Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π Α Τ Ρ Ω Ν

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

Ε Ρ Γ Α Σ Ι Α Ε Ξ Α Μ Η Ν Ο Υ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ & ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΧΡΗΣΗ ΠΛΑΣΤΙΚΟΥ ΧΡΗΜΑΤΟΣ & ΨΗΦΙΑΚΟΥ ΝΟΜΙΣΜΑΤΟΣ

ΝΙΚΗ ΛΟΥΚΕΡΗ

Α.Μ 5817

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

- **AS** – Authentication Server
- **ATM** – Automated Teller Machine
- **CA** – Certificate Authority
- **CVV** –Card Verification Value
- **DES** – Data Encryption Standard
- **ID** –IDentification
- **KDC** –Key Distribution Center
- **PIN** –Personal Identification Number
- **PKI** – Public Key Infrastructure
- **POS** –Point Of Sale
- **P2P-** peer-to-peer
- **RSA** – Ron **R**ivest, Adi **S**hamir and Len **A**dleman.
- **SET** –Secure Electronic Transaction
- **TGS** –Ticket Granting Server

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Πρόλογος

«Ο άνθρωπος είναι ον φύσει κοινωνικό και πολιτικό», αναφέρει ο φιλόσοφος Αριστοτέλης[U6] για να περιγράψει τη φύση της ανθρώπινης ύπαρξης που είναι απόλυτα συνυφασμένη με το κοινωνικό και πολιτικό πλαίσιο της πραγματικότητας, που την περικλείει. Ο Αριστοτέλης υποστήριζε ότι η προσωπική πρόοδος κάθε ανθρώπινου όντος δεν μπορεί να επιτευχθεί ανεξάρτητα από την πρόοδο του τόπου στον οποίο ζει και δρα, συνεισφέροντας βέβαια τόσο στην κοινωνική εξέλιξη όσο και στην πολιτική σκηνή του τόπου. Δηλαδή, άνθρωπος χωρίς πολιτική και κοινωνική συμμετοχή στα δρώμενα ισοδυναμεί με άνθρωπο χωρίς ατομική ταυτότητα και ύπαρξη.

Στο σημείο αυτό, πραγματοποιώντας προσπάθεια απαγκίστρωσης από το φιλοσοφικό πλαίσιο που περιβάλλει το ζήτημα, εξετάζοντας το θέμα πιο ρεαλιστικά, συμπεραίνεται ότι η βελτίωση του βιοτικού επιπέδου κάθε ανθρώπου είναι αναπόφευκτα συνδεδεμένη με την ομαλή λειτουργία της κοινωνίας στην οποία ζει. Συγκεκριμένα, όταν μία κοινωνία ευημερεί και διακατέχεται από τα προνόμια της κοινωνικής ασφάλειας και της οικονομικής ευρωστίας μπορεί να προσφέρει στους πολίτες της τη δυνατότητα να διεκδικήσουν την προσωπική άνοδο που θα οδηγήσει φυσικά και στην εκ νέου πρόοδο της κοινωνίας. Πρόκειται στην ουσία για ένα σύστημα ανατροφοδότησης που κάθε επιμέρους συνδετικός κρίκος της αλυσίδας συμβάλλει στην ανάπτυξη της κοινωνίας ως ολότητα. Στις μέρες μας, αδιαμφισβήτητα υπάρχει κοινωνική και οικονομική εξέλιξη. Η ανάπτυξη της οικονομίας έχει καταστήσει το χρήμα κινητήριο δύναμη της αγοράς ενώ η κοινωνική πρόοδος έχει προσφέρει την δυνατότητα της πολύπλευρης εκμετάλλευσής του.

Η ισχυρή αγορά διαθέτει πληθώρα αγαθών με διακύμανση τιμών. Οι ανάγκες των καταναλωτών λόγω βελτίωσης του κοινωνικού και βιοτικού τους επιπέδου καθιστούν απαραίτητη την κατοχή ολοένα και περισσότερων αγαθών δημιουργώντας τον νόμο της προσφοράς και της ζήτησης[Δ6]. Οι ανάγκες των καταναλωτών γίνονται ολοένα και περισσότερες και η κυκλοφορία περισσότερων προϊόντων και αγαθών

γίνεται ζωτικής σημασίας καθιστώντας έτσι τις συναλλαγές κυρίαρχη δύναμη της αγοράς και το χρήμα κυρίαρχο παίκτη στο παιχνίδι της καθημερινής επιβίωσης. Η σημερινή εποχή αποτελεί μια περίοδο παγκοσμιοποίησης, οι αγορές είναι προσβάσιμες και το χρήμα αποτελεί το μέσο ανόδου. Αν συνυπολογιστεί και η τεχνολογική έξαρση τότε σίγουρα συμπεραίνεται ότι ο τομέας των οικονομικών συναλλαγών διαδραματίζει σπουδαίο ρόλο στην καθημερινότητά μας.

Το διαδίκτυο, αναπόσπαστο κομμάτι της τεχνολογίας, αποτελεί την ναυαρχίδα της πληροφόρησης και της ενημέρωσης. Η εποχή της ψηφιοποίησης επιβάλλει την εισαγωγή της τεχνολογίας όχι μόνο στον τομέα της ενημέρωσης αλλά και στον τομέα των οικονομικών συναλλαγών. Η εφαρμογή της ψηφιοποίησης στον τομέα των τηλεπικοινωνιών μετέτρεψε την άλλοτε αναλογική επεξεργασία εικόνας και ήχου σε ψηφιακή, διευκολύνοντας την απευθείας μετάδοση του υλικού μέσω ειδικών ψηφιακών προγραμμάτων. Επίσης, η μετάβαση από το αναλογικό στο ψηφιακό σήμα στις σύγχρονες τηλεοράσεις οδηγεί στην βελτίωση της ευκρίνειας μετάδοσης της τηλεοπτικής εικόνας δημιουργώντας μια νέα εποχή στον τομέα του οπτικοακουστικού υλικού. Στον τομέα των οικονομικών συναλλαγών, η τεχνολογία προσέφερε το διαδίκτυο, μια πλατφόρμα αποκεντρωμένη και ελεύθερα προσβάσιμη, μετατρέποντας τις έως τότε παραδοσιακές μεθόδους πληρωμής σε ηλεκτρονικές. Ο απλός πολίτης επιθυμεί άμεσες, γρήγορες και φυσικά ασφαλείς συναλλαγές σε όποιο σημείο του πλανήτη και αν βρίσκεται.

Επομένως, η τεχνολογία δηλώνει έτοιμη να προσφέρει απλόχερα τις καινοτομίες της, εισάγοντας τις έννοιες του πλαστικού χρήματος και του ψηφιακού νομίσματος στο σύγχρονο οικονομικό προφίλ της κοινωνίας.

1.2 Το Χρήμα

Το χρήμα αποτελεί το μέτρο αξίας όλων των εμπορευμάτων και το απόλυτο μέσο διεκπεραίωσης όλων των οικονομικών συναλλαγών. Η ανακάλυψη του νομίσματος επιτεύχθηκε όταν ο άνθρωπος, θέλοντας να ανταλλάξει προϊόντα με τους συνανθρώπους του, παρατήρησε ότι ήταν μείζονος σημασίας η χρήση ενός αντιπροσωπευτικού μέτρου αξίας για τα εμπορεύματά του ώστε να λυθεί η ανισορροπία στην αξία των προϊόντων[U5] κατά την διάρκεια της μεταξύ τους ανταλλαγής χωρίς νομισματικό αντίβαρο. Έτσι από την αρχαιότητα εμφανίζονται τα πρώτα σημάδια ενεργούς χρήσης του νομίσματος.

Με το πέρασμα των χρόνων η εξέλιξη των κοινωνιών δημιούργησε και εξέλιξη στις οικονομικές συναλλαγές με αποτέλεσμα να εμφανίζονται ολοένα και περισσότερες ανάγκες στην αγοραπωλησία των προϊόντων που οδήγησε στην εξέλιξη τόσο του ίδιου του νομίσματος όσο και της αξίας του. Γεγονός αποτελεί και η δραστηριοποίηση των τραπεζών και κατ'επέκταση των τραπεζικών συναλλαγών.

Σταδιακά, πραγματοποιείται και η εμφάνιση της πρώτης πιστωτικής κάρτας, μιας «αποθήκης» χρημάτων. Η πιστωτική κάρτα απαγκίστρωσε τον απλό πολίτη από την ιδέα ότι οι οικονομικές συναλλαγές μπορούν να διεκπεραιωθούν μόνο με την άμεση πληρωμή χρημάτων. Σήμερα, μπορεί ο όρος της πιστωτικής κάρτας να είναι απόλυτα συνυφασμένος με το πλαστικό χρήμα, ωστόσο η πρώτη πιστωτική κάρτα, στην περίοδο του 1950[U16], ήταν φτιαγμένη από χαρτόνι ή ζελατίνα. Μία δεκαετία αργότερα, η πιστωτική κάρτα μπαίνει δυναμικά στο χώρο του πλαστικού χρήματος, διευκολύνοντας την πληρωμή ακόμα και με έλλειψη μετρητών.

Μέσα σε όλο αυτό το κλίμα προόδου, πραγματοποιείται και η εμφάνιση του διαδικτύου. Όπως είναι ευρέως γνωστό, το διαδίκτυο[U17][B2] είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές, που εκτείνεται παγκοσμίως σε κάθε δυνατή γωνιά του πλανήτη καθιστώντας εφικτή τη δυνατότητα ανταλλαγής μηνυμάτων και παροχής υπηρεσιών μεταξύ χρηστών, που είναι γεωγραφικά απομακρυσμένοι. Οι δυνατότητες του διαδικτύου γίνονται ολοένα και μεγαλύτερες με αποτέλεσμα το διαδίκτυο να έχει εισβάλλει ενεργά και στην οικονομική δραστηριότητα. Το σημαντικότερο πλεονέκτημα, που καθιστά το διαδίκτυο ιδιαίτερα προσφιλές για τις μελλοντικές οικονομικές δραστηριότητες είναι η απουσία μιας κεντρικής ελεγκτικής δύναμης, όπως είναι η τράπεζα.

Τα βήματα της οικονομίας οδηγούνται σταθερά και προοδευτικά στο ψηφιακό νόμισμα με το διαδίκτυο να κρατά τα ηνία των ψηφιακών συναλλαγών. Στόχος είναι οι ασφαλείς συναλλαγές με όσο το δυνατόν μικρότερη επίδραση από τρίτα πρόσωπα, που παρεμβαίνουν στην εμπιστοσύνη μεταξύ εμπόρου και καταναλωτή.

1.3 Σύνοψη

Στόχος της παρούσας εργασίας είναι να αναλυθούν λεπτομερώς δύο βασικοί τρόποι διεξαγωγής των ηλεκτρονικών συναλλαγών. Εκ πρώτης όψεως, θα δοθεί ιδιαίτερη βαρύτητα στην χρήση του πλαστικού χρήματος που αποτελεί τον βασικό τρόπο πληρωμής στην εποχή μας. Θα μελετηθεί τόσο το προσκήνιο όσο και το παρασκήνιο μέσα στο οποίο πραγματώνονται οι συναλλαγές με χρήση πιστωτικών καρτών και θα αναλυθούν τα τεχνολογικά χαρακτηριστικά, που τις απαρτίζουν. Στην συνέχεια θα περιγραφεί το μέλλον των οικονομικών συναλλαγών με χρήση του ψηφιακού νομίσματος. Θα περιγραφεί ο τρόπος διεκπεραίωσης μιας τέτοιας μορφής συναλλαγής καθώς και οι αδυναμίες της. Τέλος θα παρουσιαστεί μια συγκριτική μελέτη σχετικά με τα πλεονεκτήματα και τα μειονεκτήματα αυτών των δύο μεθόδων διεκπεραίωσης των οικονομικών συναλλαγών.

ΚΕΦΑΛΑΙΟ 2: ΠΛΑΣΤΙΚΟ ΧΡΗΜΑ

Το πρώτο στάδιο της εξελικτικής πορείας των οικονομικών συναλλαγών, το οποίο χρησιμοποιείται ευρέως στις σημερινές σύγχρονες αγοραπωλησίες, εντοπίζεται στην χρήση του πλαστικού χρήματος. Ο όρος πλαστικό χρήμα χρησιμοποιείται προκειμένου να αποσαφηνιστεί η διαφορά ανάμεσα στην ολοκλήρωση μιας συναλλαγής με χρήση μιας πλαστικοποιημένης κάρτας εικονικών χρημάτων έναντι της χρήσης μετρητών χαρτονομισμάτων. Στην σημερινή εποχή, η χρήση του πλαστικού χρήματος είναι ιδιαίτερα διαδομένη αφενός λόγω ευκολίας χρήσης της και αφετέρου λόγω απαίτησης του φορολογικού συστήματος. Στις ακόλουθες ενότητες του κεφαλαίου πρόκειται να μελετηθεί λεπτομερώς, από την τεχνολογική σκοπιά, το φαινόμενο του πλαστικού χρήματος, θα αποσαφηνιστούν βασικές έννοιες και θα αναλυθεί πλήρως ο τρόπος λειτουργίας τους.

2.1 Σύγκριση Πιστωτικής και Χρεωστικής Κάρτας

Δύο είναι τα βασικά χαρακτηριστικά δείγματα που αντιπροσωπεύουν το πλαστικό χρήμα, η πιστωτική κάρτα και η χρεωστική κάρτα. Υπάρχει μια στοιχειώδης διαφορά ανάμεσα στις δύο αυτές κάρτες συναλλαγών. Όταν πραγματοποιείται μια συναλλαγή με χρεωστική κάρτα, το ποσό της αγοράς αφαιρείται άμεσα από τον λογαριασμό του κατόχου της κάρτας αν και εφόσον ο λογαριασμός στην τράπεζα περιέχει το αναγκαίο υπόλοιπο για να καλύψει τις ανάγκες της αγοράς. Αντίθετα, μια συναλλαγή με πιστωτική κάρτα δεν απαιτεί την ύπαρξη συγκεκριμένου υπολοίπου στον λογαριασμό για την ολοκλήρωσή της. Συγκεκριμένα, το ποσό της συναλλαγής καταγράφεται στην πιστωτική κάρτα και μετά το πέρας 30-40 ημερών[Δ5] ο κάτοχος λαμβάνει έναν λογαριασμό με τα συνολικά του έξοδα κατά την διάρκεια αυτών των ημερών προκειμένου να καταβάλλει το ποσό των εξόδων. Στην ουσία, η πιστωτική κάρτα διαμορφώνει μια έννοια «δανεικών» χρημάτων. Δηλαδή, στην χρεωστική κάρτα ξοδεύουμε χρήματα που ήδη διαθέτουμε στον λογαριασμό μας ενώ στην περίπτωση της πιστωτικής κάρτας ξοδεύουμε χρήματα τα οποία δεν διαθέτουμε άμεσα αλλά πρόκειται να τα αποκτήσουμε μελλοντικά προκειμένου να ξεχρεώσουμε το ποσό των συνολικών αγορών μας.

2.1.1 Χαρακτηριστικά Χρεωστικών και Πιστωτικών Καρτών

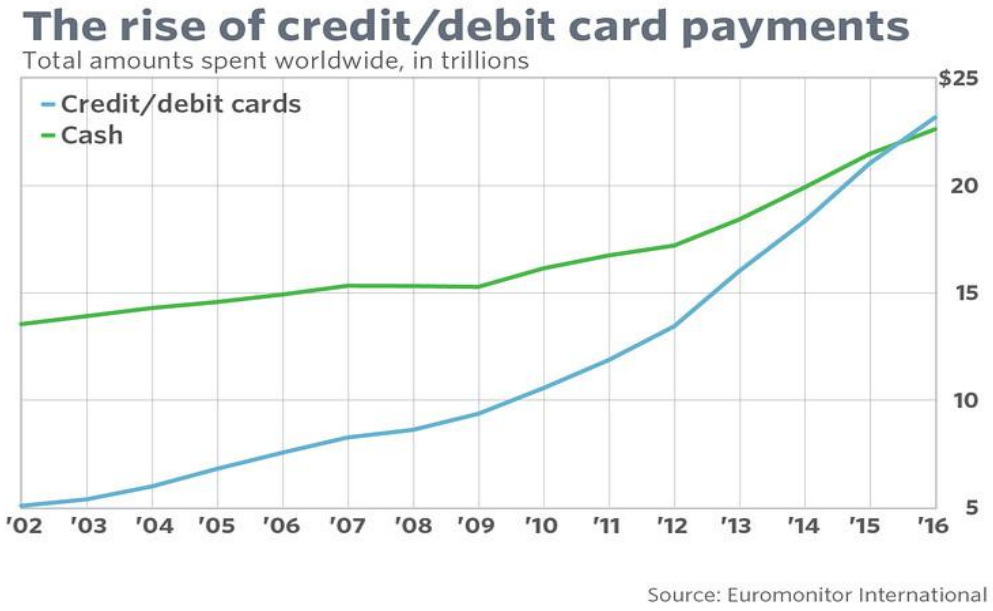
Οι χρεωστικές κάρτες[U1], όπως αναφέρθηκε, είναι ένας τρόπος πληρωμής άμεσα συνυφασμένος με την χρήση των μετρητών με την έννοια ότι ο κάτοχος μπορεί να έχει άμεση επίγνωση των οικονομικών του εξόδων καθώς δεν δημιουργούνται μελλοντικά χρέη. Κάθε χρεωστική κάρτα είναι συνδεδεμένη με έναν τραπεζικό λογαριασμό στο όνομα του κατόχου της χρεωστικής κάρτας. Όταν πραγματοποιείται μια συναλλαγή, το απαιτούμενο ποσό δεσμεύεται απευθείας από τον λογαριασμό του κατόχου και οδηγείται στα λογιστικά έξοδα της κάρτας προκειμένου να αποφευχθεί η ανάληψη του συγκεκριμένου ποσού από τον κάτοχο. Στην συγκεκριμένη φάση της διαδικασίας πληρωμής το ποσό παραμένει στον κάτοχο της κάρτας αλλά είναι δεσμευμένο χωρίς να μπορεί ο ίδιος να έχει πρόσβαση σε αυτό. Έπειτα από την πάροδο λίγων ημερών, το ποσό αφαιρείται εντελώς από τον λογαριασμό του καταναλωτή και περνά απευθείας στον λογαριασμό του εμπόρου ολοκληρώνοντας έτσι την αγορά. Με αυτόν τον τρόπο, οποιαδήποτε αγορά μπορεί να επιτευχθεί μόνο με την άμεση καταβολή του συνολικού ποσού της αγοράς. Η δυνατότητα υλοποίησης της πληρωμής με χρήση κάρτας πραγματοποιείται μέσω του συστήματος POS που διαθέτουν τα καταστήματα, όπου ο καταναλωτής καλείται να πληκτρολογήσει τον μυστικό κωδικό ασφαλείας της κάρτας PIN που δίνει πρόσβαση στον τραπεζικό λογαριασμό με τον οποίο είναι συνδεδεμένη. Το σύστημα POS είναι φυσικά συνδεδεμένο με την συνεργαζόμενη τράπεζα του εμπόρου, οπότε η πληρωμή αποτελεί καθαρά «έργο» της ελεγκτικής δύναμης της τράπεζας.

Οι πιστωτικές κάρτες τώρα[U2], δίνουν ένα φαινομενικό πλεονέκτημα στον καταναλωτή σε αντίθεση με τις χρεωστικές κάρτες. Ο κάτοχος της πιστωτικής κάρτας έχει την δυνατότητα, όπως αναφέρθηκε, να πραγματοποιήσει οποιαδήποτε αγορά και αν επιθυμεί χωρίς να κατέχει απαραίτητα το συνολικό ποσό που αντιστοιχεί στην εκάστοτε αγορά. Με αυτόν τον τρόπο, αποκτά το δικαίωμα της «πίστωσης» ώστε να καταβάλλει το ποσό μετά την πάροδο ορισμένων ημερών. Όταν ο καταναλωτής θελήσει να εκδώσει μία πιστωτική κάρτα απευθύνεται σε κάποια τράπεζα προκειμένου να αποδεχτεί το αίτημά του. Έπειτα, εφόσον το προφίλ του καταναλωτή είναι φερέγγυο η τράπεζα αποδέχεται την έκδοση πιστωτικής κάρτας στον συγκεκριμένο καταναλωτή δίνοντας του το λεγόμενο πιστωτικό όριο. Δηλαδή, ένα συνολικό ποσό που ανήκει καθαρά στην τράπεζα, σε αντίθεση με την χρεωστική κάρτα, το οποίο ο καταναλωτής μπορεί να το διαχειριστεί όπως εκείνος επιθυμεί. Μετά από ένα συγκεκριμένο χρονικό διάστημα, η τράπεζα αποστέλλει στον

καταναλωτή το συνολικό ποσό οφειλής προκειμένου να το καταβάλλει στην τράπεζα. Αυτή η διαδικασία επαναλαμβάνεται κάθε μήνα. Βέβαια, ορισμένα καταστήματα προσφέρουν την δυνατότητα της καταβολής των χρημάτων με άτοκες δόσεις. Αν ωστόσο, ο καταναλωτής δεν καταφέρει να καταβάλλει τελικά το απαιτούμενο ποσό στην τράπεζα, επιβαρύνεται με επιτόκιο γεγονός που αντισταθμίζει το πλεονέκτημα που φαινομενικά είχε σε σχέση με την χρεωστική κάρτα. Επίσης, ο κάτοχος της πιστωτικής κάρτας δεσμεύεται με ετήσια συνδρομή, μια δέσμευση η οποία δεν υπάρχει στην περίπτωση της χρεωστικής κάρτας.

