ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΙΔΙΚΕΥΣΗΣ
ΣΤΑ ΕΦΑΡΜΟΣΜΕΝΑ ΜΑΘΗΜΑΤΙΚΑ

Σύγχρονα Συστήματα Κρυπτογράφησης με Εφαρμογή στα Κρυπτονομίσματα

Modern cryptographic systems with cryptocurrency applications

Μεταπτυχιακή Διπλωματική Εργασία

Γεώργιος Θ. Κατωπόδης

Επιβλέπων: Νικόλαος Μπάρδης, Αν. Καθηγητής Σ.Σ.Ε.

Ιανουαρίος 2020

Σύγχρονα Συστήματα Κρυπτογράφησης με Εφαρμογή στα Κρυπτονομίσματα

Γεώργιος Θ. Κατωπόδης

Περίληψη

Η εφεύρεση του bitcoin και των αλυσίδων ομάδων συναλλαγών δεν θα ήταν δυνατή χωρίς την αλματώδη ανάπτυξη που έγινε στο χώρο της κρυπτογραφίας στα τέλη του 20ου αιώνα. Η χρήση κρυπτογραφικών μεθόδων όπως η ψηφιακή υπογραφή, οι συναρτήσεις κατακερματισμού και τα δέντρα Merkle εξασφαλίζουν σε κάθε χρήστη της blockchain ότι οι πληροφορίες που αποθηκεύονται και μεταδίδονται μέσω αυτής είναι επιβεβαιωμένες και ασφαλείς.

Στην παρούσα εργασία αναλύονται εκτενώς οι κρυπτογραφικές μέθοδοι που χρησιμοποιούνται στην blockchain και παρουσιάζεται η λειτουργία του βασικού κρυπτονομίσματος (bitcoin). Επίσης αναφέρονται τα κυριότερα κρυπτονομίσματα και οι διαφορετικές προσεγγίσεις τους στο οικοσύστημα των ψηφιακών νομισμάτων καθώς και οι διαφορετικές χρήσεις της blockchain σε διάφορους τομείς της οικονομίας και του εμπορίου.

Στο τέλος παρουσιάζονται κάποιοι νεώτεροι τύποι ψηφιακής υπογραφής, οι συγκεντρωτικές υπογραφές (aggregated signatures) και εξετάζεται η πιθανή υλοποίησή τους στην blockchain.

Modern cryptographic systems with cryptocurrency applications

George Th. Katopodis

Abstract

The invention of bitcoin and blockchain would not have been possible without the rapid development of cryptography in the late 20th century. The use of cryptographic methods such as digital signature, hash functions, and Merkle trees ensure that every blockchain user is assured that the information stored and transmitted through the blockchain is verified and secure.

In this work, the cryptographic methods used in blockchain are analyzed in detail and the function of the basic cryptocurrency (bitcoin) is presented. Additionally, the main cryptocurrencies and their different approaches to the digital currency ecosystem are mentioned as well as the different uses of blockchain in various sectors of the economy and commerce.

Finally we have chosen to introduce some new types of digital signatures, called aggregated signatures and we also consider their possible implementation in blockchain .

Αφιέρωση

Στους γονείς μου.
Στη σύντροφό μου και στο γιό μας.

Η παρούσα διπλωματική εργασία, εκπονήθηκε για τις ανάγκες της απόκτησης του Μεταπτυχιακού Τίτλου Σπουδών του Προγράμματος Μεταπτυχιακών Σπουδών στα Εφαρμοσμένα Μαθηματικά του Μαθηματικού Τμήματος της Σχολής Θετικών Επιστημών, του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

Τριμελής Επιτροπή

ΕΠΙΒΛΕΠΩΝ:

Νικόλαος Μπάρδης,
Αναπληρωτής Καθηγητής Σ.Σ.Ε.

ΜΕΛΗ:

Κόττα - Αθανασιάδου Ευαγγελία,
Επίκουρη Καθηγήτρια του Τμήματος Μαθηματικών του Ε.Κ.Π.Α.

Δρακόπουλος Μιχάλης,
Επίκουρος Καθηγητής του Τμήματος Μαθηματικών του Ε.Κ.Π.Α.

Ευχαριστίες

Θέλω να ευχαριστήσω τον Καθηγητή Νικόλαο Μπάρδη τόσο για την πρότασή του να ασχοληθώ με αυτό το καινοτόμο θέμα, όσο και για την πολύτιμη βοήθεια και καθοδήγησή του. Επίσης να ευχαριστήσω τη σύζυγό μου Άννα-Μαρία για την στήριξή της κατά την διάρκεια των σπουδών μου.

Περιεχόμενα

Κεφάλαιο 1

Μαθηματικό υπόβαθρο

Το μεγαλύτερο μέρος της σύγχρονης κρυπτογραφίας βασίζεται στην άλγεβρα και στη θεωρία των πρώτων αριθμών. Σε αυτό το κεφάλαιο αναφέρουμε ορισμούς και ιδιότητες βασικών αλγεβρικών δομών όπως ομάδες, δακτύλιοι, σώματα καθώς και στοιχεία από τη θεωρία των ελλειπτικών καμπυλών [1] [2] [3] [4].

1.1 Ακέραιοι

Ορισμός 1.1.1. *Το σύνολο των ακεραίων αριθμών είναι το* $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$.

1.1.1 Διαιρετότητα στο $\mathbb{Z}$

Ορισμός 1.1.2. *Έστω* $a, b \in \mathbb{Z}$. *Λέμε ότι ο* a ***διαιρεί (divides)*** *τον* b *(ισοδύναμα ο* a *είναι διαιρέτης* b*) και συμβολίζουμε* $a|b$*, αν ο* b *είναι ακέραιο πολλαπλάσιο του* a*, δηλαδή* $b = na$, $n \in \mathbb{Z}$. *Διαφορετικά, λέμε ότι ο* a *δεν διαιρεί το* b *και συμβολίζουμε με* $a \nmid b$.

Πρόταση 1.1.1. *(Ιδιότητες Διαιρετότητας) Έστω* $a,\ b,\ c \in \mathbb{Z}$.

(i) $a|a$: *(αυτοπαθής ιδιότητα).*

(ii) Αν $a|b$ *και* $a|c$*, τότε* $a|c$: *(μεταβατική ιδιότητα).*

(iii) Αν $0|a$ *τότε* $a = 0$.

(iv) $a|0, \ \forall\ a \in \mathbb{Z}$.

(v) Αν $a|b$ *και* $a|c$*, τότε* $a|\kappa b + \lambda c$*, για* $\kappa, \lambda \in \mathbb{Z}$.

(vi) Αν $a|b$ *και* $b|a$*, τότε* $b = \pm a$.

(vii) Αν $a|b$ *και* $a, b > 0$*, τότε* $a \leq b$.

(viii) Αν $a|b$ *και* $n \in \mathbb{Z}_{>0}$*, τότε* $a^n|b^n$.

Θεώρημα 1.1.2. ***(Ευκλείδεια Διαίρεση)*** *Έστω $a,\ b \in \mathbb{Z}$ με $a \neq 0$. Τότε υπάρχουν μοναδικοί $q,\ r \in \mathbb{Z}$ τέτοιοι ώστε $b = qa + r$, με $0 \leq r < |a|$.*

Ορισμός 1.1.3. *Τα q και r είναι μοναδικά και καλούνται* ***πηλίκο (quotient)*** *και* ***υπόλοιπο (remainder)*** *αντίστοιχα.*

1.1.2 Διαιρετότητα και πρώτοι αριθμοί

Ορισμός 1.1.4. ***πρώτος (prime)*** *λέγεται ο θετικός ακέραιος $p \neq 1$ του οποίου οι μόνοι διαιρέτες του είναι οι $\pm 1, \pm p$.* ***Σύνθετος (composite)*** *λέγεται ο θετικός ακέραιος n που δεν είναι πρώτος.*

Πρόταση 1.1.3. *Κάθε θετικός ακέραιος $n \neq 1$ γράφεται ως γινόμενο (όχι κατ' ανάγκη διακεκριμένων πρώτων αριθμών. Καθε ακέραιος μεγαλύτερος του 1 έχει πρώτο διαιρέτη.*

Θεώρημα 1.1.4. ***(Ευκλείδης)*** *Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.*

1.1.3 Μέγιστος κοινός διαιρέτης

Ορισμός 1.1.5. *Έστω $a, b \in \mathbb{Z}$, εκ των οποίων ένας τουλάχιστον είναι μη μηδενικός.* ***Μέγιστο κοινό διαιρέτη*** *των a, b καλούμε τον θετικό ακέραιο d για τον οποίο ισχύει ότι*

(i) ο d διαιρεί τους a, b (κοινός),

(ii) αν $c|a$ και $c|b$, τότε $c|d$ (μέγιστος).

Θεώρημα 1.1.5. *Έστω $a, b \in \mathbb{Z}$, εκ των οποίων ένας τουλάχιστον είναι μη μηδενικός. Τότε υπάρχει μοναδικός μέγιστος κοινός διαιρέτης d των a, b ο οποίος ικανοποιεί την ταυτότητα Bezout: $d = xa + yb,\ x, y \in \mathbb{Z}$.*

1.1.4 Αλγεβρικές Δομές

Ομάδες

Ορισμός 1.1.6. *(Ομάδα) Έστω G μη κενό σύνολο και $\cdot : G \times G \to G$ μία πράξη στο G. Το ζεύγος $(G, \cdot)$ θα καλείται* ***ομάδα (group)****, αν:*

(i) $\forall\, a, b \in G$, το $a \cdot b \in G$. :(κλειστότητα),

(ii) $\forall\, a, b, C \in G$, ισχύει $(a \cdot b) \cdot c = a \cdot (b \cdot c)$: (προσεταιριστική ιδιότητα),

(iii) $\exists\, e \in G$ ώστε $a \cdot e = e \cdot a,\ \forall a \in G$:(ύπαρξη ουδετέρου στοιχείου),

(iv) $\forall\, a \in G\ \ \exists\, b \in G$ ώστε $a \cdot b = b \cdot a = e$:(ύπαρξη αντιστρόφου στοιχείου).

Παρατήρηση 1. *Συμβολίζουμε με a^{-1} το αντίστροφο στοιχείο του a.*

Παρατήρηση 2. *Τα στοιχεία e και a^{-1} είναι μοναδικά.*

Ορισμός 1.1.7. *(Αβελιανή ομάδα) Η ομάδα $(G, \cdot)$ λέγεται αντιμεταθετική, μεταθετική ή αβελιανή αν για κάθε $a, b \in G$ ισχύει ότι $a \cdot b = b \cdot a$.*

Ορισμός 1.1.8. *(Τάξη ομάδας) Ορίζουμε ως **τάξη (order)** της ομάδας G το πλήθος των στοιχείων της και συμβολίζουμε με $|G|$. Αν η ομάδα έχει πεπερασμένο πλήθος στοιχείων (finite group) λέμε ότι έχει πεπερασμένη τάξη, διαφορετικά λέμε ότι είναι άπειρης τάξης.*

Παράδειγμα 1. *Αβελιανές ομάδες*

(i) τα $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{C}, +)$ είναι αβελιανές ομάδες με ουδέτερο στοιχείο το 0_R,

(ii) το $(\mathbb{Z}_n, +)$, είναι αβελιανή ομάδα πεπερασμένης τάξης n, με ουδέτερο στοιχείο το $[0]_n$.

Δυνάμεις Στοιχείων

Ορισμός 1.1.9. *) Έστω $(G, \cdot)$ ομάδα με πολλαπλασιαστική δομή, $a \in G$ και $n \in \mathbb{Z}$ με ουδέτερο στοιχείο το e. Ορίζουμε τη n-οστή δύναμη του a, ως:*

$$a^n \coloneqq \begin{cases} aa \dots a \quad (n \text{ φορές}), & n \geq 1 \\ e, & n = 0 \\ a^{-1}a^{-1} \dots a^{-1} \quad (n \text{ φορές}), & n \leq -1 \end{cases} \tag{1.1}$$

Παρατήρηση 3. *Συμβολίζουμε με a^{-1} το αντίστροφο στοιχείο του a.*

Ορισμός 1.1.10. *) Έστω $(G, +)$ ομάδα με προσθετική δομή, $a \in G$ και $n \in \mathbb{Z}$ με ουδέτερο στοιχείο το 0. Ορίζουμε το n-οστό πολλαπλασιο του a, ως:*

$$na \coloneqq \begin{cases} a + a \dots + a \quad (n \text{ φορές}), & n \geq 1 \\ 0, & n = 0 \\ (-a) + (-a) \dots + (-a) \quad (-n \text{ φορές}), & n \leq -1 \end{cases} \tag{1.2}$$

Παρατήρηση 4. *Συμβολίζουμε με a^{-1} το αντίστροφο στοιχείο του a.*

Λήμμα 1.1.6. *Έστω $(G, \cdot)$ ομάδα, $a \in G$ και $n, m \in \mathbb{Z}$. Τότε:*

(i) $a^{n+m} = a^n a^m$

(ii) $(a^n)^m = a^{nm}$

(iii) $(a^{-1})^n = (a^n)^{-1} = a^{-n}$

Αντίστοιχες εκφράσεις ισχύουν για την προσθετική δομή.

