών ροών κεφαλαίων, ξένης συμμετοχής στις εγχώριες χρηματοπιστωτικές αγορές και ανταλλαγής πληροφοριών μεταξύ χρηματοπιστωτικών ιδρυμάτων. Οι νομικοί περιορισμοί μπορεί μερικές φορές να εμποδίσουν την οικονομική ολοκλήρωση.

Η χρηματοοικονομική ολοκλήρωση γειτονικών, περιφερειακών ή παγκόσμιων οικονομιών μπορεί να πραγματοποιηθεί μέσω μιας επίσημης συνθήκης στην οποία τα διοικητικά όργανα αυτών των οικονομιών συμφωνούν να συνεργαστούν για την αντιμετώπιση χρηματοοικονομικών διαταραχών. Αλλά λόγω των πρόσφατων οικονομικών κρίσεων, υπήρξε μια ζωντανή συζήτηση μεταξύ των ακαδημαϊκών σχετικά με το κόστος και τα οφέλη της χρηματοοικονομικής ολοκλήρωσης.

Τα πλεονεκτήματα της χρηματοοικονομικής ολοκλήρωσης περιλαμβάνουν καλύτερη διακυβέρνηση, αποτελεσματική κατανομή κεφαλαίου και υψηλότερη ανάπτυξη και επενδύσεις. Ωστόσο, ένας υψηλότερος βαθμός χρηματοοικονομικής ολοκλήρωσης έχει επίσης τη δυνατότητα να προκαλέσει σοβαρή χρηματοοικονομική μετάδοση σε συνδεδεμένες οικονομίες κατά τη διάρκεια κρίσεων³⁴.

³⁴ Grinberg R., (2012), Bitcoin: An innovative alternative digital currency, Hein Online

4.3 Οι έξυπνες συμβάσεις (smart contracts)

Ένα έξυπνο συμβόλαιο (smart contract) είναι ένα αυτο-εκτελούμενο συμβόλαιο με τους όρους της συμφωνίας μεταξύ αγοραστή και πωλητή να γράφονται απευθείας σε γραμμές κώδικα. Ο κώδικας και οι συμφωνίες που περιέχονται σε αυτό υπάρχουν σε ένα κατακεντρωμένο, αποκεντρωμένο δίκτυο blockchain. Ο κώδικας ελέγχει την εκτέλεση και οι συναλλαγές είναι ανιχνεύσιμες και μη αναστρέψιμες.

Οι έξυπνες συμβάσεις επιτρέπουν την πραγματοποίηση αξιόπιστων συναλλαγών και συμφωνιών μεταξύ διαφορετικών, ανώνυμων μερών χωρίς την ανάγκη κεντρικής αρχής, νομικού συστήματος ή εξωτερικού μηχανισμού επιβολής. Ενώ η τεχνολογία blockchain έχει θεωρηθεί κυρίως ως το θεμέλιο για το bitcoin, έχει εξελιχθεί πολύ πέρα από την υποστήριξη του εικονικού νομίσματος.

Κάθε μέρα προσφέρει μια νέα ευκαιρία για να ανακαλύψουμε μια νέα εφαρμογή για τεχνολογία blockchain. Αφού σχηματίσει με επιτυχία τη ραχοκοκαλιά για μια επαναστατική κρυπτογράφηση, το blockchain παρουσιάζει στρατηγικές εξελίξεις σε διάφορους κλάδους, συμπεριλαμβανομένων των logistics, της ασφάλειας στον ιστό και ακόμη και της χρηματοδότησης του εμπορίου. Ωστόσο, πουθενά αυτή η πρόοδος δεν είναι πιο εμφανής από την αυξανόμενη λειτουργία της ως μια καινοτόμο λύση πληρωμής. Ένας από τους βασικούς πυλώνες που οδηγούν αυτήν την ταχεία υιοθέτηση είναι η αγκαλιά έξυπνων συμβάσεων³⁵.

Με απλά λόγια, τα έξυπνα συμβόλαια είναι μια μορφή αυτοματοποιημένων συμβάσεων που χρησιμοποιούν προκαθορισμένους κανόνες για τη διευκόλυνση της ανταλλαγής σχεδόν οποιουδήποτε αγαθού ή υπηρεσίας. Η πρωταρχική αρχή είναι η αύξηση της διαφάνειας της συναλλαγής, μειώνοντας παράλληλα τα τέλη και περιορίζοντας τις πιθανότητες σύγκρουσης για τη μη απόδοση. Ωστόσο, σε αντίθεση με τα παραδοσιακά

³⁵ Kaplanov N., (2012), Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, Heinonline

συμβόλαια, αυτά τα συμβόλαια δεν έχουν περιθώρια ερμηνείας επειδή όλοι οι όροι είναι προκαθορισμένοι και αυτομάτως επιβάλλονται από τη σύμβαση.

Τα έξυπνα συμβόλαια είναι απλά έξυπνα. Είναι πολύ προσεκτικά σχεδιασμένα για να εκτελούν ειδικά σχεδιασμένες λειτουργίες και εργασίες χωρίς την παρέμβαση ενός από τα μέρη που θα μπορούσαν να οδηγήσουν σε παραβίαση της εν λόγω σύμβασης. Σε περίπτωση παραβίασης, η σύμβαση βελτιστοποιείται για να διασφαλιστεί ότι το άλλο μέρος δεν θα υποστεί ζημιά από την παραβίαση.

Η αρχή της διατήρησης κεφαλαίων σε μεσεγγύηση, για παράδειγμα, επιλύεται πλήρως με έξυπνα συμβόλαια χωρίς την ανάγκη για ένα ιδιαίτερα περίπλοκο νομικό πλαίσιο που απαιτεί αμοιβές ή μεσίτη. Κάθε πλευρά προστατεύεται από τη συμφωνία. Εάν ο πωλητής αποτύχει να παραδώσει με όλους τους όρους της σύμβασης, το άλλο μέρος διατηρεί τα χρήματά του ή άλλο παραδοτέο. Το αντίστροφο ισχύει επίσης εάν ο αγοραστής αποτύχει να δημοσιεύσει τα χρήματα στο χρηματικό ποσό.

Καθώς η κρυπτογράφηση κερδίζει μεγαλύτερη εφαρμογή και υιοθέτηση, τα έξυπνα συμβόλαια επιτρέπουν αποτελεσματικά το εμπόριο με σημαντικά λιγότερα εμπόδια. Οι εταιρείες αγωνίζονται ήδη στο χώρο για να δημιουργήσουν απλές συμβατικές λύσεις για επιχειρήσεις όλων των σχημάτων και μεγεθών.

Ένα παράδειγμα αυτής της εστίασης στα έξυπνα συμβόλαια είναι η Jincor, χάρη στην απλοποίηση του συστήματος για συμβαλλόμενα μέρη που δεν είναι άνετα με την τεχνολογία blockchain ή τις εφαρμογές κρυπτογράφησης. Το σύστημα μπορεί να χειριστεί μεταφορές που συνδέονται με εμπορικές συμφωνίες ή ακόμη και να εφαρμόσει συμβάσεις εργασίας. Η ολοκληρωμένη λύση πορτοφολιού που συνοδεύεται από πρότυπα συμβολαίων και μια πλατφόρμα διαιτησίας βοηθά την Jincor να διευρύνει την έκκληση για εταιρείες που αναζητούν τρόπους να ενσωματώσουν το blockchain με τις καθημερινές επιχειρηματικές δραστηριότητες³⁶.

