ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ
ΕΥΡΥΚΛΕΙΑ ΚΩΝΣΤΑΝΤΙΝΙΔΟΥ

ΚΡΥΠΤΟΟΙΚΟΝΟΜΙΑ

ΘΕΩΡΙΑ & ΕΦΑΡΜΟΓΕΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΝΙΚΟΛΑΟΣ ΠΑΠΑΔΑΚΗΣ

ΕΦΑΡΜΟΣΜΕΝΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΡΕΥΝΑ & ΑΝΑΛΥΣΗ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΟΛΥΤΕΧΝΕΙΟΥ
ΚΡΗΤΗΣ - ΣΤΡΑΤΙΩΤΙΚΗΣ ΣΧΟΛΗΣ ΕΥΕΛΠΙΔΩΝ
ΑΘΗΝΑ 2024

Η Μεταπτυχιακή Διατριβή της Ευρύκλειας Κωνσταντινίδου εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Αναπλ. Καθηγητής Παπαδάκης Νικόλαος (ΣΣΕ, Επιβλέπων)

Νικόλαος Παπαδάκης

Καθηγητής Δάρας Νικόλαος (ΣΣΕ)

Αναπλ. Καθηγητής Τσαφαράκης Στέλιος (ΠΚ)

Stelios Tsafarakis

Digitally signed by Stelios Tsafarakis
DN: c=GR, l=Chania, o=Technical University of Crete, sn=Tsafarakis, givenName=Stelios, serialNumber=4877168308, cn=Stelios Tsafarakis
Date: 2025.02.04 11:26:44 +02'00'

,……..

ΠΕΡΙΛΗΨΗ

ΚΡΥΠΤΟΟΙΚΟΝΟΜΙΑ

ΘΕΩΡΙΑ & ΕΦΑΡΜΟΓΕΣ

Χρήμα είναι το ιδιαίτερο εμπόρευμα που εκπληρώνει το ρόλο του γενικού ισοδύναμου, δηλαδή του εμπορεύματος που εκφράζει την αξία όλων των άλλων εμπορευμάτων και μέσω του οποίου γίνονται οι ανταλλαγές τους. Κατά την οργάνωση των ανθρώπων σε κοινωνίες, από το στάδιο των ανταλλαγών, άρχισε να εμφανίζεται το χρήμα με τη μορφή διάφορων εμπορευμάτων που αποκτούσαν χαρακτήρα γενικού ισοδύναμου. Στην εξελικτική πορεία της κοινωνίας, για λόγους διευκόλυνσης αλλά και φυσικής σύστασης, άρχισαν να καθιερώνονται ως γενικό ισοδύναμο πολύτιμα μέταλλα, όπως το ασήμι ή ο χρυσός. Στη συνέχεια, θεσμοί όπως ναοί και ιερείς εμφανίζονται ως μεσολαβητές των ανταλλαγών, σημαίνοντας τις απαρχές των τραπεζικών ιδρυμάτων. Τον 20ό αιώνα τα χαρτονομίσματα αντικατέστησαν την κυκλοφορία χρυσού, διατηρώντας τον όμως σαν γενικό ισοδύναμο, αφού η αξία των χαρτονομισμάτων καταδεικνύονταν από τα αποθέματα χρυσού. Οι χώρες ανέπτυξαν το δικό τους χρήμα, ή εθνικό νόμισμα, το οποίο αντιστοιχίζεται σε διεθνές συνάλλαγμα προκειμένου να πραγματοποιούνται οι ανταλλαγές. Πλέον, τα χαρτονομίσματα δεν αντιστοιχίζονται με αποθέματα χρυσού.

Το κρυπτονόμισμα, εμφανίζεται ως μια ψηφιακή μορφή χρήματος, που υπάρχει μόνο ως ψηφιακό αποτύπωμα και όχι σε φυσική μορφή. Η υπόστασή του συνδέεται με τα μαθηματικά της κρυπτογραφίας. Μέσω πολύπλοκων υπολογισμών καθορίζεται το σύνολο των μονάδων, αλλά και το πώς και πότε δημιουργούνται μονάδες του νομίσματος. Η εξέλιξη της τεχνολογίας μπορεί να εγγυηθεί υψηλή ασφάλεια στη διεκπεραίωση των συναλλαγών. Η λειτουργία των κρυπτονομισμάτων, βασίζεται στην τεχνολογία blockchain. Είναι μια αλυσίδα μπλοκ, που περιέχουν κρυπτογραφημένες ψηφιακές συναλλαγές. Περιγράφεται ως ένα κατανεμημένο καθολικό (λογιστικό φύλλο), το οποίο υπόκειται σε δημόσια διαχείριση από τους χρήστες. Οι ίδιοι οι χρήστες επικυρώνουν και διασφαλίζουν τις πραγματοποιούμενες συναλλαγές, με τη χρήση υπολογιστικών συστημάτων. Οι έννοιες των αλυσίδων των μπλοκ και των κατανεμημένων καθολικών συναντώνται και παλαιότερα σε αστικές συναλλαγές ιδιοκτησίας, όπως ακίνητης περιουσίας. Η σύνδεση , όμως, αυτών των δύο εννοιών σε ένα (συνήθως) ασφαλές υπολογιστικό σύστημα, που θα μπορούσε να χρησιμοποιηθεί για την επίλυση πολλών πρακτικών προβλημάτων σημαίνει μια νέα εποχή.

Στην παρούσα εργασία, επιχειρείται μια ανάλυση του τρόπου λειτουργίας των κρυπτονομισμάτων, της τεχνολογίας blockchain, του θεσμικού πλαισίου στο οποίο πραγματοποιούνται οι ανταλλαγές, του επιπέδου ασφάλειας κατά τη χρήση τους, καθώς και μια πρόβλεψη για την εξέλιξη της τεχνολογίας αυτής. Επιχειρείται ακόμη, η εφαρμογή της γνώσης, με τη δημιουργία ενός κρυπτονομίσματος, (coin & token) με σκοπό τη βαθύτερη κατανόηση της λειτουργίας και χρήσης τους ως μέσο ανταλλαγής.

ABSTRACT

CRYPTOCURRENCY

THEORY & APPLICATION

Money is the particular commodity that fulfils the role of the general equivalent, that is, the commodity that expresses the value of every other commodity and through which exchanges take place. During the organisation of people in societies, from the stage of exchange, money began to appear in the form of various commodities that acquired the character of a general equivalent. In the evolutionary course of society, for reasons of convenience but also of natural composition, precious metals, such as silver or gold, began to be established as a general equivalent. Then, institutions such as temples and priests appear as mediators of exchanges, signifying the beginnings of banking institutions. In the 20th century, banknotes replaced the circulation of gold, while gold was still the general equivalent, as the value of banknotes was demonstrated by national gold reserves. Each country developed its own money, or national currency, which is denominated in international currency in order for exchanges to take place. Banknotes are no longer matched with gold reserves.

Cryptocurrency appears as a digital form of money, which exists only as a digital imprint and not in any physical form. Its essence is connected with the mathematics of cryptography. Complex calculations determine the total number of units, but also how and when currency units are created. High security in the processing of transactions can now be guaranteed by technological development. The operation of cryptocurrencies is based on blockchain technology. It is a chain of blocks, containing encrypted digital transactions. Described as a distributed ledger, which is publicly managed by users. Users themselves validate and secure the transactions, using computer systems. The concepts of blockchain and distributed ledger have been used in the past in civil property transactions, such as real estate. However, the connection of these two concepts to a (usually) secure computer system that could be used to solve many practical problems signifies a new era.

In this thesis, an analysis is attempted, regarding the operation of cryptocurrencies, blockchain technology, the institutional framework in which exchanges take place, the level of security their usage provides, as well as a prediction regarding the evolution of this technology. There will also be an attempt to create a digital currency, (coin & token) in order to deeper understand their function as an exchange equivalent.

Αφιέρωση

Αφιερώνω την παρούσα εργασία στον σύζυγό μου Ανδρέα, για την στήριξη και την αγάπη του που με βοήθησαν να ολοκληρώσω αυτό το κεφάλαιο της ζωής μου.

Στα παιδιά μου, Κωνσταντίνο, Δημήτρη και Αντιγόνη, που μου δίνουν κίνητρο και δύναμη να προχωρώ μπροστά. Η αγάπη τους είναι η πηγή έμπνευσης μου.

Στους γονείς μου, για την αδιάκοπη υποστήριξη, τις θυσίες και την πίστη τους. Για την ενθάρρυνση και την υποστήριξή τους στην ακαδημαϊκή μου πορεία.

Τέλος, θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου, για την πολύτιμη γνώση, την καθοδήγηση και αφοσίωσή τους σε όλη τη διάρκεια των σπουδών μου. Ιδιαιτέρως θα ήθελα να ευχαριστήσω τον κ.Δάρα, του οποίου η ευγένεια, η ανθρωπιά και ο επαγγελματισμός θα μου μείνουν αξέχαστα.

Με εκτίμηση,

Ευρύκλεια Κωνσταντινίδου

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΚΟΝΕΣ:

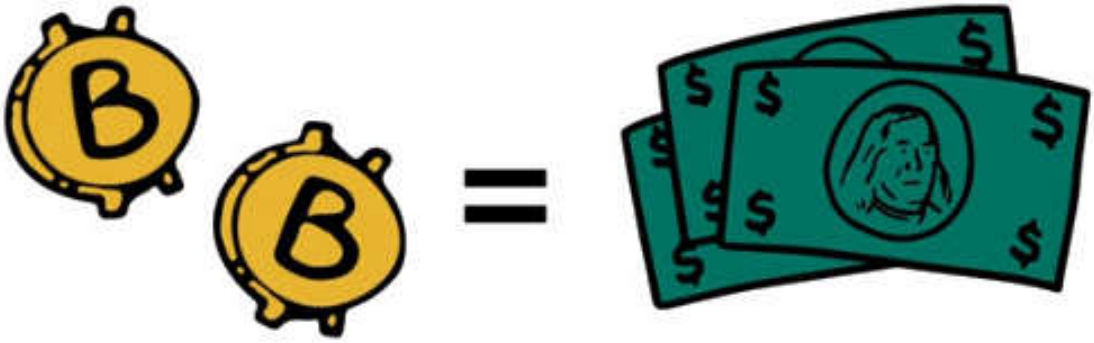
1. ΕΙΚΟΝΑ1 - ΠΗΓΗ: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency - ΣΕΛΙΔΑ 8
2. ΕΙΚΟΝΑ 2 - ΠΗΓΗ: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/, ΣΕΛΙΔΑ 10
3. ΕΙΚΟΝΑ 3 - Merkle Tree, ΣΕΛΙΔΑ 16
4. ΕΙΚΟΝΑ 4 - ΠΗΓΗ: https://www.ethereum.org/token, ΣΕΛΙΔΑ 22
5. ΕΙΚΟΝΑ 5 - ΠΗΓΗ: https://kaspersky.com/blog/the-wonders-of-hashing/4441/, ΣΕΛΙΔΑ 25
6. ΕΙΚΟΝΑ 6 - ΠΗΓΗ: Paper- Synthesizing a Bitcoin Miner SHA-256 Accelerator Core, Tommy Tracy II, ECE6502 Spring 2014, University of Virginia, ΣΕΛΙΔΑ 28
7. ΕΙΚΟΝΑ 7- BITCOIN ATM - ΠΗΓΗ: https://www.bitcoin.com/bitcoin-atm/ - ΣΕΛΙΔΑ 35
8. ΕΙΚΟΝΑ 8 - ΠΗΓΗ: Blockchain distributed ledger technologies for biomedical and healthcare applications, Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado - Journal of the American Informatics Association, Volume 24, Issue 6, Nov 2017, pages 1211-1220 - ΣΕΛΙΔΑ 36
9. ΕΙΚΟΝΑ 9 - ΠΗΓΗ: To Token or not to Token: Tools for Understanding Blockchain Tokens - Oliveira, Luis ; Zavolokina, Liudmila ; Bauer, Ingrid ; Schwabe, Gerhard - Zurich Open Repository and Archive University of Zurich Main Library - ΣΕΛΙΔΑ 43
10. ΕΙΚΟΝΑ 10 - Bitcoin logo, ΠΗΓΗ: bitcoin.otg - ΣΕΛΙΔΑ 44
11. ΕΙΚΟΝΑ 11 - Ethereum logo, ΠΗΓΗ: ethereum.org - ΣΕΛΙΔΑ 45
12. ΕΙΚΟΝΑ 12 - Cardano logo, ΠΗΓΗ: cardano.org - ΣΕΛΙΔΑ 46
13. ΕΙΚΟΝΑ 13 - Monero logo, ΠΗΓΗ: getmonero.org - ΣΕΛΙΔΑ 48
14. ΕΙΚΟΝΑ 14 - QUBES, ΠΗΓΗ: qubes-os.org/intro/ - ΣΕΛΙΔΑ 52
15. ΕΙΚΟΝΑ 15 - logo Petro, ΠΗΓΗ: whitepaperdatabase.com - ΣΕΛΙΔΑ 65
16. ΕΙΚΟΝΑ 16 - logo Diem, ΠΗΓΗ: https://www.diem.com - ΣΕΛΙΔΑ 72
17. ΕΙΚΟΝΑ 17 - Δομή Εφαρμογής - ΣΕΛΙΔΑ 95
18. ΕΙΚΟΝΕΣ 18, 19, 20, 21 - ΕΦΑΡΜΟΓΗ EKoin 1 - ΣΕΛΙΔΕΣ 105-106
19. ΕΙΚΟΝΕΣ 22, 23, 24, 25, 26, 27, 28, 29, 30 - ΕΦΑΡΜΟΓΗ EKoin 2 - ΣΕΛΙΔΕΣ 117-121
20. ΕΙΚΟΝΑ 31 - Καρτέλα δημιουργίας token - ΣΕΛΙΔΑ 127
21. ΕΙΚΟΝΑ 32 - ΔΗΜΙΟΥΡΓΙΑ token - ΣΕΛΙΔΑ 127
22. ΕΙΚΟΝΑ 33 - ΕΙΣΑΓΩΓΗ ΠΛΗΡΟΦΟΡΙΩΝ - ΣΕΛΙΔΑ 127
23. ΕΙΚΟΝΕΣ 34, 35, 36 - ΕΦΑΡΜΟΓΗ "ΕΝΑ ΑΠΛΟ ΤΟΚΕΝ" - ΣΕΛΙΔΕΣ 132, 133

ΣΧΕΔΙΑΓΡΑΜΜΑΤΑ:

1. ΤΟΠΟΛΟΓΙΑ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ, ΠΗΓΗ: Σημειώσεις από το μάθημα του κ. Ν.Μπάρδη, Κρυπτογραφία & Ασφάλεια - ΣΕΛΙΔΑ 26
2. ΠΑΡΑΔΕΙΓΜΑ blockchain - ΣΕΛΙΔΕΣ 37-39
3. ΠΑΡΑΔΕΙΓΜΑ ΚΑΤΑΛΟΓΟΥ ΣΥΝΑΛΛΑΓΩΝ - ΣΕΛΙΔΑ 39-41

ΜΕΡΟΣ ΠΡΩΤΟ

ΤΙ ΕΙΝΑΙ Η ΚΡΥΠΤΟΟΙΚΟΝΟΜΙΑ



ΕΙΚΟΝΑ1 - (ΠΗΓΗ: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency)

Στα τέλη της δεκαετίας του 1990 γεννήθηκε μια πρωτοποριακή ιδέα. Με αφετηρία την ανωνυμία των μετρητών, γεννήθηκε η ιδέα του χρήματος που δεν τυπώνεται από κάποιο κράτος αλλά προκύπτει από έναν κώδικα. Του χρήματος που δεν ανήκει στις τράπεζες αλλά στους πολίτες. Ο λεγόμενος κώδικας των πολιτών του Διαδικτύου, είχε αδιαμφισβήτητα μια ιδεολογική αφετηρία. Η βασική ιδέα όμως, αυτή του ψηφιακού χρήματος κατόρθωσε να υλοποιηθεί μέσω της εξέλιξης της τεχνολογίας, εισάγοντάς μας σε μια νέα εποχή. Για να κατανοήσει κανείς την κρυπτοοικονομία, θα πρέπει να ανατρέξει σε προγενέστερες μορφές του χρήματος και του ψηφιακού χρήματος. Κατά την οργάνωση των ανθρώπων σε κοινωνίες, δημιουργήθηκαν ανάγκες που καλύπτονταν με ανταλλαγές προϊόντων. Αυτές οι ανταλλαγές πραγματοποιούνταν αρχικά τυχαία. Στην πορεία άρχισε η παραγωγή προϊόντων με σκοπό την ανταλλαγή, η απλή εμπορευματική παραγωγή. Περνώντας από διάφορα στάδια συνθετότητας, την πρώτη περίοδο έχουμε άμεση ανταλλαγή προϊόντων. Με την εξέλιξη της κοινωνίας εμφανίζονται τα γενικά ισοδύναμα. Εμπορεύματα δηλαδή, τα οποία χρησιμοποιούνταν ως μέτρο σύγκρισης και ανταλλαγής με άλλα εμπορεύματα. Ως τέτοια χρησμοποιήθηκαν ζώα, εργαλεία και άλλα ευρέως χρήσιμα εμπορεύματα. Αργότερα προέκυψε η ανάγκη ενός πιο εύχρηστου, γενικού μέσου πληρωμής και αποθησαύρισης.

Το ρόλο του χρήματος, λόγω της φυσικής τους σύστασης που απέτρεπε τη φθορά, έπαιξαν τα πολύτιμα μέταλλα, όπως το ασήμι και ο χρυσός. Εισάγεται το πιστωτικό χρήμα, με τη μορφή χρεόγραφων που δέσμευαν τον οφειλέτη για την εξόφληση μιας υποχρέωσης. Η ανάγκη ασφαλούς αποθήκευσης οδήγησε στην ίδρυση χρηματοπιστωτικών ιδρυμάτων και στην εποχή πια της κεφαλαιοκρατικής παραγωγής, η ανάπτυξη του εμπορίου εμπορευμάτων συμπορεύεται με την ανάπτυξη του εμπορίου χρήματος. Το χρήμα, μέσω του τόκου, μετατρέπεται σε κεφάλαιο, αποκτά την ιδιότητα να παράγει πρόσθετη αξία από αυτή που ήδη περιέχει.

Τα προϊόντα του χρηματοπιστωτικού συστήματος άλλαξαν γρήγορα τον τρόπο πραγματοποίησης των συναλλαγών. Η Diner's Club ήταν η πρώτη πιστωτική κάρτα που εκδόθηκε στις ΗΠΑ και διαφημίστηκε ως το εισιτήριο για νέο, μοντέρνο τρόπο ζωής. Μέχρι το τέλος του 1970 ήταν πια διαδεδομένη στα περισσότερα νοικοκυριά των ΗΠΑ. Με την γρήγορη εξέλιξη της τεχνολογίας και την ευρύτητα της χρήσης του Διαδικτύου, γενήθηκε η ιδέα του ψηφιακού συναλλάγματος. Το ψηφιακό χρήμα βασίζεται στις αρχές της κρυπτογραφίας και συγκεκριμένα σε blockchain αλγόριθμους.

1.1 Η ΙΔΕΑ ΤΟΥ BLOCKCHAIN

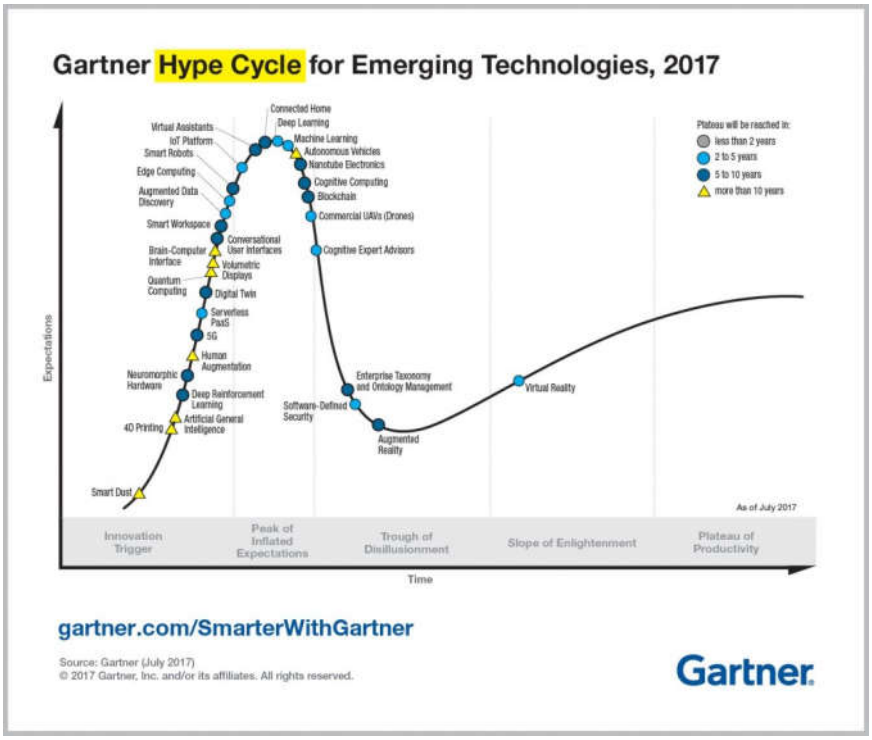
Το Blockchain αποτελεί έναν κατανεμημένο κατάλογο δεδομένων (distributed ledger), είτε δημόσιο είτε ιδιωτικό, όπου συναλλαγές ή δεδομένα διασυνδέονται με αποκεντρωμένο τρόπο σε αλληλοσυνδεόμενα μπλοκ δεδομένων. Κάθε μπλόκ, περιέχει τον αλγόριθμο κρυπτογράφησης SHA-256 (secure hash algorithm), ο οποίος κρυπτογραφεί και κατακερματίζει το περιεχόμενο του μπλοκ με μονόδρομη κρυπτογράφηση, καθιστώντας αδύνατη την αντιστροφή της διαδικασίας (one way encryption). Κάθε συναλλαγή επικυρώνεται από τους χρήστες και από την στιγμή που θα εισαχθούν, οι πληροφορίες δεν μπορούν να μεταβληθούν. Τα αντίγραφα αυτών των συναλλαγών διαμοιράζονται στους υπολογιστές όλων των χρηστών και ανανεώνονται αυτόματα με κάθε συναλλαγή. Με το διαμοιρασμό της αλυσίδας σε ένα δίκτυο peer to peer, μπορεί να λειτουργεί ως ένα σύστημα πληρωμών. Να αποτελεί δηλαδή ψηφιακό νόμισμα ανοιχτού κώδικα το οποίο χρησιμοποιεί μεθόδους κρυπτογραφίας.

Η πρώτη ιστορικά εφαρμογή της τεχνολογίας blockchain ήταν το ψηφιακό νόμισμα Bitcoin. Η ιδέα γύρω από το ψηφιακό νόμισμα, ήταν η δημιουργία μιας κοινότητας στην οποία μέσω ενός υπολογιστικού δικτύου θα εκτελούνται χρηματοοικονομικές συναλλαγές με μαθηματικώς αποδεδειγμένη ασφάλεια , ενώ ταυτόχρονα να μην υπάρχει κεντρική εξουσία που να μπορεί να επέμβει με οποιοδήποτε τρόπο στους κανονισμούς που διέπουν την πραγματοποίηση αυτών των συναλλαγών. Αυτοί οι κανονισμοί, σχεδιάστηκαν από τον προγραμματιστή ή ομάδα προγραμματιστών του συγκεκριμένου πρωτοκόλλου, ονόματι Σατόσι Νακαμότο, και αποτελούν το πρωτόκολλο συναίνεσης του Bitcoin, το οποίο χρησιμοποιεί έναν αλγόριθμο απόδειξης μόχθου. Σήμερα χρησιμοποιούνται και άλλοι αλγόριθμοι όπως ο αλγόριθμος απόδειξης μερισμάτων στο ψηφιακό νόμισμα Ethereum.

Το ψηφιακό νόμισμα δεν είναι καινούρια ιδέα. Ήδη για τις συναλλαγές που πραγματοποιούνται στην πραγματική οικονομία γνωρίζουμε πως μόνο ένα μικρό ποσοστό των χρημάτων σε κυκλοφορία υπάρχει σε φυσική μορφή. Οι συναλλαγές κατά βάση αποτελούνται από μεταβαλλόμενα δεδομένα που αποθηκεύονται σε server τραπεζικών ιδρυμάτων.

Η ειδοποιός διαφορά στην περίπτωση των κρυπτονομισμάτων είναι το γεγονός ότι στη διαδικασία της παραγωγής και της εκτέλεσης των συναλλαγών καμία κυβέρνηση και καμία τράπεζα δεν μπορεί να επέμβει. Οι συναλλαγές δεν ελέγχονται, προς το παρόν τουλάχιστον, από καμία υπηρεσία. Δεν υφίστανται εγκαταστάσεις κεντρικών server μέσω των οποίων να ελέγχεται το νόμισμα.

Νέα τεχνολογικά επιτεύγματα που απορρέουν από το blockchain, συμβάλλουν στη μεταβολή του τρόπου οργάνωσης και λειτουργίας της οικονομίας καθώς δημιουργείται το πλαίσιο μεταβολής της έννοιας της εμπιστοσύνης. Οι μέχρι σήμερα παραδοσιακές "έμπιστες οντότητες" (trusted authorities), οι συναλλαγές και οι ηλεκτρονικές υπηρεσίες είναι δυνητικά υποκείμενα μεταβολλών, αφού η τεχνολογία blockchain, προβλέπεται να λειτουργήσει ως μέσον αντικατάστασης της εμπιστοσύνης που μέχρι πρότινος βασίζονταν σε συμβατικές σχέσεις. Η εμπιστοσύνη αυτή, θα δημιουργείται πια λόγω του κατανεμημένου και ασφαλούς τρόπου αποθήκευσης, διαχείρισης, ανταλλαγής δεδομένων και πραγματοποίησης ηλεκτρονικών συναλλαγών. Η είσοδος της τεχνολογίας blockchain, δημιουργεί προυποθέσεις μεταβολής σε όλα τα οικονομικά και επιχειρησιακά μοντέλα που χρησιμοποιούμε στην καθημερινότητα. Σύμφωνα με την Gartner, η επιχειρηματική αξία του Blockchain θα φτάσει τα 176$ δισεκατομύρια μέχρι το 2025 [1], αφού μπορεί να χρησιμοποιηθεί σε μεγάλο φάσμα δραστηριοτήτων, από την οικονομία, το περιβάλλον, την υγεία και αλλού.



ΕΙΚΟΝΑ 2 - (ΠΗΓΗ: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/)

Το blockchain μας φέρνει πιο κοντά στο μέλλον, με τη δυνατότητα χρήσης του σε απεριόριστες εφαρμογές όπως αποθήκευση και επαλήθευση νομικών εγγράφων, πράξεων και πιστοποιητικών, δεδομένων υγειονομικής περίθαλψης, IoT (Internet of Things). Η τεχνολογία Blockchain έχει έξι κύρια χαρακτηριστικά: αποκέντρωση, σταθερότητα, διαφάνεια, αποτελεσματικότητα, ασφάλεια και ανωνυμία.[2]

Μπορεί να χρησιμοποιηθεί σε κλάδους όπως:

Υγειονομική Περίθαλψη: Το blockchain είναι κατάλληλο για εφαρμογές όπου οι ενδιαφερόμενοι βιοϊατρικοί / πάροχοι υγειονομικής περίθαλψης / ασθενείς / νοσοκομεία / επενδυτές, επιθυμούν να συνεργαστούν μεταξύ τους χωρίς να παραχωρήσουν τον έλεγχο σε έναν κεντρικό διαχειριστή. Αποτελεί ένα αμετάβλητο καθολικό όπου καταγράφονται ευαίσθητες πληροφορίες, ενώ η προέλευση των δεδομένων είναι ανιχνεύσιμη και άρα μπορούν να επαληθευτούν. Ένα χαρακτηριστικό παράδειγμα είναι οι ιατρικοί φάκελοι, τα αρχεία συγκατάθεσης ασθενών, και άλλα αρχεία που εμπεριέχουν ευαίσθητες πληροφορίες και κρίνεται απαραίτητη η προστασία του περιεχομένου τους. Πολλές μελέτες ή έργα που βρίσκονται σε εξέλιξη επικεντρώνονται στην ανταλλαγή δεδομένων περίθαλψης ασθενών χρησιμοποιώντας blockchain για τη βελτίωση της διαχείρισης ιατρικών αρχείων. [3]

Αγροτική Παραγωγή: Τα παραδοσιακά λογιστικά συστήματα που χρησιμοποιούνται στην προμήθεια τροφίμων και στη γεωργία αποθηκεύουν απλώς τις παραγγελίες και τις παραδίδουν στον προορισμό. Αυτά τα συμβατικά συστήματα υπολείπονται σε διάφορα χαρακτηριστικά όπως η δυνατότητα ελέγχου, η ιχνηλάτηση και η διαφάνεια. Αυτά τα χαρακτηριστικά μπορούν να βελτιώσουν την ασφάλεια και την ποιότητα των τροφίμων, και εφόσον υπάρχει τεράστια ζήτηση καλής ποιότητας τροφίμων από τους καταναλωτές, οι περισσότεροι οργανισμοί έρευνας και ανάπτυξης υιοθετούν τεχνολογίες IoT όπως για παράδειγμα ασύρματα δίκτυα αισθητήρων και αναγνώριση ραδιοσυχνοτήτων, τα οποία επιβλέπουν εξ αποστάσεως την αλυσίδα εφοδιασμού τροφίμων.

Βιομηχανική Παραγωγή: Η τεχνολογία Blockchain μπορεί να μειώσει δραστικά τη χειρωνακτική εργασία και με τη χρήση έξυπνων συμβολαίων να ψηφιοποιήσει διαδικασίες που βασίζονται σε μεγάλο βαθμό σε γραφειοκρατική εργασία. Έτσι βελτιώνεται η αποδοτικότητα και αποτελεσματικότητα της εφοδιαστικής αλυσίδας και μειώνονται σημαντικά λειτουργικοί κίνδυνοι. Ένας συνδυασμός συνδεδεμένων μηχανών και συσκευών στη βιομηχανία, σε διάφορα συστήματα παραγωγής, μπορεί να εκτοξεύσει την παραγωγή αλλά αστοχίες σε μια βιομηχανική μονάδα μπορεί να απειλήσουν ακόμα και τη ζωή των εργαζόμενων. Τέτοιες αστοχίες και λάθη μπορούν να αποφευχθούν μέσω ενός ασφαλούς και αξιόπιστου έξυπνου εργασιακού περιβάλλοντος. Το IoIT (Internet of Industrial Things) περιβάλλον αποτελείται από έξυπνες συσκευές IoT, κόμβους πύλης, και διάφορους τύπους διακομιστών. Οι πλούσιες σε πόρους συσκευές, όπως οι διακομιστές, μπορούν να δημιουργούν προβλέψεις για ορισμένα φαινόμενα (π.χ. πιθανότητες πυρκαγιάς μέσα σε ένα εργοστάσιο). Η χρήση blockchain σε ένα τέτοιο περιβάλλον, μπορεί να εγγυηθεί ασφάλεια και αξιοπιστία των δεδομένων. [8]

Ενέργεια: Καθώς οι πόροι πετρελαίου και φυσικού αερίου διαδραματίζουν ακόμα ουσιαστικό ρόλο στο ενεργειακό πεδίο, οι τεχνολογίες της βιομηχανίας πετρελαίου και φυσικού αερίου έχουν αναπτυχθεί γρήγορα τα τελευταία χρόνια, όπως η τεχνολογία έξυπνης διάτρησης, ευφυή πεδία πετρελαίου και φυσικού αερίου και θαλάσσιες ψηφιακές πλατφόρμες. [4] Σύμφωνα με τις εκθέσεις [5], [6] που εκδόθηκαν από την Deloitte τον Απρίλιο 2017, το blockchain έχει μεγάλες δυνατότητες στη βιομηχανία πετρελαίου και φυσικού αερίου κυρίως στις ακόλουθες τέσσερις πτυχές: εμπορία, διαχείριση και λήψη αποφάσεων, επίβλεψη και cyber security. Είναι ευρύ το πεδίο εφαρμογής όχι μόνο στον τομέα συμβατικών πια μορφών ενέργειας, αλλά και σε λύσεις στο πεδίο της πράσινης ενέργειας, όπως για παράδειγμα η χρήση της τεχνολογίας blockchain σε αισθητήρες για τον έλεγχο και την προσαρμογή της απόδοσης ανεμογεννητριών με σκοπό την εξοικονόμηση πόρων.

Τράπεζες: Η χρήση blockchain, αδιαμφισβήτητα θα μειώσει το κόστος, όσον αφορά την διατήρηση και την ασφάλεια των δεδομένων. Οι συναλλαγές θα είναι περισσότερο διαφανείς, θα διεξάγονται αποτελεσματικότερα. Αν και προς το παρόν το επίκεντρο βρίσκεται στην καινοτομία σχετικά με συστήματα πληρωμών, παίρνοντας υπόψιν την άνοδο του FINTECH και στην Ελλάδα, [9] η ενσωμάτωση της τεχνολογίας blockchain θα ήταν μελλοντικά πραγματική αποκάλυψη στον τομέα τραπεζικών υπηρεσιών.

Μεταφορές: Ένα έξυπνο σύστημα μεταφοράς αποτελείται ενδεχομένως από αυτοκινούμενα οχήματα (π.χ. αυτοκίνητο), μονάδες και διακομιστές cloud / fog. Αυτές οι συσκευές μπορούν να επικοινωνούν μεταξύ τους χρησιμοποιώντας το Διαδίκτυο, μέσω ενός εκτεταμένου δικτύου πολλαπλών αισθητήρων, κεραιών, με ενσωματωμένο λογισμικό και τεχνολογιών που βοηθούν στην πλοήγηση μιας σύνθετης διαδρομής. Οι έξυπνες μονάδες του συστήματος θα πρέπει να παίρνουν αποφάσεις με ταχύτητα, συνέπεια και ακρίβεια. Αυτή η τεχνολογία μπορεί να παρέχει ένα άνετο και ασφαλές ταξίδι στους επιβάτες, είναι όμως και ευάλωτη σε πολλούς τύπους επιθέσεων. Η χρήση της τεχνολογίας blockchain σε ένα έξυπνο σύστημα μεταφοράς λοιπόν, καθιστά τις μεταφορές πιο αξιόπιστες και ασφαλείς από εξωτερικές και εσωτερικές απειλές.

Στρατιωτικές Επιχειρήσεις: Το Διαδίκτυο του Intelligent Battlefield είναι ένα περιβάλλον πεδίων μάχης που αποτελούνται από έξυπνες συσκευές, όπως drones (μη επανδρωμένα εναέρια οχήματα), ρομπότ και wearable, φορητές συσκευές και όπλα για στρατιώτες. Αυτές οι συσκευές χαρτογραφούν το περιβάλλον τους και στέλνουν τα αντίστοιχα δεδομένα στο σταθμό βάσης (σύστημα ελέγχου). Έχουν επίσης ένα ενσωματωμένο συστατικό τεχνητής νοημοσύνης και βάσει αυτού του στοιχείου, οι συσκευές μπορούν να ενεργούν αυτόματα (για παράδειγμα, παρακολούθηση στόχων και αντίποινα μέσω drone). Ωστόσο, τέτοια είδη επικοινωνιακών περιβαλλόντων υποφέρουν από άποψη ασφάλειας και απορρήτου. Είναι δυνατές διάφορες επιθέσεις όπως η πλαστοπροσωπία, η διαρροή εμπιστευτικών πληροφοριών, κωδικών πρόσβασης, η διαρροή και τροποποίηση δεδομένων. Το blockchain μπορεί να παρέχει ασφάλεια σε διαφορετικούς τύπους και περιβάλλοντα Internet of Things. Με δισεκατομμύρια συνδεδεμένες συσκευές, η ανησυχία έγκειται στο κατά πόσο οι κατανεμημένες πληροφορίες είναι ασφαλείς. Επομένως, το blockchain είναι μηχανισμός που μπορεί να χρησιμοποιηθεί για την ασφάλεια στο Διαδίκτυο των Ευφυών πεδίων μάχης. [7]

Τα παραπάνω αποτελούν μερικά μόνο ενδεικτικά παραδείγματα δυνατοτήτων που προκύπτουν για την εξέλιξης της κοινωνίας και τη βελτίωση της ποιότητας ζωής με τη χρήση της τεχνολογίας blockchain.

1.2 Η ΙΣΤΟΡΙΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ

Το 1985, ο κρυπτογράφος David Chaum, δημοσίευσε το άρθρο "Security without identification- transaction system to make big brother obsolete". Στη δημοσίευση αναφέρεται για πρώτη φορά η **δημιουργία νομισμάτων με τη βοήθεια της κρυπτογραφίας**. Υπογραμμίζει πως βάσει της αρχιτεκτονικής που θα επιλέγεται για τα επικείμενα αυτοματοποιημένα συστήματα συναλλαγών μεγάλης κλίμακας, αυτά τα συστήματα μπορεί να έχουν μακροπρόθεσμο αντίκτυπο στο οικονομικό σύστημα, σε ορισμένες από τις βασικές ελευθερίες, και ακόμη και για τη δημοκρατία. Η νέα αυτή προσέγγιση θα μπορούσε να προσφέρει στα άτομα και σε μικρούς οργανισμούς την ίδια πρόσβαση σε υπηρεσίες που απολαμβάνουν οι μεγάλοι οργανισμοί. [10] Στις αρχές της δεκαετίας του 1990, δημιουργήθηκε μια λίστα αλληλογραφίας, με αντικείμενο τη μελέτη και τις συζητήσεις γύρω από την κρυπτογραφία μέσω υπολογιστή. Η λίστα αυτή, έφερε την κωδική ονομασία "Cypherpunks". Πολλές ιδέες κεντρικές για το Bitcoin αναπτύχθηκαν σε συτή τη διαδικτυακή κοινότητα, μια χαλαρά οργανωμένη ομάδα ακτιβιστών ψηφιακού απορρήτου. Στο πλαίσιο της "αποστολής" τους, προσπάθησαν να δημιουργήσουν ψηφιακό χρήμα που θα ήταν τόσο ανώνυμο όσο και τα φυσικά μετρητά. Διάφορα πειράματα σε ψηφιακά μετρητά κυκλοφόρησαν στις λίστες Cypherpunk τη δεκαετία του 1990. Ο Adam Back, ένας Βρετανός ερευνητής, δημιούργησε ένα που ονομάζεται **hashcash** που αργότερα έγινε κεντρικό συστατικό του Bitcoin. Αυτή η μέθοδος αποτελεί βασικό στοιχείο για τη δημιουργία κρυπτονομισμάτων, αλλά έχει επίσης εφαρμοστεί σε άλλους τομείς, όπως στην καταπολέμηση των ανεπιθύμητων e-mails (spam). {11]

Μια άλλη προσέγγιση στο ψηφιακό χρήμα, που ονομάστηκε b money, σχεδιάστηκε από έναν μηχανικό λογισμικού υπολογιστών, τον Wei Dai. Το 1998, στην ίδια λίστα "cypherpunks", δημοσίευσε μια πρόταση για ένα ανώνυμο, κατανεμημένο σύστημα ηλεκτρονικών χρημάτων, στην οποία ανέφερε το hashcash ως μία μέθοδο για τη δημιουργία κρυπτονομισμάτων. Όταν αυτά τα πειράματα απέτυχαν να απογειωθούν, πολλοί Cypherpunks έχασαν το ενδιαφέρον τους. Ο Nick Szabo, όμως, ακαδημαικός στο χώρο της πληροφορικής, εργάστηκε για έξι μήνες ως σύμβουλος για την εταιρεία DigiCash. Το 1998, έστειλε το περίγραμμα για τη δική του έκδοση του ψηφιακού χρήματος, το οποίο ονόμασε bit gold, σε μια μικρή ομάδα που εξακολουθούσε να παρακολουθεί τις εξελίξεις σχετικά με το ψηφιακό χρήμα, συμπεριλαμβανομένων των κυρίων Dai και Hal Finney, ενός προγραμματιστή στη Santa Barbara, που προσπάθησε να κατασκευάσει μια λειτουργική εκδοχή του bit gold.

Το Δεκέμβρη του 2005, ο Nick Szabo, δημοσίευσε στο προσωπικό του blog την πρόταση για το bitGOLD, στην οποία έκανε τροποποιήσεις έως και το Δεκέμβριο του 2008. "Τα χρήματά μας εξαρτώνται επί του παρόντος από την εμπιστοσύνη σε κάποιο τρίτο μέρος ως προς την αξία τους. Όπως έδειξαν πολλά πληθωριστικά και υπερπληθωριστικά επεισόδια κατά τον 20ο αιώνα, αυτό δεν είναι μια ιδανική κατάσταση. Παρομοίως, η έκδοση τραπεζογραμματίων ιδιωτικών τραπεζών, ενώ είχε διάφορα πλεονεκτήματα, εξαρτάται επίσης από ένα αξιόπιστο τρίτο μέρος. Τα πολύτιμα μέταλλα και άλλα συλλεκτικά αντικείμενα βρίσκονται σε έλλειψη λόγω της δαπανηρής δημιουργίας τους. Κάποτε η αξία αυτή παρείχε στα χρήματα την αξία τους, η οποία ήταν σε μεγάλο βαθμό ανεξάρτητη από οποιοδήποτε αξιόπιστο τρίτο μέρος. Ωστόσο, τα πολύτιμα μέταλλα έχουν προβλήματα. Είναι πολύ δαπανηρό να χρησιμοποιούνται μέταλλα επανειλημμένα για κοινές συναλλαγές. Έτσι, ένα αξιόπιστο τρίτο μέρος (συνήθως συνδεδεμένο με έναν φορολογούμενο που αποδέχθηκε τα κέρματα ως πληρωμή) κλήθηκε να σφραγίσει ένα τυπικό ποσό του μετάλλου σε ένα κέρμα. Επίσης είναι αδύνατη η χρήση πολύτιμων μετάλλων για online συναλλαγές. Έτσι, θα ήταν πολύ ωραίο εάν υπήρχε ένα πρωτόκολλο με το οποίο θα μπορούσαν να δημιουργηθούν ασυνήθιστα πολύτιμα κομμάτια στο διαδίκτυο με ελάχιστη εξάρτηση από αξιόπιστα τρίτα μέρη, και στη συνέχεια να αποθηκεύονται με ασφάλεια, να μεταφέρονται και να διακινούνται με αμοιβαία εμπιστοσύνη." [12]

Η πρόταση, λοιπόν του Szabo, ήταν το bitGOLD. Ένα συλλεκτικό είδος που, σε αντίθεση με τον χρυσό, θα μπορούσε να παραχθεί εύκολα από οποιονδήποτε, αλλά θα ήταν διαθέσιμο σε περιορισμένες ποσότητες, ώστε να διατηρεί την αξία του και να μην επηρεάζεται από τον πληθωρισμό. Και οι δυο ιδέες, του bitGOLD αλλά και του b-money, παρέμειναν καθαρά σε θεωρητικό επίπεδο.

Το 2008 όμως, εμφανίστηκε μια δημοσίευση, βασιζόμενη στα hashcash, b-money και bitGOLD, υπό το ψευδώνυμο Satoshi Nakamoto, με τίτλο: "Bitcoin:A Peer-to-Peer Electronic Cash System". [13] Μέχρι και σήμερα παραμένει μυστήριο η πραγματική ταυτότητα του Satoshi Nakamoto, αν πρόκειται για άτομο ή ομάδα ατόμων. Παρόλα αυτά, η οντότητα Satoshi Nakamoto έως και την άνοιξη του 2012, έδινε αρκετά τακτικά το παρόν σε φόρουμ σχετικά με το bitcoin, δίνοντας διευκρινίσεις. Αρκετοί δημοσιογράφοι ασχολήθηκαν με την ταυτοποίηση αυτής της οντότητας, με αρκετούς υποψήφιους, μεταξύ των οποίων και ο Nick Szabo. Παρότι διενεργήθηκαν πολλές δημοσιογραφικές έρευνες, η ταυτότητα του δημιουργού παραμένει αίνιγμα.

Στις αρχές του 2009, κυκλοφόρησαν τα πρώτα bitcoin. Το σύστημα βασιζόταν σε λογισμικό ανοιχτού κώδικα **(open source protocol)**, που σημαίνει ότι οποιοσδήποτε προγραμματιστής μπορούσε να εξετάσει ακριβώς πώς λειτουργεί. Ο πηγαίος κώδικας ήταν δημόσιος και διαθέσιμος για μελέτη από όποιον το επιθυμούσε. Αυτή η αρχή επιτρέπει στον καθένα την ελεύθερη και δωρεάν αντιγραφή ή ανάπτυξη δικού του λογισμικού, βασισμένου στο υπάρχον. Στις 3 Ιανουαρίου 2009, δημιουργήθηκε επίσημα η έννοια της εξόρυξης (**mining**) και του **Μπλοκ Μηδέν (Block 0 / the genesis block)**, το οποίο ήταν απαραίτητο για τη λειτουργία του Bitcoin. Ένα ηλεκτρονικό νόμισμα μπορούμε να το περιγράψουμε ως μια αλυσίδα ψηφιακών υπογραφών, όπου η μεταφορά του νομίσματος ή κλασμάτων του, πραγματοποιείται υπογράφοντας ψηφιακά ένα κατακερματισμένο κομμάτι (hash) της προηγούμενης συναλλαγής, μαζί με το κρυπτογραφημένο δημόσιο κλειδί του επόμενου κατόχου. Ο παραλήπτης, δεν μπορεί ακόμα να επαληθεύσει ότι ο προηγούμενος κάτοχος αυτού του νομίσματος δεν ξόδεψε το ίδιο νόμισμα πολλές φορές, όπως εγγυάται η παραδοσιακή ανταλλαγή χρημάτων σε φυσική μορφή. Ο Satoshi, προκειμένου να διασφαλιστεί ότι δεν θα πραγματοποιούνται διπλές δαπάνες μέσω της δημοσιοποίησης όλων των συναλλαγών, εισάγει τη χρονική σήμανση ως κρίσιμο στοιχείο. Με βάση το πότε συνέβη η συναλλαγή, μια δεύτερη συναλλαγή θα πρέπει να απορρίπτεται, με βάση τη χρονική σήμανσή της, η οποία πρέπει να δηλώνει με σαφήνεια ότι συνέβη μετά την πρώτη. Ο διακομιστής χρονικής σήμανσης (**timestamp server**) εκπέμπει ένα hash, στο οποίο αποθηκεύονται τα προηγούμενα αρχεία συναλλαγών. Με τη δημόσια μετάδοση αυτού του hash, η χρονική σήμανση που δημιουργείται από αυτήν τη δημόσια ανακοίνωση λειτουργεί ως απόδειξη για τη χρονική εκτέλεση των συναλλαγών. Κάθε νέο hash περιλαμβάνει το προηγούμενο hash μαζί με ένα νέο μπλοκ δεδομένων, σχηματίζοντας μια αλυσίδα όπου κάθε επόμενη χρονική σήμανση ενισχύει την εγκυρότητα των συναλλαγών πριν από αυτό.

Η εφαρμογή αυτού του διακομιστή χρονικής σήμανσης, πραγματοποιείται μέσω ενός **μηχανισμού απόδειξης εργασίας, (proof of work)**. Παρόμοια με το Hashcash του Adam Back, η απόδειξη περιλαμβάνει σάρωση για μια τιμή η οποία όταν κατακερματίζεται, ξεκινά με έναν συγκεκριμένο αριθμό μηδενικών bits. Η εργασία που απαιτείται για να επιτευχθεί αυτό, αυξάνεται εκθετικά με τον επιθυμητό αριθμό μηδενικών και μπορεί να επαληθευτεί σε μία μόνο διαδικασία κατακερματισμού. Η απόδειξη εργασίας αποσκοπεί στο να δώσει σε κάθε CPU στο δίκτυο μία ψήφο, όπου αντικείμενο ψηφοφορίας είναι η εγκυρότητα και η ισχύς των συναλλαγών. Η πλειοψηφική απόφαση αντιπροσωπεύεται από τη μεγαλύτερη αλυσίδα, η οποία εμπεριέχει το μεγαλύτερο "μόχθο" για την απόδειξη της εργασίας. Εάν η πλειοψηφία της CPU είναι ελεγχόμενη από έγκυρους κόμβους, η αλυσίδα αυτή θα αναπτυχθεί ταχύτερα και θα ξεπερνά άλλες αλυσίδες. Ο Satoshi υπογραμμίζει τους έγκυρους κόμβους, αφού ένας μη έγκυρος κόμβος θα μπορούσε να είναι πιθανός εισβολέας στο δίκτυο κρυπτογράφησης. Από τους μηχανισμούς που περιγράφονται, ο πιθανός εισβολέας θα πρέπει να επαναλάβει την απόδειξη όλων των μπλοκ σε μια συγκεκριμένη αλυσίδα ώστε να ξεπεράσει την αλυσίδα των έγκυρων κόμβων.

Μέσω μαθηματικών υπολογισμών των πιθανοτήτων, όπως αναλύονται στην ενότητα 11 της δημοσίευσης, [13] ο Satoshi απέδειξε ότι αυτό είναι εξαιρετικά απίθανο, με την πιθανότητα να υπολογίζεται μικρότερη του 0.1%. Η απόδειξη της εργασίας αποδεικνύεται απαραίτητη. Εάν δημιουργούνται μπλοκ πολύ γρήγορα, τότε η δυσκολία εξόρυξης αυξάνεται αυτόματα. Ο στόχος σχετικά με το χρόνο εξόρυξης ανά μπλοκ είναι τα δέκα λεπτά.

Στην ενότητα 5, περιγράφεται αναλυτικά το πώς επιτυγχάνεται η έγκριση από το δίκτυο.

1) Οι νέες συναλλαγές μεταδίδονται σε όλους τους κόμβους.

2) Κάθε κόμβος συλλέγει τις νέες συναλλαγές σε ένα μπλοκ.

3) Κάθε κόμβος εργάζεται για την εύρεση μιας δύσκολης απόδειξης εργασίας (proof of work) για το μπλοκ του.

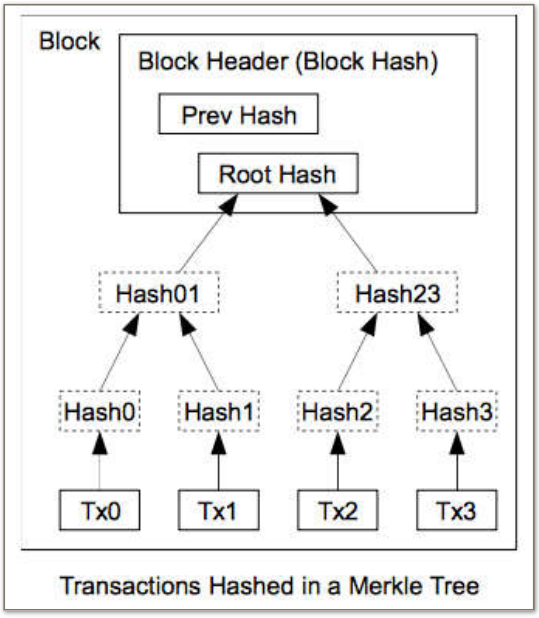
4) Όταν ένας κόμβος βρίσκει μια απόδειξη εργασίας, μεταδίδει το μπλοκ σε όλους τους κόμβους.

5) Οι κόμβοι δέχονται το μπλοκ μόνο εάν όλες οι συναλλαγές σε αυτό είναι έγκυρες και δεν έχει ήδη πραγματοποιηθεί συναλλαγή με την αξία που εμπεριέχει.

6) Οι κόμβοι εκφράζουν την αποδοχή του μπλοκ, δουλεύοντας για τη δημιουργία του επόμενου μπλοκ στην αλυσίδα, και χρησιμοποιώντας το hash του αποδεκτού μπλοκ όπως το hash του προηγούμενου μπλοκ. Η μεγαλύτερη αλυσίδα θεωρείται πάντα η σωστή και σε περίπτωση πολλαπλών αλυσίδων, συγκρίνονται οι αλυσίδες ίδιου μήκους και γίνεται αποδεκτή η πρώτη χρονικά που λήφθηκε, ενώ η δεύτερη διατηρείται σε περίπτωση που ήταν στην πραγματικότητα η σωστή. Όταν ένα νέο μπλοκ εγκριθεί σε μία από τις αλυσίδες, τότε ο δεσμός αυτός σπάει και η μικρότερη αλυσίδα εγκαταλείπεται. Το Bitcoin έχει δύο κύριες πηγές για κίνητρα εξόρυξης. Το πρώτο είναι προφανές, και είναι το στοιχείο του κέρδους μέσω της συναλλαγής. Για κάθε συναλλαγή που αποστέλλεται σε bitcoin, αυτό που αποστέλλεται είναι πάντα περισσότερο από αυτό που λαμβάνεται από τον καθορισμένο δέκτη, και η διαφορά αφήνεται στους "ανθρακωρύχους" ως επιβράβευση συναλλαγής. Η πρώτη έκδοση για υπολογιστές περιλάμβανε ένα σύστημα παραγωγής Bitcoin που προέβλεπε τη δημιουργία ενός συνολικού αριθμού 21 εκατομμυρίων Bitcoins μέχρι το έτος 2040.. Έως ότου εξορυχθούν και τα 21 εκατομμύρια νομίσματα, κάθε νέο μπλοκ έχει μια ανταμοιβή σε νόμισμα που σχετίζεται με αυτό. Αυτή η επιβράβευση μειώνεται στο μισό κάθε 210.000 μπλοκ. Το μπλοκ γένεσης είχε μια ανταμοιβή 50 νομισμάτων, και έχει ήδη μειωθεί στο ήμισυ δύο φορές η ανταμοιβή κέρματος ανά μπλοκ, από 12,5 σε 6,25 νομίσματα το 2020.

Με δεδομένο ότι το μέγεθος μιας αλυσίδας που περιέχει για παράδειγμα ένα εκατομμύριο μπλοκ είναι πάνω από 200 GB δεδομένων, ο δημιουργός προβλέπει (ενότητα 7, [13]), πώς ορισμένα στοιχεία της αλυσίδας μπορούν να "κλαδευτούν" με την πάροδο του χρόνου ώστε να μειώνεται το μέγεθος της αλυσίδας που μεταδίδεται στους διάφορους κόμβους bitcoin. Οι συναλλαγές που έχουν επαληθευτεί και "θάβονται" κάτω από άλλα αποδεκτά μπλοκ μπορούν "κλαδεύονται" χωρίς να σπάει η δομή της αλυσίδας. Χρησιμοποιώντας ένα δέντρο Merkle, η αλυσίδα μπορεί να συμπιεστεί, που σημαίνει πως ένας κόμβος δε χρειάζεται να αποθηκεύει όλο το blockchain.

Με αυτό τον τρόπο, μπορεί να "τρέξει" καταλαμβάνοντας πολύ λιγότερα gigabytes χώρου.



ΕΙΚΟΝΑ 3 - Merkle Tree : Πραγματοποιείται μια συναλλαγή όπου στέλνεται το νόμισμα T από τον αποστολέα A στον παραλήπτη B. Αυτή η συναλλαγή H, υποβάλεται σε κατακερματισμό, με θέση φύλλου κόμβου (leaf node position) = T. Οι ανθρακωρύχοι περιλαμβάνουν το hash (H) στο μπλοκ = Q. Παράγεται μια ντετερμινιστική υπογραφή των ακόλουθων συνδυασμένων στοιχείων: hash συναλλαγής, token_id, Merkle Root από το Block Q. Αυτή η υπογραφή κατακερματίζεται και ο αποστολέας έχει πλέον απόδειξη συναλλαγής. Ο δέκτης επαληθεύει όλα τα hash και τη μη συμμετοχή σε προηγούμενα μπλοκ. Ο αποστολέας έχει ήδη στείλει κάθε αναδρομική ψηφιακή υπογραφή για όλα τα προηγούμενα μπλοκ <Q + 1. Ο δέκτης επαληθεύει αυτές τις υπογραφές.