Λήμμα 1.1.7. *Έστω G αβελιανή ομάδα, $a, b \in G$ και $n \in \mathbb{Z}$. Τότε $(ab)^n = a^n b^n$.*

Τάξη στοιχείου

Ορισμός 1.1.11. *Έστω $(G, \cdot)$ και $g \in G$. Αν υπάρχει θετικός ακέραιος a για τον οποίο ισχύει ότι $g^a = e$ τότε **τάξη (order)** του g ορίζουμε τον μικρότερο τέτοιο θετικό ακέραιο και συμβολίζουμε με $|g|$. Αν δεν υπάρχει, θα λέμε ότι το στοιχείο g είναι **άπειρης τάξης**.*

Παρατήρηση 5. *(i) Για την $(G, +)$, η τάξη του a είναι ο μικρότερος θετικός ακέραιος κ ώστε $\kappa a = 0$.*

(ii) Ένα στοιχείο μιας ομάδας έχει τάξη 1 ανν είναι το ουδέτερο στοιχείο της ομάδας.

(iii) Τα στοιχεία a και a^{-1} έχουν την ίδια τάξη.

Υποομάδες

Ορισμός 1.1.12. *Έστω $(G, \cdot)$ ομάδα και $G \supseteq H \neq \emptyset$. Καλούμε την H **υποομάδα (subgroup)** της ομάδας G και συμβολίζουμε $H \leq G$ αν είναι ομάδα στην πράξη που επάγει η G στην H. Θα συμβολίζουμε $H < G$ αν $H \leq G$ και $H \neq G$ και τότε η H λέγεται **γνήσια υποομάδα (proper subgroup)** της ομάδας G.*

Πρόταση 1.1.8. *Έστω G ομάδα και $G \supseteq H \neq \emptyset$ Τότε το σύνολο H είναι υποομάδα της G αν και μόνο αν ισχύουν τα ακόλουθα:*

(i) το H είναι κλειστό στον πολλαπλασιασμό, δηλαδή για κάθε h_1, $h_2 \in H$, ισχύει ότι $h_1 h_2 \in H$.

(ii) Για κάθε $h \in H$ ισχύει ότι $h^{-1} \in H$.

Θεώρημα 1.1.9. *Έστω $(G, \cdot)$ ομάδα και $g \in G$. Ορίζουμε την **κυκλική (cyclic)** υποομάδα της G που παράγεται από το στοιχείο g και συμβολίζουμε $< g >$, το σύνολο:*

$$< g > := g^n : n \in \mathbb{Z}. \tag{1.3}$$

Πρόταση 1.1.10. *Έστω G ομάδα και $g \in G$.*

(i) Αν το g έχει άπειρη τάξη n, τότε τα στοιχεία του $< g >= g^n : n \in \mathbb{Z}$ είναι διαφορετικά ανά δύο.

(ii) Αν το g έχει πεπερασμένη τάξη n, τότε $< g >= e, g, g^2, \ldots, g^{n-1}$ και τα στοιχεία είναι διαφορετικά ανά δύο.

Ειδικότερα η τάξη της ομάδας $< g >$ και του στοιχείου g είναι ίσες.

Κυκλικές Ομάδες

Ορισμός 1.1.13. *Έστω $(G, \cdot)$ ομάδα. Το $g \in G$ θα λέγεται **γεννήτορας** της ομάδας G ή θα λέμε ότι **παράγει (generates)** την ομάδα G αν $G =< g >$. Επίσης, η ομάδα G θα λέγεται **κυκλική (cyclic)** αν έχει γεννήτορα.*

Λήμμα 1.1.11. *Έστω G ομάδα πεπερασμένης τάξης και $g \in G$. Το g είναι γεννήτορας της G αν και μόνο αν η τάξη του g είναι ίση με $|G|$.*

Πρόταση 1.1.12. *Έστω G κυκλική ομάδα πεπερασμένης τάξης, με γεννήτορα g. Τότε το g^m είναι γεννήτορας της G αν και μόνο αν $gcd(m, |G|) = 1$.*

1.2 Δακτύλιοι

Ορισμός 1.2.1. *Έστω ένα σύνολο $R \neq \emptyset$ εφοδιασμένο με τις διμελείς πράξεις:*

$$\textit{(πρόσθεση)} + : R \times R \to R \quad \textit{και} \quad \textit{(πολλαπλασιασμό)} \cdot : R \times R \to R$$

*Η τριάδα $(R, +, \cdot)$ λέγεται **δακτύλιος(ring)** εάν ισχύουν οι ιδιότητες:*

(i) Ο $(R, +)$ είναι αβελιανή ομάδα,

(ii) $\forall\, a, b, c \in R$, ισχύει $(a \cdot b) \cdot c = a \cdot (b \cdot c)$: (προσεταιριστική ιδιότητα),

(iii) $\forall\, a, b, c \in R$, ισχύει $a \cdot (b + c) = a \cdot b + a \cdot c$: (αριστερή επιμεριστική ιδιότητα),

(iv) $\forall\, a, b, c \in R$, ισχύει $(a + b) \cdot c = a \cdot c + b \cdot c$: (δεξιά επιμεριστική ιδιότητα).

Το γινόμενο $a \cdot b$ συμβολίζεται ab.

Λήμμα 1.2.1. *Έστω R δακτύλιος. Τότε υπάρχει μοναδικό $b \in R$ ώστε $a + b = b + a = a$ για κάθε $a \in R$. Το στοιχείο αυτό καλείται το **μηδενικό στοιχείο** του R και το συμβολίζουμε με 0_R.*

Λήμμα 1.2.2. *Έστω R δακτύλιος και $a \in R$. Τότε υπάρχει μοναδικό στοιχείο $a^{'} \in R$ ώστε $a + a^{'} = a^{'} + a = 0_R$. Το στοιχείο αυτό καλείται το **αντίθετο** του a και συμβολίζεται με $-a$.*

Ορισμός 1.2.2. *Ενας δακτύλιος R λέγεται **μεταθετικός** αν για κάθε $a, b \in R$ ισχύει ότι $ab = ba$.*

Ορισμός 1.2.3. *Ενα στοιχείο 1_R του R τέτοιο ώστε $1_R \cdot a = a \cdot 1_R = a$ για κάθε $a \in R$ καλείται **μοναδιαίο στοιχείο** ή **μονάδα** του R. Ενας δακτύλιος εφοδιασμένος με ένα τέτοιο στοιχείο λέγεται **μοναδιαίος**.*

1.3 Σώματα

Ορισμός 1.3.1. *Ένας μεταθετικός δακτύλιος R με μονάδα $1_R \neq 0_R$ του οποίου κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο, καλείται **σώμα(field)** και συμβ. με F.*

Πρόταση 1.3.1. *Έστω σώμα F και $a, b \in F$ με $a \neq 0_F$. Τότε η εξίσωση $ax = b$ έχει μοναδική λύση.*

Ορισμός 1.3.2. ***Πεπερασμένο σώμα** καλείται ένα σώμα με πεπερασμένο αριθμό στοιχείων.*

Ορισμός 1.3.3. ***Τάξη (Order)** ενός πεπερασμένου σώματος καλείται το πλήθος των στοιχείων του.*

Πρόταση 1.3.2. *Ένα πεπερασμένο σώμα τάξης q υπάρχει, αν και μόνο αν ο q είναι δύναμη πρώτου αριθμού.*

Πρόταση 1.3.3. *Εάν ο q είναι πρώτος αριθμός τότε υπάρχει μοναδικό πεπερασμένο σώμα τάξης q.*

Ορισμός 1.3.4. *Εάν $q = p^m$ όπου p πρώτος και m θετικός ακέραιος, τότε ο p λέγεται χαρακτηριστική του σώματος $\mathbb{F}_q$ και ο m λέγεται βαθμός επέκτασης του $\mathbb{F}_q$.*

1.3.1 Το πεπερασμένο σώμα $\mathbb{F}_q$

Ορισμός 1.3.5. *Έστω p πρώτος αριθμός. Το πεπερασμένο σώμα $\mathbb{F}_q$, καλείται πρώτο σώμα, εάν αποτελείται από ένα σύνολο ακεραίων $\{0, 1, 2, \ldots, p-1\}$, εφοδιασμένο με τις παρακάτω πράξεις:*

(i) Πρόσθεση(modulo p): Έστω $a, b \in \mathbb{F}_p$. Τότε $a + b = r$, όπου r το υπόλοιπο της διαίρεσης του $a + b$ με το p, με $0 \leq r \leq p - 1$.

(ii) Πολλαπλασιασμός(modulo p): Έστω $a, b \in \mathbb{F}_p$. Τότε $a \cdot b = s$, όπου s το υπόλοιπο της διαίρεσης του $a \cdot b$ με το p, με $0 \leq s \leq p - 1$.

(iii) Αντίστροφο στοιχείο: Έστω a μη μηδενικό στοιχείο του $\mathbb{F}_p$. Τό αντίστροφο στοιχείο του a modulo p, είναι ο μοναδικός ακέραιος $c \in \mathbb{F}_p$ για τον οποίον ισχύει ότι $a \cdot c = 1_{\mathbb{F}_p}$ και συμβολίζεται με a^{-1}.

1.4 Ελλειπτικές Καμπύλες

Εισαγωγή

Τις τελευταίες δεκαετίες η θεωρία των ελλειπτικών καμπύλων πάνω σε πεπερασμένα σώματα έχει βρει εφαρμογή στην κρυπτογραφία. Ο βασικός λόγος είναι ότι οι ελλειπτι-

κές καμπύλες είναι μία ανεξάντλητη πηγή πεπερασμένων αβελιανών ομάδων, οι οποίες, ακόμα και εάν είναι μεγάλες, υπόκεινται σε υπολογισμούς λόγω της πλούσιας δομής τους. Οι ελλειπτικές καμπύλες είναι το φυσικό ανάλογο των πολλαπλασιαστικών ομάδων των σωμάτων. Τα βασικά πλεονεκτήματα των κρυπτοσυστήματων ελλειπτικής καμπύλης επί πεπερασμένου σώματος που βασίζονται στο πρόβλημα του διακριτού λογάριθμου, σε σχέση με το κρυπτοσύστημα RSA που βασίζεται στην πρακτική δυσκολία παραγοντοποιήσης του γινομένου δύο μεγάλων πρώτων αριθμών, είναι ότι η εύρεση του λογαρίθμου είναι πολύ πιό δύσκολη από την παραγοντοποίηση κάνοντας έτσι την χρήση επίθεσης ωμής δύναμης (brute force attack) αναποτελεσματική και επιπλέον τα κλειδιά που δημιουργούνται με την κρυπτογράφηση ECC(Elliptic Curve Cryptography) είναι μικρότερα σε μήκος και το ίδιο ισχυρά σε σχέση με τα μεγαλύτερα κλειδιά που δημιουργούνται από τον RSA. Αυτό έχει σαν αποτέλεσμα να χρειάζεται μικρότερη μνήμη και μικρότερη υπολογιστική ισχύς σε σχέση με κρυπτοσυστήματα που χρησιμοποιούν τον RSA. Έτσι επιτυγχάνεται γρηγορότερη παραγωγή κλειδιών με αποτέλεσμα παραγωγή πιστοποιητικών μικρότερου μεγέθους με το ίδιο επίπεδο ασφάλειας. Επίσης η μικρότερη υπολογιστική ισχύς έχει επιπλέον το πλεονέκτημα κατανάλωσης λιγότερης ηλεκτρικής ενέργειας. Για αυτούς τους λόγους, η συνεισφορά τους στην ασφάλεια των ψηφιακών υπογραφών και των κρυπτογραφικών συστημάτων δημοσίου κλειδιού είναι εντυπωσιακή.

Ελλειπτικές καμπύλες πάνω στο $\mathbb{F}_p$

Ορισμός 1.4.1. *Έστω $p > 3$ πρώτος αριθμός. Μία ελλειπτική καμπύλη E πάνω στο σώμα $\mathbb{F}_p$ ορίζεται από μία εξίσωση της μορφής:*

$$y^2 = x^3 + ax + b \tag{1.4}$$

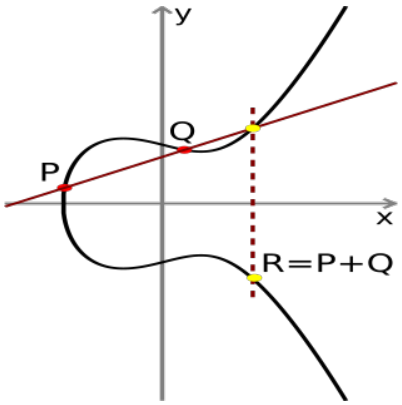
όπου $a, b \in \mathbb{F}_p$ και $4a^3 + 27b^2 \not\equiv 0 \,(\mathrm{mod} p)$. Το σύνολο $E(\mathbb{F}_p)$ αποτελείται από όλα τα σημεία $(x, y),\ \ x \in \mathbb{F}_p,\ \ y \in \mathbb{F}_p$ που ικανοποιούν την εξίσωση, μαζί με ένα φανταστικό σημείο $\mathcal{O}$ ή $O_\infty = (o_\infty, o_\infty)$ που το ονομάζουμε *σημείο στο άπειρο*.