³⁶ Kaplanov N., (2012), Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, Heinonline

Τελικά, η έννοια των έξυπνων συμβάσεων οφείλει πολύ την επιτυχία της σε δύο από τους βασικούς πυλώνες της: την αυτοματοποίηση και την εξοικονόμηση κόστους που προσφέρει. Κυρίως, η μεταφορά χρημάτων σε ψηφιακό περιβάλλον είναι πολύ ταχύτερη από τις παραδοσιακές τραπεζικές μεταφορές, οι οποίες μπορεί να είναι χρονοβόρες και δαπανηρές. Εάν τα ψηφιακά πορτοφόλια και στις δύο πλευρές μιας συναλλαγής μπορούν να επαληθευτούν, δημιουργεί μια ατμόσφαιρα εμπιστοσύνης που επιτρέπει και στα δύο μέρη να συνεργαστούν χωρίς φόβο απώλειας ή ανάγκη οικοδόμησης εμπιστοσύνης.

Όταν τα μεγάλα συμβόλαια εξαρτώνται από τις δύο πλευρές που πληρούν πολλές προϋποθέσεις, πολλά πράγματα θα μπορούσαν να πάνε στραβά. Αυτό σημαίνει ότι οι εταιρείες αντιμετωπίζουν κάποιο βαθμό κινδύνου όταν συναλλάσσονται με προμηθευτές ή πελάτες. Για να προχωρήσουμε χωρίς τον κίνδυνο μιας νομιμοποιημένης διαδικασίας σε περίπτωση που οι δύο πλευρές δεν εκπληρώσουν τις υποχρεώσεις τους, δύο οντότητες μπορούν να συνάψουν μια έξυπνη σύμβαση που καθορίζει ένα σύνολο ορόσημων για την πληρωμή που πρόκειται να αποδεσμευτεί για οποιεσδήποτε υπηρεσίες παρέχονται ή λαμβάνονται. Εκτός από το εξαιρετικό εργαλείο διαχείρισης κινδύνων, τα έξυπνα συμβόλαια μπορούν αποτελεσματικά να αφαιρέσουν την εμπιστοσύνη από την εξίσωση συναλλαγής.

Χάρη στα πολυάριθμα λειτουργικά οφέλη των έξυπνων συμβάσεων, ξεχωρίζουν ως μια από τις καλύτερες καινοτομίες που συνοδεύουν την ανάπτυξη blockchain. Εκτός από την παροχή βοήθειας σε πρώην μη ενδιαφερόμενα μέρη να υιοθετήσουν το blockchain για πληρωμές και συμφωνίες, οι προστασίες που προσφέρουν τα έξυπνα συμβόλαια αποτελούν ένα σενάριο win-win για όλους τους συμμετέχοντες.

Με την επιτάχυνση των προσπαθειών αυτοματοποίησης σε όλο τον κόσμο, το blockchain και τα ψηφιακά καθολικά θα διαδραματίσουν καθοριστικό ρόλο σε όλες τις βιομηχανίες. Για το σκοπό αυτό, τα έξυπνα συμβόλαια είναι μια χρήσιμη καινοτομία που συνοδεύει πολλές δραστηριότητες blockchain, βοηθώντας τους τελικούς χρήστες να επωφεληθούν μειώνοντας τις χρεώσεις, επιταχύνοντας τις ταχύτητες συναλλαγών, διασφαλίζοντας την απόδοση και αυξάνοντας την προστασία για συνδεδεμένα μέρη που συνάπτουν συμφωνία³⁷.

³⁷ Yermark D., (2015), Is Bitcoin a real currency? An economic appraisal, Elsevier

Ειδικότερα, οι έξυπνες συμβάσεις (smart contracts) είναι κομμάτια κώδικα που εκτελούν μια συναλλαγή όταν συμβαίνει μια προϋπόθεση (για παράδειγμα «εάν είναι η πρώτη του μήνα, τότε πληρώνεται το ασφάλιστρο μου»).

Ως εκ τούτου, το όνομα έξυπνες συμβάσεις δεν είναι ακριβές: Δεν είναι ούτε έξυπνα (δεν υπάρχει γνωστικό συστατικό, απλώς αυτόματη εκτέλεση μόλις εκπληρωθεί μια προϋπόθεση), ούτε σύμβαση υπό νομική έννοια. Για παράδειγμα, αν η ιδιοκτησία ενός σπιτιού θα καταγραφόταν σε ένα blockchain, θα ήταν δυνατό να μεταβιβαστεί η ιδιοκτησία σε άλλο μέρος εντός του δικτύου. Αλλά, βάσει μόνο του έξυπνου συμβολαίου, θα ήταν νόμιμη αυτή η μεταφορά ή απαιτούνται άλλες διατυπώσεις εκτός του blockchain για την τελειοποίηση της συναλλαγής³⁸;

Το «αν...». Το στοιχείο της έξυπνης σύμβασης βασίζεται σε δεδομένα από το εξωτερικό του blockchain που παρέχεται από ένα "oracle" - το οποίο θα μπορούσε να είναι μια βάση δεδομένων ή ένα άτομο - παρέχοντας επιβεβαίωση ότι έχει εκπληρωθεί η προϋπόθεση. Ένα έξυπνο συμβόλαιο είναι αντιδραστικό και εξίσου έξυπνο με τον αυτο-εκτελούμενο κώδικα στον οποίο βασίζεται και την πραγματική ακρίβεια της εισαγωγής δεδομένων από το oracle. Όταν τα δεδομένα λαμβάνονται αυτόματα και εισάγονται από αξιόπιστη πηγή, μπορεί να βασίζεται η ακρίβειά τους. Για παράδειγμα, ένα έξυπνο ασφαλιστήριο συμβόλαιο θα μπορούσε να έχει ως βάση δεδομένων μετεωρολογικών στατιστικών. Εάν η βάση δεδομένων καταγράφει μια καταιγίδα ή ξηρασία (όπως ορίζεται στο ασφαλιστήριο συμβόλαιο) που συμβαίνει, τότε οι ασφαλιστικές πληρωμές ενεργοποιούνται αυτόματα. Όταν το oracle είναι ένα άτομο που εισάγει δεδομένα χειροκίνητα, υπάρχει προφανώς κίνδυνος ανθρώπινου σφάλματος. Σε περίπτωση σφάλματος στην κωδικοποίηση, το αποτέλεσμα μπορεί να είναι λάθος ανεξάρτητα από την ακρίβεια της πρόβλεψης³⁹.

³⁸ Cong L., (2019), Blockchain disruption and smart contracts, Elsevier

³⁹ Kosba A., (2016), Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, Taylor and Francis

4.4 Λύσεις για την καλύτερη εφαρμογή των έξυπνων συμβάσεων

Καθώς οι δικηγόροι και οι ειδικοί της τεχνολογίας αντιμετωπίζουν αυτά τα ζητήματα, διερευνούνται διάφορες λύσεις. Η μια λύση είναι να γίνει συνδυασμός αδειοδοτημένων και μη blockchains όπου τα στοιχεία των προτεινόμενων συναλλαγών απαιτούν κάποια παρέμβαση από ένα υπεύθυνο μέρος, όπως η συμμόρφωση με τους κανονισμούς και η γνωριμία με τον εκάστοτε πελάτη. Όλοι οι συμμετέχοντες και οι χρήστες των blockchain και των έξυπνων συμβάσεων στα οποία ανταλλάσσονται προσωπικά δεδομένα είναι υπεύθυνοι επεξεργασίας δεδομένων και πρέπει να συμμορφώνονται ανεξάρτητα με όλες τις απαιτήσεις προστασίας δεδομένων. Όλα τα μέρη που εκτελούν κόμβους στο blockchain είναι επεξεργαστές δεδομένων πρέπει να συμμορφώνονται με τις σχετικές διατάξεις. Αυτό διαχειρίζεται ευκολότερα σε μια άδεια από ότι σε ένα blockchain χωρίς άδεια⁴⁰.