Στις 12 Ιανουαρίου, πραγματοποιήθηκε η πρώτη συναλλαγή στο μπλοκ 170 μεταξύ του Nakamoto και του Hal Finney. Στις 5 Οκτωβρίου, η συναλλαγματική ισοτιμία που καθόριζε την αξία ενός Bitcoin ήταν $1 = 1,309.03 BTC, υπολογισμένη με βάση το κόστος ηλεκτρικής ενέργειας που απαιτείται για την εξόρυξή του. Στις 16 Δεκεμβρίου, κυκλοφόρησε η δεύτερη έκδοση του λογισμικού για τη δημιουργία Bitcoin. Στις 6 Φεβρουαρίου 2010, ιδρύθηκε η ιστοσελίδα «Bitcoin Market», που επέτρεπε στους χρήστες να ανταλλάσσουν δολάρια με Bitcoin. Στις 22 Μαΐου, πραγματοποιήθηκε η πρώτη πραγματική συναλλαγή, όταν ένας προγραμματιστής από τη Φλόριντα πρόσφερε 10,000 BTC για μια πίτσα στον Laszlo Hanyecz μέσω του φόρουμ «Bitcoin Forum», με αξία 25$ για τα 10,000 BTC. Στις 7 Ιουλίου, κυκλοφόρησε η τρίτη έκδοση του λογισμικού για τη δημιουργία Bitcoin, η οποία οδήγησε σε σημαντική αύξηση των χρηστών. Από τις 12 Ιουλίου, για 5 ημέρες, η αξία του Bitcoin αυξήθηκε 10 φορές, από US$0.008/BTC σε US$0.080/BTC.

Η δεύτερη στοσελίδα, «MtGox Bitcoin» για ανταλλαγή δολαρίων σε Bitcoins, εξελίχθηκε στη μεγαλύτερη και πιο δημοφιλή αγορά συναλλάγματος για το Bitcoin. [14] Στις 15 Αυγούστου είχαν δημιουργηθεί περίπου 184 δισεκατομμύρια Bitcoins. Στις 4 Οκτωβρίου, κυκλοφόρησε η πρώτη wikipage με αναφορά στο Bitcoin, ανακοινώνοντας τον πρώτο client ανοιχτού κώδικα και τη δημιουργία των αντίστοιχων Bitcoins. Επίσης, η Διακυβερνητική Ομάδα Χρηματοπιστωτικής Δράσης (Intergovernmental Financial Action Task Force) δημοσίευσε έγγραφο που προειδοποιούσε ότι τα ψηφιακά νομίσματα θα μπορούσαν να χρησιμοποιηθούν από τρομοκρατικές ομάδες για χρηματοδότηση. Τον Απρίλιο του 2010 ξεκίνησαν οι πρώτες συναλλαγές στις χρηματαγορές, με την αξία του κάθε Bitcoin να κυμαίνεται στα US$ 0,14 δολάρια. Την άνοιξη του 2011, τα 10.000 εκείνα Bitcoin που είχαν προσφερθεί τότε έφτασαν να αξίζουν 272,329 δολάρια. Τον Ιούνιο του 2011, η αξία του Bitcoin αυξήθηκε στα 32 δολάρια, υποδεικνύοντας ότι ένα Bitcoin μπορούσε να μετατραπεί σε 32 αμερικανικά δολάρια. Είναι γεγονός πως το Bitcoin μέχρι το άνοιγμα των πρώτων ανταλλακτηρίων χρησιμοποιούνταν από έναν περιορισμένο αριθμό χρηστών.

Το άνοιγμα όμως του MtGox, αλλά και άλλων ανταλλακτηρίων, όπως το Bitmarket, το Bitme, το The Rock, αποτέλεσε σημείο εκκίνησης για την ευρύτερη χρήση του Bitcoin. Στην πορεία, η αξία του Bitcoin γνώρισε μεγάλες διακυμάνσεις. Μέχρι και τον Φεβρουάριο του 2013 έφτασε το ένα Bitcoin να αξίζει 2 μόλις δολάρια,. Στις 9 Απριλίου του 2013 σημειώθηκε η πρώτη σημαντική άνοδος της τιμής, φτάνοντας για πρώτη φορά τα $238 δολάρια, τιμή που παρέμεινε σταθερήμέχρι και το Νοέμβριο του 2013.

Το Δεκέμβριο του 2013 η συναλλαγματική αξία του Bitcoin κυμαινόταν μεταξύ 1200-1400 δολαρίων ανά νόμισμα. Όμως στα μέσα του μήνα και μέσα σε λιγότερο από μία ημέρα, η τιμή του έπεσε κάτω από τα 550 δολάρια. Μεγάλες ιστοσελίδες όπως η WordPress (Νοέμβριο του 2012 - Skelton, Andy 2012), η Okcupid (Απρίλιο του 2013 - Franceschi- Bicchierai, Lorenzo 2013), η AtomicMall (Νοέμβριο του 2013), η TigerDirect (Dahlberg, Nancy 2014) και η Overstock.com (Ιανουάριο του 2014 - Vaishampayan, Saumya 2014), άρχισαν να δέχονται Bitcoins.

Τον Οκτώβριο του 2013, εγκαταστάθηκε στο Vancouver του Καναδά το πρώτο ATM για Bitcoin (McMillan, Robert 2013). Στα τέλη του Φεβρουαρίου του 2014 το μεγαλύτερο ανταλλακτήριο, το MtGox "πάγωσε" όλες τις αναλήψεις και στη συνέχεια "πάγωσε" και η δημόσια πρόσβαση στην ιστοσελίδα. Την ίδια περίοδο, διέρρευσε έγγραφο όπου γινόταν αναφορά για χρόνια κλοπή, η οποία μάλιστα δεν ανιχνεύθηκε από το ανταλλακτήριο. Στο έγγραφο αυτό, 744.408 Bitcoins, αναφέρονται ως "κλεμμένα" από το ανταλλακτήριο MtGox. Οι συνολικές οφειλές δηλώθηκαν στο ύψος των εξίμιση εκατομμυρίων Yen. Κατόπιν εκδόθηκε ανακοίνωση όπου υποψίες για κλοπή των Bitcoins καταλογίζονταν σε χάκερς. Έπειτα το ανταλλακτήριο δήλωσε πτώχευση στην Ιαπωνία, στις 28 Φεβρουαρίου του 2014. [15]

Το 2014, αναπτύχθηκε ένα mining pool, (συλλογική ομάδα από miners για την ενίσχυση της υπολογιστικής ισχύος με στόχο την εξόρυξη περισσότερων μπλοκ), το GHash.IO. Η ομάδα αυτή διαχειριζόταν σχεδόν το 50% της συνολικής υπολογιστικής ισχύος του δικτύου. Με αυτή την εξέλιξη τέθηκε υπό αμφισβήτηση η ακεραιότητα του δικτύου. Η κατοχή άνω του 50% της συνολικής ισχύος του δικτύου, σηματοδοτεί μονομερή έλεγχο της αλυσίδας των μπλοκ (blockchain) κατά το δοκούν. [16]

Το 2015, η Microsoft σχεδίαζε να λανσάρει το δικό της πρόγραμμα για το Bitcoin σε παγκόσμιο επίπεδο. Την ίδια χρονιά, η Bitstamp, μια δημοφιλής πλατφόρμα ανταλλαγής κρυπτονομισμάτων, υπέστη κυβερνοεπίθεση, με αποτέλεσμα να χάσει 5 εκατομμύρια δολάρια. Παράλληλα, οι βρετανικές τράπεζες εξέφρασαν την υποστήριξή τους προς το Bitcoin, ενώ η Ingenico, ο μεγαλύτερος ευρωπαϊκός επεξεργαστής πληρωμών, υιοθέτησε επίσης το εικονικό νόμισμα. Η πτώση της αξίας του Bitcoin κάτω από το όριο των 1.000 δολαρίων προκάλεσε πολλές συζητήσεις σχετικά με το μέλλον του, καθώς οι χρήστες και οι επενδυτές εξέταζαν τις προοπτικές του νομίσματος σε ένα συνεχώς μεταβαλλόμενο οικονομικό περιβάλλον.

Σήμερα η συναλλαγματική αξία του Bitcoin κυμαίνεται μεταξύ $50.000 και $55.000 δολαρίων. Ακολουθούν με τεράστια διαφορά τα υπόλοιπα κρυπτονομίσματα. Με βάση τα παραπάνω, μπορούμε να αναφέρουμε συνοπτικά, μερικά **βασικά στοιχεία ενός κρυπτονομίσματος.**

1) Αποτελεί ανεξάρτητο μέσο ανταλλαγής. Δεν υπόκειται σε έλεγχο από κάποια κεντρική αρχή.

2) Οι συναλλαγές πραγματοποιούνται ανώνυμα. Είναι εξαιρετικά δύσκολο, χρονοβόρο αλλά και κοστοβόρο το να εντοπιστούν οι χρήστες που πραγματοποιούν συναλλαγές.

3) Το κόστος των συναλλαγών είναι ελάχιστο. Μπορούν να πραγματοποιηθούν συναλλαγές σε όλο τον κόσμο, χωρίς την υποχρέωση καταβολής εξόδων εμβασμάτων, διατραπεζικών συναλλαγών και λοιπά.

4) Πραγματοποίηση συναλλαγών χωρίς γεωγραφικούς περιορισμούς.

1.3 ΤΑ ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ ΣΗΜΕΡΑ

Μέχρι τις αρχές του 2010, το Bitcoin δεν είχε καμία αξία. Το Μάρτιο του 2010 δημιουργήθηκε το πρώτο ανταλλακτήριο bitcoinmarket.com, το οποίο σήμερα δεν λειτουργεί. Αρχικά, η ισοτιμία του bitcoin, ήταν: 1 bitcoin = 0,003 $. Όπως αναφέρθηκε, στις 22 Μαίου 2010, ένας προγραμματιστής από τη Φλόριντα των ΗΠΑ, έκανε μια δημοσίευση στο bitcointalk.org προσφέροντας 10.000 bitcoin σε όποιον του παρέδιδε δυο πίτσες και ένας αγρότης ανταποκρίθηκε στο κάλεσμα αυτό, παραγγέλνοντας δυο πίτσες που στοίχιζαν περίπου 30$ τις οποίες αντάλλαξε με 10.000 bitcoin. Το Δεκέμβρη όμως του 2017, το κάθε bitcoin είχε αξία ίση με 19.783$. Κάτι που δεν μπορούσε κανένας να προβλέψει.

Μετά την πρόοδο στην τεχνολογία του Blockchain έχουν εμφανιστεί χιλιάδες κρυπτονομίσματα μετά το Bitcoin. Αυτή τη στιγμή υπάρχουν περίπου χίλια εκατό κρυπτονομίσματα και αυξάνονται. Σήμερα υπάρχει πληθώρα εφαρμογών με ψηφιακά πορτοφόλια κρυπτονομισμάτων, στα οποία υπάρχει η δυνατότητα διαμόρφωσης **ενός "χαρτοφυλακίου" κρυπτονομισμάτων**. Τα ψηφιακά νομίσματα αποτελούν πλέον σημαντικό μέρος του χρηματοοικονομικού κόσμου, αν αναλογιστούμε πως αρκετές οντότητες τα αποδέχονται ως μέσο πληρωμής. Παραμένουν όμως ευάλωτα σε πολύ έντονες διακυμάνσεις τιμών, καθιστώντας τις επενδύσεις αρκετά υψηλού ρίσκο. Επιπλέον η χρήση ψηφιακών νομισμάτων ενέχει πάντα τον κίνδυνο κυβερνοεπιθέσεων, απώλειας περιουσιακών στοιχείων από τα ψηφιακά πορτοφόλια, προβλημάτων στην ολοκλήρωση των συναλλαγών. Στον αντίποδα, βλέπουμε να αναπτύσσονται συνεχώς νέα πρωτόκολλα και υπάρχουν συνεχείς εξελίξεις όσο αφορά τη βελτίωση της αποτελεσματικότητας και της ασφάλειας των ψηφιακών νομισμάτων, όπως για παράδειγμα η ανάπτυξη των **Decentralized Finance (DeFi) πλατφορμών**. Πλατφόρμες όπως το Aave και το Compound επιτρέπουν στους χρήστες να προχωρούν ακόμα και σε σύναψη δανειακών συμβάσεων κρυπτονομισμάτων, κερδίζοντας τόκους ή πληρώνοντας επιτόκια χωρίς την ανάγκη παρουσίας μεσολαβητή (για παράδειγμα τράπεζα).

Ένα ακόμα ζήτημα που απασχολεί σχετικά με τη χρήση ψηφιακών νομισμάτων έχει να κάνει με τον **αντίκτυπο στο περιβάλλον,** καθώς η κατανάλωση ενέργειας που απαιτείται, για την εξόρυξη κατά βάση, των κρυπτονομισμάτων κυμαίνεται σε ιδιαίτερα υψηλά επίπεδα.

Παρατίθεται μία λίστα [17] με **είκοσι πέντε κορυφαία κρυπτονομίσματα:**

1. Bitcoin (BTC)	14. Litecoin (LTC)
2. Ethereum (ETH)	15. Binance Coin (BNB)
3. XRP (XRP)	16. NEM (XEM)
4. Stellar (XNM)	17. TRON (TRX)
5. Cardano (ADA)	18. Dash (DASH)
6. Dogecoin (DOGE)	19. Zcash (ZEC)
7. Polkadot (DOT)	20. Bitcoin Gold (BTG)
8. Neo (NEO)	21. Bitcoin Cash (BCH)
9. Celsius (CEL)	22. Bitcoin SV (BSV)
10. Nano (NANO)	23. EOS (EOS)
11. Chainlink (LINK)	24. VeChain (VET)
12. Monero (XMR)	25. Dai / MakerDao (DAI)
13. Tether (USDT)	

1.4 ΤΑ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ

ΤΙ ΕΙΝΑΙ ΤΑ ΕΞΥΠΝΑ ΣΥΜΒΟΛΑΙΑ:

Με την δημιουργία της Blockchain πλατφόρμας Ethereum το 2015, έγινε η εισαγωγή της ένοιας των έξυπνων συμβολαίων (Smart Contracts). Το όνομα "Έξυπνα Συμβόλαια" καθιέρωσε ο Nick Szabo το 1994. Τα έξυπνα συμβόλαια είναι συμβάσεις ως **προγράμματα κώδικα**. Ενεργοποιούνται και εκτελούνται αυτόματα υπό συγκεκριμένες συνθήκες και οι κινήσεις καταγράφονται στο blockchain καθιστώντας την πληροφορία αμετάβλητη και αδιαμφισβήτητη. [18] Τα έξυπνα συμβόλαια προσφέρουν δύο σημαντικές λειτουργίες, ασφάλεια και μείωση κόστους. Συγκεκριμένα, ο κώδικας αυτός περιέχει ένα σύνολο κανονισμών, του τύπου «όταν συμβαίνει το Α, ενεργοποιείται μια δράση, Β» και "τρέχει" πάνω στο blockchain. Ουσιαστικά αξιολογούν τις πληροφορίες και εκτελούνται αυτόματα σε ένα πλαίσιο ΑΝ/ΤΟΤΕ. [19]

Τα έξυπνα συμβόλαια έφεραν την τεχνολογία πίσω από τα κρυπτονομίσματα, ένα καθοριστικό βήμα μπροστά, καθώς δίνουν τη δυνατότητα ανταλλαγής όχι μόνο χρήματος αλλά **και πληροφοριών ή τίτλων ιδιοκτησίας,** οτιδήποτε φέρει αξία. Παρέχουν τη δυνατότητα να πραγματοποιούνται αυτές οι συναλλαγές σε ασφαλές περιβάλλον, χωρίς την ανάγκη "ενδιάμεσων". Κάθε έξυπνο συμβόλαιο μπορεί να περιλαμβάνει όρους αλλά και ιδιαίτερα νομικά ζητήματα, εκφρασμένα σε κώδικα. Ο κώδικας του αποστολέα συνδυάζεται με τον κώδικα του παραλήπτη, καθορίζοντας με ακρίβεια τις παραμέτρους της συμφωνίας. Τα συμβόλαια θα εκτελούνται μόνο εφόσον πληρούνται όλες οι προϋποθέσεις, επιλύοντας αυτομάτως τυχόν ζητήματα χωρίς ανθρώπινη παρέμβαση. Στο Ethereum για παράδειγμα, τα έξυπνα συμβόλαια έχουν **το δικό τους μηχανισμό συντονισμού και είναι αμετάβλητα (σε ένα blockchain) και επαληθεύσιμα,** εξασφαλίζοντας υψηλό επίπεδο εμπιστοσύνης. Ας εξετάσουμε δύο παραδείγματα χρήσης:

1. Ένα παράδειγμα είναι η **αγορά ενός προϊόντος από έναν έμπορο στο εξωτερικό**, όπου αμφότεροι διστάζουν να κάνουν το πρώτο βήμα, καθώς ο αγοραστής φοβάται ότι δεν θα λάβει το προϊόν του, ενώ ο έμπορος φοβάται ότι δεν θα πληρωθεί. Παραδοσιακά, η λύση ήταν η **μεσεγγύηση** μέσω ενός τρίτου, κάτι ακριβό και χρονοβόρο. Με τη χρήση ενός έξυπνου συμβολαίου, η συναλλαγή μπορεί να ρυθμιστεί έτσι ώστε να **δεσμεύει τα χρήματα του αγοραστή και το προϊόν του εμπόρου**. Όταν τα κριτήρια της συναλλαγής που έχουν συμφωνηθεί πληρούνται, το έξυπνο συμβόλαιο εκτελεί την ανταλλαγή αυτόματα. Τα χρήματα απελευθερώνονται στον έμπορο, και το προϊόν αποστέλλεται στον αγοραστή χωρίς καθυστερήσεις ή περιττές διαδικασίες.

2. Ένα άλλο παράδειγμα χρήσης έξυπνων συμβολαίων αφορά τα **στοιχήματα για μελλοντικά γεγονότα**. Δύο φίλοι που ποντάρουν σε έναν αγώνα τένις μπορούν να δημιουργήσουν ένα έξυπνο συμβόλαιο, όπου αμφότεροι θα καταθέσουν τα στοιχήματά τους. Το έξυπνο συμβόλαιο μπορεί να συνδεθεί με έναν αξιόπιστο πάροχο αποτελεσμάτων. Όταν ανακοινωθεί ο νικητής, το συμβόλαιο θα εκτελέσει αυτόματα την πληρωμή στον νικητή, χωρίς τη δυνατότητα παρέμβασης ή αθέτησης. Με αυτόν τον τρόπο, τα έξυπνα συμβόλαια δημιουργούν **αξιοπιστία και ασφάλεια** στις συναλλαγές, διασφαλίζοντας την αυτόματη και αδιάβλητη εκτέλεση των συμφωνηθέντων.

Τα έξυπνα συμβόλαια έχουν ήδη κατακτήσει μεγάλο κομμάτι της αγοράς. Το ένα μεγάλο πλεονέκτημα των έξυπνων συμβολαίων είναι η δυνατότητα παρακολούθησης, η ικανότητα, δηλαδή, των εντολέων να παρακολουθούν την εκτέλεση της σύμβασης ή να αποδεικνύουν την απόδοσή τους σε άλλους. Ο τομέας της λογιστικής ασχολείται με τη σύναψη συμβάσεων. Οι οικονομολόγοι συζητούν για την "κρυφή γνώση", επίσης γνωστή ως "αρνητική επιλογή", η οποία υποβόσκει λόγω της έλλειψης ικανότητας παρακολούθησης πιθανών αντισυμβαλλομένων κατά τη διάρκεια των φάσεων έρευνας και διαπραγμάτευσης. Ένα άλλο σημαντικό πρόβλημα είναι οι «κρυφές ενέργειες», γνωστές και ως «ηθικοί κίνδυνοι», οι οποίες μπορεί να προκύψουν λόγω της έλλειψης επαρκούς επίβλεψης, αλλά και λόγω της πιθανότητας εγκατάλειψης της σύμβασης κατά τη φάση εκτέλεσής της. [20]

Ένα σημαντικό καθήκον των έξυπνων συμβολαίων, είναι η επικοινωνία της σημειολογίας των πρωτοκόλλων στα εμπλεκόμενα μέρη. Για παράδειγμα, τα μηχανήματα POS παντοπωλείων δεν λένε στους πελάτες εάν τα ονόματά τους συνδέονται ή όχι με τις αγορές τους σε μια βάση δεδομένων. Οι υπάλληλοι δεν γνωρίζουν καν, και έχουν επεξεργαστεί χιλιάδες τέτοιες συναλλαγές. Έτσι, μέσω “κρυφής ενέργειας” του λογισμικού, ο πελάτης δίνει πληροφορίες που μπορεί να θεωρεί πολύτιμες ή εμπιστευτικές, αλλά η σύμβαση έχει συνταχθεί και η συναλλαγή έχει σχεδιαστεί με τέτοιο τρόπο ώστε να αποκρύπτει αυτά τα σημαντικά μέρη της συναλλαγής από τον πελάτη. Η εμπιστοσύνη στις μεγάλες εταιρείες λογιστικής αλλά και δεδομένων έχει διαβρωθεί και θα διαβρωθεί ακόμη περισσότερο καθώς τέτοιες εταιρείες αρχίζουν να εκμεταλλεύονται τις τεράστιες ποσότητες εσωτερικών πληροφοριών που συλλέγουν από τις βάσεις δεδομένων των πελατών τους κατά τη διάρκεια ελέγχων. Χρησιμοποιώντας πρωτόκολλα που βασίζονται σε χαρτί σε έναν ψηφιακό κόσμο, υπάρχουν λίγοι αποτελεσματικοί τρόποι ελέγχου των ίδιων των ελεγκτών. Η χρήση κρυπτογραφικών πρωτοκόλλων, όπως τα έξυπνα συμβόλαια, ενδέχεται να βελτιώσει τα αυξανόμενα προβλήματα εξόρυξης δεδομένων και παραβίασης ιδιωτικότητας. [20]

Οφείλουμε, στον αντίποδα, να σημειώσουμε ότι τα έξυπνα συμβόλαια πάσχουν ακόμα σε ότι αφορά νομικά ζητήματα. Η επιβολή των όρων ενός τέτοιου συμβολαίου σε ένα δικαστήριο για παράδειγμα, είναι αμφίβολη. Είναι όμως βέβαιο πως τα έξυπνα συμβόλαια είναι από τις πιιο καινοτόμες και χρήσιμες δημιουργίες με blockchain, ενώ οι δυνατότητες που αναδύονται από τη χρήση τους φαίνεται να διαμορφώνουν ένα τελείως διαφορετικό τοπίο στο μέλλον της οικονομίας, σχεδόν σε όλα τα επίπεδα, λόγω της αυτοματοποίησης, της διαφάνειας, της ασφάλειας και της αμεταβλητότητας που, μεταξύ άλλων, τα διέπουν.