Παρατήρηση 6. *Από την γραφική παράσταση της ελλειπτικής καμπύλης βλέπουμε ότι:*

(i) Η ελλειπτική καμπύλη είναι συμμετρική ως προς τον άξονα x. Αν $(x, y) \in E(\mathbb{F}_p)$, τότε και $(x, -y) \in E(\mathbb{F}_p)$ και το άθροισμα των τεταγμένων τους είναι ίσο με μηδέν.

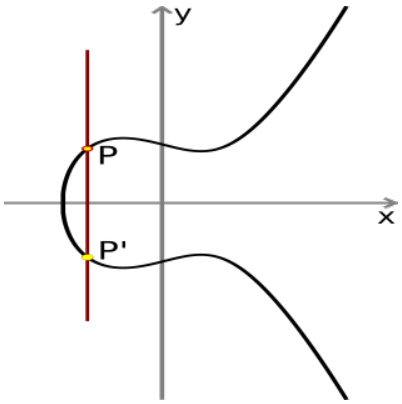
(ii) Κάθε ευθεία που διέρχεται από δύο τυχαία σημεία της ελλειπτικής καμπύλης, τέμνει την καμπύλη αυτή, σε ένα τρίτο ακόμη σημείο. Προκύπτει άμεσα από το Θεώρημα του Bezout [5].

Συμβολίζουμε με $\mathcal{P} + \mathcal{Q}$ το σημείο τομής της ελλειπτικής καμπύλης με την ευθεία που διέρχεται από το $\mathcal{P}$ και ένα σημείο $\mathcal{Q}$. Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης που σαν αποτέλεσμα έχει ένα τρίτο σημείο της ελλειπτικής καμπύλης, χρησιμοποιεί τον *κανόνα χορδής και εφαπτομένης*. Με αυτή την πράξη, το σύνολο $E(\mathbb{F}_p)$ γίνεται αβελιανή ομάδα με ουδέτερο στοιχείο το $\mathcal{O}$. Τάξη της ελλειπτικής καμπύλης πάνω στο σώμα $\mathbb{F}_p$, καλούμε το πλήθος των στοιχείων της ομάδας $E(\mathbb{F}_p)$. Η ομάδα αυτή χρησιμοποιείται για την κατασκευή κρυπτογραφικών συστημάτων ελλειπτικής καμπύλης.



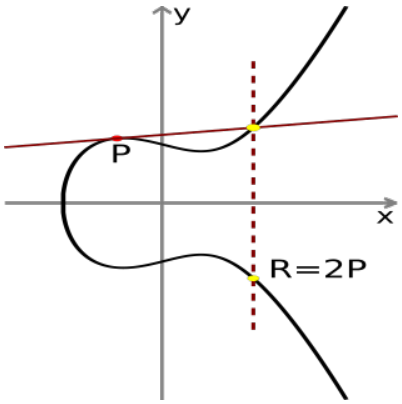
Σχήμα 1.1: Άθροισμα σημείων ελλειπτικής καμπύλης.

Η πρόσθεση αυτή εξηγείται καλύτερα γεωμετρικά (βλέπε σχήμα 1.1). Έστω $\mathcal{P} = (x_1, y_1)$ και $\mathcal{Q} = (x_2, y_2)$ δύο διακριτά σημεία της ελλειπτικής καμπύλης E. Το άθροισμα των $\mathcal{P}$ και $\mathcal{Q}$ συμβολίζεται ως $\mathcal{R} = (x_3, y_3)$, και ορίζεται ως εξής: Φέρνουμε μία ευθεία που διέρχεται από τα σημεία $\mathcal{P}$ και $\mathcal{Q}$. Η ευθεία αυτή τέμνει την ελλειπτική καμπύλη σε ένα τρίτο σημείο. Τότε το $\mathcal{R}$ είναι η ανάκλαση αυτού του σημείου στον άξονα x.



Σχήμα 1.2: Συμμετρικό και ουδέτερο στοιχείο.

Συμβολίζουμε με $\mathcal{P}'$ το συμμετρικό ενός σημείου $\mathcal{P}$ της ελλειπτικής καμπύλης ως προς τον άξονα των x. Εάν $\mathcal{P} = (x_1, y_1)$ τότε $\mathcal{P}' = (x_1, -y_1)$ οπότε $\mathcal{P} + \mathcal{P}' = \mathcal{O}$ το ουδέτερο στοιχείο της πρόσθεσης. Το $\mathcal{O}$ βρίσκεται στο άπειρο της κάθετης ευθείας που διέρχεται από τα σημεία $\mathcal{P}$ και $\mathcal{P}'$, (βλέπε σχήμα 1.2).



Σχήμα 1.3: Πρόσθεση σημείου με τον εαυτό του.

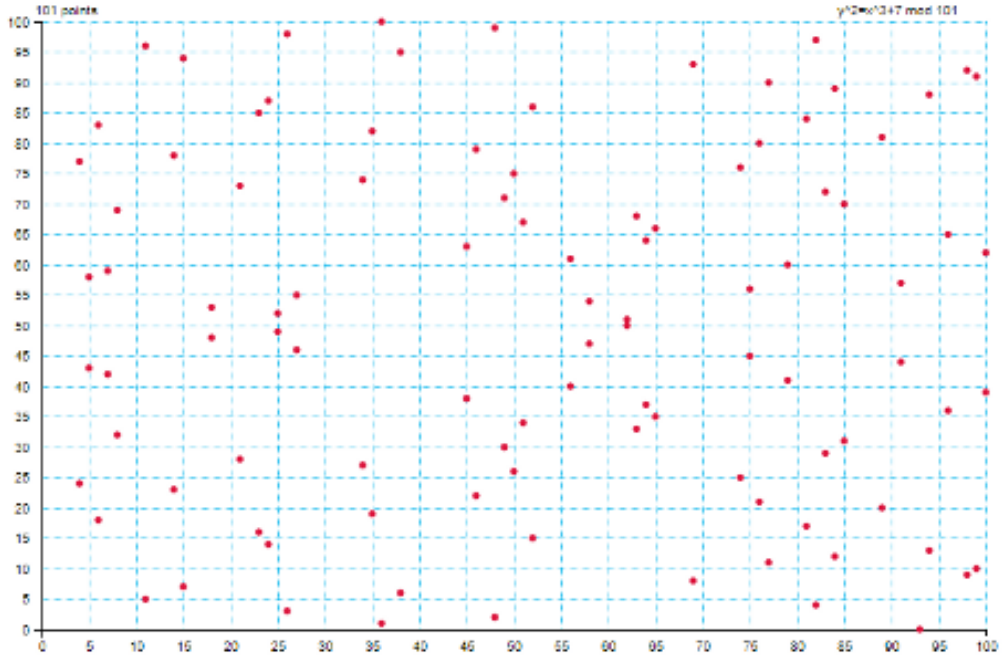
Εάν $\mathcal{P} = (x_1, y_1)$ τότε το άθροισμα $\mathcal{P} + \mathcal{P} = 2\mathcal{P}$ το συμβολίζουμε $\mathcal{R} = (x_3, y_3)$ και ορίζεται ως εξής: πρώτα φέρνουμε μία εφαπτομένη ευθεία στο σημείο $\mathcal{P}$ της ελλειπτικής καμπύλης. Η ευθεία αυτή τέμνει την καμπύλη σε ένα δεύτερο σημείο. Τότε το σημείο $\mathcal{R}$ είναι η ανάκλαση του στον άξονα των x, (βλέπε σχήμα 1.3).

Χρησιμοποιώντας την πρόσθεση που ορίσαμε παραπάνω, ορίζουμε μία πράξη πολλαπλασιασμού ως εξής:

Εάν $\mathcal{P}$ ένα σημείο της ελλειπτικής καμπύλης και k φυσικός αριθμός τότε

$$k\mathcal{P} = \mathcal{P} + \mathcal{P} \ldots \mathcal{P}, \qquad (k \text{ φορές}). \tag{1.5}$$

Τα παραπάνω σχήματα αφορούν ελλειπτικές καμπύλες πάνω στο σώμα $\mathbb{R}$. Σε ένα πεπερασμένο σώμα $\mathbb{F}_{\text{!}}$ οι γραφικές παραστάσεις των ελλειπτικών καμπύλων είναι διαφορετικές. Για παράδειγμα η ελλειπτική καμπύλη $E: \ y^2 = x^3 + 7 \mod 101$ επί του $\mathbb{F}_{101}$ έχει την ακόλουθη γραφική παράσταση, (σχήμα 1.4).



Σχήμα 1.4: Ελλειπτική καμπύλη επί πεπερασμένου σώματος.

Κεφάλαιο 2

Κρυπτογραφία

2.1 Εισαγωγή

Κρυπτογραφία είναι η επιστήμη που ασχολείται με την μελέτη, χρήση και ανάπτυξη τεχνικών κρυπτογράφησης και αποκρυπτογράφησης, με σκοπό την δημιουργία κρυπτογραφικών συστημάτων που έχουν στόχο την απόκρυψη των περιεχομένων των μηνυμάτων (ή των αποθηκευμένων δεδομένων) σε μία μορφή που να μην παρέχει καμμία πληροφορία για το περιεχόμενο αυτών σε μη εξουσιοδοτημένες οντότητες, καθώς και την διευκόλυνση της ανίχνευσης των κακόβουλων μετατροπών σε αυτά [6].

Ορισμός 2.1.1. ***Κρυπτανάλυση*** *(cryptanalysis) είναι η μελέτη για την επινόηση και δημιουργία μεθόδων και τεχνικών με σκοπό την εξαγωγή μέρους ή όλης της κρυπτογραφημένης πληροφορίας, χωρίς την γνώση του κρυφού μετασχηματισμού (κλειδιού) που χρησιμοποιήθηκε για την κρυπτογράφηση αυτής της πληροφορίας.*

2.2 Συνθήκες Ασφαλείας

Οι βασικές συνθήκες που πρέπει να ικανοποιεί ένα κρυπτογραφικό σύστημα είναι οι ακόλουθες:

- **Εμπιστευτικότητα** (confidentiality): είναι η υπηρεσία που εξασφάλιζει την μη ανάγνωση των πληροφοριών από μη εξουσιοδοτημένες οντότητες.
- **Αυθεντικότητα** (authentication): είναι η υπηρεσία που πιστοποιεί την αυθεντικότητα των χρηστών (entity authentication) δηλαδή πιστοποιεί ότι κάθε οντότητα είναι αυτή που ισχυρίζεται ότι είναι, καθώς και την ακρίβεια των πληροφοριών (data origin authentication) δηλαδή πιστοποιεί την προέλευση, την ημερομηνία προέλευσης, τον χρόνο αποστολή καθώς και το περιεχόμενο αυτών.

- **Ακεραιότητα Δεδομένων** (data integrity): είναι η υπηρεσία που αντιμετωπίζει την μη εξουσιοδοτημένη τροποποίηση (ή και αντιγραφή) των δεδομένων.
- **Μη-απάρνηση** (non-repudiation): είναι η υπηρεσία που εμποδίζει μία οντότητα από το να αρνηθεί την επικοινωνία καθώς και να αρνηθεί δεσμεύσεις ή ενέργειες που προέκυψαν από αυτήν ή κατά την διάρκειά της.
- **Διαθεσιμότητα** (availability): είναι η υπηρεσία που εξασφαλίζει ότι οι εξουσιοδοτημένες οντότητες έχουν πρόσβαση στις πληροφορίες του δικτύου όταν και όποτε τις χρειαστούν.