Όσον αφορά την κάρτα από την πλευρά του αντικειμένου και όχι της χρήσης της, και οι δύο κάρτες έχουν την ίδια ακριβώς μορφή. Αποτελούνται[U1] από το όνομα του κατόχου στο κάτω αριστερό μέρος της κάρτας και την ημερομηνία λήξης της στο μπροστινό σημείο της. Επίσης, το μπροστινό μέρος της καλύπτεται από έναν μοναδικό 16ψήφιο κωδικό που αποτελεί το αναγνωριστικό της. Επιπλέον, είτε στο μπροστινό είτε στο πίσω μέρος της κάρτας αναλόγως τον εκδότη, υπάρχει ένας αριθμός τριψήφιος ή τετραψήφιος που αποτελεί το CVV της κάρτας. Στην ουσία αποτελεί τον κωδικό αριθμό ασφαλείας με τον οποίο ο έμπορος μπορεί να διαπιστώσει αφενός αν ο κάτοχος της κάρτας είναι και ο πλέον νόμιμος και αφετέρου αν ο λογαριασμός είναι έγκυρος. Το PIN ασφαλείας κάθε πιστωτικής ή χρεωστικής κάρτας που πληκτρολογείται στο σύστημα POS για την πραγμάτωση της συναλλαγής είναι απαραίτητο να διατηρείται μυστικός προκειμένου να αποφευχθεί η δυνατότητα σε κάποιον επιτιθέμενο να πραγματοποιήσει αγορές εκ μέρους του πραγματικού κατόχου.

Συμπερασματικά, τα πλεονεκτήματα που περιβάλλουν την χρήση της χρεωστικής κάρτας είναι περισσότερα από τα πλεονεκτήματα της χρήσης της πιστωτικής κάρτας. Με την χρεωστική κάρτα, ο καταναλωτής έχει την δυνατότητα να πραγματοποιεί τις αγορές του είτε από φυσικά είτε από Online καταστήματα μέσω διαδικτύου με ασφάλεια και σύνεση. Δεν δεσμεύεται με ετήσια συνδρομή ούτε με επιτόκιο πληρωμής, Επιπρόσθετα, η χρεωστική κάρτα προσφέρει την δυνατότητα της άμεσης κατοχής μετρητών μέσω του ATM τραπέζης. Επομένως, γενικότερα είναι άμεσο, ασφαλές και φιλικό προς τον καταναλωτή η χρήση χρεωστικών καρτών στις οικονομικές συναλλαγές έναντι των πιστωτικών καρτών οι οποίες δημιουργούν την ψευδαίσθηση της ικανότητας εκπλήρωσης οποιαδήποτε αγοράς χωρίς αντίτιμο.



Εικόνα 1: Συγκριτικό διάγραμμα συναλλαγών με χρήση μετρητών και καρτών. [A1]

Στο παραπάνω διάγραμμα (Εικόνα 1) απεικονίζεται μια συγκριτική μελέτη σχετικά με την επιλογή των καταναλωτών για το μέσο πληρωμής κατά την διάρκεια διεκπεραίωσης των συναλλαγών τους για το χρονικό διάστημα 2002-2016. Το πρώτο συμπέρασμα που προκύπτει από το διάγραμμα είναι ότι μέχρι και την χρονιά του 2012 η χρήση πιστωτικών ή χρεωστικών καρτών ως μέσο πληρωμής είχε μια σταθερή άνοδο χωρίς όμως να επηρεάσει την σταθερή αξία των μετρητών τα οποία από το 2009 μέχρι και το 2012 έχουν σημαντικά αυξημένη χρήση. Εκρηκτική θεωρείται η πρόοδος στην χρήση καρτών από το 2012 μέχρι και το 2015, ένα διάστημα στο οποίο τα ποσοστά χρήσης και των δύο μεθόδων είναι αρκετά κοντά. Η αλλαγή στην καταναλωτική συμπεριφορά των πολιτών είναι ραγδαία γεγονός που οδηγεί στην καταλυτική επικράτηση της χρήσης πιστωτικών ή χρεωστικών καρτών το 2016, μια χρονιά στην οποία για πρώτη φορά η γραμμή προτίμησης των καρτών ξεπερνά την γραμμή προτίμησης των μετρητών στο καταναλωτικό κοινό.

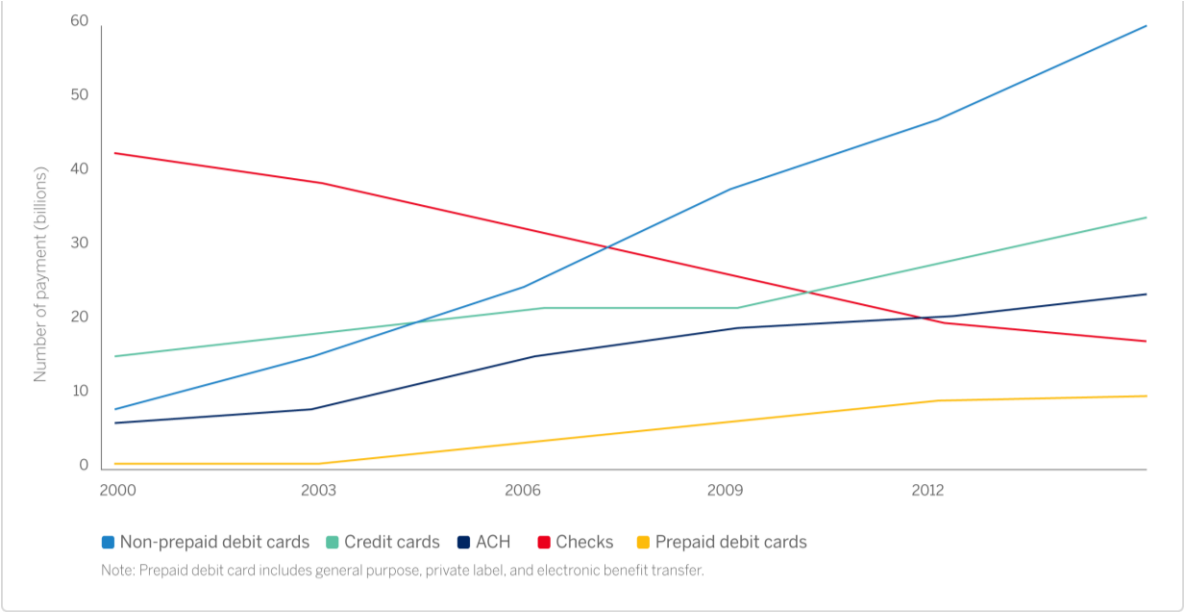
2.1.2 Προπληρωμένες κάρτες

Μια επέκταση της χρήσης των χρεωστικών καρτών αποτελούν οι λεγόμενες προπληρωμένες κάρτες. Μια προπληρωμένη κάρτα[U3] είναι στην ουσία μια κάρτα όπου ο κάτοχός της έχει καταβάλλει εξ'αρχής το ποσό το οποίο θα περιέχεται σε αυτήν χωρίς να υπάρχει σύνδεση με κάποιον άλλον ήδη υπάρχοντα λογαριασμό τραπέζης. Η χρήση τους στην σημερινή εποχή είναι ιδιαίτερα διαδεδομένη εξαιτίας των πλεονεκτημάτων που προσφέρουν στον μέσο καταναλωτή. Αρχικά, το γεγονός

ότι η προπληρωμένη κάρτα δεν συνδέεται με κάποιον ήδη υπάρχοντα καταθετικό τραπεζικό λογαριασμό, στον οποίο ο κάτοχος μπορεί να αποταμιεύει ένα σημαντικό ποσό, εξασφαλίζει την δυνατότητα της συνετής σπατάλης με τον απόλυτα ελεγχόμενο τρόπο διεκπεραίωσης κάθε αγοραπωλησίας. Ο καταναλωτής προβλέπει ένα συνολικό ποσό που θέλει να διαθέσει για την επίτευξη των αγορών του, το τοποθετεί στην κάρτα και όταν το ποσό αυτό εξαντληθεί ο καταναλωτής δεν μπορεί να συνεχίζει τις αγορές του και να ξοδεύει περισσότερα χρήματα από το αρχικά επιθυμητό ποσό. Επιπλέον, η προπληρωμένη κάρτα εξασφαλίζει και ασφάλεια των αγορών. Αν κάποιος επιτιθέμενος καταφέρει να αποσπάσει την κάρτα και φυσικά τον κωδικό PIN που απαιτείται για να έχει πρόσβαση στο ποσό της κάρτας, θα καταφέρει μόνο να σπαταλήσει το προστιθέμενο από τον νόμιμο κάτοχο ποσό το οποίο σίγουρα θα είναι αρκετά μικρότερο από την περίπτωση που είχε πρόσβαση σε κάποια άλλη πιστωτική ή χρεωστική κάρτα που συνδέεται με τραπεζικό λογαριασμό μισθοδοσίας ή κατάθεσης.

Μια ιδιαίτερη χρήση των προπληρωμένων καρτών είναι η διεκπεραίωση οικονομικών συναλλαγών μέσω του διαδικτύου. Τα πλεονεκτήματα που αναφέρθηκαν παραπάνω, σχετικά την ασφάλεια που προσδίδει στην προπληρωμένη κάρτα το γεγονός ότι ο καταναλωτής επιλέγει να καταθέσει σε αυτήν ένα μικρό ποσό για τις αγορές του, καθιστά την προπληρωμένη κάρτα ως τον ασφαλέστερο τρόπο πληρωμής για τις Online αγορές. Ο τρόπος με τον οποίο συνδέεται μια προπληρωμένη κάρτα με το Online κατάστημα είναι μέσω της πύλης ηλεκτρονικών πληρωμών PayPal[U18]. Η υπηρεσία PayPal διευκολύνει την μεταφορά χρημάτων μέσω του Internet. Ο χρήστης καλείται να δημιουργήσει έναν λογαριασμό στην πύλη PayPal και έπειτα να συνδέσει την κάρτα του με τον λογαριασμό αυτό. Όταν πραγματοποιήσει μια αγορά, το ποσό αφαιρείται από την κάρτα του καταναλωτή και μεταφέρεται στον λογαριασμό του εμπόρου εφόσον και αυτός διαθέτει σύνδεση στην πύλη PayPal. Η ασφάλεια στην πύλη PayPal επιτυγχάνεται με την διπλή προστασία των κωδικών όπου ο χρήστης καλείται να εισάγει εκτός από τον προσωπικό του username και password και ένα PayPal security key που εξασφαλίζει την αυθεντικότητά του.

Συνοπτικά, η χρήση της προπληρωμένης κάρτας δημιουργεί μια επανάσταση στον τομέα των ασφαλών και κυρίως συνετών οικονομικών συναλλαγών. Ο καταναλωτής ξοδεύει μόνο όσα χρειάζεται ενώ παράλληλα έχει επίγνωση των οικονομικών του εξόδων. Συγχρόνως, διευκολύνονται οι συναλλαγές μέσω διαδικτύου με την εύκολη μεταφορά χρημάτων στην πύλη PayPal.



Εικόνα 2: Συγκριτικό διάγραμμα των καταναλωτικών μεθόδων πληρωμής.[A2]

Στο παραπάνω διάγραμμα (Εικόνα 2) απεικονίζονται όλοι οι δυνατοί τρόποι πραγμάτωσης των οικονομικών συναλλαγών. Η γαλάζια γραμμή απεικονίζει την ραγδαία αύξηση της χρήσης των χρεωστικών καρτών που όπως αναφέρθηκε αποτελεί έναν ασφαλέστερο τρόπο πληρωμής σε σχέση με τις πιστωτικές κάρτες. Μετά το 2003, η χρήση χρεωστικών καρτών επικρατεί θριαμβευτικά σε σύγκριση με την χρήση πιστωτικών καρτών (πράσινη γραμμή). Η κίτρινη γραμμή απεικονίζει την χρήση των προπληρωμένων καρτών. Όπως διακρίνεται, μέχρι την χρονιά του 2012 μπορεί να μην αποτελεί τον πιο διαδεδομένο τρόπο πληρωμής ωστόσο η αύξηση στην χρήση της είναι σχεδόν εκθετική.

2.2 Λειτουργία πιστωτικών καρτών

Μια πιστωτική κάρτα μπορεί να χρησιμοποιηθεί είτε για μια παραδοσιακή Off-line διαδικασία πληρωμής αλλά μπορεί να αξιοποιηθεί και σε μία On-line διαδικασία πληρωμής μέσω διαδικτύου. Η διαδικασία που ακολουθείται είναι διαφορετική ανάμεσα στις δύο περιπτώσεις και ο έλεγχος ασφάλειας διαδραματίζει καθοριστικό ρόλο ιδιαίτερα στην περίπτωση που η συναλλαγή διεκπεραιώνεται μέσω του διαδικτύου καθώς οι επιθέσεις είναι αυξημένες. Σε μία Off-line διαδικασία πληρωμής απαιτείται η φυσική παρουσία του κατόχου της κάρτας στο φυσικό κατάστημα ενώ σε μία On-line διαδικασία πληρωμής, το λεγόμενο Ηλεκτρονικό εμπόριο[Δ3], η διαδικασία πληρωμής διεκπεραιώνεται εξ αποστάσεως μεταξύ εμπόρου και καταναλωτή.

2.2.1 Παραδοσιακή Off-line πληρωμή

Μια Off-line[Δ3] διαδικασία πληρωμής αποτελεί μια παραδοσιακή διαδικασία πληρωμής με την διαφορά ότι ο πελάτης δεν πληρώνει με μετρητά αλλά με πίστωση. Όταν ο καταναλωτής ολοκληρώσει την επιθυμητή του αγορά, στο ταμείο ακολουθείται η εξής διαδικασία:

- Ο καταναλωτής υπογράφει ένα έγγραφο συναλλαγής με τα στοιχεία της πιστωτικής του κάρτας και το παραδίδει στον έμπορο του καταστήματος.
- Το υπογεγραμμένο έγγραφο προωθείται στην τράπεζα προκειμένου να εξεταστούν τα στοιχεία της πιστωτικής κάρτας και να γνωστοποιηθεί η εγκυρότητα της πληρωμής.
- Η τράπεζα εφόσον γνωστοποιήσει την εγκυρότητα της πληρωμής τοποθετεί το συνολικό ποσό της αγοράς στο πιστωτικό υπόλοιπο του καταναλωτή.
- Έμπορος και καταναλωτής ενημερώνονται για την ολοκλήρωση της συναλλαγής.

2.2.2 Ηλεκτρονική On-line πληρωμή

Μια διαδικασία πληρωμής μέσω διαδικτύου με χρήση πιστωτικών καρτών ανήκει στην κατηγορία μίας ηλεκτρονικής συναλλαγής. Ο τρόπος και η φιλοσοφία διεκπεραίωσης της διαδικτυακής πληρωμής είναι ανάλογος με τον παραδοσιακό τρόπο της Off-line πληρωμής με την διαφορά ότι προστίθενται επιπλέον διαδικασίες που εξασφαλίζουν την ασφάλεια και την εγκυρότητα των συναλλαγών σε ένα χώρο ελεύθερα προσβάσιμο και επομένως ευάλωτο σε επιθέσεις υποκλοπής των προσωπικών στοιχείων κάθε καταναλωτή. Στόχος μιας ηλεκτρονικής συναλλαγής είναι να προσφέρει την εμπιστοσύνη στην επικοινωνία μεταξύ των οντοτήτων που ανταλλάσσουν πληροφορίες. Επομένως κρίνεται απαραίτητο να εξασφαλίζεται:

- Η ταυτοποίηση του αγοραστή και του πωλητή.
- Η εμπιστευτική μετάδοση δεδομένων πληρωμής.

Η πρώτη απαίτηση εξασφαλίζεται μέσω της ***Διαδικασίας Αγοράς*** ενώ η δεύτερη απαίτηση μέσω της ***Διαδικασίας Πληρωμής***[Δ10].

- **Διαδικασία Αγοράς**

Η διαδικασία αγοράς σε μία ηλεκτρονική συναλλαγή αποτελεί το πρώτο βήμα της συναλλαγής στο οποίο ο καταναλωτής πραγματοποιεί έρευνα αγοράς στο On-line κατάστημα της επιλογής του και έπειτα από την ολοκλήρωση της απόφασης αγοράς μεταβαίνει στο αντίστοιχο πεδίο που ορίζει το κατάστημα για την ολοκλήρωση της παραγγελίας του. Κατά την διαδικασία της παραγγελίας ο καταναλωτής θα δηλώσει επίσημα τόσο τα επιθυμητά προϊόντα της αγοράς του όσο και τα προσωπικά στοιχεία με τα οποία θα πραγματοποιήσει την πληρωμή στο κατάστημα. Αυτά τα στοιχεία θα ελεγχθούν λεπτομερώς προκειμένου να εξακριβωθεί η εγκυρότητά τους και να ταυτοποιηθεί ο αγοραστής. Η ίδια διαδικασία ταυτοποίησης ακολουθείται και για τον πωλητή προκειμένου να αναγνωριστεί και η δική του εγκυρότητα με σκοπό η συναλλαγή να επιτευχθεί κάτω από έγκυρες βάσεις. Η Διαδικασία Αγοράς περιλαμβάνει τα ακόλουθα 4 βήματα:

1. Αρχική Αίτηση
2. Απάντηση Αιτήματος
3. Αίτημα Αγοράς
4. Απάντηση στο Αίτημα Αγοράς

1. **Διαδικασία Αγοράς: Αρχική Αίτηση**

Κατά την έκδοση μιας πιστωτικής κάρτας, ο κάτοχος λαμβάνει όλα τα απαραίτητα πιστοποιητικά που εξακριβώνουν την εγκυρότητα της ταυτότητάς του και της κατοχής της κάρτας του. Η αρχική λοιπόν απαίτηση του αγοραστή κατά την διαδικασία της παραγγελίας είναι να λάβει όλα τα απαραίτητα αντίγραφα των πιστοποιητικών του εμπόρου και της πύλης πληρωμής προκειμένου να επιβεβαιώσει την ταυτότητα του προσώπου με τον οποίο θα ανταλλάξει προσωπικά του στοιχεία. Μέρος αυτής της αίτησης είναι ο τύπος της πιστωτικής κάρτας του εμπόρου, η ταυτότητα του εμπόρου καθώς και ένας μοναδικός αριθμός, ο λεγόμενος nonce, που είναι μοναδικός αριθμός σε κάθε επικοινωνία αγοράς.

2. **Διαδικασία Αγοράς: Απάντηση αιτήματος**

Ο έμπορος τώρα οφείλει να ανταποκριθεί στο αίτημα του αγοραστή και να στείλει τα απαραίτητα έγγραφα πιστοποίησης. Η απάντηση του εμπόρου περιλαμβάνει τον αριθμό nonce του πελάτη, τον αριθμό nonce του ίδιου καθώς και το

αναγνωριστικό της συναλλαγής για την αγορά. Υπογράφει την απάντησή του με το ιδιωτικό κλειδί του και την αποστέλλει στον αγοραστή. Επιπλέον στην απάντηση του εμπόρου περιλαμβάνεται το πιστοποιητικό της υπογραφή του ίδιου, για την γνησιότητα της ταυτότητάς του, καθώς και το πιστοποιητικό της ανταλλαγής κλειδιών της πύλης πληρωμών του.