Μια άλλη λύση είναι να αποφασιστεί τι συμβαίνει στο blockchain ή στο έξυπνο συμβόλαιο και τι καθορίζεται εκτός του blockchain. Παρόλο που είναι δυνατόν να συμπεριληφθούν διατάξεις σχετικά με την ευθύνη, τη δικαιοδοσία και άλλες νομικές πτυχές στο έξυπνο συμβόλαιο, αυτό δεν επιτρέπει περιθώρια ελιγμών ή ερμηνείας επειδή βασίζεται σε όρους.

Μια ακόμη καλύτερη λύση μπορεί να είναι να αποθηκευτεί ένα «πραγματικό» συμβόλαιο εκτός της αλυσίδας, αλλά να συνδυαστεί με μια ασφαλή τιμή κατακερματισμού, έτσι ώστε τα μέρη να μπορούν να έχουν εμπιστοσύνη ότι η συμφωνημένη έκδοση είναι αυτή που βασίζεται εκμεταλλευόμενη την ικανότητα χρονικής σήμανσης του blockchain.

Εκτός από τα γενικά νομικά ζητήματα, υπάρχουν επίσης συγκεκριμένα για τη βιομηχανία, όπως ο κανονισμός για την ευρωπαϊκή αγορά υποδομών για εταιρείες

⁴⁰ Wang S., (2019), Blockchain-enabled smart contracts: architecture, applications, and future trends

χρηματοοικονομικών υπηρεσιών, σήμανση CE στον τομέα της αυτοκινητοβιομηχανίας και κανονισμοί για τη διατήρηση της φύσης που επηρεάζουν τις εξορυκτικές βιομηχανίες. Σε ορισμένες περιπτώσεις μπορεί να είναι δυνατό να δημιουργηθεί αποδεδειγμένη συμμόρφωση στο blockchain ενώ άλλες μπορεί να απαιτούν λύση εκτός της αλυσίδας.

ΚΕΦΑΛΑΙΟ 5: ΤΟ ΔΙΚΑΙΟ ΤΟΥ BLOCKCHAIN ΚΑΙ ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΞΕΠΛΥΜΑΤΟΣ ΧΡΗΜΑΤΩΝ

5.1 Οι ρυθμίσεις του Blockchain

Οι τρόποι ρύθμισης περιγράφονται ως οι τρόποι με τους οποίους το κράτος μπορεί να ρυθμίσει το σχεδιασμό και τη λειτουργία αποκεντρωμένων δικτύων blockchain και να επιβάλει τους δικούς του κανόνες που κατοχυρώνονται στους νόμους. Μια βασική θεωρία είναι αυτή των κουκίδων του Lessig που παρουσιάστηκε πριν από σχεδόν δύο δεκαετίες, για να συζητήσει τις ευκαιρίες του κράτους να ρυθμίσει την τεχνολογία blockchain μέσω νόμων, κοινωνικών κανόνων, παρέμβασης στην αγορά και κώδικα. Όσον αφορά τους νόμους, επικεντρωνόμαστε στα σημεία στα οποία το κράτος μπορεί να παρεμβαίνει στη λειτουργία ενός αποκεντρωμένου τεχνολογικού δικτύου⁴¹.

Η ανάλυση μας στρέφεται στη συνέχεια στα πλεονεκτήματα και τις δυσκολίες της ρύθμισης τεχνολογιών blockchain με άλλα μέσα. Οι δυνάμεις της αγοράς νοούνται ως κρατικές αγορές και πωλήσεις κρυπτονομισμάτων μέσω άμεσης παρέμβασης στην αγορά, για αύξηση ή μείωση του κόστους των υπηρεσιών στις οποίες αυτά τα διακριτικά καθιστούν προσβάσιμα. Η ρύθμιση μέσω κοινωνικών κανόνων νοείται ως η διακυβέρνηση της τεχνολογίας και οι διαδικασίες, τα θεσμικά όργανα και οι λογικές της λήψης αποφάσεων εντός της κοινότητας προγραμματιστών. Η ρύθμιση της μέσω αρχιτεκτονικής συζητείται ως ευκαιρία να απαιτηθούν ορισμένες λειτουργίες στον κώδικα, η εφαρμογή διαδικασιών πιστοποίησης κώδικα ή ο κυβερνητικός κώδικας παραγωγής. Η ανάλυση ολοκληρώνεται με μια σύντομη συζήτηση ορισμένων ρυθμιστικών συμβιβασμών ιδίως την προϋπόθεση ανταλλαγής μεταξύ ρύθμισης και καινοτομίας, υποστηρίζοντας ότι μια υπερβολικά ζήλια ρυθμιστική προσέγγιση μπορεί

⁴¹ Mullan, P., (2014), *The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations*. U.S.A.: Palgrave Macmillan US

να καταπνίξει την καινοτομία σε δίκτυα από άκρο σε άκρο, σε μη ρυθμιζόμενους τομείς λογισμικού και αγορές.

Έτσι λοιπόν ο λεπτομερής και πειστικός λογαριασμός για το πώς μπορούν τελικά να ρυθμιστούν τα blockchain φαίνεται να έρχεται σε αντίθεση με το επιχείρημα ότι η τεχνολογία blockchain είναι δύσκολη, αν όχι αδύνατη, να ρυθμιστεί. Κατά κάποιο τρόπο, αυτό το επιχείρημα υπονομεύει πολλές από τις περιπτώσεις χρήσης και τα υποτιθέμενα οφέλη της τεχνολογίας.

Δεύτερον, η ρύθμιση των τεχνο-κοινωνικών συνελεύσεων με αποκεντρωμένη τεχνολογία στο επίκεντρο τους είναι ένα πρόβλημα τόσο παλιά όσο το τυπογραφικό, αν όχι παλαιότερο. Ένας μεγάλος αριθμός συγκεκριμένων ρυθμιστικών πλαισίων και ένας ακόμη μεγαλύτερος αριθμός επιστημονικών αναλύσεων είναι διαθέσιμες για να συζητήσουμε αυτό το πρόβλημα τόσο σε γενικό επίπεδο, όσο και σε λεπτομερείς λεπτομέρειες. Η δυνατότητα ρύθμισης των δικτύων peer-to-peer αναπτύχθηκε και επεξεργάστηκε στο πλαίσιο της επιβολής πνευματικών δικαιωμάτων. Οι κανονιστικές ανταλλαγές μεταξύ της ενεργοποίησης ενός συγκεκριμένου επιπέδου εγκληματικής δραστηριότητας σε αντάλλαγμα για την ασφάλεια και την ασφάλεια των διαδικτυακών επικοινωνιών συζητήθηκαν εκτενώς στο πλαίσιο της τεχνολογίας TOR που ενισχύει την προστασία της ιδιωτικής ζωής και άλλων PET.