2.3 Ασύμμετρη Κρυπτογραφία

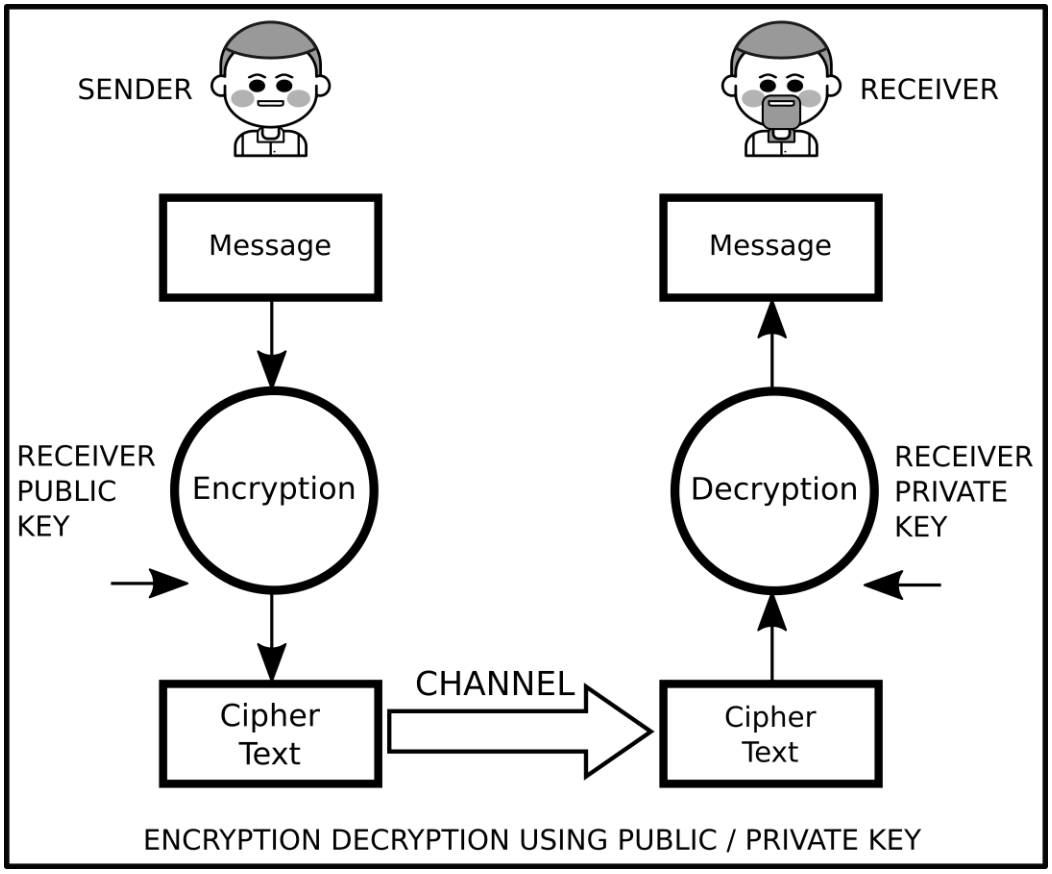
Η ασύμμετρη κρυπτογραφία αναφέρεται σε ένα τύπο κρυπτογραφίας όπου το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφησή τους. Γνωστή και ως **κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography)**, χρησιμοποιεί δημόσια και ιδιωτικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Επίσης χρησιμοποιείται για την υπογραφή μηνυμάτων από τον αποστόλεα και την επαλήθευση και αυθεντικότητα αυτών από τον λήπτη.

Το σχήμα 2.1 εξηγεί πως ο αποστολέας κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο μήνυμα μεταδίδεται ελεύθερα στο δίκτυο και φθάνει στον παραλήπτη. Ο παραλήπτης το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί. Με αυτό τον τρόπο το ιδιωτικό κλειδί παραμένει στα χέρια του παραλήπτη και δεν χρειάζεται διαμοιρασμός των κλειδιών για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων σε αντίθεση με την συμμετρική κρυπτογράφηση.

Το σχήμα 2.2 εξηγεί πως η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται για την επαλήθευση και την ακεραιότητα του ληφθέντος μηνήματος από τον παραλήπτη. Στο σύστημα αυτό, ο αποστολέας υπογράφει τα δεδομένα χρησιμοποιώντας το ιδιωτικό του κλειδί και τα μεταδίδει μέσω του δικτύου στον παραλήπτη. Όταν ο παραλήπτης λάβει τα δεδομένα χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να επικυρώσει την ακεραιότητα των δεδομένων. Σε αυτό το μοντέλο δεν πραγματοποιείται καμμία κρυπτογράφηση και χρησιμοποιείται μόνο για επικύρωση και αυθεντικοποίηση των δεδομένων.

Ιδιωτικά and Δημόσια Κλειδιά

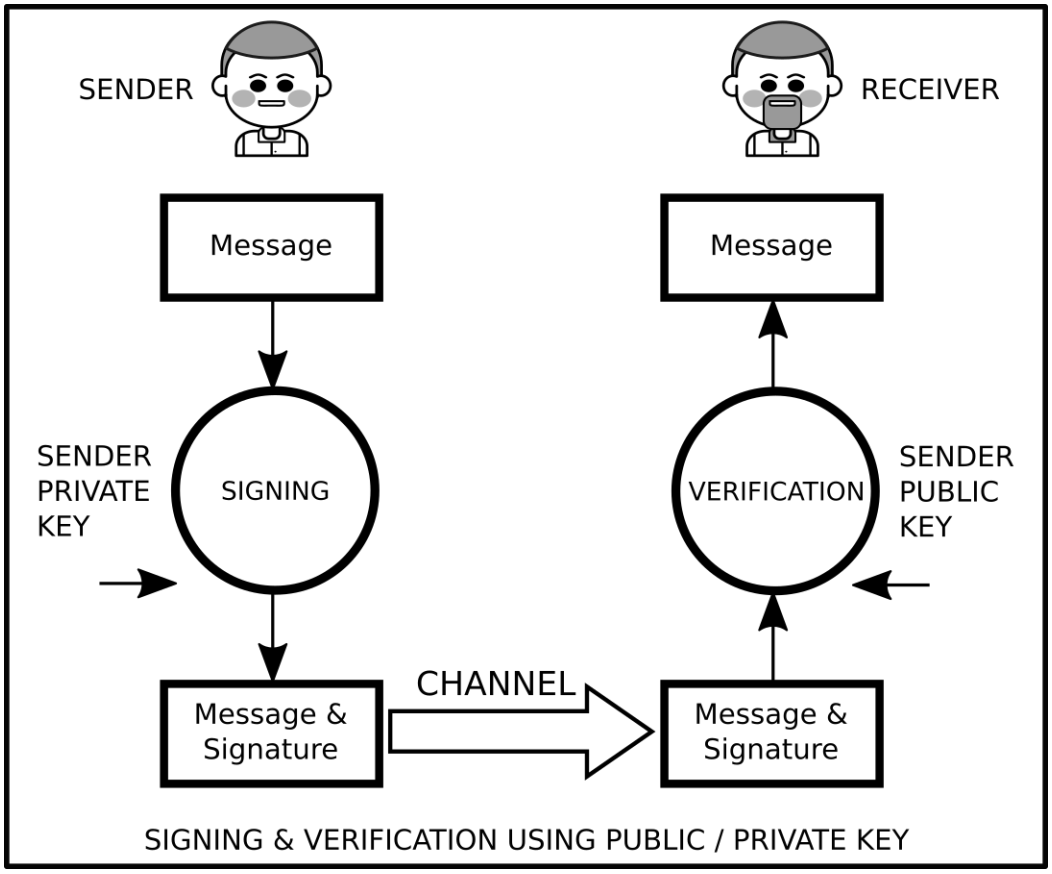
Ιδιωτικό κλειδί καλείται ένας τυχαία παραγόμενος αριθμός ο οποίος είναι μυστικός και φυλάσσεται ιδιωτικά από τον χρήστη. Το ιδιωτικό κλειδί πρέπει να φυλάσσεται και να



Σχήμα 2.1: Κρυπτογράφηση/Αποκρυπτογράφηση με χρήση δημοσίου/ιδιωτικού κλειδιού.

προστατεύεται από τον ιδιοκτήτη, διαφορετικά το όλο σχήμα της κρυπτογραφίας δημοσίου κλειδιού τίθεται σε κίνδυνο, αφού αυτό το ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων.

Το **Δημόσιο κλειδί** είναι το δημόσιο μέρος του ζεύγους ιδιωτικό-δημόσιο κλειδί. Είναι γνωστό δημόσια και δημοσιεύεται από τον κάτοχο του ιδιωτικού κλειδιού. Οποιοσδήποτε θελήσει να στείλει κάποιο κρυπτογραφημένο μήνυμα στον κάτοχο του δημοσίου κλειδιού μπορεί να το κάνει κρυπτογραφώντας το μήνυμα με το δημόσιο κλειδί και αποστέλλοντάς το στον κάτοχο του ιδιωτικού κλειδιού. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί.



Σχήμα 2.2: Μοντέλο συστήματος υπογραφής με κρυπτογραφία δημοσίου κλειδιού.

2.4 ECDSA

Το πρόβλημα του διακριτού λογαρίθμου επί ελλειπτικής καμπύλης, βασίζεται στην ιδέα ότι κάτω από συγκεκριμένες συνθήκες, όλα τα σημεία μίας ελλειπτικής καμπύλης σχηματίζουν μία κυκλική ομάδα.

Σε μία ελλειπτική καμπύλη, το δημόσιο κλειδί είναι ένα τυχαίο πολλαπλάσιο ενός σημείου G της ελλειπτικής καμπύλης, που το καλούμε σημείο βάσης ή γεννήτορα ενώ το ιδιωτικό κλειδί είναι ένας τυχαία επιλεγμένος ακέραιος που χρησιμοποιείται για να δημιουργήσει το πολλαπλάσιο αυτό.

Το **πρόβλημα διακριτού λογαρίθμου επί ελλειπτικής καμπύλης** (elliptic curve discrete logarithm problem-ECDLP) είναι το ακόλουθο: δοσμένης μίας ελλειπτικής καμπύλης ορισμένης επί ενός σώματος $\mathbb{F}_p$, ενός σημείου $\mathcal{P} \in E(\mathbb{F}_p)$ τάξης n, και ενός σημείου $\mathcal{Q} = k\mathcal{P}$ όπου $0 \leq k \leq n-1$, να υπολογιστεί το k.

2.4.1 Εισαγωγή

Ο ECDSA (Elliptic Curve Digital Signature Algorithm) [7] είναι το βασισμένο στις ελλειπτικές καμπύλες ανάλογο του DSA (Digital Signature Algorithm). Ο αλγόριθμος ψηφιακής υπογραφής DSA (Digital Signature Algorithm) καθορίστηκε στο πρότυπο Federal Information Processing Standard (FIPS) με τίτλο Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard-DSS) [8]. Η ασφάλειά του βασίζεται στην δυσκολία εύρεσης υπολογιστικής λύσης στο πρόβλημα του διακριτού λογαρίθμου σε υποομάδες με τάξη πρώτο αριθμό του $\mathbf{Z}_p^*$.

Η πρώτη χρήση των ελλειπτικών καμπύλων στην κρυπτογραφία ήταν ο αλγόριθμος παραγοντοποίησης ελλειπτικών καμπύλων του H. W. Lenstra [9]. Εμπνευσμένοι από αυτόν, οι Neal Koblitz [10] και Victor Miller [11] εφηύραν ταυτόχρονα το 1985 τα κρυπτοσυστήματα ελλειπτικής καμπύλης (Elliptic vurve cryptosystems-ECC). Είναι τα βασισμένα στις ελλειπτικές καμπύλες ανάλογα, των παλαιότερων κρυπτοσυστημάτων διακριτού λογαρίθμου (discrete logarithm problem), στα οποία η υποομάδα του $\mathbf{Z}_p^*$ έχει αντικατασταθεί από την ομάδα των σημείων μίας ελλειπτικής καμπύλης επί ενός πεπερασμένου σώματος. Η μαθηματική βάση για την ασφάλεια των κρυπτοσυστημάτων ελλειπτικής καμπύλης βασίζεται αντίστοιχα στην δυσκολία εύρεσης υπολογιστικής λύσης στο πρόβλημα του διακριτού λογαρίθμου επί ελλειπτικής καμπύλης (elliptic curve discrete logarithm problem-ECDLP).

Δεδομένου ότι το ECDLP φαίνεται να είναι σημαντικά δυσκολότερο από το DLP, η αντοχή ανά κλειδί ανά bit είναι ουσιαστικά μεγαλύτερη σε συστήματα ελλειπτικών καμπυλών σε σχέση με τα συμβατικά διακριτά συστήματα λογαρίθμων. Έτσι στα ECC μπορούν να χρησιμοποιηθούν μικρότεροι παραμέτροι, αλλά με ισοδύναμα επίπεδα ασφάλειας, σε σχέση με συστήματα DL. Τα πλεονεκτήματα από τις μικρότερες παραμέτρους περιλαμβάνουν πιο γρήγορους υπολογισμούς και μικρότερα κλειδιά και πιστοποιητικά. Αυτά τα πλεονεκτήματα είναι σημαντικά σε περιπτώσεις που η επεξεργαστική ισχύς, ο χώρος αποθήκευσης, το εύρος ζώνης ή η κατανάλωση ηλεκτρικής ενέργειας είναι περιορισμένη.