3. Διαδικασία Αγοράς: Αίτημα αγοράς

Ο αγοραστής αφού λάβει την απάντηση του εμπόρου στο αίτημα εκκίνησης αγοράς είναι σε θέση να επαληθεύσει τα δύο πιστοποιητικά που έλαβε χρησιμοποιώντας την αρχή έκδοσης του πιστοποιητικού. Έπειτα, εφόσον τις επαληθεύσει δημιουργεί τις πληροφορίες σχετικά με την επιθυμητή παραγγελία που θέλει να κάνει η οποία φυσικά περιλαμβάνει και τις πληροφορίες πληρωμής. Στον έμπορο λοιπόν, πρόκειται να σταλεί μια αίτηση που θα περιλαμβάνει τις πληροφορίες που σχετίζονται με την αγορά, πληροφορίες σχετικές με την παραγγελία καθώς και το πιστοποιητικό που αφορά τον ίδιο. Οι πληροφορίες στέλνονται στον έμπορο μαζί με ένα μοναδικό συμμετρικό κλειδί κρυπτογράφησης της μεταξύ τους επικοινωνίας.

4. Διαδικασία Αγοράς: Απάντηση αιτήματος αγοράς

Ο έμπορος τώρα λαμβάνει ένα δεύτερο αίτημα από τον αγοραστή στο οποίο αρχικά οφείλει να επιβεβαιώσει την εγκυρότητα των δύο πιστοποιητικών που έλαβε από τον αγοραστή και έπειτα να επαληθεύσει την εγκυρότητα της διπλής υπογραφής του αγοραστή. Η αναγνώριση της πιστοποίησης της διπλής υπογραφής θα γίνει με βάση το δημόσιο κλειδί του πελάτη. Εφόσον οι ενέργειες αυτές αποδειχθούν έγκυρες ακολουθεί η επεξεργασία της παραγγελίας του πελάτη. Στην παραγγελία περιλαμβανόταν και η πληροφορία πληρωμής. Οπότε ο έμπορος στέλνει τα στοιχεία πληρωμής στην πύλη πληρωμής για να λάβει την έγκριση πληρωμής. Τέλος, συγκεντρώνει όλα τα απαραίτητα στοιχεία, υπογράφει με το ιδιωτικό του κλειδί και τα αποστέλλει στον αγοραστή μαζί με το πιστοποιητικό εγκυρότητας της υπογραφής του για να είναι σε θέση να την επαληθεύσει.

Όταν παραλάβει τα στοιχεία ο πελάτης θα επαληθεύσει το πιστοποιητικό του εμπόρου, και την υπογραφή του στο μήνυμα και έπειτα θα ολοκληρωθεί η διαδικασία αγοράς.

- **<u>Διαδικασία Πληρωμής</u>**

Μετά την ολοκλήρωση της Διαδικασίας Αγοράς ακολουθεί η Διαδικασία Πληρωμής προκειμένου να επιβεβαιωθεί η ασφάλεια των δεδομένων που θα μεταδοθούν στην διαδικασία της πληρωμής. Αυτή η διαδικασία περιλαμβάνει συνολικά 2 στάδια:

1. Έγκριση Πληρωμής
2. Καταβολή Πληρωμής

1. <u>Διαδικασία Πληρωμής: Έγκριση Πληρωμής</u>

Για να γίνει δεκτή μια αίτηση πληρωμής θα πρέπει να δοθεί η κατάλληλη άδεια από την πύλη πληρωμής. Για τον λόγο αυτό, ο έμπορος στέλνει ειδικό μήνυμα αίτησης λήψης άδειας στην πύλη πληρωμής με συγκεκριμένες πληροφορίες. Αρχικά αποστέλλει ένα σύνολο πληροφοριών σχετικά με τις πληροφορίες του, το ποσό της πληρωμής, τη διπλή υπογραφή του πελάτη που προκύπτει από τις πληροφορίες παραγγελίας και πληρωμής που έστειλε ο αγοραστής στον έμπορο και είναι υπογεγραμμένες με το ιδιωτικό μοναδικό του κλειδί, την σύνοψη των πληροφοριών παραγγελίας που διαθέτει ο έμπορος καθώς και τον ψηφιακό φάκελο. Έπειτα ακολουθούν οι πληροφορίες που σχετίζονται με την άδεια και περιλαμβάνουν το μοναδικό ID της συναλλαγής υπογεγραμμένο και αυτό με το ιδιωτικό κλειδί του εμπόρου και κρυπτογραφημένο με το συμμετρικό κλειδί που απέστειλε ο αγοραστής στον έμπορο στην Διαδικασία Αγοράς στο 3^{ο} βήμα Αίτημα Αγοράς καθώς και τα απαραίτητα πιστοποιητικά με το κλειδί της υπογραφής του κατόχου της πιστωτικής κάρτας δηλαδή του αγοραστή, το πιστοποιητικό για το κλειδί του εμπόρου, καθώς και πιστοποιητικό για το κλειδί ανταλλαγής πληροφορίας μεταξύ εμπόρου και καταναλωτή.

2. <u>Διαδικασία Πληρωμής: Καταβολή Πληρωμής</u>

Στο στάδιο αυτό επιτελούνται όλες οι απαραίτητες ενέργειες για την επαλήθευση της εγκυρότητας των πιστοποιητικών και την έγκριση λήψης άδειας πληρωμής. Συγκεκριμένα, επιβεβαιώνεται η εγκυρότητα όλων των πιστοποιητικών που ελήφθησαν και αποκρυπτογραφείται ο ψηφιακός φάκελος που στάλθηκε με αποτέλεσμα να υπάρχει πλήρη πρόσβαση στο συμμετρικό κλειδί που θα βοηθήσει στην αποκρυπτογράφηση του συμπεριλαμβανόμενου μηνύματος. Επίσης, επιβεβαιώνεται η υπογραφή του εμπόρου ενώ παράλληλα αποκρυπτογραφούνται τα

στοιχεία πληρωμής που περιλαμβάνονταν στον ψηφιακό φάκελο. Επαληθεύεται η διπλή υπογραφή καθώς και το αναγνωριστικό της συναλλαγής που έλαβε η πύλη από τον έμπορο με σκοπό να συγκριθεί με το αναγνωριστικό που έλαβε από τον πελάτη. Εάν αυτά συμφωνούν, τότε η πύλη στέλνει αίτηση εξουσιοδότησης από τον εκδότη της πιστωτικής κάρτας με σκοπό να ολοκληρώσει την διαδικασία πληρωμής.

Όλη η παραπάνω διαδικασία που περιγράφηκε, ακολουθείται προκειμένου να είναι εφικτή η διεκπεραίωση μιας ασφαλής οικονομικής συναλλαγής μέσω διαδικτύου. Ο τρόπος λειτουργίας της είναι μια επέκταση του παραδοσιακού τρόπου πληρωμής με πιστωτική κάρτα με την κύρια διαφορά, αφενός της ύπαρξης πιστοποιητικών και ειδικών κλειδιών κρυπτογράφησης με σκοπό την επίτευξη ασφάλειας, και αφετέρου την ύπαρξη της πύλης πληρωμής που διασυνδέει τα δίκτυα του Internet με τα δίκτυα των ιδιωτικών τραπεζών.

2.3 Ψηφιακές Υπογραφές

Η μελέτη της λειτουργίας των πιστωτικών καρτών επικεντρώνεται ιδιαίτερα σε δύο βασικούς τομείς προκειμένου να επιτευχθεί η διαδικασία ασφαλούς επικοινωνίας μεταξύ εμπόρου και αγοραστή. Στην εφαρμογή των ψηφιακών υπογραφών και στην ανταλλαγή των πιστοποιητικών. Το διαδίκτυο αποτελεί μια αποκεντρωμένη πλατφόρμα ελεύθερα προσβάσιμη γεγονός που ενισχύει την επικινδυνότητα της επικοινωνίας. Οι ψηφιακές υπογραφές[Δ2][Δ3], το πρώτο σκέλος διασφάλισης ασφαλούς επικοινωνίας, αποτελούν το ηλεκτρονικό «υποκατάστατο» της πραγματικής γνήσιας υπογραφής που ως στόχο έχει την απόδειξη της γνησιότητας της ταυτότητας του προσώπου που επικοινωνεί. Σε οποιαδήποτε διαδικτυακή επικοινωνία και ιδιαίτερα στην ανταλλαγή πληροφοριών που σχετίζονται με τα προσωπικά απόρρητα στοιχεία των χρηστών κρίνεται απαραίτητη η εφαρμογή των ψηφιακών υπογραφών για την προστασία της πιθανούς υποκλοπής των στοιχείων τους. Για το λόγο αυτό, έχουν αναπτυχθεί κατάλληλα πρωτόκολλα υποστήριξης της εφαρμογής των ψηφιακών υπογραφών με σκοπό να πιστοποιηθεί και τεχνολογικά η προστασία των επικοινωνιών με απώτερο σκοπό την ενθάρρυνση διεξαγωγής ολοένα και περισσότερων ηλεκτρονικών συναλλαγών.

2.3.1 Πρωτόκολλα

Η ασφαλής και πιστοποιημένη επικοινωνία μεταξύ των εξουσιοδοτημένων οντοτήτων, που στοχεύουν στην ανταλλαγή πληροφοριών, θέτει ως βασικό στόχο την πραγματοποίηση τριών δομημένων βημάτων:

- την παραγωγή των κλειδιών για κάθε οντότητα
- την εγκυροποίησή τους με την ψηφιακή υπογραφή και
- την διανομή τους μεταξύ των οντοτήτων που επικοινωνούν.

Η έννοια «κλειδί» αποτελεί στην ουσία έναν «κωδικό» που είναι ξεχωριστός αφενός για κάθε οντότητα και αφετέρου για κάθε διαδικασία επικοινωνίας. Η μοναδική «ταυτότητα», που απαιτείται για την αναγνώριση μιας οντότητας ως αξιόπιστης για επικοινωνία, προϋποθέτει την αυθεντικοποίηση της γνησιότητας του κλειδιού που έχει παραχθεί. Αυτό επιτυγχάνεται με την ψηφιακή υπογραφή.

Τέλος, αναπόσπαστο κομμάτι της ολοκλήρωσης της ηλεκτρονικής συναλλαγής αποτελεί η ανταλλαγή κλειδιών μεταξύ εμπόρου και καταναλωτή και η δημιουργία αντιγράφων των κλειδιών. Επομένως, ο τομέας της τεχνολογικής ασφάλειας των ηλεκτρονικών συναλλαγών οφείλει να εφαρμοστεί στην σωστή παραγωγή κλειδιών, στην πιστοποίηση της αυθεντικότητάς τους και στην μεταβίβαση τους ανάμεσα στις εξουσιοδοτημένες οντότητες. Άμεσο επακόλουθο των παραπάνω αποτελεί η δυνατότητα αναγνώρισης οποιασδήποτε παραμόρφωσης που μπορεί να επιτευχθεί στο μεταδιδόμενο μήνυμα ή κλειδί.

<u>Παραγωγή κλειδιών</u>

Το κλειδί, που αποτελεί τον προσωπικό κωδικό μιας οντότητας δεν μπορεί να είναι εύκολα προβλέψιμο από οποιονδήποτε επιτιθέμενο. Για τον λόγο αυτό, αποφεύγονται κλειδιά που μπορεί να παραπέμπουν σε αριθμούς τηλεφώνου, ημερομηνία γεννήσεων, όνομα ή επίθετο ακόμα και σε γεννήτριες τυχαίων αριθμών διότι παρουσιάζουν χαρακτηριστικά συναφή με διαφορετικές κατηγορίες γεννητριών. Σκοπός αποτελεί η εξασφάλιση της τυχαιότητας. Η «μέθοδος του ζαριού» ή η «μέθοδος του νομίσματος» είναι δύο βασικές μέθοδοι παραγωγής κλειδιού που βασίζονται στην τυχαιότητα ρίψης του νομίσματος ή του ζαριού. Έτσι, επιλέγεται ένας επιθυμητός αριθμός ρίψεων και ανάλογα με τον συνδυασμό που προκύπτει κάθε φορά δημιουργείται και ένα κλειδί βασιζόμενο στο δυαδικό σύστημα που ως γνωστών λαμβάνει δύο τιμές 0 και 1 όπως δύο είναι και οι πιθανές τιμές κατά την ρίψη του νομίσματος ή του ζαριού (κορώνα - γράμματα, ζυγά - μονά).

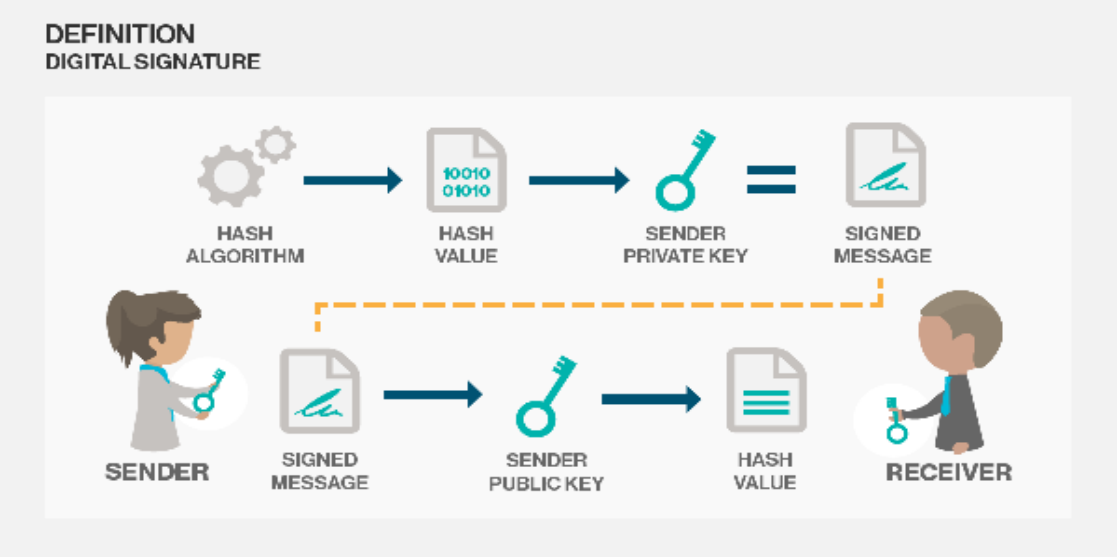
Αυθεντικότητα κλειδιού

Εφόσον έχει ολοκληρωθεί η διαδικασία παραγωγής κλειδιού, ακολουθεί η διαδικασία αυθεντικοποίησής του με τρόπο μοναδικό για κάθε οντότητα. Η ψηφιακή υπογραφή αποτελεί το μέσο διεκπεραίωσης της αυθεντικότητας. Ο χρήστης «υπογράφει» με την μοναδική του «ταυτότητα» το μεταδιδόμενο μήνυμα με σκοπό ο επιτιθέμενος να μην είναι σε θέση να το τροποποιήσει καθώς δεν θα γνωρίζει το προσωπικό κλειδί του αποστολέα. Ένας βασικός αλγόριθμος που λειτουργεί ως ψηφιακή υπογραφή είναι το πρωτόκολλο RSA[Δ7].

Ο αλγόριθμος RSA[Δ8][B1] ακολουθεί την εξής βασική λογική της κρυπτογραφίας δημοσίου κλειδιού: Κάθε οντότητα που συμμετέχει στην επικοινωνία έχει ένα μοναδικό κλειδί ,το οποίο είναι ιδιωτικό και προσβάσιμο αποκλειστικά και μόνο από την οντότητα που το δημιουργεί, καθώς και ένα δημόσιο κλειδί που είναι προσπελάσιμο από τον οποιοδήποτε ακόμα και επιτιθέμενο. Η οντότητα θα «υπογράψει» το μήνυμα που θέλει να μεταδώσει με βάση το ιδιωτικό κλειδί της και έπειτα θα το αποστείλει στον παραλήπτη. Ο παραλήπτης θα μπορέσει να το αποκρυπτογραφήσει με βάση το δημόσιο κλειδί του αποστολέα. Έτσι, αν ο αποστολέας είναι ο πλέον νόμιμος, ο παραλήπτης θα μπορέσει να το αποκρυπτογραφήσει διότι θα έχει υπογραφεί με το ιδιωτικό κλειδί του αποστολέα, αλλιώς θα αντιληφθεί την τροποποίηση του προσώπου του αποστολέα. Έτσι μπορεί ένας επιτιθέμενος να έχει πρόσβαση στο μεταδιδόμενο μήνυμα αλλά θα μπορεί να πιστοποιήσει τον πραγματικό αποστολέα του μηνύματος. Δηλαδή, προσοχή πρέπει να δοθεί στο γεγονός ότι η ψηφιακή υπογραφή δεν προστατεύει το «απόρρητο» του μηνύματος με σκοπό να αποτραπεί η κλοπή του αλλά διαβεβαιώνει τον παραλήπτη σχετικά με το «ποιος» έστειλε το μήνυμα.

Σημαντικό κομμάτι αποτελεί και η χρήση της συνάρτησης κατακερματισμού, hash[Δ8][B1]. Η συνάρτηση κατακερματισμού εφαρμόζεται στο μεταδιδόμενο μήνυμα και όχι στο κλειδί. Έπειτα, ο αποστολέας «υπογράφει» το κατακερματισμένο μήνυμα και το αποστέλλει στον παραλήπτη, ο οποίος αποκρυπτογραφεί με βάση το δημόσιο κλειδί του αποστολέα το κατακερματισμένο μήνυμα και όχι το απλό. Με την συνάρτηση κατακερματισμού προστατεύεται το ίδιο το μήνυμα με απώτερο σκοπό να αποφευχθεί ο επιτιθέμενος, που θα έχει πρόσβαση στο μήνυμα να το αποκρυπτογραφήσει αυτούσιο. Αυτό επιτυγχάνεται εξαιτίας της φύσης της συνάρτησης κατακερματισμού η οποία είναι μη αντιστρέψιμη. Δηλαδή δεδομένου ενός μηνύματος m με συνάρτηση κατακερματισμού h(m) δεν μπορεί να βρεθεί

μήνυμα m’ που θα έχει συνάρτηση κατακερματισμού ίση με hash(m). Άρα, αν m ≠m’ => hash(m) ≠ hash(m’).



Εικόνα 3: Ψηφιακή Υπογραφή στην Κρυπτογράφηση και Αποκρυπτογράφηση.[A3]

Σύμφωνα λοιπόν με την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης όπως παρουσιάζεται στην παραπάνω εικόνα (Εικόνα 3), ο αποστολέας στέλνει διπλό μήνυμα στον παραλήπτη με το μήνυμα και το υπογεγραμμένο κατακερματισμένο μήνυμα (m,S(h(m))). Ο παραλήπτης λαμβάνει το διπλό μήνυμα και αξιοποιεί το δημόσιο κλειδί του αποστολέα προκειμένου να αποκρυπτογραφήσει το υπογεγραμμένο μήνυμα. Όταν το επιτύχει έχει πρόσβαση στο κατακερματισμένο μήνυμα. Συγκρίνει το κατακερματισμένο μήνυμα που προέκυψε από την αποκρυπτογράφηση με το κατακερματισμένο μήνυμα που δημιουργεί δεδομένου του m. Αν υπάρχει ταύτιση τότε είναι έγκυρη η αυθεντικότητα αλλιώς απορρίπτεται.

Γενικότερα, η υπογραφή ενός μηνύματος προκύπτει ως:

- **Κρυπτογράφηση**: $S= HASH(m)^d mod n$, με d το ιδιωτικό κλειδί του αποστολέα.
- **Αποκρυπτογράφηση**: $HASH(m)= S^e mod n$ με e το δημόσιο κλειδί του αποστολέα.

2.3.2 Σύστημα Kerberos

Άμεσο επακόλουθο της παραγωγής κλειδιών και της εξασφάλισης της αυθεντικότητάς τους μέσω της ψηφιακής υπογραφής είναι η διανομή των κλειδιών μεταξύ των εξουσιοδοτημένων οντοτήτων που πραγματοποιούν μια ηλεκτρονική συναλλαγή. Από την στιγμή λοιπόν που τίθεται το ζήτημα της διανομής κλειδιών στον κυβερνοχώρο, ενισχύεται η αναγκαιότητα προστασίας και φυσικά εμπιστοσύνης μεταξύ των επικοινωνούντων οντοτήτων. Επομένως, ενισχύεται η αναγκαιότητα της αυθεντικότητας των οντοτήτων. Ένα από τα πλέον γνωστά συστήματα διασφάλισης της αυθεντικότητας κάθε εξουδιοτοδημένης οντότητας είναι το σύστημα Kerberos[U4][B1][Δ3],το οποίο σχεδιάστηκε πρώτη φορά στο MIT και αποτελεί μέρος της δομής των Windows για την αυθεντικοποίηση των χρηστών.