Η αυξανόμενη προβολή της «κοινής οικονομίας» - η άνοδος των online μονοπωλίων πλατφόρμας που συγκεντρώνουν πόρους - προκάλεσε ζωνές συζητήσεις σχετικά με το πώς τέτοιες πλανητικές τεχνολογικές υποδομές θα μπορούσαν να γίνουν για να συμμορφωθούν με μια πληθώρα τοπικών, συχνά αντιφατικών κανονισμών, συμπεριλαμβανομένων των κανονισμών ομιλίας, εργατικοί νόμοι και κανόνες κατά των διακρίσεων. Οι συζητήσεις αφορούσαν τον ρόλο τους στην παρακολούθηση της συμπεριφοράς των χρηστών τους, τις υποχρεώσεις τους για την επιβολή νόμων έναντι τρίτων και ο ρόλος τους στον πόλεμο στον κυβερνοχώρο και τη γενική παροχή ασφάλειας στον κυβερνοχώρο⁴².

⁴² Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate

Επίσης η ρύθμιση θεωρείται ως πιθανή απειλή για την καινοτομία και την ανάπτυξη. Και πάλι, αυτή είναι μια προσέγγιση που επικεντρώνεται στις ΗΠΑ και ακόμη και τότε, η εγκυρότητά της είναι αμφισβητήσιμη. Οι ΗΠΑ είχαν παραδοσιακά μια πολύ πιο ανταγωνιστική προσέγγιση στον κυβερνητικό κανονισμό από ό, τι, για παράδειγμα, στην Ευρώπη. Ένα ευρύ φάσμα επιχειρημάτων και ιδεολογιών κινητοποιείται συνεχώς για να αντικρούσει την πιθανή κυβερνητική παρέμβαση στην εταιρική ή ατομική αυτονομία. Σε αυτό το πλαίσιο, η υποτιθέμενη σύγκρουση μεταξύ καινοτομίας και ρύθμισης αντικατοπτρίζει άκριτα την ελευθεριακή ιδεολογία που κυριαρχεί τόσο στην κοινότητα προγραμματιστών όσο και στην κοινότητα χρηστών. Στο βαθμό που ο αντίκτυπος των κυβερνο-ελευθεριακών, κρυπτο-αναρχικών ριζών της κοινότητας στην αρχιτεκτονική της τεχνολογίας απαιτεί κριτικό προβληματισμό, έτσι θα μπορούσε το επιχείρημα εναντίον της καινοτομίας να χρησιμοποιήσει μια πιο κριτικά ενημερωμένη ανάλυση. Ο κανονισμός δεν χρειάζεται απαραίτητα να καταπνίξει την καινοτομία. Αντίθετα, πολλές μελέτες υποστηρίζουν ότι η καινοτομία εξαρτάται από μια σειρά προϋποθέσεων που παρέχει ο κανονισμός: ασφάλεια δικαίου, ισχυρά δικαιώματα ιδιοκτησίας, εκτέλεση συμβάσεων και ικανότητα επίλυσης προβλημάτων συλλογικής δράσης. Αυτά τα ζητήματα επηρεάζουν επίσης σε μεγάλο βαθμό τον νεοεμφανιζόμενο τομέα blockchain, οπότε πρέπει να αναρωτηθούμε αν η γενική απόρριψη της ρύθμισης για την προώθηση της καινοτομίας είναι μια χρήσιμη προσέγγιση χωρίς να λαμβάνεται υπόψη ποιοι τύποι κανονισμών μπορούν πραγματικά να βοηθήσουν την καινοτομία σε διαφορετικές χώρες και δικαιοδοσίες.

Ακόμη όπως συζητάμε παρακάτω, μια πιο λεπτή κατανόηση της έννοιας της ρύθμισης θα μπορούσε να αποκάλυψε ότι η σύγκρουση δεν αφορά σε ποιο βαθμό οι κυβερνήσεις μπορούν ή πρέπει να ρυθμίσουν τις τεχνολογίες blockchain. Αντίθετα, κάποιος θα μπορούσε να υποστηρίξει ότι ο πραγματικός αγώνας είναι μεταξύ, αφενός, των ιδιωτικών τρόπων ρύθμισης (αυτορύθμιση πλατφορμών, επιχειρήσεων και τεχνολογικών δικτύων) και των ιδιωτικών παραγγελιών που επιτρέπουν και, αφετέρου, οι κανόνες που επινοήθηκαν και επιβλήθηκαν μέσω δημοκρατικά υπεύθυνων διαδικασιών και θεσμών. Το ερώτημα λοιπόν δεν είναι αν το ένα θα αντικαταστήσει το άλλο, αλλά τι είδους

λογικές μπορούν να επιτρέψουν στους ιδιωτικούς τρόπους παραγγελίας να κυριαρχήσουν σε ορισμένους τομείς, εις βάρος δημοκρατικά διαπραγματευόμενων και υπεύθυνων κανόνων⁴³.

Αυτό μας οδηγεί στο τελευταίο μας σημείο σχετικά με αυτό την ενότητα δηλαδή τη γλώσσα που χρησιμοποιείται για τη συζήτηση των προβλημάτων της ρύθμισης. Η ενότητα αναφέρεται στη ρύθμιση ως ικανότητα του κράτους να επιβάλλει τη θέλησή του σε μια τεχνολογία. Η συζήτηση επικεντρώνεται κυρίως στις τεχνολογικές διαστάσεις της ρυθμισιμότητας, δηλαδή εκείνα τα τεχνικά χαρακτηριστικά που εμποδίζουν ή επιτρέπουν την επιβολή των νόμων από το κράτος. Το ίδιο ερώτημα φαίνεται αρκετά διαφορετικό όταν συζητείται από νομική άποψη. Από αυτή την άποψη, η κατανόηση της τεχνολογίας είναι μόνο ένα πρώτο βήμα προς την αντιμετώπιση ουσιαστικών νομικών ζητημάτων. Αυτές περιλαμβάνουν ερωτήσεις σχετικά με το εφαρμοστέο δίκαιο, την αρμόδια δικαιοδοσία, τον προσδιορισμό και τη νομική κατάσταση των μερών σε μια συμφωνία, συμβατικές και νόμιμες υποχρεώσεις ή την έκθεση σε ευθύνη από διαφορετικά μέρη στο οικοσύστημα blockchain. Οποιαδήποτε ρύθμιση ή κατάσταση θα πρέπει να διευκρινίσει αυτά τα ερωτήματα (και περισσότερα) εάν θέλει να είναι κατανοητή από νομική άποψη. Μια καλή εικόνα αυτού του σημείου είναι η εκτεταμένη συζήτηση σχετικά με τη σύγκρουση μεταξύ της αρχιτεκτονικής της τεχνολογίας blockchain και των νομικών κανόνων στον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ. Άλλα παραδείγματα περιλαμβάνουν τις κανονιστικές προκλήσεις γύρω από λογισμικό ανοιχτού κώδικα ή τη ρύθμιση διασυνοριακών εγκληματικών δραστηριοτήτων με δυνατότητα Internet.