2.4.2 ECDSA domain parameters

Οι παράμετροι για τον ECDSA συνίστανται από μία κατάλληλα επιλεγμένη ελλειπτική καμπύλη E, ορισμένη πάνω σε ένα πεπερασμένο σώμα $\mathbb{F}_q$ χαρακτηριστικής p, και ενός σημείου βάσης (base point) ή γεννήτορα (generator) G που ανήκει στην $E(\mathbb{F}_q)$.

Οι παράμετροι αυτοί αποτελούνται από:

1. ένα σώμα με q στοιχεία όπου είτε $q = p$ (με $p > 2$, p πρώτος) είτε $q = 2^m$,
2. δύο στοιχεία a, b στο $\mathbb{F}_q$, τα οποία ορίζουν την εξίσωση της ελλειπτικής καμπύλης E

επί του $\mathbb{F}_q$ (π.χ $y^2 = x^3 + ax + b$) για $p > 3$),

3. Δύο στοιχεία x_G και y_G στο $\mathbb{F}_q$ τα οποία ορίζουν ένα σημείο $G = (x_G, y_G)$ με τάξη πρώτο αριθμό, στην $E(\mathbb{F}_q)$,
4. την τάξη n του στοιχείου G με $n > 2^{160}$ και $n > 4\sqrt{q}$.
5. τον συμπαράγοντα (cofactor) $h = \#E(\mathbb{F}_q)/n$ όπου $\#E(\mathbb{F}_q)$ το πλήθος των σημείων της ελλειπτικής καμπύλης.

2.4.3 Ζεύγη κλειδιών του ECDSA

Ένα ζεύγος κλειδιών του ECDSA σχετίζεται άμεσα με τις παραμέτρους μίας ελλειπτικής καμπύλης. Το δημόσιο κλειδί είναι ένα τυχαίο πολλαπλάσιο του γεννήτορα G και το ιδιωτικό κλειδί είναι ένας ακέραιος που χρησιμοποιείται για να παραχθεί αυτό το πολλαπλάσιο.

2.4.4 Παραγωγή του ζεύγους κλειδιών

Το ζεύγος κλειδιών μίας οντότητας A σχετίζεται με το σύνολο παραμέτρων της ελλειπτικής καμπύλης $D = (q, a, b, G, n, h)$. Η σχέση αυτή μπορεί να επιβεβαιωθεί κρυπτογραφικά είτε με χρήση πιστοποιητικών από κάποια κεντρική αρχή, είτε από ένα γενικό πλαίσιο στο οποίο έχουν συμφωνήσει όλες οι οντότητες (π.χ όλες οι οντότητες χρησιμοποιούν τις ίδιες παραμέτρους).

Παραγωγή του ζεύγους κλειδιών με ECDSA

Για την παραγωγή κλειδιών με χρήση του ECDSA κάθε οντότητα A κάνει τα εξής:

1. Επιλέγε ένα τυχαίο ή ψευδοτυχαίο ακέραιο d στο διάστημα $[1, n-1]$.
2. Υπολογίζει $Q = dG$.
3. Το δημόσιο κλειδί της οντότητας A είναι το Q ενώ το ιδιωτικό της κλειδί είναι το d.

2.4.5 Επικύρωση του δημοσίου κλειδιού

Μέθοδοι επικύρωσης δημοσίων κλειδιών

Η διασφάλιση ότι ένα δημόσιο κλειδί Q είναι έγκυρο μπορεί να εξασφαλιστεί χρησιμοποιώντας κάποια από τις παρακάτω μεθόδους.

1. Η οντότητα A παράγει μόνη της το δημόσιο κλειδί Q χρησιμοποιώντας ένα αξιόπιστο σύστημα.

2. Η οντότητα A λαμβάνει την διαβεβαίωση από μία κεντρική αρχή ότι το Q παράχθηκε χρησιμοποιώντας ένα αξιόπιστο σύστημα.
3. Η οντότητα A λαμβάνει την διαβεβαίωση από ένα αξιόπιστο μέρος T (π.χ μία αρχή έκδοσης πιστοποιητικών), ότι το T έχει εκτελέσει σαφή επικύρωση του δημόσιου κλειδιού της A χρησιμοποιώντας τον ακόλουθο αλγόριθμο.
4. Η οντότητα A εκτελεί σαφή επικύρωση του δημόσιου κλειδιού χρησιμοποιώντας τον παρακάτω αλγόριθμο.

Αλγόριθμος 2.4.1. *ΕΠΙΚΥΡΩΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ECDSA*

Είσοδος: Ένα δημόσιο κλειδί $Q = (x_Q, y_Q)$ *με παραμέτρους* (q, a, b, G, n, h).

Έξοδος: Αποδοχή ή απόρριψη της εγκυρότητας του Q.

1. *Έλεγχος εάν* $Q \neq \mathcal{O}$
2. *Έλεγχος εάν τα* x_Q *και* y_Q *είναι στοιχεία του* $\mathbb{F}_q$ (*π.χ, για* $q = p$ *να είναι ακέραιοι στο διάστημα* $[0, p-1]$).
3. *Έλεγχος εάν το* Q *ανήκει στην ελλειπτική καμπύλη που ορίζεται από τα* a *και* b.
4. *Έλεγχος ότι* $nQ = \mathcal{O}$.
5. *Εάν αποτύχει ο οποιοσδήποτε έλεγχος, τοτε το* Q *δεν είναι έγκυρο. Διαφορετικά το* Q *είναι έγκυρο.*

2.4.6 Απόδειξη κατοχής ιδωτικού κλειδιού

Εάν μία οντότητα C μπορεί να πιστοποιήσει ότι το δημόσιο κλειδί μίας οντότητας A είναι δικό της, τότε η C μπορεί να ισχυριστεί ότι τα υπογεγραμμένα μηνύματα της A προήλθαν από την C. Για να αποφευχθεί αυτό, μία κεντρική αρχή (Central Authority-CA) πρέπει να απαιτήσει από όλες τις οντότητες A να αποδεικνύουν ότι κατέχουν τα ιδιωτικά κλειδιά που αντιστοιχούν στα αντίστοιχα δημόσια κλειδιά τους, πριν η CA πιστοποιήσει ότι το δημόσιο κλειδί ανήκει στην A. Η απόδειξη της κατοχής γίνεται με διάφορους τρόπους, για παράδειγμα με το να απαιτηθεί από την A να υπογράψει ένα μήνυμα επιλογής της CA, ή χρησιμοποιώντας τεχνικές μηδενικής γνώσης (zero proof knowledge) [12] [13]. Σημειώνεται ότι η απόδειξη κατοχής ιδιωτικού κλειδιού παρέχει διαφορετικές διαβεβαιώσεις από την επικύρωση του δημόσιου κλειδιού. Το πρώτο αποδεικνύει την κατοχή ενός ιδιωτικού κλειδιού, παρόλο που μπορεί να αντιστοιχεί σε ένα μη έγκυρο δημόσιο κλειδί ενώ ενώ το τελευταίο αποδεικνύει την εγκυρότητα ενός δημόσιου κλειδιού, αλλά όχι την ιδιοκτησία του αντίστοιχου ιδιωτικού κλειδιού. Η πραγματοποίηση και των δύο παρέχει ένα υψηλό επίπεδο ασφάλειας.

2.4.7 Παραγωγή και επικύρωση υπογραφής ECDSA

Ψηφιακή υπογραφή

Η ψηφιακή υπογραφή είναι ένα κρυπτογραφικό σύστημα που ικανοποιεί τις συνθήκες ασφαλείας της αυθεντικότητας (authentication), της εξουσιοδότησης (authorization) και της μή απάρνησης (non-repudiation). Χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού εγγράφου. Ο σκοπός μίας ψηφιακής υπογραφής είναι να συνδέσει μία οντότητα με ένα κομμάτι πληροφορίας. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι αυτό δεν αλλοιώθηκε ή παραποιήθηκε κατά την μεταφορά.

Παραγωγή υπογραφής ECDSA

Για να υπογράψει ένα μήνυμα m, μία οντότητα A με παραμέτρους ελλειπτικής καμπύλης $D = (q, a, b, G, n, h)$ και ζεύγος κλειδιών (d, Q) κάνει τα εξής:

1. Επιλογή ένός τυχαίου ή ψευδοτυχαίου ακεραίου k, με $1 \leq k \leq n - 1$.
2. Υπολογισμός του γινομένου $kG = (x_1, y_1)$ και μετατροπή του x_1 σε ακέραιο $\bar{x}_1$.
3. Υπολογισμός του $r = x_1 \mod n$. Αν $r = 0$ τότε πήγαινε στο βήμα 1.
4. Υπολογισμός του $k^{-1} \mod n$.
5. Υπολογισμός του SHA-2(m) και μετατροπή αυτής της συμβολοσειράς (bitstring) σε ένα ακέραιο e.
6. Υπολογισμός του $s = k^{-1}(e + dr) \mod n$. Εάν $s = 0$ τότε πήγαινε στο βήμα 1.
7. Η υπογραφή της οντότητας A για το μήνυμα m είναι το (r, s).

Επικύρωση υπογραφής ECDSA

Για να επικυρώσει μία οντότητα B την υπογραφή (r, s) σε ένα μήνυμα m μίας οντότητας A, αποκτά ένα γνήσιο αντίγραφο των παραμέτρων $D = (q, a, b, G, n, h)$ που χρησιμοποιεί η A καθώς και το σχετιζόμενο με αυτές δημόσιο κλειδί της. Κατόπιν πράττει ως εξής:

1. Επιβεβαιώνει ότι οι r και s είναι πράγματι ακέραιοι στο διάστημα $[1, n - 1]$.
2. Υπολογισμός του SHA-2(m) και μετατροπή αυτής της συμβολοσειράς (bitstring) σε ένα ακέραιο e.
3. Υπολογισμός του $w = s^{-1} \mod n$
4. Υπολογισμός του γινομένου $u_1 = ew \mod n$ και του $u_2 = rw \mod n$.
5. Υπολογισμός του $X = u_1G + u_2Q$.

6. Εάν $X = \mathcal{O}$, τότε η υπογραφή απορρίπτεται. Διαφορετικά, γίνεται μετατροπή της x συντεταγμένης x_1 του X σε ένα ακέραιο $\bar{x}_1$, και υπολογίζεται το $v = \bar{x}_1 \mod n$.
7. Αποδοχή της υπογραφής αν και μόνο αν $v = r$.

Αποδεικνύεται ότι η διαδικασία επικύρωσης της υπογραφής είναι καλά ορισμένη γιατί αν μία υπογραφή (r, s) σε ένα μήνυμα m είχε πράγματι παραχθεί από την οντότητα A, τότε $s = k^{-1}(e + dr) \mod n$. Οπότε

$$\begin{aligned} k \equiv s^{-1}(e + dr) &\equiv s^{-1}e + s^{-1}rd \equiv we + wrd \\ &\equiv u_1 + u_2 d \mod n. \end{aligned} \tag{2.1}$$

Άρα $u_1 G + u_2 Q = (u_1 + u_2 d)G = kG$, συνεπώς $v = r$.

Η ελλειπτική καμπύλη secp256k1

Το πρωτόκολλο Bitcoin χρησιμοποιεί τον Elliptic Curve Digital Signature Algorithm (ECDSA) βασισμένο στην ελλειπτική καμπύλη **secp256k1** [14]. Οι παράμετροί της προσδιορίζονται από την εξάδα $T = (p, a, b, G, n, h)$ όπου το πεπερασμένο σώμα $\mathbb{F}_p$ ορίζεται από:

$$\begin{aligned} p &= \texttt{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\ &\quad \texttt{FFFFFC2F} \\ &= 2^{256} - 2^{32} - 2^9 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

Η καμπύλη $E: \ y^2 = x^3 + ax + b$ επί του $\mathbb{F}_p$ ορίζεται από τις:

$$\begin{aligned} a &= \texttt{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \texttt{00000000} \\ b &= \texttt{00000000 00000000 00000000 00000000 00000000 00000000 00000000} \\ &\quad \texttt{00000007} \end{aligned}$$

Το σημείο βάσης G σε συμπιεσμένη μορφή είναι:

$$\begin{aligned} G = \quad & \texttt{02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\ & \texttt{59F2815B 16F81798} \end{aligned}$$

και σε ασυμπίεστη μορφή είναι:

$$\begin{aligned} G = \quad & \texttt{04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9} \\ & \texttt{59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448} \\ & \texttt{A6855419 9C47D08F FB10D4B8} \end{aligned}$$

Η τάξη n του G και του συμπαράγοντα h είναι:

$n =$ FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF BAAEDCE6 AF48A03B BFD25E8C D0364141

$h =$ 01

2.5 Συναρτήσεις Κατακερματισμού (Hash Functions)

Μία κρυπτογραφική συνάρτηση κατακερματισμού ή συμπύκνωσης (cryptographic hash function - CHF) [15] είναι μία μαθηματική συνάρτηση που δέχεται σαν είσοδο(input) μία δυαδική ακολουθία χαρακτήρων αυθαίρετου μήκους (μήνυμα m) και επιστρέφει στην έξοδο, μία δυαδική ακολουθία χαρακτήρων πεπερασμένου μήκους n που καλείται τιμή κατακερματισμού ή σύνοψη (hash) του μηνύματος.

$$H : \{0,1\}^* \mapsto \{0,1\}^n, \quad \{0,1\}^* \ni m \mapsto h = H(m) \in \{0,1\}^n. \tag{2.2}$$

Όταν $|\{0,1\}^*| > |\{0,1\}^t|$ τότε η συνάρτηση H προφανώς δεν είναι συνάρτηση $1-1$. Αυτό υπονοεί οτι αναπόφευκτα θα υπάρχουν συγκρούσεις (collisions), δηλαδή θα έχουμε ζεύγη εισόδων που θα δίνουν ίδιες εξόδους. Αν περιορίσουμε την H σε ένα πεδίο ορισμού $\{0,1\}^t$, $t > n$ και αν θεωρήσουμε την συνάρτηση κατακερματισμού H τυχαία, με την έννοια ότι όλες οι έξοδοι είναι ισοπίθανες, τότε 2^{t-n} είσοδοι θα απεικονίζονται σε 2^n εξόδους και δύο τυχαία επιλεγμένες είσοδοι θα απεικονίζονται στην ίδια έξοδο με πιθανότητα 2^{-n}.