ΠΩΣ ΜΟΙΑΖΕΙ ΕΝΑ ΕΞΥΠΝΟ ΣΥΜΒΟΛΑΙΟ :

```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                           // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

(ΕΙΚΟΝΑ 4 - ΠΗΓΗ: https://www.ethereum.org/token

1.5 ΣΥΝΑΡΤΗΣΕΙΣ HASH

Οι Hash συναρτήσεις, ή αλλιώς **συναρτήσεις κατατεμαχισμού / κατακερματισμού**, είναι μαθηματικές συναρτήσεις, στις οποίες εισέρχονται δεδομένα τυχαίου μεγέθους και επιστρέφονται ακέραια, σταθερά μεγέθη αναπαράστασης (από 32bit μέχρι 256bit ή περισσότερα, ανάλογα με το λόγο χρήσης της συνάρτησης). Οι τιμές που επιστρέφει η συνάρτηση Hash, ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά hashes. Οι τιμές αυτές θα πρέπει να είναι διαφορετικές για διαφορετική είσοδο, καθώς η κύρια χρησιμότητα αυτών των συναρτήσεων είναι να ταυτοποιούν τα δεδομένα. Αυτή η ιδιότητα μπορεί να χρησιμοποιηθεί στη δημιουργία ψηφιακών υπογραφών όπου χρησιμοποιούνται τιμές κατατεμαχισμού μεγάλου μεγέθους για να ελαχιστοποιηθεί ο κίνδυνος πλαστογράφησής τους. Ο όρος "συνάρτηση κατακερματισμού" προέρχεται από τη γαλλική λέξη "hacher" που σημαίνει "τεμαχισμός σε μικρά κομμάτια", υποδεικνύοντας πώς η συνάρτηση κατακερματισμού έχει σχεδιαστεί για να "τεμαχίζει" τα δεδομένα.

Η συνάρτηση κατακερματισμού θα πρέπει να αντιστοιχίζει κάθε είσοδο σε διαφορετική τιμή κατατεμαχισμού. Αν ας πούμε εισάγω το όνομά μου, Eva, σε μια online hash generator, (https://passwordsgenerator.net/sha256-hash-generator/), με τη χρήση του SHA-1, το hash που δημιουργείται είναι:

10AF 29D0 4264 1FDB CC37 5F36 E3D9 A194 6468 F9E8

Αν εισάγω το όνομα Eve, αλλάζοντας ένα μόνο γράμμα, το αποτέλεσμα είναι τελείως διαφορετικό:

9A01 8ECC 48A3 7A92 47A6 404F D83E 0853 84B4 45AA

Αν τώρα εισάγω τη φράση: "Hash functions are the used in cryptocurrency technology":

2756 5F4D 99A6 4A3C 7D6D 91D5 554A B1C0 5B30 C4D9

Παρατηρούμε πως ανεξάρτητα από το πλήθος των χαρακτήρων που εισάγονται, το hash που επιστρέφεται αποτελείται από 40 χαρακτήρες. Η ιδιότητα αυτή, της συμπύκνωσης ολόκληρων κειμένων σε σαράντα χαρακτήρες είναι εξαιρετικά ενδιαφέρουσα και χρήσιμη. Ανάλογα με την χρήση για την οποία προορίζεται, η συνάρτηση κατατεμαχισμού σχεδιάζεται με διαφορετικές προδιαγραφές. Οι κρυπτογραφικές συναρτήσεις κατακερματισμού, δημιουργούν μια συμβολοσειρά χαρακτήρων σταθερού μήκους (40 στο παράδειγμά μας), από εγγραφές δεδομένων οποιουδήποτε μήκους, από μια λέξη ή πρόταση, μέχρι ολόκληρα κείμενα ή ακόμα και αρχεία. Οι συναρτήσεις αυτές, που χρησιμοποιούνται κυρίως για λόγους ασφαλείας, αποτελούν τη "ραχοκοκαλιά" της ασφάλειας στην κρυπτογράφηση. Η μετατροπή μιας συναλλαγής σε μια συμβολοσειρά byte με σταθερό μήκος και δομή, διευκολύνει τον εντοπισμό συναλλαγών στην αλυσίδα των μπλοκ.

Μια απλουστευμένη εξήγηση του τρόπου λειτουργίας των συναρτήσεων κατακερματισμού θα ήταν το μέγεθος και η τιμή των burger για παράδειγμα σε ένα εστιατόριο.

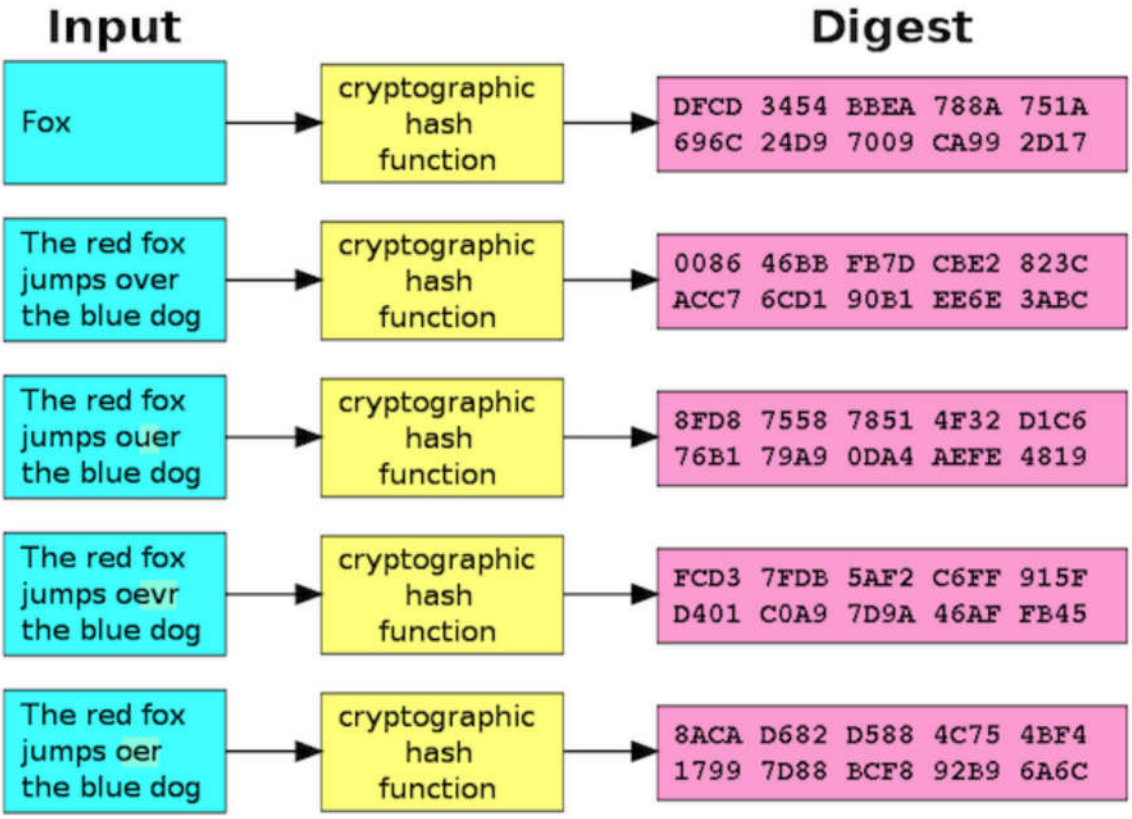
Αν υποθέσουμε πως το κόστος του burger καθορίζεται από το μέγεθός του, στη συγκεκριμένη περίπτωση, το κόστος είναι συνάρτηση του μεγέθους. Αν υποθέσουμε ότι τα μικρά, μεσαία και μεγάλα burger κοστίζουν αντίστοιχα 1,50 $, 2,50 $ και 3,50 $. Τότε η "είσοδος" (input) είναι το μέγεθος του burger. Η "έξοδος" (output) είναι το κόστος του burger.

Αφού οι Diffie και Hellman εντόπισαν για πρώτη φορά την ανάγκη μιας μονόδρομης συνάρτησης κατακερματισμού στο σεμινάριο του 1976 σχετικά με την κρυπτογραφία δημόσιου κλειδιού, τις επόμενες δύο δεκαετίες οι εξελίξεις στην κρυπτογραφία ήταν καταιγιστικές. Το 1990, ο κρυπτογράφος και καθηγητής του MIT, Ronald Rivest, εφήυρε τη συνάρτηση κατακερματισμού MD4 και αργότερα τις λειτουργίες MD5 και MD6. Το 1995, η NSA (Εθνική Υπηρεσία Ασφάλειας) σχεδίασε τον SHA-1 (Secure Hash Algorithm 1) με βάση το σχεδιασμό του Rivest, ακολουθούμενο από την ενημέρωση SHA-2 το 2001. Ο SHA-2 είναι το πρότυπο που ενέπνευσε τον SHA-256, το οποίο εξυπηρετούσε ως βάση για τον αλγόριθμο του Bitcoin.

Μια συνάρτηση κρυπτογραφικού κατακερματισμού θα πρέπει να έχει **γρήγορη απόδοση**, να δημιουργεί την άμεσα τιμή κατακερματισμού. Πρέπει να είναι **ντετερμινιστική** - κάθε φορά που εισάγεται μια συγκεκριμένη είσοδος, πρέπει να παράγει την ίδια έξοδο. Να είναι **ανθεκτική**, να μην αποκαλύπτει καμία πληροφορία σχετικά με την είσοδο στην έξοδο. Να είναι **ανθεκτική σε "συγκρούσεις"**, να διασφαλίζει ότι δύο διαφορετικές είσοδοι δεν πρέπει να παράγουν την ίδια έξοδο. Το ντετερμινιστικό χαρακτηριστικό, η ανθεκτικότητα στην εικόνα και η αντίσταση σε σύγκρουση, αποτελούν τις τρεις πιο σημαντικές ιδιότητες, για τη χρήση συναρτήσεων κατακερματισμού στη διαδικασία εξόρυξης Bitcoin.

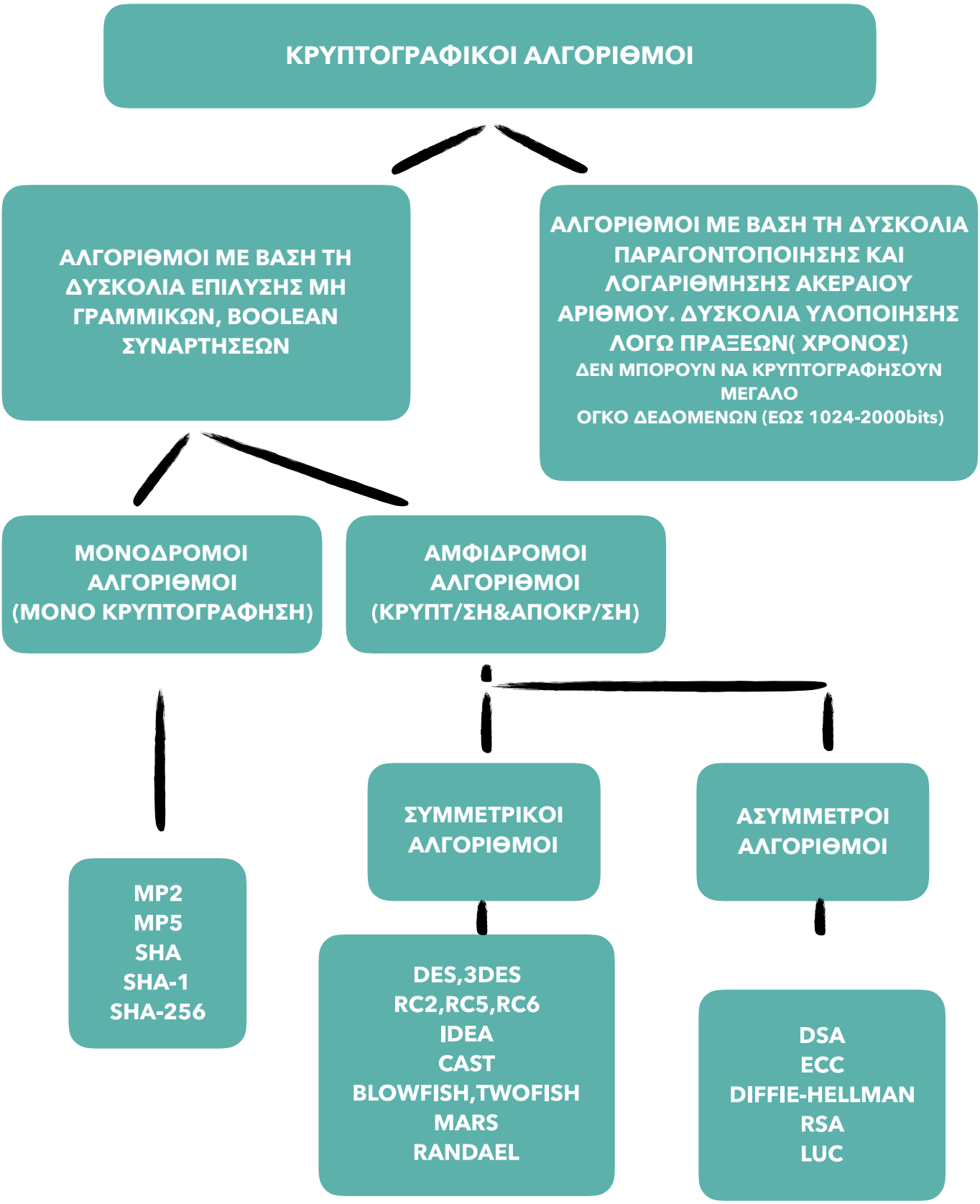
Χαρακτηριστικά, λοιπόν, στο δίκτυο Bitcoin, ένα μπλοκ ομαδοποιείται και περιέχει πολλές συναλλαγές καθώς και πληροφορίες για το προηγούμενο μπλοκ. Αυτό σημαίνει ότι εάν κάποιος ήθελε να αλλάξει το καθολικό θα πρέπει να αλλάξει το hash σε όλα τα προηγούμενα μπλοκ. Για να προστεθεί το ομαδοποιημένο μπλοκ στο blockchain, οι ανθρακωρύχοι πρέπει να βρουν ένα hash που να ανταποκρίνεται στη δυσκολία του στόχου. Κάθε μπλοκ περιέχει ένα "blockheader" με τον αριθμό του μπλοκ, το hash του προηγούμενου μπλοκ και ένα "nonce", το οποίο περιλαμβάνει μια χρονική σήμανση. Ο σκοπός ενός nonce είναι η μεταβολή της εισόδου σε μια συνάρτηση κρυπτογραφικού κατακερματισμού, δηλαδή η αυξημένη τυχαιότητα, στον υπολογισμό κατά τη διάρκεια της διαδικασίας εξόρυξης. Στη συνέχεια, ο κόμβος ξεκινά κατακερματισμό των δεδομένων μετατρέποντάς τα σε τιμή κατακερματισμού (hash), η οποία πρέπει πάντα να περιέχει έναν ορισμένο αριθμό μηδενικών. Ο κόμβος ελέγχει εάν ένα hash πληρεί τα κριτήρια δυσκολίας. Ο κατακερματισμός πρέπει να ξεκινά με τη σωστή ποσότητα μηδενικών. Εάν ο κατακερματισμός πληρεί τα κριτήρια, μεταδίδεται στους άλλους ανθρακωρύχους στο δίκτυο. Ο πρώτος ανθρακωρύχος που βρίσκει ένα έγκυρο hash επικυρώνει το μπλοκ σε ένα νέο μπλοκ και λαμβάνει ως "ανταμοιβή" Bitcoin. Εάν ο κατακερματισμός δεν πληρεί τα κριτήρια του δικτύου, επιλέγεται για κατακερματισμό άλλο nonce. Οι ανθρακωρύχοι πιθανότατα πρέπει να δημιουργήσουν πολλούς κατακερματισμούς με πολλά nonces μέχρι να βρουν ένα nonce που να ανταποκρίνεται. Αυτή είναι η επαναλαμβανόμενη και εντατική ενέργεια διαδικασία γνωστή ως εξόρυξη Bitcoin και απαιτεί εκτεταμένη υπολογιστική ισχύ. Οι λειτουργίες Hash αποτελούν τη ραχοκοκαλιά της διαδικασίας. Χωρίς επιβεβαίωση και παραγωγή συναλλαγών κατακερματισμού, το blockchain δεν θα ήταν αδιάβλητο και δεν θα ήταν δυνατό να αποδειχθεί ποιος είχε το ποσό του Bitcoin σε ποια στιγμή.

Δημοφιλείς συναρτήσεις Hash: MD5 (Message Digest Algorithm 5 - hash 128bit - θεωρείται ανασφαλής)



ΕΙΚΟΝΑ 5 - ΠΗΓΗ: https://kaspersky.com/blog/the-wonders-of-hashing/4441/

1.6 ΤΟΠΟΛΟΓΙΑ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΑΛΓΟΡΙΘΜΩΝ



1.7 ΑΛΓΟΡΙΘΜΟΣ SHA - 256

Το SHA-2 δημοσιεύθηκε για πρώτη φορά από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ως ομοσπονδιακό πρότυπο των ΗΠΑ (FIPS). Η οικογένεια αλγορίθμων SHA-2 κατοχυρώνεται με δίπλωμα ευρεσιτεχνίας ΗΠΑ. Οι Ηνωμένες Πολιτείες έχουν εκδώσει το δίπλωμα ευρεσιτεχνίας με άδεια χωρίς δικαιώματα. Προς το παρόν, οι καλύτερες επιθέσεις σπάνε την αντίσταση στην προτίμηση για 52 από τους 64 γύρους του SHA-256 ή 57 από τους 80 γύρους του SHA-512 και την αντίσταση σύγκρουσης για 46 από τους 64 γύρους του SHA-256. Αυτός ο αλγόριθμος κατακερματισμού χρησιμοποιείται, όπως αναφέρθηκε και στην προηγούμενη ενότητα, από το Bitcoin, ως εγγύηση της ακεραιότητας των πληροφοριών που είναι αποθηκευμένες σε ένα block. Όπως σχεδόν σε όλες οι εξελίξεις στην κρυπτογραφία, οι κυβερνήσεις του κόσμου έπαιξαν θεμελιώδη ρόλο στην ανάπτυξη και χρήση του αλγόριθμου SHA ή Secure Hash Algorithm, με αφορμή τον πόλεμο. Αυτός ο κρυπτογραφικός αλγόριθμος αναπτύχθηκε από τον Οργανισμό Εθνικής Ασφάλειας των Ηνωμένων Πολιτειών (NSA) και το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST). Στόχος του είναι να δημιουργήσει hash ή μοναδικούς κωδικούς που βασίζονται σε ένα πρότυπο με το οποίο τα έγγραφα ή τα δεδομένα του υπολογιστή θα μπορούσαν να ασφαλιστούν από οποιονδήποτε εξωτερικό παράγοντα που επιθυμεί να τα τροποποιήσει. Αυτός ο αλγόριθμος ήταν και αποτελεί ακόμα μια μεγάλη πρόοδο στον τρόπο διασφάλισης του απορρήτου του περιεχομένου κατά την επεξεργασία πληροφοριών.

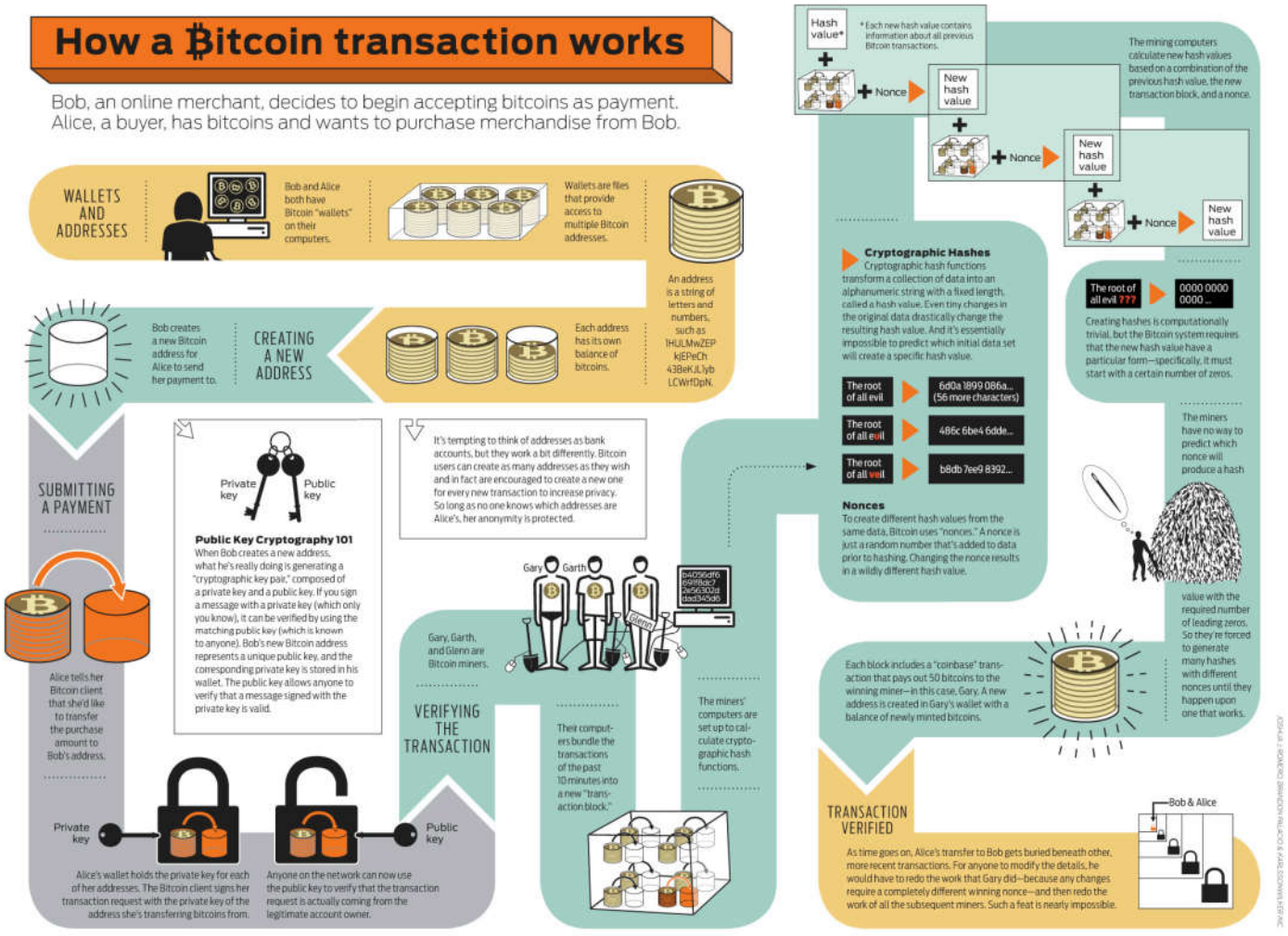
Το 1993 ήρθε στο φως το πρώτο πρωτόκολλο SHA, το οποίο ονομάστηκε SHA-0 Δύο χρόνια αργότερα, κυκλοφόρησε μια ισχυρότερη, βελτιωμένη παραλλαγή, το SHA-1. Λίγα χρόνια αργότερα κυκλοφόρησε το SHA-2, το οποίο έχει τέσσερις παραλλαγές ανάλογα με τον αριθμό των bit, όπως SHA-224, SHA-256, SHA-384, SHA-512.

Ένας αλγόριθμος κατακερματισμού, όπως αναλύσαμε, λειτουργεί μόνο προς μία κατεύθυνση: αυτό σημαίνει ότι από οποιοδήποτε περιεχόμενο μπορούμε να δημιουργήσουμε ένα hash (το "ψηφιακό δακτυλικό αποτύπωμά του"), αλλά από ένα hash δεν υπάρχει τρόπος δημιουργίας του περιεχομένου που σχετίζεται με αυτό, εκτός από την επαναλαμβανόμενη τυχαία προσπάθεια μέχρι να βρεθεί το περιεχόμενο. Μεταξύ των διαφορετικών τρόπων δημιουργίας hash, ο αλγόριθμος που χρησιμοποιείται από το SHA-256 είναι ένας από τους πιο ευρέως χρησιμοποιούμενους γιατί ισορροπεί μεταξύ ασφάλειας και υπολογιστικού κόστους παραγωγής. Μια άλλη από τις ιδιαιτερότητες του αλγορίθμου κατακερματισμού SHA-256 είναι ότι το μήκος του κατακερματισμού που προκύπτει είναι πάντα το ίδιο, ανεξάρτητα από το πόσο εκτενές είναι το περιεχόμενο που χρησιμοποιείται για τη δημιουργία του κατακερματισμού: είτε ένα γράμμα είτε όλες οι λέξεις. Το αποτέλεσμα είναι πάντα μια συμβολοσειρά 40 γραμμάτων και αριθμών (256-bit, κωδικοποιημένη 32-byte). Ο σκοπός του SHA-256 (και οποιασδήποτε συνάρτησης κατακερματισμού) είναι να δημιουργήσει μια “περίληψη”. Να συμπυκνώσει την πληροφορία.

Στο Bitcoin, το SHA-256 χρησιμοποιείται για τη διαδικασία εξόρυξης (δημιουργία bitcoin), αλλά και για τη διαδικασία δημιουργίας διευθύνσεων bitcoin. Αυτό οφείλεται στο υψηλό επίπεδο ασφάλειας που προσφέρει. Μέσα στο δίκτυο blockchain όλοι οι κόμβοι θα έχουν ένα αντίγραφο του hash 40 χαρακτήρων που αντιπροσωπεύει τις πληροφορίες που εμπεριέχει, για παράδειγμα, ένα ολόκληρο μπλοκ. Μόλις αυτές οι πληροφορίες επικυρωθούν από το δίκτυο καταχωρείται στην αλυσίδα, ενώ οποιαδήποτε χειραγώγηση αυτών των πληροφοριών, θα εντοπιστεί αμέσως και θα απορριφθεί.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

ΠΩΣ ΠΡΑΓΜΑΤΟΠΟΙΟΥΝΤΑΙ ΚΡΥΠΤΟ-ΣΥΝΑΛΛΑΓΕΣ



ΕΙΚΟΝΑ 6 - (ΠΗΓΗ: Paper- Synthesizing a Bitcoin Miner SHA-256 Accelerator Core, Tommy Tracy II, ECE6502 Spring 2014, University of Virginia)

2.1 MINING(ΕΞΟΡΥΞΗ) & ΕΠΕΝΔΥΣΕΙΣ

Η δημιουργία κρυπτονομισμάτων πραγματοποιείται μέσω της επίλυσης ενός περίπλοκου μαθηματικού αλγόριθμου, μια διαδικασία που ονομάζεται **εξόρυξη** ή **mining**. Οι συμμετέχοντες (miners) χρησιμοποιούν **υπολογιστική ισχύ για να επιλύσουν κρυπτογραφικούς γρίφους**, οι οποίοι είναι απαραίτητοι για την **επαλήθευση και καταγραφή των συναλλαγών σε ένα blockchain**. Κάθε φορά που επιλύεται ένας τέτοιος γρίφος, προστίθεται ένα νέο μπλοκ στην αλυσίδα (blockchain), και οι miners ανταμείβονται με μια ποσότητα κρυπτονομισμάτων (π.χ. bitcoin). Αυτή η διαδικασία διασφαλίζει την ακεραιότητα και την ασφάλεια του δικτύου. Η ενέργεια που απαιτείται, καθιστά εξαιρετικά δύσκολη την αλλοίωση της αλυσίδας.

Έστω **ένα σύνολο N = {1, ..., N} miners** στο δίκτυο Bitcoin με N ≥ 2. Κάθε miner, i ∈ N έχει σχετική **ισχύ κατακερματισμού α(i)> 0 έτσι ώστε Σ α(j) = 1, j∈N**. Οι N miner, εμπλέκονται σε έναν αγώνα προς τη λύση ενός μαθηματικού προβλήματος. Αυτό το μαθηματικό πρόβλημα επιλύεται με μια στρατηγική **"trial and error",** δοκιμής και αποτυχίας. Αν η επίλυση του προβλήματος μοντελοποιηθεί ως τυχαία μεταβλητή που ακολουθεί **κατανομή Poisson**, η πολυπλοκότητα της εύρεσης ενός μπλοκ προσαρμόζεται δυναμικά έτσι ώστε αυτή η λειτουργία να διαρκεί 600 δευτερόλεπτα. Τότε, **η διαδικασία εξόρυξης έχει παράμετρο λ = 1/600> 0 για ολόκληρο το δίκτυο.** Ο αριθμός των συναλλαγών που περιλαμβάνονται σε ένα μπλοκ προς επίλυση επιλέγεται από κάθε miner. Αυτός ο αριθμός δεν επηρεάζει την πολυπλοκότητα του μαθηματικού προβλήματος ή το κόστος για να λυθεί. Ωστόσο, μόλις ένας miner βρει ένα μπλοκ με συγκεκριμένο αριθμό συναλλαγών σε αυτό, πρέπει να μεταδώσει τη λύση του στο δίκτυο Bitcoin και για τη λύση του πρέπει επιτευχθεί συναίνεση. Ο χρόνος που απαιτείται για να επιτευχθεί συναίνεση για ένα μπλοκ εξαρτάται από τον αριθμό συναλλαγών που περιλαμβάνονται σε αυτό το μπλοκ. Αν το k (x) να είναι ο χρόνος που απαιτείται για ένα μπλοκ συμπεριλαμβανομένων των συναλλαγών x για την επίτευξη συναίνεσης. Θα κάνουμε την υπόθεση ότι η συνάρτηση είναι γραμμική, k (x) = k.x με k> 0. Ο πρώτος miner έχει βρει ένα μπλοκ που επιτυγχάνει συναίνεση κερδίζει (σε bitcoin) μια σταθερή επιβράβευση R ≥ 0 και μια μεταβλητή c.x με γ ≥ 0. Υποθέτουμε ότι όλοι οι miners αρχίζουν να προσπαθούν να βρουν ένα νέο μπλοκ ταυτόχρονα. Καθε miner i ∈ N περιλαμβάνει x(i)> 0 συναλλαγές στο μπλοκ που προσπαθεί να εντοπίσει. Έστω διάνυσμα x = (x1, ..., xn) η ακολουθία του αριθμού των συναλλαγών που περιλαμβάνονται στο νέο μπλοκ που θα βρεθεί, μία για κάθε miner. Έτσι μπορεί να υπολογιστεί η πιθανότητα ο i miner να βρεί ένα μπλόκ μεταξύ t και t+dt, και να είναι ο πρώτος που επιτυγχάνει τη συναίνεση. [21] Οι miners, λοιπόν, χρησιμοποιώντας υπολογιστική ισχύ, επιλύουν έναν κρυπτογραφικό γρίφο, ο οποίος αποδεικνύει την εγκυρότητα ενός συνόλου συναλλαγών. Ο υπολογιστής "μαντεύει" hashes μέχρι να βρει το σωστό που επιλύει το γρίφο. Αυτή η διαδικασία αποτελεί **απόδειξη μόχθου ή proof of work** και οι miners λαμβάνουν για την ενέργεια και το χρόνο που κατανάλωσαν μια **ανταμοιβή** η οποία αποτελείται:

Α. Από ένα ποσό σε Bitcoin. Το 2009 για κάθε προστιθέμενο μπλοκ στην αλυσίδα η αμοιβή ανέρχονταν στα 50 Bitcoin. Το ποσό αυτό βάσει πρωτοκόλλου μειώνεται περίπου στο μισό κάθε τέσσερα χρόνια, άρα η αμοιβή σήμερα ανέρχεται στα 6.25 Bitcoin ανά μπλοκ.

Β. Από το τέλος επικύρωσης συναλλαγών. Ο miner κλείνοντας το μπλοκ επικυρώνει μια σειρά συναλλαγών που έχουν πραγματοποιηθεί με Bitcoin. Ένα μικρό ποσό από τις συναλλαγές πληρώνεται στους miners ως "τέλος επικύρωσης". Με την πάροδο των ετών και τη μείωση των παραγόμενων Bitcoin ανά μπλόκ, αυτό προβλέπεται να είναι το κύριο έσοδο των miners στο μέλλον.

Το κάθε μπλοκ αποτελείται από **το hash της συναλλαγής, (transaction hash)**, **το hash του προηγούμενου μπλοκ (previous hash) και ένα nonce,** έναν θετικό, ακέραιο αριθμό, ο οποίος σε συνδυασμό με τα hash της συναλλαγής και του προηγούμενου μπλοκ, **δημιουργεί τον κατακερματισμό του μπλοκ**. Ουσιαστικά το nonce είναι το ¨κλειδί" του γρίφου. Ας πάρουμε το παράδειγμα μιας υποθετικής συναλλαγής.

Ο χρήστης Χ, στέλνει ως αμοιβή στο χρήστη Ψ το ποσό των 0,02 BTC, χρησιμοποιώντας ένα ηλεκτρονικό πορτοφόλι. Ο Χ υπογράφει τη συναλλαγή με το ιδιωτικό του κλειδί, μεταδίδεται στο δίκτυο μέσω του ηλεκτρονικού πορτοφολιού και προστίθεται στις μη επιβεβαιωμένες συναλλαγές. Στη συνέχεια ένας miner επιλέγει τη συγκεκριμένη συναλλαγή και προσπαθεί να βρει το σωστό nonce ώστε να δημιουργηθεί το επόμενο μπλοκ. Η συναλλαγή κατακερματίζεται και συνδυάζεται με τον κατακερματισμό του προηγούμενου μπλοκ. Το σωστό nonce εξάγει έναν τελικό κατακερματισμό **(block hash)**. Ο miner δημιουργεί με αυτό τον τρόπο ένα νέο μπλοκ που προστίθεται στην αλυσίδα. Οι συναλλαγές με αυτό τον τρόπο επικυρώνονται και παγιώνονται. Για να μπορέσει κάποιος να μεταβάλλει μια υπάρχουσα συναλλαγή θα πρέπει να εξορύξει όλα τα μπλοκ που έπονται της συναλλαγής αυτής. Κάτι εξαιρετικά χρονοβόρο και δαπανηρό. Οι συναλλαγές επικυρώνονται κατά την προσθήκη τους σε ένα νέο μπλοκ και επιβεβαιώνονται σε κάθε επόμενη συναλλαγή που τις συμπεριλαμβάνει. Η εξόρυξη, λοιπόν εκτός του ότι δημιουργεί νέα μπλοκ, επικυρώνει και πραγματοποιούμενες συναλλαγές. Αυτό σημαίνει ότι μετά την εξόρυξη όλων των είκοσι ένα εκατομμυρίων νομισμάτων του Bitcoin , το mining θα πρέπει να συνεχιστεί, ώστε να επιβεβαιώνονται οι συναλλαγές.

Ο **χρόνος παραγωγής ενός νέου μπλοκ**, όπως αναφέρθηκε και στην προηγούμενη ενότητα, είναι δέκα λεπτά, ανεξάρτητα από τον αριθμό προσπαθειών των miners. Το πρωτόκολλο του Bitcoin, προβλέπει προσαρμογή δυσκολίας, δηλαδή αύξηση του συνόλου των πιθανών nonces , ώστε οι πιθανότητες να βρεθεί το σωστό να μειώνονται με την αύξηση της υπολογιστικής ισχύος.

Η **ποσότητα των παραγόμενων κρυπτονομισμάτων** δεν υπαγορεύεται από τη βούληση κάποιου κράτους ή οργανισμού. Το δίκτυο καθορίζει αυτόματα το ρυθμό δημιουργίας τους, γεγονός που συμβάλλει στη σχετική σταθερότητα της προσφοράς τους. Θεωρητικά, η δημιουργία νέων νομισμάτων είναι προγραμματισμένη και προβλέψιμη, άρα δεν μπορεί να αυξηθεί απότομα η προσφορά τους, κάτι που περιορίζει τον κίνδυνο υποτίμησης της αξίας τους. Αυτό το χαρακτηριστικό καθιστά, σε θεωρητικό επίπεδο, τα κρυπτονομίσματα «αλεξίσφαιρα» απέναντι στον πληθωρισμό, τις οικονομικές κρίσεις κι άλλα προβλήματα που αντιμετωπίζουν τα συμβατικά νομίσματα στην οικονομία σήμερα. Αυτή η θεωρητική προσέγγιση πλαισίωνε τη λογική των κρυπτονομισμάτων πολύ πριν την εμφάνισή τους. Εδώ όμως οφείλουμε να υπογραμμίσουμε πως η κρυπτοοικονομία δε λειτουργεί αυτόνομα. **Ενδεχομένως σε βάθος χρόνου, να αποτελέσει την εξέλιξη της μορφής του γενικού ισοδύναμου. Δεν μπορεί όμως να επηρεάζει τον τρόπο συσχέτισης των μέσων παραγωγής, ο οποίος αποτελεί την πηγή των προβλημάτων που εκδηλώνονται σε επίπεδο οικονομίας.** Οι χρήστες ζουν και συναλλάσσονται σε δεδομένο οικονομικό περιβάλλον το οποίο καθορίζει σε μεγάλο βαθμό και τη σχετιζόμενη με την κρυπτοοικονομία δραστηριότητά τους. Παρατηρείται, άλλωστε, **ομοιότητα στη συμπεριφορά και τη διακύμανση της συναλλαγματικής ισοτιμίας των κρυπτονομισμάτων με αυτή των μετοχών, όσον αφορά πληροφορίες ή εξελίξεις που σχετίζονται με την κρυπτοοικονομία**. Το παράδειγμα του ανταλλακτηρίου Thodex, στην Τουρκία, είναι χαρακτηριστικό παράδειγμα, καθώς με την ανακοίνωση της πιθανότητας απάτης στις 20 Απριλίου 2021, η συναλλαγματική ισοτιμία όλων των κρυπτονομισμάτων κατέρρευσε, ακολουθώντας καθοδική πορεία για τις επόμενες τέσσερις μέρες. Αντίστοιχα παρατηρήθηκε πτώση μετά τις δηλώσεις του προέδρου Μπαιντέν για επικείμενη φορολογική μεταρρύθμιση με αύξηση του συντελεστή φορολόγησης σε εισοδήματα που προκύπτουν από επενδύσεις.

Αντίθετα, είδαμε σε ανοδική πορεία για παράδειγμα το νόμισμα Dogecoin, μετά από δηλώσεις του Elon Musk ότι προτίθεται να επενδύσει στο συγκεκριμένο κρυπτονόμισμα, ανεβάζοντας έτσι τη συναλλαγματική του αξία.

Η **συναλλαγματική ισοτιμία** των κρυπτονομισμάτων είναι πλήρως εξαρτημένη από τη ζήτηση των χρηστών, χωρίς να ελέγχεται από κάποια κεντρική αρχή ή ομάδα. Όταν αυξάνεται η ζήτηση για ένα κρυπτονόμισμα, η τιμή του ανεβαίνει, ενώ όταν μειώνεται, η τιμή πέφτει. Οι χρήστες με τη συμπεριφορά τους καθορίζουν την αξία του νομίσματος, γεγονός που το διαφοροποιεί από τα παραδοσιακά νομίσματα, τα οποία συνδέονται με φυσικά αγαθά, όπως ο χρυσός. Το κρυπτονόμισμα λειτουργεί αποκλειστικά σε ψηφιακό περιβάλλον, επιτρέποντας συναλλαγές μέσω ενός κατανεμημένου δικτύου, χωρίς τη μεσολάβηση τρίτων, στο σύστημα "P2P" (peer-to-peer). Ωστόσο, η τιμή των κρυπτονομισμάτων παραμένει αρκετά ασταθής, κυρίως επειδή το πεδίο αυτό δεν ρυθμίζεται από κάποια καθιερωμένη νομοθεσία. Κάθε ανακοίνωση από κυβερνήσεις, ισχυρούς επιχειρηματίες ή προσπάθειες ρύθμισης της ψηφιακής οικονομίας των κρυπτονομισμάτων μπορεί να προκαλέσει τεράστιες διακυμάνσεις στις αντιδράσεις των χρηστών, και κατά συνέπεια, στην αξία των κρυπτονομισμάτων.

MINING

Το Bitcoin εξακολουθεί να είναι το κρυπτονόμισμα με τη μεγαλύτερη ισοτιμία, με μεγάλη διαφορά από το Ethereum που ακολουθεί στη δεύτερη θέση. Όμως έχει αλλάξει αρκετά **η διαδικασία απόκτησης** ενός ψηφιακού κρυπτονομίσματος σε σχέση με τα πρώτα έτη εμφάνισής τους. Το 2009, θεωρητικά μπορούσε κανείς με ένα απλό laptop ή οποιαδήποτε σταθερή μονάδα υπολογιστή, με έναν απλό επεξεργαστή (**CPU**), να πραγματοποιήσει τη διαδικασία εξόρυξης κρυπτονομισμάτων (mining). Αποδείχθηκε στην πράξη πως οι **κάρτες γραφικών** έπαιζαν ρόλο στη διαδικασία αυτή. Καθώς εξελίσσονταν η τεχνολογία σχετικά με την εξόρυξη και έμπαιναν περισσότεροι χρήστες στη διαδικασία αυτή, τόσο πιο δύσκολα μπορούσε κανείς να αποκτήσει ένα κρυπτονόμισμα. Χρειαζόταν όλο και μεγαλύτερη υπολογιστική ισχύ. Έτσι στην πορεία ο μόνος τρόπος πραγματοποίησης εξόρυξης κρυπτονομισμάτων ήταν η χρήση ενός **ASIC** (Application Specific Integrated Circuit), ή Ολοκληρωμένο Κύκλωμα για συγκεκριμένες εφαρμογές. Επεξεργαστές που λειτουργούν αποκλειστικά για mining. Ένα ASIC, σε αντίθεση με οποιονδήποτε άλλο επεξεργαστή ή κάρτα γραφικών, μπορεί να πραγματοποιεί μία μόνο εργασία, αλλά πολύ πιο γρήγορα και πολύ πιο αποδοτικά. Στην προκειμένη περίπτωση η εργασία που απαιτείται είναι η επίλυση αλγόριθμων και ο επεξεργαστής “μαντεύει” hashes, έως ότου βρεί το hash που επιλύει το μπλοκ.

Το 2012, κυκλοφόρησε το Avalon One, από την εταιρεια Avalon. Ήταν ένα από τα πρώτα **ASIC Miner** για bitcoin. Η συσκευή αυτή μπορούσε να υπολογίσει 165 MegaHash/Watt που ήταν εξαιρετική απόδοση για το 2012. Η απόδοση σήμερα μετριέται σε εκατομμύρια MegaHash, δηλαδή σε TeraHash ανά δευτερόλεπτο. Έχει καταστεί πλέον σχεδόν αδύνατον να πραγματοποιήσει κανείς μόνος του εξόρυξη κρυπτονομισμάτων με σκοπό να πάρει ως αμοιβή τα κρυπτονομίσματα που θα παράξει μέσα από αυτή τη διαδικασία και να βγεί κερδισμένος. Η επένδυση σε hardware που απαιτείται έχει πολύ μεγάλο κόστος. Μπορεί όμως οποιοσδήποτε να συμμετέχει στη διαδικασία της εξόρυξης, μέσω της συμμετοχής σε μια mining pool. Οι χρήστες εγγράφονται ως μέλη σε τέτοιες ιστοσελίδες, και συμμετέχουν από το σπίτι με το δικό τους εξοπλισμό. Το δίκτυο χρησιμοποιεί αθροιστικά την υπολογιστική ισχύ των συμμετεχόντων ώστε να πραγματοποιούνται εξορύξεις. Έτσι είναι πολύ πιο εφικτό το να κλείσει ένα μπλοκ και να δώσει τα αντίστοιχα Bitcoin ως ανταμοιβή στους χρήστες. Η αμοιβή κατανέμεται στους συμμετέχοντες ανάλογα με την υπολογιστική ισχύ που διαθέτουν και ένα μέρος κρατείται ως αμοιβή για την ιστοσελίδα. Για να κατανοήσουμε το μέγεθος της ισχύος, η πιο

γνωστή τέτοια ιστοσελίδα είναι η Slushpool, (https://slushpool.com/home/) η οποία διαθέτει υπολογιστική ισχύ της τάξης των τεσσάρων κόμμα εννέα ExaHash, ή τεσσάρων εκατομμυρίων εννιακοσίων χιλιάδων TeraHash, με σχεδόν 150.000 συμμετέχοντες, ενώ υπολογίζεται πως παράγει περίπου το 11% όλων των μπλοκ διεθνώς.

Το πλεονέκτημα που προσφέρει η συμμετοχή σε ένα mining pool, είναι το γεγονός πως υπάρχει η δυνατότητα απόκτησης ενός σταθερού εισοδήματος από ψηφιακά νομίσματα, που να βασίζεται στον χρόνο διεξαγωγής του mining και στην ποιότητα του εξοπλισμού. Γνωρίζοντας όμως την κατανομή με βάση τη συμμετέχουσα υπολογιστική ισχύ, είναι απαραίτητη η απόκτηση τουλάχιστον ενός ASIC ώστε να είναι συμφέρουσα η απόδοση της επένδυσης.

ΕΠΕΝΔΥΣΕΙΣ

Η Αρχή Χρηματοπιστωτικής Συμπεριφοράς του Ηνωμένου Βασιλείου (FCA), Ιανουάριο του 2021, προειδοποιεί τους επενδυτές για απώλεια των χρημάτων τους και πιθανή "φούσκα" στον τομέα της κρυπτοοικονομίας. Υπογραμμίζει ότι τα επενδυτικά προϊόντα τα οποία συνδέονται με τα ψηφιακά νομίσματα "ενέχουν πολύ σοβαρούς κινδύνους". Έχοντας γνώση ότι ορισμένες εταιρείες προσφέρουν επενδύσεις σε περιουσιακά στοιχεία σχετιζόμενα με ψηφιακά νομίσματα, δανεισμό ή επενδύσεις που συνδέονται με τα εν λόγω περιουσιακά στοιχεία και υπόσχονται παχυλές αποδόσεις, κρούει τον κώδωνα του κινδύνου, προειδοποιώντας εκείνους που κυνηγούν τα γρήγορα κέρδη, ότι «όσοι επενδύουν σε αυτούς τους τύπους προϊόντων, θα πρέπει να είναι έτοιμοι να χάσουν όλα τα χρήματά τους». [22] Η πρωτοβουλία της Αρχής Χρηματοπιστωτικής Συμπεριφοράς υλοποιείται εν μέσω πολύ ακραίων διακυμάνσεων στην αγορά των κρυπτογραφημένων νομισμάτων. Το bitcoin και άλλα ψηφιακά νομίσματα καταγράφουν μεγάλες απώλειες αλλά και απότομες εκτινάξεις σε νέα υψηλά επίπεδα ρεκόρ. Οι επενδυτές βλέπουν όλο και περισσότερο στα κρυπτονομίσματα "ευκαιρία", όπως είναι η επένδυση σε χρυσό εν μέσω περιόδων οικονομικών κρίσεων, απαξίωσης νομισμάτων και ανόδου του πληθωρισμού.

Οι πολύ μεγάλες **διακυμάνσεις** στη συναλλαγματική αξία του bitcoin και των άλλων κρυπτονομισμάτων, οδηγεί στο φόβο της "φούσκας", αφού το μεγαλύτερο στην κατηγορία των ψηφιακών νομισμάτων παγκοσμίως, μέσα σε μόνο δώδεκα μήνες έχει σημειώσει άνοδο ακόμα και της τάξης του 300%. Η FCA ήταν για τους παραπάνω λόγους ιδιαίτερα επιφυλλακτική με τα ψηφιακά νομίσματα, απαγορεύοντας την πώληση παραγώγων τους σε επενδυτές λιανικής. Προσεγγίζοντας, λοιπόν, από οικονομική σκοπιά την νέα αυτή αγορά, διαπιστώνει κανείς πως η εξέλιξη της τεχνολογίας επιφυλάσσει δραστικές αλλαγές στην οικονομία. Η αγορά των ψηφιακών νομισμάτων έρχεται ως ένα νέο χρηματιστήριο ψηφιακών αξιών με απίστευτες διακυμάνσεις, όπου ο καθένας μπορεί να επενδύσει. Εισάγονται στην αγορά όλο και περισσότερες νέες startup εταιρείες που λανσάρουν project εμπνευσμένα από το blockchain και διαθέτουν στους χρήστες τα δικά τους ψηφιακά νομίσματα που συνδέονται με το προϊόν/υπηρεσία τους. Η αρνητική όψη, έγκειται στην έλλειψη μίας σταθερής πηγής αξιόπιστης πληροφόρησης. Η αγορά αυτή των ψηφιακών νομισμάτων, λοιπόν, είναι εξαιρετικά απρόβλεπτη και χαρακτηρίζεται από αρκετά υψηλό ρίσκο όσον αφορά τον τομέα των επενδύσεων.

Στην ίδια ρότα, παρατηρούμε είσοδο των κρυπτονομισμάτων σε προιόντα της πραγματικής οικονομίας. Η Bakkt (πλατφόρμα η οποία συγκεντρώνει ψηφιακά περιουσιακά στοιχεία για να επιτρέψει την άμεση ρευστότητα και να δώσει τη δυνατότητα στους χρήστες να ανταλλάσσουν, να μεταφέρουν και να

πληρώνουν), ανακοίνωσε την έκδοση των **Bitcoin Futures και Options Contracts**, (παράγωγα επενδυτικά προϊόντα βασισμένα στο Bitcoin). [23]

Μέσω της συμμετοχής σε μια **επενδυτική πλατφόρμα κρυπτονομισμάτων**, (π.χ. Binance), μπορεί οποιοσδήποτε να διαμορφώσει το δικό του "χαρτοφυλάκιο" σε κρυπτονομίσματα, δημιουργώντας το ψηφιακό του πορτοφόλι. Ανάλογα με την εφαρμογή που χρησιμοποιείται, το ψηφιακό πορτοφόλι κάθε χρήστη αποτελεί κεντρικό στοιχείο στις συναλλαγές με κρυπτονομίσματα, καθώς περιέχει ένα ιδιωτικό κλειδί, το οποίο παρέχει τη δυνατότητα να ξοδέψει τα Bitcoins που είναι συνδεδεμένα με αυτό το πορτοφόλι. Το **ιδιωτικό κλειδί** είναι ένας μυστικός αριθμός μεγέθους 256 bit, που είναι συνδεδεμένος με μια διεύθυνση στο blockchain. Αποδεικνύει την κυριότητα και το δικαίωμα του χρήστη να χρησιμοποιεί τα κρυπτονομίσματα του πορτοφολιού του, μέσω κρυπτογραφικής υπογραφής.

Το ψηφιακό πορτοφόλι διαφέρει από τις πιστωτικές κάρτες, καθώς η εξουσία επί των συναλλαγών ανήκει αποκλειστικά στον χρήστη που κατέχει το ιδιωτικό κλειδί. Ο χρήστης μπορεί να δει το συνολικό του υπόλοιπο σε Bitcoin και να στείλει συγκεκριμένα ποσά σε άλλους χρήστες, όπως θα έκανε με ένα φυσικό πορτοφόλι. Το ιδιωτικό κλειδί αποθηκεύεται είτε στον υπολογιστή του χρήστη (σε πορτοφόλι λογισμικού), είτε σε απομακρυσμένους διακομιστές (διαδικτυακό πορτοφόλι), εξασφαλίζοντας την ιδιωτικότητα και την ασφάλεια των συναλλαγών. Η προστασία του ιδιωτικού κλειδιού είναι θεμελιώδης, καθώς παρέχει την ασφάλεια των συναλλαγών. Αν το ιδιωτικό κλειδί χαθεί ή κλαπεί, ο χρήστης χάνει την πρόσβαση στα κρυπτονομίσματα του. Αυτός είναι και ο λόγος που το ιδιωτικό κλειδί πρέπει να προστατεύεται και να διατηρείται ασφαλές.

2.2 ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΚΡΥΠΤΟΝΟΜΙΣΜΑ

Για να πραγματοποιήσουμε συναλλαγές με κρυπτονομίσματα, όπως το Bitcoin, απαιτείται ένα ψηφιακό πορτοφόλι. Αυτό το πορτοφόλι μπορεί να πάρει διάφορες μορφές:

1. **Εφαρμογή στον υπολογιστή**: Μπορεί να κατεβάσει κανείς ένα λογισμικό πορτοφολιού στον υπολογιστή του. Αυτή η εφαρμογή αποθηκεύει το ιδιωτικό κλειδί και επιτρέπει τη διαχείριση των κρυπτονομισμάτων και των συναλλαγών.

2. **Ειδική συσκευή (Hardware Wallet)**: Πρόκειται για μια συσκευή που σχεδιάστηκε αποκλειστικά για την ασφαλή αποθήκευση του ιδιωτικού κλειδιού και των κρυπτονομισμάτων. Το hardware wallet προσφέρει αυξημένη ασφάλεια, καθώς το κλειδί δεν εκτίθεται στο διαδίκτυο και τις απειλές που υπάρχουν σε υπολογιστές ή κινητά.

3. **Λογαριασμός σε σχετική υπηρεσία (Web Wallet)**: Οι χρήστες μπορούν να δημιουργήσουν έναν λογαριασμό σε μια διαδικτυακή υπηρεσία (όπως ανταλλακτήρια κρυπτονομισμάτων), όπου το πορτοφόλι τους αποθηκεύεται σε απομακρυσμένους διακομιστές. Παρόλο που αυτή η λύση είναι βολική, η ασφάλεια του πορτοφολιού εξαρτάται από τον πάροχο της υπηρεσίας.

Αυτές οι επιλογές προσφέρουν διάφορα επίπεδα ευκολίας και ασφάλειας, επιτρέποντας στους χρήστες να επιλέξουν ποια ταιριάζει καλύτερα στις ανάγκες τους.

- Πως πραγματοποιούνται οι συναλλαγές με κρυπτονομίσματα:

Ας υποθέσουμε πως ένας έμπορος κι ένας πελάτης πραγματοποιούν μια συναλλαγή χρησιμοποιώντας κρυπτονομίσματα. Θα πρέπει ο πελάτης να χρησιμοποιήσει το ψηφιακό του πορτοφόλι ώστε να πραγματοποιήσει την πληρωμή. Ένα αντίστοιχο ψηφιακό πορτοφόλι θα πρέπει να διαθέτει και ο έμπορος. Τα πορτοφόλια είναι φάκελοι που παρέχουν πρόσβαση σε πολλαπλές διευθύνσεις, οι οποίες έχουν τη μορφή: 2UJKLeIULjuvhkIOnjI780NjoiHUI345Gk. Υπάρχουν αξιόπιστες εφαρμογές διαθέσιμες για τη δημιουργία wallet, όπως για παράδειγμα η Electrum bitcoin wallet (https://electrum.org/#home). Σε κάθε διεύθυνση υπάρχει ένα υπόλοιπο κρυπτονομισμάτων, περίπου όπως στον τραπεζικό μας λογαριασμό αντιστοιχίζεται ένα υπόλοιπο σε χρήμα. Με τη διαφορά ότι οι χρήστες κρυπτονομισμάτων μπορούν να δημιουργούν νέα διεύθυνση για κάθε συναλλαγή που πραγματοποιούν. Ένας έμπορος, λοιπόν, μπορεί να διαθέσει τη διεύθυνση του πορτοφολιού του στους πελάτες του ή να δημιουργήσει έναν κωδικό QR για μεγαλύτερη ευκολία.

ΒΗΜΑ 1: Ο έμπορος δημιουργεί μια νέα διεύθυνση, δημιουργώντας ένα ζευγάρι κλειδιών, ένα δημόσιο κι ένα ιδιωτικό. Η διεύθυνση του εμπόρου αποτελεί ένα μοναδικό δημόσιο κλειδί και στο πορτοφόλι του αποθηκεύεται το ιδιωτικό. Το δημόσιο κλειδί επιτρέπει σε οποιονδήποτε να επιβεβαιώσει ότι ένα μήνυμα υπογεγραμμένο με το ιδιωτικό κλειδί είναι έγκυρο.

ΒΗΜΑ 2: Ο πελάτης δίνει εντολή μεταφοράς συγκεκριμένου ποσού κρυπτονομισμάτων σε αυτή τη νέα διεύθυνση του εμπόρου. Η εντολή του πελάτη εκτελείται, υπογράφοντας τη συναλλαγή με το ιδιωτικό κλειδί της διεύθυνσης του πελάτη. Έτσι οποιοσδήποτε στο δίκτυο μπορεί να χρησιμοποιήσει το δημόσιο κλειδί ώστε να επιβεβαιώσει ότι η συναλλαγή προέρχεται από έγκυρο χρήστη.

ΒΗΜΑ 3: Οι χρήστες που συμμετέχουν στη διαδικασία mining κατά τη χρονική διάρκεια της συναλλαγής, "δένουν" τη συναλλαγή σε ένα νέο μπλοκ. Ο miner που κλείνει το μπλοκ λαμβάνει ως αμοιβή τα αντίστοιχα κρυπτονομίσματα σε μια νέα διεύθυνση που δημιουργείται στο ψηφιακό του πορτοφόλι και η συναλλαγή επικυρώνεται και συμπεριλαμβάνεται στην αλυσίδα.

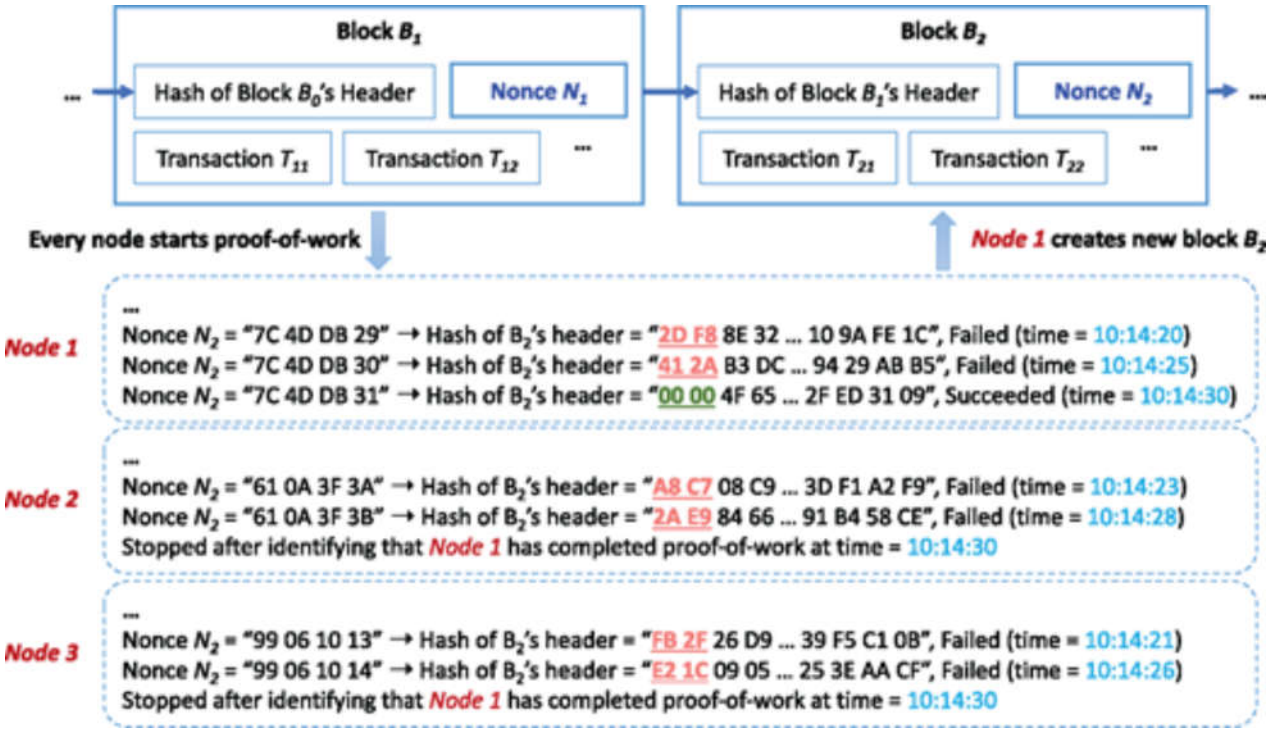
Για να αποκτήσουμε ένα ψηφιακό κρυπτονόμισμα η πιο απλή μέθοδος είναι να αγοράσουμε με την τρέχουσα ισοτιμία είτε σε δολλάρια είτε σε ευρώ. Υπάρχουν δεκάδες σελίδες στο διαδίκτυο που επιτρέπουν την αγορά κρυπτονομισμάτων. Υπάρχουν επίσης και αντίστοιχα ATM, τα οποία μας επιτρέπουν να αγοράσουμε κρυπτονομίσματα με την πιστωτική ή τη χρεωστική μας κάρτα ή και να πουλήσουμε κρυπτονομίσματα. Στο site coinatmradar.com, μπορούμε να εντοπίσουμε τα ATM κρυπτονομισμάτων στην Ελλάδα.

Πολλές επιχειρήσεις υποστηρίζουν πλέον συναλλαγές με κρυπτονομίσματα, έχοντας προσθέσει αυτό τον τρόπο συναλλαγών ως μέθοδο πληρωμής. Ο καταναλωτής σε αυτές τις επιχειρήσεις μπορεί να πραγματοποιήσει συναλλαγές χωρίς να χρειάζεται να μετατρέψει τα κρυπτονομίσματά του σε χρήμα. Η ιστοσελίδα weacceptbitcoin.gr, για παράδειγμα, καταγράφει δεκάδες επιχειρήσεις που δέχονται συναλλαγές με bitcoin σε όλη την Ελλάδα.

ΕΙΚΟΝΑ 7 - BITCOIN ATM - ΠΗΓΗ: https://www.bitcoin.com/bitcoin-atm/

2.3 Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

Ένα blockchain, όπως είπαμε, είναι ένα διανεμημένο ημερολόγιο, εντελώς ανοικτό για οποιονδήποτε. Η καταγραφή μιας πληροφορίας στο blockchain είναι διαδικασία μη αναστρέψιμη και ως εκ τούτου πάρα πολύ δύσκολο αυτή η πληροφορία να αλλάξει ή να αλλοιωθεί. Ένα μπλοκ σε μια αλυσίδα δεδομένων (blockchain) περιέχει: δεδομένα συναλλαγών, το hash του τρέχοντος μπλοκ και το hash του προηγούμενου μπλοκ. Αυτά τα στοιχεία είναι θεμελιώδη για την ακεραιότητα και την ασφάλεια της αλυσίδας. Όταν μια νέα συναλλαγή πραγματοποιείται, ενημερώνονται όλοι οι κόμβοι του δικτύου (peer-to-peer), προσθέτοντας τη συναλλαγή στα υπάρχοντα δεδομένα της αλυσίδας, σχεδόν σε πραγματικό χρόνο. Κάθε κόμβος διατηρεί ένα αντίγραφο της αλυσίδας, ενώ τα hashes διασφαλίζουν ότι κάθε μπλοκ συνδέεται αδιάρρηκτα με το προηγούμενο. Η ακεραιότητα της αλυσίδας διασφαλίζεται λοιπόν και με τον όγκο των συναλλαγών. Όσο πιο πολλοί οι κόμβοι, τόσο πιο ασφαλές το δίκτυο.



ΕΙΚΟΝΑ 8 - ΠΗΓΗ: Blockchain distributed ledger technologies for biomedical and healthcare applications, Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado - Journal of the American Informatics Association, Volume 24, Issue 6, Nov 2017, pages 1211-1220.

Τι συμβαίνει αν αφαιρέσουμε ή αλλάξουμε ένα μπλοκ;

Ας υποθέσουμε ότι αφαιρούμε το μπλοκ Νο545 από μια αλυσίδα που αποτελείται από 15.000 μπλοκ, ή επιχειρούμε να τροποποιήσουμε τα δεδομένα του. Σε αυτή την περίπτωση:

1. **Αποτυχία επαλήθευσης**: Η αλυσίδα δεν θα μπορέσει να επαληθευτεί. Κάθε μπλοκ περιέχει το hash του προηγούμενου μπλοκ, και αν αφαιρεθεί ή αλλάξει το μπλοκ No545, τότε το hash του μπλοκ 546 δεν θα ταιριάζει πλέον με το προηγούμενο, καταστρέφοντας την ακεραιότητα της αλυσίδας.

2. **Αλυσιδωτή επίδραση**: Η αλλαγή του hash στο μπλοκ 545 θα επηρεάσει όλα τα επόμενα μπλοκ, από το 546 μέχρι το 15.000, καθώς τα hashes είναι αλληλένδετα. Κάθε hash θα πρέπει να υπολογιστεί ξανά, κάτι που είναι εξαιρετικά δύσκολο και ενεργοβόρο, καθιστώντας την τροποποίηση της αλυσίδας πρακτικά αδύνατη.

3. **Ενημέρωση κόμβων**: Για να γίνει οποιαδήποτε αλλαγή στο blockchain, θα πρέπει όλοι οι κόμβοι του δικτύου να ενημερωθούν και να αποδεχθούν τη νέα εκδοχή της αλυσίδας. Αυτή η διαδικασία απαιτεί την πλειοψηφία των κόμβων να συμφωνήσουν (μηχανισμός συναίνεσης), κάτι που είναι εξαιρετικά δύσκολο να επιτευχθεί, ειδικά αν κάποιος προσπαθήσει να αλλάξει δεδομένα για δικό του όφελος.

4. **Ψηφιακή πιστοποίηση**: Κάθε συναλλαγή στο blockchain είναι ψηφιακά υπογεγραμμένη από τα εμπλεκόμενα μέρη, και οποιαδήποτε αλλαγή θα απαιτούσε να επαναληφθεί αυτή η διαδικασία πιστοποίησης από όλες τις πλευρές, προσθέτοντας ένα ακόμη επίπεδο δυσκολίας.

Συνοπτικά, η δομή του blockchain καθιστά την αλλοίωση των δεδομένων εξαιρετικά δύσκολη και ακριβή, τόσο σε χρόνο όσο και σε πόρους, διασφαλίζοντας έτσι την ακεραιότητα και την ασφάλεια των δεδομένων που περιέχει.

Ένα Bitcoin blockchain για παράδειγμα, αποθηκεύει τις λεπτομέρειες σχετικά με μια συναλλαγή μέσα στο μπλοκ ως εξής: Αποστολέας, Δέκτης και Ποσό νομισμάτων. Το κάθε μπλοκ χαρακτηρίζεται από ένα **hash**, που μπορούμε να αναπαραστήσουμε ως το δαχτυλικό αποτύπωμα του μπλοκ, αφού προσδιορίζει το περιεχόμενο του μπλοκ και είναι μοναδικό. Με τη δημιουργία ενός μπλοκ δεδομένων υπολογίζεται το αντίστοιχο hash. Οποιαδήποτε αλλαγή στα δεδομένα του μπλόκ, θα προκαλέσει και την αλλαγή του hash. Τα hashes, λοιπόν είναι πολύ χρήσιμα εαν σκοπεύει κανείς να ανιχνεύσει αλλαγές σε μπλοκ. Εάν αλλάξει το δαχτυλικό αποτύπωμα του μπλόκ, τότε αυτό δεν είναι πλέον το ίδιο μπλοκ. Το **τρίτο** στοιχείο μέσα σε κάθε μπλοκ, είναι το hash του προηγούμενου μπλοκ. Με αυτό τον τρόπο δημιουργείται μια αλυσίδα μπλοκ, που συνδέονται μεταξύ τους, προστατεύοντας αποτελεσματικά τα δεδομένα που περιέχουν. Ας πάρουμε ένα απλό παράδειγμα:

	1	2	3
HASH	1Z8F	6BQ1	3H4Q
PREVIOUS HASH	0 0 0 0	1Z8F	6BQ1

Παρατηρούμε ότι το μπλοκ 3 μας οδηγεί στο μπλοκ 2, και το μπλοκ 2 στο μπλοκ 1. Το πρώτο μπλοκ αποτελεί τη γεννήτρια. Αν υποθέσουμε ότι παραβιάζεται το μπλοκ 2, αυτό προκαλεί την αλλαγή hash του μπλοκ:

	1	2	3
HASH	1Z8F	H62Y	3H4Q
PREVIOUS HASH	0 0 0 0	1Z8F	6BQ1

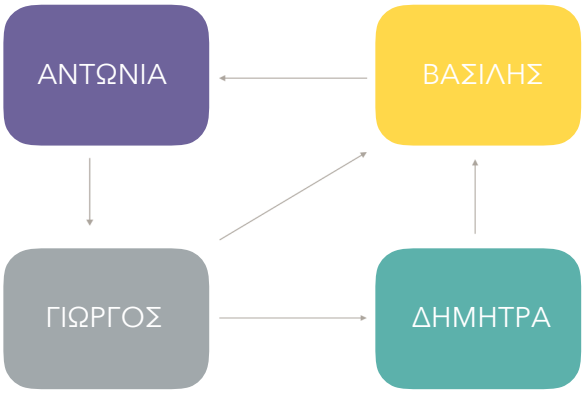
Ως αποτέλεσμα, το μπλοκ 3 και όλα τα επόμενα καθίστανται μη έγκυρα, εφόσον δεν αποθηκεύεται πλέον ένα έγκυρο hash του προηγούμενου μπλοκ. Άρα αλλάζοντας ένα μπλοκ, όλα τα ακόλουθα καθίστανται μη έγκυρα. Η χρήση όμως hash δεν αρκεί ώστε να αποτρέπεται η αλλοίωση. Η πρόοδος της τεχνολογίας σήμερα, έχει καταστήσει τους ηλεκτρονικούς υπολογιστές ικανούς να υπολογίζουν εκατοντάδες χιλιάδες hash ανά δευτερόλεπτο. Είναι εφικτό να παραβιαστεί ένα μπλοκ και να υπολογιστούν εκ νέου τα hash των επόμενων μπλοκ ώστε να πραγματοποιηθεί επαναφορά της αλυσίδα μπλόκ. Για να μετριαστούν τέτοιες ενέργειες, τα μπλοκ περιέχουν ένα μηχανισμό που ονομάζεται "proof of work". Ο μηχανισμός αυτός επιβραδύνει τη δημιουργία νέων μπλοκ. Στην περίπτωση των Bitcoin, χρειάζονται περίπου δέκα λεπτά για τον υπολογισμό της απαιτούμενης "απόδειξης εργασίας" ώστε να προστεθεί ένα ακόμα μπλοκ στην αλυσίδα. Αυτός ο μηχανισμός καθιστά εξαιρετικά δύσκολη την παραβίαση, διότι εαν παραβιαστεί ένα μπλοκ, θα πρέπει να υπολογιστεί ξανά η "απόδειξη εργασίας" για όλα τα επόμενα μπλοκ.

Έτσι η ασφάλεια ενός μπλοκ προέρχεται από τη δημιουργική χρήση του hash και του μηχανισμού "proof of work". Υπάρχει όμως ακόμη ένας μηχανισμός ασφαλείας. Και αυτός είναι η διανομή τους. Αντί να χρησιμοποιείται μια κεντρική οντότητα που διαχειρίζεται την αλυσίδα, χρησιμοποιείται ένα peer-to-peer δίκτυο, όπου όλοι επιτρέπεται να συμμετέχουν. Με τη συμμετοχή ενός νέου χρήστη, ο χρήστης παραλαμβάνει πλήρες αντίγραφο ολόκληρης της αλυσίδας. Όταν λοιπόν δημιουργήσει ένα νέο μπλοκ, αυτό αποστέλλεται σε όλους όσους συμμετέχουν στο δίκτυο. Στη συνέχεια κάθε κόμβος επαληθεύει το μπλοκ, ώστε να επιβεβαιωθεί ότι το δίκτυο δεν έχει παραβιαστεί. Εάν η προσθήκη είναι έγκυρη, κάθε κόμβος προσθέτει το νέο μπλοκ στην αλυσίδα. Όλοι οι κόμβοι του δικτύου δημιουργούν με τον τρόπο αυτό, αυτό που ονομάζουμε συναίνεση ή consensus. Διαμορφώνεται δηλαδή συμφωνία σχετικά με τα μπλοκ που είναι έγκυρα και αυτά που δεν είναι. Τα μπλοκ στα οποία εντοπίζεται αλλοίωση, θα απορριφθούν από άλλους κόμβους στο δίκτυο. Προκειμένου, λοιπόν, να παραβιαστεί αποτελεσματικά μια αλυσίδα, θα πρέπει να παραβιαστούν όλα τα μπλοκ της αλυσίδας, να επαναληφθεί το "proof of work" κάθε μπλοκ, και να ανακτηθεί έλεγχος άνω του 50% του δικτύου.

Μόνο τότε μπορεί το παραβιασμένο μπλοκ να γίνει αποδεκτό από όλους ώστε να αποτελέσει μέρος της αλυσίδας. Κάτι σχεδόν αδύνατον.

Ας δούμε λοιπόν τι ακριβώς συμβαίνει πρακτικά κατά την πραγματοποίηση κρυπτοσυναλλαγών. Έστω τέσσερις χρήστες, η Αντωνία, ο Βασίλης, ο Γιώργος και η Δήμητρα. Οι χρήστες αυτοί διατηρούν έναν κατάλογο, στον οποίο αναγράφονται όλες οι συναλλαγές που πραγματοποιούν μεταξύ τους. Ο κατάλογος αυτός είναι κοινόχρηστος και δημόσιος, όπως μια ιστοσελίδα στην οποία οποιοσδήποτε μπορεί να προσθέσει περιεχόμενο.

ΚΑΤΑΛΟΓΟΣ ΣΥΝΑΛΛΑΓΩΝ
Η ΑΝΤΩΝΙΑ ΧΡΩΣΤΑΕΙ 20$ ΣΤΟ ΒΑΣΙΛΗ
Ο ΒΑΣΙΛΗΣ ΧΡΩΣΤΑΕΙ 40$ ΣΤΗ ΔΗΜΗΤΡΑ
Η ΔΗΜΗΤΡΑ ΧΡΩΣΤΑΕΙ 10$ ΣΤΟ ΓΙΩΡΓΟ
Ο ΓΙΩΡΓΟΣ ΧΡΩΣΤΑΕΙ 5$ ΣΤΗΝ ΑΝΤΩΝΙΑ
Ο ΒΑΣΙΛΗΣ ΧΡΩΣΤΑΕΙ 45$ ΣΤΟ ΓΙΩΡΓΟ
.....
.....
.....



Χρειάζεται όμως κάποιου είδους εξασφάλιση, ότι οι συναλλαγές που συμπληρώνονται στον κατάλογο είναι αληθείς και συμφωνούν για την πραγματοποίησή τους και τα δυο μέρη. Δίπλα λοιπόν σε κάθε συναλλαγή, προστίθεται μια ψηφιακή υπογραφή που υποδηλώνει πως ο χρήστης στον οποίο αναφέρεται γνωρίζει για τη συναλλαγή αυτή και την εγκρίνει. Η ψηφιακή υπογραφή δημιουργείται με την έκδοση ενός ζεύγους κλειδιών, ενός δημόσιου και ενός ιδιωτικού. Σε αντίθεση με τη συμμετρική κρυπτογράφηση, όπου η κρυπτογράφηση και η αποκρυπτογράφηση πραγματοποιούνται με το ίδιο κλειδί, στην ασύμμετρη κρυπτογράφηση χρειαζόμαστε δύο κλειδιά. Ο χρήστης ο οποίος επιθυμεί να κρυπτογραφήσει το μήνυμά του και να το στείλει σε κάποιον άλλον, δημιουργεί ένα ζεύγος κλειδιών. Τα κλειδιά αυτά συνδέονται μαθηματικά. Το ένα χρησιμοποιείται για κρυπτογράφηση και το ιδωτικό για αποκρυπτογράφηση του μηνύματος. Το ιδιωτικό κλειδί λοιπόν, πρέπει να περιφρουρείται. Έτσι αν η Αντωνία θέλει για παράδειγμα να συνομιλήσει ιδιωτικά με τη Δήμτρα, δημιουργεί ένα ζεύγος κλειδιών και μοιράζεται με τη Δήμητρα το δημόσιο κλειδί της. Η Δήμητρα της στέλνει το μήνυμά της κρυπτογραφημένο με το δημόσιο κλειδί της Αντωνίας και η Αντωνία αποκρυπτογραφεί με το ιδιωτικό της κλειδί το μήνυμα. Αντίστοιχα, η Δήμητρα δημιουργεί ένα ζεύγος κλειδιών και μοιράζεται με την Αντωνία το δημόσιο κλειδί της ώστε να κρυπτογραφεί τα μηνύματα που της στέλνει και με το ιδιωτικό της κλειδί τα αποκρυπτογραφεί. Πώς όμως γνωρίζει η Αντωνία ότι το μήνυμα που παρέλαβε είναι έγκυρο και προέρχεται όντως από τη Δήμητρα; Αυτό επιτυγχάνεται με τις υπογραφές. Οι ψηφιακές υπογραφές επιβεβαιώνουν πως το μήνυμα που παρελήφθη, στάλθηκε από το άτομο που πιστεύεις ότι το έστειλε, αφού συνδέονται με το ιδιωτικό κλειδί ως εξής:

ΑΠΟΣΤΟΛΕΑΣ :

1. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη.
2. Υπογράφει το μήνυμα με το δικό του ιδιωτικό κλειδί.

ΠΑΡΑΛΗΠΤΗΣ :

1.Επικυρώνει την υπογραφή του Αποτολέα, με το δημόσιο κλειδί του Αποστολέα.
2. Αποκρυπτογραφεί το μήνυμα με το δικό του ιδιωτικό κλειδί.

Όταν κρυπτογραφείται το μήνυμα, συνδέεται με τη ψηφιακή υπογραφή του Αποστολέα και έτσι η παραμικρή παρεμβολή μεταβάλλει και την ψηφιακή υπογραφή του, καθιστώντας το μήνυμα μη έγκυρο ή ύποπτο. Συνήθως κατά την αποκρυπτογράφηση μπορούμε να δούμε την ένδειξη "Good Signature", που σημαίνει not modified, ότι το μήνυμά μας δηλαδή είναι έγκυρο και ο Αποστολέας είναι έγκυρος. Οι πιθανότητες αλλοίωσης της ψηφιακής υπογραφής χωρίς να γνωρίζει κανείς το ιδιωτικό κλειδί είναι μηδαμηνές. Συγκεκριμένα θα πρέπει να κάνει τυχαίο έλεγχο χρησιμοποιώντας το δημόσιο κλειδί. Αν υποθέσουμε πως το μέγεθος της υπογραφής είναι 256 bit, τότε οι πιθανές υπογραφές είναι 2^256.

Επιστρέφοντας στο παράδειγμα με τον Κατάλογο, εκτός του ζητήματος της εγκυρότητας του περιεχομένου του μηνύματος και των συμβαλλόμενων μερών, χρειάζεται η διασφάλιση της μοναδικότητας της κάθε συναλλαγής. Κάθε συναλλαγή θα πρέπει να χαρακτηρίζεται από κάποιο αναγνωριστικό που την καθιστά μοναδική. Κάθε συναλλαγή λοιπόν απαιτεί μια νέα ψηφιακή υπογραφή από τον Αποστολέα.

Έχουμε λοιπόν στον Κατάλογό μας τον αριθμό της συναλλαγής, τη σειρά με την οποία πραγματοποιούνται οι συναλλαγές και την υπογραφή των αντισυμβαλλόμενων σε κάθε συναλλαγή. Ο κατάλογος αυτός όμως, δεν μπορεί να ανήκει σε κάποιον ιστότοπο ή οι κανόνες του να καθορίζονται από κάποιον "ιδιοκτήτη". Όλοι οι χρήστες πρέπει να έχουν ένα **αξιόπιστο αντίγραφο** του καταλόγου, με όλες τις πραγματοποιημένες συναλλαγές. Η εγκυρότητα των καταλόγων πιστοποιείται μέσω της υπολογιστικής εργασίας (proof of work). Εδώ εισέρχονται οι κρυπτογραφικές συναρτήσεις κατακερματισμού. Εαν η **υπολογιστική εργασία** χρησιμοποιείται ως **βάση εμπιστοσύνης**, τότε οι δόλιες συναλλαγές και οι αντικρουόμενοι κατάλογοι θα πρέπει να απαιτούν έναν ανέφικτο αριθμό υπολογισμών προκειμένου να ληφθούν υπόψιν ως έγκυροι.

Το **πρώτο μπλοκ** της αλυσίδας, κρυπτογραφεί τη λίστα των συναλλαγών χρησιμοποιώντας έναν κρυπτογραφικό αλγόριθμο κατακερματισμού, όπως τον SHA-256, και εξάγει ένα Hash. Κάθε νέο μπλοκ περιέχει το Hash του προηγούμενου, τις νέες συναλλαγές και ένα nonce. Το nonce, είναι μια συντομογραφία για τον "αριθμό που χρησιμοποιείται μόνο μία φορά". Είναι ένας αριθμός που προστίθεται σε ένα κατακερματισμένο μπλοκ του blockchain. Κάθε φορά επαναπροσδιορίζεται ώστε να πληρεί τους περιορισμούς του επιπέδου δυσκολίας που ορίζονται από το πρωτόκολλο του εκάστοτε κρυπτονομίσματος. Σύμφωνα με το πρωτόκολλο του Bitcoin για παράδειγμα, ο αριθμός αυτός αλλάζει περιοδικά, ώστε ο χρόνος εξόρυξης κάθε μπλοκ να είναι τα δέκα λεπτά. Το Ethereum ορίζει αντίστοιχο χρόνο τα δεκαπέντε δευτερόλεπτα, το Litecoin τα δυόμιση λεπτά και ούτω καθεξής. Έτσι με την είσοδο περισσότερων miners στο δίκτυο, η εξόρυξη γίνετσι όλο και δυσκολότερη, απαιτεί όλο και μεγαλύτερο όγκο υπολογιστικής εργασίας.

Το **nonce** είναι ο αριθμός τον οποίο αναζητούν οι ανθρακωρύχοι ώστε να "εξορύξουν" τα μπλοκ. Η διαδικασία αυτή απαιτεί υπολογιστική εργασία η οποία αποτελεί την απόδειξη εργασίας.

ΚΑΤΑΛΟΓΟΣ ΣΥΝΑΛΛΑΓΩΝ

3. …….
4. ……..
5. Η ΑΝΤΩΝΙΑ ΧΡΩΣΤΑΕΙ 20$ ΣΤΟ ΒΑΣΙΛΗ - Βασίλης
6. Ο ΒΑΣΙΛΗΣ ΧΡΩΣΤΑΕΙ 40$ ΣΤΗ ΔΗΜΗΤΡΑ - Δήμητρα
7. Η ΔΗΜΗΤΡΑ ΧΡΩΣΤΑΕΙ 10$ ΣΤΟ ΓΙΩΡΓΟ - Γιώργος
8. Ο ΓΙΩΡΓΟΣ ΧΡΩΣΤΑΕΙ 5$ ΣΤΗΝ ΑΝΤΩΝΙΑ - Αντωνία
9. Ο ΒΑΣΙΛΗΣ ΧΡΩΣΤΑΕΙ 45$ ΣΤΟ ΓΙΩΡΓΟ - Γιώργος
10. ……
11. …….
12. …….

Η σωστή αλυσίδα, η αλυσίδα με την οποία συμφωνούν οι χρήστες, και είναι έγκυρη, είναι αυτή η οποία ενσωματώνει το μεγαλύτερο όγκο υπολογιστικής εργασίας.

Ο Κατάλογός μας, λοιπόν, χωρίζεται σε μπλοκ, και κάθε μπλοκ αποτελείται τελικά από μια λίστα συναλλαγών κρυπτογραφημένων σε ένα Hash, το Hash του προηγούμενου μπλοκ, και τον αριθμό που αποδεικνύει την υπολογιστική εργασία, το nonce. Η κάθε συναλλαγή θεωρείται έγκυρη μόνο όταν περιέχει ψηφιακή υπογραφή του Αποστολέα. Το nonce καθορίζει τον αριθμό των μηδενικών με τα οποία ξεκινάει το εξαγόμενο Hash του μπλοκ, και είναι αυτό που καθιστά το κάθε μπλοκ έγκυρο. Το Hash του προηγούμενου μπλοκ ορίζει τη σειρά των μπλοκ στην αλυσίδα και διασφαλίζει, όπως αναλύσαμε και παραπάνω, τη διατήρηση των ορθών δεδομένων στην αλυσίδα. Το μπλοκ περιέχει στη λίστα συναλλαγών και την αμοιβή του χρήστη που θα καταβάλει την υπολογιστική εργασία ώστε να το προσθέσει στην αλυσίδα, που είναι και η μοναδική συναλλαγή που δεν απαιτεί ψηφιακή υπογραφή από κάποιον αποστολέα και εισάγει νέα νομίσματα στο περιβάλλον της ψηφιακής αυτής οικονομίας. Με τον τρόπο αυτό, στην περίπτωση ύπαρξης δυο ή περισσότερων αλυσίδων με αντικρουόμενα δεδομένα, έγκυρη θεωρείται η αλυσίδα η οποία ενσωματώνει το μεγαλύτερο όγκο υπολογιστικής εργασίας. Το δεδομένο αυτό δημιουργεί αποκεντρωμένη συναίνεση από την πλευρά των χρηστών.

Η τεχνολογία των blockchain εξελίσσεται διαρκώς. Εξέλιξη αποτέλεσε η δημιουργία των "έξυπνων συμβολαίων". Τα προγράμματα που αποθηκεύονται στο blockchain και μπορούν να χρησιμοποιηθούν για αυτόματες συναλλαγές υπό συγκεκριμένες προυποθέσεις.

Η ανάπτυξη της τεχνολογίας blockchain, προσέλκυσε το ενδιαφέρον πολλών τομέων της οικονομίας όπως αναλύθηκε στο πρώτο μέρος, καθώς βρίσκει πεδίο εφαρμογής σε αυτούς. Ταυτόχρονα, δίνει λύσεις για big data, smart contracts, κρυπτονομίσματα, ασφάλεια προσωπικών δεδομένων, ψηφιακή διακυβέρνηση, ναυτιλία, μεταφορές, εφοδιαστική αλυσίδα και πολλά άλλα, καθιστώντας τις συναλλαγές μας πιο γρήγορες και ασφαλείς.

2.4 COINS & TOKENS

Η κρυπτοοικονομία περιλαμβάνει νομίσματα - coins - και tokens. Τα coins, είναι ανεξάρτητες οντότητες που λειτουργούν ως πλατφόρμα. Στην κατηγορία αυτή ανήκουν ενδεικτικά τα Bitcoin, Bitcoin cash, Ethereum. Τα tokens, είναι επί της ουσίας "έξυπνα συμβόλαια" και απαιτείται η ύπαρξη κάποιας άλλης πλατφόρμας ώστε να λειτουργήσουν. Η πλειοψηφία των tokens βασίζονται στο Ethereum, όπως τα augur, omisego, golem. Στην ιστοσελίδα coinmarketcap.com , βλέπουμε όλα τα κρυπτονομίσματα σε κυκλοφορία. Αυτή τη στιγμή βρίσκονται σε κυκλοφορία 4.026 tokens και 1.085 coins.

Η εμφάνιση ενός νέου κύματος έργων που βασίζονται σε blockchain έφερε και το νέο πεδίο των Tokenomics (από economics). Σε γενικές γραμμές ένα token είναι ένα σύμβολο, που αναπαριστά μια έννοια ή κάτι μοναδικό. Στο χώρο της κρυπτοοικονομίας, υπάρχουν πολλές πλευρές στη χρήση τους που μπορούν να τα καθιστούν χρήσιμα εργαλεία. Μπορούν να χρησιμοποιηθούν ως :

- τυπικό συνάλλαγμα, μέσο μετάδοσης αξίας, μέσο αποθήκευσης πλούτου.

- μέσο διασφάλισης της συναίνεσης και της εγκυρότητας των συναλλαγών και των δεδομένων.

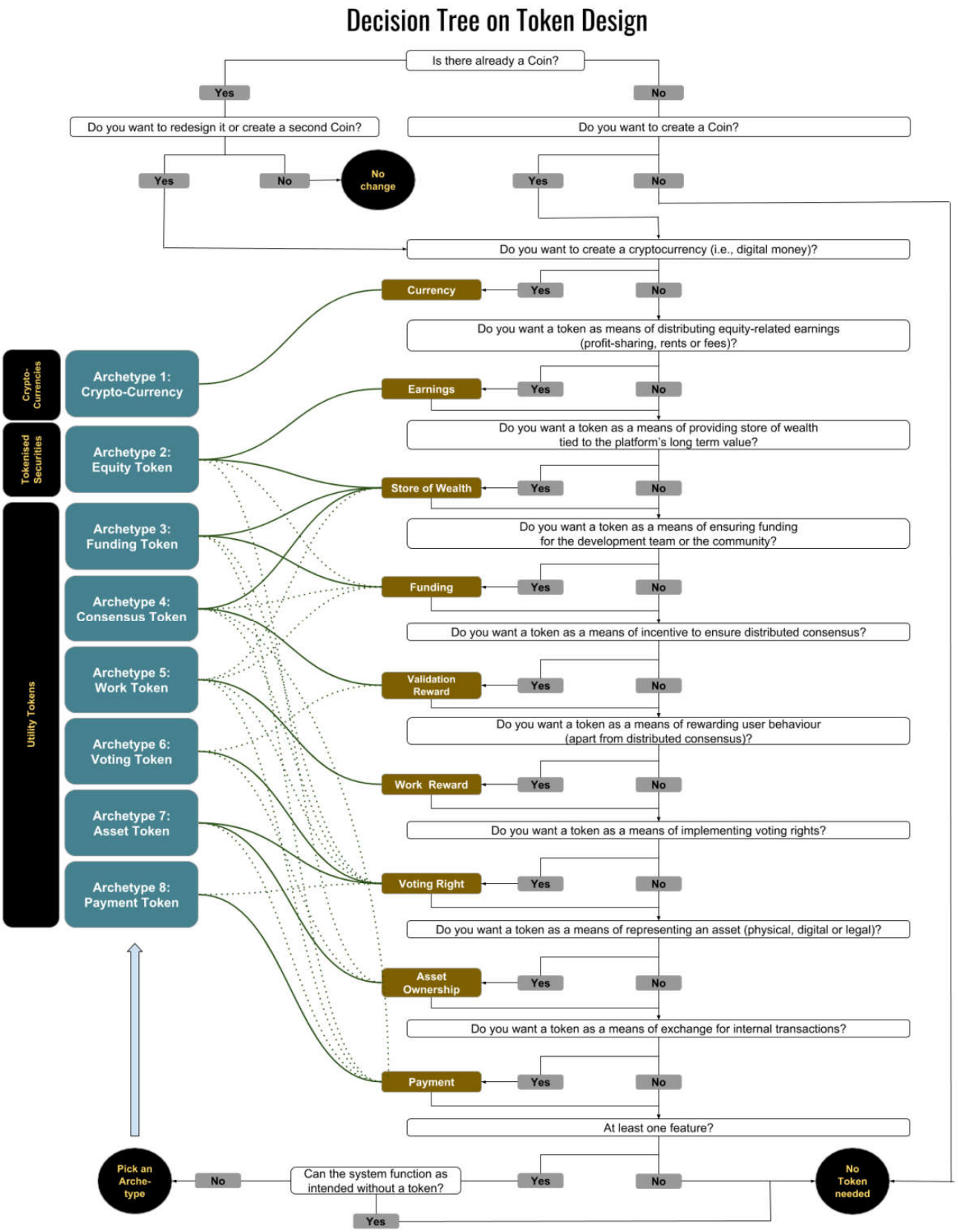
- κίνητρο για την προώθηση της χρήσης μιας πλατφόρμας, επιτρέποντας τη χρήση τους μέσα στη συγκεκριμένη πλατφόρμα.

- εργαλείο διαχείρισης, αποτρέποντας ανεπιθύμητα μηνύματα ή παρέχοντας δυνατότητα συμμετοχής σε ανάπτυξη κάποιας πλατφόρμας.

- χρηματοδοτικό μέσο, χρησιμοποιώντας τα έσοδα από πώληση token για τη χρηματοδότηση της ομάδας ανάπτυξης ή της κοινότητας.

- μέσο κατανομής κερδών, μερισμάτων ή ισοδύναμων.

Τα token μπορούν να χρησιμοποιηθούν σε ευρεία γκάμα πρακτικών εφαρμογών και να δώσουν λύσεις σε ζητήματα εμπιστοσύνης και εγκυρότητας, να συμβάλλουν στο σχεδιασμό της στρατηγικής των επιχειρηματικών μονάδων, του επιχειρηματικού μοντέλου που θα ακολουθείται. Σε έναν όμιλο επιχειρήσεων, για παράδειγμα, ένα token θα μπορούσε να υιοθετηθεί ως bonus για εργαζόμενους και στελέχη και ως προνόμιο για τους πελάτες παρέχοντάς τους πρόσβαση σε ξεχωριστές υπηρεσίες από τις συμβατικές, να αποτελεί μέσο κατανομής κερδών στα στελέχη της επιχείρησης ή να χρησιμοποιείται ως κίνητρο. Σε κάθε περίπτωση, τα tokens παρέχουν τη δυνατότητα ανάπτυξης απόλυτα συμβατών εφαρμογών με το επιχειρησιακό μοντέλο και τους στρατηγικούς στόχους της κάθε επιχειρηματικής μονάδας, κάτι που στο μέλλον αναμένεται να προσθέσει αξία συνολικά στην τεχνολογία blockchain. [24]



ΕΙΚΟΝΑ 9 - ΠΗΓΗ; To Token or not to Token: Tools for Understanding Blockchain Tokens - Oliveira, Luis ; Zavolokina, Liudmila ; Bauer, Ingrid ; Schwabe, Gerhard - Zurich Open Repository and Archive University of Zurich Main Library

2.5 Η ΕΞΕΛΙΞΗ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ - BITCOIN, ETHEREUM, CARDANO

Από τη στιγμή που εμφανίστηκε το Bitcoin, τα κρυπτονομίσματα έχουν εξελιχθεί τεχνολογικά και προγραμματιστικά, ώστε να βελτιώνεται η λειτουργία τους, να καλύπτονται αδυναμίες που εμφανίζοντια κατά τη χρήση αλλά και νέες ανάγκες που προκύπτουν.

BITCOIN - ΠΡΩΤΗ ΓΕΝΙΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Η πρώτη γενιά κρυπτονομισμάτων, το Bitcoin, άνοιξε το δρόμο ενός αποκεντρωμένου δικτύου συναλλαγών σε περιβάλλον ψηφιακής οικονομίας. Η δημιουργία, το πρωτόκολλο και η χρήση του αποτέλεσαν πραγματική καινοτομία στον τομέα της πληροφορικής, της οικονομίας και της κρυπτογραφίας, όπως αναλύσαμε σε προηγούμενες παραγράφους. Με το Bitcoin δημιουργήθηκε το πρώτο αποκεντρωμένο δίκτυο συναλλαγών. Όμως, η εξόρυξη Bitcoin με τον αλγόριθμο συναίνεσης Proof of Work, απαιτεί όλο και μεγαλύτερα ποσά ενέργειας, κάτι που οδηγεί σε συγκεντροποίηση του νομίσματος σε ισχυρούς επιχειρηματικούς ομίλους που διαθέτουν τα κεφάλαια και τη δυνατότητα επενδύσεων στην αγορά κρυπτονομισμάτων. Κάτι αντίθετο με τη φιλοσοφία των κρυπτονομισμάτων που περιστρέφεται γύρω από το αποκεντρωμένο δίκτυο και την ανωνυμία του χρήστη. Σε αυτή τη βάση αναπτύχθηκε ένας νέος αλγόριθμος συναίνεσης, Proof of Stake, που χρησιμοποιήθηκε σε επόμενα κρυπτονομίσματα. Ο αλγόριθμος αυτός δεν επιτρέπει σε όλους να κάνουν mining. Επιλέγεται τυχαία κάποιος κόμβος, ο οποίος δεν πραγματοποιεί εξόρυξη (mining), αλλά "σφυρηλάτηση" του μπλοκ (forging/minting). Για τον προγραμματισμό του Bitcoin χρησιμοποιήθηκε γλώσσα προγραμματισμού Turing Incomplete, που σημαίνει πως αντιλαμβάνεται μικρό εύρος εντολών. Ένα πιο πολύπλοκο σύστημα απαιτεί διαφορετική γλώσσα προγραμματισμού, διαφορετικό δίκτυο υπολογιστών. Έτσι δημιουργήθηκε το Ethereum.

ΕΙΚΟΝΑ 10 - Bitcoin logo, ΠΗΓΗ: bitcoin.otg

ETHEREUM - ΔΕΥΤΕΡΗ ΓΕΝΙΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Το Ethereum έρχεται μετά το Bitcoin, να θέσει νέους κανόνες στην αγορά κρυπτονομισμάτων. Η είσοδος των έξυπνων συμβολαίων δεν ήταν ακριβώς καινοτομία, αφού και το Bitcoin χρησιμοποιεί έξυπνα συμβόλαια. Το Ethereum δημιουργήθηκε το 2013 από τον Vitalik Buterik, συνιδρυτή του Bitcoin Magazine, και εισήλθε στην αγορά το 2014. Η πλατφόρμα Ethereum, δημιουργήθηκε με σκοπό τη δημιουργία αποκεντρωμένων εφαρμογών (Dapps- Decentralized Applications). Η γλώσσα προγραμματισμού που χρησιμοποιεί ονομάζεται Solidity, και είναι γλώσσα Turing Complete. Το νόμισμα της πλατφόρμας ονομάστηκε Ether. Οι προγραμματιστές μπορούν να συντάσσουν ένα έξυπνο συμβόλαιο χρησιμοποιώντας τη γλώσσα Solidity και έπειται η πλατφόρμα του Ethereum, το εκτελεί. Όταν ένα συμβόλαιο συντεθεί στην πλατφόρμα Ethereum, δεν

μπορεί να μεταβληθεί, να διορθωθεί ή να ανασταλεί. Εκτελείται αυτόνομα. Εδώ παρατηρούμε το πλεονέκτημα αλλά ταυτόχρονα και μειονέκτημα της πλατφόρμας, το γεγονός ότι ο συντάκτης του συμβολαίου, ιδιαίτερα όταν το εν λόγω συμβόλαιο είναι περίπλοκο, θα πρέπει να λάβει υπόψιν όλες τις πιθανές εκβάσεις και να τις συμπεριλάβει στον κώδικά του ώστε το συμβόλαιο να δρα σύμφωνα με τις προθέσεις του συντάκτη.

Ένα πορτοφόλι Ethereum, λειτουργεί περίπου όπως και ένα πορτοφόλι Bitcoin. Υπάρχει ένα ιδιωτικό κλειδί και μια δημόσια διεύθυνση που χρησιμοποιούνται για τις συναλλαγές. Με τη διαφορά όμως πως στην περίπτωση του Ethereum, ο χρήστης χειρίζεται ένα λογαριασμό ή **Externally Owned Account (EOA**), ο οποίος χρησιμοποιείται για τη σύνταξη και εκτέλεση **έξυπνων συμβολαίων**. Εκτός από τις διευθύνσεις EOA, υπάρχουν και οι Contract Accounts, διευθύνσεις που διαφέρουν δομικά από το πορτοφόλι και σχετίζονται περισσότερο με σύνταξη κώδικα, μπορούν όμως να δέχονται και να αποστέλλουν Ether. Στην περίπτωση του Bitcoin, κατά τις συναλλαγές μεταφέρεται αξία. Στην περίπτωση του Ether, εκτός από μεταφορά αξίας, οι συναλλαγές μπορούν να χρησιμοποιηθούν για σύνθεση ή εκτέλεση συμβολαίων. Τα Ethereum πορτοφόλια χωρίζονται σε ολοκληρωμένες εκδοχές (full nodes) και σε light (light nodes). Τα πορτοφόλια ολοκληρωμένων κόμβων (full nodes), είναι αυτά τα οποία λαμβάνουν τις πληροφορίες συναλλαγών ολόκληρης της αλυσίδας και εκτελούν τον κώδικα που τις συνοδεύει. Υπάρχουν αρκετά προγράμματα που "τρέχουν" ολοκληρωμένους κόμβους, όπως το Geth, του Ethereum Foundation, που αφορά κυρίως προγραμματιστές, το Mist, που επιτρέπει και σε μη έμπειρους χρήστες να συμμετέχουν στην πλατφόρμα και το Parity, που αφορά περισσότερο επαγγελματίες. Οι μερικοί κόμβοι από την άλλη, (light nodes), είναι αρκετά πιο εύχρηστοι, αφού απαιτείται λιγότερος χώρος για τη λειτουργία τους και μπορούν να λειτουργούν ακόμα και μέσω εφαρμογών σε κινητά τηλέφωνα.

ΕΙΚΟΝΑ 11 - Ethereum logo, ΠΗΓΗ: ethereum.org

CARDANO - ΤΡΙΤΗ ΓΕΝΙΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Το Cardano, εμφανίστηκε το Σεπτέμβρη 2017, μετά από δουλειά δύο ετών. Λέγεται πως αποτελεί την τρίτη γενιά κρυπτονομισμάτων μετά το Bitcoin και το Ethereum. Έρχεται να διορθώσει τρεις παραμέτρους: α) βιωσιμότητα (sustainability) , β) διαλειτουγικότητα (interoperability), γ) επεκτασιμότητα (scalability).

α) **Βιωσιμότητα:** Η ομάδα που εμπνεύστηκε το Cardano, δημιούργησε ένα θησαυροφυλάκιο. Ένα έξυπνο συμβόλαιο, που απελευθερώνει πόρους σε όποιον συμβάλλει στη βελτίωση του πρωτοκόλλου του Cardano.

Ο προγραμματιατής υποβάλλει γραπτά πρόταση, συμπεριλαμβάνοντας τις ιδέες του και τη χρηματοδότηση που απαιτείται για την πραγματοποίησή τους και έπειτα η κοινότητα αποφασίζει ποια πρόταση θα πρέπει να υλοποιηθεί. Η ιδέα του θησαυροφυλακίου, μπορεί να στηρίξει τη βιωσιμότητα του Cardano, καθώς θα πραγματοποιείται συνεχώς έρευνα και θα αναπτύσσεται η αλυσίδα τεχνολογικά.

β) **Διαλειτουργικότητα**: Η ομάδα του Cardano παίρνει υπόψιν το γεγονός ότι υπάρχουν πολλά κρυπτονομίσματα και η ιδέα είναι να υπάρχει ένα κρυπτονόμισμα που να μπορεί να συνδιαλλάσσεται με τα υπόλοιπα χωρίς μεσάζοντες. Να μπορούν να μεταφέροντια αξίες από μια αλυσίδα σε μια άλλη. Ταυτόχρονα, προκειμένου να συνδέεται με την πραγματική οικονομία, δίνει τη δυνατότητα στο χρήστη να εισάγει τα δεδομένα του, ταυτότητα, αιτία συναλλαγής και ότι άλλο χρειάζεται προκειμένου να μπορεί να χρησιμοποιεί το Cardano ακόμα και μέσω τραπεζικών ιδρυμάτων.

γ) **Επεκτασιμότητα (Scalability**): Το κομμάτι αυτό σχετίζεται με τρεις παράγοντες. Το χρόνο εκτέλεσης συναλλαγών, (συναλλαγές ανά δευτερόλεπτο), την αποθήκευση δεδομένων και το εύρος ζώνης του δικτύου, (ταχύτητα ροής δεδομένων). Ο χρόνος εκτέλεσης συναλλαγών είναι δεδομένο πως απαιτεί μεταβολές στην περίπτωση των κρυπτονομισμάτων. Προκειμένου να καθιερωθεί ένα κρυπτονόμισμα ως παγκόσμιο μέσο πληρωμών, είναι αυτονόητο πως ο χρόνος διεξαγωγής των συναλλαγών πρέπει να είναι μικρός. Το Cardano έρχεται να λύσει το πρόβλημα με τον αλγόριθμο Ouroboros, που χρησιμοποιεί αλγόριθμο Proof of Stake αντί για αλγόριθμο Proof of Work, όπως το Bitcoin. Η διαδικασία mining με τον αλγόριθμο Proof of Work, απόδειξης μόχθου δηλαδή, αποτελεί αιτία σπατάλης τεράστιου ποσού ενέργειας, υπολογιστικής και ηλεκτρικής. Το Cardano από την άλλη, δεν επιτρέπει σε όλους να κάνουν mining. Το δίκτυο επιλέγει κάποιους κόμβους που θα λειτουργούν ως miners, που ονομάζει slot leaders. Ο χρόνος χωρίζεται σε Εποχές (epochs) και οι εποχές χωρίζονται σε slots. Slots είναι μικρά διαστήματα χρόνου κατά τα οποία δημιουργείται ένα μπλοκ. Το δίκτυο εκλέγει ένα slot leader. Μόνο αυτός μπορεί να εξορύξει ένα μπλοκ. Κάθε slot αντιστοιχεί σε ένα stake pool όπου ο slot leader δημιουργεί ένα μπλοκ. Ένα slot κλείνει ανά είκοσι δευτερόλεπτα και κάθε Εποχή (epoch), περιλαμβάνει εικοσιένα χιλιάδες εξακόσια (21.600) slots. Ένα Epoch λοιπόν χρειάζεται πέντε ημέρες προκειμένου να ολοκληρωθεί. Το ουσιαστικό όμως είναι πως μπορούν να τρέχουν παράλληλα από μια έως Ν Εποχές, ανάλογα με τις δυνατότητες του δικτύου. Αυτό γεννά τεράστιες δυνατότητες ως προς το χρόνο διεξαγωγής των συναλλαγών. Όσον αφορά το εύρος ζώνης δικτύου. Το blockchain, αποθηκεύεται σε ένα δίκτυο peer - to - peer. Κάθε κόμβος σε αυτό το δίκτυο λαμβάνει ένα αντίγραφο όλων των συναλλαγών που έχουν πραγματοποιηθεί. Εάν όμως πραγματοποιούνται χιλιάδες συναλλαγές ανά δευτερόλεπτο, θα απαιτούνταν ένα τεράστιο εύρος ζώνης δικτύου ώστε να μεταδίδεται η αλυσίδα. Για να λυθεί το πρόβλημα αυτό, το Cardano χωρίζει το δίκτυο σε υπο-δίκτυα, χρησιμοποιώντας την τεχνική RINA (Recursive InterNetwotk Architecture) ή αναδρομική αρχιτεκτονική δικτύου. Με τον τρόπο αυτό, ο κάθε κόμβος αποτελεί μέρος ενός μικρότερου δικτύου ή υποσυνόλου και μπορεί να επικοινωνεί με τα υπόλοιπα δίκτυα αν χρειάζεται.

Τέλος, όσο αφορά την αποθήκευση δεδομένων, η ομάδα που δημιούργησε το Cardano, έχει υπόψιν τεχνικές όπως συμπίεση (compression) ή διαμέριση (partitionng) που όμως δεν απαιτούνται αυτή τη στιγμή. [25]

ΕΙΚΟΝΑ 12- Cardano logo, ΠΗΓΗ: cardano.org

2.6 MONERO

Το Monero είναι ένα κρυπτονόμισμα που βασίζεται, όπως το Bitcoin, στην εξόρυξη μέσω της χρήσης του αλγόριθμου απόδειξης εργασίας (Proof of Work) για την επίτευξη κατανεμημένης συναίνεσης. Στα κρυπτονομίσματα που εξετάσαμε μέχρι στιγμής, οι συναλλαγές αποθηκεύονται σε ένα δημόσιο κατάλογο. Όλοι όσοι βρίσκονται στο δίκτυο μπορούν να δούν τα δεδομένα των συναλλαγών που πραγματοποιούνται ανάμεσα σε δύο διευθύνσεις, τις διευθύνσεις, τη συχνότητα των συναλλαγών, εάν οι διευθύνσεις δεν αλλάζουν για κάθε συναλλαγή, τα ποσά που ανταλλάσσονται. Ακόμα και αν ο χρήστης δημιουργεί νέα διεύθυνση για κάθε συναλλαγή υπάρχει τρόπος να συνδεθεί η πραγματική του ταυτότητα εαν για παράδειγμα αγόρασε τα κρυπτονομίσματα μέσω εφαρμογής που απαιτεί επαλήθευση των στοιχείων του χρήστη. Ακόμα και αν δε συνδεθεί η πραγματική ταυτότητα του χρήστη, εάν πραγματοποιηθεί συναλλαγή με κάποιο γνωστό μεγάλο κατάστημα, μπορεί να παρακολουθείται το πορτοφόλι του χρήστη ως προς τις καταναλωτικές συνήθειες ώστε να δέχεται προσωποποιημένες διαφημίσεις. Και τέλος υπάρχει η πιθανότητα να γίνει ο χρήστης υποκείμενο επιθέσεων στην περίπτωση που φανεί πως έχει στην κατοχή του μεγάλες ποσότητες νομισμάτων, από τις συναλλαγές που πραγματοποιεί. Με βάση τα παραπάνω, προέκυψε η ανάγκη δημιουργίας ενός ανώνυμου αλλά και ιδιωτικού κρυπτονομίσματος, στο οποίο δεν φανερώνεται ο αποστολέας, ο παραλήπτης και τα ποσά που ανταλλάσσουν. Το Monero είναι το πιο δημοφιλές κρυπτονόμισμα αυτής της κατηγορίας. Αυτό που ξεχωρίζει στο Monero, είναι το γεγονός πως είναι μη ανιχνεύσιμο και προστατεύει τη δημόσια διεύθυνση του χρήστη. Αν για παράδειγμα προσπαθήσουμε να ανιχνεύσουμε τι συναλλαγές έχουν πραγματοποιηθεί από μια δημόσια διεύθυνση του δικτύου Monero, αυτό δε θα είναι εφικτό. Στην ουσία όλοι οι χρήστες έχουν μια δημόσια διεύθυνση, όπως και στις περιπτώσεις των υπόλοιπων κρυπτονομισμάτων. Όμως οι διαθέσιμοι πόροι του χρήστη δε συνδέονται με το πορτοφόλι του.

Εάν ένας χρήστης στείλει κρυπτονομίσματα στη δημόσια διεύθυνση κάποιου άλλου, στην πραγματικότητα τα στέλνει σε μια τυχαία διαμορφωμένη διεύθυνση που θα χρησιμοποιηθεί μόνο μια φορά. Οπότε η δημόσια διεύθυνση του χρήστη δε θα εμφανιστεί ποτέ σε κάποιο κατάλογο συναλλαγών. Χρησιμοποιείται μια **διεύθυνση Stealth**, ή αλλιώς δημόσιο κλειδί "μιας χρήσης", με τρόπο που μόνο ο αποστολέας και ο παραλήπτης μπορούν να αναγνωρίσουν τα εισερχόμενα/εξερχόμενα νομίσματα. Αυτό το δημόσιο κλειδί δημιουργείται και καταγράφεται ως μέρος της συναλλαγής και υποδεικνύει ποιος μπορεί να ξοδέψει νομίσματα σε κάποια μεταγενέστερη συναλλαγή. Ένας εξωτερικός παρατηρητής δεν μπορεί να εντοπίσει ποιός στέλνει χρήματα σε ποιόν, ή να συνδέσει διευθύνσεις πορτοφολιών μεταξύ τους μόνο παρατηρώντας το blockchain. Αν υποθέσουμε ότι ένας έμπορος χρησιμοποιεί Monero για τις συναλλαγές του, τα δεδομένα του θα ήταν απολύτως ιδιωτικά, αφού δε θα υπήρχε τρόπος να διασταυρωθεί πόσους πελάτες εξυπηρετεί, αν είναι ένας ή περισσότεροι και πόσο συχνά ψωνίζουν από το μαγαζί του. Αυτά τα δεδομένα σήμερα τα αντλούν μεγάλες εταιρείες δεδομένων δωρεάν από τους χρήστες, ενώ στην πραγματικότητα θα έπρεπε να ερωτούνται ή ακόμα και να πληρώνονται για αυτά. Η διεύθυνση του πορτοφολιού του χρήστη, είναι μια ακολουθία ενενήντα πέντε χαρακτήρων και αποτελείται από το δημόσιο κλειδί προβολής (**public send key**) και το δημόσιο κλειδί αποστολής (**public view key**). Όταν ο χρήστης Α στέλνει Monero στο χρήστη Β, τότε το πορτοφόλι του χρήστη Α χρησιμοποιεί το δημόσιο κλειδί προβολής του Β, το δημόσιο κλειδί αποστολής του Β, καθώς και ορισμένα τυχαία δεδομένα για τη δημιουργία ενός μοναδικού δημόσιου κλειδιού μίας χρήσης για τη συναλλαγή του χρήστη Β. Όλοι μπορούν να δουν το κλειδί αυτό, όμως μόνο οι χρήστες Α και Β μπορούν να γνωρίζουν ότι υπήρξε κάποια συναλλαγή μεταξύ τους. Το πορτοφόλι του χρήστη Β έπειτα δημιουργεί ένα μοναδικό ιδιωτικό κλειδί μιας χρήσης, το οποίο συνδέεται με το δημόσιο κλειδί μιας χρήσης και μπορεί να ξοδέψει τα χρήματα που έλαβε με το ιδιωτικό κλειδί δαπανών που υπάρχει στο πορτοφόλι του. Αυτό που κάνουν λοιπόν οι διευθύνσεις Stealth, είναι να αποτρέπουν τη σύνδεση των πραγματοποιούμενων συναλλαγών με τις πραγματικές διευθύνσεις των πορτοφολιών των χρηστών. Εδώ χρησιμοποιούνται οι υπογραφές δακτυλίου, (ring signatures).

Στην κρυπτογραφία, μια **ring signature** είναι ένας τύπος ψηφιακής υπογραφής που μπορεί να εκτελεστεί από οποιοδήποτε μέλος μιας ομάδας χρηστών που ο καθένας έχει κλειδιά. Επομένως, ένα μήνυμα υπογεγραμμένο με μια ring signature, εγκρίνεται από κάποιον σε μια συγκεκριμένη ομάδα ατόμων. Μία από τις ιδιότητες ασφαλείας μιας υπογραφής δακτυλίου είναι ότι θα πρέπει να είναι υπολογιστικά ανέφικτο να προσδιοριστεί ποια από τα κλειδιά των μελών της ομάδας χρησιμοποιήθηκαν για την παραγωγή της υπογραφής. Για παράδειγμα, μια τέτοια υπογραφή θα μπορούσε να χρησιμοποιηθεί για την ανώνυμη υπογραφή υψηλόβαθμου αξιωματούχου του Λευκού Οίκου, χωρίς να αποκαλυφθεί ποιος αξιωματούχος υπέγραψε το μήνυμα. Οι υπογραφές δακτυλίου είναι οι κατάλληλες για την εφαρμογή Monero, επειδή η ανωνυμία μιας υπογραφής δεν μπορεί να ανακληθεί. Μια υπογραφή δακτυλίου χρησιμοποιεί τα κλειδιά του λογαριασμού του χρήστη και έναν αριθμό δημόσιων κλειδιών (επίσης γνωστών ως outputs) που "τραβήχτηκαν" από το blockchain χρησιμοποιώντας μια μέθοδο τριγωνικής διανομής. Με την πάροδο του χρόνου, τα προηγούμενα outputs θα μπορούσαν να χρησιμοποιηθούν πολλές φορές για να σχηματίσουν πιθανούς συμμετέχοντες. Σε έναν "δακτύλιο" πιθανών υπογραφόντων, όλα τα μέλη του δακτυλίου είναι ίσα και έγκυρα. Δεν υπάρχει κανένας τρόπος ώστε ένας εξωτερικός παρατηρητής να μπορεί να ανιχνεύσει ποιος από τους πιθανούς υπογράφοντες σε μια ομάδα υπογραφών ανήκει σε συγκεκριμένο λογαριασμό. Έτσι, οι υπογραφές αυτές διασφαλίζουν ότι τα αποτελέσματα των συναλλαγών δεν μπορούν να ανιχνεύονται. [26]

ΕΙΚΟΝΑ 13 - Monero logo, ΠΗΓΗ: getmonero.org

2.7 ΑΣΦΑΛΕΙΑ, ΑΝΩΝΥΜΙΑ & ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Η δομή και ο τρόπος λειτουργίας του blockchain, προσφέρει αυξημένη ασφάλεια, αφού η αλλοίωση των δεδομένων απαιτεί ουσιαστικά παραβίαση κάθε υπολογιστή του δικτύου. Η **αρχιτεκτονική του blockchain** το καθιστά ιδιαίτερα ελκυστικό για διάφορους τομείς, όπως χρηματοοικονομικές συναλλαγές, εφοδιαστική αλυσίδα, υγειονομική περίθαλψη και κυβερνητικές υπηρεσίες, καθώς προσφέρει **ασφάλεια, ιδιωτικότητα και ανωνυμία**. Αυτά τα χαρακτηριστικά είναι κρίσιμα για την ευρύτερη εφαρμογή του σε ένα μέλλον όπου οι ψηφιακές συναλλαγές θα είναι πιο συχνές. Με κορωνίδα την ασφάλεια, την ιδιωτικότητα και την ανωνυμία που παρέχει στους χρήστες, αποτελεί αναμφισβήτητα μέρος μιας συνολικότερης μελλοντικής τεχνολογικής εξέλιξης.

Με βάση την έρευνα που πραγματοποιήθηκε στα προηγούμενα μέρη, παρατηρούμε πως οι συναλλαγές μέσω κρυπτονομισμάτων θεωρούνται **γενικά ιδιωτικές και ανώνυμες**, όμως στην πραγματικότητα υπάρχουν διαφορές ως προς την ανωνυμία και την ιδιωτικότητα, ανάλογα με την τεχνολογία στην οποία στηρίζεται το κάθε κρυπτονόμισμα. Είδαμε ότι το Bitcoin για παράδειγμα μπορεί να συνδεθεί με την πραγματική ταυτότητα του χρήστη, ακόμα και αν για κάθε συναλλαγή χρησιμοποιείται διαφορετική διεύθυνση, ενώ το Monero είναι πολύ πιο ασφαλές ως προς τη διατήρηση της ανωνυμίας και της ιδιωτικότητας λόγω των stealth addresses και ring signatures στα οποία στηρίζεται. Στα περισσότερα κρυπτονομίσματα, τα δεδομένα των χρηστών και οι συναλλαγές είναι **ψευδώνυμα (pseudonymous) και όχι ανώνυμα**. Οι συναλλαγές που πραγματοποιούνται με κρυπτονομίσματα, θα ήταν εντελώς ανώνυμες μόνο αν ήταν απολύτως αδύνατο να εντοπιστούν οι συναλλασσόμενοι. Στην πράξη είναι πολύ δύσκολη, αλλά όχι απόλυτα αδύνατη, η ταυτοποίηση των χρηστών σχετικών συναλλαγών. Υπάρχουν τρόποι, ακόμα και με άλλα κρυπτονομίσματα πλην του Monero να διατηρηθεί η ανωνυμία και η ιδιωτικότητα του χρήστη, που όμως εγείρουν **ερωτήματα ως προς τη νομιμότητα των συναλλαγών.** Γιατί δηλαδή να μπεί ο χρήστης σε κόπο ώστε να "κρύψει" κάποια συναλλαγή. Και ίσως με τους τρόπους αυτούς να τραβάει περισσότερη προσοχή στις δραστηριότητές του ενώ επιθυμεί το αντίθετο.

Χρησιμοποιώντας κανείς το διαδίκτυο, πρέπει να χρησιμοποιεί πηγές όπως παρόχους υπηρεσιών διαδικτύου και server οι οποίοι ανήκουν σε τρίτα μέρη τα οποία δεν ελέγχει ο χρήστης. Έτσι δεν μπορεί να ελέγξει με κάποιο τρόπο τί δεδομένα συλλέγονται από την οποιαδήποτε δραστηριότητα στο διαδίκτυο και με ποιο τρόπο αυτά αξιοποιούνται. Εαν κάποιος επιθυμεί να αυξήσει την ανωνυμία και την ιδιωτικότητα χρησιμοποιώντας το διαδίκτυο, θα πρέπει να χρησιμοποιήσει κάποια υπηρεσία που να προσφέρει ανωνυμοποίηση και συγκεκριμένες ιδιωτικές διαδικτυακές υπηρεσίες. Συνδυασμός αυτών των υπηρεσιών προσφέρεται κυρίως στο κομμάτι του διαδικτύου που ονομάζεται σκοτεινός ιστός ή Dark Web. Τέλος θα πρέπει να φροντίζει για την ασφάλεια του δικτύου και του υπολογιστή που χρησιμοποιεί ώστε ακόμα και με αυτά τα μέσα να διατηρεί τα δεδομένα του ιδιωτικά. Μερικοί από τους πιο διαδεδομένους τρόπους διατήρησης της ιδιωτικότητας περιλαμβάνουν:

1. **Ανάμειξη συναλλαγών (mixing services ή tumblers):** Οι υπηρεσίες αυτές ανακατεύουν τις συναλλαγές πολλών χρηστών, καθιστώντας δύσκολο να εντοπιστεί ποια συναλλαγή προέρχεται από ποιον.

2. **Κρυπτονομίσματα με τεχνικές ανωνυμοποίησης:** Κρυπτονομίσματα όπως το **Zcash** χρησιμοποιούν

τεχνολογίες όπως το zk-SNARKs, οι οποίες επιτρέπουν την επαλήθευση των συναλλαγών χωρίς την αποκάλυψη των διευθύνσεων του αποστολέα ή του παραλήπτη, διατηρώντας έτσι την ανωνυμία των συναλλαγών.

3. **Χρήση VPN ή TOR:** Η χρήση εργαλείων όπως τα VPN (Virtual Private Networks) και το **TOR** (The Onion Router) για ανωνυμοποίηση της σύνδεσης στο διαδίκτυο. Αυτά τα εργαλεία κρύβουν τη διεύθυνση IP του χρήστη και δυσκολεύουν τον εντοπισμό της πραγματικής τοποθεσίας του.

4. **Χρήση υπηρεσιών του Dark Web:** Το **Dark Web** προσφέρει ανωνυμία και πρόσβαση σε υπηρεσίες που λειτουργούν εκτός των κανονικών δικτύων, αλλά η χρήση του συχνά συνδέεται με παράνομες δραστηριότητες. Ενώ είναι εφικτό να χρησιμοποιήσει κάποιος τις υπηρεσίες αυτές για νόμιμους σκοπούς, οι ρυθμιστικές αρχές μπορεί να το θεωρήσουν ύποπτο.

❖ TOR - THE ONION ROUTER

Το TOR, είναι το πιο δημοφιλές **ανώνυμο δίκτυο,** του οποίου οι χρήστες μπορούν να έχουν πρόσβαση ή και να παρέχουν υπηρεσίες σε ιστοσελίδες του Deep Net και του Dark Net. Η τεχνική onion routing, είναι μια τεχνική δρομολόγησης που αναπτύχθηκε από τον αμερικάνικο στρατό με σκοπό την ανώνυμη επικοινωνία μέσα σε δίκτυο υπολογιστών. Οι χρήστες μπορούν να χρησιμοποιούν το TOR ακόμα και αν δεν επιθυμούν την πρόσβαση σε κάποια ιστοσελίδα του Deep Net, προκειμένου να προστετέψουν τα προσωπικά τους δεδομένα. Κάθε φορά που κάποιος χρήστης χρησιμοποιεί για παράδειγμα την αναζήτηση μέσω Google, η Google μπορεί να έχει πρόσβαση σε δεδομένα όπως τί αναζητήσεις πραγματοποίησε ο χρήστης, ποιές ιστοσελίδες επισκέφθηκε και πόση ώρα παρέμεινε σε αυτές, προηγούμενη δραστηριότητα του χρήστη και πολλά άλλα δεδομένα, τα οποία ενδεχομένως να έπρεπε να είναι ιδιωτικά. Είναι γνωστό πως ιστοσελίδες που έχουν κουμπί like ή share της Google, της Facebook και άλλων εταιρειών, φέρουν ένα κομμάτι κώδικα το οποίο μεταφέρει τα δεδομένα του χρήστη, τη δραστηριότητά του στη συγκεκριμένη σελίδα δηλαδή, στις εταιρείες αυτές. Και δεν είναι προαπαιτούμενο να έχει δημιουργήσει κανείς προσωπικό λογαριασμό - προφίλ στις εφαρμογές των εταιρειών αυτών. Το Facebook φημολογείται πως δημιουργεί ακόμα και ψεύτικα προφίλ χρηστών που μπορεί να μην διατηρούν λογαριασμό, συλλέγοντας δεδομένα μέσω των ιστοσελίδων στις οποίες υπάρχει κάποιο κομμάτι κώδικα, όπως το κουμπί like/share, σχετικά με την επισκεψιμότητα του site, την ώρα που παραμένουν οι χρήστες σε αυτά, αγορές που πραγματοποιούν και οτιδήποτε μπορεί να σχετίζεται με τη δραστηριότητά τους. Εαν οι χρήστες επιθυμούν να προστατέψουν τα προσωπικά τους δεδομένα, έχουν την επιλογή να χρησιμοποιήσουν τον browser TOR. Όταν ένας χρήστης συνδεθεί στη Google για παράδειγμα, μέσω TOR, συμβαίνει το εξής. Ο υπολογιστής του συδέεται πρώτα σε διαφορετικούς κόμβους/server, προτού συνδεθεί στη Google. Η Google μπορεί να "δει" μόνο τον τελευταίο κόμβο που συνδέεται με τον δικό της server και όχι τον χρήστη. Επίσης τα δεδομένα που εισέρχονται στο δίκτυο TOR κρυπτογραφούνται. Έτσι ο πάροχος δικτύου θα μπορούσε να γνωρίζει πως ο χρήστης χρησιμοποιεί το δίκτυο TOR, δεν μπορεί όμως να γνωρίζει σε ποιές ιστοσελίδες αποκτά πρόσβαση. Χρησιμοποιώντας λοιπόν το δίκτυο TOR για συναλλαγές με κρυπτονομίσματα, προστίθεται μια δικλείδα ασφαλείας ως προς την ιδιωτικότητα και την ανωνυμία. [27] Θα μπορούσε κανείς να επιχειρηματολογήσει πως συνολικά η λύση θα ήταν να δρομολογεί όλη του τη διαδικτυακή δραστηριότητα μέσω TOR. Όμως στην περίπτωση αυτή η ταχύτητα του δικτύου θα μειωνόταν σημαντικά.

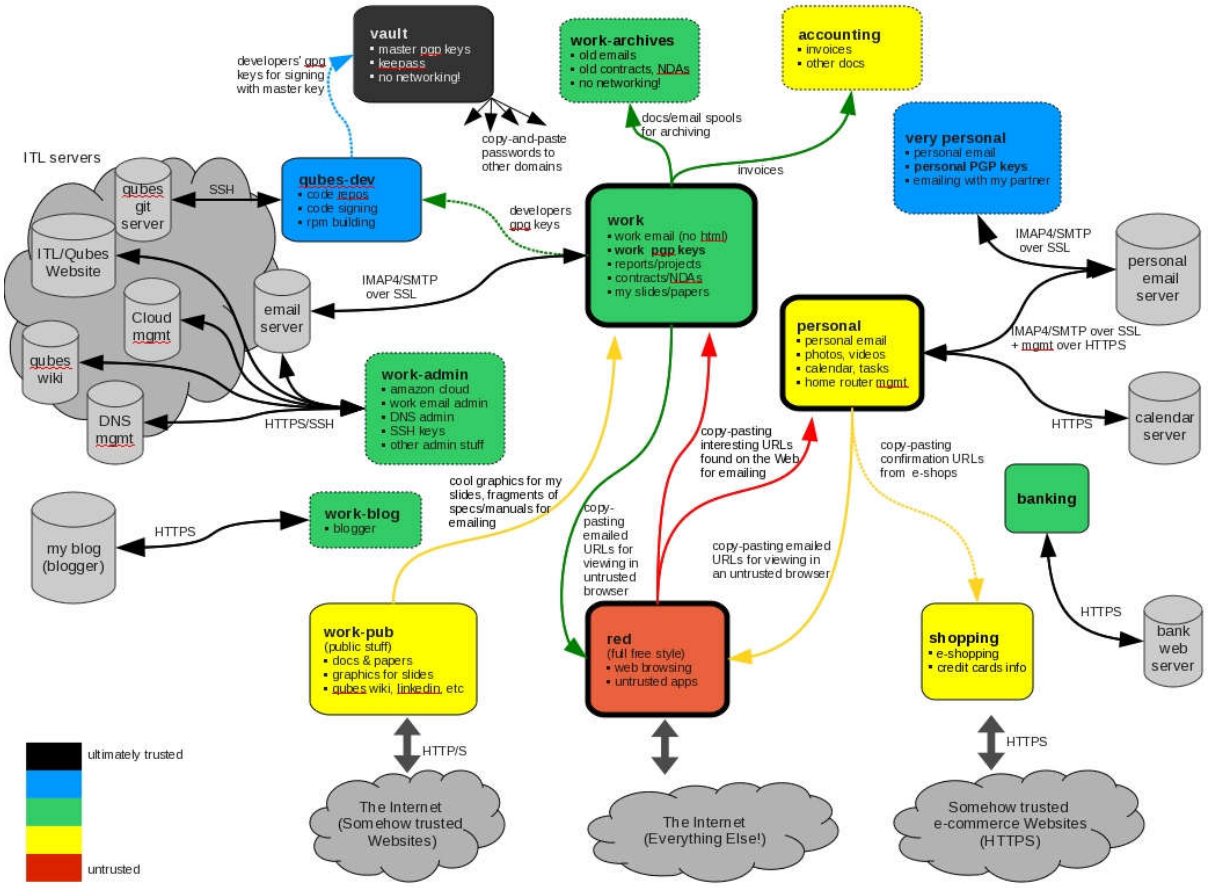
Ακόμα τα δεδομένα που "φεύγουν" από τον κόμβο του χρήστη εισέρχονται στο δίκτυο TOR μή κρυπτογραφημένα και άρα ακόμα και με αυτό τον τρόπο ο χρήστης δεν είναι απολύτως ασφαλής.

❖ TAILS - THE AMNESIC INCOGNITO LIVE SYSTEM

Μια ασφαλέστερη μέθοδος προστασίας της ιδιωτικότητας του χρήστη είναι η χρήση του λογισμικού TAILS. Όπως μπορούμε να ερμηνεύσουμε από την πλήρη ονομασία του, είναι ένα "αμνησιακό σύστημα ανώνυμης περιήγησης", ένα σύστημα δηλαδή **το οποίο δεν αφήνει ίχνη (amnesic), αφού χρησιμοποιεί μόνο τη RAM του υπολογιστή, είναι ιδιωτικό και ανώνυμο (incognito), και λειτουργεί εξ ολοκλήρου μέσω φορητών συσκευών (live) όπως cd ή ακόμα καλύτερα sticks usb και μπορεί να χρησιμοποιηθεί σε οποιοδήποτε υπολογιστικό σύστημα.** Ακόμη και στην περίπτωση πραγματοποίησης ελέγχου στον υπολογιστή του χρήστη, δε θα υπάρχουν ίχνη σχετικά με τη δραστηριότητά του. Δε θα υπάρχουν καν ίχνη ότι χρησιμοποίησε TAILS σε αυτό τον υπολογιστή. Έτσι θεωρητικά θα μπορούσε κανείς να παραμείνει απολύτως ανώνυμος και ασφαλής, διατηρώντας ιδιωτικά τα δεδομένα του, χρησιμοποιώντας το σύστημα TAILS ώστε να εισέλθει στον ιστό μέσω TOR. Με τον τρόπο αυτό ο χρήστης μπορεί να διατηρήσει τις κρυπτο-συναλλαγές του ασφαλείς και ιδιωτικές. Εδώ όμως εγείρονται ερωτήματα, αφού δυστυχώς τα συστήματα αυτά χρησιμοποιούνται περισσότερο για παράνομες δραστηριότητες και λιγότερο για την προστασία των δεδομένων ενός μέσου χρήστη. [28]

❖ QUBES

Το TAILS λοιπόν μπορεί να προσφέρει μεγαλύτερη προστασία στο χρήστη. Το πρόβλημα όμως είναι πως το TAILS λειτουργεί κάτω από ένα domain. Έτσι στην περίπτωση που υπάρξει κάποια κακόβουλη ενέργεια, ο εισβολέας έχοντας πρόσβαση στον υπολογιστή θα μπορεί να έχει πρόσβαση σε όλες τις πληροφορίες του χρήστη παρακάμπτοντας τις δικλείδες ασφαλείας. Μια λύση σε αυτό το πρόβλημα θα ήταν ο χρήστης να χρησιμοποιεί διαφορετικούς υπολογιστές για κάθε δραστηριότητα, έναν υπολογιστή για την εργασία του, έναν για τις προσωπικές του υποθέσεις, έναν για πρόσβαση σε ιστότοπους που δεν εμπιστεύεται και λοιπά. Αυτή η λύση όμως δεν είναι εφαρμόσιμη. Μια εναλλακτική θα ήταν ο χρήστης να λειτουργεί με διαφορετικά sticks usb μέσω της εφαρμογής TAILS, κάτι που ξανά δεν είναι εύχρηστο και άρα εύκολα εφαρμόσιμο. Τη λύση στο πρόβλημα μπορεί να δώσει το λειτουργικό σύστημα QUBES. Το QUBES δίνει τη δυνατότητα στο χρήστη **να διαχωρίζει τη δραστηριότητά του σε διαφορετικά domains, σα να χειρίζεται διαφορετικούς υπολογιστές.** Το κάθε domain λειτουργεί ξεχωριστά, σα να έχει τη δική του RAM και CPU και είναι τελείως αποκομμένο από τα υπόλοιπα, λειτουργεί σαν μοναδικός εικονικός υπολογιστής. Ακόμα και αν κάποιος εισβάλει σε ένα domain, είναι σχεδόν ανέφικτο να αποκτήσει πρόσβαση στα υπόλοιπα. Το QUBES λοιπόν προσφέρει μεγαλύτερη ιδιωτικότητα και ανωνυμία, επειδή είναι πιο ασφαλές, διαμερισματοποιώντας τους τομείς δραστηριότητας του χρήστη. [29]



ΕΙΚΟΝΑ 14 - QUBES, ΠΗΓΗ: qubes-os.org/intro/

Το ζήτημα της ασφάλειας και των προσωπικών δεδομένων σχετικά με τη χρήση της κρυπτοοικονομίας απασχολεί χρήστες αλλά και κράτη και επιχειρήσεις, ιδιαίτερα με την ανακοίνωση της πρόθεσης του **Facebook** να εκδόσει δικό του κρυπτονόμισμα, το οποίο αρχικά έφερε την ονομασία **Libra**. Σε αντίθεση με το καθαρά αποκεντρωμένο blockchain του Bitcoin χωρίς αποκλεισμούς χωρίς την ύπαρξη κάποιου αξιόπιστου τρίτου μέρους ως εγγύηση, η ιδέα είναι οι συναλλαγές στο Libra blockchain να διέπονται από το Libra Association ως κεντρική αρχή που αποτελείται από 28 ιδρυτικά μέλη, τα περισσότερα από τα οποία είναι εταιρείες-κολοσσοί από τις Ηνωμένες Πολιτείες όπως Visa, MasterCard, PayPal, Facebook Calibra και eBay.

Το ήδη σκανδαλώδες παρελθόν, με τα φαινόμενα παραβίασης του απορρήτου και εκμετάλλευσης των δεδομένων των χρηστών του Facebook, (βλ. σκάνδαλο αποκάλυψης δεδομένων Cambridge Analytica) έχει εντείνει την αντίθεση μεταξύ των αρχών και τον σκεπτικισμό μεταξύ των συμμετεχόντων στον κλάδο. Οπως και με οποιαδήποτε νέα τεχνολογία blockchain, το ψηφιακό κρυπτονόμισμα της Facebook αναμένεται να προκαλέσει βραχυπρόθεσμα αναταραχές στην υπάρχουσα αγορά ψηφιακών νομισμάτων που σχηματίζεται την τελευταία δεκαετία. Ωστόσο, μακροπρόθεσμα, ένα σταθερό παγκόσμιο κρυπτονόμισμα θα φέρει επανάσταση στα ηλεκτρονικά συστήματα πληρωμών και μεταφοράς χρημάτων. Έχει περάσει μια δεκαετία από το ντεμπούτο του Bitcoin τον Ιανουάριο του 2009 και μέχρι σήμερα εξακολουθούν σε ολόκληρο τον κόσμο να μην υπάρχουν ρυθμίσεις σχετικά με τα κρυπτονομίσματα. [30] Είτε λοιπόν το κρυπτονόμισμα του Facebook ή κάποιας άλλης εταιρείας που θα τολμήσει ένα τέτοιο εγχείρημα, θα εκτοξευθεί και θα

δημιουργήσει αναταραχές στην αγορά κρυπτονομισμάτων και στην πραγματική οικονομία, με τις επιπτώσεις που μπορεί να έχει στα καθολικά των τραπεζικών ιδρυμάτων αφενός, ενισχύοντας και το ενδεχόμενο έκδοσης κι άλλων blockchain νομισμάτων στηριζόμενα από ομίλους αφετέρου, είτε θα πάρει τη θέση του καρτερικά ανάμεσα στα υπόλοιπα κρυπτονομίσματα έως ότου υπάρξει κάποια νομοθετική ρύθμιση. Ενας από τους πρώτους που σχολίασε την εξέλιξη ήταν ο Γάλλος υπουργός Οικονομικών Μπρουνό Λεμέρ, που απέκλεισε να γίνει το Libra ένα κανονικό νόμισμα, ενώ αξιωματούχοι των G7, ανακοίνωσαν ότι σχεδιάζουν να δημιουργήσουν φορέα αποτίμησης των κινδύνων από ψηφιακά νομίσματα όπως το Bitcoin. Επιπλέον, ο Μάρκους Φέρμπερ, Γερμανός ευρωβουλευτής, προειδοποίησε ότι το Facebook θα μπορούσε να γίνει «σκιώδης τράπεζα». Μετά το σκάνδαλο της Cambridge Analytica η οποία χρησιμοποίησε τα δεδομένα του Facebook δόλια, με σκοπό να επηρεάσει πολλαπλά αποτελέσματα εκλογών, με το Brexit και την εκλογή Trump στην Αμερική ως κύρια παραδείγματα, επιχειρείται πια μια διάσπαση του Internet σε γεωγραφικές και πολιτικές ζώνες όπου θα επιβάλλεται έλεγχος ως προς το περιεχόμενο που θα μπορούν να δημοσιεύουν οι εταιρείες και στο οποίο θα έχουν πρόσβαση οι πολίτες.