Το σύστημα Kerberos είναι μια έμπιστη υπηρεσία πιστοποίησης, στην οποία κάθε εξυπηρετούμενος εμπιστεύεται την κρίση του Κέρβερου προκειμένου να ελέγξει την ταυτότητα των συμμετεχόντων. Κάθε μεμονωμένη οντότητα που συμμετέχει στο σύστημα Kerberos αναπαρίσταται με μια τριάδα στοιχείων.

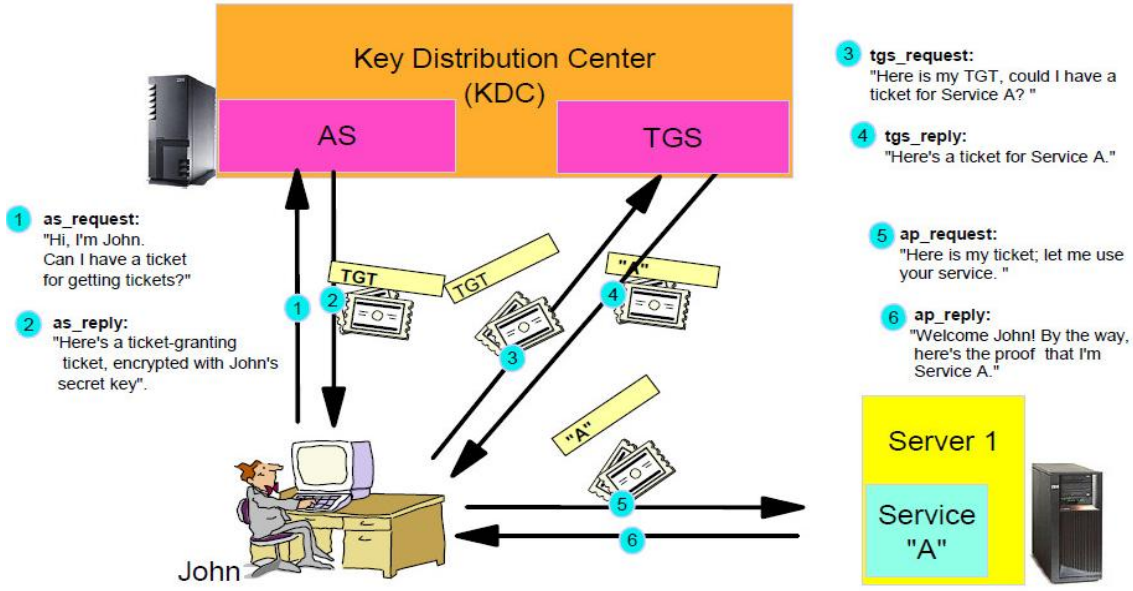
- Το αναγνωριστικό του χρήστη: αποτελεί το όνομα του χρήστη ή της υπηρεσίας.
- Το στιγμιότυπο: χρησιμεύει για να διαχωρίζει τις διαφοροποιήσεις του αναγνωριστικού του χρήστη, δηλαδή του πρωτεύοντος ονόματος. Για τους μεμονωμένους χρήστες το στιγμιότυπο μπορεί να αναφέρεται σε ειδικά χαρακτηριστικά ή δικαιώματα του χρήστη όπως την διαφοροποίηση ανάμεσα σε root και admin. Για κάποια υπηρεσία το στιγμιότυπο αναφέρεται πιθανόν στην μηχανή στην οποία τρέχει ο εξυπηρετητής.
- Το realm: αναφέρεται στο όνομα της οντότητας διαχειριστής που διατηρεί τα δεδομένα πιστοποίησης.

Κάθε χρήστης εισέρχεται στο σύστημα χρησιμοποιώντας το δικό του password το οποίο είναι απόρρητο. Αυτό το κλειδί λειτουργεί ως αφετηρία για την μετέπειτα παραγωγή άλλων βασικών κλειδιών. Από το Password παράγεται αρχικά το ιδιωτικό κλειδί που είναι γνωστό μόνο στον συγκεκριμένο χρήστη και το σύστημα Kerberos. Το σύστημα διατηρεί μια μεγάλη βάση δεδομένων στην οποία έχει καταχωρημένους όλους τους πελάτες μαζί με τα ιδιωτικά τους κλειδιά. Όταν μια υπηρεσία εγγράφεται στο σύστημα Kerberos προκειμένου να πιστοποιήσει την αυθεντικότητά της οφείλει να καταχωρήσει όλους τους πελάτες της μαζί με τα ιδιωτικά τους κλειδιά που διαμορφώνονται ανάλογα κατά την καταχώρηση.

Το σύστημα Kerberos διατηρεί τρία διαφορετικά επίπεδα προστασίας, όπου ανάλογα με τις απαιτήσεις του προγραμματιστή της εκάστοτε εφαρμογής επιλέγει το πλέον κατάλληλο.

- Πιστοποίηση κατά την έναρξη σύνδεσης.
- Πιστοποίηση σε κάθε μήνυμα.
- Πιστοποίηση σε κάθε μήνυμα και επιπλέον κρυπτογράφηση του μηνύματος.

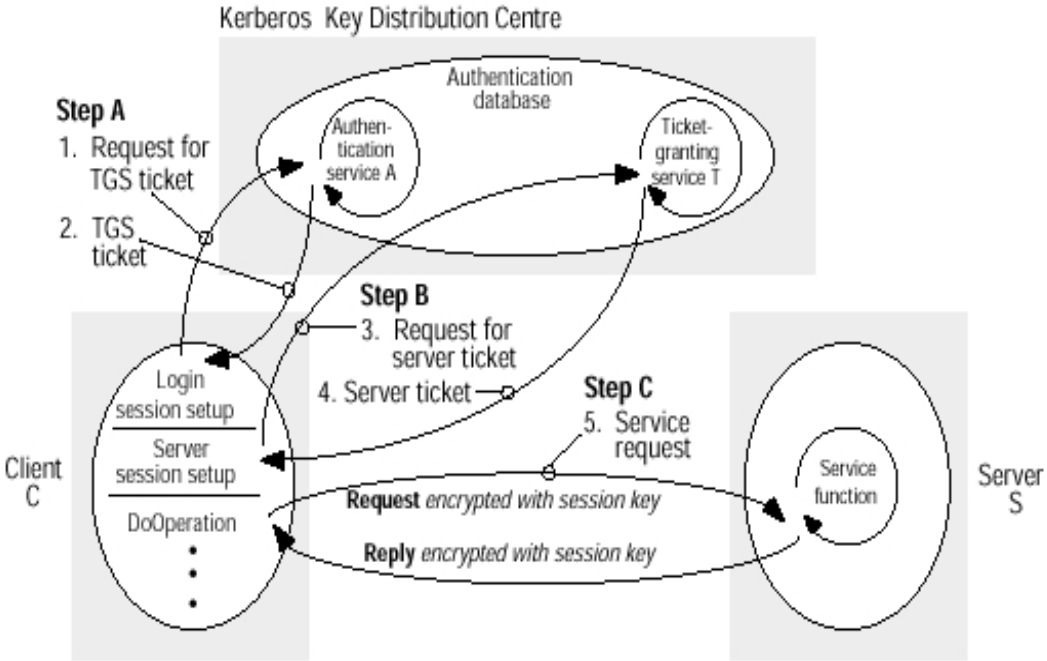
Στην λειτουργία του συστήματος Kerberos περιλαμβάνεται και η έκδοση διαπιστευτηρίων προκειμένου να υλοποιηθεί όλη η ενδιάμεση επικοινωνία. Υπάρχουν δύο βασικά είδη διαπιστευτηρίων, τα **εισιτήρια** και οι **πιστοποιητές**. Το εισιτήριο χρησιμοποιείται για να περάσει τη ταυτότητα κάποιου χρήστη από τον εξυπηρέτη πιστοποίησης στον εξυπηρέτη εφαρμογής ενώ ο πιστοποιητής περιλαμβάνει πρόσθετες πληροφορίες που επιβεβαιώνουν ότι ο χρήστης του εισιτηρίου είναι αυτός για τον οποίο εκδόθηκε.



Εικόνα 4:Λειτουργία συστήματος Kerberos από την οπτική του χρήστη.[A4]

Στην παραπάνω εικόνα (Εικόνα 4) διακρίνεται σχηματικά η λειτουργία του συστήματος Kerberos από την οπτική γωνία του χρήστη. Συνοπτικά και περιγραφικά λοιπόν, ο χρήστης που έχει προηγουμένως εγγραφεί στο σύστημα πιστοποίησης Kerberos απευθύνεται με το όνομα του, το λεγόμενο username(John), στο AS Center, δηλαδή στον εξυπηρέτη πιστοποίησης ζητώντας του το εισιτήριο που είναι αναγκαίο για να έχει πρόσβαση στις υπηρεσίες. Αυτό το εισιτήριο θα αποτελέσει την πηγή

παραγωγής άλλων εισιτηρίων πρόσβασης σε διαφορετικές υπηρεσίες. Δηλαδή με αυτό το εισιτήριο θα παράγονται άλλα νέα εισιτήρια, κάθε φορά που ο χρήστης απευθύνεται στον εξυπηρέτη έκδοσης εισιτηρίων για πρόσβαση σε κάποια νέα υπηρεσία του Server. Ο Authentication Server, AS, αναγνωρίζει την εγκυρότητα του χρήστη και εκδίδει το εισιτήριο το οποίο και αποστέλλει ,κρυπτογραφημένο βέβαια με το ιδιωτικό κλειδί του χρήστη που έχει προκύψει από το Password εισόδου του στο σύστημα. Στο σημείο αυτό, βήμα 3 στην παραπάνω εικόνα, ο χρήστη δεδομένου του εισιτηρίου που διαθέτει απευθύνεται στον εξυπηρέτη έκδοσης εισιτηρίων TGS, ζητώντας του εισιτήριο για να αποκτήσει πρόσβαση στην υπηρεσία A. Όπως αναφέρθηκε και προηγουμένως, τα εισιτήρια πρόσβασης στις διάφορες υπηρεσίες προέρχονται από το βασικό εισιτήριο εγκυρότητας που εξέδωσε ο AS στον χρήστη. Ο TGS εγκρίνει στο βήμα 4 την άδεια έκδοσης εισιτηρίου και την αποστέλλει στον χρήστη. Μετά την έγκριση, ο χρήστης μπορεί να έχει πρόσβαση στην υπηρεσία A για την οποία ζήτησε το εισιτήριο. Απευθύνεται λοιπόν στον Service Provider με το εισιτήριό του προκειμένου να του εγκρίνει την τελική πρόσβαση. Στο τελευταίο βήμα ο Service Provider ελέγχει το εισιτήριο του χρήστη και του εγκρίνει την πρόσβαση στην υπηρεσία A. Ταυτόχρονα βέβαια του αποστέλλει και την βεβαίωση της υπηρεσίας στην οποία αποκτά πρόσβαση. Έτσι ολοκληρώνεται η διαδικασία πιστοποίησης και ελέγχου μέσω του συστήματος Kerberos, από την εξωτερική οπτική του χρήστη.



Εικόνα 5: Λειτουργία συστήματος Kerberos από την οπτική του συστήματος.[A7]

Προηγουμένως, περιγράφηκε η διαδικασία λειτουργίας του συστήματος Kerberos από την εξωτερική οπτική του χρήστη. Σκοπός τώρα είναι να περιγραφεί η διαδικασία και εσωτερικά, από την πλευρά δηλαδή των λειτουργιών του συστήματος. Η λειτουργία του συστήματος Kerberos (Εικόνα 5) βασίζεται στο κέντρο KDC (Key Distribution Center) το οποίο διαχωρίζεται στο AS (Authentication Server) και TGS κέντρο (Ticket Granting Server). Στην ουσία τα δύο κέντρα AS και TGS υλοποιούν τα δύο διαπιστευτήρια των εισιτηρίων και των πιστοποιητών αντίστοιχα.

Ένα εισιτήριο περιέχει:

- το Όνομα εξυπηρέτη & εξυπηρετούμενου
- την IP διεύθυνση εξυπηρετούμενου
- μια χρονοσφραγίδα
- το χρόνο ζωής εισιτηρίου
- ένα τυχαίο κλειδί συνόδου

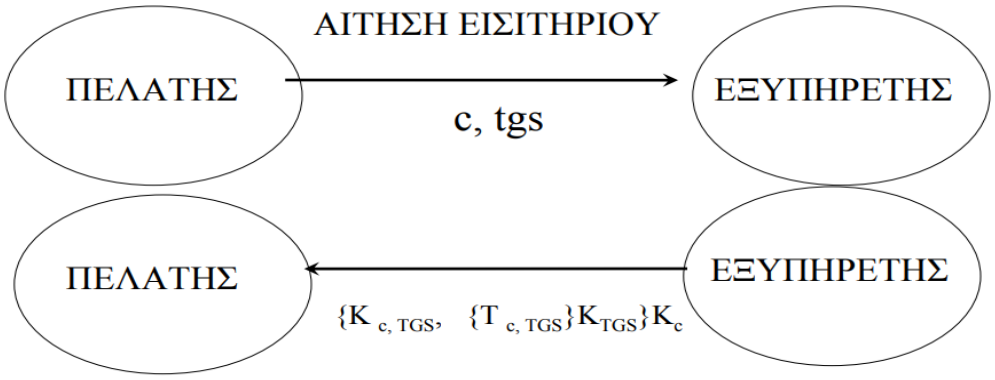
Ένας πιστοποιητής κρυπτογραφείται με το κλειδί συνόδου του εισιτηρίου και περιλαμβάνει:

- το όνομα εξυπηρετούμενου
- την IP διεύθυνση εξυπηρέτη
- τον τρέχοντα χρόνο.

Σύμφωνα λοιπόν με τις απαιτήσεις του εισιτηρίου και του πιστοποιητή στα κέντρα AS και TGS διαμορφώνεται και η λειτουργία του συστήματος Kerberos. Συγκεκριμένα[U4][B1][Δ3], το πρώτο βήμα είναι η παραλαβή του αρχικού εισιτηρίου. Ο χρήστης απευθύνεται στο AS Center με το όνομά του (username) και ζητά έγκριση αίτησης εξυπηρέτησης πιστοποίησης. Η υπηρεσία πιστοποίησης αναγνωρίζει τον χρήστη εφόσον αυτός είναι καταγεγραμμένος στο σύστημα με βάση το username που έδωσε και εκδίδει εισιτήριο για την επικοινωνία του με το TGS, την υπηρεσία έκδοσης εισιτηρίου δηλαδή. Αυτό το λεγόμενο εισιτήριο στην ουσία αποτελεί ένα κλειδί, το κλειδί συνόδου $K_{CLIENT-TGS}$ που θα χρησιμοποιηθεί μετέπειτα στην επικοινωνία του χρήστη με την υπηρεσία έκδοσης εισιτηρίων TGS. Το εισιτήριο αυτό, αρχικά κρυπτογραφεί το κλειδί $K_{CLIENT-TGS}$ με το κλειδί K_{TGS}, το οποίο είναι γνωστό μόνο στον KDC, και έπειτα ολόκληρο το εισιτήριο κρυπτογραφείται με το ιδιωτικό κλειδί του πελάτη. Τελικά, το εισιτήριο αποστέλλεται στον χρήστη.

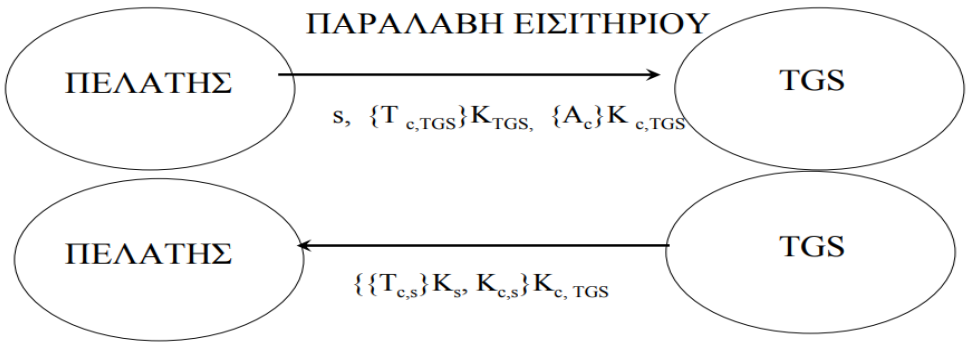
Ο πελάτης τώρα λαμβάνει το μήνυμα, {Kclient, TGS{Tclient,TGS}K_{TGS}}Kclient, που έχει αποσταλεί από τον AS και προσπαθεί να το αποκρυπτογραφήσει. Αρχικά, χρησιμοποιεί τον κωδικό πρόσβασής του, password,

προκειμένου να παράγει το ιδιωτικό κλειδί του $K_{client.}$ Αυτό το κλειδί που θα προκύψει θα βοηθήσει στην αποκωδικοποίηση του εισιτηρίου καθώς όπως αναφέρθηκε έχει κρυπτογραφηθεί ολόκληρο με βάση το ιδιωτικό κλειδί του πελάτη. Μετά την αποκρυπτογράφηση, ο πελάτης έχει πλέον στην διάθεσή του το μήνυμα που στάλθηκε από τον AS και περιλαμβάνει το εισιτήριο επικοινωνίας με τον TGS καθώς και τον πιστοποιητή.



Εικόνα 6: Αίτημα και παραλαβή αρχικού εισιτηρίου.[U4]

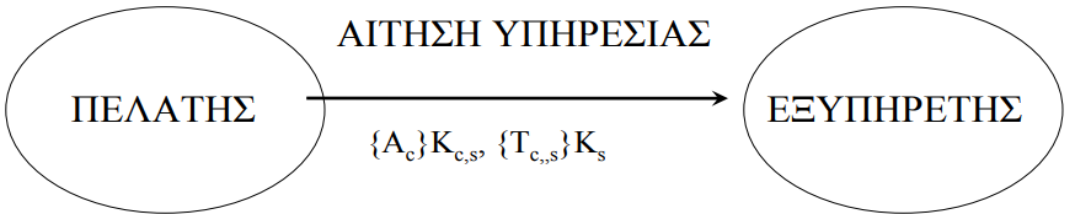
Ο πελάτης τώρα μπορεί να επικοινωνήσει με τον TGS προκειμένου να του εκδώσει εισιτήριο για την πρόσβαση σε συγκεκριμένη υπηρεσία του Service Provider. Ο πελάτης αποστέλλει ένα μήνυμα που περιλαμβάνει την υπηρεσία που επιθυμεί, τον πιστοποιητή του κρυπτογραφημένο με το κλειδί $K_{CLIENT-TGS,}$που χρησιμοποιείται μόνο στην μεταξύ τους επικοινωνία και εισιτήριο κρυπτογραφημένο με το κλειδί K_{TGS} που αναγνωρίζει μόνο ο TGS. Ο TGS τώρα δέχεται το μήνυμα του πελάτη και παράγει το εισιτήριο που θα του επιτρέψει την πρόσβαση στην υπηρεσία της επιλογής του. Κρυπτογραφεί το εισιτήριο πρόσβασης στην υπηρεσία με το κλειδί K_{SP}, το οποίο είναι γνωστό μόνο ανάμεσα στον KDC και στον Service Provider και στην συνέχεια όλο το μήνυμα του session key κρυπτογραφείται με το κλειδί $K_{CLIENT-TGS}$ και αποστέλλεται στον πελάτη.