⁴³ Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate

5.2 Το δίκαιο του Blockchain

Αφού εξετάσει τη ρύθμιση της τεχνολογίας, η ενότητα αυτή αφορά τη ρύθμιση από την τεχνολογία. Έτσι αναφέρονται ορισμένα από τα θέματα σχετικά με την ενσωμάτωση νόμων στον κώδικα υπολογιστή και άλλα τεχνολογικά συστήματα που ρυθμίζουν τις ανθρώπινες δραστηριότητες. Έτσι η υπόσχεση της τεχνολογίας blockchain σε αυτόν τον τομέα είναι διπλή. Πρώτον, σε επίπεδο υποδομής ή πρωτοκόλλου, ο αποκεντρωμένος, αδιάβροχος χαρακτήρας των blockchains υπόσχεται ότι η τεχνολογία μπορεί να λειτουργήσει ως ουδέτερος, άφθαρτος διαιτητής και επιβολή κανόνων που ενσωματώνονται σε αυτήν. Δεύτερον, το επίπεδο έξυπνης σύμβασης πάνω από τη βασική υποδομή blockchain δίνει στα ιδιωτικά μέρη την ευκαιρία να εφαρμόσουν καθεστώτα ιδιωτικών παραγγελιών, επίσης ουδέτερα και άφθαρτα⁴⁴.

Τα πλεονεκτήματα τέτοιων νομικών συστημάτων βάσει κώδικα είναι ενδεικτικά τα εξής:

- Αποτελεσματικότητα
- υψηλότερα επίπεδα προβλεψιμότητας και συνέπειας
- λιγότερη αβεβαιότητα και ασάφεια στην ερμηνεία των κανόνων
- και τελικά την προσαρμοστικότητα των κανόνων

Ο κώδικας Blockchain λέγεται επίσης ότι μπορεί να παρακολουθεί τη νομική συμμόρφωση, καθώς και να αυτοματοποιεί και να ομοιομορφώνει την επιβολή με τρόπο που δεν εισάγει διακρίσεις. Υπάρχουν φυσικά περιορισμοί στην προσέγγιση «κώδικας ως νόμος». Για παράδειγμα, μπορεί να αποδειχθεί δύσκολο να μεταφερθούν σκόπιμα διαφορούμενοι και αόριστοι νομικοί κανόνες σε σαφή και ντετερμινιστικό τεχνικό κώδικα. Οι εξουσίες ερμηνείας και διακριτικής ευχέρειας είναι βαθιά ριζωμένα χαρακτηριστικά των νομικών μας συστημάτων, αλλά είναι δύσκολο να εφαρμοστούν σε άκαμπτα συστήματα βασισμένα σε κώδικα. Επιπλέον, η αυτόματη επιβολή καταργεί τις εξουσίες διακριτικής ευχέρειας του κράτους ή των ιδιωτών σχετικά με τον τρόπο εφαρμογής νόμων σε συγκεκριμένα πλαίσια ή σχετικά με την παραβίαση της σύμβασης όταν αυτό είναι μια πιο αποτελεσματική πορεία δράσης. Η ευπάθεια του κώδικα σε

⁴⁴ Rodriques U., (2018), Law and the Blockchain, Hein online

τυχερά παιχνίδια, εκμετάλλευση ή πειρατεία είναι επίσης ένα επαναλαμβανόμενο ζήτημα. Η αλγοριθμική εξατομίκευση των κανόνων και των νόμων εγείρει ζητήματα με άλλες θεμελιώδεις αξίες στο νομικό και δικαστικό σύστημα, όπως η επίσημη ισότητα ενώπιον του νόμου.

Επομένως, αναρωτιέται κανείς, ποια είναι ακριβώς η πηγή των υποτιθέμενων κερδών απόδοσης για συστήματα βασισμένα σε blockchain - ή γενικότερα, αλγοριθμική λήψη αποφάσεων - και συστήματα επιβολής κανόνων; Εάν η πηγή της αποτελεσματικότητας είναι η έλλειψη ανθρώπινης εποπτείας ή διακριτικής ευχέρειας ή η περιορισμένη ικανότητα των χρηστών να αμφισβητούν, να αμφισβητούν, να αμφισβητούν και να διορθώνουν αλγοριθμικές αποφάσεις, τότε το ερώτημα που πρέπει να θέσουμε δεν είναι εάν ένα τέτοιο σύστημα είναι τεχνικά δυνατό ή αποδοτικό, αλλά αν είναι επιθυμητό.

Υπάρχει αυξανόμενη εμπειρική και θεωρητική υποτροφία σχετικά με τη λειτουργία και τον αντίκτυπο των αυτοματοποιημένων, αλγοριθμικών συστημάτων στο δημόσιο τομέα, στους τομείς της αστυνόμευσης, της ευημερίας, της υγειονομικής περίθαλψης και στον ιδιωτικό τομέα, όπως χρησιμοποιείται από τις ασφαλιστικές εταιρείες, τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας, την αναζήτηση κινητήρες κ.λπ. Από αυτές τις μελέτες είναι σαφές ότι τέτοια συστήματα απέχουν πολύ από αυτό που αναμενόταν να είναι: ένας ουδέτερος, αμερόληπτος, δίκαιος δικαστής και επιβολή κανόνων. Είναι όλο και πιο προφανές ότι είναι πολύ δύσκολο - αν όχι αδύνατο - να αντιμετωπιστούν οι ρητές και σιωπηρές προκαταλήψεις που κωδικοποιούνται σε αλγοριθμικά συστήματα. Εφ' όσον υπάρχουν τέτοιες προκαταλήψεις, είναι λογικό να απαιτείται περισσότερη (όχι λιγότερο) ανθρώπινη εποπτεία όταν δημόσιοι και ιδιωτικοί φορείς αρχίζουν να εκχωρούν μέρος της εξουσίας τους σε αλγοριθμικά συστήματα. Παρά τον πλούτο και το βάθος των συζητήσεων σχετικά με την τεχνητή νοημοσύνη, τη διακυβέρνηση των δεδομένων, τον καπιταλισμό παρακολούθησης, την προγνωστική αστυνόμευση, τις αλγοριθμικές διακρίσεις και τα συναφή πεδία, υπήρξε μικρή προσπάθεια να τα συνδέσουμε με το ζήτημα της ρύθμισης μέσω τεχνολογιών blockchain⁴⁵.

Πρέπει επίσης να ρωτήσουμε εάν η ρύθμιση μέσω της τεχνολογίας blockchain είναι στην πραγματικότητα η άκαμπτη, αμετάβλητη, αυτόματη εκτέλεση της μηχανής επιβολής.

⁴⁵ Rodrigues U., (2018), Law and the Blockchain, Hein online

Υποψιαζόμαστε ότι, εκτός από αυτό το αυστηρό καθεστώς επιβολής, οι μπλοκ κινητοποίησης κινητοποιούν επίσης ένα άλλο, εντελώς διαφορετικό ρυθμιστικό καθεστώς, βάσει οικονομικών κινήτρων. Σε τελική ανάλυση, τα blockchains ενσωματώνουν ένα σύνθετο σύστημα κρυπτοοικονομικών κινήτρων στο σχεδιασμό της τεχνολογίας. Η κρυπτο-οικονομία προσπαθεί να κωδικοποιήσει θεωρητικές γνώσεις παιχνιδιών στην υποδομή λογισμικού για να ενθαρρύνει συγκεκριμένες συμπεριφορές, ενώ αποθαρρύνει άλλους. Πολλά εγγενή χαρακτηριστικά της τεχνολογίας blockchain, όπως το αμετάβλητο, επιτυγχάνονται όχι καθιστώντας τα τεχνικά αδύνατα, αλλά μέσω της αποαισθητοποίησης της εξαπάτησης, δηλαδή καθιστώντας την ανεπιθύμητη συμπεριφορά απαγορευτικά δαπανηρή. Επιπλέον, καθώς λαμβάνει χώρα η πρόσφατη αποκέντρωση σε διάφορα επίπεδα αποκεντρωμένης τεχνολογίας blockchain, λεπτά κρυπτο-οικονομικά αντικίνητρα ενσωματώνονται σε μερικά από τα πρωτόκολλα για την αποτροπή της συγκέντρωσης δραστηριοτήτων και τη συμπαιγνία των ηθοποιών. Παρά την προφανή κεντρικότητά του στη λειτουργία των blockchain, η κρυπτο-οικονομία αναφέρεται μόνο σε μία μόνο υποσημείωση, η οποία αποτελεί εκπληκτική παράλειψη⁴⁶.