Οι συναρτήσεις κατακερματισμού χωρίζονται σε δύο κατηγορίες:

- **Συναρτήσεις κατακερματισμού χωρίς κλειδί** (unkeyed hash functions): στον υπολογισμό της εισόδου δεν υπεισέρχεται κάποιο μυστικό κλειδί.
- **Συναρτήσεις κατακερματισμού με κλειδί** (keyed hash functions): στον υπολογισμό της εισόδου χρησιμοποιείται κάποιο μυστικό κλειδί [16] [17].

Θα ασχοληθούμε μόνο με συναρτήσεις κατακερματισμού χωρίς κλειδί, αφού τόσο η SHA-256 όσο και η RIPEMD-160 που χρησιμοποιούνται στο Bitcoin είναι αυτού του είδους.

Μία κρυπτογραφική συνάρτηση κατακερματισμού έχει τις ακόλουθες ιδιότητες:

(i) **Αιτιοκρατική** (Deterministic): όσες φορές και αν κατακερματίσουμε μία συγκεκριμένη είσοδο, η σύνοφη (hash) θα είναι πάντα ίδια,

(ii) **Συμπίεση** (Compression): δέχεται είσοδο οσοδήποτε μήκους και παράγει έξοδο σταθερού μήκους (ίσου ή μικρότερου της εισόδου),

(iii) **Ευκολία υπολογισμού** (Ease of Computation): δοσμένης της συνάρτησης κατακερματισμού H και μίας εισόδου x, ο υπολογισμός $H(x) = y$ είναι εύκολος,

(iv) **preimage resistance**: δοσμένης της συνάρτησης κατακερματισμού H και μίας εξόδου y, είναι υπολογιστικά δύσκολο να βρεθεί x τέτοιο ώστε $H(x) = y$,

(v) **2nd preimage resistance** (weak collision resistance) : δοσμένης της συνάρτησης κατακερματισμού H και μίας εισόδου x είναι υπολογιστικά δύσκολο να βρεθεί διαφορετική είσοδος x' ώστε $H(x) = H(x')$,

(vi) **Collision resistance** (strong collision resistance) : δοσμένης της συνάρτησης κατακερματισμού H είναι υπολογιστικά δύσκολο να βρεθούν διαφορετικοί είσοδοι x_1 και x_2 τέτοιοι ώστε $H(x_1) = H(x_2)$.

Όλες σχεδόν οι συναρτήσεις κατακερματισμού, είναι επαναληπτικές διαδικασίες που κατακερματίζουν μία είσοδο αυθαίρετου μήκους, επεξεργάζοντας διαδοχικές ομάδες(blocks) σταθερού μήκους της εισόδου. Η είσοδος x συμπληρώνεται (padded) σε ένα πολλαπλάσιο του μεγέθους του block και στη συνέχεια διαιρείται σε t το πλήθος blocks από x_1 έως x_t. Η συνάρτηση κατακερματισμού H μπορεί να περιγραφεί ως εξής:

$$h_0 = IV, \quad h_i = f(h_{i-1}, x_i), \quad 1 \leq i \leq t, \quad H(x) = h_t. \tag{2.3}$$

Η f είναι η συνάρτηση συμπίεσης της H, h_i είναι η μεταβλητή της αλυσιδωτής σύνδεσης μεταξύ των σταδίων $i-1$ και i και IV είναι η αρχική τιμή (Initial Value).

Οι συναρτήσεις κατακερματισμού SHA-256 και RIPEMD-160 που θα αναπτυχθούν παρακάτω, ανήκουν στη κατηγορία των MDCs (modification detection codes). Σκοπός τους είναι η παροχή μιας αντιπροσωπευτικής εικόνας ή σύνοψης (hash) ενός μηνύματος με στόχο να παράσχουν, σε συνεργασία και με άλλους μηχανισμούς, διαβεβαίωση για την ακεραιότητα των δεδομένων όπου απαιτείται.

2.5.1 SHA-256 (Secure Hash Algorithm 256)

Η συνάρτηση κατακερματισμού SHA-256 [18], [19] συμπιέζει οποιαδήποτε είσοδο με μήκος μικρότερο από 2^{64} bits σε μία σύνοψη μήκους 256 bits. Κάθε μήνυμα επεξεργάζεται σε block των $512 = 16 \times 32$ bits, με κάθε block να χρειάζεται 64 γύρους. Το μήνυμα εισόδου πρώτα συμπληρώνεται έτσι ώστε το μήκος του να είναι πολλαπλάσιο των 512 bits και ύστερα αναλύεται σε block μηνυμάτων των 512 bits: $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$. Τα block αυτά επεξεργάζονται ένα κάθε φορά, ξεκινώντας με μία αρχική τιμή κατακερματισμού $H^{(0)}$. Ο υπολογισμός της επόμενης τιμής μέχρι τον υπολογισμό της τελικής τιμής, δινεται από τον ακόλουθο γενικό τύπο:

$$H^{(i)} = H^{(i-1)} + C_{M^{(i)}}(H^{(i-1)}), \tag{2.4}$$

όπου C είναι η SHA-256 συνάρτηση συμπίεσης και $+$ είναι η πρόσθεση modulo 2^{32}. Η σύνοψη (hash) του μηνύματος M είναι τελικά η $H^{(N)}$.

Περιγραφή του SHA-256

Η συνάρτηση συμπίεσης SHA-256 εφαρμόζεται σε block μηνύματος 512 bit και σε μία ενδιάμεση τιμή κατακερματισμού 256 bit. Ουσιαστικά είναι ένας κρυπτογραφικός αλγόριθμος δέσμης (block cipher algorithm) 256 bit ο οποίος κρυπτογραφεί την ενδιάμεση τιμή κατακερματισμού, χρησιμοποιώντας το block μηνύματος για κλειδί.

Συμβολισμοί

$\oplus$	bitwise XOR
$\wedge$	bitwise AND
$\vee$	bitwise OR
$\neg$	bitwise complement
$+$	mod 2^{32} addition
R^n	right shift by n bits
S^n	right rotation by n bits

Οι ακόλουθοι τελεστές ενεργούν σε λέξεις των 32 bit.

Η αρχική τιμή κατακερματισμού (**initial hash value**) $H^{(0)}$ είναι η επόμενη ακολουθία λέξεων 32 bit (οι οποίες είναι το δεκαδικό μέρος των τετραγωνικών ριζών των πρώτων οκτώ πρώτων αριθμών):

$$H_1^{(0)} = \texttt{6a09e667} \quad H_1^{(0)} = \texttt{bb67ae85} \quad H_3^{(0)} = \texttt{3c6ef372} \quad H_4^{(0)} = \texttt{xa54ff53a}$$
$$H_5^{(0)} = \texttt{510e527f} \quad H_6^{(0)} = \texttt{9b05688c} \quad H_7^{(0)} = \texttt{1f83d9ab} \quad H_8^{(0)} = \texttt{5be0cd19}$$

Προεπεξεργασία

1. Έστω ότι το μήκος του μηνύματος M έχει μήκος l bits. Πρώτα επισυνάπτεται το bit 1 στο τέλος του μηνύματος, και μετά k μηδενικά bits, όπου k είναι η μικρότερη μη αρνητική λύση της εξίσωσης $l + 1 + k \equiv 448 \mod 512$. Σε αυτό επισυνάπτεται ένα block 64 bit, που είναι ίσο με τον αριθμό l σε δυαδική μορφή. Για παράδειγμα το (8-bit ASCII) μήνυμα ”abc” έχει μήκος $8 \cdot 3 = 24$ οπότε συμπληρώνεται πρώτα με το 1 μετά με $448 - (24 + 1) = 423$ zero bits και στο τέλος με το μήκος του. Έτσι έχουμε το απλωμένο μήνυμα:

$$\texttt{01100001 01100010 1} \underbrace{\texttt{00...0}}_{423} \underbrace{\texttt{00...011000}}_{64}$$

Πλέον, το μήκος του διευρυμένου μηνύματος είναι πολλαπλάσιο των 512 bits.

2. Αναλύουμε το μήνυμα σε N block των 512 bit $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$. Τα πρώτα 32 bits του i-στου block συμβολίζονται ως $M_0^{(i)}$, τα επόμενα 32 bits είναι $M_1^{(i)}$, μέχρι το $M_{15}^{(i)}$. Χρησιμοποιείται η αναπαράσταση big-endian, έτσι σε κάθε λέξη των 32 bit, το bit που βρίσκεται στην πιο αριστερή θέση, αποθηκεύεται στην πιο σημαντική bit θέση.

Ορισμοί λογικών συναρτήσεων

Στον SHA-256 χρησιμοποιούνται έξι λογικές συναρτήσεις. Κάθε μία από αυτές ενεργεί σε λέξεις των 32 bit και παράγει έξοδο μία λέξη των 32 bit. Οι συναρτήσεις ορίζονται ακολούθως:

$$\begin{aligned} Ch(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \\ Maj(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \oplus (y \wedge z) \\ \Sigma_0(x) &= S^2(x) \oplus S^{13}(x) \oplus S^{22}(x) \\ \Sigma_1(x) &= S^6(x) \oplus S^{11}(x) \oplus S^{25}(x) \\ \sigma_0(x) &= S^7(x) \oplus S^{18}(x) \oplus R^3(x) \\ \sigma_1(x) &= S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x) \end{aligned}$$

Επέκταση των μηνυμάτων

Τα διευρυμένα block μηνυμάτων $W_0, W_1, \ldots, W_{63}$ υπολογίζονται με τον αλγόριθμο:

for $j = 0, 1, \ldots, 15$ **do**
  $W_j = M_j^{(i)}$
end for
for $j = 16$ **to** 63 **do**
  $W_j \leftarrow \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$
end for

Ορισμός σταθερών λέξεων

Στον SHA256 χρησιμοποιείται η ακολουθία σταθερών λέξεων $K_0, \ldots, K_{63}$, που είναι τα πρώτα 32 bit των δεκαδικών μερών των κυβικών ριζών των πρώτων 8 πρώτων αριθμών, σε δεκαεξαδική μορφή:

```
428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
```

e49b69c1 efbe4786 0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2

Υπολογισμός της τιμής κατακερματισμού (hash value) - Κυρίως loop.

Έστω N ο αριθμός των block του διευρυμένου μηνύματος.

for $i = 1$ **to** N **do**

- Αρχικοποίηση των καταχωρητών a, b, c, d, e, f, g, h με την ενδιάμεση τιμή κατακερματισμού η οποία είναι η αρχική τιμή κατακερματισμού για $i = 1$.

  $a \leftarrow H_1^{(i-1)}$
  $b \leftarrow H_2^{(i-1)}$
  $\vdots$
  $h \leftarrow H_8^{(i-1)}$

- Εφαρμογή της **συνάρτησης συμπύκνωσης SHA-256** για την ανανέωση των καταχωρητών a, b, c, d, e, f, g, h. Υπολογισμός των συναρτήσεων $Ch(e, f, g)$, $Maj(a, b, c)$, $\Sigma_0(a)$, $\Sigma_1(a)$ και W_j.

  $T_1 \leftarrow h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$
  $T_2 \leftarrow \Sigma_0(a) + Maj(a, b, c)$
  $h \leftarrow g$
  $g \leftarrow f$
  $f \leftarrow e$
  $e \leftarrow d + T_1$
  $d \leftarrow c$
  $c \leftarrow b$
  $b \leftarrow a$
  $a \leftarrow T_1 + T_2$

- Υπολογισμός της i-οστής ενδιάμεσης τιμής κατακερματισμού $H^{(i)}$.