Έτσι προκύπτουν πολλά ερωτήματα που σχετίζονται με την **ασφάλεια και ιδιωτικότητα του χρήστη** ακόμα όμως **και με τις ελευθερίες του χρήστη ως πολίτη**. Αν υποθέσουμε ότι το κράτος υιοθετούσε ευρέως την τεχνολογία Blockchain στο μέλλον, θα μπορούσαν δυνητικά όλα τα προσωπικά δεδομένα των πολιτών από τη γέννηση τους να αποθηκεύονται σε κάποια αλυσίδα, πάνω στην οποία θα μπορούσαν να "τρέχουν" έξυπνα συμβόλαια που να εκτελούν αυτόματα διαδικασίες. Αυτό από τη μια θα διευκόλυνε και θα αυτοματοποιούσε πολλές χρονοβόρες και γραφειοκρατικές σήμερα διαδικασίες, από την άλλη όμως θα δημιουργούσε αμφιλεγόμενα προβλήματα. Αν κάποιος ιδιοκτήτης ακινήτων πραγματοποιούσε μια δήλωση εκμίσθωσης ακινήτου μέσω κάποιας αντίστοιχης πλατφόρμας με το TaxisNet για παράδειγμα, και για διάφορους λόγους ο ενοικιαστής καθυστερούσε την καταβολή του ενοικίου, ένα έξυπνο συμβόλαιο σε περιβάλλον Internet of Things θα μπορούσε να κλειδώσει τον μισθωτή έξω από το σπίτι. Αντίστοιχα για τους οφειλέτες, θα μπορούσε η περιουσία τους να δεσμεύεται ή να κατάσχεται, δίχως δυνατότητα αντιστροφής της διαδικασίας.

Με το 5G αλλά και το **Internet of Things** τόσο κοντά μας, αυτό που οφείλουμε να αναλογιστούμε είναι ότι μπορούμε να αποκτήσουμε πρόσβαση σε τεχνολογικά μέσα και πολύτιμα δεδομένα που θα μας βοηθήσουν να βελτιώσουμε πολλούς τομείς της ζωής μας , να αναπτύξουμε νέες τεχνολογίες για την βελτίωση της υγείας και άλλων τομέων. Όμως το επίκεντρο και οι απαντήσεις ως προς το ποιός θα ωφελείται από την τεχνολογία αυτή τελικά, βρίσκονται στο ποιός θα τη χρησιμοποιεί και με τί σκοπό. Οφείλουμε να αναλογιζόμαστε ότι ενώ θεωρητικά το διαδίκτυο είναι ένα αποκεντρωμένο περιβάλλον στο οποίο οποιοσδήποτε μπορεί να έχει πρόσβαση, **στην πραγματικότητα είναι ένα περιβάλλον που αποτελεί μεγάλο μέρος της πραγματικής οικονομίας και ταυτόχρονα ένα κερδοσκοπικό εργαλείο για τους επιχειρηματικούς ομίλους οι οποίοι αντιμετωπίζουν τους χρήστες άλλοτε ως πελάτες και άλλοτε ως προιόν, αλιεύοντας και εμπορευματοποιώντας τα προσωπικά τους δεδομένα.** Πως τελικά η προσπάθεια νομοθέτησης και "καναλιζαρίσματος" του διαδικτύου γενικότερα και της κρυπτοοικονομίας ειδικότερα, **πραγματοποιείται στα πλαίσια ενός ήδη διαμορφωμένου οικονομικού περιβάλλοντος** στο οποίο υπάρχουν ιδιοκτήτες των μέσων παραγωγής και εργαζόμενοι σε αυτά και άρα οποιαδήποτε εκτίμηση ή πρόβλεψη σχετικά με την τεχνολογική εξέλιξη και την αξιοποίηση αυτής, θα πρέπει να λαμβάνει υπόψιν το περιβάλλον αυτό.

2.8 DARK WEB & CRYPTOCURRENCY

Το Διαδίκτυο μπορεί να περιγραφεί ως αποτελούμενο από στρώματα: το «ανώτερο» επίπεδο, ή το Surface Web, είναι εύκολα προσβάσιμο με τακτικές αναζητήσεις. Είναι το κομμάτι του διαδικτύου που χρησιμοποιεί ένας μέσος χρήστης. Ωστόσο, τα «βαθύτερα» επίπεδα, το περιεχόμενο του Deep Web, δεν έχουν καταχωρηθεί σε μηχανές αναζήτησης όπως της Google. Ο Μάικλ Κ. Μπέργκμαν που έγραψε το σεμινάριο στο Deep Web, συνέκρινε την αναζήτηση στο Διαδίκτυο με το να σύρει ένα δίχτυ στην επιφάνεια του ωκεανού: μπορεί να πιαστούν πολλά στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκεται βαθύτερα και παραμένει άπιαστος. Στην πραγματικότητα, οι περισσότερες από τις πληροφορίες του Διαδικτύου αποθηκεύονται σε ιστότοπους και οι τυπικές μηχανές αναζήτησης δεν μπορούν να έχουν πρόσβαση σε αυτές.

Το Darknet ή Dark web, είναι γνωστό ότι είναι ένα σημαντικό κανάλι διανομής επιβλαβούς περιεχομένου καθώς και παράνομων προϊόντων και δραστηριοτήτων. Αποτελεί **τμήμα του Deep Web**, στο οποίο μπορεί κανείς να έχει πρόσβαση μέσω εξειδικευμένου λογισμικού. Η χρήση κρυπτονομισμάτων στο σκοτεινό ιστό, σχετίζεται σε μεγάλο ποσοστό με παράνομες δραστηριότητες όπως παράνομη πώληση ναρκωτικών, πυροβόλων όπλων και εκρηκτικών, λαθρεμπόριο ανθρώπων, νομιμοποίηση εσόδων από παράνομες δραστηριότητες, τρομοκρατικές δραστηριότητες και πολλά άλλα.

Ο όρος darknet αρχίζει να χρησιμοποιείται από τη δεκαετία του 1970 ως όρος που υποδηλώνει δίκτυα με υψηλό **επίπεδο ιδιωτικότητας**. Αυτό το φαινομενικά κρυφό μέρος του Διαδικτύου, στην αρχή, ήταν αθώο, σταδιακά όμως έγινε καταφύγιο για τον προγραμματισμό εγκληματικών δραστηριοτήτων. Ο σκοτεινός ιστός, εκτός από την εμφάνιση αυτών των παράνομων σχεδίων, διευκόλυνε επίσης το εμπόριο. Τα κρυπτονομίσματα και ειδικά το Bitcoin, άρχισαν να χρησιμοποιούνται σε παράνομες συναλλαγές. Ο Ross Ulbricht καταδικάστηκε σε ισόβια κάθειρξη για την προσπάθειά του να πουλήσει ναρκωτικά αξίας άνω του 1 δισεκατομμυρίου δολαρίων τον Φεβρουάριο του 2015. Τον Μάρτιο, ο Tomáš Jiříkovský συνελήφθη στην Τσεχική Δημοκρατία αφού προσπάθησε να κλέψει χιλιάδες Bitcoin (ή εκατομμύρια δολάρια) από μια αγορά του darknet. Έξι μήνες αργότερα, τον Σεπτέμβριο, ο Τρίντον Σάβερς παραδέχτηκε ότι διήυθυνε ένα σχήμα Ponzi 150 εκατομμυρίων δολαρίων. Λίγο μετά από αυτό, ο Γάλλος Mark Karpelès υπεξαίρεσε ένα χρηματικό ποσό ύψους 390 εκατομμυρίων δολαρίων από μια ανταλλαγή κρυπτονομισμάτων. Συνελήφθη και κατηγορήθηκε για απάτη λίγο μετά. Αυτά βέβαια, δεν φάνηκε να πλήττουν τη δραστηριότητα στο Darknet, ούτε τη χρήση κρυπτονομισμάτων σε αυτό. Οι παράνομες αγορές Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas και AlphaBay, ήταν οι επτά κορυφαίες και πιο ενεργές αγορές σκοτεινού Ιστού. Και οι επτά χρησιμοποιούν το ίδιο λογισμικό για τη διαχείριση του Bitcoin διερευνώντας συναλλαγές σε αυτές τις αγορές. Ωστόσο, το λογισμικό σταμάτησε να χρησιμοποιείται από τον Μάιο του 2016 αφού δεν μπορούσε πια να παρέχει ανωνυμία. Οι αγορές του Σκοτεινού Ιστού συνεχίζουν να ευδοκιμούν επειδή οι χρήστες μεταναστεύουν σε νέες αγορές όταν κλείνουν οι υπάρχουσες. Ο συνολικός όγκος πωλήσεων στο Silk Road ήταν εκατόν ενενήντα δύο κόμμα επτά (192,7) εκατομμύρια δολάρια μεταξύ Ιουνίου 2012 και Οκτωβρίου 2013. Τα αντίστοιχα στοιχεία για το Silk Road 2.0, Agora, Evolution, Nucleus και Abraxas ήταν εκατόν δώδεκα κόμμα εννέα (112,9), διακόσια είκοσι κόμμα επτά, (220,7), εξήντα εννέα κόμμα επτά (69,7), ογδόντα οχτώ κόμμα τρία (88,3) και τριάντα πέντε κόμμα έξι (35,6) εκατομμύρια δολάρια ΗΠΑ, αντίστοιχα. Τα στοιχεία για το AlphaBay ήταν εκατόν εξήντα έξι (166,0) εκατομμύρια δολάρια ΗΠΑ μεταξύ Δεκεμβρίου 2014 και Φεβρουαρίου 2016. [31]

Μια αυστραλιανή μελέτη που πραγματοποιήθηκε ανέφερε ότι περίπου το 47% των συναλλαγών που αφορούν το Bitcoin πραγματοποιούνται στον σκοτεινό ιστό. Όταν εμφανίστηκε το Bitcoin, υποσχέθηκε πλήρη ανωνυμία

και αυτό έκανε την παγκόσμια κοινότητα να το αγκαλιάσει. Ωστόσο στην πορεία κατέστη σχετικά εύκολο το να γίνει κανείς "σκιά" στις διευθύνσεις των ατόμων που πραγματοποιούν τεράστιες συναλλαγές στο δίκτυο. Τα κρυπτονομίσματα όπως το Litecoin και το Monero άρχισαν να χρησιμοποιούνται περισσότερο, αφού επεξεργάζονται συναλλαγές γρηγορότερα και με ένα ορισμένο επίπεδο αξιοπιστίας, ενώ υποστηρίζουν την έννοια της ανωνυμίας καλύτερα.

Το Blockchain είναι αναπόσπαστο μέρος του σκοτεινού ιστού και η κρυπτογράφηση συνέβαλε καθοριστικά στην ανάπτυξή του. Η πρόσφατη καταστολή στον σκοτεινό ιστό και η σταδιακή αραίωση της χρήσης του Bitcoin, λόγω της τεράστιας αύξησης της ισοτιμίας του αλλά και λόγω της δημοτικότητάς του, που αύξησε τη χρήση του και τα κόστη των συναλλαγών, έβαλαν ένα φρένο στις συναλλαγές της σκοτεινής πλευράς του διαδικτύου. Επίσης είναι γεγονός πως πια οι περισσότερες κυβερνήσεις καταβάλουν προσπάθειες να νομοθετήσουν και να καναλιζάρουν τη νέα αυτή οικονομία του Blockchain. Άλλωστε, μερικά από τα μεγαλύτερα ονόματα στις σκοτεινές αγορές (DarkNet Markets) αντιμετώπισαν ήδη ταραχώδεις στιγμές. Ιστοσελίδες όπως οι Alphabay και Hansa έκλεισαν από το 2015 και μετά, και αρκετοί άλλοι αντιμετώπισαν έντονες αντιθέσεις, είτε μέσω επιθέσεων DDoS (Destributed Denial of Service - Η επίθεση DDoS στέλνει πολλαπλά αιτήματα στον πόρο ιστού που έχει επιτεθεί, με σκοπό την υπέρβαση της ικανότητας του ιστότοπου να χειρίζεται πολλαπλά αιτήματα ώστε να εμποδίζει τη σωστή λειτουργία του ιστότοπου.) - είτε μέσω πτωχεύσεων.

2.9 ΟΙΚΟΝΟΜΙΚΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Το ζήτημα της **κυβερνοασφάλειας** είναι μείζον και για τις κυβερνήσεις και για τους επιχειρηματικούς ομίλους. Η ενίσχυση της ασφάλειας στον κυβερνοχώρο συνδέεται με την ευρωστία και τη σταθερότητα στην οικονομία. Οι επιχειρήσεις τείνουν να υποεπενδύουν σε ζητήματα ασφαλείας. Όμως πάνω από 3,8 δισεκατομμύρια άνθρωποι σε όλο τον κόσμο συνδέονται διαδικτυακά και αυτός ο αριθμός με την πάροδο του χρόνου αυξάνεται. Ο κόσμος του διαδικτύου αναδύει πρωτοφανείς ανακαλύψεις και ευκαιρίες. Το Διαδίκτυο γίνεται με την πάροδο του χρόνου το μέσο για την οικονομική ευημερία και η πλατφόρμα για την προώθηση μιας κοινωνικής αλλαγής. Για να είναι κερδοφόρες, οι επιχειρήσεις πια πρέπει να έχουν παρουσία στο διαδίκτυο και να καινοτομούν για να απολαμβάνουν μέρος της πίτας της ψηφιακής οικονομίας.

Η τεχνολογική εξέλιξη μπολιάστηκε με την οικονομία αλλάζοντας τον τρόπο εφαρμογής της επιχειρηματικής δραστηριότητας αφού άνοιξε δρόμος σε μια νέα αγορά για τη δημιουργία πλούτου. Η πληροφορία είναι σήμερα πολύτιμο εργαλείο και η ψηφιακή εξέλιξη επηρεάζει τον κόσμο σε πολλές πτυχές. Οι επιχειρήσεις που επενδύουν στον κυβερνοχώρο, ανταγωνίζονται για τους περιορισμένους πόρους. Οι εταιρείες πρέπει να αναπτύσσουν και να εφαρμόζουν νέες πρακτικές, νέες τεχνολογίες και νέες προσεγγίσεις - και γρήγορα. Ένα από τα ζητήματα λοιπόν που τις απασχολούν είναι ο τρόπος με τον οποίο η ασφάλεια στον κυβερνοχώρο επηρεάζει τους προϋπολογισμούς και τις εκτιμήσεις κινδύνων.

Η Kaspersky πραγματοποίησε έρευνα, παίρνοντας συνέντευξη από 5.266 ερωτηθέντες σε 31 χώρες σχετικά με την κατάσταση της ασφάλειας πληροφορικής στις εταιρείες τους, τις απειλές που αντιμετωπίζουν και το κόστος μετά την επίθεση που υπέστησαν. Δυστυχώς, οι μεγάλες εταιρείες είχαν μειώσει τις δαπάνες στον τομέα της ασφάλειας στον κυβερνοχώρο από κατά μέσο όρο 18,9 εκατομμύρια δολάρια το 2019 σε 14 εκατομμύρια δολάρια το 2020. Αντιμέτωποι με το κόστος και τις απώλειες που σχετίζονται με τον COVID-19, οι οποίες ήταν σε μεγάλο βαθμό απρόβλεπτες, τέτοιες περικοπές δεν προκαλούν έκπληξη. Η εικόνα των μικρών και μεσαίων επιχειρήσεων είναι διαφορετική: Οι προϋπολογισμοί που αφορούσαν την ασφάλεια στο διαδίκτυο εκεί αυξήθηκαν ελαφρώς (από 267.000 $ το 2019 σε 275.000 $ το 2020). Παρόλα αυτά, το 71% των εταιρειών σκοπεύουν να αυξήσουν τις επενδύσεις τους σε ζητήματα ασφάλειας τα επόμενα τρία χρόνια. Ανεξάρτητα από το μέγεθος της εταιρείας, οι ερωτηθέντες ανέφεραν την αυξημένη πολυπλοκότητα της υποδομής πληροφορικής και την ανάγκη αύξησης της εμπειρογνωμοσύνης των εργαζομένων ως τους κύριους λόγους για την αύξηση αυτή. Ορισμένοι (17%) ελπίζουν να διατηρήσουν τις δαπάνες στον κυβερνοχώρο στο ίδιο επίπεδο και μόνο το 12% εξετάζει περαιτέρω περικοπές στον προϋπολογισμό ως μέρος της συνολικής βελτιστοποίησης ή με την πεποίθηση ότι οι προηγούμενες επενδύσεις έχουν ήδη βοηθήσει στην επίλυση των βασικών ζητημάτων. [32]

Η τεχνολογία blockchain, θα μπορούσε να συμβάλει σημαντικά στη μείωση του κόστους των επενδύσεων σε ζητήματα ασφάλειας στο διαδίκτυο και τα επόμενα χρόνια αναμένεται να δούμε κρίσιμες αλλαγές, καινοτομίες και εφαρμογές εφάμιλλες με την εμφάνιση των μηχανών αναζήτησης τη δεκαετία του 1990. Το crowdfunding στον τομέα των επιχειρήσεων, έχει αναδείξει το ενδιαφέρον του κοινού όχι μόνο για το εκάστοτε εγχείρημα, αλλά και για το μερίδιο συμμετοχής που ενδέχεται να λάβει ως αντάλλαγμα. Με αυτό το σκεπτικό είναι πιθανή η εξέλιξη στην οικονομία των token και των ψηφιακών νομισμάτων συνολικότερα. Φαίνεται πως ενισχύεται συνεχώς το ενδιαφέρον σχετικά με την κρυπτοοικονομία και την κατηγορία περιουσιακών στοιχείων στην οποία εμπίπτουν τα κρυπτονομίσματα. Είναι όμως αναγκαία η έρευνα και η ανάπτυξη λύσεων σε επίπεδο ασφάλειας, αφού ο χώρος αυτός αποτελεί εύφορο έδαφος για εγκληματική

δραστηριότητα, ενώ ταυτόχρονα δεν υπάρχει η βεβαιότητα πως οι επενδυτές δε θα χάσουν τα κεφάλαιά τους, ή κάποιο εχέγγυο που να επιβεβαιώνει την αξία τέτοιων περιουσιακών στοιχείων. Το ερώτημα λοιπόν είναι εαν το blockchain και οι εφαρμογές του μπορούν να ρυθμιστούν κατάλληλα ώστε να βρίσκουν εφαρμογή στο υπάρχον οικονομικό περιβάλλον, με το μέγιστο δυνατό επίπεδο ασφάλειας. Εάν αυτό συμβεί, θα δούμε ραγδαίες τεχνολογικές εξελίξεις σε όλους τους τομείς της οικονομίας. Δεδομένου ότι τα κρυπτονομίσματα, όπως το bitcoin, έχουν μια παγκόσμια εμβέλεια χωρίς να εξαρτώνται από κάποια γεωγραφική τοποθεσία ή κεντρικές τράπεζες, το Blockchain μπορεί έτσι να επιτρέπει σε επιχειρηματίες από οπουδήποτε στον κόσμο να έχουν πρόσβαση σε κεφάλαια εκκίνησης και αναπτυξιακό κεφάλαιο.

Όμως το ζήτημα της ασφάλειας στον κυβερνοχώρο είναι κρίσιμο, αφού η εκτεταμένη χρήση των μέσων κοινωνικής δικτύωσης βοηθά εν μέρει τους "εισβολείς". Δυστυχώς, είναι εξαιρετικά απλό για τους χάκερ να αποκτήσουν πληροφορίες όπως διευθύνσεις email, αριθμούς κινητών τηλεφώνων και προσωπικά στοιχεία, όπως ονόματα κατοικίδιων και παιδικά ψευδώνυμα (συνηθισμένοι κωδικοί πρόσβασης που χρησιμοποιούν οι διαδικτυακοί χρήστες). Δικλείδες ασφαλείας που βασίζονται στην παραδοσιακή ταυτοποίηση δύο παραγόντων είναι επομένως ευάλωτες σε χάκερ που επιδιώκουν να αποκτήσουν πρόσβαση στα ψηφιακά πορτοφόλια των επενδυτών. Το κλεμμένα κρυπτονομίσματα μπορούν στη συνέχεια να μετατραπούν σε πραγματικό νόμισμα ή άλλα κρυπτογραφημένα κρυπτονομίσματα με σχεδόν απίθανο το ενδεχόμενο να εντοπιστεί ο εισβολέας. Η εκτεταμένη χρήση της blockchain τεχνολογίας στο μέλλον, λοιπόν, θα είναι απαραίτητο να συνοδεύεται από τις κατάλληλες ρυθμίσεις αλλά και από σειρά μέτρων για την ενίσχυση των επενδύσεων στον τομέα της κυβερνοασφάλειας. [33]

ΜΕΡΟΣ ΤΡΙΤΟ

ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΚΡΥΠΤΟΟΙΚΟΝΟΜΙΑΣ

3.1 ΝΟΜΟΘΕΤΙΚΗ ΟΡΙΟΘΕΤΗΣΗ ΣΥΝΑΛΛΑΓΩΝ ΜΕ ΚΡΥΠΤΟΝΟΜΙΣΜΑ

Το σκεπτικό πίσω από την άρνηση της αναγνώρισης των περιουσιακών στοιχείων που προκύπτουν από την αγορά των κρυπτονομισμάτων, είναι **το στοιχείο της αποκέντρωσης, της έλλειψης μιας αρχής έκδοσης**. Με την απουσία κάποιας νομικής αναγνώρισης ή ρύθμισης αυτής της αγοράς τα κρυπτονομίσματα δεν μπορούν να γίνουν επίσημα αποδεκτός τρόπος πληρωμής και να χρησιμοποιούνται ευρέως για συναλλαγές εντός της οικονομίας που υποστηρίζεται από την κεντρική τράπεζα της εκάστοτε κυβέρνησης. Ο Νόμος περί Ασφαλείας των ΗΠΑ του 1933 διέπει την έκδοση νέων τίτλων στο δημόσιο τομέα. Ο Νόμος απαιτεί από τους επενδυτές να λαμβάνουν οικονομικές και άλλες σημαντικές πληροφορίες σχετικά με τους τίτλους που προσφέρονται για δημόσια πώληση, και απαγορεύει την απάτη, τις παραπλανητικές δηλώσεις και άλλες απάτες στην πώληση κινητών αξιών. Με μια σαφή ταξινόμηση των κρυπτονομισμάτων ως τίτλων, και αυτό εμπίπτει στον τομέα των ρυθμιστικών αρχών κινητών αξιών, το επόμενο βήμα θα ήταν η ρύθμιση των επενδυτικών κεφαλαίων και των συμβούλων. Στις Η.Π.Α. για παράδειγμα, ο νόμος περί εταιρικών επενδύσεων του 1940 ρυθμίζει την οργάνωση εταιρειών, συμπεριλαμβανομένων των αμοιβαίων κεφαλαίων, οι οποίες ασχολούνται κυρίως με την επένδυση, επανεπένδυση και διαπραγμάτευση τίτλων. Ο νόμος απαιτεί από αυτές τις εταιρείες να αποκαλύπτουν πληροφορίες σχετικά με τα αμοιβαία κεφάλαια, και τους επενδυτικούς στόχους, καθώς και ως προς τη δομή και τις λειτουργίες της εταιρείας επενδύσεων, στο επενδυτικό κοινό. Ο ίδιος νόμος οριοθετεί επίσης τους συμβούλους επενδύσεων, απαιτώντας από εταιρείες ή μεμονωμένους επαγγελματίες να αποζημιώνονται για την παροχή συμβουλών σε άλλους σχετικά με τις επενδύσεις σε κινητές αξίες και να συμμορφώνονται με κανονισμούς που έχουν σχεδιαστεί για την προστασία των επενδυτών. [33]

Οι περιπτώσεις εξαπάτησης στην οικονομία των tokens, ιδιαίτερα μέσω των **Αρχικών Προσφορών Νομισμάτων (Initial Coin Offerings - ICOs)**, είναι ένα φαινόμενο που έχει προβληματίσει την αγορά. Επειδή οι ICOs δεν υπόκεινται σε συγκεκριμένο ρυθμιστικό πλαίσιο, είναι πιο ευάλωτες σε κακόβουλες πρακτικές και απάτες. Οι εγκληματίες εκμεταλλεύονται το ενδιαφέρον των επενδυτών για καινοτόμα πρότζεκτ, τα οποία συχνά δεν έχουν κανένα ουσιαστικό σχέδιο ή βάση. Οι επενδυτές αγοράζουν tokens ή μετοχές σε υποτιθέμενες εταιρείες, συνήθως με τη χρήση κρυπτονομισμάτων όπως το Bitcoin ή το Ethereum, και αναμένουν μερίδιο από τα μελλοντικά κέρδη του εγχειρήματος. Ωστόσο, σε πολλές περιπτώσεις, οι εταιρείες αυτές είτε δεν υπάρχουν είτε τα πρότζεκτ είναι απλώς ιδέες χωρίς καμία υποδομή για υλοποίηση. Οι εγκληματίες πίσω από τέτοιες απάτες δημιουργούν παραπλανητικά website και λευκά βιβλία (whitepapers) για να πείσουν τους επενδυτές ότι πρόκειται για ένα υποσχόμενο εγχείρημα. Αυτές οι **"pump-and-dump" απάτες** λειτουργούν με τον ίδιο τρόπο που γίνονται σε παραδοσιακές αγορές: οι εγκληματίες δημιουργούν ψευδή ζήτηση για τα tokens τους, προσελκύοντας επενδυτές με υποσχέσεις τεράστιων αποδόσεων. Μόλις συγκεντρώσουν αρκετά κεφάλαια, εξαφανίζονται, αφήνοντας τους επενδυτές με άχρηστα tokens χωρίς πραγματική αξία.

Η **έλλειψη ρυθμιστικού πλαισίου** σημαίνει ότι οι επενδυτές συχνά δεν έχουν νομικά μέσα να διεκδικήσουν τα χρήματά τους πίσω, καθώς οι ICOs δεν ελέγχονται από κρατικές αρχές όπως συμβαίνει με τις παραδοσιακές χρηματιστηριακές εταιρείες. Αυτό καθιστά τον χώρο των κρυπτονομισμάτων ιδιαίτερα επικίνδυνο για ανυποψίαστους επενδυτές. [34]

Το ζήτημα λοιπόν της καθυστέρησης κάποιας επίσημης αναγνώρισης ή ένταξης των κρυπτονομισμάτων σε ένα ρυθμιστικό πλαίσιο ως μέσο ανταλλαγής, αλλά και ως εργαλείο επενδύσεων και θησαυρισμού είναι εμπόδιο για την ενίσχυση των νόμιμων χρήσεων των κρυπτονομισμάτων, καθώς σε συνδυασμό με τα ζητήματα ασφαλείας στον κυβερνοχώρο δημιουργείται ανησυχία και δισταγμός στον επιχειρηματικό κόσμο.

Από την άλλη πλευρά, όμως, η ρύθμιση σύμφωνα με τους κανόνες και τους κανονισμούς των πράξεων που ρυθμίζουν τα μη ψηφιακά χρεόγραφα, η ένταξη των κρυπτονομισμάτων σε κάποια ρυθμιστική αρχή, έρχεται σε αντίθεση σε ένα βαθμό με το σκοπό για τον οποίο δημιουργήθηκαν τα κρυπτονομίσματα αλλά και με την ίδια την αποκεντρωμένη τους φύση που θέλει τους ίδιους τους χρήστες κύριους και όχι οποιοδήποτε τρίτο μέρος ακόμα κι αν είναι θεωρητικά αξιόπιστο. Είναι, ακόμα, δεδομένο πως τα τραπεζικά ιδρύματα δε θα παραμείνουν αμέτοχοι παρατηρητές στην άνθιση μιας οικονομίας στην οποία δεν απολαμβάνουν μερίδιο. Υπάρχει λοιπόν ακόμα **διχογνωμία ως προς την κατεύθυνση που πρέπει να κινηθούν οι ρυθμιστικές αρχές και τους τρόπους χειρισμού της κρυπτοοικονομίας.**

Νομοθετική οριοθέτηση και δεδικασμένο στις ΗΠΑ

Η αρχή Οικονομικού Εγκλήματος των ΗΠΑ ορίζει ως πραγματικό ή νόμιμο χρήμα το «νόμισμα ή χαρτονόμισμα των Ηνωμένων Πολιτειών ή οποιασδήποτε άλλης χώρας, που:

[i] έχει οριστεί ως νόμιμο χρήμα

[ii] κυκλοφορεί στην αγορά και

[iii] χρησιμοποιείται συνήθως και γίνεται αποδεκτό ως μέσο ανταλλαγής στη χώρα έκδοσης.

Σε αντίθεση με το πραγματικό νόμισμα, το «εικονικό» νόμισμα είναι ένα μέσο ανταλλαγής που λειτουργεί σαν νόμισμα σε ορισμένα περιβάλλοντα, αλλά δεν έχει όλα τα χαρακτηριστικά του πραγματικού νομίσματος. Συγκεκριμένα, το εικονικό νόμισμα δεν μπορεί να λειτουργεί με καθεστώς νόμιμου χρήματος σε καμία δικαιοδοσία. Αυτή η οδηγία αναφέρεται σε «μετατρέψιμο» εικονικό νόμισμα. Αυτός ο τύπος εικονικού νομίσματος έχει είτε ισοδύναμη αξία σε πραγματικό νόμισμα ή ενεργεί ως υποκατάστατο του πραγματικού νομίσματος. [35] Η γενική κατεύθυνση ως προς τη ρύθμιση χρήσης κρυπτονομισμάτων περιστρέφεται γύρω από την εξής σκέψη. Ένα άτομο που δημιουργεί μονάδες ενός μετατρέψιμου εικονικού νομίσματος και το χρησιμοποιεί για να αγοράσει πραγματικό ή εικονικά αγαθά και υπηρεσίες είναι χρήστης του μετατρέψιμου εικονικού νομίσματος και δεν υπόκειται κανονισμούς ως πομπός χρημάτων. Αντίθετα, ένα άτομο που δημιουργεί μονάδες μετατρέψιμου εικονικού νομίσματος και πωλεί αυτές τις μονάδες σε άλλο άτομο για

πραγματικό νόμισμα είναι πομπός χρημάτων. Επιπλέον, ένα άτομο υπόκειται σε κανονισμούς ως πομπός χρημάτων, εάν το άτομο δέχεται αποκεντρωμένο μετατρέψιμο εικονικό νόμισμα από ένα άτομο και το διαβιβάζει σε τρίτο άτομο ως μέρος αποδοχής και μεταφοράς νομίσματος, κεφαλαίων ή άλλης αξίας που αντικαθιστά το νόμισμα. Μέσω δεδικασμένων στις ΗΠΑ, μπορούμε να βγάλουμε ένα συμπέρασμα ως προς τις προθέσεις των νομοθετών.

❖ *ΗΠΑ κατά Ulbricht*

Η υπόθεση αυτή άνοιξε τον ασκό του Αιόλου όσον αφορά την αρχή του δεδικασμένου. Ο Ulbricht, ο δημιουργός του «Δρόμου του Μεταξιού» (Silk Road), της πλατφόρμας του σκοτεινού διαδικτύου που διευκόλυνε την παράνομη αγορά ναρκωτικών, όπλων, και άλλων προϊόντων, υποστήριξε ότι τα bitcoin με βάση το ισχύον νομοθετικό πλαίσιο αποτελούν "περιουσία" και όχι "νόμισμα", συνεπώς το αδίκημα της νομιμοποίησης εσόδων από παράνομες δραστηριότητες δεν μπορεί να ισχύει εφόσον οι συναλλαγές που πραγματοποίησε δεν είναι χρηματοοικονομικής φύσης. Το Δικαστήριο έκρινε ότι η νομοθεσία περί νομιμοποίησης εσόδων από παράνομες δραστηριότητες «είναι αρκετά ευρεία ώστε να συμπεριλαμβάνει τη χρήση bitcoin στις χρηματοπιστωτικές συναλλαγές.» Η απόφαση αυτή επέτρεψε στο FBI να εντοπίσει σχεδόν ένα εκατομμύριο χρήστες της πλατφόρμας. Η ουσία της υπόθεσης βασίστηκε στο ότι εφόσον χρησιμοποιούνται bitcoin για ξέπλυμα χρήματος προερχόμενο από εγκληματικές δραστηριότητες, ο δικαστής οφείλει να συμπεριλάβει την δραστηριότητα αυτή στο πεδίο εφαρμογής των υπαρχόντων νομοθετημάτων αν και αυτά εκ πρώτης όψεως δεν καλύπτουν τα κρυπτονομίσματα. [34], [36]

Μετά την απόφαση στην υπόθεση Ulbricht, η Αμερικανική κυβέρνηση έχει επιχειρηματολογήσει με τον ίδιο τρόπο σε μια σειρά από παρόμοιες υποθέσεις.

Στην υπόθεση ΗΠΑ κατά Faiella, ανέκυψε άλλη μια φορά το ερώτημα αν το bitcoin είναι νόμισμα ή περιουσιακό στοιχείο. Η Νότια Περιφέρεια της Νέας Υόρκης επιχειρηματολόγησε πως ο κατηγορούμενος διευκόλυνε τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες μέσω της χρήσης bitcoin στην πλατφόρμα Silk Road. Το δικαστήριο έκρινε ότι **το bitcoin μπορεί να θεωρηθεί χρήμα** επειδή μπορεί να αγοραστεί εύκολα με αντάλλαγμα νόμιμο χρήμα, ενεργεί ως παρονομαστής αξίας και χρησιμοποιείται για τη διεξαγωγή οικονομικών συναλλαγών. Η απόφαση αυτή θεωρείται πως αποτελεί και έναν ορισμό του bitcoin στην ομοσπονδιακή νομολογία, αν και έρχεται σε αντίθεση με την ως τότε ισχύουσα άποψη ότι το bitcoin είναι περιουσιακό στοιχείο. [34]

Τον Σεπτέμβριο του 2016 κατατέθηκε προσφυγή στο περιφερειακό δικαστήριο της Νέας Υόρκης για την υπόθεση ΗΠΑ εναντίον Murgio σε σχέση με τη λειτουργία επιχείρησης ξεπλύματος χρήματος. Ο δικαστής όρισε περαιτέρω ως χρήματα αυτά που "**παίρνουν τη μορφή, ή που αποτελούνται από χρήματα** ". Το δικαστήριο δήλωσε ότι τα χρήματα ορίζονται ως "...**ένα ευρύτερα αποδεκτό μέσο ανταλλαγής** ... "κι επανέλαβε το επιχείρημα στις υποθέσεις ΗΠΑ κατά Ulbricht και Faiella, ότι δηλαδή τα bitcoin χαρακτηρίζονται ως χρήματα βάσει του ομοσπονδιακού νόμου. [34]

Παρά τις αποφάσεις στις ανωτέρω υποθέσεις, το bitcoin δεν έχει επίσημα αναγνωριστεί ως χρήμα στην αμερικανική νομοθεσία ή από ρυθμιστικούς φορείς. Η νομοθεσία εξακολουθεί να είναι αποσπασματική και διφορούμενη. Παρά τις προσπάθειες από την Επιτροπή Κεφαλαιαγοράς (SEC) και την Επιτροπή Εμπορίου Συμβολαίων Μελλοντικής Εκπλήρωσης Εμπορευμάτων (CFTC) για τη ρύθμιση της αγοράς, η σαφής

οριοθέτηση αρμοδιοτήτων **παραμένει σε εκκρεμότητα**. Η εστίαση παραμένει κυρίως στην εφαρμογή κανόνων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML), ενώ νέες πρωτοβουλίες σε εθνικό επίπεδο δυσχεραίνονται από πολιτικές αντιπαραθέσεις.

Διεθνείς προσπάθειες ρυθμίσεων

Οι προσπάθειες νομοθετικής οριοθέτησης της κρυπτοοικονομίας σε διεθνές επίπεδο, βρίσκονται ακόμα σε πρώιμα στάδια. Σε αρκετές χώρες όπως το **Μπαγκλαντές, η Βολιβία και ο Ισημερινός η χρήση κρυπτονομισμάτων απαγορεύεται καθολικά, στην Κίνα και το Βιετνάμ το 2013 και 2014, απαγορεύθηκε με νόμο η διεξαγωγή συναλλαγών σε κρυπτονομίσματα,** των επιχειρήσεων που παρέχουν χρηματοπιστωτικές υπηρεσίες. Πρέπει να συνυπολογίσουμε ότι οι Κεντρικές τράπεζες δε θα μείνουν αμέτοχες στο πέρασμα της οικονομίας σε μια ψηφιακή εποχή.

Οι συγκρούσεις θα είναι μεγάλες και οι εναλλακτικές προτάσεις πολλές. Στην Κίνα για παράδειγμα η απαγόρευση αυτή συνδέεται με τα σχέδια έκδοσης ψηφιακού νομίσματος και την προώθηση της τεχνολογίας **CBDC (Central Bank Digital Currency)**. Οι πολίτες θα μπορούν να πραγματοποιούν συναλλαγές απευθείας, με τη χρήση των ψηφιακών τους πορτοφολιών, σκανάροντας κωδικούς QR, ή μέσω των ψηφιακών τους διευθύνσεων. Το σύστημα αυτό όμως δε θα είναι αποκεντρωμένο, θα στηρίζεται στην Κεντρική τράπεζα ως εγγυητή. Και άλλες χώρες ανά διαστήματα εξετάζουν με θέρμη την υιιοθέτηση ψηφιακών νομισμάτων ή και εθνικών κρυπτονομισμάτων, όπως η Ρωσία, η Βενεζουέλα και άλλες.

Σε επίπεδο θεσμών, **το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC) , η Ιντερπόλ και η Europol** καταβάλλουν προσπάθειες οριοθέτησης της χρήσης κρυπτονομισμάτων που σχετίζονται με παράνομες δραστηριότητες. Μέσα σε αυτές συμπεριλαμβάνονται και οι τρομοκρατικές ενέργειες. Η **Ειδική Ομάδα Κρούσης για τη Χρηματοοικονομική Δράση (FATF)** , η διακυβερνητική οργάνωση που αποτελείται από τριάντα πέντε κράτη μέλη και δύο περιφερειακές οργανώσεις, επου αποτελεί και το επίκεντρο των παγκόσμιων προσπαθειών καταπολέμησης της χρηματοδότησης της τρομοκρατίας, ιδρύθηκε το 1989 και έχει δημοσιεύσει περισσότερες από 40 συστάσεις, δημιουργώντας παγκόσμια πρότυπα για την προώθηση μιας κοινής προσέγγισης στο ξέπλυμα βρώμικου χρήματος. Οι κατευθυντήριες γραμμές του φορέα είναι μη δεσμευτικές και δομούνται με βάση το ρίσκο παρέχοντας παράλληλα στους εθνικούς ρυθμιστικούς φορείς τη διακριτική ευχέρεια ως προς τον τρόπο εφαρμογής των σχετικών μέτρων. Οι κατευθυντήριες γραμμές της FATF έχουν επίσης εφαρμοστεί στα κρυπτονομίσματα. Αρχικά, μια έκθεση του 2013 αξιολόγησε γενικά τα συστήματα πληρωμών που βασίζονται στο Διαδίκτυο, ενώ επόμενες εκθέσεις αναγνώρισαν την προοπτική των κρυπτονομισμάτων και την τεχνική τους πολυπλοκότητα και περιείχαν περαιτέρω συστάσεις για να βοηθήσουν τους παράγοντες της αγοράς να εντοπίσουν και να δράσουν εναντίον των απειλών νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Οι κατευθυντήριες γραμμές της FATF αφορούν την διασυνοριακή ανταλλαγή πληροφοριών καθώς και τη διαδικασία επιβολής κυρώσεων με βάση αποτελεσματικές, αναλογικές και αποτρεπτικές κυρώσεις (ποινικές, αστικές ή διοικητικές). Η FATF έχει επίσης καταθέσει προτάσεις για τον τρόπο ρύθμισης των συναλλαγών των εικονικών νομισμάτων, γνωστές και ως προτάσεις FAFT 40 σημείων. Αυτές ορίζουν ότι κάθε χώρα που συμμετέχει σε μεταφορές χρημάτων θα πρέπει να έχει λάβει μέτρα που αποδεικνύουν ότι το νομικό πρόσωπο που παρέχει την υπηρεσία μεταφοράς χρημάτων έχει λάβει άδεια και έχει ρυθμιστεί ώστε να υπόκειται σε συμμόρφωση και παρακολούθηση.

Γενικά, σε περιοχές, όπως η Ασία και η Μέση Ανατολή, παρατηρείται μία προσέγγιση που συνδυάζει

αυστηρότερη ρύθμιση με την προώθηση ενός ευνοϊκού επιχειρηματικού περιβάλλοντος. Το Χονγκ Κονγκ και τα Ηνωμένα Αραβικά Εμιράτα, ειδικά το Ντουμπάι, υιοθετούν ένα μοντέλο ρύθμισης που εστιάζει στην προστασία των καταναλωτών και τη διασφάλιση της συμμόρφωσης, ενώ παράλληλα ενθαρρύνουν την ανάπτυξη του τομέα των κρυπτονομισμάτων και τη δημιουργία κέντρων καινοτομίας.

Πλαίσιο ρυθμίσεων στην Ευρωζώνη

Η Ευρωπαϊκή Ένωση (ΕΕ) έχει προωθήσει προσπάθειες νομοθέτησης της χρήσης κρυπτονομισμάτων με σκοπό κυρίως την αντιμετώπιση του ξεπλύματος βρώμικου χρήματος και την παράνομη δραστηριότητα που στηρίζεται στην αγορά κρυπτονομισμάτων. Το 2007 η ΕΕ υιοθέτησε ένα νομικό πλαίσιο για τις υπηρεσίες πληρωμών, γνωστό ως **Οδηγία για τις υπηρεσίες πληρωμών (PSD)**. Οι υπηρεσίες πληρωμών στο πλαίσιο της Οδηγίας νοούνται ως σχετικές με την έννοια των κεφαλαίων, τα οποία ορίζονται ως "τραπεζογραμμάτια και κέρματα, χρήματα γραφής και ηλεκτρονικό χρήμα όπως ορίζεται στο άρθρο 1 παράγραφος 3 στοιχείο β) της Οδηγίας 2000/46/ΕΚ" . Αυτό σημαίνει ότι, ακόμη και αν οι υπηρεσίες εικονικού νομίσματος θεωρούνται υπηρεσίες πληρωμών στο πλαίσιο του PSD, θα μπορούσε να εφαρμοστεί μόνο ένα πολύ περιορισμένο σύνολο διατάξεων της Οδηγίας. Η Γαλλική αρχή τραπεζικής εποπτείας υποστήριξε ότι οι ανταλλαγές κρυπτονομισμάτων οδηγούν στην παραλαβή κεφαλαίων, τραπεζογραμματίων, η οποία με τη σειρά της οδηγεί σε υπηρεσίες πληρωμών. Ωστόσο, αυτή η προσέγγιση δεν βρήκε απήχηση εκτός της Γαλλίας. [34]

Η δεύτερη Οδηγία για τις υπηρεσίες πληρωμών επέτρεπε στα κράτη μέλη να ερμηνεύσουν συγκεκριμένες διατάξεις της ανάλογα με τις τοπικές τους ιδιαιτερότητες. Δεν προβλεπόταν παρόλα αυτά συμπερίληψη των κρυπτονομισμάτων σε αυτές τις Οδηγίες. Η Ευρωπαϊκή Επιτροπή, στην πρότασή της για τροποποιήσεις στην τέταρτη Οδηγία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, δήλωσε ρητά ότι δεν επιθυμεί να φέρει τις πλατφόρμες ανταλλαγής εικονικών νομισμάτων στο πεδίο εφαρμογής της δεύτερης Οδηγίας για τις υπηρεσίες πληρωμών, δεδομένου ότι τούτο θα "τα υποβάλει σε ευρύτερους κανόνες προστασίας των καταναλωτών, απαιτήσεις αδειοδότησης και απαιτήσεις διασφάλισης". Με τον τρόπο αυτό θα νομιμοποιούνταν η χρήση των κρυπτονομισμάτων και θα περνούσε το μήνυμα πως «τα εικονικά νομίσματα είναι ασφαλή και υγιή προϊόντα». [34]

Σε γενικές γραμμές οι πρώτες επεξεργασίες αφορούσαν συνολικά το ηλεκτρονικό χρήμα, το οποίο ορίζεται ως "ηλεκτρονικά, συμπεριλαμβανομένης της μαγνητικής, αποθηκευμένης χρηματικής αξίας η οποία αντιπροσωπεύεται από αξίωση για τον εκδότη που εκδίδεται με την παραλαβή των κεφαλαίων για τη διενέργεια πράξεων πληρωμής"και η οποία γίνεται δεκτή από φυσικό ή νομικό πρόσωπο διαφορετικό από τον εκδότη ηλεκτρονικού χρήματος. Δεν υπήρχε κάποια ξεκάθαρη οδηγία ως προς τα κρυπτονομίσματα, τα ψηφιακά νομίσματα που στηρίζονται στην τεχνολογία blockchain. Ακόμα και οι οδηγίες που αφορούσαν την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, δε συμπεριελάμβαναν ρυθμίσεις σχετικές με τα κρυπτονομίσματα. Επικεντρώνονταν στα περιουσιακά στοιχεία που αποτελούν προϊόντα εγκληματικής δραστηριότητας, δηλαδή "περιουσιακά στοιχεία κάθε είδους, υλικά ή άυλα, κινητά ή ακίνητα, και νομικά έγγραφα ή μέσα, υπό οποιαδήποτε μορφή, συμπεριλαμβανομένων ηλεκτρονικών ή ψηφιακών, ή συμφέρον σε τέτοια περιουσιακά στοιχεία". Αυτός ο ευρύς ορισμός θα μπορούσε, θεωρητικά, να συμπεριλάβει τα εικονικά νομίσματα ως άυλο περιουσιακό στοιχείο. Συμπεριλαμβάνοντας τα εικονικά νομίσματα σε αυτή την κατηγορία, οι οντότητες που παρέχουν εικονικά νομίσματα ενδεχομένως να θεωρηθούν πιστωτικά ιδρύματα ή χρηματοπιστωτικά ιδρύματα. Τα εικονικά νομίσματα όμως σύμφωνα με τους ορισμούς που δίνονται δεν εμπίπτουν στο πεδίο εφαρμογής τέτοιων ιδρυμάτων.

Η δυσκολία των θεσμών στην Ευρώπη αλλά και διεθνώς να υπάρξει **ενιαίο ρυθμιστικό πλαίσιο για την κρυπτοοικονομία**, έγκειται στο γεγονός ότι με την αναγνώριση των εικονικών νομισμάτων ως μορφή χρήματος, θα πρέπει να δοθεί συγκεκριμένη περιγραφή και για τους παρόχους υπηρεσιών εικονικού νομίσματος. Από την άλλη η έλλειψη ρύθμισής τους αποτελεί ενδεχομένως παράγοντα αύξησης της χρήσης εικονικών νομισμάτων για εγκληματικούς σκοπούς. Η Ευρωπαϊκή Επιτροπή προσπάθησε να περιορίσει περαιτέρω την ανωνυμία γύρω από τις συναλλαγές σε εικονικά νομίσματα μέσω της χρήσης των εθνικών Μονάδων Χρηματοπιστωτικής Πληροφόρησης (ΜΧΠ ή FIU) για τη δυνατότητα σύνδεσης των διευθύνσεων εικονικού νομίσματος με την ταυτότητα του ιδιοκτήτη των εικονικών νομισμάτων. Οι ΜΧΠ κατευθύνουν τις εργασίες των οικονομικών φορέων για τον εντοπισμό συναλλαγών για τις οποίες υπάρχουν υπόνοιες ότι συνδέονται με τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή με τη χρηματοδότηση της τρομοκρατίας. Η 5η οδηγία λοιπόν συμπεριελάμβανε στοιχεία ως προς τη χρήση κρυπτονομισμάτων, περιορίζοντας το ζήτημα της ανωνυμίας. Μετά από την οδηγία αυτή, οι χρήστες που αποκτούν κρυπτονομίσματα μέσω πλατφορμών ή ψηφιακών ανταλλακτηρίων, ή χρησιμοποιούν τις υπηρεσίες παρόχων υπηρεσιών πορτοφολιού στις πληρωμές τους, πρέπει **να επαληθεύουν την ταυτότητά τους προς αυτούς τους παρόχους υπηρεσιών**. Επιπρόσθετα, δημιουργήθηκε μια **κεντρική βάση δεδομένων** (https://translate.googleusercontent.com/translate_f#_ftn86) που περιλαμβάνει όλους τους χρήστες των κρυπτονομισμάτων. [34], [38], [39]

Η Ευρωπαϊκή Κεντρική Τράπεζα έβαλε όρια στη χρήση της έννοιας του «νομίσματος» για τα κρυπτονομίσματα κατά την συζήτηση της Οδηγίας, ώστε να υπογραμμίζεται σαφώς ότι τα κρυπτονομίσματα δεν αποτελούν νόμιμο χρήμα, διαφορετικά διέτεινε ενδεχόμενο κίνδυνο αστάθειας και διατάραξης του χρηματοπιστωτικού συστήματος. Επιπρόσθετα, σημείωσε πως η μερική συμπερίληψη ορισμένων κρυπτονομισμάτων ή εικονικών νομισμάτων σε ένα ρυθμιστικό πλαίσιο για την καταπολέμηση των εσόδων από παράνομες δραστηριότητες, πιθανόν να δημιουργούσε σύγχυση στους καταναλωτές. Έτσι υποστήριξε ότι υπάρχει ανάγκη για μια πανευρωπαϊκή ενιαία ρύθμιση που να καλύπτει ως σύνολο τη χρήση εικονικών νομισμάτων και να προστατεύει επαρκώς τους καταναλωτές. Στις 13/1/2021, η πρόεδρος της ΕΚΤ Κριστίν Λαγκάρντ εξαπέλυσε επίθεση στο χώρο της κρυπτοοικονομίας και συγκεκριμένα στο Bitcoin, επιχειρηματολογώντας πως αποτελεί μέσο κερδοσκοπίας με αποδεικτικό στοιχείο την αστάθεια στην τιμή του. Υπογραμμίζει ακόμα πως χρησιμοποιείται για δραστηριότητες ξεπλύματος χρήματος και θα πρέπει να υπάρξει ρυθμιστικό πλαίσιο που να κλείνει όλες τις διόδους διαφυγής. Πρέπει να λαμβάνουμε υπόψιν ως προς τις δηλώσεις αυτές και το γεγονός πως η Κριστίν Λαγκάρντ προτίθεται να προωθήσει το ψηφιακό ευρώ, το οποίο όπως δήλωσε θα κυκλοφορήσει το αργότερο μέσα στην επόμενη πενταετία. [34]

Το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο πρότειναν στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (ΕΟΚΕ) , τη δημιουργία ενός πιλοτικού καθεστώτος για τις υποδομές της αγοράς που βασίζονται σε τεχνολογία κατανεμημένου καθολικού. Η ΕΟΚΕ όμως επισήμανε σε σχετική γνωμοδότηση πως το πενταετές πιλοτικό πρόγραμμα που προτείνεται δεν είναι δόκιμο, από τη στιγμή που αναφερόμαστε σε τεχνολογίες που εξελίσσονται με αυτούς τους ρυθμούς και πως θα πρέπει να υπάρξει σύντομα μια ενιαία απόφαση ως προς το χειρισμό αυτής της τεχνολογίας από όλα τα κράτη-μέλη ώστε να μη διασπάται το πεδίο της οικονομίας με ξεχωριστές αποφάσεις από το κάθε κράτος-μέλος ή από χρηματοπιστωτικά ιδρύματα που εδρεύουν σε αυτά ή από κατευθυντήριες γραμμές ρυθμιστικών αρχών του κλάδου. Όπως χαρακτηριστικά αναφέρει, "Παρότι έχουν κοινό σκοπό, αυτές οι παρεμβάσεις ενέχουν τον κίνδυνο δημιουργίας κατακερματισμένου και ανομοιογενούς κανονιστικού πλαισίου στην εσωτερική αγορά. Αντιθέτως, άλλα κράτη δεν έχουν μέχρι στιγμής λάβει καμία σχετική πρωτοβουλία, συμβάλλοντας έτσι και αυτά σε ένα ανομοιόμορφο και κατακερματισμένο κανονιστικό πλαίσιο όπου συνυπάρχουν διαφόρων ειδών κανονιστικές παρεμβάσεις ή απουσιάζουν παντελώς". [38]

Ο στόχος που θέτει η ΕΟΚΕ είναι να υπάρξει ένα ρυθμιστικό πλαίσιο σε σύνδεση με κάποιες δράσεις που θα ενισχύουν την επαρκή πληροφόρηση των καταναλωτών και επενδυτών για τους κανόνες που θα ισχύουν, τους κινδύνους και τα οφέλη της χρήσης τεχνολογίας κατανεμημένου καθολικού στο χρηματοπιστωτικό και επενδυτικό τομέα.[38]

Στην Ευρωπαϊκή Ένωση, το 2024 σηματοδοτεί την πλήρη εφαρμογή του Κανονισμού για τις Αγορές Κρυπτονομισμάτων (MiCA). Ο Κανονισμός για τις Αγορές Κρυπτονομισμάτων (Markets in Crypto-Assets - MiCA) αποτελεί μια από τις πιο σημαντικές νομοθετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης για τη ρύθμιση της αγοράς κρυπτονομισμάτων. Εγκρίθηκε το 2023 και αναμένεται να τεθεί πλήρως σε ισχύ από το 2024, σηματοδοτώντας μια ενιαία και ολοκληρωμένη προσέγγιση για την κανονιστική ρύθμιση των κρυπτονομισμάτων σε όλα τα κράτη μέλη της ΕΕ.

Σκοπός και Κύρια Σημεία του MiCA

1. **Ενιαίο Ρυθμιστικό Πλαίσιο:** Το MiCA στοχεύει στη δημιουργία ενός ενιαίου ρυθμιστικού πλαισίου για τα κρυπτονομίσματα και τις σχετικές δραστηριότητες στην ΕΕ. Αυτό περιλαμβάνει την παροχή σαφών κανόνων για τους εκδότες κρυπτονομισμάτων και τους παρόχους υπηρεσιών, προκειμένου να διασφαλιστεί η σταθερότητα και η προστασία των επενδυτών.

2. **Προστασία Καταναλωτών:** Ο κανονισμός ενισχύει την προστασία των καταναλωτών, απαιτώντας από τους εκδότες κρυπτονομισμάτων να παρέχουν σαφείς και διαφανείς πληροφορίες για τα περιουσιακά στοιχεία που προσφέρουν, καθώς και να τηρούν αυστηρές απαιτήσεις κεφαλαιακής επάρκειας.

3. **Καταπολέμηση Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες (AML):** Το MiCA ενσωματώνει μέτρα για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και τη χρηματοδότηση της τρομοκρατίας, απαιτώντας αυστηρούς ελέγχους και διαδικασίες αναγνώρισης πελατών (KYC).

4. **Σταθερά Νομίσματα (Stablecoins):** Ο κανονισμός θέτει ειδικές απαιτήσεις για τα stablecoins, τα οποία θεωρούνται ως σημαντικά για την σταθερότητα των χρηματοπιστωτικών αγορών. Οι εκδότες stablecoins πρέπει να πληρούν αυστηρά κριτήρια διαχείρισης αποθεματικών και διαφάνειας.

Το MiCA θεωρείται ότι θα αυξήσει την εμπιστοσύνη στην αγορά των κρυπτονομισμάτων στην ΕΕ. Ωστόσο, η εφαρμογή του θα απαιτήσει από τις εταιρείες που δραστηριοποιούνται στον τομέα των κρυπτονομισμάτων να συμμορφωθούν με νέα ρυθμιστικά πρότυπα, τα οποία ενδέχεται να επιβαρύνουν τις μικρότερες επιχειρήσεις με αυξημένο κόστος συμμόρφωσης. Αναμένεται να αποτελέσει πρότυπο και για άλλες περιοχές του κόσμου, καθοδηγώντας τις παγκόσμιες συζητήσεις για τη ρύθμιση των κρυπτονομισμάτων, ενώ ταυτόχρονα θα επιτρέψει στην ΕΕ να διαδραματίσει ηγετικό ρόλο στη διαμόρφωση του διεθνούς κανονιστικού πλαισίου για τα ψηφιακά περιουσιακά στοιχεία.

3.2 ΤΟ ΕΘΝΙΚΟ ΚΡΥΠΤΟΝΟΜΙΣΜΑ & ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ CBDC (CENTRAL BANK DIGITAL CURRENCY)

• ΤΟ ΕΘΝΙΚΟ ΚΡΥΠΤΟΝΟΜΙΣΜΑ

Η ιδέα ενός εθνικού κρυπτονομίσματος, υπάρχει ως σκέψη από την πρώτη εκτίναξη του Bitcoin. Το 2018, δημοσιεύθηκε το άρθρο : "Digital Trade Coin (DTC): Towards a more stable digital currency", των Alex Lipton, Thomas Hardjono, Alex Pentland, μέσω του Πανεπιστημίου MIT (Massachusetts Institute of Technology Cambridge, MA, USA). Στο άρθρο αυτό περιγράφεται ένα ψηφιακό νόμισμα βασισμένο σε τεχνολογία κατανεμημένου καθολικού, blockchain, το οποίο θα μπορούσε να παίξει το ρόλο ενός εθνικού αλλά και υπερεθνικού νομίσματος, διευκολύνοντας τις διεθνείς συναλλαγές. Σύμφωνα με τους εμπνευστές, το Trade Coin έχει πραγματική αξία, επειδή η τιμή του συνδέεται με ένα αντιπροσωπευτικό καλάθι εμπορευμάτων. Επιπρόσθετα, ·η τιμή του DTC έναντι ενός νομίσματος fiat έχει πολύ χαμηλή μεταβλητότητα σε σύγκριση με άλλα κρυπτονομίσματα. Έτσι, ένα DTC μπορεί να χρησιμοποιηθεί ως κύριο νόμισμα συναλλαγής, με το DTC μιας χώρας να είναι φυσικά ευθυγραμμισμένο με ορισμένα από τα κύρια εμπορεύματα. Το DTC μπορεί , δηλαδή, να χρησιμοποιηθεί ως μονάδα αξιολόγησης αξίας αλλά και ως μέσο θησαυρισμού (όπως και ο χρυσός ή το πετρέλαιο). Η σταθερότητα στην τιμή αλλά και η σύνδεσή του με πραγματικά εμπορεύματα, θα επέτρεπαν σε μικρά κράτη που μέχρι τώρα δεν είχαν τη δυνατότητα να συμμετέχουν στο διεθνές εμπόριο, θεωρητικά προστατευμένα από τις πολιτικές και στρατηγικές των ισχυρότερων κρατών. [40]

❖ Η ΕΜΠΕΙΡΙΑ ΤΗΣ ΒΕΝΕΖΟΥΕΛΑΣ

Η Βενεζουέλα υπήρξε το πρώτο κράτος που εφάρμοσε αυτή την ιδέα. Ανακοίνωσε την «κυκλοφορία» του Petro, ενός κρυπτονομίσματος με τα χαρακτηριστικά που περιγράφονται για το Trade Coin. Το νόμισμα συνδέθηκε με τα αποθέματα της χώρας σε ορυκτά καύσιμα, κυρίως με το πετρέλαιο (από το οποίο προέρχεται και η ονομασία), τον κρατικό χρυσό και τα διαμάντια της. Το Petro είναι ένα κρυπτονόμισμα που αναπτύχθηκε από το κράτος της Βενεζουέλας για διαπραγμάτευση σε εθνικό επίπεδο και διεθνώς, για την πληρωμή των υποχρεώσεων προς το κράτος της Βενεζουέλας, και για την ανταλλαγή peer-to-peer. Η αξία του Petro «καθορίζεται» από την κυβέρνηση της Βενεζουέλας ανάλογα με την τιμή αγοράς του βαρελιού πετρελαίου της Βενεζουέλας και όχι ανάλογα με τη ζήτηση και την προσφορά του, όπως συμβαίνει με τα περισσότερα κρυπτονομίσματα, τουλάχιστον κατά τη στιγμή της αρχικής τους πώλησης. Κάθε Petro υποστηρίζεται ρητά από ένα συμβόλαιο «αγοράς-πώλησης» που σχετίζεται με ένα βαρέλι πετρελαίου που ανήκει στη Βενεζουέλα ή

ΕΙΚΟΝΑ 15 - logo Petro, ΠΗΓΗ: whitepaperdatabase.com

σε οποιοδήποτε άλλο εμπόρευμα που μπορεί να αποφασιστεί από τη Βενεζουέλα, παρότι υπάρχει διαφωνία σχετικά με τη φύση του εμπορεύματος που υποστηρίζει το Petro. Σύμφωνα με την κυβέρνηση της Βενεζουέλας, το Petro "είναι ένα κυρίαρχο κρυπτοδραστικό (cryptoactive) νόμισμα, εγγυημένο και εκδιδόμενο από τη Βολιβιανή Δημοκρατία της Βενεζουέλας, βασισμένο σε μια ομοσπονδιακή πλατφόρμα blockchain που είναι διαθέσιμη για εμπορία αγαθών και υπηρεσιών. Η κυβέρνηση αποτελεί τον εγγυητή - τρίτο, και το Petro θεωρείται επίσημα κυβερνητικό χρήμα που μπορεί να χρησιμοποιείται στις τρεις διαστάσεις του ως μέσο εμπορίου, αποταμίευσης-θησαυρισμού, αλλά και επενδύσεων ως τεχνολογική πλατφόρμα". [42]

Η εκτελεστική εξουσία της Βενεζουέλας έχει μεγάλο βαθμό ελέγχου στο Petro, καθώς ρυθμίζει την αρχική έκδοση, τη χρήση εντός της Βενεζουέλας για την πληρωμή υποχρεώσεων του δημοσίου, όπως φόρων ή τελών, και εξουσιοδοτεί παρόχους ανταλλαγής, μεταξύ άλλων. Αυτό κάνει το Petro το πρώτο κρυπτονόμισμα που υποστηρίζεται από το κράτος. Αυτός ο κρατικός έλεγχος έρχεται βέβαια σε αντίθεση με την ιδέα του κρυπτονομίσματος, που εμφανίστηκε για πρώτη φορά ως ένα έργο που θα εισήγαγε ουσιαστικά μια ηλεκτρονική έκδοση μετρητών, χωρίς όμως τη δυνατότητα παρέμβασης από "κακόβουλες κυβερνήσεις" ή τραπεζικά ιδρύματα. Μέχρι σήμερα, η Βενεζουέλα ισχυρίζεται ότι έχει εκδώσει (και εν μέρει πωλήσει) εκατό εκατομμύρια (100.000.000) Petro, αξίας $60 (USD) το καθένα, αντικατοπτρίζοντας τη μέση τιμή πώλησης του βαρελιού πετρελαίου της Βενεζουέλας τη στιγμή έκδοσης. Σύμφωνα με την κυβέρνηση της Βενεζουέλας, τα κονδύλια που προέρχονται από τις συναλλαγές με Petro, προορίζονται για την αγορά τροφίμων και βιομηχανικών προμηθειών, με στόχο την ανακούφιση της χώρας από τις συνέπειες της οικονομικής κρίσης. [42] Το Petro αποτελεί έμπνευση του πρώην Προέδρου Hugo Chavez και του οράματός του για τη δημιουργία μιας εναλλακτικής λύσης, ενός διεθνούς νομίσματος για τις αναπτυσσόμενες χώρες που να υποστηρίζεται από πρώτες ύλες και εμπορεύματα, όπως πετρέλαιο, διαμάντια, φυσικό αέριο και όχι από κράτη και τραπεζικά ιδρύματα ως παραδοσιακό χρήμα (fiat). Η πολιτική πλαισίωση της σκέψης ήταν η απομάκρυνση από το "σύστημα καταπιστευτικής διαχείρισης" που ισχύει αυτήν τη στιγμή. Στη Λευκή Βίβλο Petro Cryptocurrency της Βενεζουέλας, το Petro περιγράφεται ως ένα «μέσο για την οικονομική ασφάλεια και την οικονομική ανεξαρτησία της Βενεζουέλας, σε συνδυασμό με ένα φιλόδοξο και παγκόσμιο όραμα για τη δημιουργία ενός πιο ελεύθερου, πιο ισορροπημένου και δικαιότερου διεθνούς χρηματοπιστωτικού συστήματος». [41]

Ενώ είναι σαφές ότι το Petro, και οποιοδήποτε κρυπτονόμισμα, έχει ικανότητα δημιουργίας ενός πιο ελεύθερου και ανεξάρτητου συστήματος διεθνούς εμπορίου, ένα ζωτικό ερώτημα για τη Βενεζουέλα είναι αν η εισαγωγή του Petro, και η σύνδεση του Bolivar στο Petro, θα λειτουργήσει πραγματικά ως μέσο για την οικονομική ασφάλεια της Βενεζουέλας. Η κυβέρνηση της Βενεζουέλας ανακοίνωσε ότι το Bolivar επρόκειτο να συνδεθεί με το Petro, και το Bolivar υποτιμήθηκε κατά 96% σε μια προσπάθεια να σταματήσει η ελεύθερη πτώση του. Το Petro θεωρήθηκε ικανό να βελτιώσει την οικονομία της Βενεζουέλας δεδομένου ότι θα μπορούσε να παρακάμψει τις κυρώσεις των ΗΠΑ και να αποκτήσει η χώρα πρόσβαση στη διεθνή χρηματοδότηση. [41] Παράλληλα, συζητήθηκαν φορολογικά μέτρα, περικοπές στις επιδοτήσεις ορισμένων προϊόντων όπως της βενζίνης, ενώ η κυβέρνηση ανακοίνωσε και τρίμηνη επιδότηση των μικρών και μεσαίων ιδιωτικών επιχειρήσεων στις διαφορές που θα προέκυπταν στους μισθούς εργαζομένων από το πέρασμα στο νέο νόμισμα.

Με την έκδοση του Petro, η κρατική εταιρεία πετρελαίου της Βενεζουέλας σκοπεύει να αυξήσει την παραγωγή στα 1,25 εκατ. βαρέλια τη μέρα, εφόσον έκλεισε συμφωνίες με επτά εταιρείες, συμπεριλαμβανομένων των «Shandong Kerui» (όμιλος με έδρα την Kiva) και «Helios Petroleum Services» του Παναμά. Πολλοί είναι όμως οι

αναλυτές που αντιτείνουν ότι το Petro δεν αποτελεί πραγματικό κρυπτονόμισμα, αλλά ένα οικονομικό εργαλείο βασιζόμενο την τεχνολογία Blockchain, που δημιουργήθηκε από την κυβέρνηση της Βενεζουέλας. Δεν μπορεί να εξορύσσεται, ούτε υποστηρίζεται στην πραγματικότητα από αποθέματα πετρελαίου, η κυβέρνηση διατηρεί τον πλήρη έλεγχό του, δεν είναι νόμισμα διεθνώς διαπραγματεύσιμο, ενώ η εγγενής αξία του είναι αυθαίρετη. [41]

Συνολικά, τα μέτρα που πάρθηκαν από την κυβέρνηση της Βενεζουέλας, φαίνεται πως **δεν επηρεάζουν τη βάση της οικονομίας της.** Η εκτεταμένη χρήση ενός εθνικού κρυπτονομίσματος απαιτεί εκπαίδευση του πληθυσμού, και δυνατότητα πρόσβασης σε τεχνολογικά μέσα. Ακόμα και έτσι όμως, από οικονομική σκοπιά, η επίλυση των σοβαρών προβλημάτων βιοτικού επιπέδου που αντιμετωπίζουν τα φτωχότερα στρώματα της Βενεζουέλας, δεν συσχετίζεται πρακτικά με τη γενικευμένη χρήση μιας διαφορετικής μορφής χρήματος. Απαιτούνται άλλου είδους ανατροπές σε επίπεδο οικονομίας. Παρόλα αυτά, η προσπάθεια της Βενεζουέλας άνοιξε το δρόμο, θέτοντας το ζήτημα υιοθέτησης εθνικών κρυπτονομισμάτων, ή ψηφιακών νομισμάτων, επί τάπητος για πολλές χώρες. Η Ρωσία, η Τράπεζα της Αγγλίας και η Κεντρική Τράπεζα της Κίνας έχουν εκφράσει ενδιαφέρον να χρησιμοποιήσουν την τεχνολογία του Bitcoin για τα δικά τους ψηφιακά νομίσματα, ενώ η Κεντρική Τράπεζα της Γερμανίας, προτίθεται να χρησιμοποιήσει την τεχνολογία blockchain για την προστασία των συναλλαγών. Για τους λόγους αυτούς, και οι τρεις αυτές χώρες έχουν θέσει περιοριστικά και απαγορευτικά μέτρα στην εξαγωγή συναλλάγματος με τη χρήση του Bitcoin.

• ΤΟ ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ

Το **ψηφιακό νόμισμα, το οποίο προέρχεται από κάποια Κεντρική Τράπεζα (CBDC),** είναι τελείως διαφορετικής λογικής από τα κρυπτονομίσματα. Διαφέρει τεχνολογικά και λειτουργεί με διαφορετική φιλοσοφία. Στην πραγματικότητα αποτελεί εξέλιξη των ψηφιακών συναλλαγών, χωρίς να απομακρύνεται εξαιρετικά από αυτό που γνωρίζουμε σήμερα. Φαινομενικά, τα χρήματα είναι ήδη ψηφιακά, καθώς οι πιστωτικές κάρτες και οι εφαρμογές πληρωμών όπως το Apple Pay στις ΗΠΑ και το WeChat στην Κίνα εξαλείφουν την ανάγκη για χαρτονομίσματα ή κέρματα. Όμως οι εφαρμογές αυτές αποτελούν τρόπους να μεταφέρονται χρήματα ηλεκτρονικά. Το CBDC διαφοροποιείται επειδή αποτελεί το νόμιμο χρήμα σε ψηφιακή μορφή, το οποίο υποστηρίζεται από την κεντρική τράπεζα και είναι πλήρως ελεγχόμενο από αυτήν. Ενώ τα κρυπτονομίσματα, όπως το Bitcoin, λειτουργούν εκτός του παραδοσιακού χρηματοπιστωτικού συστήματος και δεν αναγνωρίζονται ως νόμιμο χρήμα, τα CBDC σχεδιάζονται για να παρέχουν στις κυβερνήσεις και στις κεντρικές τράπεζες τον έλεγχο της προσφοράς και της κυκλοφορίας των χρημάτων σε ψηφιακή μορφή. Ένα παράδειγμα είναι το **Ψηφιακό Γουάν (e-CNY)**, (επίσημα ονομάζεται **Digital Currency Electronic Payment - DCEP**). Το e-CNY είναι ένα ψηφιακό νόμισμα που εκδίδεται και ελέγχεται από την **Λαϊκή Τράπεζα της Κίνας (PBOC)**, η οποία είναι η κεντρική τράπεζα της χώρας. Το έργο για την ανάπτυξή του ξεκίνησε το **2014**, όταν η κεντρική τράπεζα της Κίνας δημιούργησε μια ομάδα για την έρευνα και ανάπτυξη του ψηφιακού νομίσματος. Οι πρώτες πιλοτικές δοκιμές του e-CNY ξεκίνησαν το **2020** σε διάφορες πόλεις της Κίνας, όπως το Σενζέν, η Σούζου και το Πεκίνο, με στόχο την ευρύτερη διάδοσή του και την προώθησή του ως συμπλήρωμα του φυσικού χρήματος, παρέχοντας στη χώρα τη δυνατότητα να παρακολουθεί καλύτερα τόσο την οικονομία όσο και τις οικονομικές δραστηριότητες των πολιτών της, σε αντίθεση με την ανωνυμία που χαρακτηρίζει πολλά κρυπτονομίσματα.

Το ψηφιακό νόμισμα, αναμένεται να συμβάλλει στη βελτιστοποίηση των λειτουργιών πληρωμής, στη μείωση της εξάρτησης από υπηρεσίες πληρωμών που παρέχονται από τον ιδιωτικό τομέα, στην "ανακούφιση" των κεντρικών τραπεζών από επιβαρύνσεις και πιέσεις γραφειοκρατικού και ρυθμιστικού χαρακτήρα. Επιπλέον, η έκδοση ψηφιακού νομίσματος CBDC αναμένεται να συμβάλλει στην αντιμετώπιση διλημμάτων που προκύπτουν στην εφαρμογή σύγχρονων νομισματικών πολιτικών, συμπεριλαμβανομένων των δυσκολιών στη μετάδοση μιας νέας πολιτικής, στη ροή του νομίσματος από την πραγματική οικονομία στην εικονική οικονομία και στην ανεπαρκή διαχείριση των προσδοκιών μιας πολιτικής.

Συγκεκριμένα, ένας πιθανός τρόπος εισαγωγής ενός τέτοιου νομίσματος, μέσω της κεντρικής τράπεζας θα ήταν η κυκλοφορία του ψηφιακού νομίσματος μεταξύ ιδιωτών και επιχειρήσεων, με κωδικούς QR για παράδειγμα και ηλεκτρονικά πορτοφόλια, με σπάνιο το ενδεχόμενο επανακατάθεσης χρημάτων πίσω στην κεντρική τράπεζα. Όπως το bitcoin, αυτή η προσέγγιση θα χρησιμοποιούσε κάποια μορφή τεχνολογίας κατανεμημένου καθολικού προκειμένου να επαληθεύεται η αλυσίδα και να επικυρώνονται οι συναλλαγές, χωρίς να απαιτείται η άμεση συμμετοχή της κεντρικής τράπεζας ή οποιουδήποτε άλλου τρίτου. Σε αντίθεση με το bitcoin και άλλα κρυπτονομίσματα, ωστόσο, η κεντρική τράπεζα θα καθορίζει την προσφορά των νομισμάτων CBDC, που θα καθορίζεται σε ονομαστικούς όρους και θα μπορεί να χρησιμοποιείται ως νόμιμο χρήμα. Επιπλέον, η κεντρική τράπεζα θα μπορούσε να καθιερώσει διαφανείς διαδικασίες για την ενσωμάτωση κατάλληλων ενημερώσεων στο λογισμικό αυτό - μια πρόκληση που έχει αποδειχθεί δύσκολη στην περίπτωση των εικονικών νομισμάτων. Κάτω από τον εναλλακτικό αυτό σχεδιασμό (που είναι ανάλογος με αυτόν των χρεωστικών καρτών), τα άτομα και οι εταιρείες θα διαχειρίζονται κεφάλαια ηλεκτρονικά, σε λογαριασμούς / πορτοφόλια CBDC που θα ανήκουν και θα διατηρούνται στην κεντρική τράπεζα ή σε ειδικούς λογαριασμούς εποπτευόμενων ιδρυμάτων. Υπό αυτήν την προσέγγιση, η κεντρική τράπεζα θα επεξεργαζόταν κάθε συναλλαγή πληρωμής απλά χρεώνοντας το λογαριασμό CBDC του πληρωτή και πιστώνοντας το λογαριασμό CBDC του δικαιούχου. Ένα σημαντικό πλεονέκτημα ενός τέτοιου συστήματος που βασίζεται στους λογαριασμούς, είναι ότι θα μπορούσαν οι πληρωμές με CBDC να πραγματοποιούνται στιγμιαία και χωρίς κόστος. Η δημιουργία και η ταυτοποίηση ενός νέου χρήστη ενδεχομένως να ήταν χρονοβόρα σε αρχικό στάδιο, ενώ θα απαιτούνταν και αρκετά μέτρα ασφαλείας ώστε να οι συναλλαγές να παραμένουν ασφαλείς.

Στην περίπτωση χρήσης ενός συστήματος που βασίζεται σε tokens, το κόστος θα ήταν πολύ μεγαλύτερο, αφού θα πρέπει να βρεθούν λύσεις αποθήκευσης των αλυσίδων κρυπτογραφημένου καθολικού (blockchain) με δεδομένο ότι ένα αντίγραφο αυτού του καθολικού πρέπει να αποθηκεύεται σε κάθε κόμβο του δικτύου πληρωμών. Οι νέες συναλλαγές θα συλλέγονται σε μπλοκ που πρέπει να επαληθευτούν προτού προστεθούν μόνιμα στην αλυσίδα. Αυτή η διαδικασία επαλήθευσης - που πραγματοποιείται στο στάδιο εξόρυξης - περιλαμβάνει υπολογιστικές διαδικασίες που είναι πολύ περίπλοκες και απαιτούν χρόνο αλλά και ενέργεια. Ένα CBDC βασισμένο στην τεχνολογία των κρυπτονομισμάτων, μπορεί να είναι προτιμότερο από τις υπάρχουσες φόρμες συναλλαγών, αλλά θα ήταν πολύ λιγότερο αποτελεσματικό από ένα CBDC που λειτουργεί με ταυτοποιημένους λογαριασμούς χρηστών.

Ακόμα, ένα ψηφιακό νόμισμα CBDC δεν είναι απαραιτητο να στοχεύει σε μονοπώλιο του συστήματος πληρωμών, αλλά θα μπορούσε και να συμπληρώνει τις υπηρεσίες πληρωμών που παρέχονται από ιδιωτικούς φορείς. [43]

Τέλος, είναι αρκετοί αυτοί που υποστηρίζουν πως **το φυσικό χρήμα θα αντικατασταθεί σε ένα βάθος χρόνου με το ψηφιακό χρήμα**. Πρέπει σε αυτό το συλλογισμό να λάβουμε υπόψιν το εξής. Η οικονομία βασισμένη σε ψηφιακά νομίσματα, αφενός είναι πολύ πιθανό να μαστίζεται από αβεβαιότητα, καθώς ενδέχεται να μην μπορεί να υπάρξει σχετική ισορροπία χωρίς πολύ μεγάλες διακυμάνσεις των τιμών. Κάποιοι αναλυτές υποστηρίζουν πως η σταθερότητα των τιμών μπορεί να διασφαλιστεί με την έκδοση ενός CBDC σε **συνδυασμό με ένα κατάλληλο πλαίσιο νομισματικής πολιτικής** (ανάλυση των Fernández-Villaverde και Sanches, 2017). Το ζήτημα όμως της σταθερότητας συνδέεται και με την ίδια **τη φύση των τραπεζών ως πιστωτικά ιδρύματα.** Πρέπει να τονιστεί ότι αυτές οι ανησυχίες δεν είναι ακαδημαϊκές, επισημαίνονται και από κεντρικούς τραπεζίτες. Για παράδειγμα, ο Nicolaisen (2017) προειδοποίησε συγκεκριμένα για τους κινδύνους που σχετίζονται με το σενάριο σύμφωνα με το οποίο η νορβηγική οικονομία δεν θα έχει πλέον κανένα λειτουργικό νόμιμο χρήμα. Αν υποθέσουμε ότι το χαρτονόμισμα καθίσταται ξεπερασμένο και ότι η νομισματική βάση περιλαμβάνει αποκλειστικά τα αποθεματικά των τραπεζών που βρίσκονται στην κεντρική τράπεζα. Δημιουργείται αβεβαιότητα ως προς το αν για παράδειγμα το επιτόκιο στα αποθεματικά (IOR) θα παραμένει στενά συνδεδεμένο με τα επιτόκια της αγοράς, έτσι ώστε η κεντρική τράπεζα να μπορεί να συνεχίσει να προσαρμόζεται στις νομισματικές συνθήκες, όπως απαιτείται. Το IOR παρέχει ένα κατώτατο όριο για το διατραπεζικό επιτόκιο δανεισμού, και με επαρκώς υψηλό βαθμό αποθεματικών, ουσιαστικά καθορίζει το επίπεδο των επιτοκίων της αγοράς. Υπάρχουν λοιπόν ανησυχίες για δυνητικά αδύναμους δεσμούς μεταξύ των επιτοκίων της αγοράς και IOR. Φυσικά, αυτή η λογική οδηγεί στο σκεπτικό για την εισαγωγή ενός CBDC με την ικανότητα να φέρει επιτόκια και που να μπορεί να είναι διαχειρίσιμο, ώστε να διασφαλίζεται η ικανότητα της κεντρικής τράπεζας να διαχειρίζεται τα επιτόκια της αγοράς με την πάροδο του χρόνου. [43]

Η εισαγωγή ενός CBDC μπορεί, λοιπόν, να μην σημαίνει τον αποκλεισμό των ιδιωτικών συστημάτων πληρωμών, αλλά τη συμπληρωματική τους χρήση. Η χρήση του ψηφιακού γουάν (e-CNY) έχει προσφέρει σημαντικές πληροφορίες και συμπεράσματα, τόσο στην Κίνα όσο και παγκοσμίως, για το μέλλον των ψηφιακών νομισμάτων κεντρικών τραπεζών (CBDCs). Τα βασικά συμπεράσματα από τη χρήση του περιλαμβάνουν:

1. **Βελτιστοποίηση των Πληρωμών**: Το e-CNY έχει βελτιώσει τις διαδικασίες πληρωμών, κάνοντάς τις πιο γρήγορες και αποδοτικές, ειδικά για συναλλαγές χαμηλού κόστους, όπως οι καθημερινές αγορές. Οι χρήστες μπορούν να κάνουν πληρωμές χωρίς την ανάγκη παραδοσιακών τραπεζικών μεσαζόντων.

2. **Ενίσχυση της Οικονομικής Συμμετοχής**: Το ψηφιακό γουάν προωθεί την οικονομική συμπερίληψη, καθώς μπορεί να χρησιμοποιηθεί από ανθρώπους που δεν έχουν πρόσβαση σε παραδοσιακές τραπεζικές υπηρεσίες, μέσω απλών ηλεκτρονικών πορτοφολιών.

3. **Έλεγχος και Παρακολούθηση**: Το e-CNY παρέχει στη Λαϊκή Τράπεζα της Κίνας τη δυνατότητα να παρακολουθεί τις οικονομικές συναλλαγές σε πραγματικό χρόνο. Αυτό ενισχύει τον έλεγχο της κυβέρνησης πάνω στην οικονομία και μπορεί να χρησιμοποιηθεί για την καταπολέμηση της φοροδιαφυγής και του ξεπλύματος χρήματος.

4. **Περιορισμός της Ανωνυμίας**: Σε αντίθεση με τα κρυπτονομίσματα όπως το Bitcoin, το e-CNY δεν προσφέρει ανωνυμία. Οι συναλλαγές μπορούν να ελέγχονται από τις αρχές, κάτι που εγείρει ανησυχίες για την ιδιωτικότητα των χρηστών.

5. **Αντικατάσταση Μετρητών**: Το ψηφιακό γουάν θεωρείται ένα βήμα προς τη μείωση της χρήσης φυσικού χρήματος, ιδιαίτερα στην Κίνα, όπου οι ψηφιακές πληρωμές μέσω εφαρμογών όπως το WeChat Pay και το Alipay κυριαρχούν ήδη.

6. **Διεθνείς Συναλλαγές**: Το e-CNY θα μπορούσε να χρησιμοποιηθεί για να μειώσει την εξάρτηση από το δολάριο ΗΠΑ στις διεθνείς συναλλαγές και να ενισχύσει τη θέση της Κίνας στο παγκόσμιο χρηματοοικονομικό σύστημα. Ωστόσο, μέχρι τώρα οι διεθνείς χρήσεις του είναι περιορισμένες.

7. **Ανταγωνισμός με Ιδιωτικές Πλατφόρμες Πληρωμών**: Το e-CNY δημιουργεί ανταγωνισμό για τις ιδιωτικές πλατφόρμες πληρωμών όπως το WeChat Pay και το Alipay, δίνοντας στο κράτος μεγαλύτερο έλεγχο στο οικοσύστημα των πληρωμών.

8. **Πιλοτικές Δοκιμές και Υιοθέτηση**: Αν και οι πιλοτικές δοκιμές του e-CNY έδειξαν θετική αποδοχή, η ευρεία υιοθέτησή του από τους πολίτες δεν είναι ακόμη σίγουρη. Υπάρχει ανταγωνισμός από τις ήδη καθιερωμένες ψηφιακές πλατφόρμες, και η πλήρης μετάβαση σε ένα ψηφιακό νόμισμα θα απαιτήσει χρόνο.

Το 2024, τα ψηφιακά νομίσματα των κεντρικών τραπεζών (CBDCs) παρουσίασαν ραγδαία εξέλιξη σε παγκόσμιο επίπεδο. Συγκεκριμένα, **134 χώρες είχαν προχωρήσει σε εξερεύνηση ή εφαρμογή CBDCs, καλύπτοντας το 98% της παγκόσμιας οικονομίας.** Από αυτές, οι 66 χώρες βρίσκονταν σε προηγμένες φάσεις, όπως ανάπτυξη, πιλοτικές δοκιμές ή ακόμα και πλήρης εφαρμογή. Οι Μπαχάμες, η Τζαμάικα και η Νιγηρία έχουν ήδη κυκλοφορήσει τα CBDCs τους σε εθνικό επίπεδο.

Πολλές χώρες της **G20**, όπως η Βραζιλία, η Ιαπωνία, η Ινδία, η Αυστραλία και η Ρωσία, προχώρησαν σε **πιλοτικές φάσεις**, ενώ η Ευρώπη εξετάζει σοβαρά την εφαρμογή **ψηφιακού ευρώ** τόσο σε εσωτερικό επίπεδο όσο και για διασυνοριακές συναλλαγές. Ορισμένα έργα, όπως το «**mBridge**» που συνδέει την Κίνα, την Ταϊλάνδη, τα Ηνωμένα Αραβικά Εμιράτα, το Χονγκ Κονγκ και τη Σαουδική Αραβία, έχουν ως στόχο την ανάπτυξη ενός εναλλακτικού συστήματος πληρωμών που μειώνει την εξάρτηση από το δολάριο.

Οι κεντρικές τράπεζες διαδραματίζουν καθοριστικό ρόλο σε αυτήν τη μετάβαση, με προσεκτική ανάλυση για τη διασφάλιση της διαφάνειας και της ασφάλειας στις συναλλαγές.[45]

3.3 ΠΡΑΓΜΑΤΙΚΗ ΟΙΚΟΝΟΜΙΑ - ΕΠΙΧΕΙΡΗΣΕΙΣ & ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Πολλές φορές, ένα εξαιρετικά ρυθμιζόμενο χρηματοοικονομικό περιβάλλον, μπορεί να δημιουργεί προβλήματα σε αναπτυσσόμενες επιχειρήσεις, κυρίως σε θέματα που σχετίζονται με πίστωση ή χρηματοδότηση, συγκέντρωση κεφαλαίων και άλλα. Η έκδοση ενός **εταιρικού κρυπτονομίσματος** ή **token**, θεωρητικά θα μπορούσε να προσπεράσει τις δυσκολίες αυτές, αφού η επιχείρηση θα μπορεί να δανείζεται από τρίτους ή ακόμα και από εσωτερικά τμήματα της ίδιας της εταιρείας, να αποκτά επενδυτές που θα συνδέονται άμεσα με την επιχείρηση. Ωστόσο, στην πράξη, απαιτείται δημόσια αποδοχή του κρυπτονομίσματος αυτού και η επιτυχία εξαρτάται σε μεγάλο βαθμό από το δίκτυο εντός του οποίου το χρησιμοποιεί η εταιρεία. Πρέπει να υπάρχει μια τάση για συναλλαγές με το συγκεκριμένο μέσο ανταλλαγής ώστε να αποκτά αξία και να μπορούν εν τέλει να πραγματοποιούνται οι επιθυμητές συναλλαγές. Εαν αυτό είναι κατορθωτό, και πάλι θεωρητικά σε μια ανοιχτή αγορά αποτελεί αναμφισβήτητη βοήθεια προς τους μεσαίους επιχειρηματίες για τη συγκέντρωση κεφαλαίων, και την επέκταση των δραστηριοτήτων τους σε μια ευρύτερη κοινότητα. Από την άλλη πλευρά, όμως, είναι σημειωτέο πως η αξιοποίηση μιας τέτοιας τεχνολογίας απαιτεί και ένα αρκετά υψηλό επίπεδο τεχνολογικών γνώσεων που πιθανώς απουσιάζει σε μεγάλο αριθμό μικρών και μεσαίων επιχειρήσεων, αλλά και μεγάλο βαθμό εξοικείωσης με αυτή την τεχνολογία του κοινού στο οποίο απευθύνεται η επιχείρηση. Σε επίπεδο επιχειρήσεων, υπάρχει μικρή εμπειρία. Έχουμε δει κάποιες επιχειρήσεις να εκδίδουν tokens και να τα μετατρέπουν αργότερα σε μετοχές, ή να τα χρησιμοποιούν για επενδυτικούς και άλλους λόγους χωρίς όμως να αποκτούν ιδιαίτερη δημοφιλία.

Η μεγαλύτερη προσπάθεια κατασκευής ενός τέτοιου μέσου ανταλλαγής πραγματοποιείται από την εταιρεία **Facebook**, που όπως αναφέρθηκε και σε προηγούμενη παράγραφο προσβλέπει στη δημιουργία του δικού της κρυπτονομίσματος, αναμένοντας το κατάλληλο ρυθμιστικό πλαίσιο. Η βλέψη αυτή όπως είναι φυσικό έχει ταράξει τους οικονομικούς κύκλους, αφού μιλάμε για μια πλατφόρμα με εκατομμύρια χρήστες και μια τέτοια ενέργεια είναι πιθανό να διαδραματίσει καθοριστικό ρόλο για τα τεκταινόμενα στον τομέα της οικονομίας παγκοσμίως. Αυτός είναι και ο λόγος που οι ρυθμιστικές αρχές υπογραμμίζουν τη μετατροπή της πλατφόρμας σε "σκιώδη τράπεζα" και ενίστανται σχετικά με την προστασία των προσωπικών δεδομένων των χρηστών, απευθύνθηκαν όμως ανοιχτά και στο ζήτημα ενδεχόμενης διατάραξης της χρηματοοικονομικής σταθερότητας από ένα τέτοιο εγχείρημα. Ο **Ντέιβιντ Μάρκους**, επικεφαλής της Facebook Financial, γνωστής και ως F2, επιμένει: «Ελπίζουμε ότι θα συμμετέχουμε με το Novi (ψηφιακό πορτοφόλι) και το Diem (κρυπτονόμισμα) στις μεγάλες αλλαγές του 2021, λαμβάνοντας τις ρυθμιστικές εγκρίσεις όπου χρειάζεται να τις λάβουμε», μεταξύ άλλων, στο Singapore FinTech Festival, απαντώντας σε ερώτηση για τις μεγαλύτερες αλλαγές στις χρηματοοικονομικές υπηρεσίες για τη χρονιά που έρχεται. Το πρότζεκτ με το κρυπτονόμισμα του Facebook μετά από την κριτική που δέχτηκε από τις ρυθμιστικές αρχές, μεταβλήθηκε ως προς τους στρατηγικούς στόχους καθώς και ως προς την ονομασία που θα έφερε. Αρχικά η ονομασία που είχε αποδοθεί στο κρυπτονόμισμα ήταν Libra και προορίζονταν να είναι διαχειρίσιμο από μια μη κερδοσκοπική κοινοπραξία 28 μεγάλων εταιρειών με την ονομασία Libra Association, ενώ το ψηφιακό πορτοφόλι έφερε την ονομασία Calibra. Στο κλίμα άρνησης, η Libra Association ανέστειλε τα σχέδιά της και ανακοίνωσε ότι θα προσφέρει σταθερά νομίσματα που θα υποστηρίζονται μόνο από ένα εθνικό νόμισμα. Έπειτα το όνομα της κοινοπραξίας μεταβλήθηκε σε Diem Association, με έδρα την Ελβετία. Η Diem Association αυτή τη στιγμή αναμένει έγκριση από την ελβετική επιτροπή κεφαλαιαγοράς. [44]

Το Diem περιγράφεται ως κρυπτονόμισμα όμως στην πραγματικότητα θα λειτουργεί περίπου ως ψηφιακό νόμισμα, αφού στηρίζεται από ένα ισχυρό όμιλο. Ακόμη ενδέχεται να υποστηρίζεται και από ένα παραστατικό νόμισμα (fiat currency) ή αλλιώς νόμισμα αναγκαστικής κυκλοφορίας που δεν θα καλύπτεται από αποθεματικό άλλων υλικών (όπως πχ. ο χρυσός), κάτι που είναι εκτός της φιλοσοφίας των κρυπτονομισμάτων. Η Diem Association, προσβλέπει στη δημιουργία ενός απλού στη χρήση, παγκόσμιου, καινοτόμου συναλλάγματος, και βρίσκεται σε διάλογο με κεντρικούς τραπεζίτες, ρυθμιστικές αρχές και άλλους φορείς προκειμένου να καρπωθεί μερίδιο του λέοντος στην ψηφιακή εξέλιξη της οικονομίας, παντρεύοντας την τεχνολογία blockchain, με αποδεκτά ρυθμιστικά πλαίσια. Να χρησιμοποιείται το δικό της ψηφιακό συνάλλαγμα δίπλα στα τοπικά συναλλάγματα, μειώνοντας δραστικά τα κόστη διεθνών συναλλαγών. [44]

Η τεχνολογία στην οποία θα βασιστεί ένα τέτοιο εγχείρημα, οι οικονομικές επιπτώσεις αλλά και η ευρύτερη επίδραση στους επιχειρηματικούς κύκλους, είναι παράγωγα ζητήματα εξαιρετικού ενδιαφέροντος.

ΕΙΚΟΝΑ 16 - Diem logo, ΠΗΓΗ: https://www.diem.com

3.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ & ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΧΡΗΣΗΣ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

- ΠΛΕΟΝΕΚΤΗΜΑΤΑ

1. Διακίνηση κεφαλαίων χωρίς κόστος : Τα κρυπτονομίσματα παρέχουν τη δυνατότητα μεταφοράς χρηματικών ποσών ανεξαρτήτως ύψους, άμεσα, οπουδήποτε στον κόσμο, οποιαδήποτε στιγμή, χωρίς να βαρύνεται με χρεώσεις. Τα πολιτικά τεκταινόμενα της κάθε χώρας δεν μπορούν να επηρεάσουν τις συναλλαγές. Ο χρήστης ελέγχει πλήρως τα κεφάλαιά του.

2. Ασφάλεια & Σχετική ιδιωτικότητα συναλλαγών: Οι συναλλαγές δεν ελέγχονται από καμία κεντρική τράπεζα ή κάποιο εξουσιοδοτημένο τρίτο φορέα. Άρα δεν είναι εύκολα εφικτή η καταγραφή και παρακολούθηση των συναλλαγών κάποιου χρήστη. Ο χρήστης μπορεί εαν έχει τις γνώσες να προστατέψει τα προσωπικά του δεδομένα, κάνοντας χρήση των κατάλληλων λογισμικών, ενώ ο λογαριασμός του δεν μπορεί να δεσμευτεί από κάποιον πάροχο.

3. Χρήση Υποδιαιρέσεων (units): Κάθε Bitcoin είναι υποδιαιρέσιμο έως 8 δεκαδικά ψηφία (έως 0,00000001). Παρομοίως, υποδιαιρέσεις υπάρχουν σε όλα τα κρυπτονομίσματα, ώστε ανεξαρτήτως ισοτιμίας, να επιτρέπονται μικρό-συναλλαγές. Χαρακτηριστικό που ξεχωρίζει τα κρυπτονομίσματα από τα συμβατικά χρήματα.

4. Φορητότητα και ασφάλεια : Τα «πορτοφόλια» όπου φυλάσσονται τα κρυπτονομίσματα (wallets), είναι εύχρηστα και μεταφέρονται σε συμβατικά smartphones. Ακόμα, ανάλογα με την εφαρμογή που χρησιμοποιεί ο κάθε χρήστης, υπάρχουν δικλείδες ασφαλείας, ώστε σε διάφορες περιπτώσεις να διατηρήσει τον έλεγχο του ψηφιακού του πορτοφολιού.

- ΜΕΙΟΝΕΚΤΗΜΑΤΑ

1. Επίπεδο εξοικείωσης χρηστών : Ο αριθμός των επιχειρήσεων αλλά και του συνόλου των χρηστών που χρησιμοποιούν κρυπτονομίσματα για καθημερινές συναλλαγές είναι ακόμα πολύ μικρός. Ως εκ τούτου, οι συναλλαγές όπως και οι ισοτιμίες είναι ευμετάβλητες και εξαρτώμενες από τον όγκο των συναλλαγών, τις συμπεριφορές των χρηστών και τις εκάστοτε ανακοινώσεις των ρυθμιστικών αρχών και των κυβερνήσεων. Τα εγχειρίδια που έχουν εκδοθεί δεν αποτελούν ευρύ εκπαιδευτικό υλικό που να μπορεί να καλύψει το σύνολο ενός μη εξοικειωμένου με την τεχνολογία πληθυσμού.

2. Εξασφάλιση των ιδιωτικών κλειδιών: Η τεχνολογία blockchain, χαρακτηρίζεται για την ασφάλεια που δύναται να παρέχει στο μέσο χρήστη, υπάρχει όμως πάντα η πιθανότητα προσβολής από κακόβουλα λογισμικά. Γύρω από την εξελισσόμενη τεχνολογία πληθαίνουν και τα κακόβουλα λογισμικά που μπορούν να βλάψουν τον χρήστη με ανοιχτό το ενδεχόμενο ακόμη και να χάνονται χρηματικά ποσά. Έτσι λοιπόν οι χρήστες θα πρέπει να κρατούν ως επτασφράγιστο μυστικό τα ιδιωτικά τους κλειδιά ώστε να είναι ασφαλείς απέναντι σε τέτοιες επιθέσεις.

3. Διακύμανση ισοτιμίας: Τα κρυπτονομίσματα εκ φύσεως είναι ανεξάρτητα από κάποια κεντρική αρχή με τη δυνατότητα να παρεμβαίνει στις εξελίξεις ή τις διακυμάνσεις της προσφοράς και της ζήτησης όπως συμβαίνει με τα κοινά νομίσματα. Είναι όμως επιρρεπή σε πολύ μεγάλες διακυμάνσεις της ισοτιμίας τους με τα περισσότερα φυσικά σε κυκλοφορία νομίσματα. Επιπλέον παράγοντας που επηρεάζει το παραπάνω φαινόμενο είναι ο μικρός όγκος χρηστών και συναλλαγών συγκριτικά με το σύνολο των συναλλαγών που πραγματοποιούνται, πράγμα που σημαίνει ότι όταν συναλλάσσονται μεγάλα ποσά σε κρυπτονομίσματα, επηρεάζονται δυσανάλογα οι ισοτιμίες στα ανταλλακτήρια.

4. Παράνομες αγορές και δραστηριότητες: Εφόσον τα κρυπτονομίσματα στερούνται ρυθμιστικού πλαισίου, και λόγω της ψευδωνυμοποίησης των συναλλαγών, αποτελούν εργαλεία που μπορούν να χρησιμοποιηθούν για παράνομες διαδικτυακές συναλλαγές, όπως αυτές που αφορούν φάρμακα, ναρκωτικά, όπλα, είδη ή αντικείμενα μεγάλης αξίας τα οποία δεν είναι εύκολο να συναλλαχθούν σε πραγματικές αγορές χωρίς να υπάρξει κάποιος έλεγχος. Έχουν αναπτυχθεί ακόμα και κακόβουλες διαδικτυακές ιστοσελίδες, οι οποίες διαφημίζονται ως ανταλλακτήρια αλλά στην πραγματικότητα εκμαιεύουν χρηματικά ποσά από τον χρήστη, ή υποκλέπτουν τα στοιχεία του.

5. Βρίσκεται σε στάδιο ανάπτυξης: Τέλος, τα κρυπτονομίσματα και η τεχνολογία πάνω στην οποία βασίζονται, είναι αυτή τη στιγμή σε αρχικά σχετικά στάδια ανάπτυξης. Έτσι εμφανίζονται αδυναμίες στη λειτουργία που αφορούν θέματα ασφάλειας, προσβασιμότητας, ανάπτυξης εργαλείων και υπηρεσιών, χωρητικότητας, χρόνου εκτέλεσης των συναλλαγών και πολλά άλλα. Από την άλλη μπορούμε να επιχειρηματολογήσουμε πως ακριβώς το ίδιο χαρακτηριστικό αποτελεί "ευκαιρία" για τους επενδυτές ώστε να αποσπάσουν κέρδη αλλά και τους επιστήμονες της πληροφορικής ώστε να καινοτομήσουν στο πεδίο αυτό.

3.5 ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ - ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΚΡΥΠΤΟΟΙΚΟΝΟΜΙΑΣ

Οι **τεχνολογικές εξελίξεις στον τομέα της οικονομίας συνολικά**, απασχολούν όλες τις κυβερνήσεις και τις Κεντρικές Τράπεζες παγκοσμίως. Η εισαγωγή και η απογείωση του Bitcoin, έφεραν την τεχνολογία Blockchain στην καθημερινότητα. Οι εφαρμογές γύρω από αυτή την τεχνολογία θα απασχολήσουν όλους σχεδόν τους τομείς της οικονομίας και όχι μόνο καθεαυτό τον τομέα της οικονομίας, τις ρυθμιστικές αρχές ή τις κυβερνήσεις και τις κεντρικές τράπεζες.

Έχει σημασία να υπογραμμίσουμε αρχικά ότι η εξέλιξη της τεχνολογίας πραγματοποιείται στα πλαίσια ενός οικονομικού περιβάλλοντος και σε αυτά τα πλαίσια οφείλουμε να εξετάζουμε τις επιπτώσεις ή να προβλέπουμε τις εξελίξεις που σχετίζονται με αυτήν. Η δημιουργία μιας "από τα κάτω" οικονομίας, μιας οικονομίας ελεγχόμενης αποκλειστικά από τους συμμετέχοντες-χρήστες, είναι μια πολύ ελκυστική ιδέα, όμως δεν πρέπει να αφαιρούμε από το συλλογισμό αυτό ότι τα κρυπτονομίσματα εισάγονται σε μια οικονομική πραγματικότητα τελείως διαφορετική. Ότι δεν μπορεί να υπάρξει μια οικονομία που να κινείται παράλληλα ή μέσα στην υπάρχουσα πραγματικότητα, αλλά πάντα αργά ή γρήγορα θα συμμορφώνεται στους κανόνες που ισχύουν ευρύτερα στην κοινωνία. Η κοινωνία δομείται σε μια οικονομική βάση, η οποία χαρακτηρίζεται από την ιδιοκτησία ως προς τα μέσα παραγωγής και τις σχέσεις που προκύπτουν από αυτήν. Ο πυρήνας αυτός δεν μπορεί να μεταβάλλεται λόγω εξελίξεων, αντιθέτως καθορίζει τις εξελίξεις στον κοινωνικό ιστό. Βλέπουμε λοιπόν, ότι ακόμα και αν υποθέσουμε ότι στις πρώτες συναλλαγές που πραγματοποιούνταν οι χρήστες μπορούσαν να ανταλλάσουν προϊόντα και υπηρεσίες κάνοντας χρήση μιας νέας, ουσιαστικά, μορφής χρήματος, του Bitcoin, αφενός το νόμισμα αυτό τη δεδομένη χρονική στιγμή δεν είχε καμία αξία ευρύτερα στην κοινωνία, αφετέρου στην πορεία, αποκτώντας δημοφιλία, παρατηρούμε και την εισαγωγή μεγάλων "παικτών", επενδυτών με μεγάλα κεφάλαια που έχουν τη δυνατότητα να καθορίζουν με τις κινήσεις τους την αξία και τη χρησιμότητα του Bitcoin αλλά και των άλλων δημοφιλών κρυπτονομισμάτων. Η τεχνολογική εξέλιξη ακόμα και της μορφής του χρήματος, δεν μπορεί να αναιρέσει ή να μεταβάλλει στη βάση τους τις σχέσεις ιδιοκτησίας ως προς τα μέσα παραγωγής, που είναι και αυτές που καθορίζουν τελικά την αξία και τη μορφή του χρήματος.

Ένα ζήτημα που θα απασχολήσει, λοιπόν, τα επόμενα χρόνια κυβερνήσεις και κεντρικές τράπεζες, είναι η **ψηφιοποίηση της οικονομίας**, στη βάση όμως της ψηφιοποίησης φυσικού χρήματος που βρίσκεται σε κυκλοφορία, δημιουργία δηλαδή ψηφιακών νομισμάτων κεντρικών τραπεζών με αντίκρυσμα στην πραγματική οικονομία, τουλάχιστον σε αρχικό στάδιο. Επτά μεγάλες κεντρικές τράπεζες, μεταξύ των οποίων η κεντρική τράπεζα των ΗΠΑ, η Τράπεζα της Αγγλίας, η Ευρωπαϊκή Κεντρική Τράπεζα, η Ελβετική κεντρική τράπεζα και η Τράπεζα της Ιαπωνίας, ήδη έχουν συνεργαστεί με την **Τράπεζα Διεθνών Διακανονισμών (BIS),** ώστε να καθοριστούν σε κοινή βάση τα χαρακτηριστικά των ψηφιακών νομισμάτων: "η ανθεκτικότητα, η διαθεσιμότητα σε χαμηλό ή μηδενικό κόστος, τα κατάλληλα πρότυπα και ένα ξεκάθαρο νομικό πλαίσιο καθώς και ένας κατάλληλος ρόλος για τον ιδιωτικό τομέα". Ο υποδιοικητής της Τράπεζας της Αγγλίας (BoE) και πρόεδρος της επιτροπής πληρωμών της BIS Τζον Κάνλιφ, υπογράμμισε ότι "η αύξηση των πληρωμών χωρίς μετρητά μετά τα μέτρα καραντίνας για την αντιμετώπιση της πανδημίας επιτάχυνε τον ρόλο της τεχνολογίας στην αλλαγή των μορφών του χρήματος". Η κεντρική τράπεζα της Κίνας έχει ήδη προχωρήσει σε ένα πιλοτικό πρόγραμμα και σκοπεύει να κυκλοφορήσει το ψηφιακό γουάν κατά τη διάρκεια των Ολυμπιακών Αγώνων. Παράλληλα, τα σχέδια της Facebook για δημιουργία ψηφιακού νομίσματος, στηριζόμενο από ένα σύνολο μεγάλων νομισμάτων και κρατικού χρέους, σε συνδυασμό με τον οξυνόμενο ανταγωνισμό μεταξύ των

κρατών, πιέζουν για ταχείες εξελίξεις σχετικά με τα ψηφιακά νομίσματα, αφού όπως δήλωσε και ο επικεφαλής καινοτομίας της BIS, Μπενουά Κερέ, "δεν υπάρχει κάποια διεθνής κούρσα ανταγωνισμού, αλλά υπάρχει ένα πλεονέκτημα για τις κεντρικές τράπεζες στο να φτάσουν γρήγορα τον ιδιωτικό τομέα και να προηγηθούν για να διαμορφώσουν το μέλλον". [46]

Ένα δεύτερο ζήτημα που προκύπτει, είναι η χρήση της τεχνολογίας Blockchain για την προστασία των συναλλαγών αλλά και για ευρεία γκάμα εφαρμογών, όπως περιγράφηκε στο πρώτο κεφάλαιο, που θα μας εισάγει σε μια τελείως διαφορετική καθημερινότητα, με πολύ μεγάλες δυνατότητες. Παράλληλα απασχολεί όλο και πιο έντονα το ζήτημα προστασίας των προσωπικών δεδομένων, στο οποίο η τεχνολογία Blockchain αναμένεται να παίξει καθοριστικό ρόλο.

Παρά τις δυσκολίες και το δισταγμό αρκετών, αυτό που έχει μεγαλύτερη σημασία να συνειδητοποιήσουμε είναι πως μια αλλαγή που ήδη βρίσκεται υπό εξέλιξη, δεν έχει να κάνει μόνο με τα κρυπτονομίσματα ως μέσο ανταλλαγής ή εργαλείο, αλλά συνολικά με τον τρόπο που θα πραγματοποιούνται οι συναλλαγές. Η τεχνολογία blockchain έχει ανοίξει το κουτί της Πανδώρας. Και όλα προμηνύουν πως το μέλλον των χρηματοοοικονομικών συναλλαγών, ιδιαίτερα με τις δυσκολίες που αντιμετωπίζουν σήμερα, έγκειται στην αξιοποίηση αυτών των τεχνολογιών .

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα ψηφιακά νομίσματα έρχονται στο προσκήνιο ταχύτερα από το αναμενόμενο. Με τα υπέρ και τα κατά τους, οι νομοθέτες, οι κυβερνήσεις και οι κεντρικές τράπεζες, εξετάζουν την είσοδο σε μια νέα εποχή, με προσεκτικά και ενδελεχή μέτρα. Η παγκόσμια τάση για ρύθμιση των κρυπτονομισμάτων αντανακλά την ανάγκη για ένα ισχυρό πλαίσιο που θα διασφαλίζει την ασφάλεια και τη διαφάνεια των συναλλαγών, χωρίς να εμποδίζει την ανάπτυξη και την καινοτομία. Καθώς οι νομοθετικές ρυθμίσεις εξελίσσονται, το 2024 αναμένεται να είναι μια καθοριστική χρονιά για τη μελλοντική διαμόρφωση των αγορών κρυπτονομισμάτων.

ΜΕΡΟΣ ΤΕΤΑΡΤΟ

ΕΦΑΡΜΟΓΗ

ΔΗΜΙΟΥΡΓΙΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΟΣ ΜΕ ΧΡΗΣΗ PYTHON

Στο μέρος αυτό, επιχειρείται η δημιουργία ενός κρυπτονομίσματος, με σκοπό τη βαθύτερη κατανόηση του τρόπου αξιοποίησης της τεχνολογίας αλλά και της πρακτικής λειτουργίας των κρυπτονομισμάτων. Για το σκοπό αυτό γίνεται χρήση της εφαρμογής PyCharm.

Η αρχή σε κάθε κρυπτονόμισμα γίνεται με το Genesis Block, το πρώτο μπλοκ της αλυσίδας. Στη δημιουργία του πρώτου μπλοκ, αποδίδεται το Hash του μπλοκ το οποίο μεταφέρεται στο επόμενο. Έτσι κάθε επόμενο μπλοκ θα φέρει το Hash του προηγούμενου.

Μελετώντας τον κώδικα άλλων κρυπτονομισμάτων, εφόσον ο κώδικας είναι ανοιχτός προς όλους τους χρήστες, μπορούμε να δούμε τί χρειάζεται για την κατασκευή ενός νέου κρυπτονομίσματος. Βλέπουμε, για παράδειγμα, στον παρακάτω σύνδεσμο, https://github.com/bitcoin/bitcoin, τον κώδικα που χρησιμοποιείται για το bitcoin, καθώς και τις βελτιώσεις που έχουν προστεθεί στην πορεία. Σε αυτή τη λογική κινούμενοι, ξεκινάμε στην εφαρμογή PyCharm, τη δημιουργία ενός διαφοροποιημένου κρυπτονομίσματος με χρήση της γλώσσας Python, αντί της C++ που χρησιμοποιήθηκε για το bitcoin. Για τη δημιουργία ενός απλού blockchain με python ακολουθούνται κάποια βασικά βήματα. Ορίζουμε το πρώτο μπλόκ και την αλυσίδα, χρησιμοποιούμε κάποιο αλγόριθμο επιβεβαίωσης της εγκυρότητας της αλυσίδας, ορίζουμε τον τρόπο κατά τον οποίο προστίθενται τα μπλοκ.

Ορίζουμε τη συνάρτηση __init __ (), η οποία θα εκτελεστεί όταν δημιουργηθεί ένα αντικείμενο της κλάσης Block. Παρέχω τις ακόλουθες παραμέτρους που χρησιμοποιούνται στη λειτουργία έναρξης:

self - αυτό αναφέρεται στην παρουσία της κλάσης Block, καθιστώντας δυνατή την πρόσβαση στις μεθόδους και τα χαρακτηριστικά που σχετίζονται με την κλάση.

index – αυτό παρακολουθεί τη θέση του μπλοκ εντός του blockchain.

proof_no – αυτός είναι ο αριθμός που δημιουργήθηκε κατά τη δημιουργία ενός νέου μπλοκ (που ονομάζεται εξόρυξη).

prev_hash - αυτό αναφέρεται στο κατακερματισμό του προηγούμενου μπλοκ εντός της αλυσίδας.

data – αυτό δίνει μια καταγραφή όλων των συναλλαγών που έχουν ολοκληρωθεί, όπως η ποσότητα αγορασμένος

timestamp – αυτό τοποθετεί μια χρονική σήμανση για τις συναλλαγές.

Ο SHA-256 εισάγεται στο έργο για τον κατακερματισμό των δεδομένων των μπλοκ. Αφού οι τιμές έχουν εισαχθεί στον αλγόριθμο κρυπτογραφικού κατακερματισμού, η συνάρτηση θα επιστρέψει μια συμβολοσειρά 256-bit που αντιπροσωπεύει τα περιεχόμενα του μπλοκ. Έτσι επιτυγχάνεται η ασφάλεια αφού κάθε μπλοκ έχει μοναδικό hash και αυτό θα βασίζεται στο hash του προηγούμενου μπλοκ. Ως εκ τούτου, εάν κάποιος προσπαθήσει να θέσει σε κίνδυνο οποιοδήποτε μπλοκ στην αλυσίδα, αμφισβητείται η εγκυρότητα των μπλοκ, οδηγώντας σε διακοπή ολόκληρου του blockchain.

Πρώτα θα πρέπει να δημιουργήσουμε το πρώτο μπλοκ. Εισάγουμε στο πρόγραμμα που χρησιμοποιούμε τα απαραίτητα εργαλεία από τις βιβλιοθήκες αν δεν υπάρχουν, όπως τον αλγόριθμο sha-256. Έπειτα ορίζουμε το πρώτο μπλόκ και την αλυσίδα:

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

#εισαγωγή του sha256
from hashlib import sha256

#για την εισαγωγή δεδομένων και τη μετατροπή τους με τον sha-256
def updatehash(*args):
    hashing_text = ""; h = sha256()

    #hashing όλων των δεδομένων
    for arg in args:
        hashing_text += str(arg)

    h.update(hashing_text.encode('utf-8'))
    return h.hexdigest()

#Ο κάθε κόμβος έχει ως σημείο αναφοράς το προηγούμενο μπλόκ μέσω του μοναδικού του
hash.
class Block():

    #ορισμοί των δεδομένων, του προηγούμενου hash, του nonce
    def __init__(self,number=0, previous_hash="0"*64, data=None, nonce=0):
        self.data = data
        self.number = number
        self.previous_hash = previous_hash
        self.nonce = nonce
```

```
    #επιστροφή κρυπτογραφημένου hash στα δεδομένα του μπλοκ.
    def hash(self):
        return updatehash(
            self.number,
            self.previous_hash,
            self.data,
            self.nonce
        )
```

```
    #επιστρέφει σειρά των δεδομένων του μπλοκ
    def __str__(self):
        return str("Block#: %s\nHash: %s\nPrevious: %s\nData: %s\nNonce: %s\n" %(
            self.number,
            self.hash(),
            self.previous_hash,
            self.data,
            self.nonce
            )
        )
```

```
#ορισμός της αλυσίδας μπλοκ
class Blockchain():
    #ορισμός του αριθμού των μηδενικών μπροστά σε κάθε hash
    difficulty = 4
```