Εικόνα 7: Αίτηση και παραλαβή εισιτηρίου πρόσβασης σε υπηρεσία.[U4]

Ο πελάτης τώρα είναι σε θέση να επικοινωνήσει με τον Service Provider για την τελική επιβεβαίωση έγκρισης πρόσβασης στην επιθυμητή υπηρεσία για την οποία έβαλε το session key δηλαδή το εισιτήριο πρόσβασης σε αυτήν από τον TGS. Στέλνει λοιπόν αίτηση στον Service Provider η οποία περιλαμβάνει session key εισιτήριο που έλαβε από τον TGS κρυπτογραφημένο με το κλειδί K_{SP} και έπειτα τον πιστοποιητή του κρυπτογραφημένο με το session κλειδί $K_{CLIENT-SP,}$ το οποίο έστειλε ο TGS στον πελάτη για την επικοινωνία του με τον Service Provider.Τέλος, ο Service Provider λαμβάνει την αίτηση του χρήστη και αποκρυπτογραφεί το μήνυμα με το κλειδί $K_{SP.}$ Από την αποκρυπτογράφηση λαμβάνει το κλειδί $K_{CLIENT-SP}$ αποκρυπτογραφεί τον πιστοποιητή του πελάτη, βεβαιώνεται για την εγκυρότητα του πελάτη και του στέλνει ένα timestamp κρυπτογραφημένο με αυτό το κλειδί $K_{CLIENT-SP.}$Ο πελάτης αποκρυπτογραφεί με το ίδιο κλειδί το timestamp και αν είναι έγκυρο επιβεβαιώνεται η έναρξη επικοινωνίας του με τον Service Provider. Το κλειδί $K_{CLIENT-SP}$ είναι το session key που χρησιμοποιείται σε κάθε επικοινωνία μεταξύ client και server. Το timestamp που στέλνεται από τον server είναι στην ουσία μια χρονοσφραγίδα που αποτρέπει την επαναχρησιμοποίηση της ίδιας αίτησης με το ίδιο εισιτήριο. Δηλαδή, ο εξυπηρέτης διατηρεί πληροφορίες με όλες τις παλιές αιτήσεις που έχουν έγκυρη χρονοσφραγίδα. Έτσι δεν εξυπηρετεί αίτηση με το ίδιο εισιτήριο και την ίδια χρονοσφραγίδα αποτρέποντας πιθανές επιθέσεις.

Επομένως, ολοκληρώνεται και η διαδικασία εσωτερικής περιγραφής της λειτουργίας του συστήματος Kerberos.



Εικόνα 8: Αίτηση πρόσβασης σε υπηρεσία στον Service Provider.[U4]

Πιθανά προβλήματα στην λειτουργία του συστήματος Kerberos είναι οι ακόλουθες επιθέσεις:

- ΕΠΙΘΕΣΕΙΣ ΕΠΑΝΑΧΗΣΙΜΟΠΟΙΗΣΗΣ.
- ΑΠΑΤΕΣ ΚΑΤΑ ΤΟ LOGIN
- ΑΣΦΑΛΕΙΑ ΥΠΗΡΕΣΙΩΝ ΧΡΟΝΟΥ.
- ΕΠΙΘΕΣΕΙΣ ΕΥΡΕΣΗΣ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ.

2.4 Πιστοποιητικά

Ιδιαίτερη αποτελεί η σπουδαιότητα της χρήσης των πιστοποιητικών. Η λειτουργία των πιστωτικών καρτών όπως και του συστήματος Kerberos, που αναφέρθηκε, βασίζεται σε μία οντότητα που υλοποιεί την πιστοποίηση, την αναγνώριση δηλαδή της εγκυρότητας των κλειδιών που εκδίδονται. Στις μεθόδους κρυπτογράφησης στις οποίες υπάρχει η έννοια του δημοσίου κλειδιού, στην κρυπτογράφηση δηλαδή δημοσίου κλειδιού, η κάθε οντότητα που συμμετέχει στο δίκτυο επικοινωνίας κοινοποιεί το δημόσιο κλειδί της. Αυτή η δημοσιοποίηση καθιστά αναγκαία την προστασία και διασφάλιση της εγκυρότητας του κλειδιού από οποιονδήποτε επιτιθέμενο προσπαθήσει να αποσπάσει και τελικά να αντικαταστήσει το δημόσιο κλειδί της οντότητας.

Από την στιγμή λοιπόν που τίθεται θέμα διατάραξης της εμπιστοσύνης μεταξύ δύο οντοτήτων που επικοινωνούν, πρέπει να υπάρχει μια υποδομή που θα διασφαλίζει την «χαμένη» ή διακινδυνευμένη εμπιστοσύνη μεταξύ τους. Αυτή η επιθυμητή υποδομή είναι η υποδομή Δημοσίου Κλειδιού PKI, η οποία καθιστά ασφαλή την κοινοποίηση των δημοσίων κλειδιών. Αυτή λοιπόν η υποδομή, αποτελείται από ένα τρίπτυχο λειτουργιών, την Αρχή Πιστοποίησης, την Αρχή Επικύρωσης και μια Βάση δεδομένων αποθήκευσης πιστοποιητικών, και ένα μητρώο.[Β1][Δ1][Δ3][Β2]

Η Αρχή Πιστοποίησης είναι μια έγκυρη Τρίτη Οντότητα που χειρίζεται την Υποδομή του Δημοσίου Κλειδιού, εκδίδει πιστοποιητικά, παρακολουθεί τα παλαιά και μη έγκυρα και διατηρεί ένα αρχείο με πληροφορίες για την κατάστασή τους. Στην ουσία, προσπαθεί να συσχετίσει το δημόσιο κλειδί με έναν κάτοχο για την αναγνώριση της νομιμότητάς του.

Η Αρχή Επικύρωσης επιβεβαιώνει στην Αρχή Πιστοποίησης τα περιεχόμενα ενός πιστοποιητικού που έχει εκδοθεί. Δηλαδή, επικυρώνει την εγκυρότητα μιας πιστοποίησης.

Η Βάση Πιστοποιητικών είναι μια βάση με πιστοποιητικά, τα οποία είναι διαθέσιμα προς τους χρήστες.

2.4.1 Λειτουργία Πιστοποιητικών

Για να κατανοήσουμε την σπουδαιότητα και κατ' επέκταση την λειτουργία των πιστοποιητικών θα πρέπει να αναφερθεί το πρόβλημα ή καλύτερα η επικινδυνότητα κοινοποίησης του δημοσίου κλειδιού χωρίς την μεσολάβηση της υποδομής PKI[B1][Δ1][Δ3][B2]. Πρόκειται δηλαδή να αναδείξουμε μια πιθανή και κακόβουλη επίθεση εις βάρος των επικοινωνούντων οντοτήτων.

Κοινοποίηση δημοσίου κλειδιού χωρίς χρήση υποδομής PKI

Ας υποθέσουμε ότι υπάρχουν δύο οντότητες Α και Β οι οποίες θέλουν να επικοινωνήσουν μεταξύ τους ανταλλάσσοντας μηνύματα. Για την μεταξύ τους επικοινωνία χρησιμοποιείται η κρυπτογραφία δημοσίου κλειδιού. Έστω λοιπόν ότι η οντότητα Α θέλει να στείλει μήνυμα στην οντότητα Β. Το μήνυμα πρέπει να κρυπτογραφηθεί με βάση το δημόσιο κλειδί της οντότητας Β, η οποία το έχει κοινοποιήσει για να είναι προσβάσιμο σε όποιον θέλει να επικοινωνήσει μαζί της. Άρα η οντότητα Α έχει ότι χρειάζεται για την κρυπτογράφηση του μηνύματος. Επομένως, αρχικά κρυπτογραφεί το μήνυμα με το ιδιωτικό της κλειδί ώστε να εξασφαλίσει την ακεραιότητά του δηλαδή την αυθεντικότητα του αποστολέα και μετά το κρυπτογραφεί και με το δημόσιο κλειδί της οντότητας Β, ώστε εκείνη να μπορέσει να το αποκρυπτογραφήσει μόνο με το ιδιωτικό της κλειδί.

Αυτή η διαδικασία κρυπτογράφησης είναι ταυτόσημη με την κρυπτογράφηση δημοσίου κλειδιού στην οποία αρχικά εξασφαλίζεται η ακεραιότητα του αποστολέα κρυπτογραφώντας το μήνυμα με το ιδιωτικό κλειδί και έπειτα την εμπιστευτικότητα κρυπτογραφώντας το με το δημόσιο κλειδί του παραλήπτη. Έτσι ο παραλήπτης θα μπορεί αρχικά με το ιδιωτικό του κλειδί να αποκρυπτογραφήσει το αρχικό μήνυμα εξασφαλίζοντας το μοναδικό πλεονέκτημα ότι μόνο ο ίδιος έχει πρόσβαση στο ιδιωτικό κλειδί και έπειτα να αποκρυπτογραφήσει το τελικό μήνυμα με το δημόσιο κλειδί του αποστολέα ώστε να εξασφαλίσει την ακεραιότητα της ταυτότητά του. Έτσι κανένας δεν μπορεί να «διαβάσει» το μεταδιδόμενο μήνυμα γιατί κανένας άλλος δεν γνωρίζει το ιδιωτικό κλειδί του παραλήπτη.

Υπάρχει ωστόσο η εξής επικινδυνότητα. Μια τρίτη κακόβουλη οντότητα που θέλει να διαταράξει την ασφαλή επικοινωνία μπορεί να αντικαταστήσει το δημόσιο κλειδί του Β, το οποίο είναι ελεύθερα προσβάσιμο, τοποθετώντας ένα δικό του. Έτσι, όταν ο Α στέλνει ένα κρυπτογραφημένο μήνυμα στον Β, η κακόβουλη οντότητα παρεμβαίνει και διαβάζει το μήνυμα αποκρυπτογραφώντας το με βάση το δικό της ιδιωτικό κλειδί, αφού έχει τοποθετήσει το δικό της δημόσιο κλειδί, και έπειτα με το

δημόσιο κλειδί του Α. Έτσι, η κακόβουλη οντότητα μπορεί να δημιουργήσει ένα δικό της μήνυμα και να το κρυπτογραφήσει με βάση το πραγματικό δημόσιο κλειδί της οντότητας Β, αφού το γνωρίζει μετά την υποκλοπή. Επομένως, η οντότητα Β θα λάβει ένα μήνυμα με την ψευδαίσθηση ότι προέρχεται από την οντότητα Α. Η επίθεση επιτεύχθηκε.

Περιεχόμενα ενός Πιστοποιητικού

Ένα ψηφιακό Πιστοποιητικό περιλαμβάνει:

- Αναγνωριστικά πιστοποιητικού: Τύπος, Έκδοση, Πρότυπο, Σειριακός Αριθμός, Αλγόριθμος υπογραφής.
- Περίοδος ισχύος
- Πληροφορίες Εκδότη: Όνομα, σημείο πρόσβασης, Αναγνωριστικό κλειδιού
- Υποκείμενο: Πλήρες Όνομα του κατόχου του πιστοποιητικού
- Δημόσιο κλειδί υποκειμένου
- Επεκτάσεις
- Υπογραφή εκδότη
- Σύνοψη πιστοποιητικού ως κλειδί αναφοράς.

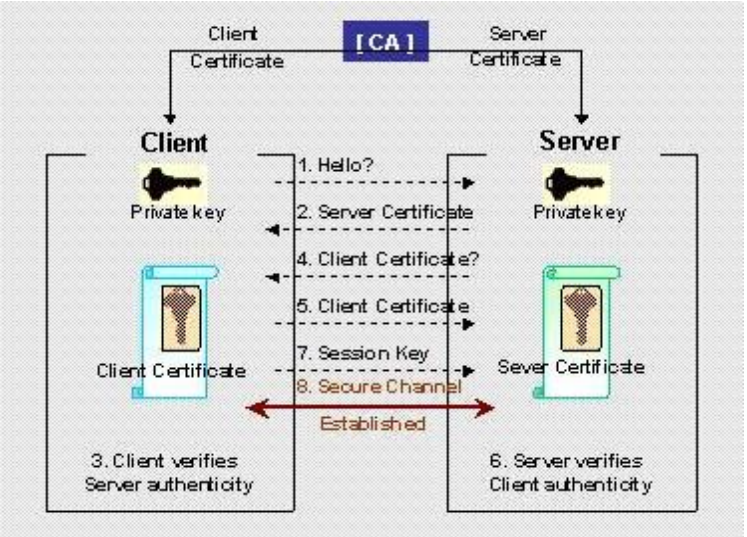
Δημιουργία Πιστοποιητικών

Εικόνα 9: Δημιουργία ψηφιακού πιστοποιητικού.[A6]

Η εικόνα (Εικόνα 9) παρουσιάζει τις ενέργειες που λαμβάνουν χώρα κατά την διάρκεια δημιουργίας ενός πιστοποιητικού. Αρχικά ο χρήστης στέλνει ένα αίτημα για έκδοση πιστοποιητικού στον CA. Αυτός ανταποκρίνεται και στέλνει την προς

συμπλήρωση αίτηση. Έπειτα ο χρήστης συμπληρώνει την αίτηση και δημιουργεί ένα ζεύγος κλειδιών μέσω της CA. Υπογράφει με χρήση των ψηφιακών υπογραφών την αίτηση και την υποβάλλει στον RA. Εκείνος ελέγχει την εγκυρότητα της αίτησης και ειδικότερα την ταυτότητα του αποστολέα. Μετά την επιβεβαίωση αποστέλλει αίτημα στο CA για έκδοση πιστοποιητικού. Ο CA αποκρυπτογραφεί το μήνυμα μέσω του ιδιωτικού του κλειδιού και εκδίδει πιστοποιητικό.

Χρήση Πιστοποιητικού



Εικόνα 10: Χρήση Πιστοποιητικού στην επικοινωνία.[A5]

Η παραπάνω εικόνα (Εικόνα 10) παρουσιάζει αναλυτικά την διαδικασία που ακολουθείται κάθε φορά που δύο οντότητες, εδώ client και server, θέλουν να επικοινωνήσουν. Ο client και ο server έχουν εκδώσει κατάλληλα πιστοποιητικά σύμφωνα με την Αρχή πιστοποίησης CA. Έτσι, όταν ο client στέλνει ένα μήνυμα στον server, εκείνος για να ανταποκριθεί πρέπει να εξακριβώσει την ταυτότητα του αποστολέα. Αρχικά στέλνει το δικό του πιστοποιητικό αυθεντικότητας στον client και ζητά επιπλέον και την επιβεβαίωση του πιστοποιητικού του client. Εκείνος επιβεβαιώνει την εγκυρότητα του πιστοποιητικού που έλαβε από τον server και ανταποκρίνεται στέλνοντας το πιστοποιητικό αυθεντικότητάς του. Ο server επιβεβαιώνει και την εγκυρότητα του πιστοποιητικού του client. Έτσι, ο client στέλνει και το session key της επικοινωνίας. Το κανάλι επικοινωνίας είναι τώρα έγκυρο, ασφαλές και έτοιμο να δεχτεί την ανταλλαγή μηνυμάτων.

Η λειτουργία των πιστοποιητικών τόσο στην διαδικασία της έκδοσης όσο και στην διαδικασία της χρήσης είναι ανάλογη και στην επικοινωνία εμπόρου-καταναλωτή για την διεκπεραίωση μιας Online ηλεκτρονικής συναλλαγής. Όπως έχει αναφερθεί σε κάθε αίτημα συναλλαγής ήταν απαραίτητη η αποστολή κατάλληλων πιστοποιητικών επιβεβαίωσης της ταυτότητάς τους ώστε να διασφαλιστεί η αναγκαία εμπιστοσύνη μεταξύ άγνωστων και απρόσωπων οντοτήτων σε ένα ελεύθερα προσβάσιμο περιβάλλον όπως αυτό του διαδικτύου.

2.5 Πρωτόκολλο SET

Εφόσον έχουν αναλυθεί και περιγραφεί πλήρως τα τεχνολογικά χαρακτηριστικά και η χρησιμότητα των ψηφιακών υπογραφών και των πιστοποιητικών, πρόκειται να μελετηθεί το πρωτόκολλο SET, το οποίο αποτελεί το βασικό πρωτόκολλο λειτουργίας των πιστωτικών καρτών. Τόσο οι ψηφιακές υπογραφές όσο και τα πιστοποιητικά αποτελούν σημαντικό τμήμα του πρωτοκόλλου για την διασφάλιση της ορθής και ασφαλής υλοποίησης της συναλλαγής.

Το πρωτόκολλο SET[Δ10] αναπτύχθηκε από τις εταιρείες Visa και MasterCard. Η επιτυχία του βασίζεται στην κρυπτογράφηση όλων των μηνυμάτων που ανταλλάσσονται. Το πρωτόκολλο SET παρέχει αφενός εμπιστοσύνη μέσω της χρήσης των ψηφιακών πιστοποιητικών και αφετέρου προστασία του απορρήτου των προσωπικών δεδομένων μέσω των διπλών υπογραφών. Όπως θα αναλυθεί και στην συνέχεια, οι διπλές υπογραφές καθιστούν ικανή την ανταλλαγή δεδομένων μεταξύ εμπόρου και καταναλωτή αποτρέποντας την κοινοποίηση των προσωπικών δεδομένων των καταναλωτών, εξασφαλίζοντας ότι κάθε οντότητα θα έχει πρόσβαση μόνο στις πληροφορίες που έχει ανάγκη για την διεκπεραίωση της συναλλαγής και όχι σε επιπλέον στοιχεία.

Διαδικασία συναλλαγής μέσω πρωτοκόλλου SET

Για να πραγματοποιηθεί μια συναλλαγή μέσω ηλεκτρονικού εμπορίου[Δ3][Δ10], ο πελάτης οφείλει να ανοίξει έναν λογαριασμό με τον εκδότη της κάρτας που επιθυμεί. Όταν απευθυνθεί στον αντίστοιχο εκδότη της επιλογής του θα λάβει ένα πιστοποιητικό από την τράπεζα που θα πιστοποιεί την έκδοση πιστωτικής κάρτας στον συγκεκριμένο κάτοχο. Η ηλεκτρονική συναλλαγή μπορεί να επιτευχθεί μόνο στην περίπτωση που ο έμπορος δέχεται πιστωτικές κάρτες του ίδιου τύπου. Ο

έμπορος με την σειρά του οφείλει να διαθέτει 2 πιστοποιητικά, ένα για την υπογραφή και ένα για την ανταλλαγή κλειδιών.

Όταν ο πελάτης αποφασίσει να πραγματοποιήσει μια ηλεκτρονική συναλλαγή, δίνει εντολή στον έμπορο για την επιθυμία του να πραγματοποιήσει μια αγορά. Ο έμπορος λαμβάνει αντίγραφο του πιστοποιητικού του πελάτη και το εξετάζει ώστε να επαληθεύσει την εγκυρότητά του. Παράλληλα, ο πελάτης πραγματοποιεί μια σχετική αγορά και στέλνει τις πληροφορίες παραγγελίας και πληρωμής στον έμπορο.

Για την διαδικασία τώρα της πληρωμής, ο έμπορος ζητά έγκριση πληρωμής από την πύλη πληρωμής πριν την αποστολή της παραγγελίας. Επιβεβαιώνει παράλληλα την παραγγελία που έκανε ο πελάτης και συγκεντρώνει τα προϊόντα ώστε να τα αποστείλει. Τέλος, ο έμπορος ζητά την πληρωμή του από την πύλη πληρωμής, η οποία έχει δεσμεύσει το ποσό της πληρωμής από την πιστωτική κάρτα του πελάτη.

Απαιτήσεις πρωτοκόλλου SET

Το πρωτόκολλο SET[Δ10] δομείται πάνω σε κάποιες σημαντικές παραμέτρους ως προς την διεκπεραίωση του ρόλου τον οποίο έχει αναλάβει, δηλαδή την ασφαλή και ομαλή λειτουργία των ηλεκτρονικών συναλλαγών. Για το λόγο αυτό οι απαιτήσεις του πρωτοκόλλου SET είναι οι ακόλουθες

- Διασφάλιση ακεραιότητας όλων των δεδομένων.
- Απόρρητο πληρωμών και πληροφοριών παραγγελίας.
- Πιστοποίηση νόμιμης κατοχής της πιστωτικής κάρτας.
- Πιστοποίηση της δυνατότητας του εμπόρου να μπορεί να δεχτεί συναλλαγές μέσω πιστωτικής κάρτας.
- Χρήση βέλτιστων πρακτικών ασφάλειας και τεχνικών σχεδιασμού του συστήματος για την προστασία όλων των τμημάτων σε μια ηλεκτρονική συναλλαγή.
- Πρωτόκολλο ανεξάρτητο των μηχανισμών ασφάλειας μεταφοράς των δεδομένων.
- Διευκόλυνση και ενθάρρυνση της διαλειτουργικότητας μεταξύ του λογισμικού και των παρόχων.