  $H_1^{(i)} \leftarrow a + H_1^{(i-1)}$
  $H_2^{(i)} \leftarrow b + H_2^{(i-1)}$
  $\vdots$
  $H_8^{(i)} \leftarrow h + H_8^{(i-1)}$

  end for

Η τιμή κατακερματισμού (hash value) του μηνύματος M είναι η ακόλουθη:

$$H^N = (H_1^{(N)}, H_2^{(N)}, \ldots, H_8^{(N)},). \tag{2.5}$$

2.5.2 RIPEMD-160 (Race Integrity Primitives Evaluation 160)

Ο RIPEMD-160 [20, 21, 4, 22] ουσιαστικά αποτελείται από δύο παράλληλες εφαρμογές του MD4 [23], με μερικές βελτιώσεις στις μετακινήσεις (shifts) και στην μετάθεση των λέξεων του μηνύματος. Οι δύο παράλληλες εφαρμογές διαφέρουν μόνο στις σταθερές που χρησιμοποιούνται σε κάθε γύρο. Στο τέλος του αλγόριθμου συμπίεσης, τα μισά των λέξεων από τον αριστερό και δεξί κλάδο συνενώνονται.

Περιγραφή του RIPEMD-160

Η συνάρτηση κατακερματισμού RIPEMD-160 συμπιέζει οποιαδήποτε είσοδο με μήκος μικρότερο από 2^{64} bits σε μία σύνοψη μήκους 160 bits. Η είσοδος διευρύνεται σε blocks μήκους 512 bits τα οποία επεξεργάζονται με την επαναληπτική διαδικασία Merkle-Damgard. Κάθε ένα από τα 512-bit blocks συμπιέζονται σε μία σύνοψη 160-bit με τη χρήση της συνάρτησης συμπίεσης που αποτελείται από δύο κλάδους που τρέχουν παράλληλα. Τον αριστερό και το δεξί κλάδο. Κάθε κλάδος περιέχει 5 γύρους και κάθε γύρος περιέχει 16 βήματα. Ο RIPEMD-160 χρησιμοποιεί "αλυσιδωτές μεταβλητές" (chaining variables). Αυτές έχουν αρχικές τιμές που ορίζονται από τον αλγόριθμο και σε κάθε γύρο ανανεώνονται με βάση τον αλγόριθμο και τις τιμές του εκάστοτε block μηνύματος. Στον RIPEMD-160 οι μεταβλητές αυτές περνάνε ανεξάρτητα από κάθε κλάδο και συνενώνονται στο τέλος.

Προεπεξεργασία Ο RIPEMD-160 χρησιμοποιεί την ίδια επέκταση μηνύματος και την ίδια συνθήκη endianess όπως ο αλγόριθμος MD5 [24, 25] (ο MD5 χρησιμοποιεί συνθήκη big-endian σε επίπεδο bit και συνθήκη little-endian σε επίπεδο byte).

1. **Επισύναψη των bit επέκτασης** Το μήνυμα επεκτείνεται έτσι ώστε το μήκος του σε bits να είναι ισουπόλοιπο με το 448, modulo 512. Δηλαδή το μήνυμα επεκτείνεται έτσι ώστε να είναι ακριβώς 64 bits μικρότερο από το να είναι πολλαπλάσιο μήκους των 512 bits. Η επέκταση αυτή εκτελείται πάντα, ακόμα και αν το μήκος του μηνύματος είναι ήδη ισουπόλοιπο με το 448, modulo 512. Η επέκταση αυτή γίνεται όπως στην περίπτωση του αλγορίθμου SHA-256 που αναφέραμε προηγούμένως.
2. **Επισύναψη μήκους** Στο αποτέλεσμα του προηγούμενου βήματος, επισυνάπτεται μία αναπαράσταση 64-bit του μήκους (ας το συμβολίσουμε με b) του μηνύματος, προτού να προστεθούν τα bit επέκτασης. Το μήνυμα που θα προκύψει μετά την επέκταση με τα bits και με το b θα έχει μήκος που θα είναι ίσο με κάποιο πολλαπλάσιο των 512 bits. Ισοδύναμα το μύνημα αυτό θα έχει μήκος ίσο με πολλαπλάσιο των δεκαέξι (32-bit) λέξεων. Δηλαδή $M = (m_1, m_2, \ldots, m_{N-1})$, όπου N πολλαπλάσιο του 16.

Αλυσιδωτές Μεταβλητές Υπάρχουν πέντε αλυσιδωτές μεταβλητές, A, B, C, D και E, οι οποίες αρχικά λαμβάνουν τις ακόλουθες τιμές (σε δεκαεξαδική μορφή):

$$\begin{aligned} A &= \texttt{0x67452301} \\ B &= \texttt{0xEFCDAB89} \\ C &= \texttt{0x98BADCFE} \\ D &= \texttt{0x10325476} \\ E &= \texttt{0xC3D2E1F0} \end{aligned}$$

Κάθε τιμή είναι μετάθεση ενός υποσυνόλου και των 16 δεκαεξαδικών ψηφίων.

Συμβολισμοί Οι ακόλουθοι τελεστές ενεργούν σε λέξεις των 32 bit.

$\oplus$	bitwise XOR
$\wedge$	bitwise AND
$\vee$	bitwise OR
$\neg$	bitwise complement
$+$	mod 2^{32} addition
$\ll s$	circular shift, s bit positions to the left

Ορισμοί λογικών συναρτήσεων Στον RIPEMD-160 χρησιμοποιούνται πέντε λογικές συναρτήσεις που ενεργούν σε λέξεις 32 bit x, y, z και ορίζονται ακολούθως:

$$\begin{aligned} F_1(x,y,z) &= x \oplus y \oplus z \\ F_2(x,y,z) &= (x \wedge y) \vee (\neg x \wedge z) \\ F_3(x,y,z) &= (x \vee \neg y) \oplus z \\ F_4(x,y,z) &= (x \wedge z) \vee (y \wedge \neg z) \\ F_5(x,y,z) &= x \oplus (y \vee \neg z) \end{aligned}$$

Branch	Round 1	Round 2	Round 3	Round 4	Round 5
left	F_1	F_2	F_3	F_4	F_5
right	F_5	F_4	F_3	F_2	F_1

Διάταξη των λέξεων του μηνύματος Ας υποθέσουμε ότι έχουμε ένα μόνο block μηνύματος , μεγέθους 512 bits. Το block αυτό χωρίζεται σε δεκαέξι λέξεις των 32 bit $M = (m_0, m_1, \ldots, m_{15})$. (Ας σημειωθεί ότι κάθε μία από τις αλυσιδωτές μεταβλητές έχει μέγεθος 32 bits). Για κάθε γύρο, οι λέξεις διατάσσονται με βάση τις ακόλουθες μεταθέσεις:

$$\rho \quad = \quad [7, 4, 13, 1, 10, 6, 15, 3, 12, 0, 9, 5, 2, 14, 11, 8]]$$

Η μετάθεση π ορίζεται ως $\pi_i = 9i + 5 \pmod{16}$, $i = 0, \ldots, 15$.

$$\pi \quad = \quad [5, 14, 7, 0, 9, 2, 11, 4, 13, 6, 15, 8, 1, 10, 3, 12]$$

Από αυτές τις δύο μεταθέσεις, προκύπτουν οκτώ άλλες μεταθέσεις, πλέον της ταυτοτικής όπου στον αριστερό κλάδο και στον πρώτο γύρο το $X = M$ όπου $X = \{X_0, X_1, \ldots, X_{15}\}$ και $M = \{m_0, m_1, \ldots, m_{15}\}$. Οι μεταθέσεις αυτές χρησιμοποιούνται στους κλάδους και στους αντίστοιχους γύρους ως εξής:

Branch	Round 1	Round 2	Round 3	Round 4	Round 5
left	$id(X)$	$\rho(X)$	$\rho^2(X)$	$\rho^3(X)$	$\rho^4(X)$
right	$\pi(X)$	$\rho\pi(X)$	$\rho^2\pi(X)$	$\rho^3\pi(X)$	$\rho^4\pi(X)$

Για παράδειγμα η μετάθεση $\rho^3\pi(X)$ αναλύεται ως $\rho(\rho(\rho(\pi(X))))$, όπου σε κάθε γύρο το X συμβολίζει την καινούργια μετάθεση των 16 λέξεων.

Για τον αριστερό κλάδο και για κάθε ένα από τα δεκαέξι βήματα κάθε γύρου από τους πέντε, οι μεταθέσεις έχουν ως εξής:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_1^l(i)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu_2^l(i)$	7	4	13	1	10	6	15	3	12	0	9	5	2	14	11	8
$\mu_3^l(i)$	3	10	14	4	9	15	8	1	2	7	0	6	13	11	5	12
$\mu_4^l(i)$	1	9	11	10	0	8	12	4	13	3	7	15	14	5	6	2
$\mu_5^l(i)$	4	0	5	9	7	12	2	10	14	1	3	8	11	6	15	13

Πίνακας 2.5.1: Μεταθέσεις αριστερού κλάδου

όπου $\mu_1^l(i) = id(X)$, $\mu_2^l(i) = \rho(X)$, $\mu_3^l(i) = \rho^2(X)$, $\mu_4^l(i) = \rho^3(X)$, $\mu_5^l(i) = \rho^4(X)$ και $i = 1, 2, \ldots, 16$ συμβολίζει κάθε ένα απο τα δεκαέξι βήματα κάθε γύρου.

Για τον δεξιό κλάδο και για κάθε ένα από τα δεκαέξι βήματα κάθε γύρου από τους πέντε, οι μεταθέσεις έχουν ως εξής:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_1^r(i)$	5	14	7	0	9	2	11	4	13	6	15	8	1	10	3	12
$\mu_2^r(i)$	6	11	3	7	0	13	5	10	14	15	8	12	4	9	1	2
$\mu_3^r(i)$	15	5	1	3	7	14	6	9	11	8	12	2	10	0	4	13
$\mu_4^r(i)$	8	6	4	1	3	11	15	0	5	12	2	13	9	7	10	14
$\mu_5^r(i)$	12	15	10	4	1	5	8	7	6	2	13	14	0	3	9	11

Πίνακας 2.5.2: Μεταθέσεις δεξιού κλάδου

όπου $\mu_1^r(i) = \pi(X)$, $\mu_2^r(i) = \rho\pi(X)$, $\mu_3^r(i) = \rho^2\pi(X)$, $\mu_4^r(i) = \rho^3\pi(X)$, $\mu_5^r(i) = \rho^4\pi(X)$ και $i = 1, 2, \ldots, 16$ συμβολίζει κάθε ένα απο τα δεκαέξι βήματα κάθε γύρου.

Μετακινήσεις (Shifts) Για κάθε κλάδο έχουμε τις παρακάτω κυκλικές μετακινήσεις (circular shifts) $\ll s$, όπου s_i^l τα shifts για τον αριστερό κλάδο, s_i^r τα shifts για τον δεξιό κλάδο, $i = 1, \ldots, 5$ και j είναι ο δείκτης για κάθε λέξη από τις δεκαέξι του μηνύματος σε κάθε γύρο:

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_1^l	11	14	15	12	5	8	7	9	11	13	14	15	6	7	9	8
s_2^l	7	6	8	13	11	9	7	15	7	12	15	9	11	7	13	12
s_3^l	11	13	6	7	14	9	13	15	14	8	13	6	5	12	7	5
s_4^l	11	12	14	15	14	15	9	8	9	14	5	6	8	6	5	12
s_5^l	9	15	5	11	6	8	13	12	5	12	13	14	11	8	5	6

Πίνακας 2.5.3: Μετακινήσεις (Shifts) αριστερού κλάδου

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_1^r	8	9	9	11	13	15	15	5	7	7	8	11	14	14	12	6
s_2^r	9	13	15	7	12	8	9	11	7	7	12	7	6	15	13	11
s_3^r	9	7	15	11	8	6	6	14	12	13	5	14	13	13	7	5
s_4^r	15	5	8	11	14	14	6	14	6	9	12	9	12	5	15	8
s_5^r	8	5	12	9	12	5	14	6	8	13	6	5	15	13	11	11