Έτσι ο κανονισμός πλαισιώνεται ως μάχη μεταξύ κώδικα και νόμου, μεταξύ κράτους και τεχνολογίας. Ωστόσο, γνωρίζουμε ότι τέτοιοι τεχνητοί διαχωρισμοί σπάνια προσφέρουν ένα χρήσιμο πλαίσιο για να κατανοήσουμε πώς διατάσσονται ορισμένοι κοινωνικοί, οικονομικοί, πολιτικοί και ανθρωπίνι τομείς, πώς οργανώνεται η εξουσία και οργανώνει τις σχέσεις μεταξύ διαφορετικών συστατικών. Όπως υποστήριξε ο Foucault, το Κράτος με τις νομικές του εξουσίες για καταστολή δεν είναι ο μόνος (και συχνά όχι ακόμη και ο πιο σημαντικός) παίκτης στο σύνθετο δίκτυο διαφορετικών θεσμών, πρακτικών και τεχνολογιών, που μέσω των αλληλεπιδράσεων, των αγώνων και του ανταγωνισμού διαμορφώστε τη σειρά των πραγμάτων. Αυτή η δήλωση φαίνεται ιδιαίτερα εφαρμόσιμη σε έναν τομέα όπου οι ψηφιακές τεχνολογίες είναι εξέχουσες: ισχυρές, διασυνοριακές και δικτυωμένες τεχνολογίες συγκεντρώνουν τις δραστηριότητες αμέτρητων διαφορετικών συστατικών στοιχείων, συμπεριλαμβανομένων ιδιωτικών και δημόσιων

⁴⁶ Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber

φορέων. Με τη σειρά τους, αυτές οι τεχνολογίες λειτουργούν από μια χούφτα πολυεθνικών εταιρειών, όπως η Google ή το Facebook (τουλάχιστον σε δυτικές κοινωνίες), οι οποίες είναι συχνά αρκετά ισχυρές για να ωθήσουν τις κυβερνητικές προσπάθειες για τη ρύθμισή τους, αλλά μερικές φορές οδηγούν σε τυχαίες εξεγέρσεις των υπαλλήλων τους ή οι χρήστες σχετικά με ορισμένες λεπτομερέστερες λεπτομέρειες σχετικά με τους κώδικες συμπεριφοράς και τους όρους υπηρεσίας τους. Ο υπολογιστής δεν μπορεί να απομονωθεί από αυτό το πολύπλοκο δίκτυο ως αυτόνομος πράκτορας. Ούτε έχει νόημα να εξομοιώνουμε την εξουσία με το κράτος μόνο. Κατά συνέπεια, η παράθεση κώδικα λογισμικού (και των κωδικοποιητών) δίπλα στο νόμο και στο κράτος που το παράγει και επιβάλλει είναι περιορισμένης χρήσης για την αντιμετώπιση των προκλήσεων που θέτουν οι τεχνολογίες blockchain και άλλες αποκεντρωμένες τεχνολογικές συναθροίσεις.

5.3 Ξέπλυμα χρήματος μέσω της χρήσης της τεχνολογίας

Blockchain

Ένας απλός αλλά όχι πολύ αποτελεσματικός τρόπος για να νομιμοποιήσει κάποιος βρώμικο ψηφιακό χρήμα είναι να συνδυάσει χειροκίνητα τις συναλλαγές. Έτσι όσοι θέλουν να εμπλακούν σε τέτοιες δραστηριότητες μπορούν να διπλασιάσουν και να στείλουν χρήματα μέσω πολλών πορτοφολιών διαφορετικών χρηστών. Παρόλο που η μέθοδος μπορεί να προκαλέσει σύγχυση σε έναν αρχάριο που προσπαθεί να πάρει ένα πλήρες ιστορικό λογαριασμού και την προέλευση της κρυπτογράφησης, οι επαγγελματίες δεν θα έχουν τέτοιο πρόβλημα⁴⁷.

Υπηρεσίες τρίτων όπως το LocalBitcoins ή φόρουμ όπως το Bitalk.org ή το Telegram χρησιμοποιούνται επίσης για νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Ωστόσο, η εξαργύρωση κεφαλαίων μέσω τέτοιων πλατφορμών P2P σχετίζεται με μεγάλο

⁴⁷ Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., (2012). Evaluating User Privacy in Bitcoin

κίνδυνο, καθώς κανείς δεν εγγυάται την ειλικρίνεια των πωλητών και των αγοραστών. Επιπλέον, οι πλατφόρμες επιδιώκουν να προστατευθούν από την απάτη αφαιρώντας τη δυνατότητα αγοράς κρυπτονομισμάτων με μετρητά.

Μια άλλη καυτή ιδέα της μετατροπής παράνομων εικονικών νομισμάτων σε μετρητά είναι η χρήση υπηρεσιών μικτών συναλλαγών. Υπάρχει τεράστιος αριθμός τέτοιων ιστότοπων στο δίκτυο. Δεν αποκλείονται από παρόχους διαδικτύου και λειτουργούν σε σταθερή νομική βάση. Η ατέλεια του νομοθετικού συστήματος των περισσότερων χωρών σε σχέση με τις ψηφιακές τεχνολογίες ευθύνεται. Για παράδειγμα, ένας αναμίκτης Bitcoin σάς επιτρέπει να διαιρείτε τις συναλλαγές σε διάφορα μέρη και να τις συνδυάζετε με αυτές των χιλιάδων άλλων πορτοφολιών. Ως αποτέλεσμα, ο παραλήπτης λαμβάνει το ζητούμενο ποσό από διαφορετικούς χρήστες, αλλά είναι σχεδόν αδύνατο να δημιουργηθεί σύνδεση μεταξύ του αποστολέα και του παραλήπτη.

Αν και η χρήση αυτοματοποιημένων αναμεικτών είναι πιο αποτελεσματική από τη μη αυτόματη ανάμιξη, οι σύγχρονοι αλγόριθμοι σάς επιτρέπουν να παρακολουθείτε το ιστορικό συναλλαγών σας.

Ο πιο σίγουρος τρόπος για να «καθαρίσει» κάποιος την κρυπτογράφηση θα ήταν τα ηλεκτρονικά πορτοφόλια με υψηλό βαθμό ανωνυμίας, όπως Electrum ή blockchain συμβόλαια για τη μίξη συναλλαγών. Το πιο σημαντικό, αυτή η αποκεντρωμένη προσέγγιση δεν έχει ακόμη εφαρμοστεί. Η τεχνολογία των αυτο-εκτελεστικών συμβάσεων συνεπάγεται διαφάνεια, έτσι τα μέρη που εμπλέκονται σε συναλλαγές μπορούν να αναγνωριστούν εύκολα αναλύοντας το ιστορικό συναλλαγών κατάθεσης και ανάληψης⁴⁸.