Ορίζουμε τη συνάρτηση __init __ (), η οποία θα εκτελεστεί όταν δημιουργηθεί ένα αντικείμενο της κλάσης Block.

```
    #η συνάρτηση __init __ (), θα εκτελείται όταν δημιουργηθεί ένα αντικείμενο της
κλάσης Block
    def __init__(self):
        self.chain = []
```

Ορίζουμε τη διαδικασία προσθήκης και αφαίρεσης Block.

```
    #προσθήκη νέου μπλοκ στην αλυσίδα
    def add(self, block):
        self.chain.append(block)
```

```
    #αφαίρεση μπλοκ από την αλυσίδα
    def remove(self, block):
        self.chain.remove(block)
```

```
    #ορισμός εύρεσης του σωστού μπλοκ ώστε να προστεθεί στην αλυσίδα
    def mine(self, block):
        #ανάκτηση του προηγούμενου hash.
        #IndexError στην περίπτωση του πρώτου μπλοκ.
        try: block.previous_hash = self.chain[-1].hash()
        except IndexError: pass

        #πραγματοποίηση επαναλήψεων μέχρι να βρεθεί nonce που να ικανοποιεί τις
συνθήκες
        while True:
            if block.hash()[:self.difficulty] == "0" * self.difficulty:
                self.add(block); break
            else:
                #increase the nonce by one and try again
                block.nonce += 1
```