Διπλές Υπογραφές

Το πρωτόκολλο SET για να δομηθεί βασίζεται αφενός σε ένα σύνολο απαιτήσεων και αφετέρου σε ένα σύνολο τεχνολογικών εργαλείων. Η εμπιστευτικότητα των δεδομένων υλοποιείται με συμμετρική κρυπτογραφία και συγκεκριμένα με τον αλγόριθμο DES, ενώ η ακεραιότητα των δεδομένων αξιοποιεί την λειτουργία των ψηφιακών υπογραφών που πιστοποιούν την ταυτότητα των εξουσιοδοτημένων οντοτήτων αλλά και τις σημαντικές ιδιότητες των συναρτήσεων κατακερματισμού. Επίσης, χρησιμοποιούνται τα ψηφιακά πιστοποιητικά για την επαλήθευση της ταυτότητας του εμπόρου και του καταναλωτή αλλά και τον έλεγχο της ταυτότητας του λογαριασμού κάθε κατόχου πιστωτικής κάρτας. Άρα, όπως παρατηρείται όλες οι ψηφιακές τεχνολογίες που αναλύθηκαν σε προηγούμενες ενότητες αποτελούν βασικό δομικό λίθο στην λειτουργία των πιστωτικών καρτών. Τέλος, μια ιδιαίτερα σημαντική τεχνολογία που χρησιμοποιείται είναι οι διπλές υπογραφές.

Οι διπλές υπογραφές[B1][Δ10] χρησιμοποιούνται για την προστασία του απορρήτου των προσωπικών δεδομένων. Διασφαλίζουν ότι όλες οι πληροφορίες και τα στοιχεία που είναι διαθέσιμα σε μια ηλεκτρονική συναλλαγή δεν οφείλουν να είναι ορατά σε όλες τις οντότητες που συμμετέχουν στην συναλλαγή. Συγκεκριμένα, κάθε οντότητα οφείλει να γνωρίζει μόνο όσες πληροφορίες και στοιχεία χρειάζεται και τίποτα παραπάνω. Με αυτό τον τρόπο, εξασφαλίζεται η αποφυγή της απρόσκοπτης ροής δεδομένων που θα μπορούσε να διαταράξει την ομαλή λειτουργία μιας ηλεκτρονικής συναλλαγής.

Η βασική ιδέα που δομεί την λειτουργία των διπλών υπογραφών είναι η δημιουργία δύο ξεχωριστών μηνυμάτων που θα προορίζονται σε δύο διαφορετικούς δέκτες:

- Πληροφορίες Παραγγελίας: μια διαδικασία στην οποία έχουν πρόσβαση μόνο ο πελάτης και ο έμπορος.
- Πληροφορίες Πληρωμής: μια διαδικασία στην οποία έχουν πρόσβαση μόνο ο πελάτης και η τράπεζα.

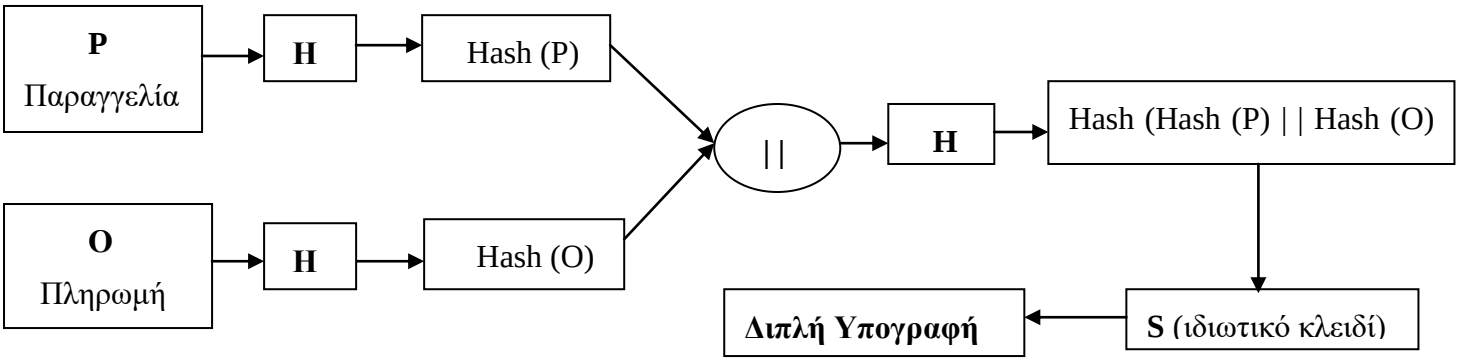
Σύμφωνα λοιπόν με τον παραπάνω διαχωρισμό, οι πληροφορίες διαχωρίζονται ώστε κάθε οντότητα να γνωρίζει μόνο όσες πληροφορίες είναι αναγκαίες και όχι παραπάνω. Δηλαδή, ο έμπορος χρειάζεται να γνωρίζει μόνο τις

πληροφορίες παραγγελίας και όχι τις πληροφορίες πληρωμής οι οποίες περιλαμβάνουν και τον αριθμό πιστωτικής κάρτας του πελάτη. Επιπρόσθετα, η τράπεζα δεν χρειάζεται τα στοιχεία της παραγγελίας του πελάτη παρά μόνο τα στοιχεία της πληρωμής. Τέλος, ο πελάτης διασφαλίζει ότι τα προσωπικά του δεδομένα είναι προστατευμένα διότι ο έμπορος θα αποτραπεί να χρησιμοποιήσει τον αριθμό πιστωτικής κάρτας του πελάτη για να πραγματοποιήσει κάποια άλλη συναλλαγή, παραβιάζοντας το νόμιμο τρόπο συναλλαγής. Αν δηλαδή είχε πρόσβαση στις πληροφορίες πληρωμής και τον αριθμό πιστωτικής κάρτας του πελάτη, θα μπορούσε να αντιστοιχήσει τις πληροφορίες πληρωμής που θα γνώριζε με μία δεύτερη παραγγελία πιθανότερα μεγαλύτερης οικονομικής απολαβής. Έτσι, η τράπεζα που θα λάμβανε τις πληροφορίες πληρωμής από τον έμπορο και όχι από τον πελάτη απευθείας δεν θα μπορούσε να έχει γνώση σχετικά με την αλλαγή της παραγγελίας. Οπότε απλά θα διεκπεραίωνε την πληρωμή και ο πελάτης θα είχε εξαπατηθεί. Για τον λόγο αυτό χρησιμοποιείται η ιδέα του διαχωρισμού των πληροφοριών, δηλαδή των διπλών υπογραφών.

Οι διπλές υπογραφές βέβαια, χρησιμεύουν ώστε να διασυνδέουν τις διαφορετικές αυτές πληροφορίες παραγγελίας και πληρωμής. Η διασύνδεση είναι απαραίτητη προκειμένου να υπάρχει αντιστοιχία ανάμεσα στα στοιχεία της συγκεκριμένης παραγγελίας με τα στοιχεία της συγκεκριμένης πληρωμής. Έτσι αποφεύγεται η αξιοποίηση των στοιχείων πληρωμής σε κάποια άλλα στοιχεία παραγγελίας διαφορετικά από τα ζητούμενα.

Τεχνολογία Διπλών Υπογραφών

Ο πελάτης λοιπόν δημιουργεί 2 διαφορετικά μηνύματα, ένα μήνυμα με τις πληροφορίες παραγγελίας και ένα μήνυμα με τις πληροφορίες πληρωμής. Έπειτα, χρησιμοποιείται η τεχνολογία των συναρτήσεων κατακερματισμού ώστε να κατακερματίζουν τις δύο διαφορετικές πληροφορίες. Έτσι, προκύπτει το hash(στοιχείων παραγγελίας) και το hash(στοιχείων πληρωμής) τις οποίες έστω ότι τις συμβολίζουμε ως hash(O) και hash(P) αντίστοιχα. Στην συνέχεια συνδυάζονται, ενώνονται δηλαδή οι δύο κατακερματισμένες πληροφορίες και δημιουργούν ένα κοινό μήνυμα που περιέχει και τις δύο. Έστω, ότι ο συμβολισμός είναι [hash(O) | | hash(P)] . Αυτό το κοινό μήνυμα τώρα κατακερματίζεται και υπογράφει το τελικό κατακερματισμένο μήνυμα με το ιδιωτικό του κλειδί χρησιμοποιώντας τεχνολογία ψηφιακών υπογραφών.



Εικόνα 11: Διπλή Υπογραφή

- **<u>Έμπορος</u>**

Όταν η διπλή Υπογραφή είναι στην διάθεση του εμπόρου εκείνος θα προσπαθήσει να την αποκρυπτογραφήσει προκειμένου να έχει πρόσβαση στις πληροφορίες παραγγελίας. Από το αντίγραφο του ψηφιακού πιστοποιητικού του πελάτη που έλαβε γνωρίζει το δημόσιο κλειδί του. Έτσι αποκρυπτογραφεί την ψηφιακή υπογραφή που έγινε στο τελευταίο βήμα της εφαρμογής της διπλής υπογραφής. Από αυτή την αποκρυπτογράφηση έχει τώρα πρόσβαση στο τελικό κατακερματισμένο μήνυμα. Ο έμπορος δεν έχει πρόσβαση στα στοιχεία πληρωμής άρα δεν μπορεί να βρει την συνάρτηση κατακερματισμού που δημιουργεί τον κατακερματισμό της πληρωμής. Ωστόσο, έχει πρόσβαση στις πληροφορίες παραγγελίας και μπορεί να εφαρμόσει τον κατακερματισμό. Αν υπάρχει ταύτιση στις δύο αυτές πληροφορίες τότε υπάρχει εγκυρότητα.

Hash (P | | Hash (O))

Hash (Hash (P) | | Hash (O))

- **<u>Τράπεζα</u>**

Όταν η διπλή Υπογραφή είναι στην διάθεση της τράπεζας εκείνη θα προσπαθήσει να την αποκρυπτογραφήσει προκειμένου να έχει πρόσβαση στις πληροφορίες πληρωμής. Από το αντίγραφο του ψηφιακού πιστοποιητικού του πελάτη που διαθέτει γνωρίζει το δημόσιο κλειδί του. Έτσι αποκρυπτογραφεί την ψηφιακή υπογραφή που έγινε στο τελευταίο βήμα της εφαρμογής της διπλής υπογραφής. Από αυτή την αποκρυπτογράφηση έχει τώρα πρόσβαση στο τελικό κατακερματισμένο μήνυμα. Η τράπεζα δεν έχει πρόσβαση στα στοιχεία παραγγελίας άρα δεν μπορεί να

βρει την συνάρτηση κατακερματισμού που δημιουργεί τον κατακερματισμό της παραγγελίας. Ωστόσο, έχει πρόσβαση στις πληροφορίες πληρωμής και μπορεί να εφαρμόσει τον κατακερματισμό. Αν υπάρχει ταύτιση στις δύο αυτές πληροφορίες τότε υπάρχει εγκυρότητα.

Hash (Hash (P) | | O)

Hash (Hash (P) | | Hash (O))

Συνοψίζοντας, ο έμπορος έχει πρόσβαση μόνο στις πληροφορίες παραγγελίας, η τράπεζα μόνο στις πληροφορίες πληρωμής και ο πελάτης κατάφερε να συνδυάσει αποτελεσματικά τις δύο αυτές πληροφορίες προστατεύοντας παράλληλα τα προσωπικά του δεδομένα. Άρα, η λειτουργία των πιστωτικών καρτών προσφέρει τόσο την επιθυμητή ασφάλεια όσο και την διευκόλυνση διεκπεραίωσης των ηλεκτρονικών συναλλαγών.

ΚΕΦΑΛΑΙΟ 3: ΨΗΦΙΑΚΟ ΝΟΜΙΣΜΑ

Στο προηγούμενο κεφάλαιο, αναλύθηκε λεπτομερώς η λειτουργία των πιστωτικών καρτών στην διεκπεραίωση των ηλεκτρονικών συναλλαγών. Το ηλεκτρονικό εμπόριο βρίσκεται σε ιδιαίτερη άνθιση αυτή την περίοδο γεγονός που καθιστά το πλαστικό χρήμα ευρέως χρησιμοποιούμενο. Ωστόσο, παρατηρείται μια ιδιαίτερη τεχνολογική έξαρση στο σύστημα blockchain. Το blockchain σύστημα δημιουργεί μια επανάσταση στον τομέα των συναλλαγών καθώς βασίζεται στην ιδέα του ψηφιακού νομίσματος. Αποτέλεσμα λοιπόν αυτής της εξελικτικής πορείας είναι, η μετάβαση από το πλαστικό χρήμα που αποτελεί την βάση στις ηλεκτρονικές συναλλαγές του παρόντος, στο ψηφιακό νόμισμα που πρόκειται να αποτελέσει τον δομικό λίθο των μελλοντικών ηλεκτρονικών συναλλαγών.

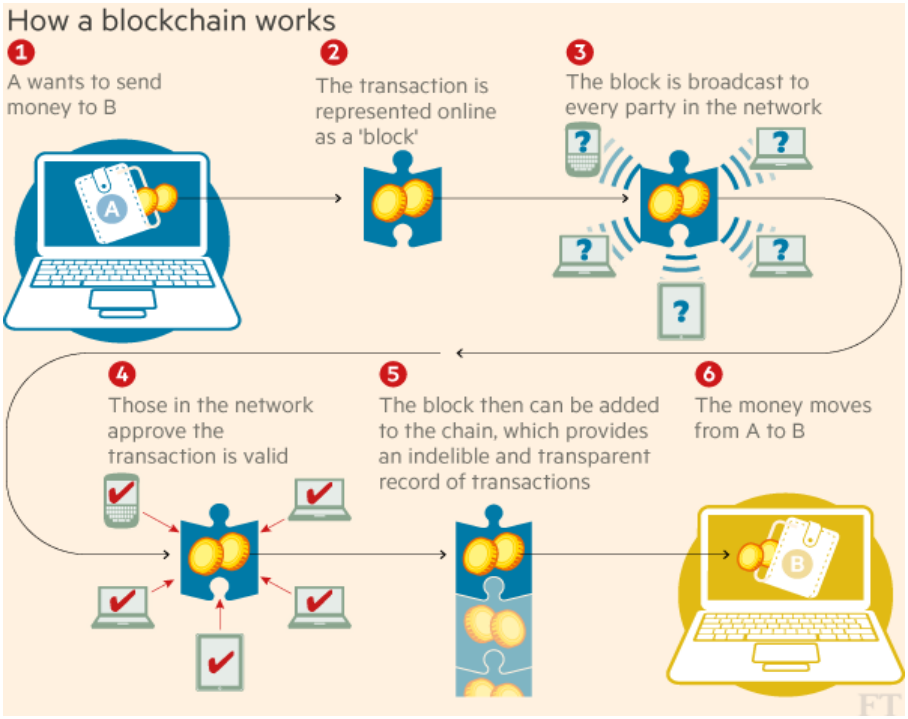
3.1 Σύστημα blockchain

Το σύστημα blockchain αποτελεί μια κατανεμημένη βάση δεδομένων, ένα μητρώο δηλαδή, που διατηρεί αποθηκευμένη μια συνεχώς αυξανόμενη λίστα καταχωρήσεων, δηλαδή συναλλαγών, που ονομάζεται block. Ένα block, μια ομάδα δηλαδή συναλλαγών που έχουν υποβληθεί στο δίκτυο για επιβεβαίωση εγκυρότητας, περιλαμβάνει μια χρονική σήμανση και μία σύνδεση με ένα προηγούμενο block. Η αλυσίδα, που περιλαμβάνει το σύνολο των blocks που έχουν επιβεβαιωθεί και εγκριθεί από την $1^{η}$ χρονικά έως την πιο πρόσφατη ομάδα συναλλαγών, αποκαλείται Blockchain[U8][U9][U10]. Στην ουσία, το blockchain σύστημα λειτουργεί στην βάση ενός δικτύου μέσω της χρήσης ενός λογισμικού ανοιχτού κώδικα.

Ο κύριος λόγος στον οποίο είναι γνωστή η λειτουργία και η χρήση του συστήματος blockchain είναι η πραγματοποίηση online συναλλαγών. Στις συναλλαγές αυτές γίνεται χρήση του λεγόμενου ψηφιακού κρυπτονομίσματος bitcoin.Το σύστημα blockchain προσφέρει πολλά πλεονεκτήματα στην διεκπεραίωση των οικονομικών συναλλαγών με το κυριότερο να επικεντρώνεται στον έλεγχο και την επαλήθευση της εγκυρότητας ανταλλαγής κρυπτονομισμάτων. Παρόλα αυτά το blockchain μπορεί να χρησιμοποιηθεί και ως «αποθήκη» καταγραφής και ελέγχου δεδομένων. Για παράδειγμα, αξιοποιείται στην καταγραφή ιατρικών αρχείων,

καταγραφή γεγονότων ή ακόμα και στην επεξεργασία των συναλλαγών από την πλευρά των στατιστικών αναλύσεων. Άλλωστε, ο τρόπος σχεδιασμού του συστήματος το καθιστά ιδιαίτερα ανθεκτικό σε κακόβουλες επιθέσεις, γεγονός που ενισχύει την δημοτικότητά επιλογής του συστήματος στην εφαρμογή διαφορετικών τομέων.

3.1.1 Χαρακτηριστικά blockchain



Εικόνα 12: Τρόπος λειτουργίας blockchain.[A8]

Στην παραπάνω εικόνα (Εικόνα 12) διακρίνεται ο τρόπος λειτουργίας του συστήματος blockchain. Συγκεκριμένα, παρουσιάζεται η χρήση του στην διεκπεραίωση μιας οικονομικής συναλλαγής μέσω μεταφοράς χρημάτων. Έστω λοιπόν, μια οντότητα Α που είναι συνδεδεμένη στο δίκτυο και θέλει να στείλει ένα ποσό χρημάτων στην οντότητα Β. Το ποσό αυτό λοιπόν των χρημάτων, αποτελεί μια συναλλαγή η οποία αναπαρίσταται με την μορφή ενός block. Αυτό το block διατίθεται στο δίκτυο για επιβεβαίωση από τους υπόλοιπους κόμβους του. Κάθε μέλος του δικτύου εξετάζει αυτή την συναλλαγή και εγκρίνει την διεκπεραίωσή της. Εφόσον, το block της συναλλαγής επιβεβαιώθηκε από τους κόμβους του δικτύου αποτελεί μια έγκυρη και διαφανής συναλλαγή. Επομένως, μπορεί να εισαχθεί στην αλυσίδα των επιβεβαιωμένων καταγραφών Blockchain. Έτσι, ολοκληρώνεται η μεταφορά χρημάτων στην οντότητα Β.

Το σύστημα blockchain[U8][U9][U10] λοιπόν, υποστηρίζει την διεκπεραίωση συναλλαγών στο περιβάλλον του διαδικτύου. Το διαδίκτυο, ως ελεύθερα προσβάσιμη πλατφόρμα, εγκυμονεί κινδύνους. Οι κίνδυνοι αυτοί, δημιουργούν αμφιβολίες στην επιλογή χρήσης του ως σύστημα συναλλαγών. Πόσο μάλλον, όταν οι συναλλαγές λαμβάνουν χώρα μεταξύ εντελώς άγνωστων προσώπων. Το σύστημα blockchain δημιουργεί ασφάλεια σε κάθε κόμβο του δικτύου συναλλαγών καθώς χρησιμοποιεί κρυπτογράφηση για κάθε μήνυμα ή συναλλαγή που ανταλλάσσεται ή αποθηκεύεται. Κάθε συναλλαγή χρησιμοποιεί τις ψηφιακές υπογραφές για την ασφάλεια και την εγκυρότητα της ταυτοποίησης των συναλλασσόμενων προσώπων. Ο αποστολέας, όταν δημιουργεί μια νέα συναλλαγή με την μορφή block, την υποβάλλει στο σύστημα υπογεγραμμένη με την ιδιωτική του υπογραφή. Ο κάθε κόμβος του δικτύου επιβεβαιώνει την εγκυρότητα της συναλλαγής. Ο παραλήπτης έχοντας την έγκριση από του κόμβους του δικτύου θα δεχτεί τα χρήματα από τον παραλήπτη, εφόσον πιστοποιήσει την αυθεντικότητα του αποστολέα με την αποκρυπτογράφηση του block μέσω του δημοσίου κλειδιού του αποστολέα.