⁴⁸ Rodriques U., (2018), Law and the Blockchain, Hein online

5.4 Το δίκαιο του Blockchain σε σύγκριση με το δίκαιο του διαδικτύου

Η τεχνολογική καινοτομία του δικτύου blockchain επηρέασε τον τρόπο με τον οποίο σκεφτόμαστε τη μεταφορά και την ιδιοκτησία πληροφοριών και αξίας. Η χρήση του έχει αποδειχθεί ότι είναι ουσιαστικά να επιταχύνει τις συναλλαγές, να μειώσει το κόστος, να αφαιρέσει μεσάζοντες και να παρέχει διαφάνεια συναλλαγών.

Αυτό σημαίνει ότι οι όροι της σύμβασης μπορούν πλέον να εκτελεστούν από ένα ηλεκτρονικό πρωτόκολλο με μικρή ή καθόλου τριβή μεταξύ συμβαλλομένων μερών. Αναδύθηκαν νέα αποκεντρωμένα μοντέλα, όπως η αποκεντρωμένη διακυβέρνηση, οι αυτόνομες οργανώσεις, η διαιτησία και το crowdfunding με τη μορφή αρχικών προσφορών νομισμάτων. Ο νομικός τομέας συνεχίζει να επανεξετάζει πώς πρέπει να ασκεί το δίκαιο με βάση την αλλαγή των αναγκών των πελατών, την τεχνολογική πρόοδο, τη σχέση κόστους-αποτελεσματικότητας και την αποτελεσματικότητα παροχής νομικών υπηρεσιών.

Στην περίπτωση των τεχνολογιών blockchain το πιο προφανές νομικό ζήτημα είναι αυτό της ανωνυμίας. Το εκάστοτε ψηφιακό νόμισμα μπορεί να χρησιμοποιηθεί για τη χρηματοδότηση παραοικονομικών δραστηριοτήτων και να κάνει τα συνηθισμένα χρήματα να "εξαφανιστούν" από τον έλεγχο του νόμου. Είναι επίσης ένας τρόπος απόκρυψης συναλλαγών που υπόκεινται σε φόρο.

Οι blockchains κάνουν καλύτερη και ταχύτερη δουλειά καταγράφοντας συναλλαγές και έτσι θα μπορούσαν ενδεχομένως να αντικαταστήσουν τις τράπεζες ως κατόχους και διαχειριστές οποιουδήποτε νομίσματος. Το νομικό ζήτημα εκεί περιλαμβάνει το γεγονός ότι οι τράπεζες είναι ρυθμιζόμενες και οι διαχειριστές blockchain δεν είναι.

Αυτό που μπορεί να κάνει πολύ καλά το blockchain είναι η δημιουργία και η εκτέλεση ψηφιακών συμβάσεων. Τα ψηφιακά συμβόλαια όπως έχουμε δει είναι συμβόλαια που είναι γραμμένα σε κώδικα υπολογιστή και επιβάλλονται από λογισμικό όταν πληρούνται ορισμένες προκαθορισμένες προϋποθέσεις. Όταν πληρούνται οι προϋποθέσεις το blockchain μπορεί να εκτελέσει τις συναλλαγές και να πληρώσει χρήματα.

Επίσης οι blockchains έχουν τη δυνατότητα να παρακολουθούν τις αλλαγές στην ιδιοκτησία ή την κατάσταση του ακινήτου, συμπεριλαμβανομένων των ακινήτων και των μισθωμένων αγαθών. Τα συμβόλαια για τη μεταβίβαση τέτοιων περιουσιακών στοιχείων θα ήταν ουσιαστικά άθραυστα, διότι κανείς δεν θα μπορούσε να υποστηρίξει ότι «δεν ήξερα τι υπέγραψα» ή «ήμουν υπό πίεση». Ένας δικηγόρος που συμβουλεύει για μια σύμβαση blockchain θα πρέπει επίσης να κατανοήσει τον προγραμματισμό και τη τεχνολογία των υπολογιστών.

Υπάρχουν πιθανότατα πολλά άλλα ζητήματα με blockchain που θα αντιμετωπίσουν οι δικηγόροι καθώς η τεχνολογία εξελίσσεται περαιτέρω. Έτσι λοιπόν υπάρχουν σημαντικές διαφορές ανάμεσα στο δίκαιο του blockchain το οποίο είναι αρκετά πιο πολύπλοκο από το δίκαιο που ισχύει στο διαδίκτυο για την απλή προστασία των προσωπικών δεδομένων και των συναλλαγών.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Αντικείμενο της εργασίας αυτής ήταν η μελέτη της τεχνολογίας blockchain με έμφαση στη νομοθεσία αυτής και στους νομικούς περιορισμούς που υπάρχουν προκειμένου η τεχνολογία αυτή να είναι τόσο επικερδής για τους επενδυτές αλλά και σύννομη.

Όπως είδαμε και στο κύριο μέρος της εργασίας μία από τις επαναλαμβανόμενες αφηγήσεις της τεχνολογικής ρύθμισης είναι η ελαστικότητα της νομοθεσίας έναντι της νομοθεσίας. Αυτό δημιουργεί ανταγωνιστικές, συχνά δυαδικές και αμοιβαία αποκλειστικές σχέσεις μεταξύ δύο στενά καθορισμένων εναλλακτικών λύσεων: η κατάσταση έναντι του blockchain, ο νόμος έναντι του κώδικα, δικηγόροι εναντίον κωδικοποιητών και συγκεντρωτικά θεσμικά όργανα εναντίον αποκεντρωμένων, αυτοοργανωμένων κινήσεων. Ενώ είναι ελκυστικό να παρουσιάσουμε το πρόβλημα της τεχνολογικής ρύθμισης ως αγώνα μεταξύ δύο αυτόνομων, ανεξάρτητων και ανταγωνιστικών δυνάμεων, πιστεύουμε ότι στην πράξη αυτό δεν είναι συνήθως το πώς οι δύο σχετίζονται μεταξύ τους. Διαφορετικοί τρόποι οικονομικών, κοινωνικών, πολιτικών, πολιτιστικών και αρχιτεκτονικών τρόπων οργάνωσης μπορούν να συνυπάρχουν, να συνεργαστούν και να οργανωθούν σε αμοιβαία εξαρτώμενα δίκτυα.

Το κράτος και η τεχνολογία είναι δύο μέλη μιας πολύ μεγαλύτερης ομάδας συστατικών των δικτύων μας, των ψηφιακών, των κοινωνιών της πληροφορίας, όπου διάφοροι ενδιαφερόμενοι ακολουθούν διαφορετικές ατζέντες, ανταποκρίνονται σε διαφορετικά κίνητρα και αλληλεπιδρούν με δυναμικούς - συχνά απρόβλεπτους - τρόπους. Το γεγονός ότι τέτοια περίπλοκα συστήματα είναι σχεδόν ντετερμινιστικά δεν περιορίζει τις επιστημονικές και άλλες εικασίες σχετικά με το τι θα μπορούσε να συμβεί. Αντ' αυτού, είναι δυνατόν να εντοπίσουμε τουλάχιστον ορισμένες από τις συνθήκες και τη λογική που διαμορφώνουν την ανάπτυξη τέτοιων σύνθετων τεχνο-κοινωνικών συστημάτων και να τα χρησιμοποιήσουν ως σημείο εκκίνησης για μια κριτική ανάλυση.