Πραγματοποίηση ελέγχου εγκυρότητας, χρησιμοποιώντας true/false συναρτήσεις υπό συνθήκες:

```
    #έλεγχος εγκυρότητας
    def isValid(self):

        for i in range(1,len(self.chain)):
            _previous = self.chain[i].previous_hash
            _current = self.chain[i-1].hash()
            #σύγκριση του previous hash με το hash του προηγούμενου μπλοκ
            if _previous != _current or _current[:self.difficulty] !=
"0"*self.difficulty:
                return False

        return True
```

Έλεγχος των αποτελεσμάτων

```
#τεστ λειτουργικότητας της αλυσίδας
def main():
    blockchain = Blockchain()
    database = ["trade", "coin", "crypto", "repeat", "christmas", "chain"]

    num = 0

    for data in database:
        num += 1
        blockchain.mine(Block(num, data=data))
```

```
    for block in blockchain.chain:
        print(block)

    print(blockchain.isValid())

    blockchain.chain[2].data = "NEW DATA"
    blockchain.mine(blockchain.chain[2])
    print(blockchain.isValid())


if __name__ == '__main__':
    main()
```

Όταν δοκιμάσουμε να "τρέξουμε" το πρόγραμμα στην εφαρμογή, πραγματοποιείται mining και στο terminal εμφανίζεται ως αποτέλεσμα το εξής:

Block#: 1
Hash: 0000f4b88c611ff153217341fdf1d35ce4d0a3a0c4b5a8a6e0c1e60d5bee67d3
Previous: 0000000000000000000000000000000000000000000000000000000000000000
Data: trade
Nonce: 37970

Block#: 2
Hash: 00001dea334b0557c8c3b5a3f723349a46704bb03d4e3b0b62a15b9e282f10fe
Previous: 0000f4b88c611ff153217341fdf1d35ce4d0a3a0c4b5a8a6e0c1e60d5bee67d3
Data: coin
Nonce: 66533

Block#: 3
Hash: 000042573e1be0ebec263fa768ca2d80c9a1e78d7f02cf9819b294020a3639c4
Previous: 00001dea334b0557c8c3b5a3f723349a46704bb03d4e3b0b62a15b9e282f10fe
Data: crypto
Nonce: 81304

Block#: 4
Hash: 0000d17abb587273177716e843311f8fdbaaba9ddbba17115d129741c5d3351c
Previous: 000042573e1be0ebec263fa768ca2d80c9a1e78d7f02cf9819b294020a3639c4
Data: repeat
Nonce: 42337

Block#: 5
Hash: 0000f228ab98d4cdb5bd4dd66ea33af94aa1cd3919c20e24a76155694cc01bbd
Previous: 0000d17abb587273177716e843311f8fdbaaba9ddbba17115d129741c5d3351c
Data: christmas
Nonce: 173660

Block#: 6
Hash: 0000c389481f61f60b72114b239fa69ef38bb70ffdf67f140dc524ed381b6f56
Previous: 0000f228ab98d4cdb5bd4dd66ea33af94aa1cd3919c20e24a76155694cc01bbd
Data: chain
Nonce: 102679

True
False

Process finished with exit code 0

Εδώ βλέπουμε με ποιο τρόπο προστίθενται νέα μπλοκ με mining.
Τα Nonce μας δείχνουν πόσα hashes χρειάστηκαν ώστε να βρεθεί το hash με την αντίστοιχη δυσκολία. Έτσι για παράδειγμα στο Block#: 6 χρειάστηκαν 102679 προσπάθειες ώστε να βρεθεί το Hash :0000c389481f61f60b72114b239fa69ef38bb70ffdf67f140dc524ed381b6f56

Τώρα θα δοκιμάσουμε να πραγματοποιήσουμε μια συναλλαγή.