Το blockchain σύστημα βασίζεται στην ύπαρξη ενός P2P (peer-to-peer) δικτύου. Σε ένα peer-to-peer[U7] δίκτυο κάθε κόμβος δηλαδή κάθε χρήστης-υπολογιστής είναι ισότιμος με τα ίδια δικαιώματα και υποχρεώσεις με όλους τους υπόλοιπους κόμβους του δικτύου. Αυτός ο τύπος δικτύου, απορρίπτει την ιδέα ύπαρξης ενός συστήματος server-client, καθώς κάθε κόμβος μπορεί να διεκπεραιώσει και τους δύο ρόλους. Δηλαδή σε ένα client-server δίκτυο, το αποθηκευμένο περιεχόμενο βρίσκεται υπό την ευθύνη του κεντρικού εξυπηρετητή ενώ σε ένα P2P δίκτυο το αποθηκευμένο περιεχόμενο βρίσκεται υπό των έλεγχο μεμονωμένων υπολογιστών. Έτσι, το δίκτυο P2P διευκολύνει την μεταφορά δεδομένων σε πραγματικό χρόνο χωρίς την παρεμβολή καμίας άλλης τρίτης ελεγκτικής δύναμης.

Είναι ένα αποκεντρωμένο, λοιπόν, σύστημα στο οποίο οι συναλλαγές δεν απαιτούν την έγκριση της τράπεζας για την ολοκλήρωσή τους. Ωστόσο, η ανάγκη ολικής επιβεβαίωσης της συναλλαγής εξακολουθεί να είναι άκρως αναγκαία. Σκοπός όμως είναι να μην γίνει παρεμβολή κάποιας τρίτης ελεγκτικής δύναμης με σκοπό όλη η διαδικασία να λαμβάνει χώρα αυστηρά μεταξύ των πόρων του συστήματος. Η ορθή επιβεβαίωση λοιπόν των συναλλαγών σε ένα P2P δίκτυο γίνεται με βάση την επίλυση ενός δύσκολου μαθηματικού προβλήματος γνωστό ως «proof of work». Κάθε μπλοκ θα μπορέσει να γίνει αποδεκτό μόνο εφόσον λυθεί ένα ειδικό μαθηματικό πρόβλημα. Ο κάθε κόμβος του δικτύου αναλαμβάνει να βρει λύση σε αυτό το μαθηματικό ζήτημα. Έτσι, ο δημιουργός του μπλοκ θα αποδείξει ότι το μπλοκ περιλαμβάνει αρκετούς υπολογιστικούς πόρους για να λυθεί το μαθηματικό πρόβλημα. Ο

μαθηματικός αυτός γρίφος διατίθεται στο δίκτυο και μεταδίδεται από κόμβο σε κόμβο μέχρι να λυθεί. Αν ταυτόχρονα λυθούν περισσότερα από ένα μπλοκ τότε δημιουργούνται διακλαδώσεις.

Όταν ένα μπλοκ επιβεβαιωθεί, μετά την λύση του μαθηματικού γρίφου, προστίθεται στην αλυσίδα Blockchain. Η αλυσίδα αυτή υπάρχει προκειμένου να αποφευχθεί το πρόβλημα που υπάρχει στην σειρά έλευσης των μπλοκ. Δεν υπάρχει κάποιος ιδιαίτερος τρόπος ελέγχου της σειράς με την οποία καταφθάνουν τα μπλοκ σε κάθε κόμβο για να εγκριθούν. Έτσι, ένα μπλοκ μπορεί να επιβεβαιωθεί διπλά και να χρεωθεί διπλό το ποσό των κρυπτονομισμάτων. Η αλυσίδα εξασφαλίζει την χρονική αλληλοσυσχέτιση μεταξύ των ήδη επιβεβαιωμένων μπλοκ. Κάθε μπλοκ περιλαμβάνει το hash του προηγούμενο μπλοκ κ.τ.λ. Με αυτόν τον τρόπο, μπορεί να υπάρχει έλεγχος από το $1^{ο}$ χρονικά δημιουργημένο μπλοκ μέχρι το πιο πρόσφατο.

3.1.2 Πλεονεκτήματα blockchain

Το βασικότερο πλεονέκτημα του συστήματος blockchain είναι η ιδιότητα της αποκέντρωσης που προσφέρει. Η έννοια της αποκέντρωσης προέρχεται από την έννοια απουσίας τρίτης ελεγκτικής δύναμης που παρεμβαίνει στις συναλλαγές. Αυτό είναι άμεσο επακόλουθο της δομής του peer-to-peer δικτύου. Τα δεδομένα μοιράζονται αυστηρά μεταξύ των υπολογιστών-κόμβων και κάθε κόμβος μπορεί να έχει πρόσβαση σε αυτά μετά την άδεια των χρηστών. Με αυτόν τον τρόπο, τα δεδομένα ασφαλίζονται από κακόβουλες ενέργειες τρίτων προσώπων που θα μπορούσαν να φθείρουν την ασφάλεια του δικτύου αφού θα είχαν πρόσβαση σε αυτά. Έτσι, το σύστημα blockchain εξασφαλίζει την περιορισμένη επέκταση της δημοσιοποίησης των δεδομένων, διατηρώντας τα ασφαλή.

Ένα ακόμα πλεονέκτημα του Blockchain είναι η χρήση κρυπτογράφησης σε κάθε μήνυμα με την μορφή block που διατίθεται στο δίκτυο. Κάθε μπλοκ «υπογράφεται» και διατίθεται στο δίκτυο για επιβεβαίωση. Αν όλοι οι κόμβοι του δικτύου το εγκρίνουν αυτό προστίθεται στην αλυσίδα Blockchain. Έτσι το δίκτυο, διαθέτει μόνο έγκυρες συναλλαγές και αποθηκευμένα δεδομένα.

Στα πλεονεκτήματα του συστήματος ανήκει και η δυνατότητα ύπαρξης διαφορετικών εκδόσεων του πρωτοκόλλου λειτουργίας του συστήματος. Στο blockchain σύστημα δίνεται ιδιαίτερη σημασία στην ομαλή επικοινωνία και κοινή γραμμή πλεύσης μεταξύ όλων των κόμβων. Για το λόγο αυτό, αν κάποιος από τους κόμβους-χρήστες δεν συμφωνούν με την προτεινόμενη αλλαγή στο πρωτόκολλο

λειτουργίας του συστήματος, το σύστημα δίνει την δυνατότητα επιλογής. Δηλαδή κάθε χρήστης επιλέγει την έκδοση που επιθυμεί και τον διευκολύνει. Έτσι, δημιουργούνται «παρακλάδια» διαφορετικών εκδόσεων με διαφορετική ιστορία και πορεία το καθένα, από την εκκίνηση δημιουργίας τους.

Στα βασικά χαρακτηριστικά του συστήματος είναι και το πλεονέκτημα «permissionless», δηλαδή η απουσία ελέγχου πρόσβασης και κατ΄επέκταση φύλαξης των δεδομένων από κακόβουλες ενέργειες. Άρα, αυτό το πλεονέκτημα δίνει την δυνατότητα της αυτόνομης εισαγωγής εφαρμογών στο blockchain,χωρίς να απαιτείται έλεγχος. Τα δεδομένα είναι ελεύθερα προσβάσιμα και παρέχονται για έρευνα και στατιστικές αναλύσεις.

Τέλος, αδιαμφισβήτητα το σύστημα blockchain είναι φιλικό προς το χρήστη καθώς βασίζεται στην λειτουργία του λογισμικού ανοιχτού κώδικα Bitcoin με απουσία κεντρικής δύναμης ελέγχου.

3.2 Bitcoin

Το blockchain σύστημα για την λειτουργία του χρησιμοποιεί το ψηφιακό κρυπτονόμισμα bitcoin.Το bitcoin είναι ένα νόμισμα σε ηλεκτρονική μορφή, το οποίο δεν υπόκειται σε έλεγχο και δεν μπορεί να εκτυπωθεί. Η παραγωγή τους προκύπτει μέσω της επίλυσης μαθηματικών προβλημάτων κατά την διάρκεια επιβεβαίωσης ενός block συναλλαγής. Τα κρυπτονόμισμα δεν έχουν φυσική παρουσία παρά μόνο εικονική, ωστόσο η λειτουργία τους είναι ανάλογη της φυσικής χρήσης των νομισμάτων. Χρησιμοποιούνται δηλαδή για την αγοραπωλησία προϊόντων και υπηρεσιών Online μέσω του λογισμικού ανοιχτού κώδικα.

Κάθε συναλλαγή που λαμβάνει χώρα στο blockchain σύστημα είναι απόλυτα έγκυρη και διαφανής, αλλά μη αναστρέψιμες. Το περιβάλλον είναι αποκεντρωμένο και ανώνυμο, οπότε υπάρχει ελευθερία.

3.2.1 Δημιουργία Bitcoins

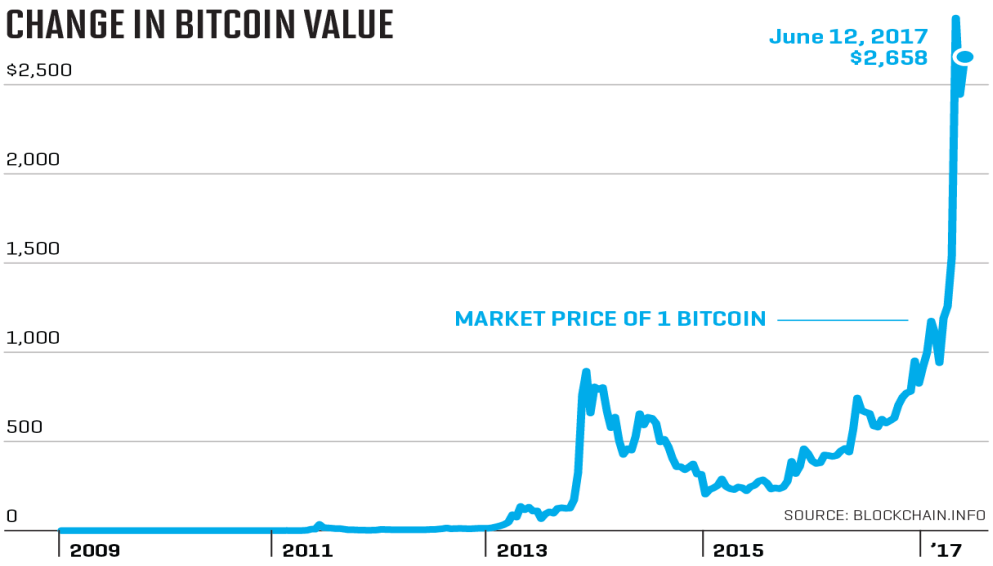
Η διαδικασία δημιουργίας των κρυπτονομισμάτων bitcoins ονομάζεται Mining[U19]. Όπως έχει αναφερθεί, κάθε συναλλαγή προς διεκπεραίωση διατίθεται στο δίκτυο για επιβεβαίωση μεταξύ των κόμβων. Όταν αυτή εγκριθεί, το μπλοκ προστίθεται στην αλυσίδα επιβεβαιωμένων μπλοκ που ονομάζεται Blockchain. Κάθε δέκα λεπτά περίπου, ένα νέο μπλοκ δημιουργείται και ελέγχεται για να εισαχθεί στην

αλυσίδα. Για να εγκρίνει ένας κόμβος το μπλοκ πρέπει να ανταπεξέλθει στην λύση ενός μαθηματικού προβλήματος. Μόλις βρεθεί η λύση, δημιουργείται νέο μπλοκ και συγκεκριμένος αριθμός bitcoins.

Όσο περισσότεροι είναι οι χρήστες-κόμβοι που προσπαθούν να λύσουν ένα μαθηματικό γρίφο τόσο δυσκολότερο είναι το συγκεκριμένο μαθηματικό πρόβλημα. Κάθε κόμβος, εκτός από την επίλυση του γρίφου συμμετέχει και στην προστασία του δικτύου από επιθέσεις, ελέγχοντας παράλληλα την εγκυρότητα κάθε συναλλαγής. Ο χρήστης λαμβάνει ένα ποσό των bitcoins ανάλογα με την προσφορά του στην επίλυση του γρίφου. Όσο περισσότερο συνεισφέρει τόσα περισσότερα bitcoins κερδίζει. Βέβαια, το ποσό των bitcoins που δίνεται σε κάποιον που βρίσκει την λύση του μαθηματικού γρίφου υποδιπλασιάζεται κάθε τέσσερα χρόνια. Το 2012 πραγματοποιήθηκε ο πρώτος υποδιπλασιασμός μειώνοντας το ποσό των bitcoins στα 25.

Τέλος, η δημιουργία των bitcoins είναι καθαρά αποτέλεσμα της λειτουργίας του δικτύου. Αυτό το πλεονέκτημα του blockchain συστήματος το καθιστά ανθεκτικό σε οποιοδήποτε επηρεασμό οικονομικής κρίσης.

Το ακόλουθο διάγραμμα (Εικόνα 13) παρουσιάζει την πορεία στην εξέλιξη της αξίας του bitcoins. Διακρίνεται λοιπόν, ότι την χρονιά 2010 η αξία του ήταν αρκετά χαμηλή σε αντίθεση με την πιο πρόσφατη χρονιά 2017 που η πορεία της αξίας του είναι ανοδική. Το διάγραμμα παρουσιάζει μια παραβολική γραμμή ανόδου.



Εικόνα 13: Διάγραμμα σχετικά με την αξία του bitcoin.[A10]

3.2.2 Επιθέσεις

Μπορεί το σύστημα blockchain να είναι αρκετά επαναστατικό και ισχυρό, ωστοσο το κρυπτονόμισμα bitcoin υπόκειται και αυτό σε κακόβουλες ενέργειες υποτίμησης της αξίας του. Δύο είναι οι βασικές επιθέσεις στο ψηφιακό νόμισμα bitcoin.

- 51% attack
- Goldfinger attack

Η επίθεση 51% attack[U11] σχετίζεται με την διατάραξη της ισότιμης σχέσης μεταξύ όλων των κόμβων. Δηλαδή αν ένας συγκεκριμένος κόμβος συμμετείχε στην διαδικασία του Mining έχοντας το μεγαλύτερο ποσοστό επιτυχίας τότε μπορεί να κατέχει περισσότερα bitcoins και να εξουσιάζει το σύστημα blockchain. Αυτό μπορεί να επιτευχθεί από την στιγμή που το δίκτυο είναι ελεύθερο και η κατοχή περισσότερης υπολογιστικής ισχύς σηματοδοτεί την κυριαρχία.

Η δεύτερη επίθεση Goldfinger attack[Δ9] σχετίζεται με την υποτίμηση της αξίας του bitcoin ως κρυπτονόμισμα. Μια πλειοψηφία χρηστών που κυριαρχούν στην διαδικασία του mining μπορούν να προκαλέσουν ρήξη στην σταθερότητα της αξίας του κρυπτονομίσματος.

3.3 Σύστημα Ethereum

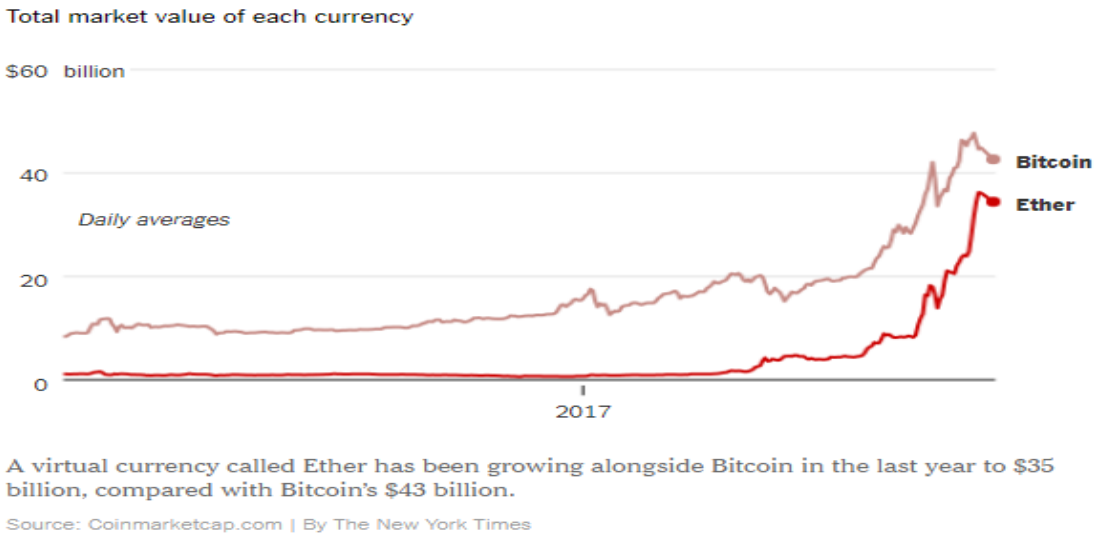
Ένας κόσμος με συνεχώς εξελισσόμενη τεχνολογία, καθιστά εξελισσόμενη και την πορεία του οικονομικού συστήματος. Η μορφή και η αξία του χρήματος αλλάζει συνεχώς, καθώς αναζητούνται νέοι τρόποι πραγματοποίησης των συναλλαγών. Το blockchain σύστημα, όπως αναφέρθηκε, προσφέρει μια επανάσταση στον τομέα των οικονομικών συναλλαγών καθώς εισάγει την χρήση ψηφιακού δηλαδή εικονικού νομίσματος. Μια ακόμα πιο επαναστατική ιδέα στον τομέα της χρήσης του εικονικού νομίσματος, προσφέρει το νέο σύστημα Ethereum[U13] .Το Ethereum εισάγει ένα νέο εικονικό νόμισμα, το Ether, που πρόκειται να αποτελέσει τον κύριο ανταγωνιστή του εικονικού νομίσματος bitcoin. Στην ουσία, το σύστημα Ethereum «τρέχει» εφαρμογές βασισμένες στο υπάρχον σύστημα blockchain.

3.3.1 Χαρακτηριστικά & Πλεονεκτήματα Ethereum

Το σύστημα Ethereum αποτελεί μια αποκεντρωμένη νομισματική πλατφόρμα βασισμένη σε λογισμικό ανοιχτού κώδικα. Οι χρήσεις του συστήματος επικεντρώνονται κυρίως σε οικονομικές συναλλαγές αλλά και στην κατασκευή ή διανομή εφαρμογών παρέχοντας την δυνατότητα ελεύθερης προσθήκης τους στο σύστημα χωρίς καμία παρέμβαση διακοπής, λογοκρισίας ή παρεμβολής τρίτων ελεγκτικών δυνάμεων.

Το νόμισμα Ether, πρόκειται να αποτελέσει τον κύριο ανταγωνιστή του bitcoin καθώς θα παρέχει έξυπνους και γρήγορους τρόπους δημιουργίας Online αγορών και προγραμματισμένων συναλλαγών. Δημιουργεί δηλαδή, «έξυπνα συμβόλαια».

Στα γενικά του χαρακτηριστικά το σύστημα Ethereum προσφέρει ανάλογα πλεονεκτήματα με το σύστημα Blockchain. Τα πλεονεκτήματα αυτά αναφέρονται κυρίως στα χαρακτηριστικά της Open και αποκεντρωμένης πλατφόρμας αποθήκευσης δεδομένων και συναλλαγών με κύριο βασικό όραμα την απαλλαγή από τις κακόβουλες επιθέσεις και τον έλεγχο πρόσβασης. Άλλωστε, το σύστημα Ethereum δεν αποτελεί απλώς μια νομισματική πλατφόρμα αλλά έναν χώρο που μπορείς να επιλύσεις πολλά προβλήματα σε διαφορετικές πτυχές της οικονομίας ακόμα και της βιομηχανίας.



Εικόνα 14: Σύγκριση αξίας κρυπτονομισμάτων bitcoin και Ether.[A11]

Στο παραπάνω διάγραμμα(Εικόνα 14) παρατηρείται ότι την χρονιά 2017 η άνοδος στην αξία του Ether είναι ραγδαία, φτάνοντας κοντά στην αξία του bitcoin, παρόλο που κυριαρχεί στον επιχειρηματικό κόσμο περισσότερο καιρό.