Οι τεχνολογίες Blockchain πρέπει να έχουν την ικανότητα να επιβάλλουν αλλαγές στον πραγματικό κόσμο, εάν επιθυμούν να είναι συναφείς σε εφαρμογές πραγματικού κόσμου, όπως δημόσια αρχεία. Όμως, όπως και πολλά από τα ζητήματα που αφορούν τα

blockchains, αυτό το ζήτημα δεν είναι εγγενές στην τεχνολογία. Αντίθετα, σχετίζεται με τα θεσμικά, νομικά, οικονομικά, πολιτικά πλαίσια στα οποία ενσωματώνεται η τεχνολογία και τα οποία μπορούν να διευκολύνουν ή να αποτρέψουν την επιβολή αλυσίδων εκτός αλυσίδας. Προχωρώντας περαιτέρω, και εξετάζοντας το ερώτημα πώς θα συνέβαινε αυτή η συγχρονικότητα, θα μπορούσε να οδηγήσει την ανάλυση σε τελείως διαφορετική κατεύθυνση, η οποία δίνει έμφαση στην αμοιβαία αλληλεξάρτηση του νόμου και της τεχνολογίας, παρά στην ανταγωνιστική αντίθεση μεταξύ των διαφόρων καθεστώτων εξουσίας.

Ακόμη σχετικά με το δίκαιο της τεχνολογίας blockchain στο επίπεδο της δικονομίας και κυρίως των αποδεικτικών μέσων, η νέα τεχνολογία θα έχει συνέπειες, καθώς είναι βέβαιο ότι η απόδειξη τίτλων κυριότητας, συναλλαγών ή και το βέβαιο της χρονολογίας πραγματικών περιστατικών θα γίνεται με την προσκόμιση των στοιχείων που αφορούν την καταχώρισή τους σε μία πλατφόρμα blockchain. Τα στοιχεία αυτά, θα μπορεί να επαληθεύει με βεβαιότητα ο δικαστής χωρίς τη συνδρομή ειδικών, αφού όλες οι καταχωρήσεις στις – ανοιχτές – βάσεις δεδομένων blockchain είναι δημόσιες και διαθέσιμες. Ομοίως γνωστοποιήσεις με βέβαιο χρονολογίας, βέβαιο περιεχόμενο και βέβαιη παραλαβή θα μπορούν να γίνονται με βάση τη νέα τεχνολογία.

Έτσι όπως είδαμε και προηγουμένως ένα από τα βασικά χαρακτηριστικά των έξυπνων συμβάσεων είναι η αυτοματοποιημένη εκπλήρωση των συμβατικών όρων εφόσον συντρέξουν οι συμφωνηθείσες προϋποθέσεις. Το χαρακτηριστικό αυτό, δηλαδή η εκπλήρωση των συμβατικών υποχρεώσεων ανεξάρτητα από τη βούληση των μερών και χωρίς τη συνδρομή ενός τρίτου μέρους, θα έχει ως συνέπεια τον περιορισμό της ανάγκης προσφυγής σε διαδικασία εκτέλεσης στις συμβατικές ενοχές.

Κλείνοντας ο μελλοντικός αντίκτυπος της τεχνολογίας blockchain θα είναι ορατός στις αλλαγές που προκαλεί στις επιχειρήσεις αλλά και σε θεσμικές πρακτικές. Γνωρίζουμε ότι πολλές από αυτές τις θεσμικές αλλαγές (ή την έλλειψη αυτών) συμβαίνουν ανεξάρτητα από την οικονομική λογική τους. Καθοδηγούνται από άλλους παράγοντες: θεσμική αδράνεια, ιστορία, μακροχρόνιες κοινωνικές δομές, έθιμα, παράλογα ανθρώπινα χαρακτηριστικά συμπεριφοράς, παράξενα δομημένα κίνητρα κ.λπ.

Υπάρχει μια πληθώρα θεωρητικών πλαισίων που λαμβάνουν υπόψη αυτούς τους παράγοντες και κατά συνέπεια παρέχει χρήσιμα αναλυτικά εργαλεία για την αντιμετώπιση των δυνατοτήτων της τεχνολογίας blockchain να αλλάξει την κοινωνική

πραγματικότητα. Η γραφειοκρατική θεωρία του Max Weber, η ανάλυση της δύναμης του Foucault, η θεωρία του δικτύου του Lourour Actor, ή η θεωρία του υγρού εκσυγχρονισμού του Bauman ή τα οικονομικά συμπεριφοράς, για να αναφέρουμε μόνο μερικά, όλα προσφέρουν κάτι πολύτιμο για τους ερευνητές blockchain. Ωστόσο, η εργασία αυτή υποθέτει απλώς ότι θα υπάρξει θεσμική αλλαγή λόγω της ακαταμάχητης δύναμης της τεχνολογικής αποκέντρωσης και της οικονομικής αποτελεσματικότητας που συνεπάγεται αυτό. Μια τέτοια αναγωγική προσέγγιση δεν φαίνεται να δικαιολογείται πλήρως, είτε θεωρητικά είτε εμπειρικά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Grinberg R., (2012), Bitcoin: An innovative alternative digital currency, Hein Online
- Kaplanov N., (2012), Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, Heinonline
- Yermark D., (2015), Is Bitcoin a real currency? An economic appraisal, Elsevier
- Bordo M., Levin A., (2017), Central bank digital currency and the future of monetary policy, Nber
- Engert W., Fung B., (2017), Central bank digital currency: motivations and implications, Researchgate
- Gans J., Halaburda H., (2015), Some economics of private digital currency, Nber
- Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., (2012). Evaluating User Privacy in Bitcoin
- European Central Bank, (ECB), (2015), Virtual currency schemes –a further analysis
- Mullan, P., (2014), The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations. U.S.A.: Palgrave Macmillan US
- Beigel, O., 2015. How to Safely Deposit and Withdraw Bitcoins from a Paper Wallet, Jstor
- Rodrigues U., (2018), Law and the Blockchain, Hein online
- Yeung K., (2019), Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law, Wiley
- Giannopoulou A., (2019), Blockchain and the law, Ssrn
- Dimitropoulos G., (2020), The Law of Blockchain, Ssrn
- Corrales M., (2019), Legal Tech, Smart Contracts and Blockchain, Springer
- Alston E., (2020), Blockchain and the Law–Legality, Law-like Characteristics, and Legal Applications, Ssrn

Nadimi P., (2019), Practicing Blockchain Law, Hein online

Κυριαζόγλου I., (2019), Προστασία προσωπικών δεδομένων (GDPR Protection), εκδόσεις Φυλάτος

Κοτσαλής Λ., Μενουδάκος Κ., (2018), Γενικός κανονισμός για την προστασία των προσωπικών δεδομένων (GDPR), εκδόσεις Νομική βιβλιοθήκη

Πλατής Ε., (2018), Προσωπικά δεδομένα, εκδόσεις Παπαδόπουλος

Νόμος 4624 / 2019

Block H. Jarn, Colombo G. Massimo, Cumming J. Douglas, Vismara Silvio, 2016, New players in entrepreneurial finance and why they are there, pp.6-9

J.D. von Pischke, 1997, Poverty, Human Development and Financial Services, pp.2-6

McKinsey Global Institute, 2016, Digital Finance for All: Powering Inclusive Growth in emerging economies, pp. 12-64

Peterson Kitakogelu Ozili, 2018, Impact of Digital Finance on Financial Inclusion and Stability, pp. 5-25

World Development Report, 2016, Enabling Digital Development, pp.1-5

World Economic Forum, 2016, The Role of Financial Services in Society: Understanding the impact of technology-enabled innovation on financial stability, pp.8-10

World Economic Forum, 2017, Unlocking Digital Value to Society: A new framework for growth, pp.15-24