ΒΗΜΑ 1 - ΔΗΜΙΟΥΡΓΙΑ ΑΠΛΟΥ Blockchain

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)
```

```
    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        self.pending_transactions.append({
            'sender': sender,
            'receiver': receiver,
            'amount': amount
        })

    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(), self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)

# Δημιουργία ενός blockchain
blockchain = Blockchain()
```

ΒΗΜΑ 2 - ΠΡΟΣΘΗΚΗ ΣΥΝΑΛΛΑΓΩΝ

```
# Προσθήκη μιας συναλλαγής
blockchain.add_transaction("Alice", "Bob", 50)
blockchain.add_transaction("Bob", "Charlie", 25)
```

ΒΗΜΑ 3 - ΕΠΑΛΗΘΕΥΣΗ ΚΑΙ ΠΡΟΣΘΗΚΗ ΤΟΥ ΜΠΛΟΚ ΣΤΗΝ ΑΛΥΣΙΔΑ

```
# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)
```

ΒΗΜΑ 4 - ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΝΕΑΣ ΑΛΥΣΙΔΑΣ

```
# Εκτύπωση της αλυσίδας
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")
```

ΟΛΟΚΛΗΡΟ ΤΟ ΠΡΟΓΡΑΜΜΑ

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)

    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        self.pending_transactions.append({
            'sender': sender,
            'receiver': receiver,
            'amount': amount
        })
    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(), self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)

# Δημιουργία ενός blockchain
blockchain = Blockchain()

# Προσθήκη μιας συναλλαγής
blockchain.add_transaction("Alice", "Bob", 50)
blockchain.add_transaction("Bob", "Charlie", 25)

# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")
```

Με αυτό το πρόγραμμα, μπορούμε να δημιουργήσουμε μια απλή αλυσίδα μπλοκ, να προσθέσουμε συναλλαγές, επαληθεύοντας τα μπλοκ και προσθέτοντάς τα στην αλυσίδα. Στη συνέχεια, μπορούμε να εξάγουμε την αλυσίδα με τις συναλλαγές. Το αποτέλεσμα που παίρνουμε όταν τρέχουμε το πρόγραμμα είναι το εξής:

```
Block 0 [8e3a66d6ffa2efbea9a46989d9475aad64aa3a7214534fcfde18047a38f8dcb5]:
Block 1 [5fec56d7ccfc24763f34da4dc9cf1b165ca4c6ec29462406baf03859f940c120]:
 Alice -> Bob: 50
 Bob -> Charlie: 25

Process finished with exit code 0
```

Μια νέα συναλλαγή :

Θα επεκτείνουμε τον κώδικα για να συμπεριλάβουμε μια νέα συναλλαγή. Θα εκτυπώσουμε τη νέα κατάσταση της αλυσίδας για να δούμε τη συναλλαγή. Ολόκληρο το πρόγραμμα μαζί με την προσθήκη μιας νέας συναλλαγής:

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)

    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        self.pending_transactions.append({
            'sender': sender,
            'receiver': receiver,
            'amount': amount
        })

    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof
```

```
  def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == “0000"


    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(), self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)

# Δημιουργία ενός blockchain
blockchain = Blockchain()

# Προσθήκη μιας αρχικής συναλλαγής
blockchain.add_transaction("Alice", "Bob", 50)
blockchain.add_transaction("Bob", "Charlie", 25)

# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας πριν την νέα συναλλαγή
print("Αλυσίδα πριν τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")

# Προσθήκη μιας νέας συναλλαγής
blockchain.add_transaction("Charlie", "Dave", 10)

# Εύρεση απόδειξης εργασίας (proof of work) για το νέο μπλοκ
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας μετά την νέα συναλλαγή
print("\nΑλυσίδα μετά τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")
```

Το αποτέλεσμα που παίρνουμε όταν τρέξουμε την αλυσίδα αυτή έχει ως εξής:

Αλυσίδα πριν τη νέα συναλλαγή:
Block 0 [8a49129081fc6a951312b4f25cbce5e5420bbd9565de1a0c6ed25d3b183a1c72]:
Block 1 [15f902d03a3fe8cd87ed3a4c584e86ff6568f6d0a328e3b7e14e4bb2336d34bf]:
Alice -> Bob: 50
Bob -> Charlie: 25

Αλυσίδα μετά τη νέα συναλλαγή:
Block 0 [8a49129081fc6a951312b4f25cbce5e5420bbd9565de1a0c6ed25d3b183a1c72]:
Block 1 [15f902d03a3fe8cd87ed3a4c584e86ff6568f6d0a328e3b7e14e4bb2336d34bf]:
Alice -> Bob: 50

```
Bob -> Charlie: 25
Block 2 [84efc8d986ef0708edcc9e946c1a31534051aa0734f495a4b67cb98ef4e63a1c]:
Charlie -> Dave: 10

Process finished with exit code 0
```

Μια νέα συναλλαγή :

Θα επεκτείνουμε τον κώδικα για να συμπεριλάβουμε ακόμα μια συναλλαγή. Θα εκτυπώσουμε τη νέα κατάσταση της αλυσίδας για να δούμε τη συναλλαγή. Ολόκληρο το πρόγραμμα μαζί με την προσθήκη μιας νέας συναλλαγής:

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)

    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        self.pending_transactions.append({
            'sender': sender,
            'receiver': receiver,
            'amount': amount
        })

    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(), self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)
```

```
# Δημιουργία ενός blockchain
blockchain = Blockchain()

# Προσθήκη μιας αρχικής συναλλαγής
blockchain.add_transaction("Alice", "Bob", 50)
blockchain.add_transaction("Bob", "Charlie", 25)

# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας πριν την νέα συναλλαγή
print("Αλυσίδα πριν τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")

# Προσθήκη μιας νέας συναλλαγής
blockchain.add_transaction("Charlie", "Dave", 10)

# Εύρεση απόδειξης εργασίας (proof of work) για το νέο μπλοκ
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας μετά την νέα συναλλαγή
print("\nΑλυσίδα μετά τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")

# Προσθήκη μιας νέας συναλλαγής
blockchain.add_transaction("Dave", “Margaret", 8)

# Εύρεση απόδειξης εργασίας (proof of work) για το νέο μπλοκ
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας μετά την νέα συναλλαγή
print("\nΑλυσίδα μετά τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}: {transaction['amount']}")
```

Το αποτέλεσμα που παίρνουμε είναι το εξής:

Αλυσίδα πριν τη νέα συναλλαγή:
Block 0 [b766cb5469b923e5d5b2bf54c5581d5714842af6c696892bdd6314f51483545a]:
Block 1 [04934879ad333ef84074c6d5751c40aecda40d39400023dc8cfc34f33d31382f]:
 Alice -> Bob: 50
 Bob -> Charlie: 25

Αλυσίδα μετά τη νέα συναλλαγή:
Block 0 [b766cb5469b923e5d5b2bf54c5581d5714842af6c696892bdd6314f51483545a]:
Block 1 [04934879ad333ef84074c6d5751c40aecda40d39400023dc8cfc34f33d31382f]:
Alice -> Bob: 50
Bob -> Charlie: 25

Block 2 [adc643367572ce9f2cc4cf7aebfa2ecd2985e1aef6c457c7a9665e133ee79c39]:
Charlie -> Dave: 10

Αλυσίδα μετά τη νέα συναλλαγή:
Block 0 [b766cb5469b923e5d5b2bf54c5581d5714842af6c696892bdd6314f51483545a]:
Block 1 [04934879ad333ef84074c6d5751c40aecda40d39400023dc8cfc34f33d31382f]:
Alice -> Bob: 50
Bob -> Charlie: 25
Block 2 [adc643367572ce9f2cc4cf7aebfa2ecd2985e1aef6c457c7a9665e133ee79c39]:
Charlie -> Dave: 10
Block 3 [1184b8b7f8cb9f5bdecf728856d7729f9592a32f20af9ddc69cc78746068617d]:
Dave -> Margaret: 8

Process finished with exit code 0

Με τον τρόπο αυτό, μπορούμε να πραγματοποιούμε συναλλαγές οι οποίες επαληθεύονται και προστίθενται στην αλυσίδα.

Δημιουργήσαμε ένα βασικό blockchain. Για μια πλήρη εφαρμογή κρυπτονομίσματος, χρειαζόμαστε επιπλέον λειτουργίες:

1. Διευθύνσεις και ψηφιακές υπογραφές. Χρήση δημόσιων και ιδιωτικών κλειδιών για τη δημιουργία διευθύνσεων και χρήση ψηφιακών υπογραφών για την υπογραφή των συναλλαγών.
2. Ασφάλεια και επαλήθευση των συναλλαγών. Επιβεβαίωση ότι οι συναλλαγές είναι έγκυρες (αληθείς, δεν υπάρχουν διπλές εγγραφές κ.ο.κ.) και επαλήθευση των υπογραφών των συναλλαγών.
3. Δίκτυο Peer to Peer (P2P), για το διαμοιρασμό της αλυσίδας και το συγχρονισμό με άλλους κόμβους.
4. Πρωτόκολλα, Proof of work/Proof of Stake.
5. Πορτοφόλι Χρηστών.

ΒΗΜΑ 1 - BLOCKCHAIN

Τώρα θα προσθέσουμε τη λειτουργικότητα για να δημιουργήσουμε ένα κρυπτονόμισμα με 50,000 μονάδες το οποίο θα έχει την ονομασία EKoin. Επίσης, θα προσθέσουμε μια απλή δομή δεδομένων για τους χρήστες και θα διασφαλίσουμε ότι οι συναλλαγές δεν μπορούν να ξεπεράσουν τα διαθέσιμα υπόλοιπα των χρηστών. Επεκτείνουμε την κλάση Blockchain με τη δυνατότητα διαχείρισης χρηστών και ελέγχου υπολοίπων:

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}
{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.balances = {'genesis': 50000}  # Δημιουργία της αρχικής ποσότητας EKoin
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)

    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        if self.is_valid_transaction(sender, amount):
            self.pending_transactions.append({
                'sender': sender,
                'receiver': receiver,
                'amount': amount
            })
            return True
        return False
```

```
    def is_valid_transaction(self, sender, amount):
        if sender not in self.balances:
            return False
        if self.balances[sender] < amount:
            return False
        return True

    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(),
self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)
        self.update_balances(new_block)

    def update_balances(self, block):
        for tx in block.transactions:
            sender = tx['sender']
            receiver = tx['receiver']
            amount = tx['amount']
            if sender in self.balances:
                self.balances[sender] -= amount
            else:
                self.balances[sender] = -amount

            if receiver in self.balances:
                self.balances[receiver] += amount
            else:
                self.balances[receiver] = amount

# Δημιουργία ενός blockchain
blockchain = Blockchain()

# Προσθήκη μιας αρχικής συναλλαγής
blockchain.add_transaction("genesis", "Alice", 5000)
```

```
# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας πριν τη νέα συναλλαγή
print("Αλυσίδα πριν τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}:
{transaction['amount']}")

# Προσθήκη μιας νέας συναλλαγής
blockchain.add_transaction("Alice", "Dave", 10)

# Εύρεση απόδειξης εργασίας (proof of work) για το νέο μπλοκ
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας μετά τη νέα συναλλαγή
print("\nΑλυσίδα μετά τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}:
{transaction['amount']}")

# Προσθήκη μιας νέας συναλλαγής
blockchain.add_transaction("Dave", "Margaret", 8)

# Εύρεση απόδειξης εργασίας (proof of work) για το νέο μπλοκ
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας μετά τη νέα συναλλαγή
print("\nΑλυσίδα μετά τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}:
{transaction['amount']}")
```

```
# Εκτύπωση των υπολοίπων των χρηστών
print("\nΥπόλοιπα χρηστών:")
for user, balance in blockchain.balances.items():
    print(f"  {user}: {balance} EKoin")
```

Επεξηγήσεις:

1. Δημιουργία Χρηστών και Υπολοίπων:
   - Στο `__init__` της κλάσης `Blockchain`, ορίσαμε το αρχικό υπόλοιπο για το χρήστη `'genesis'`.
   - Προσθέσαμε τη μέθοδο `update_balances` για να ενημερώνει τα υπόλοιπα των χρηστών όταν προστίθεται ένα νέο μπλοκ.
2. Ενημέρωση Συναλλαγών:
   - Στη μέθοδο `add_transaction`, ελέγχουμε αν ο αποστολέας έχει αρκετό υπόλοιπο.
   - Η μέθοδος `update_balances` ανανεώνει τα υπόλοιπα των χρηστών μετά την προσθήκη ενός μπλοκ.

Με αυτές τις αλλαγές, το blockchain θα μπορεί τώρα να διαχειρίζεται υπόλοιπα χρηστών και να ελέγχει τη διαθεσιμότητα πριν από την πραγματοποίηση συναλλαγών.

Τώρα αν τρέξουμε τον κώδικα στο τερματικό μας εμφανίζεται το εξής αποτέλεσμα:

Αλυσίδα πριν τη νέα συναλλαγή:

Block 0 [c795c9d664128a6b51e1bc44cc229ec289e05a5e0c48150caf18032dcecb6f26]:
Block 1 [bc7a5373a74d0bad9d2396bf2d4cd883191163e41893e4eb47749698d9f4800f]:
  genesis -> Alice: 5000

Αλυσίδα μετά τη νέα συναλλαγή:

Block 0 [c795c9d664128a6b51e1bc44cc229ec289e05a5e0c48150caf18032dcecb6f26]:
Block 1 [bc7a5373a74d0bad9d2396bf2d4cd883191163e41893e4eb47749698d9f4800f]:
  genesis -> Alice: 5000
Block 2 [291f65ff59c365f32a60a920b7bbd751dedccc570a7c81c68e374bfd465011fe]:
  Alice -> Dave: 10

Αλυσίδα μετά τη νέα συναλλαγή:

Block 0 [c795c9d664128a6b51e1bc44cc229ec289e05a5e0c48150caf18032dcecb6f26]:
Block 1 [bc7a5373a74d0bad9d2396bf2d4cd883191163e41893e4eb47749698d9f4800f]:
  genesis -> Alice: 5000
Block 2 [291f65ff59c365f32a60a920b7bbd751dedccc570a7c81c68e374bfd465011fe]:
  Alice -> Dave: 10

Block 3 [b6ec5a3d2d88b64aecf893af722290b67c16ea0dc331fff79ba275e75b1fde15]:
Dave -> Margaret: 8

Υπόλοιπα χρηστών:
genesis: 45000 EKoin
Alice: 4990 EKoin
Dave: 2 EKoin
Margaret: 8 EKoin

Process finished with exit code 0

Εδώ βλέπουμε πώς καταγράφονται οι συναλλαγές στον κώδικα. Για να δημιουργήσουμε μια εφαρμογή στην οποία να μπορεί ένας χρήστης να πραγματοποιήσει εγγραφή και συναλλαγή θα χρησιμοποιήσουμε το Flask.

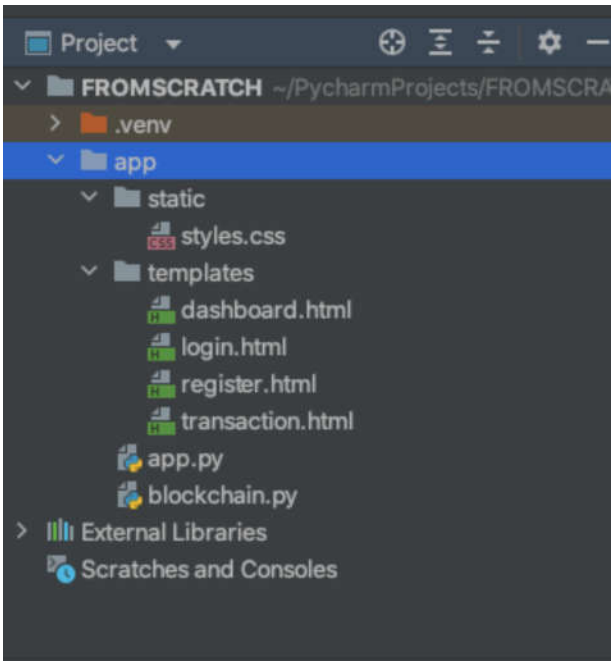
ΒΗΜΑ 2 - ΧΡΗΣΗ FLASK

Για να επεκτείνουμε τον υπάρχοντα κώδικα κρυπτονομίσματος και να δημιουργήσουμε μια εφαρμογή Flask που ικανοποιεί τις παραπάνω απαιτήσεις, θα ακολουθήσουμε τα εξής βήματα:

1. Δημιουργία του Backend με Flask:
   - Εγγραφή χρήστη.
   - Σύνδεση και αποσύνδεση.
   - Πραγματοποίηση συναλλαγής.
   - Εμφάνιση λίστας συναλλαγών και υπόλοιπου.

2. Δημιουργία του Frontend με HTML και CSS:
   - Σελίδα εισόδου και εγγραφής.
   - Σελίδα συναλλαγών.
   - Εμφάνιση της λίστας συναλλαγών και του υπολοίπου.

Ξεκινάμε με βάση το blockchain που αναπτύξαμε και στήνουμε τη δομή του προγράμματος.
Χρησιμοποιούμε το PyCharm Community Edition. Δημιουργώ νέο Project με χρήση virtual environment. Φτιάχνω φάκελο τον οποίο ονομάζω app. Μέσα στο φάκελο δημιουργώ δύο αρχεία python, blockchain.py και app.py καθώς και δύο φακέλους, έναν φάκελο static ο οποίος εμπεριέχει αρχείο css και έναν φάκελο templates με όλα τα html αρχεία που θα χρειαστούν. Η δομή του προγράμματος έχει ως εξής:



ΕΙΚΟΝΑ 17 - Δομή εφαρμογής στο PyCharm

Ο ΚΩΔΙΚΑΣ ΓΙΑ ΤΑ ΑΡΧΕΙΑ

1. BLOCKCHAIN.PY

```
import hashlib
import time

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}
{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
```

```
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.balances = {'genesis': 50000}  # Δημιουργία της αρχικής ποσότητας EKoin
        self.usernames = {}  # Νέο λεξικό για τα ονόματα χρηστών
        self.create_genesis_block()

    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)

    def get_last_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        if self.is_valid_transaction(sender, amount):
            self.pending_transactions.append({
                'sender': sender,
                'receiver': receiver,
                'amount': amount
            })
            return True
        return False
    def is_valid_transaction(self, sender, amount):
        if sender not in self.balances:
            return False
        if self.balances[sender] < amount:
            return False
        return True

    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(),
self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)
        self.update_balances(new_block)

    def update_balances(self, block):
```

```
        for tx in block.transactions:
            sender = tx['sender']
            receiver = tx['receiver']
            amount = tx['amount']
            if sender in self.balances:
                self.balances[sender] -= amount
            else:
                self.balances[sender] = -amount

            if receiver in self.balances:
                self.balances[receiver] += amount
            else:
                self.balances[receiver] = amount

# Δημιουργία ενός blockchain
blockchain = Blockchain()

# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)
```



```
# Εκτύπωση της αλυσίδας πριν τη νέα συναλλαγή
print("Αλυσίδα πριν τη νέα συναλλαγή:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}:
{transaction['amount']}")


# Εκτύπωση των υπολοίπων των χρηστών
print("\nΥπόλοιπα χρηστών:")
for user_email, balance in blockchain.balances.items():
    user_name = blockchain.usernames.get(user_email, user_email)
    print(f"  {user_name}: {balance} EKoin")
```

2. APP.PY

```
from flask import Flask, request, jsonify, render_template, redirect, url_for,
session
from werkzeug.security import generate_password_hash, check_password_hash
from blockchain import Blockchain
import hashlib
import time

app = Flask(__name__)
app.secret_key = 'super_secret_key'

users = {}
blockchain = Blockchain()

@app.route('/')
def home():
    if 'user' in session:
        return redirect(url_for('dashboard'))
    return render_template('login.html')

@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        email = request.form.get('email')
        password = request.form.get('password')
        name = request.form.get('name')  # Χρησιμοποιούμε request.form.get() για να
αποφύγουμε το KeyError

        if not email or not password or not name:
            return 'All fields are required.'

        if email in users:
            return 'User already exists'

        users[email] = generate_password_hash(password)
        blockchain.usernames[email] = name

        # Αν αυτός είναι ο πρώτος χρήστης
        if len(users) == 1:
            # Μεταφορά όλου του υπολοίπου από τον genesis στον πρώτο χρήστη
            genesis_balance = blockchain.balances['genesis']
            blockchain.balances[email] = genesis_balance
            blockchain.balances['genesis'] = 0
        else:
            blockchain.balances[email] = 0
```



```
        return redirect(url_for('login'))
```

```
    return render_template('register.html')

@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        email = request.form['email']
        password = request.form['password']
        if email not in users or not check_password_hash(users[email], password):
            return 'Invalid credentials'
        session['user'] = email
        return redirect(url_for('dashboard'))
    return render_template('login.html')
@app.route('/logout')
def logout():
    session.pop('user', None)
    return redirect(url_for('login'))
@app.route('/dashboard')
def dashboard():
    if 'user' not in session:
        return redirect(url_for('login'))
    return render_template('dashboard.html', user=session['user'],
balance=blockchain.balances[session['user']], chain=blockchain.chain)
@app.route('/transaction', methods=['POST'])
def transaction():
    if 'user' not in session:
        return redirect(url_for('login'))
    sender = session['user']
    receiver = request.form['‘receiver']
    amount = int(request.form['amount'])

    if blockchain.add_transaction(sender, receiver, amount):
        last_proof = blockchain.get_last_block().proof
        proof = blockchain.proof_of_work(last_proof)
        blockchain.add_block(proof)
        return redirect(url_for('dashboard'))
    return 'Invalid transaction'

if __name__ == '__main__':
    app.run(debug=True, port= 5000)
```

3. LOGIN.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EKoin Login</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <h1>EKoin - Queen of Transactions</h1>
        <form action="/login" method="post">
            <input type="email" name="email" placeholder="Email" required>
            <input type="password" name="password" placeholder="Password" required>
            <button type="submit">Login</button>
        </form>
        <a href="/register">Register</a>
    </div>
</body>
</html>
```

4. REGISTER.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EKoin Register</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <h1>EKoin - Queen of Transactions</h1>
        <form action="/register" method="post">
            <input type="email" name="email" placeholder="Email" required>
            <input type="password" name="password" placeholder="Password" required>
            <label for="name">Name:</label>
        <input type="text" id="name" name="name" required>
        <br>
            <button type="submit">Register</button>
        </form>
        <a href="/login">Login</a>
    </div>
</body>
</html>
```

5. TRANSACTION.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EKoin Transaction</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <h1>EKoin - Queen of Transactions</h1>
        <h2>Make a Transaction</h2>
        <form method="post" action="{{ url_for('transaction') }}">
        <label for="receiver">Receiver:</label>
        <input type="email" name="receiver" required><br>
        <label for="amount">Amount:</label>
        <input type="number" name="amount" required><br>
        <button type="submit">Send</button>
        </form>
        <a href="{{ url_for('dashboard') }}">Back to Dashboard</a>
</form>
    </div>
</body>
</html>
```

6. DASHBOARD.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EKoin Dashboard</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <h1>EKoin - Queen of Transactions</h1>
        <h2>Welcome, {{ user }}!</h2>
        <p>Your balance: {{ balance }} EKoin</p>
        <form action="/transaction" method="post">
            <input type="text" name="receiver" placeholder="Receiver" required>
            <input type="number" name="amount" placeholder="Amount" required>
            <button type=“submit">Send</button>
```

```
        </form>
        <h3>Transaction History</h3>
        <ul>
            {% for block in chain %}
                <li>Block {{ block.index }} [{{ block.hash }}]
                    <ul>
                        {% for transaction in block.transactions %}
                            <li>{{ transaction.sender }} ->
{{ transaction.receiver }}: {{ transaction.amount }} EKoin</li>
                        {% endfor %}
                    </ul>
                </li>
            {% endfor %}
        </ul>
        <a href="/logout">Logout</a>
    </div>
</body>
</html>
```

7. STYLES.CSS

```
body {
    font-family: Arial, sans-serif;
    background-color: #f4f4f4;
    display: flex;
    justify-content: center;
    align-items: center;
    height: 100vh;
    margin: 0;
}
.container {
    background-color: white;
    padding: 20px;
    border-radius: 10px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
    width: 300px;
    text-align: center;
}
h1 {
    margin-bottom: 20px;
}
form {
    display: flex;
    flex-direction: column;
}
```

```
input {
    padding: 10px;
    margin: 10px 0;
    border: 1px solid #ddd;
    border-radius: 5px;
}

button {
    padding: 10px;
    border: none;
    background-color: #5cb85c;
    color: white;
    border-radius: 5px;
    cursor: pointer;
}

button:hover {
    background-color: #4cae4c;
}

a {
    display: block;
    margin-top: 20px;
    color: #007bff;
    text-decoration: none;
}

a:hover {
    text-decoration: underline;
}
ul {
    list-style-type: none;
    padding: 0;
}

ul li {
    margin: 5px 0;
}
```

ΑΠΟΤΕΛΕΣΜΑΤΑ ΚΩΔΙΚΑ

- Μόλις τρέξουμε το blockchain.py στο τερματικό εμφανίζεται το εξής αποτέλεσμα:

Αλυσίδα πριν τη νέα συναλλαγή:
Block 0 [752e48d84a8167ea2bc5bfa966e7987a81a169bf9e9957a7c4c56462a1669128]:
Block 1 [b00eee06e074dd9a52ba5a2ec2018970016fe1231dccb5fe9859652e01ee14d7]:

Υπόλοιπα χρηστών:
genesis: 50000 EKoin

Process finished with exit code 0

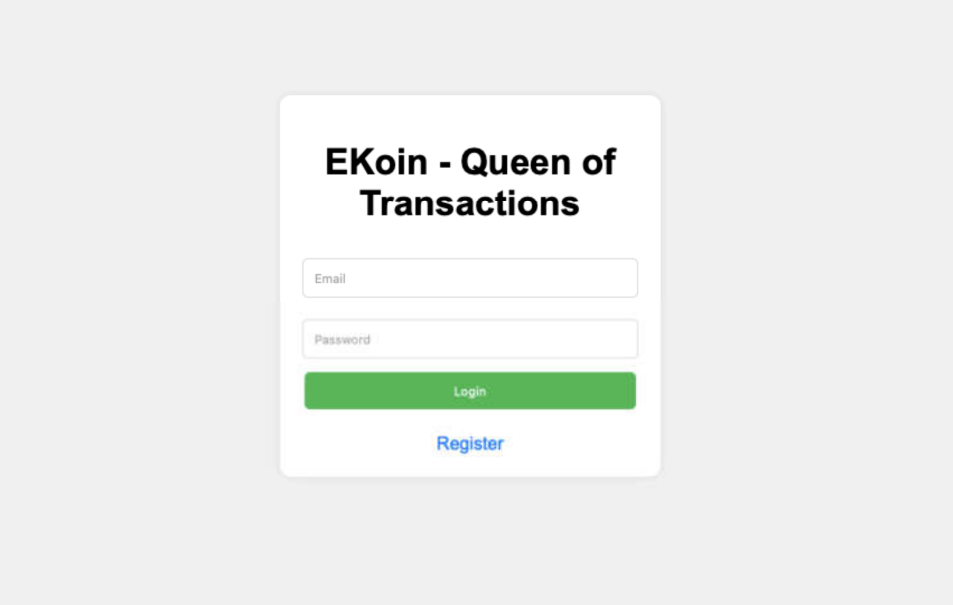
- Όταν τρέξουμε το app.py παίρνουμε το εξής:

Αλυσίδα πριν τη νέα συναλλαγή:
Block 0 [841e6a8e863eb0bcc29863ee314e24aeb3f03950b5fcac8d40c653f50b2eeda2]:
Block 1 [7a05e20a0e879a1c3a55388fd3f90cf4b1b2fd9cc4acfdd200c118537bd5a6e9]:

Υπόλοιπα χρηστών:
genesis: 50000 EKoin
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
** Serving Flask app 'app'*
** Debug mode: on*
** **Running on http://127.0.0.1:5000 (Press CTRL+C to quit)***
** Restarting with stat*
Αλυσίδα πριν τη νέα συναλλαγή:
Block 0 [8983a5e06d5f2c48d2bcc1377fab26b8bbe0bf67505f8bdc7c6da503825680d4]:
Block 1 [d155d2fc91c1d79aec28d63705112ec9d162ce067f0b73927ba421f85afadf39]:

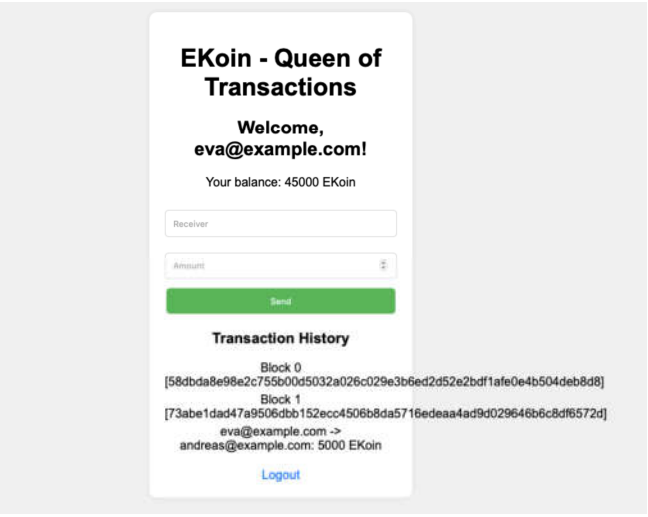
Υπόλοιπα χρηστών:
genesis: 50000 EKoin
** Debugger is active!*
** Debugger PIN: 794-555-883*

Όταν πατήσουμε τη σελίδα μας εμφανίζεται η παρρακάτω εικόνα:

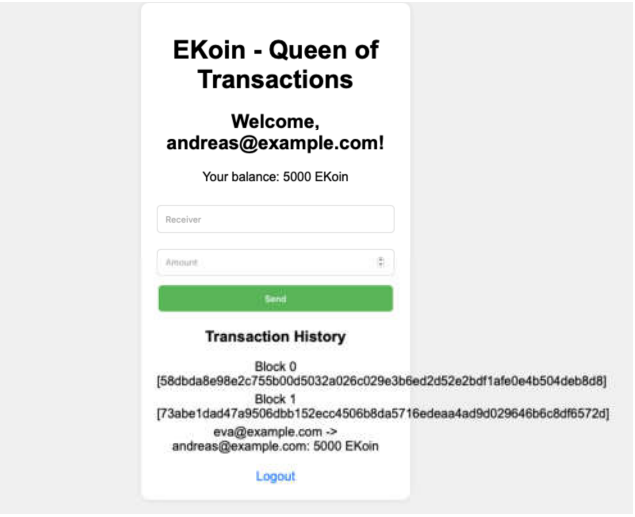


ΕΙΚΟΝΑ 18 - EKOIN APP1

Τώρα μπορούμε να δημιουργήσουμε ένα νέο χρήστη. Έχουμε σχεδιάσει τον κώδικα ώστε ο πρώτος χρήστης που θα πραγματοποιήσει εγγραφή να λάβει το σύνολο των νομισμάτων. Δημιουργώ τον χρήστη Eva : eva@example.com, password1, στον οποίο απονέμονται οι 50.000 μονάδες EKoin. Δημιουργώ κατόπιν ένα δεύτερο χρήστη, τον Andreas: andreas@example.com, password2. Έπειτα εισέρχομαι ως Eva και στέλνω 5.000 EKoin στον Andreas. Η σελίδα εμφανίζεται ως εξής:



ΕΙΚΟΝΑ 19 - EKOIN APP1



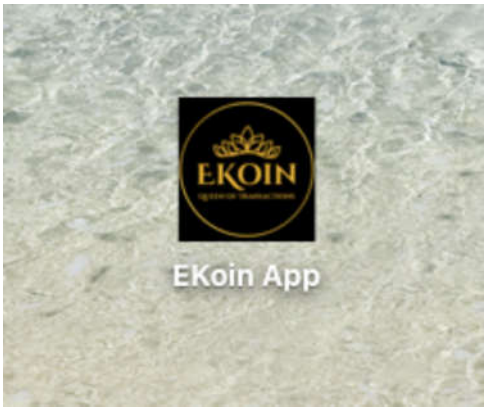
ΕΙΚΟΝΑ 20 - EKOIN APP1

Το υπόλοιπο του χρήστη Eva ενημερώθηκε με 45.000 EKoin, ενώ από κάτω εμφανίζεται και η αλυσίδα με το ιστορικό των συναλλαγών. Επίσης βλέπουμε πως ενημερώθηκε αντίστοιχα και το πορτοφόλι του χρήστη Andreas.

Μπορούμε για λόγους ευχρηστίας να δημιουργήσουμε ένα εικονίδιο στον υπολογιστή από το οποίο να ανοίγει η εφαρμογή που δημιουργήσαμε. Χρησιμοποιώντας την εφαρμογή Automator, δημιουργούμε μια εφαρμογή η οποία μέσω του shell script:

```
#!/bin/bash
open -a "Safari" http://localhost:5000
```

Με αυτό τον τρόπο, θα ανοίγει απευθείας στον περιηγητή την εφαρμογή. Το εικονίδιο στην επιφάνεια εργασίας εμφανίζεται ως εξής:



ΕΙΚΟΝΑ 21 - EKOIN APP1

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Δημιουργήσαμε μια απλή εφαρμογή ψηφιακού νομίσματος, με την ονομασία **"EKoin", το οποίο αποτελείται από 50.000 μονάδες**. Βάσει του κώδικα που δημιουργήσαμε, οι μονάδες αυτές αποδίδονται στον πρώτο χρήστη που πραγματοποιεί εγγραφή και έπειτα μπορούν να πραγματοποιηθούν συναλλαγές μεταξύ των χρηστών που εγγράφονται. Έπειτα από κάθε συναλλαγή εμφανίζεται στους χρήστες και η **αλυσίδα με το ιστορικό συναλλαγών**. Η εφαρμογή εμπεριέχει τα στοιχεία της ασφάλειας και επαλήθευσης συναλλαγών, **πρωτόκολλο Proof of work με τη χρήση του SHA-256, δημιουργία ψηφιακού πορτοφολιού για τους χρήστες.**

Ας προχωρήσουμε στην ενσωμάτωση ψηφιακών υπογραφών. Επίσης θα αλλάξουμε αισθητικά κάποια στοιχεία στο css ώστε να γίνει πιο λειτουργική και πιο εμφανίσιμη η εφαρμογή μας.

Ο ΚΩΔΙΚΑΣ ΜΕ ΔΗΜΟΣΙΟ & ΙΔΙΩΤΙΚΟ ΚΛΕΙΔΙ & ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

1. BLOCKCHAIN.PY

```
import hashlib
import time
import ecdsa

class Block:
    def __init__(self, index, previous_hash, timestamp, transactions, proof):
        self.index = index
        self.previous_hash = previous_hash
        self.timestamp = timestamp
        self.transactions = transactions
        self.proof = proof
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        block_string = f"{self.index}{self.previous_hash}{self.timestamp}
{self.transactions}{self.proof}"
        return hashlib.sha256(block_string.encode()).hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = []
        self.pending_transactions = []
        self.balances = {'genesis': 50000}  # Δημιουργία της αρχικής ποσότητας EKoin
        self.usernames = {}  # Νέο λεξικό για τα ονόματα χρηστών
        self.public_keys = {} #Νέο λεξικό για δημόσια κλειδιά
        self.create_genesis_block()
    def create_genesis_block(self):
        genesis_block = Block(0, "0", time.time(), [], 100)
        self.chain.append(genesis_block)
    def get_last_block(self):
        return self.chain[-1]
    def add_transaction(self, sender, receiver, amount, signature):
        if self.is_valid_transaction(sender, receiver, amount, signature):
            self.pending_transactions.append({
                'sender': sender,
                'receiver': receiver,
                'amount': amount,
                'signature': signature
            })
            return True
        return False
```

```
    def is_valid_transaction(self, sender, receiver, amount, signature):
        if sender not in self.balances or self.balances[sender] < amount:
            return False
        if sender not in self.public_keys:
            return False
        public_key = self.public_keys[sender]
        message = f"{sender}{receiver}{amount}".encode()
        try:
            public_key.verify(signature, message)
            return True
        except ecdsa.BadSignatureError:
            return False


    def proof_of_work(self, last_proof):
        proof = 0
        while not self.valid_proof(last_proof, proof):
            proof += 1
        return proof

    def valid_proof(self, last_proof, proof):
        guess = f"{last_proof}{proof}".encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"

    def add_block(self, proof):
        last_block = self.get_last_block()
        new_block = Block(len(self.chain), last_block.hash, time.time(),
self.pending_transactions, proof)
        self.pending_transactions = []
        self.chain.append(new_block)
        self.update_balances(new_block)

    def update_balances(self, block):
        for tx in block.transactions:
            sender = tx['sender']
            receiver = tx['receiver']
            amount = tx['amount']
            if sender in self.balances:
                self.balances[sender] -= amount
            else:
                self.balances[sender] = -amount

            if receiver in self.balances:
                self.balances[receiver] += amount
            else:
                self.balances[receiver] = amount

# Δημιουργία ενός blockchain
blockchain = Blockchain()
```

```
# Εύρεση απόδειξης εργασίας (proof of work)
last_proof = blockchain.get_last_block().proof
proof = blockchain.proof_of_work(last_proof)

# Προσθήκη του νέου μπλοκ στην αλυσίδα
blockchain.add_block(proof)

# Εκτύπωση της αλυσίδας πριν τη νέα συναλλαγή
print("Blockchain:")
for block in blockchain.chain:
    print(f"Block {block.index} [{block.hash}]:")
    for transaction in block.transactions:
        print(f"  {transaction['sender']} -> {transaction['receiver']}:
{transaction['amount']}(signature: {transaction['signature']})")


# Εκτύπωση των υπολοίπων των χρηστών
print("\nΥπόλοιπα χρηστών:")
for user_email, balance in blockchain.balances.items():
    user_name = blockchain.usernames.get(user_email, user_email)
    print(f"  {user_name}: {balance} EKoin")
```

2. APP.PY

```
from flask import Flask, request, jsonify, render_template, redirect, url_for,
session
from werkzeug.security import generate_password_hash, check_password_hash
from blockchain import Blockchain
import hashlib
import time
import ecdsa
import binascii

app = Flask(__name__)
app.secret_key = 'super_secret_key'
users = {}
blockchain = Blockchain()

def generate_keys():
    private_key = ecdsa.SigningKey.generate(curve=ecdsa.SECP256k1)
    public_key = private_key.get_verifying_key()
    return private_key, public_key
def sign_transaction(private_key, sender, receiver, amount):
    message = f"{sender}{receiver}{amount}".encode()
    signature = private_key.sign(message)
    return signature
```

```
@app.route('/')
def home():
    if 'user' in session:
        return redirect(url_for('dashboard'))
    return render_template('login.html')
@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        email = request.form.get('email')
        password = request.form.get('password')
        name = request.form.get('name')
        if not email or not password or not name:
            return 'Όλα τα πεδία είναι υποχρεωτικά.', 400
        if email in users:
            return 'Ο χρήστης υπάρχει ήδη.', 400
        private_key, public_key = generate_keys()
        users[email] = {
            'password': generate_password_hash(password),
            'private_key': binascii.hexlify(private_key.to_string()).decode(),
            'public_key': binascii.hexlify(public_key.to_string()).decode()
        }
        blockchain.usernames[email] = name
        blockchain.public_keys[email] = public_key
        if len(users) == 1:
            genesis_balance = blockchain.balances['genesis']
            blockchain.balances[email] = genesis_balance
            blockchain.balances['genesis'] = 0
        else:
            blockchain.balances[email] = 0
        return jsonify({
            'message': 'Η εγγραφή ήταν επιτυχής.',
            'public_key': users[email]['public_key'],
            'private_key': users[email]['private_key']
        }), 201
    return render_template('register.html')

@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        email = request.form['email']
        password = request.form['password']
        if email not in users or not check_password_hash(users[email]['password'],
password):
            return 'Μη έγκυρα στοιχεία εισόδου.', 400
        session['user'] = email
        session['name'] = blockchain.usernames.get(email, email)  # Αποθήκευση του
ονόματος
        return redirect(url_for('dashboard'))
    return render_template('login.html')
```

```
@app.route('/logout')
def logout():
    session.pop('user', None)
    return redirect(url_for('login'))

@app.route('/dashboard')
def dashboard():
    if 'user' not in session:
        return redirect(url_for('login'))
    return render_template('dashboard.html', user=session['user'],
balance=blockchain.balances[session['user']], chain=blockchain.chain)

@app.route('/transaction', methods=['POST'])
def transaction():
    if 'user' not in session:
        return redirect(url_for('login'))

    sender = session['user']
    receiver = request.form['receiver']
    amount = int(request.form['amount'])

    private_key_string = users[sender]['private_key']
    private_key =
ecdsa.SigningKey.from_string(binascii.unhexlify(private_key_string),
curve=ecdsa.SECP256k1)
    signature = sign_transaction(private_key, sender, receiver, amount)

    if blockchain.add_transaction(sender, receiver, amount, signature):
        last_proof = blockchain.get_last_block().proof
        proof = blockchain.proof_of_work(last_proof)
        blockchain.add_block(proof)
        return redirect(url_for('dashboard'))

    return 'Μη έγκυρη συναλλαγή.', 400

if __name__ == '__main__':
    app.run(debug=True, port=8001)
```

3. LOGIN.HTML

```
<!doctype html>
<html lang="el">
<head>
    <meta charset="UTF-8">
    <title>EKoin - Queen of Transactions</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}”>
```

```
</head>
<body>
    <div class="container">
        <img src="{{ url_for('static', filename='EKoin.png') }}" alt="EKoin Logo"
class="logo"> <!-- Λογότυπο -->
        <h1>EKoin - Καλωσόρισες</h1>
        <h2>Σύνδεση</h2>
        <form method="post">
            Email: <input type="email" name="email" required><br>
            Κωδικός: <input type="password" name="password" required><br>
            <button type="submit">Σύνδεση</button>
        </form>
        <a href="{{ url_for('register') }}">Δεν έχετε λογαριασμό; Εγγραφή</a>
    </div>
    <footer>EKoin - Queen of Transactions @ 2024</footer> <!-- Footer -->
</body>
</html>
```

4. REGISTER.HTML

```
<!doctype html>
<html lang="el">
<head>
    <meta charset="UTF-8">
    <title>Εγγραφή</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <img src="{{ url_for('static', filename='EKoin.png') }}" alt="EKoin Logo"
class="logo"> <!-- Λογότυπο -->
        <h1>EKoin - Εγγραφή</h1>
        <form method="post">
            Email: <input type="email" name="email" required><br>
            Κωδικός: <input type="password" name="password" required><br>
            Όνομα: <input type="text" name="name" required><br>
            <button type="submit">Εγγραφή</button>
        </form>
        <a href="{{ url_for('login') }}">Έχετε ήδη λογαριασμό; Συνδεθείτε</a>
    </div>
    <footer>EKoin - Queen of Transactions</footer> <!-- Footer -->
</body>
</html>
```

5. TRANSACTION.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EKoin Transaction</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <img src="{{ url_for('static', filename='EKoin.png') }}" alt="EKoin Logo"
class="logo"> <!-- Λογότυπο -->
        <h1>EKoin - Queen of Transactions</h1>
        <h2>Make a Transaction</h2>
        <form method="post" action="/transaction">
            <label for="receiver">Receiver:</label>
            <input type="email" name="receiver" required><br>
            <label for="amount">Amount:</label>
            <input type="number" name="amount" required><br>
            <button type="submit">Send</button>
        </form>
        <a href="/dashboard">Back to Dashboard</a>
    </div>
    <footer>EKoin - Queen of Transactions</footer> <!-- Footer -->
</body>
</html>
```

6. DASHBOARD.HTML

```
<!doctype html>
<html lang="el">
<head>
    <meta charset="UTF-8">
    <title>Πίνακας Ελέγχου</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='styles.css') }}">
</head>
<body>
    <div class="container">
        <img src="{{ url_for('static', filename='EKoin.png') }}" alt="EKoin Logo"
class="logo"> <!-- Λογότυπο -->
        <h1>Καλώς ήρθες, {{ session['name'] }}</h1>
        <p>Υπόλοιπο: {{ balance }} EKoin</p>
        <h3>Πραγματοποίηση Συναλλαγής</h3>
        <form method="post" action="{{ url_for('transaction') }}">
```

```
            Παραλήπτης: <input type="text" name="receiver" required><br>
            Ποσό: <input type="number" name="amount" required><br>
            <button type="submit">Αποστολή</button>
        </form>
        <h3>Blockchain</h3>
        <ul>
            {% for block in chain %}
                <li>Μπλοκ {{ block.index }} [{{ block.hash }}]
                    <ul>
                        {% for transaction in block.transactions %}
                            <li>{{ transaction.sender }} ->
{{ transaction.receiver }}: {{ transaction.amount }} (υπογραφή:
{{ transaction.signature }})</li>
                        {% endfor %}
                    </ul>
                </li>
            {% endfor %}
        </ul>
        <a href="{{ url_for('logout') }}">Αποσύνδεση</a>
    </div>
    <footer>EKoin - Queen of Transactions</footer> <!-- Footer -->
</body>
</html>
```

7. STYLES.CSS

```
/* Γενικές Ρυθμίσεις */
body {
    font-family: Arial, sans-serif;
    background-color: #f4f4f4;
    display: flex;
    flex-direction: column;
    align-items: center;
    margin: 0;
    padding: 0;
    min-height: 100vh;
}

/* Στυλ για το Κουτί */
.container {
    background-color: #ffffff; /* Άσπρο χρώμα για το κουτί */
    padding: 20px;
    border-radius: 10px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
    width: 90%;
    max-width: 600px; /* Εξασφαλίζει ότι το κουτί δεν είναι πολύ μεγάλο */
    text-align: center;
```

```
    margin: 20px;
    box-sizing: border-box;
    overflow: hidden; /* Εξασφαλίζει ότι το περιεχόμενο δεν βγαίνει έξω από το κουτί */
}

/* Στυλ για τα κουμπιά */
button {
    padding: 10px;
    border: none;
    background-color: #b3e0ff; /* Ανοιχτό γαλάζιο χρώμα */
    color: white;
    border-radius: 5px;
    cursor: pointer;
    font-size: 16px;
}

button:hover {
    background-color: #99c2ff; /* Ελαφρώς σκούρο γαλάζιο για το hover */
}

/* Στυλ για τα πεδία εισόδου */
input {
    padding: 10px;
    margin: 10px 0;
    border: 1px solid #ddd;
    border-radius: 5px;
    box-sizing: border-box;
    width: calc(100% - 24px); /* Εξασφαλίζει ότι τα πεδία ταιριάζουν με το κουτί */
}

/* Στυλ για τον τίτλο */
h1 {
    margin-bottom: 20px;
    color: #0099ff; /* Ανοιχτό γαλάζιο χρώμα */
    font-size: 24px; /* Μεγαλύτερη γραμματοσειρά για τον τίτλο */
}

/* Στυλ για τον τίτλο footer */
footer {
    text-align: center;
    color: #0099ff; /* Ανοιχτό γαλάζιο χρώμα */
    font-size: 1.2em;
    margin-top: 20px;
}

/* Στυλ για το λογότυπο */
.logo {
    display: block;
    margin: 0 auto;
```

```
    max-width: 150px; /* Ρύθμισε το μέγεθος σύμφωνα με την προτίμησή σου */
    height: auto;
    padding: 10px 0;
}

/* Στυλ για τα hyperlinks */
a {
    display: block;
    margin-top: 20px;
    color: #0099ff; /* Ανοιχτό γαλάζιο χρώμα */
    text-decoration: none;
}

a:hover {
    text-decoration: underline;
}

/* Στυλ για λίστες */
ul {
    list-style-type: none;
    padding: 0;
}

ul li {
    margin: 5px 0;
}

/* Στυλ για μεγάλα κείμενα */
p, ul li {
    text-align: left; /* Εξασφαλίζει ότι το κείμενο δεν είναι ευθυγραμμισμένο στο κέντρο */
    overflow-wrap: break-word; /* Κάνει το κείμενο να σπάει σε νέες γραμμές αν είναι πολύ μεγάλο */
    word-wrap: break-word;
}
```

ΑΠΟΤΕΛΕΣΜΑΤΑ ΚΩΔΙΚΑ

Με την εκτέλεση της εφαρμογής εμφανίζεται στο τερματικό μας το εξής:

Blockchain:

Block 0 [8c0213b91db0b16629b6b4ebb8dbfb1cb041152720535b530bfb0d72aabb5f50]:

Block 1 [0437a73910818fecba99e0d40f097367785135d2364a85ddad71aa0b4b0ac401]:

Υπόλοιπα χρηστών:

genesis: 50000 EKoin

** Serving Flask app 'app'*

** Debug mode: on*

WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.

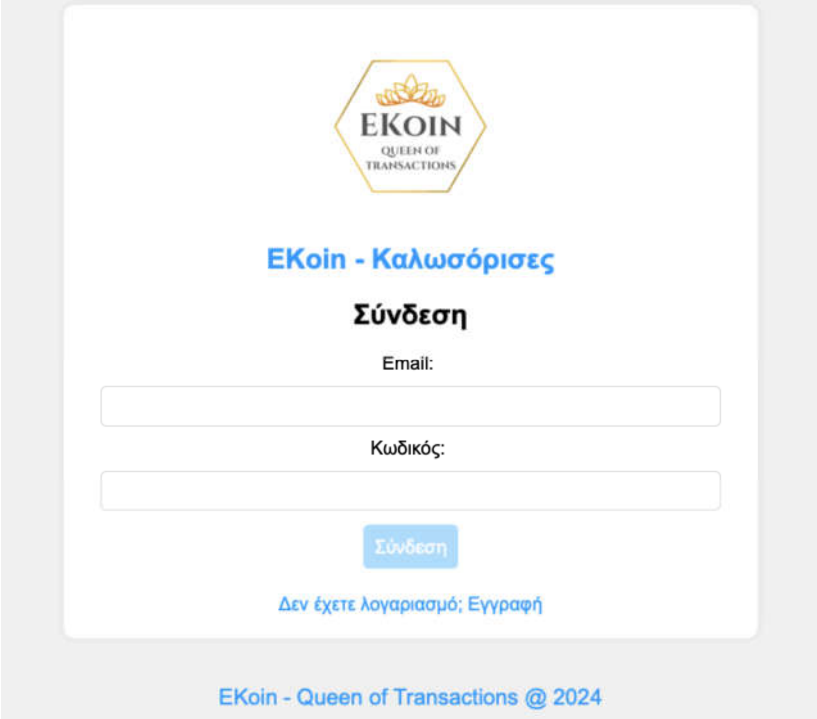
**** Running on http://127.0.0.1:8001***

Press CTRL+C to quit

** Debugger is active!*

** Debugger PIN: 119-166-999*

Πατώντας τη σύνδεση μας εμφανίζεται η εικόνα:



ΕΙΚΟΝΑ 22 - EKOIN APP2

Πραγματοποιώ εγγραφή. Μόλις πιέσουμε το κουμπί της εγγραφής, βλέπουμε στην οθόνη μας το παρακάτω μήνυμα:

ΕΙΚΟΝΑ 23 - ΕΚΟΙΝ APP2

Στο μήνυμα αυτό βλέπουμε τα κλειδιά που δημιουργούνται για τον χρήστη που πραγματοποίησε εγγραφή. Τα κλειδιά που δημιουργούνται εδώ, χρησιμοποιούνται για την ψηφιακή υπογραφή των συναλλαγών, η οποία είναι ουσιαστική για την επικύρωση της ταυτότητας του αποστολέα και για την αποτροπή διαστρέβλωσης των δεδομένων της συναλλαγής.

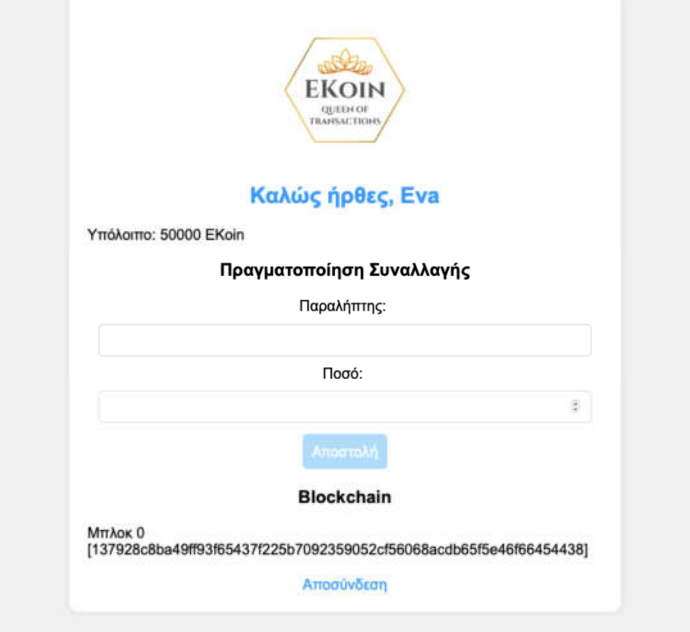
Χρήση κλειδιών:

1.Δημόσιο Κλειδί: Το κλειδί αυτό χρησιμοποιείται για την ταυτοποίηση του χρήστη στο σύστημα. Είναι γνωστό σε όλους και αποθηκεύεται στο blockchain ως μέρος της συναλλαγής.

2.Ιδιωτικό Κλειδί: Χρησιμοποιείται για την υπογραφή των συναλλαγών. Είναι γνωστό μόνο στον κάτοχο και πρέπει να φροντίζει να το κρατάει σε ασφαλές μέρος. Η υπογραφή δημιουργείται από το ιδιωτικό κλειδί και επιβεβαιώνεται από το δημόσιο.

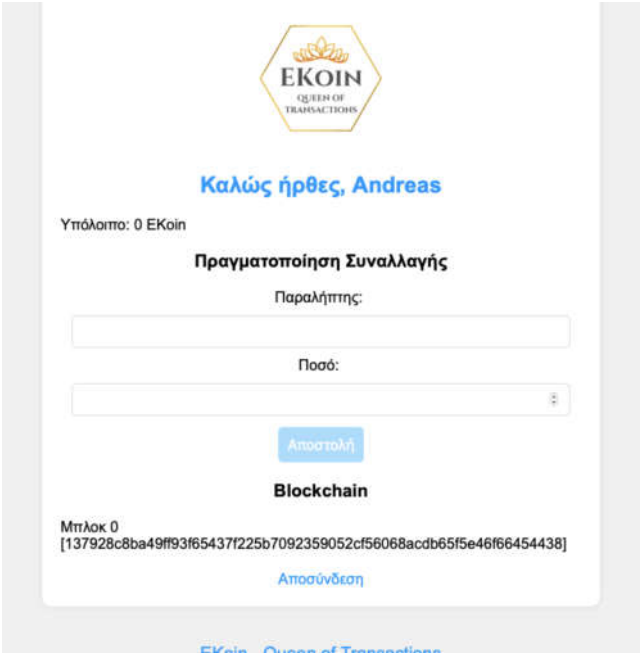
Υπογραφή Συναλλαγών: Όταν ένας χρήστης πραγματοποιεί μια συναλλαγή, χρησιμοποιεί το ιδιωτικό κλειδί για να υπογράψει τα δεδομένα της συναλλαγής, (αποστολέας, παραλήπτης, ποσό). Ύστερα η υπογραφή αυτή προστίθεται στη συναλλαγή και αποστέλλεται μαζί με τα υπόλοιπα δεδομένα στο δίκτυο. Οι κόμβοι του δικτύου μπορούν να επαληθεύσουν την υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να επιβεβαιώσουν ότι η συναλλαγή δεν έχει αλλοιωθεί και ότι ο αποστολέας είναι έγκυρος.