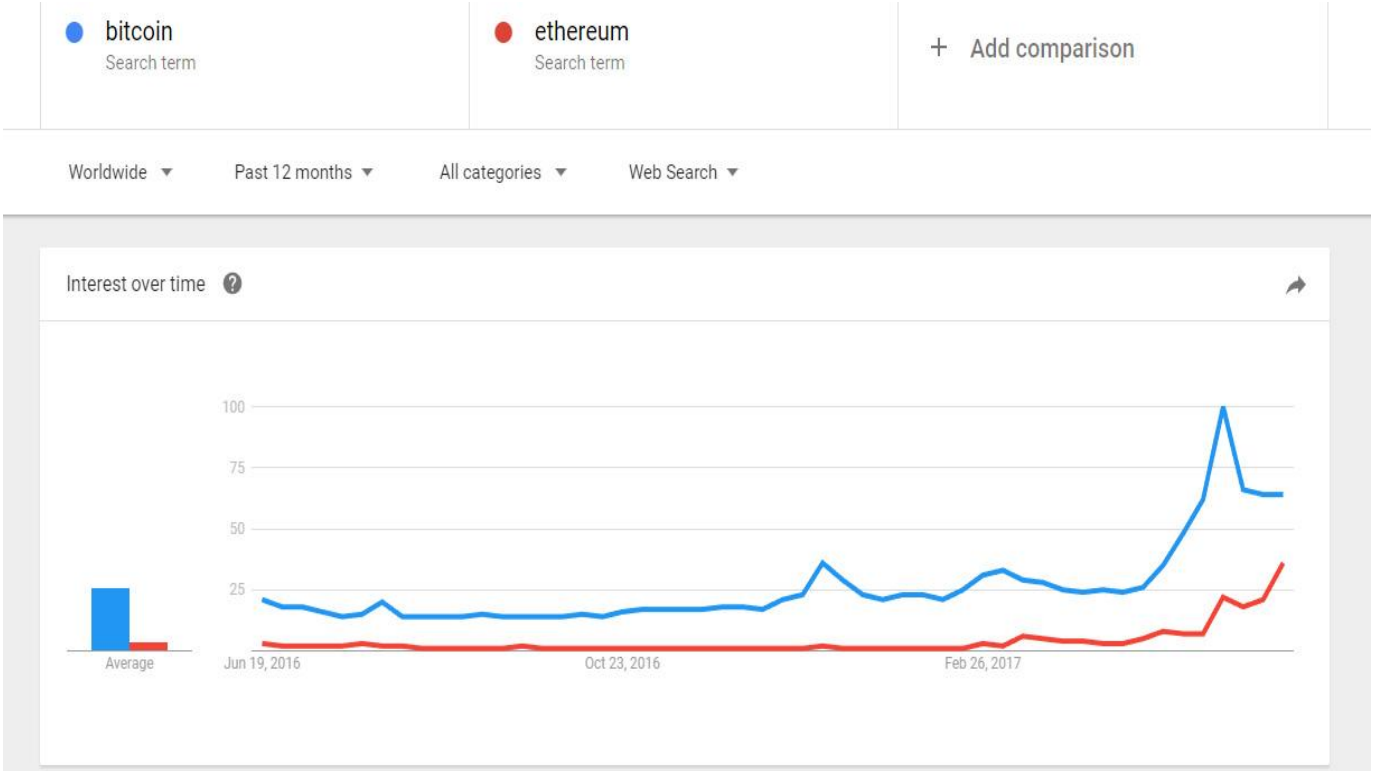
3.3.2 Εφαρμογές Blockchain & Ethereum

Οι περισσότερες εφαρμογές του συστήματος blockchain έχουν ως κύριο αντικείμενο την πιστοποίηση. Αυτή η πιστοποίηση μπορεί να αφορά[U10] είτε την πιστοποίηση κάποιου εγγράφου, την πιστοποίηση της ταυτότητας ενός πολίτη ή ακόμα και την προστασία των πνευματικών δικαιωμάτων φωτογραφιών, έργων τέχνης ή πρωτοπόρων ανακαλύψεων. Τέλος, εφαρμογές υπάρχουν και στο χρηματοπιστωτικό σύστημα με την πραγματοποίηση συναλλαγών με κρυπτονομίσματα.

Ένα χαρακτηριστικό παράδειγμα, στο οποίο η χρήση συστήματος blockchain και Ethereum είναι ιδιαίτερα σημαντική είναι η μουσική βιομηχανία. Ο χώρος της δισκογραφίας υπόκειται στον κίνδυνο διαφύλαξης των πνευματικών δικαιωμάτων κάθε δημιουργίας. Η κατανεμημένη βάση δεδομένων του συστήματος που διατηρεί χρονική αλληλουχία δημιουργίας κάθε αποθηκευμένου και επιβεβαιωμένου σε αυτή δεδομένο, μπορεί να διασφαλίσει την πνευματική ιδιοκτησία κάθε μουσικού κομματιού.

Τέλος, συστήματα όπως το Google Drive, το Dropbox ακόμα και το Cloud υπόκεινται στον κίνδυνο διατάραξης της ασφάλειας των προσωπικών στοιχείων που διατηρούν αποθηκευμένα. Από την στιγμή που λειτουργούν στο διαδίκτυο, η επίθεση είναι ένα πιθανό γεγονός. Ένα P2P δίκτυο, το Storj[Δ4], προσφέρει την δυνατότητα ασφαλής αποθήκευσης των δεδομένων χωρίς την εμπιστοσύνη σε κάποιο τρίτο πρόσωπο, όπως το blockchain σύστημα. Έτσι αυξάνεται η ιδιωτικότητα στην μεταφορά και στην κοινοποίηση προσωπικών στοιχείων, ενισχύοντας την εμπιστοσύνη.

3.4 Σύγκριση συστημάτων Blockchain με Ethereum



Εικόνα 15: Σύγκριση χρήσης των συστημάτων blockchain και Ethereum[A9].

Τα δύο αυτά συστήματα έχουν παρόμοια λειτουργία και χρήση[U12] .Η κύρια διαφορά μεταξύ των δύο συστημάτων είναι ότι το σύστημα Ethereum παρέχει επιπλέον την δυνατότητα των «έξυπνων συμβολαίων». Τα «έξυπνα συμβόλαια»[U15] διευρύνουν την λειτουργία του συστήματος Ethereum πέρα από την νομισματική του οπτική. Το Ethereum επιτρέπει την δημιουργία ψηφιακών μαρκών που μπορούν να χρησιμοποιηθούν για την αναπαραγωγή εικονικών μετοχών, περιουσιακών στοιχείων, αποδεικτικών στοιχείων συμμετοχής κτλ. Γενικότερα, το σύστημα blockchain θεωρείται περισσότερο ως ένα σχετικά σταθερό ψηφιακό νομισματικό σύστημα μέσω του bitcoin, ενώ το Ethereum στοχεύει να καλύψει, μέσω του νομίσματος Ether, περισσότερες εφαρμογές και όχι μόνο οικονομικές συναλλαγές.

Στις τεχνικές τους τώρα διαφορές, ο μέσος χρόνος δημιουργίας ενός μπλοκ στο σύστημα blockchain είναι περίπου 10 λεπτά ενώ στο Ethereum μόνο λίγα δευτερόλεπτα, κατά μέσο όρο 12 δευτερόλεπτα μέσω του πρωτοκόλλου Ghost. Όσον αφορά τώρα την προσφορά τους σε κρυπτονομίσματα, το σύστημα blockchain «δίνει» περισσότερα κρυπτονομίσματα στους χρήστες που έχουν συνεισφέρει περισσότερο στην διαδικασία Mining, ενώ το Ethereum εκτόξευσε το κεφάλαιό του με αποτέλεσμα μέχρι το πέμπτο έτος λειτουργιάς του μόνο τα μισά κρυπτονομίσματα θα έχουν εξορυχθεί.

Μια άλλη στοιχειώδης διαφορά είναι στην ανταμοιβή. Η εξόρυξη bitcoin πέφτει περίπου κάθε τέσσερα χρόνια, ενώ στο Ethereum οι χρήστες-miners ανταμείβονται με βάση τον μαθηματικό αλγόριθμό του για την «απόδειξη εργασίας» που ονομάζεται Ethash, δίνοντας 5 Ether για κάθε νέο μπλοκ.

Επίσης, το Ethereum διαθέτει τον δικό του ολοκληρωμένο εσωτερικό κώδικα Turing, που σημαίνει ότι οτιδήποτε μπορεί να υπολογιστεί με αρκετή υπολογιστική ισχύ και αρκετό χρόνο. Το Bitcoin δεν έχει αυτή τη δυνατότητα. Παρόλο που υπάρχουν σίγουρα πλεονεκτήματα για τον κώδικα Turing, η πολυπλοκότητά του οδήγησε σε επιπλοκές ασφάλειας.

Τέλος, όσον αφορά το κόστος, στο blockchain οι συναλλαγές περιορίζονται από το μέγεθος του μπλοκ κι ανταγωνίζονται μεταξύ τους, ενώ στο Ethereum η κοστολόγηση των συναλλαγών εξαρτάται από τις ανάγκες αποθήκευσης, την πολυπλοκότητα και τη χρήση εύρους ζώνης.

ΚΕΦΑΛΑΙΟ 4: ΣΥΜΠΕΡΑΣΜΑΤΑ

4.1 Σύγκριση Πλαστικό Χρήμα με Ψηφιακό Νόμισμα

Συνοψίζοντας την αναλυτική παρουσίαση των δύο διαφορετικών και σύγχρονων μεθόδων διεκπεραίωσης των οικονομικών συναλλαγών, ακολουθεί μια συγκριτική μελέτη σχετικά με τα πλεονεκτήματα και τα μειονεκτήματα των δύο τρόπων συναλλαγής.

Αρχικά, το σύστημα οικονομικής συναλλαγής με χρήση του πλαστικού χρήματος αποτελεί, επί του παρόντος, μια φιλική προς το χρήστη μέθοδος και κυρίως φαινομενικά ασφαλής. Ο πελάτης, μπορεί να κατανοήσει εύκολα την έννοια της πιστωτικής κάρτας καθώς μπορεί ανά πάσα στιγμή να έχει πρόσβαση στο περιεχόμενο της τραπεζικής του κατάθεσης, γεγονός που του προσφέρει ασφάλεια. Το σύστημα blockchain, όπως και το Ethereum, δεν είναι ιδιαίτερα φιλικό προς το χρήστη, εξαιτίας της αυξημένης χρήσης της τεχνολογίας. Άλλωστε, η ιδέα εικονικού χρήματος δημιουργεί ανασφάλεια και πολλά ερωτηματικά. Άρα, από την πλευρά του χρήστη το σύστημα του πλαστικού χρήματος θεωρείται πιο φιλικό και ασφαλές καθώς πληροί περισσότερο τις προδιαγραφές του μέσου γνωστικού επιπέδου σε αντίθεση με το σύστημα blockchain το οποίο απαιτεί τεχνολογικές γνώσεις για την κατανόηση του τρόπου λειτουργίας του.

Βέβαια, ο κόσμος των επιχειρήσεων είναι άρρηκτα συνδεδεμένος με τον κόσμο της τεχνολογίας. Η πρόοδος στον τομέα της επιχειρηματικότητας προϋποθέτει και πρόοδο στον τομέα της τεχνολογίας. Για τον λόγο αυτό το σύστημα blockchain και το ακόμα πιο μελλοντικό Ethereum, πρόκειται να απασχολήσει ιδιαίτερα τον επιχειρηματικό κόσμο. Το βασικό πλεονέκτημα είναι η απουσία κεντρικής ελεγκτικής δύναμης γεγονός που καθιστά τα διαμοιραζόμενα δεδομένα ασφαλή και το σύστημα ανθεκτικό σε τροποποιήσεις.

Βέβαια, δεν μπορεί να μην υπάρχει ο φόβος εξαιτίας της υποτίμησης του εικονικού νομίσματος bitcoin που είναι ήδη σε χρήση. Οι πιθανές επιθέσεις στην αξία του ψηφιακού νομίσματος, μπορεί να προκαλέσει αμφιβολία και να συνεισφέρει δυσμενώς στην δημιουργία ιεραρχικής εξουσίας στο σύστημα blockchain εξαλείφοντας το σημαντικό πλεονέκτημα της ισότιμης συμμετοχής όλων των κόμβων στο σύστημα. Αυτός ο φόβος, δεν υπάρχει στο πλαστικό χρήμα καθώς υπάρχει επικοινωνία και συναλλαγή μεταξύ δύο οντοτήτων. Στο πλαστικό χρήμα συμμετέχει

η ελεγκτική δύναμη της τράπεζας γεγονός που οδηγεί στην ασφάλιση της προστασίας των συναλλαγών μέσω της κρυπτογραφίας.

4.2 Μελλοντικές εκτιμήσεις

Κάθε τεχνολογική αλλαγή κρίνεται με βάση την πορεία της στο χρόνο. Μπορεί καθετί καινούριο να αποτελεί μια επανάσταση και να ελκύει το κοινό ενδιαφέρον, ωστόσο η πορεία είναι εκείνη που καθιστά μια τεχνολογία σταθερή και ανθεκτική.

Το σύστημα πλαστικού χρήματος έχει αποδείξει την αξία του χρονικά, με ιδιαίτερα την τωρινή χρήση της χρεωστικής κάρτας ως βασικό φορολογικό μέσο συναλλαγής. Το σύστημα blockchain και Ethereum τώρα, είναι σχετικά πρόσφατα συστήματα, που ενώ η εκκίνηση εισαγωγής τους στο οικονομικό σύστημα ήταν ιδιαίτερα ενθαρρυντική, σύμφωνα με κάποιες μελέτες όμως, επικράτησε μια κρίση στην αξία των κρυπτονομισμάτων. Σύμφωνα με την μελέτη[U15],το πρόβλημα εντοπίστηκε στην πτώση της αξίας των κρυπτονομισμάτων bitcoin και Ether σε μία μόλις μέρα έως και 25% χωρίς να καταφέρουν γρήγορα να ανακάμψουν την νομισματική τους αξία. Το λεγόμενο αυτό ζήτημα ονομάστηκε «bubble»[U14],θεωρώντας δηλαδή «φούσκα» την λειτουργία του συστήματος.

Συμπερασματικά λοιπόν, δεν μπορεί να υπάρχει ακριβής εικόνα σχετικά με την μελλοντική εξέλιξη της πορείας του κρυπτονομίσματος. Οι πιο πρόσφατες μελέτες, την χρονιά 2017, έδειξαν ότι κατάφερε να ανταπεξέλθει στην παλαιότερη κρίση και να ανέβει δυναμικά, δημιουργώντας εξαιρετικές επιδόσεις στο κρυπτονόμισμα του. Έτσι, η παλαιότερη ασταθή βάση στην ανθεκτικότητα της διατήρησης της αξίας τους ξεπεράστηκε επιτυχώς. Το μέλλον είναι εκείνο που θα διαλευκάνει αν τελικά το σύστημα blockchain ανήκει στην κατηγορία «bubble» ή τελικά μπορεί να ανταγωνιστεί επάξια το φυσικό χρήμα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία:

[Β1] William Stallings, *Βασικές Αρχές Ασφάλειας Δικτύων*, 3η αμερικανική έκδοση, Αθήνα, Εκδόσεις Κλειδάριθμος.

[Β2] Άρης Αλεξόπουλος & Γιώργος Λαγογιάννης, *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών,* 10η έκδοση (2016), Αθήνα, Εκδόσεις Γιαλός

[Β3] Tanenbaum & Wetherall, *Δίκτυα Υπολογιστών,* 5η αμερικανική έκδοση, Αθήνα, Εκδόσεις Κλειδάριθμος.

Δημοσιεύσεις:

[Δ1]https://dspace.lib.uom.gr/bitstream/2159/2323/4/KatsidouMSc2007.pdf

[Δ2]http://nefeli.lib.teicrete.gr/browse/sdo/ba/2013/MoursellaEleftheria/attached-document-1382436011-535759-16697/MoursellaEleftheria2013.pdf

[Δ3]http://www.tex.unipi.gr/undergraduate/notes/ecom_multimedia/kef7.pdf

[Δ4]https://storj.io/storj.pdf

[Δ5]http://www.hba.gr/5Ekdosis/UplPDFs/deltia/1-2006/101-108.pdf

[Δ6]https://eclass.teicrete.gr/modules/document/file.php/DBI105/%CE%A0%CE%95%CE%A1%CE%99%CE%95%CE%A7%CE%9F%CE%9C%CE%95%CE%9D%CE%9F/%CE%A0%CE%91%CE%A1%CE%9F%CE%A5%CE%A3%CE%99%CE%91%CE%A3%CE%95%CE%99%CE%A3/K.6-/Micro_lectures.29-33.pdf

[Δ7]http://users.sch.gr/geokasap/site/images/pdf/rsa.pdf

[Δ8]http://dspace.lib.ntua.gr/dspace2/bitstream/handle/123456789/6442/kefalad_digitalsignatures.pdf?sequence=3

[Δ9]http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf

[Δ10]file:///C:/Users/%CE%9D%CE%99%CE%9A%CE%91%CE%95%CE%9B%CE%91/Downloads/EPDO_0054.pdf

URLs:

[U1] http://coolweb.gr/ti-einai-xreostiki-karta-pos-leitourgei/

[U2]https://www.e-biografiko.gr/%CE%B4%CE%B9%CE%B1%CF%86%CE%BF%CF%81%CE%AD%CF%82-%CF%80%CE%B9%CF%83%CF%84%CF%89%CF%84%CE%B9%CE%BA%CE%AE%CF%82-%CE%BA%CE%B1%CE%B9-%CF%87%CF%81%CE%B5%CF%89%CF%83%CF%84%CE%B9%CE%BA%CE%AE%CF%82/

[U3]http://coolweb.gr/propliromenes-kartes-information/

[U4]http://caclab.csd.auth.gr/Kerveros.pdf

[U5]http://ebooks.edu.gr/modules/ebook/show.php/DSGL-A114/547/3586,15282/

[U6]http://ebooks.edu.gr/modules/ebook/show.php/DSGYM-C119/464/3085,12349/

[U7]https://effrosyniboutsika.wordpress.com/2017/09/07/%CE%B7-%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1-blockchain-%CF%84%CE%BF-bitcoin-%CE%BA%CE%B1%CE%B9-%CE%AC%CE%BB%CE%BB%CE%B5%CF%82-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD/

[U8] http://www.moneyguru.gr/analyseis/blockchain-i-tehnologia-piso-apo-bitcoin-9452

[U9] http://www.cnn.gr/tech/story/6299/h-elliniki-startup-piso-apo-tin-texnologia-blockchain

[U10]http://www.insomnia.gr/topic/594043-bitcoin-blockchain-%CF%80%CF%81%CE%BF%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1%CF%84%CE%B9%CF%83%CE%BC%CF%8C%CF%82-%CE%BA%CE%B1%CE%B9-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82-%CF%84%CE%B7%CF%82-%CF%84%CE%B5%CF%8

[U11]https://learncryptography.com/cryptocurrency/51-attack

[U12]https://www.huffingtonpost.com/ameer-rosic-/ethereum-vs-bitcoin-whats_b_13735404.html

[U13]http://www.bitclub-greece.gr/exorixi-bitcoin/ethereum/ti-einai

[U14]http://www.fortunegreece.com/article/ine-to-bitcoin-ke-to-ethereum-apla-fouskes/

[U15]http://www.insider.gr/hristika/ependyseis/9959/ethereum-antipalo-deos-toy-bitcoin

[U16]http://www.mixanitouxronou.gr/i-proti-pistotiki-karta-itan-apotelesma-mias-kakias-stigmis-giati-onomastike-dinners-pia-itan-i-proti-chrisi-pou-aforouse-apoklistika-epichirimaties/

[U17]http://hermes.di.uoa.gr/exe_activities/diadiktio/11_____.html

[U18]http://www.teomaragakis.com/el/howto/paypal/

[U19]https://bitcoinx.gr/%CF%80%CF%89%CF%82-%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%BF%CF%8D%CE%BD%CF%84%CE%B1%CE%B9-%CF%84%CE%B1-bitcoins/

Αναφορές Εικόνων:

[A1]https://www.marketwatch.com/story/this-year-will-be-a-turning-point-for-cash-2016-09-26

[A2]https://blog.spreedly.com/2017/05/18/credit-card-vs-debit-card-decline-rates-processing-fees/

[A3]http://searchsecurity.techtarget.com/definition/digital-signature

[A4]http://help.blackberry.com/en/blackberry-dynamics-sdk-ios/current/blackberry-dynamics-sdk-ios-devguide/jxg1474486221930.html

[A5]http://www.linkintime.co.in/tcs/faqs/gfaqs.htm

[A6]https://www.lynda.com/CISSP-tutorials/Create-digital-certificate/516600/556467-4.html

[A7]https://www.researchgate.net/figure/228970093_fig2_Figure-8-System-Architecture-of-Kerberos-8

[A8]https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/

[A9]http://cryptomining-blog.com/tag/bitcoin-vs-ethereum/

[A10]http://fortune.com/2017/06/26/bitcoin-blockchain-cryptocurrency-market/

[A11]https://streetsignals.com/currency/cryptocurrency/missed-bitcoin-dont-miss-ether/