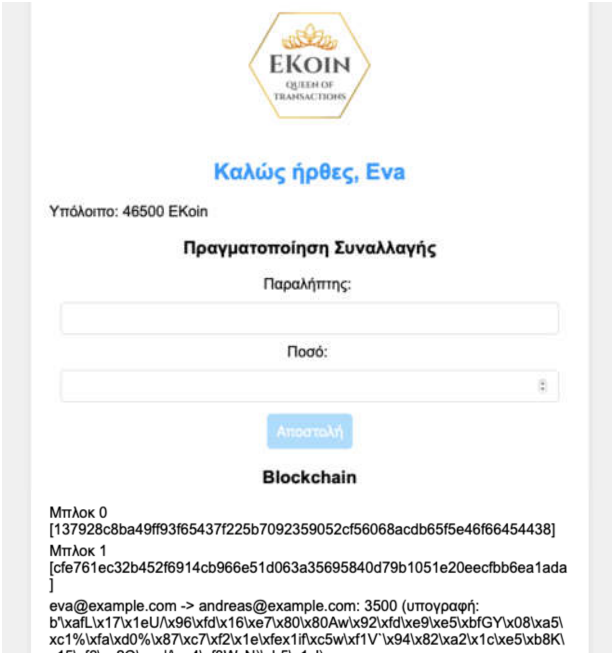
Επιστρέφοντας στην αρχική σελίδα, μπορούμε να πραγματοποιήσουμε είσοδο. Βλέπουμε πως απονέμονται στον πρώτο χρήστη και οι 50000 μονάδες EKoin.:



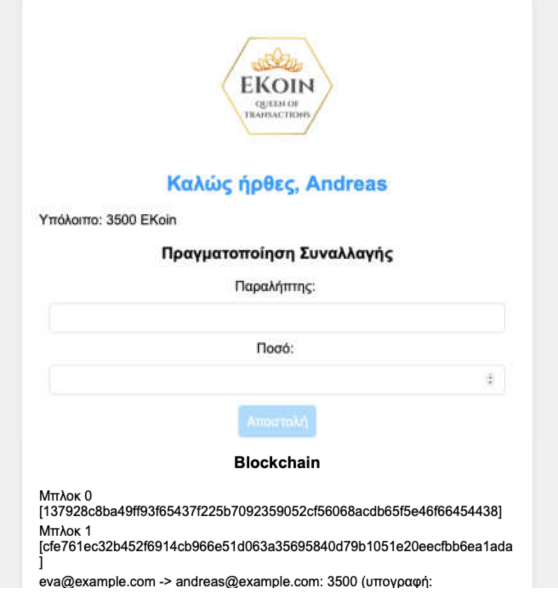
ΕΙΚΟΝΑ 24 - EKOIN APP2

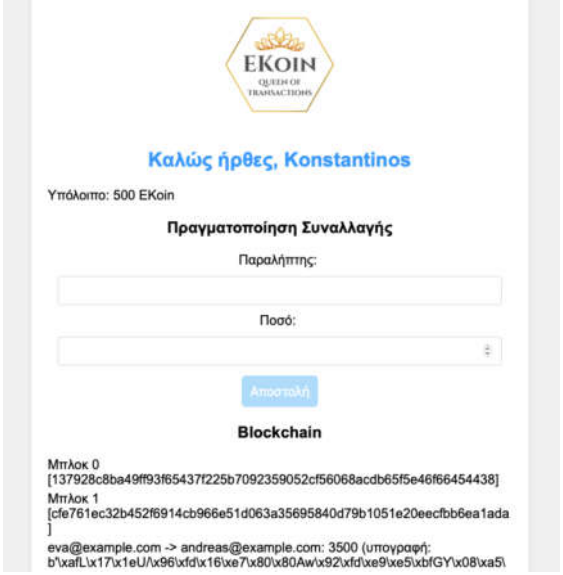
Έπειτα εγγράφω νέους χρήστες και πραγματοποιώ συναλλαγές:





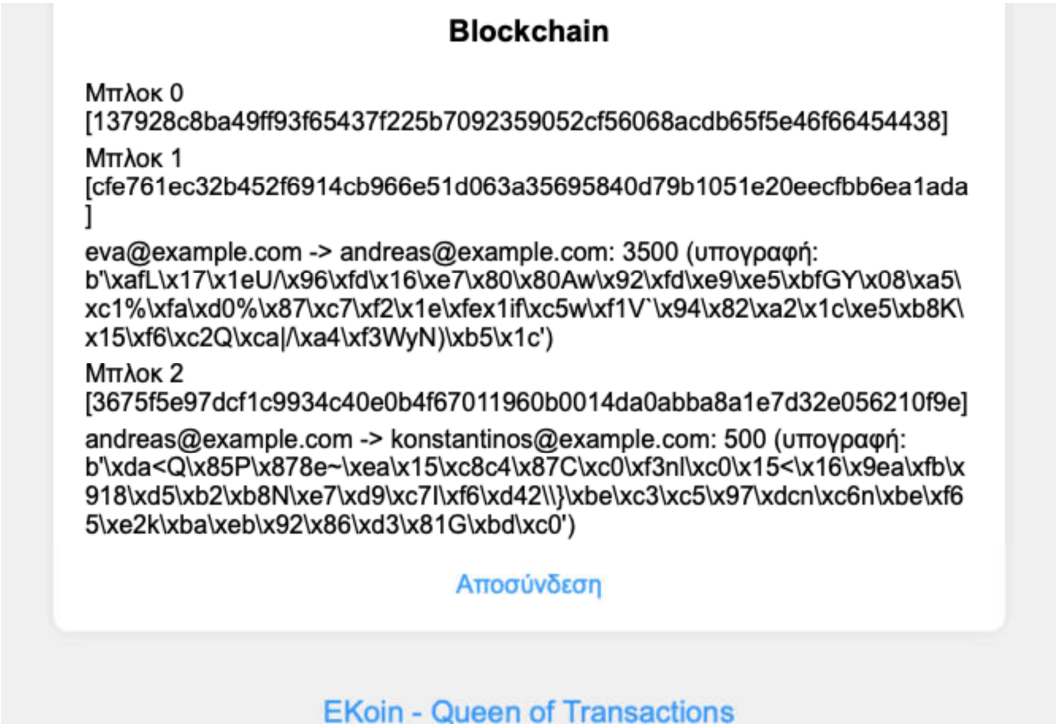
ΕΙΚΟΝΕΣ 25 & 26 -EKOIN APP2





ΕΙΚΟΝΕΣ 27 & 28- EKOIN APP2

Βλέπουμε πως ενημερώθηκαν τα υπόλοιπα των χρηστών, καταγράφηκαν οι συναλλαγές, φέρουν ψηφιακή υπογραφή και όλοι οι χρήστες μπορούν να δουν την αλυσίδα στο προφίλ τους.



ΕΙΚΟΝΑ 29 - EKOIN APP2

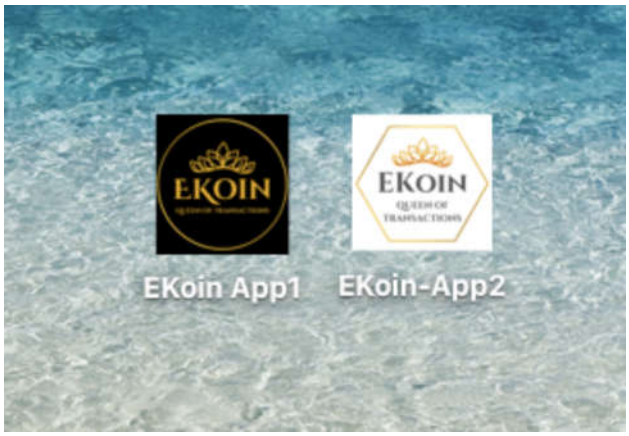
Χρησιμοποιώντας ξανά το Automator, δημιουργώ εικονίδιο στην επιφάνεια εργασίας μου με το script:

```
#!/bin/bash
open -a "Safari" http://localhost:8001
```

Έπειτα επιστρέφω στο PyCharm, δημιουργώ αρχείο start app.sh και εισάγω στο τερματικό την εντολή:

```
chmod +x start app.sh
./startapp.sh
```

ώστε να μπορεί η εφαρμογή να εκτελείται ανεξάρτητα. Στην επιφάνεια εργασίας βλέπουμε τώρα και τις δύο εφαρμογές ως εξής:



ΕΙΚΟΝΑ 30 - EKOIN APP2

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ

Επεκτείναμε τον κώδικα της προηγούμενης εφαρμογής ψηφιακού νομίσματος, και δημιουργήσαμε μια νέα, με την ονομασία "EKoin-App2", του οποίου τα χαρακτηριστικά παραμένουν ίδια, αποτελείται από 50.000 μονάδες, βάσει του κώδικα που δημιουργήσαμε, οι μονάδες αυτές αποδίδονται στον πρώτο χρήστη που πραγματοποιεί εγγραφή και έπειτα μπορούν να πραγματοποιηθούν συναλλαγές μεταξύ των χρηστών που εγγράφονται. Έπειτα από κάθε συναλλαγή εξακολουθεί να εμφανίζεται στους χρήστες και η αλυσίδα με το ιστορικό συναλλαγών, με το πρόσθετο στοιχείο των ψηφιακών υπογραφών με χρήση ιδιωτικών και δημόσιων κλειδιών. Η εφαρμογή εμπεριέχει τα στοιχεία της ασφάλειας και επαλήθευσης συναλλαγών, πρωτόκολλο Proof of work, χρήση του SHA-256, δημιουργία ψηφιακού πορτοφολιού για τους χρήστες, υπογραφή των συναλλαγών. Συνοπτικά:

Εφαρμογή: "EKoin-App2"

Σκοπός: Δημιουργία και διαχείριση κρυπτονομισμάτων με βάση την τεχνολογία της αλυσίδας μπλοκ (blockchain).

Πλατφόρμα: Web εφαρμογή χρησιμοποιώντας Python (Flask) και JavaScript.

Χαρακτηριστικά της Εφαρμογής:

1. Εγγραφή και Σύνδεση Χρηστών
   - **Εγγραφή:** Δημιουργία νέου λογαριασμού με email, κωδικό πρόσβασης και όνομα.
   - **Σύνδεση:** Είσοδος στην εφαρμογή με email και κωδικό πρόσβασης.
2. Διαχείριση Συναλλαγών
   - **Αποστολή Κρυπτονομισμάτων:** Δημιουργία και αποστολή συναλλαγών μεταξύ χρηστών.
   - **Επαλήθευση Συναλλαγών:** Χρήση ψηφιακών υπογραφών για επαλήθευση και ασφάλεια.
3. Blockchain
   - **Προβολή Blockchain:** Εμφάνιση όλων των μπλοκ και συναλλαγών που έχουν καταγραφεί στην αλυσίδα μπλοκ.
4. Διαχείριση Υπολοίπων
   - **Εμφάνιση Υπολοίπων:** Εμφάνιση του υπολοίπου του χρήστη και των αλλαγών που προκύπτουν από συναλλαγές.

Δομή της Εφαρμογής:

1. Frontend (HTML/CSS)
   - **Login.html:** Σελίδα σύνδεσης χρηστών.
   - **Register.html:** Σελίδα εγγραφής νέου χρήστη.
   - **Dashboard.html:** Κύρια σελίδα χρήστη με τη δυνατότητα αποστολής συναλλαγών και προβολής του blockchain.
   - **Transaction.html:** Σελίδα για την πραγματοποίηση συναλλαγών (παρόμοια με το Dashboard.html).
2. Backend (Python/Flask)
   - **app.py:** Περιέχει τη λογική της εφαρμογής, τη διαχείριση χρηστών, και την υλοποίηση της διαχείρισης συναλλαγών.
   - **blockchain.py:** Υλοποιεί τη λογική της αλυσίδας μπλοκ, συμπεριλαμβανομένων των μπλοκ, συναλλαγών και αλγορίθμων απόδειξης εργασίας.

Παράδειγμα Χρήσης:

1. Εγγραφή Χρήστη:
   - Ο χρήστης εγγράφεται παρέχοντας email, κωδικό πρόσβασης, και όνομα. Το σύστημα δημιουργεί ένα νέο λογαριασμό και παρέχει δημόσιο και ιδιωτικό κλειδί για τις συναλλαγές.
2. Σύνδεση Χρήστη:
   - Ο χρήστης συνδέεται με το email και τον κωδικό πρόσβασης. Μετά τη σύνδεση, κατευθύνεται στη σελίδα του dashboard.
3. Πραγματοποίηση Συναλλαγής:
   - Ο χρήστης μπορεί να στείλει κρυπτονόμισμα σε άλλον χρήστη. Η συναλλαγή επικυρώνεται με ψηφιακή υπογραφή και προστίθεται στην αλυσίδα μπλοκ.
4. Προβολή Blockchain:
   - Ο χρήστης μπορεί να δει την αλυσίδα μπλοκ με όλα τα μπλοκ και τις συναλλαγές που έχουν πραγματοποιηθεί.

Δομή Blockchain:

Μπλοκ 0

- **Hash:** 137928c8ba49ff93f65437f225b7092359052cf56068acdb65f5e46f66454438
    - **Περιγραφή:** Το πρώτο μπλοκ της αλυσίδας, γνωστό και ως "Genesis Block" ή αρχικό μπλοκ. Αυτό το μπλοκ είναι το θεμέλιο της αλυσίδας μπλοκ και συνήθως περιέχει αρχικά δεδομένα.

Μπλοκ 1

- **Hash:** cfe761ec32b452f6914cb966e51d063a35695840d79b1051e20eecfbb6ea1ada
    - **Περιγραφή:** Το δεύτερο μπλοκ στην αλυσίδα, που ακολουθεί το αρχικό μπλοκ. Περιέχει συναλλαγές που έχουν καταγραφεί μετά την δημιουργία του Genesis Block.

Συναλλαγές Στο Μπλοκ 1

- **Συναλλαγή:** eva@example.com -> andreas@example.com: 3500
    - **Υπογραφή:** b'\x af L\x17\x1eU/\x96\xfd\x16\xe7\x80\x80Aw\x92\xfd\xe9\xe5\xbfGY\x08\xa5\xc1%\xfa\xd0%\x87\xc7\xf2\x1e\xfex1if\xc5w\xf1V\x94\x82\xa2\x1c\xe5\xb8K\x15\xf6\xc2Q\xcal/\xa4\xf3WyN)\xb5\x1c`
    - **Περιγραφή:** Αυτή η συναλλαγή δείχνει μια μεταφορά 3500 EKoin από τον χρήστη `eva@example.com`στον χρήστη `andreas@example.com`. Η υπογραφή είναι ένα ψηφιακό αποτύπωμα που χρησιμοποιείται για την επαλήθευση της εγκυρότητας της συναλλαγής.

Μπλοκ 2

- **Hash:** 3675f5e97dcf1c9934c40e0b4f67011960b0014da0abba8a1e7d32e056210f9e
    - **Περιγραφή:** Το τρίτο μπλοκ στην αλυσίδα, που περιέχει νέες συναλλαγές προστιθέμενες στην αλυσίδα μετά το μπλοκ 1.

Συναλλαγές Στο Μπλοκ 2

- **Συναλλαγή:** andreas@example.com -> konstantinos@example.com: 500
    - **Υπογραφή:**b'\xda<Q\x85P\x878e~\xea\x15\xc8c4\x87C\xc0\xf3nl\xc0\x15<\x16\x9ea\xfb\x918\xd5\xb2\xb8N\xe7\xd9\xc7I\xf6\xd42\\}\xbe\xc3\xc5\x97\xdcn\xc6n\xbe\xf65\xe2k\xba\xeb\x92\x86\xd3\x81G\xbd\xc0'
    - **Περιγραφή:** Αυτή η συναλλαγή δείχνει μια μεταφορά 500 EKoin από τον χρήστη `andreas@example.com` στον χρήστη `konstantinos@example.com`. Η υπογραφή παρέχει την ασφάλεια ότι η συναλλαγή είναι έγκυρη και δεν έχει τροποποιηθεί.

Ανάλυση Στοιχείων

1. **Hash:** Κάθε μπλοκ έχει έναν μοναδικό κωδικό, το hash, που υπολογίζεται με βάση τα δεδομένα του μπλοκ (προηγούμενος hash, χρονική σήμανση, συναλλαγές κλπ.). Το hash διασφαλίζει ότι το μπλοκ δεν έχει τροποποιηθεί.

2. **Συναλλαγές:** Κάθε μπλοκ μπορεί να περιέχει πολλές συναλλαγές. Κάθε συναλλαγή περιγράφει την μεταφορά κρυπτονομισμάτων από έναν χρήστη σε άλλον. Περιλαμβάνει επίσης μια υπογραφή που χρησιμοποιείται για την επαλήθευση της εγκυρότητας της συναλλαγής.

3. **Υπογραφή:** Η υπογραφή είναι το ψηφιακό αποτύπωμα της συναλλαγής, δημιουργημένο με το ιδιωτικό κλειδί του αποστολέα. Είναι κρίσιμη για την επαλήθευση της αυθεντικότητας της συναλλαγής.

Σημασία της Δομής

Η δομή της αλυσίδας μπλοκ διασφαλίζει την ακεραιότητα και την ασφάλεια των δεδομένων. Κάθε νέο μπλοκ επηρεάζει το hash του προηγούμενου μπλοκ, δημιουργώντας μια αδιάσπαστη αλυσίδα από το Genesis Block μέχρι το πιο πρόσφατο μπλοκ. Οι συναλλαγές επαληθεύονται μέσω ψηφιακών υπογραφών, και τα μπλοκ που έχουν προσθεθεί στην αλυσίδα δεν μπορούν να τροποποιηθούν χωρίς να επηρεαστούν όλα τα επόμενα μπλοκ, κάτι που καθιστά την αλυσίδα εξαιρετικά ασφαλή.

Τέλος, η εφαρμογή που φτιάξαμε λειτουργεί με μια κεντρική αρχιτεκτονική και δεν ενσωματώνει ένα πραγματικό P2P δίκτυο. Η ενσωμάτωσή ενός P2P δικτύου θα μπορούσε να προσφέρει πλεονεκτήματα, όπως μεγαλύτερη αντοχή σε αποτυχίες και αποκέντρωση, αλλά απαιτεί πρόσθετη πολυπλοκότητα στην ανάπτυξη και διαχείριση. Για μια ολοκληρωμένη εφαρμογή κρυπτονομίσματος απαιτείται δίκτυο Peer-to-Peer (P2P):

Δίκτυο Peer-to-Peer (P2P)

Ένα δίκτυο Peer-to-Peer (P2P) είναι μια αρχιτεκτονική δικτύου όπου όλοι οι κόμβοι (ή "peers") λειτουργούν ως ίσοι συμμετέχοντες χωρίς την ανάγκη κεντρικού διακομιστή. Στο P2P δίκτυο, κάθε κόμβος έχει την ικανότητα να ενεργεί τόσο ως πελάτης όσο και ως εξυπηρετητής, επιτρέποντας άμεση επικοινωνία και ανταλλαγή δεδομένων μεταξύ των κόμβων.

Στην παρούσα φάση της ανάπτυξης της εφαρμογής, δεν ενσωματώθηκε ένα P2P δίκτυο κυρίως για τους εξής λόγους:

1. **Πολυπλοκότητα Υλοποίησης:** Η ενσωμάτωσή ενός P2P δικτύου απαιτεί την ανάπτυξη και συντήρηση μηχανισμών για τη συγχρονισμένη διαχείριση δεδομένων μεταξύ πολλών κόμβων, όπως επίσης και την επίλυση διαφορών (forks) και την επικύρωση συναλλαγών σε αποκεντρωμένο περιβάλλον.

2. **Απαιτήσεις Υποδομών:** Η λειτουργία ενός P2P δικτύου απαιτεί συγκεκριμένες υποδομές για επικοινωνία, συγχρονισμό και επικύρωση που δεν ήταν διαθέσιμες ή εύκολα διαχειρίσιμες στην παρούσα έκδοση της εφαρμογής.

3. **Σκοπός και Εύρος Εφαρμογής:** Η αρχική υλοποίηση της εφαρμογής επικεντρώθηκε σε κεντρική διαχείριση και έλεγχο, με σκοπό την απλούστερη ανάπτυξη και τη γρηγορότερη υλοποίηση των βασικών λειτουργιών.

Λειτουργία της Εφαρμογής με P2P Δίκτυο

Σε περίπτωση ενσωμάτωσης ενός P2P δικτύου στην εφαρμογή, η λειτουργία θα ήταν ως εξής:

Πρωτόκολλα Επικοινωνίας: Είναι τα εργαλεία που χρησιμοποιούνται για να επιτρέψουν στους κόμβους (nodes) του δικτύου να επικοινωνούν μεταξύ τους. Τα κυριότερα πρωτόκολλα: HTTP, WebSockets ή RPC. Αυτά τα πρωτόκολλα επιτρέπουν την αποτελεσματική διαχείριση αιτήσεων και απαντήσεων μεταξύ κόμβων, καθώς και την επικοινωνία σε πραγματικό χρόνο για την ενημέρωση του blockchain στους κόμβους (nodes) του δικτύου να επικοινωνούν μεταξύ τους. Εδώ είναι τα κυριότερα πρωτόκολλα:

- HTTP (Hypertext Transfer Protocol):
    - Εύκολο στη χρήση και ευρέως υποστηριζόμενο. Χρησιμοποιείται συχνά για τη διαχείριση αιτήσεων και απαντήσεων μεταξύ των κόμβων.
    - Παράδειγμα: Αντί να χρησιμοποιείται μόνο το Flask για τη διαχείριση των αιτήσεων, μπορεί να χρησιμοποιηθούν HTTP αιτήσεις για την επικοινωνία με άλλους κόμβους.
- WebSockets:
    - Παρέχει συνεχή, δύο κατευθύνσεων επικοινωνία μεταξύ κόμβων, γεγονός που το καθιστά ιδανικό για εφαρμογές που απαιτούν γρήγορη και συνεχή επικοινωνία, όπως για την επικοινωνία με άλλους κόμβους σε πραγματικό χρόνο.
    - Παράδειγμα: Χρήση WebSockets για την άμεση ενημέρωση των κόμβων όταν μια νέα συναλλαγή ή μπλοκ προστίθεται στο blockchain.
- RPC (Remote Procedure Call):
    - Μηχανισμός που επιτρέπει την κλήση μεθόδων ή συναρτήσεων σε απομακρυσμένο κόμβο σαν να ήταν τοπικές, χρησιμοποιώντας διάφορα πρωτόκολλα όπως JSON-RPC ή gRPC.

    - Παράδειγμα: Χρησιμοποίησε RPC για να καλέσεις συναρτήσεις επικύρωσης και προσθήκης μπλοκ σε άλλους κόμβους.

4. **Συγχρονισμός Δεδομένων:** Όταν ένας κόμβος προσθέτει ένα νέο μπλοκ ή συναλλαγή, αυτό το δεδομένο θα διανέμεται σε όλους τους άλλους κόμβους του δικτύου. Οι κόμβοι θα ενημερώνονταν αυτόματα για τις τελευταίες αλλαγές μέσω μηχανισμών συγχρονισμού, διασφαλίζοντας ότι όλοι έχουν την πιο πρόσφατη έκδοση του blockchain.

5. **Επικύρωση Συναλλαγών:** Κάθε κόμβος θα επαληθεύει τις συναλλαγές και τα μπλοκ πριν τα προσθέσει στο blockchain. Οι διαδικασίες επικύρωσης περιλαμβάνουν τον έλεγχο εγκυρότητας των συναλλαγών και την επιβεβαίωση των κριτηρίων όπως το proof-of-work, εξασφαλίζοντας την ακεραιότητα των δεδομένων.

6. **Αντοχή σε Αποτυχίες:** Ενσωματώνοντας P2P δίκτυο, η εφαρμογή θα ήταν ανθεκτική σε αποτυχίες κόμβων. Εάν ένας κόμβος αποτύχει, οι υπόλοιποι κόμβοι συνεχίζουν να λειτουργούν κανονικά, διασφαλίζοντας τη συνεχιζόμενη λειτουργία του δικτύου και την αδιάλειπτη διαχείριση των συναλλαγών.

Η ενσωμάτωσή ενός P2P δικτύου στην εφαρμογή θα επέτρεπε μια αποκεντρωμένη, πιο ανθεκτική αρχιτεκτονική, διασφαλίζοντας την ακεραιότητα και τη συνέπεια των δεδομένων. Ωστόσο, για την αρχική υλοποίηση, η κεντρική διαχείριση παρέχει μια πιο απλή και ελεγχόμενη λύση.

ΔΗΜΙΟΥΡΓΙΑ TOKEN

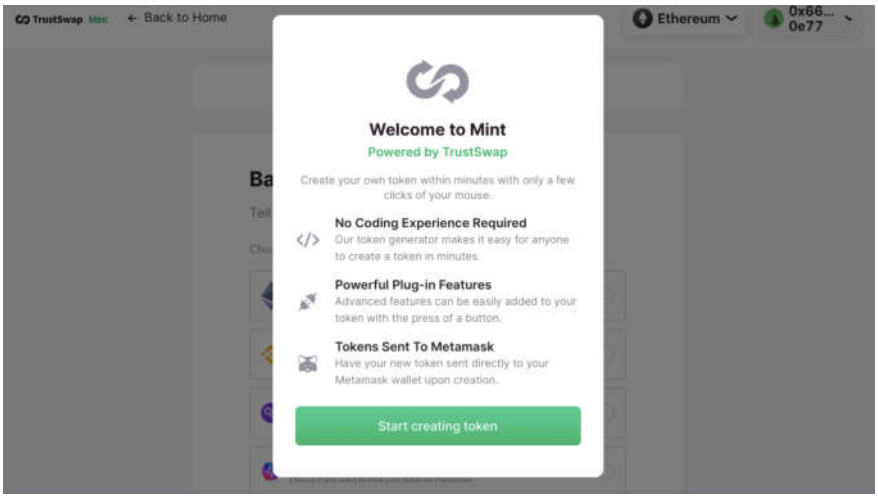
❖ ΜΕ ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΑΚΗΣ ΠΛΑΤΦΟΡΜΑΣ

Η δημιουργία ενός token, πέρα από τη συγγραφή κώδικα ενός έξυπνου συμβολαίου, μπορεί να πραγματοποιηθεί πλέον και με τη χρήση εφαρμογών όπως το MetaMask, χωρίς καμία γνώση προγραμματισμού. Ουσιαστικά πρόκειται για ένα online "πορτοφόλι" βασισμένο σε blockchain κρυπτονομισμάτων όπως του Ethereum. Στην προκειμένη, πρόκειται για μια επέκταση που μπορεί ο χρήστης να εγκαταστήσει στον browser που χρησιμοποιεί. Το MetaMask επιτρέπει στον χρήστη να δημιουργεί και να διαχειρίζεται τις δικές του ταυτότητες (μέσω ιδιωτικών κλειδιών, τοπικού πορτοφολιού χρήστη και πορτοφολιών υλικού όπως το Trezor™), οπότε όταν ένας χρήστης θέλει να πραγματοποιήσει μια συναλλαγή και να την προσθέσει στο blockchain, ο χρήστης αποκτά μια ασφαλή διεπαφή για έλεγχο της συναλλαγής, πριν την εγκρίνει ή την απορρίψει.

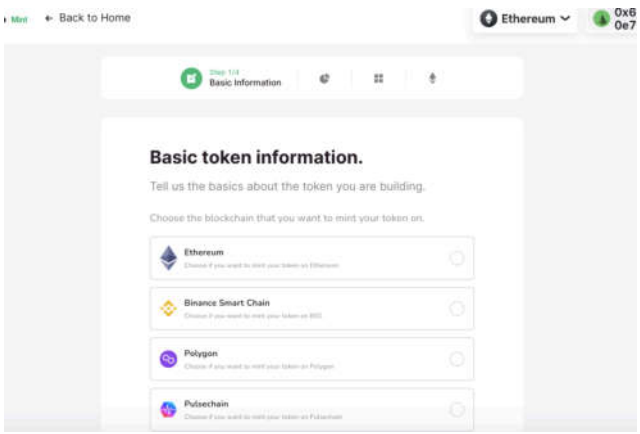
Επειδή προσθέτει λειτουργικότητα στο κανονικό περιβάλλον του προγράμματος περιήγησης, το MetaMask απαιτεί άδεια ανάγνωσης και εγγραφής σε οποιαδήποτε ιστοσελίδα. Η "πηγή" του MetaMask είναι πάντα ορατή και ο πηγαίος κώδικας δημοσιευμένος στο Github. [47]

Μιλάμε για ένα έξυπνο συμβόλαιο που "τρέχει" σε μια αλυσίδα μπλοκ. Επομένως, πολλά tokens μπορεί να φιλοξενούνται στην ίδια αλυσίδα. Χρησιμοποιώντας εφαρμογές online όπως η OpenSea, είναι σχετικά εύκολο να ορίσει κανείς και να εισάγει ένα δικό του token.

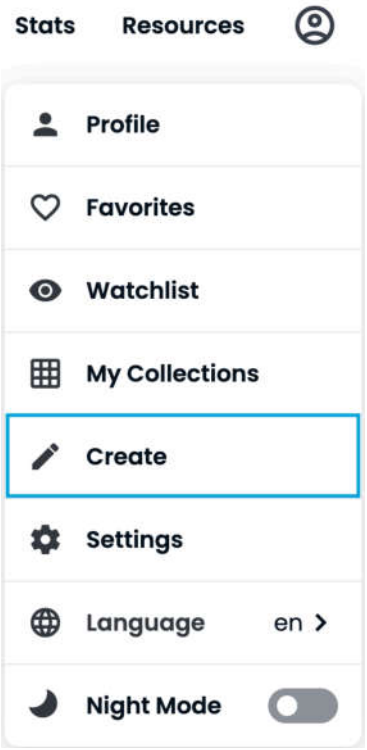
Για τους σκοπούς της εργασίας θα χρησιμοποιήσουμε την εφαρμογή Trustswap Mint (https://mint.trustswap.org). Συνδέουμε το πορτοφόλι που δημιουργήσαμε στο MetaMask και επιλέγουμε Create Coin. Εισάγουμε τις βασικές πληροφορίες, αφού επιλέξουμε την αλυσίδα πάνω στην οποία θα "τρέχει" το token. Εισάγουμε την ονομασία και ένα logo, την ποσότητα των νομισμάτων που θα κυκλοφορήσουν. Ύστερα επιλέγουμε τη δημιουργία του token, το οποίο αυτόματα περνά στο ψηφιακό μας πορτοφόλι, με μια χρέωση του ύψους των $21,82, με την τρέχουσα ισοτιμία του Ethereum, για δημιουργία token 1.000.000.000.000 μονάδων που θα τρέχει στην αλυσίδα Ethereum.



[ΕΙΚΟΝΑ 31 - ΚΑΡΤΕΛΑ ΔΗΜΙΟΥΡΓΙΑΣ OPENSEA]



[ΕΙΚΟΝΑ 33 - ΕΙΣΑΓΩΓΗ ΒΑΣΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ]



[ΕΙΚΟΝΑ 32 - ΔΗΜΙΟΥΡΓΙΑ token]

❖ ΔΗΜΙΟΥΡΓΙΑ TOKEN ΣΕ PYTHON

Για να δημιουργήσουμε ένα απλό token σε Python, μπορούμε να χρησιμοποιήσουμε την βιβλιοθήκη secrets που παρέχει ασφαλείς τυχαίους αριθμούς και συμβολοσειρές, αφού ένα token ουσιαστικά είναι απλά μια μοναδική συμβολοσειρά που μπορεί να χρησιμοποιηθεί για την αναγνώριση ή την επικύρωση ενός χρήστη ή μιας ενέργειας.

Ακολουθεί ένα παράδειγμα για τη δημιουργία ενός token:

```
import secrets

def generate_token(length=32):
    return secrets.token_hex(length)

token = generate_token()
print(f"Generated Token: {token}")
```

Αυτός ο κώδικας δημιουργεί ένα τυχαίο token με μήκος 32 bytes (64 χαρακτήρες όταν αναπαρίσταται σε δεκαεξαδική μορφή). Ο παραπάνω κώδικας, χρησιμοποιεί τη συνάρτηση secrets.token_hex για να δημιουργήσει ένα ασφαλές, τυχαίο token. Η συνάρτηση generate_token παίρνει ως παράμετρο το μήκος του token και επιστρέφει μια τυχαία δεκαεξαδική συμβολοσειρά.

Ας υποθέσουμε ότι θέλουμε να χρησιμοποιήσουμε το token που δημιουργήσαμε για να επαληθεύσουμε χρήστες σε μια εφαρμογή ιστού. Δημιουργώ ένα νέο Project PyCharm με **αρχεία app.py, index.html, styles.css**:

APP.PY

```
from flask import Flask, request, jsonify, render_template
import secrets
from datetime import datetime, timedelta

app = Flask(__name__)
users = {}  # Ένα λεξικό για αποθήκευση χρηστών και των tokens τους
def generate_token(length=32):
    return secrets.token_hex(length)

@app.route('/')
def index():
    return render_template('index.html')
```

```
@app.route('/login', methods=['POST'])
def login():
    username = request.json.get('username')
    if username:
        token = generate_token()
        users[username] = {'token': token, 'expires_at': datetime.utcnow() +
timedelta(hours=1)}
        return jsonify({'token': token}), 200
    return jsonify({'error': 'Username is required'}), 400

@app.route('/validate', methods=['POST'])
def validate():
    username = request.json.get('username')
    token = request.json.get('token')
    user_data = users.get(username)

    if not user_data:
        return jsonify({'message': 'Invalid token'}), 400

    if user_data['token'] == token:
        if datetime.utcnow() > user_data['expires_at']:
            return jsonify({'message': 'Token expired'}), 401
        return jsonify({'message': 'Valid token'}), 200

    return jsonify({'message': 'Invalid token'}), 400

if __name__ == '__main__':
    app.run(debug=True, port=5001)
```

INDEX.HTML

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Ένα απλό TOKEN</title>
    <link rel="stylesheet" href="{{ url_for('static', filename='css/
styles.css') }}">

</head>
<body>
    <div class="container">
        <h1>Ένα απλό TOKEN</h1>
        <div>
            <h2>Δημιουργία Token</h2>
```

```
            <input type="text" id="username" class="input-field"
placeholder="Username">
            <button class="button" onclick="login()">Get Token</button>
            <p id="login-response" class="response"></p>
        </div>
        <div>
            <h2>Επικύρωση Token</h2>
            <input type="text" id="token" class="input-field" placeholder="Token"
readonly>
            <button class="button" onclick="validate()">Validate</button>
            <p id="validate-response" class="response"></p>
        </div>
    </div>
    <script>
        async function login() {
            const username = document.getElementById('username').value;
            const response = await fetch('/login', {
                method: 'POST',
                headers: {
                    'Content-Type': 'application/json',
                },
                body: JSON.stringify({ username }),
            });
            const data = await response.json();
            document.getElementById('login-response').innerText =
JSON.stringify(data);
            if (data.token) {
                document.getElementById('token').value = data.token;
            }
        }

        async function validate() {
            const username = document.getElementById('username').value;
            const token = document.getElementById('token').value;
            const response = await fetch('/validate', {
                method: 'POST',
                headers: {
                    'Content-Type': 'application/json',
                },
                body: JSON.stringify({ username, token }),
            });
            const data = await response.json();
            document.getElementById('validate-response').innerText =
JSON.stringify(data);
        }
    </script>
</body>
</html>
```

STYLES.CSS

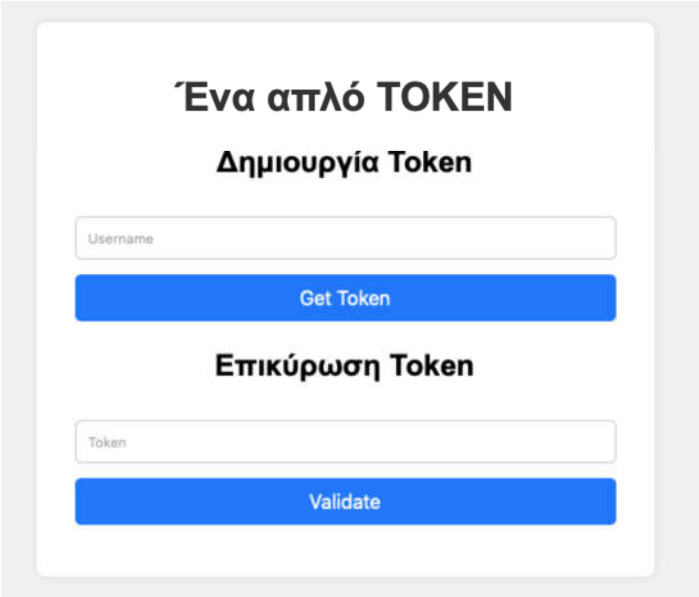
```
/* static/css/styles.css */
body {
    font-family: Arial, sans-serif;
    background-color: #f4f4f4;
    display: flex;
    justify-content: center;
    align-items: center;
    height: 100vh;
    margin: 0;
}

.container {
    background: #fff;
    border-radius: 8px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
    padding: 20px;
    width: 100%;
    max-width: 500px;
    box-sizing: border-box; /* This ensures padding is included in the element's
total width and height */
    text-align: center;
}
h1 {
    color: #333;
    margin-bottom: 20px;
    word-wrap: break-word; /* Ensures long words break properly within the container
*/
}
.input-field, .button {
    width: calc(100% - 22px); /* Adjust width to account for padding and border */
    box-sizing: border-box; /* Ensures padding and border are included in the
element's width */
}
.input-field {
    padding: 10px;
    margin: 10px 0;
    border: 1px solid #ccc;
    border-radius: 5px;
}
.button {
    font-size: 16px;
    color: #fff;
    background-color: #007bff;
    padding: 10px;
    border: none;
    border-radius: 5px;
    cursor: pointer;
```

```
    text-decoration: none;
}

.button:hover {
    background-color: #0056b3;
}

.response {
    margin-top: 20px;
    color: #333;
}
```

Σε αυτό το παράδειγμα, **η εφαρμογή Flask επιτρέπει στους χρήστες να "συνδεθούν" και να λάβουν ένα μοναδικό token, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για να επαληθεύσουν τις ενέργειές τους**. Όταν τρέξουμε την εφαρμογή βλέπουμε το εξής:

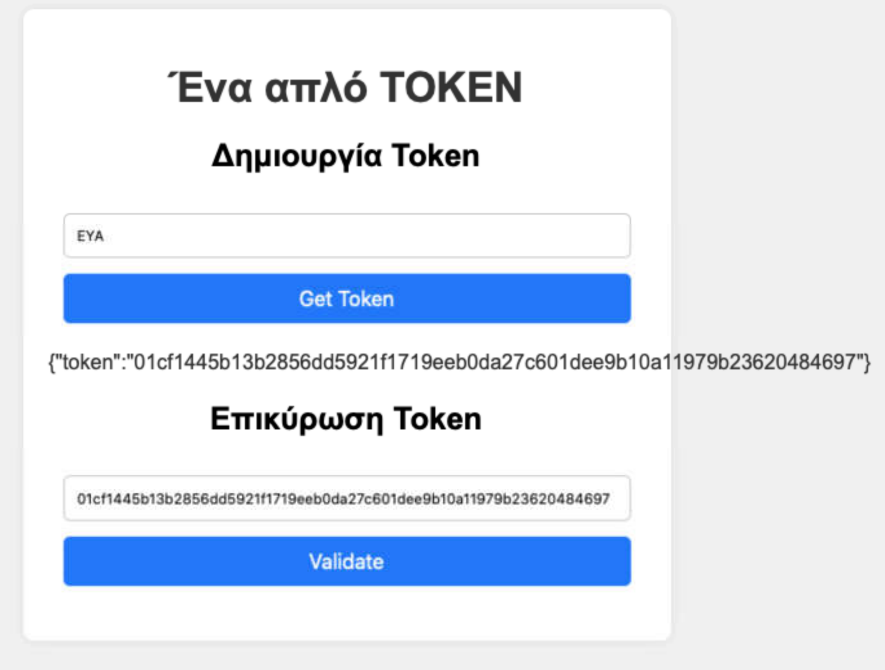
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Serving Flask app 'app'
* Debug mode: on
* Running on http://127.0.0.1:5001 (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 794-555-883

Η σελίδα στην οποία μας οδηγεί ο σύνδεσμος:



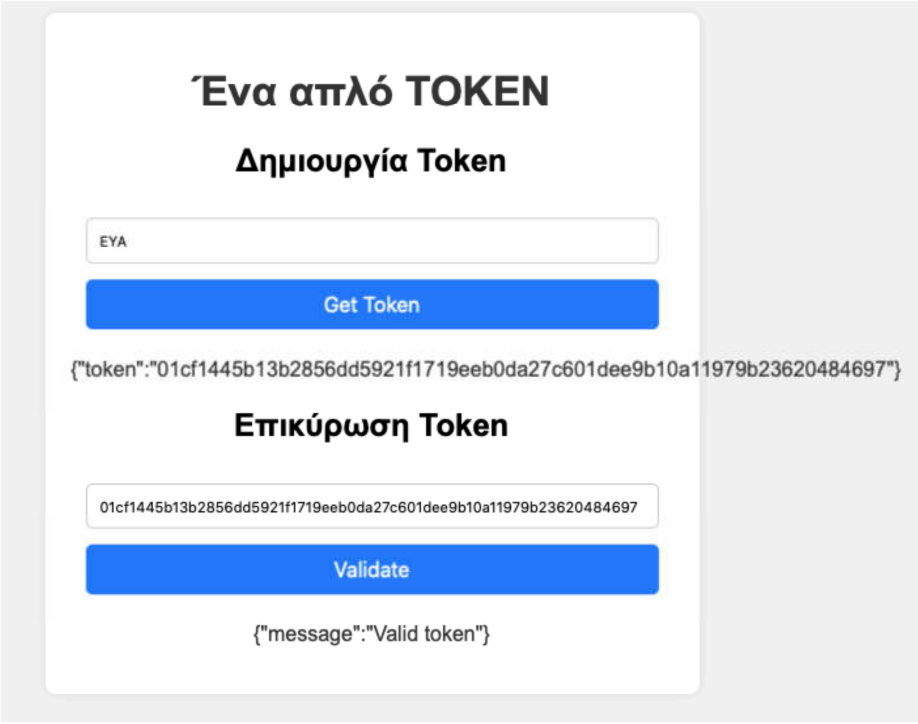
[ΕΙΚΟΝΑ 34 - ΕΝΑ ΑΠΛΟ token]

Εγγραφή χρήστη και δημιουργία Token:



[ΕΙΚΟΝΑ 35 - ΕΝΑ ΑΠΛΟ token]

Επικύρωση Token:



[ΕΙΚΟΝΑ 36 - ΕΝΑ ΑΠΛΟ token]

ΣΥΜΠΕΡΑΣΜΑΤΙΚΑ:

Τα tokens και τα κρυπτονομίσματα εξυπηρετούν διαφορετικούς σκοπούς και βασίζονται σε διαφορετικές τεχνολογικές υποδομές. Η δημιουργία ενός token μπορεί να είναι απλή, χρησιμοποιώντας υπάρχουσες πλατφόρμες blockchain, ενώ για τη δημιουργία ενός κρυπτονομίσματος απαιτείται η ανάπτυξη μιας αλυσίδας blockchain από την αρχή.

Ακόμα, τα tokens χρησιμοποιούνται για σκοπούς όπως η πρόσβαση σε συγκεκριμένες υπηρεσίες, ή δυνατότητες μιας πλατφόρμας, για ψηφοφορία με χρήση αποκεντρωμένων συστημάτων, για επαλήθευση ταυτότητας κ.α. Τα κρυπτονομίσματα όμως χρησιμοποιούνται ως μέσο ανταλλαγής και απεικόνισης αξίας. Μπορούν να χρησιμοποιηθούν σε οικονομικές συναλλαγές και επενδύσεις.

ΑΝΑΦΟΡΕΣ-ΒΙΒΛΙΟΓΡΑΦΙΑ-ΠΗΓΕΣ

ΑΝΑΦΟΡΕΣ

[1] Forecast: Blockchain Business Value, Worldwide, 2017-2030 : https://www.gartner.com/guest/purchase/registration?resId=3627117.

[2] H. F. Atlam and G. B. Wills, "Characteristics of blockchain" in Technical Aspects of Blockchain and IoT, Amsterdam, The Netherlands:Elsevier, pp. 8-10, 2018.

[3] Baxendale G . Can Blockchain Revolutionise EPRs? *ITNOW*, Volume 58, Issue 1, Spring 2016, Pages 38–39, Published: 16 February 2016, https://academic.oup.com/itnow/article/58/1/38/2392002.

[4] Oil and Gas Industry—Blockchain, the Disruptive Force of the 21st Century, Infosys, Bengaluru, India, 2018 : https://www.infosys.com/industries/oil-and-gas/features-opinions/ Documents/blockchain-disruptive-force.pdf

[5] Deloitte. (2017). Blockchain: Overview of the Potential Applications for the Oil and Gas Market and the Related Taxation Implications: https://www2.deloitte.com/content/ dam/Deloitte/global/Documents/Energy-and-Resources/gx-oil-gasblockchain-article.pdf

[6] M. Koeppen, D. Shrier, and M. Bazilian. (2017). Is Blockchain's Future in Oil and Gas Transformative or Transient? Deloitte: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/energyresources/gx-blockchain-report-future-in-oil-and-gas.pdf

[7] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, ''Blockchain-empowered secure Internet-of-battlefield things (IoBT) architecture,'' in Proc. IEEE Mil. Commun. Conf. (MILCOM), Los Angeles, CA, USA, Oct. 2018, pp. 593–598: https://ieeexplore.ieee.org/document/8599758

[8] Umesh Bodkhe, Karan Parekh, Pimal Khanpara - Institute of Technology, Nirma University, Ahmedabad, India- Sudhanshu Tyagi, Neeraj Kumar ,Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, India - Mamoun Alazab, College of Engineering, IT and Environment, Charles Darwin University, Casuarina, Australia - "Blockchain for Industry 4.0: A Comprehensive Review", https://ieeexplore.ieee.org/abstract/document/9069885

[9] Αναπληρωτής Καθηγητής Παναγιώτης Κουρουθανάσης, Ιόνιο Πανεπιστήμιο, Καθηγητής Γεώργιος Δουκίδης, Οικονομικό Πανεπιστήμιο Αθηνών, Σεπτέμβριος 2018 - ΔΙΕΘΝΕΙΣ ΤΑΣΕΙΣ ΤΟΥ ΚΛΑΔΟΥ ΕΤΑΙΡΕΙΩΝ ΧΡΗΜΑΤΟ-ΟΙΚΟΝΟΜΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ (FINTECH) ΚΑΙ ΠΡΟΟΠΤΙΚΕΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ Επιτελική Σύνοψη, http://docplayer.gr/106075414-Diethneis-taseis-toy-kladoy-etaireion-hrimato-oikonomikis-tehnologias-fintech-kai-prooptikes-gia-tin-ellada-epiteliki-synopsi.html

[10] SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE - DAVID CHAUM, https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf

[11] Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin, By NATHANIEL POPPER, MAY 15, 2015 - https://core.ac.uk/reader/301669050

[12] Bit Gold - Nick Szabo, December 29, 2005, https://nakamotoinstitute.org/bit-gold/

[13] Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf

[14] 5 Things About Mt. Gox's Crisis , By Paul Vigna, Feb. 25, 2014, The Wall Street Journal, https://www.wsj.com/articles/BL-263B-352

[15] Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss - Carter Dougherty and Grace Huang, 28 Φεβρουαρίου 2014, https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy

[16] Bitcoin currency could have been destroyed by '51%' attack, Alex Hern, Mon 16 Jun 2014, https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io

[17] The Top 25 Cryptocurrencies to Know in 2021: BTC, ETH, XRP, XLM and More, Thomas Yeung , https://www.nasdaq.com/articles/the-top-25-cryptocurrencies-to-know-in-2021%3A-btc-eth-xrp-xlm-and-more-2021-01-13

[18] Introduction to smart contracts, https://ethereum.org/en/developers/docs/smart-contracts/

[19] Smart contracts reduce mental transaction costs, Nick Szabo, Apr 2006, https://unenumerated.blogspot.com/2006/04/smart-contracts-reduce-mental.html

[20] Formalising and securing relationships on public networks, Nick Szabo, https://firstmonday.org/ojs/index.php/fm/article/view/548/469

[21] The Bitcoin mining game, Paper by Nicolas Houy, March 2014,GROUPE D'ANALYSE ET DE THÉORIE ÉCONOMIQUE LYON - ST ÉTIENNE

[22] FCA warns consumers of the risks of investments advertising high returns based on cryptoassets, https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets

[23] Setting the standard for institutional crypto markets. https://www.bakkt.com/bakkt-markets

[24] To Token or not to Token: Tools for Understanding Blockchain Tokens - Oliveira, Luis ; Zavolokina, Liudmila ; Bauer, Ingrid ; Schwabe, Gerhard - Zurich Open Repository and Archive University of Zurich Main Library

[25] What is ADA? - https://cardano.org/what-is-ada/

[26] Ring Signatures, Stealth Address https://www.getmonero.org/resources/moneropedia/

[27] TOR Browser information, https://www.torproject.org/

[28] TAILS System information, https://tails.boum.org/index.en.html

[29] QUBES OS information, qubes-os.org/intro/

[30] Is Facebook's Libra Project Already a Miscarriage? John Taskinsoy University Malaysia Sarawak (UNIMAS), August 15, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3437857

[31] Measuring dark web marketplaces via Bitcoin transactions: From birth to independence, NaokiHiramoto, YoichiTsuchiya, Forensic Science International: Digital Investigation, Volume 35, December 2020, 301086

[32] Cybersecurity economics, https://www.kaspersky.com/blog/it-security-economics-2020-main/37205/

[33] Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty, by Douglas Cumming, Sofia Johan, Anshum Pant, *J. Risk Financial Manag.* 2019, *12*(3), 126; https://doi.org/10.3390/jrfm12030126, Received: 9 May 2019 / Revised: 12 July 2019 / Accepted: 12 July 2019 / Published: 24 July 2019

[34] Μελέτη: Η Χρήση Κρυπτονομισμάτων για Παράνομες Δραστηριότητες και Σχετικές Νομοθετικές Πρωτοβουλίες - Νικόλαος Θεοδωράκης, Λέκτορας και Συνεργάτης, University of Oxford, Συνεργάτης, Stanford University

[35] FinCEN, March 18, 2013, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, available at: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[36] Denial of Defense Motion: Opinion & Order, United States of America v. Ulbricht, Forrest, Doc. 14-cr-68 (S.D.N.T., July 9, 2014) at 48.

[37] Draft updated Guidance for a risk-based approach to virtual assets and VASPs, https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf

[38] Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέματα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις αγορές κρυπτοστοιχείων και για την τροποποίηση της οδηγίας (ΕΕ) 2019/1937» [COM(2020) 593 final – 2020/0265 (COD)] και «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ένα πιλοτικό καθεστώς για τις υποδομές της αγοράς που βασίζονται σε τεχνολογία κατανεμημένου καθολικού» [COM(2020) 594 final – 2020/0267 (COD)] (2021/C 155/05) Εισηγητής: Giuseppe GUERINI, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 30.04.2021

[39] ΕΚΘΕΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ για την αξιολόγηση του πλαισίου συνεργασίας μεταξύ των μονάδων χρηματοοικονομικών πληροφοριών, Βρυξέλλες, 24.7.2019, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52019DC0371&from=EN

[40] Digital Trade Coin (DTC): Towards a more stable digital currency, Alex Lipton, Thomas Hardjono, Alex Pentland, MIT Connection Science Massachusetts Institute of Technology Cambridge, MA, USA, http://tradecoin.mit.edu/sites/default/files/documents/mit-tradecoin-rsos.pdf

[41] Petro White Paper, https://whitepaperdatabase.com/venezuela-petro-cryptocurrency-ptr-english-whitepaper/

[42] Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'? Ignacio Herrera Anchustegui and Tina Soliman Hunter, Posted: 17 Dec 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3291272

[43] CENTRAL BANK DIGITAL CURRENCY AND THE FUTURE OF MONETARY POLICY Michael D Bordo, Andrew T Levin, Working Paper 23711, http://www.nber.org/papers/w23711 NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, MA 02138 August 2017

[44] Diem Official White Paper, https://www.diem.com/en-us/white-paper/

[45] Atlantic Council: **CBDC Tracker,** https://www.atlanticcouncil.org/cbdctracker, IMF: Central Bank Digital Currencies (CBDCs), https://www.imf.org/en/Topics/fintech/cbdc, BIS (Bank for International Settlements): CBDCs: An Opportunity for the Monetary System, https://www.bis.org/publ/arpdf/ar2024e.htm, Watcher Guru: G20 Countries Progress in CBDC Development, https://watcher.guru/news/g20-countries-progress-in-cbdc-development, Central Bank Digital Currency Tracker: **CBDC Projects Overview,** https://www.cbdctracker.org

[46] Ψηφιακό Νόμισμα Κεντρικής Τράπεζας (CBDC): Η στάση του Ευρωσυστήματος, https://www.bankofgreece.gr/AmiPayT2S/AMI-PAY-GR-NSG/[AMI-PayGR-NSG]-04-11-20-(7)-CBDC.pdf

[47] Πληροφορίες για το MetaMask : https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΜΕΛΕΤΗ/ΠΗΓΕΣ

Clinch, M. (2013). *Bitcoin recognized by Germany as 'private money*, από http://www.cnbc.com/id/100971898.

De Vries, A. (2018). Bitcoin's Growing Energy Problem *Joule 2*, May 16,2018 pp 801-809.
Dowd, K. (1988). Private Money, The path to Monetary Stability Groundbreaking analysis of the benefits of free banking, *The Institute of Economic Affairs*, Hobart Paper 112.
Dowd, K. (2014). New Private Monies – a Bit-part Player? *Cobden Centre and The Institute of* Economic Affairs, Hobart Paper 174.
Freeman, A. (2011). Further Observations on Bitcoin, Digital Currencies, Privacy and Liberty.

Friedman, M. (1970). *The Counter-Revolution in Monetary Theory*, Occasional paper 33, Institute of Economic Affairs.

Friedman, M. (1984). Currency Competition: A Skeptical View. Χάγη: Martinus Nijhoff, pp. 42-46.

Hartge-Hazelman, B. (2013). *Glenn Stevens says Bitcoins show promise, but so did* tulips. The Australian Financial Review.http://www.afr.com/p/national/glenn_stevens_says_bitcoins_show_GWLQFcefJfF4RmiE0Z08AJ

Hayek, F.A. (1976). *Choice in Currency – A way to stop inflation*. ονδίνο:The Institute of Economic Affairs.

Hayek, F.A. (1990). Denationalisation of Money – The Argument Refined: An Analyses of the Theory and Practice of Concurrent Currencies, ονδίνο: The Institute of Economic Affairs.

Kubat, M. (2014). An analysis of Bitcoin. 13TH International Academic Conference Antibes.

Pedro, F. (2014). Understanding Bitcoin, Cryptography, Engineering and Economics. pp. 3-10. H.A.: Wiley Finance series.

Popper, N. (2018). Goldman will open trade unit for Bitcoin. *New York Times*, σ. B1.

Anonymous Peer-to-Peer File Sharing. University of Cambridge, Queens' College – Computer Science. https://queenscompsci.wordpress.com/2015/02/12/anonymous-peer-to-peer-file-sharing/

University of Nicosia. Ανακτήθηκε από https://www.unic.ac.cy/el/study/admissions/financial-information/payment-options
What is Bitcoin. (2018). Ανακτήθηκε 31 αϊου 2018 από https://bitcoin.org/el/faq#what-is-bitcoin.

Weber, B. (2014). *Bitcoin and the legitimacy crisis of money*. Cambridge Journal of Economics. http://dx.doi.org/10.1093/cje/beu067

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

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΜΕΛΕΤΗ/ΠΗΓΕΣ ΓΙΑ ΤΙΣ ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΤΟΝ ΚΩΔΙΚΑ

ΒΙΒΛΙΑ

1. "Mastering Bitcoin" του Andreas M. Antonopoulos: Antonopoulos, A. M. (2017). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.

2. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" του Daniel Drescher: Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.

3. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" του Imran Bashir: Bashir, I. (2018). Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. Packt Publishing.

ΑΡΘΡΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

1. Bitcoin Whitepaper του Satoshi Nakamoto: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

2. Coursera Course on Blockchain: Coursera. (2024). Blockchain Basics. Retrieved from https://www.coursera.org/learn/blockchain-basics

ΑΡΘΡΑ ΚΑΙ TUTORIALS

1. A Gentle Introduction to Blockchain Technology" του Antony Lewis: Lewis, A. (2018). A Gentle Introduction to Blockchain Technology. Retrieved from https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/

2. "Build your own blockchain – The basics" από το Hackernoon: Hackernoon. (2018). Build your own blockchain – The basics. Retrieved from https://hackernoon.com/learn-blockchains-by-building-one-117428612f46

3. UDemy - Courses on Demand, Build a Blockchain & Cryptocurrency using Python, Dr. Zakwan Jaroucheh

ΓΙΑ ΤΗ ΔΗΜΙΟΥΡΓΙΑ Token σε Python:

1. Flask Documentation - Quickstart Guide: Γρήγορος οδηγός εκκίνησης (Quickstart Guide) για δημιουργία απλού web application χρησιμοποιώντας το Flask.

- Σύνδεσμος: Flask Quickstart Guide

2. Flask Documentation - API Reference: αναλυτική περιγραφή των διαφορετικών συναρτήσεων και κλάσεων.

- Σύνδεσμος: Flask API Reference

3. Python Documentation - secrets module: Για τη δημιουργία των τυχαίων tokens, μπορείς να αναφέρεσαι στην τεκμηρίωση της Python για το module secrets.

- Σύνδεσμος: Python secrets module documentation

ΓΙΑ ΤΗ ΔΙΑΦΟΡΑ ΜΕΤΑΞΥ Token και Κρυπτονομισμάτων:

1. Cryptocurrency vs Token: What's the Difference? - CoinMarketCap

- Σύνδεσμος: Cryptocurrency vs Token: What's the Difference? - CoinMarketCap

2. Understanding Tokens and Their Role in Cryptocurrency Ecosystems - Binance Academy:

- Σύνδεσμος: Understanding Tokens and Their Role in Cryptocurrency Ecosystems - Binance Academy

3. ERC-20 Token Standard - ethereum.org

- Σύνδεσμος: ERC-20 Token Standard - ethereum.org