Πίνακας 2.5.4: Μετακινήσεις (Shifts) δεξιού κλάδου

Στον επόμενο πίνακα, δίνονται αναλυτικά όλες οι τιμές των μεταθέσεων των λέξεων

του μυνήματος καθώς και οι μετακινήσεις για κάθε κλάδο, γύρο και βήμα:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_1^l(i)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu_1^r(i)$	5	14	7	0	9	2	11	4	13	6	15	8	1	10	3	12
s_1^l	11	14	15	12	5	8	7	9	11	13	14	15	6	7	9	8
s_1^r	8	9	9	11	13	15	15	5	7	7	8	11	14	14	12	6
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_2^l(i)$	7	4	13	1	10	6	15	3	12	0	9	5	2	14	11	8
$\mu_2^r(i)$	6	11	3	7	0	13	5	10	14	15	8	12	4	9	1	2
s_2^l	7	6	8	13	11	9	7	15	7	12	15	9	11	7	13	12
s_2^r	9	13	15	7	12	8	9	11	7	7	12	7	6	15	13	11
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_3^l(i)$	3	10	14	4	9	15	8	1	2	7	0	6	13	11	5	12
$\mu_3^r(i)$	15	5	1	3	7	14	6	9	11	8	12	2	10	0	4	13
s_3^l	11	13	6	7	14	9	13	15	14	8	13	6	5	12	7	5
s_3^r	9	7	15	11	8	6	6	14	12	13	5	14	13	13	7	5
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_4^l(i)$	1	9	11	10	0	8	12	4	13	3	7	15	14	5	6	2
$\mu_4^r(i)$	8	6	4	1	3	11	15	0	5	12	2	13	9	7	10	14
s_4^l	11	12	14	15	14	15	9	8	9	14	5	6	8	6	5	12
s_4^r	15	5	8	11	14	14	6	14	6	9	12	9	12	5	15	8
i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mu_5^l(i)$	4	0	5	9	7	12	2	10	14	1	3	8	11	6	15	13
$\mu_5^r(i)$	12	15	10	4	1	5	8	7	6	2	13	14	0	3	9	11
s_5^l	9	15	5	11	6	8	13	12	5	12	13	14	11	8	5	6
s_5^r	8	5	12	9	12	5	14	6	8	13	6	5	15	13	11	11

Πίνακας 2.5.5: Μετακινήσεις (Shifts) δεξιού κλάδου

Σταθερές Χρησιμοποιούνται οι ακόλουθες σταθερές. Λαμβάνονται τα ακέραια μέρη (συμβολίζουμε με $[\cdot]$) των αντίστοιχων γινομένων:

$$\begin{array}{lllllllll}
K_1^l & = & \texttt{0x00000000} & = & 0 & K_1^r & = & \texttt{0x50A28BE6} & = & [2^{30} \cdot \sqrt[3]{2}] \\
K_2^l & = & \texttt{0x5A827999} & = & [2^{30} \cdot \sqrt{2}] & K_2^r & = & \texttt{0x5C4DD124} & = & [2^{30} \cdot \sqrt[3]{3}] \\
K_3^l & = & \texttt{0x6ED9EBA1} & = & [2^{30} \cdot \sqrt{3}] & K_3^r & = & \texttt{0x6D703EF3} & = & [2^{30} \cdot \sqrt[3]{5}] \\
K_4^l & = & \texttt{0x8F1BBCDC} & = & [2^{30} \cdot \sqrt{5}] & K_4^r & = & \texttt{0x7A6D76E9} & = & [2^{30} \cdot \sqrt[3]{7}] \\
K_5^l & = & \texttt{0xA953FD4E} & = & [2^{30} \cdot \sqrt{7}] & K_2^r & = & \texttt{0x00000000} & = & 0
\end{array}$$

Branch	Round 1	Round 2	Round 3	Round 4	Round 5
left	K_1^l	K_2^l	K_3^l	K_4^l	K_5^l
right	K_1^r	K_2^r	K_3^r	K_4^r	K_5^r

Περιγραφή της Συνάρτησης Κατακερματισμού

Η συνάρτηση κατακερματισμού που χρησιμοποιείται απο τον RIPEMD-160 ξεκινά παίρνοντας σαν είσοδο τις μεγέθους 160-bit αλυσιδωτές μεταβλητές $AM = (A, B, C, D, E)$, τις οποίες και ανανεώνει σε 80 βήματα (5 γύροι, κάθε γύρος έχει 16 βήματα) για κάθε κλάδο.

Αρχικοποίηση Αλυσιδωτών Μεταβλητών Κάθε κλάδος ξεκινά με τις ίδιες αρχικές τιμές στις αλυσιδωτών μεταβλητών.

$$X_{-4} = Y_{-4} = A^{\ll 10}, \quad X_{-3} = Y_{-3} = E^{\ll 10}$$
$$X_{-2} = Y_{-2} = D^{\ll 10}, \quad X_{-1} = Y_{-1} = C, \quad X_0 = Y_0 = B$$

Μετασχηματισμός Ανανέωσης Κατάστασης Σε κάθε γύρο $j(1 \leq j \leq 4)$, τα X_i (αριστερός κλάδος) και Y_i (δεξιός κλάδος), $i(1 \leq i \leq 80)$ (i ο αριθμός των βημάτων κάθε κλάδου), ανανεώνονται ως ακολούθως:

$$X_i = (X_{i-4})^{\ll 10} + \Big(\big(X_{i-4}\big) + F_j(X_{i-1}, X_{i-2}, (X_{i-3}^{\ll 10})\big) + \mu_j^l(i) + K_j^l \Big)^{\ll s_i^l} \tag{2.6}$$

$$Y_i = (Y_{i-4})^{\ll 10} + \Big(\big(Y_{i-4}\big) + F_{6-j}(Y_{i-1}, Y_{i-2}, (Y_{i-3}^{\ll 10})\big) + \mu_j^r(i) + K_j^r \Big)^{\ll s_i^r} \tag{2.7}$$

Οι λογικές συναρτήσεις F_j και οι σταθερές K_j^L, K_j^r εξαρτούνται από τον γύρο j και από την χρήση τους από τον αριστερό ή δεξί κλάδο αντίστοιχα.

Οριστικοποίηση Η σύνοψη του μηνύματος M προκύπτει συνδυάζοντας τις αρχικές τιμές των αλυσιδωτών μεταβλητών A, B, C, D, E με τις εξόδους των δύο κλάδων. Οι πέντε λέξεις 32 bit $A', B', C'D', E'$ που συνθέτουν την συμπίεση του αρχικού μηνυματος, υπολογίζονται ως εξής:

$$A' = B + X_{79} + (Y_{78}^{\lll 10}), \qquad B' = C + (X_{78}^{\lll 10}) + (Y_{77}^{\lll 10}),$$
$$C' = D + (X_{77}^{\lll 10}) + (Y_{76}^{\lll 10}), \quad D' = E + (X_{76}^{\lll 10}) + Y_{80},$$
$$E' = A + X_{80} + Y_{79}.$$

2.5.3 Length extension attack

Στην κρυπτογραφία σαν **Length extension attack** (επίθεση επέκτασης μήκους), χαρακτηρίζεται μία μορφή επίθεσης όπου ο επιτιθέμενος χρησιμοποιεί την σύνοψη ενός μηνύματος Hash(message1) και το μήκος του μηνύματος (message1), για να υπολογίσει την σύνοψη Hash(message1 || message2) όπου το message2 τίθεται από τον επιτιθέμενο, χωρίς να γνωρίζει το περιεχόμενο του message1 [26], [27].

Για την αντιμετώπιση αυτών των επιθέσεων προτάθηκε η χρήση διπλής συνάρτησης κατακερματισμού [15] και πιό συγκεκριμένα η SHA-255(SHA-256(x)) η αλλιώς "SHA-256d" [28]. Στο κρυπτονόμισμα Bitcoin χρησιμοποιείται επίσης και η διπλή συνάρτηση κατακερματισμού RIPEMD160(SHA256(x)) ή Hash160.

Κεφάλαιο 3

Κρυπτονομίσματα

3.1 Εισαγωγή

Η εμφάνιση βιώσιμου ψηφιακού χρήματος είναι στενά συνδεδεμένη με τις εξελίξεις στην κρυπτογραφία εάν σκεφτούμε ότι χρησιμοποιούνται bits για αντιπροσώπευση αξίας που μπορεί να ανταλλαγεί με αγαθά και υπηρεσίες, αντί για τυπωμένο νόμισμα. Με την αποδοχή ψηφιακού χρήματος προκύπτουν δύο βασικές ερωτήσεις.

1. Πως μπορούμε να έχουμε εμπιστοσύνη στη γνησιότητα του ψηφιακού χρήματος;

2. Πως μπορούμε να είμαστε σίγουροι ότι κανένας άλλος δεν θα ισχυριστεί ότι αυτό το χρήμα ανήκει σε αυτόν και όχι σε εμάς; (Έτσι προκύπτει το πρόβλημα του διπλοξοδέματος - double spend problem).

Οι εκδότες του χάρτινου νομίσματος (κεντρικές τράπεζες) προσπαθούν να καταπολεμήσουν την πλαστογραφία με εξειδικευμένα χαρτιά και ειδικές και πολύπλοκες εκτυπώσεις. Το τυπωμένο χρήμα αντιμετωπίζει εύκολα το πρόβλημα του διπλοξοδέματος εύκολα, επειδή ένα χαρτονόμισμα δεν γίνεται να βρίσκεται ταυτόχρονα σε δύο διαφορετικά σημεία. Βέβαια το συμβατικό χρήμα μπορεί να αποθηκευτεί και να διακινηθεί και ηλεκτρονικά. Σε όλες τις περιπτώσεις τα προβλήματα πλαστογραφίας και διπλοξοδέματος αντιμετωπίζονται με την εκκαθάριση των ηλεκτρονικών συναλλαγών από κεντρικές αρχές οι οποίες έχουν μία συνολική παγκόσμια οπτική για το χρήμα που βρίσκεται σε κυκλοφορία. Επειδή το ψηφιακό χρήμα δεν μπορεί να εκμεταλλευθεί τις σύγχρονες τεχνικές εκτύπωσης και παραγωγής των ειδικών χαρτιών, η κρυπτογραφία παρέχει την βάση για να εμπιστευθεί κάποιος ένα χρήστη ότι πράγματι κατέχει την αξία που ισχυρίζεται ότι έχει. Το πρόβλημα του διπλοξοδέματος αντιμετωπίζεται με την χρήση των ψηφιακών υπογραφών.

Όταν προς τα τέλη της δεκαετίας του 1980 η κρυπτογραφία άρχισε να γίνεται ευρύτερα διαθέσιμη και κατανοητή πολλοί ερευνητές άρχισαν να χρησιμοποιούν την κρυπτογραφία για την κατασκευή ψηφιακών νομισμάτων. Αυτές οι πρώιμες εργασίες ψηφιακού χρήματος εξέδιδαν ψηφιακό νόμισμα, συνήθως υποστηριζόμενο από ένα εθνικό νόμισμα ή πολύτιμο μέταλλο όπως ο χρυσός. Αυτά τα νομίσματα ήταν αξιόπιστα, όμως επειδή ήταν κεντροποιημένα δηλαδή ακολουθούσαν το μοντέλο εκκαθάρισης των συναλλαγών που χρησιμοποιούσαν οι κεντρικές τράπεζες, ήταν ευάλωτα σε επιθέσεις από κυβερνήσεις και hackers. Έτσι προέκυψε η ανάγκη για ένα πλήρως αποκεντρωμένο σύστημα, ελεύθερο από τον έλεγχο της οποιασδήποτε κεντρικής αρχής. Το bitcoin είναι ένα τέτοιο σύστημα και αποτελεί την κορύφωση δεκαετιών έρευνας στην κρυπτογραφία και στα αποκεντρωμένα συστήματα.

Το bitcoin περιλαμβάνει τέσσερεις βασικές καινοτομίες που λειτουργούν μαζί σε ένα μοναδικό και ισχυρό συνδυασμό:

- Ένα αποκεντρωμένο peer-to-peer δίκτυο (Πρωτόκολλο Bitcoin)
- Ένα δημόσιο διπλογραφικό καθολικό συναλλαγών(blockchain)
- Μία αποκεντρωμένη έκδοση χρήματος που βασίζεται σε ένα μαθηματικό πρόβλημα (distributed mining)
- Ένα αποκεντρωμένο σύστημα επιβεβαίωσης και επαλήθευσης των συναλλαγών (tran -saction script)

3.2 Bitcoin

3.2.1 Εισαγωγή

Το Bitcoin εφευρέθηκε το 2008 με την έκδοση μίας εργασίας με τον τίτλο “Bitcoin: A Peer-to- Peer Electronic Cash System” [29] με συγγραφέα (ψευδώνυμο) τον Satoshi Nakamoto. Ο Nakamoto συνδύασε πολλές υπάρχουσες καινοτομίες όπως το ”b-money” [30], το ”Hash Cash” [31] και άλλες, με σκοπό να δημιουργήσει ένα πλήρως αποκεντρωμένο ηλεκτρονικό σύστημα χρήματος που δεν βασίζεται σε κάποια κεντρική αρχή για την έκδοση νομισμάτων και για την εκκαθάριση και επικύρωση των συναλλαγών. Η βασική καινοτομία του ήταν η χρήση ενός αποκεντρωμένου υπολογιστικού συστήματος που καλείται απόδειξη εργασίας (proof of work) για την διενέργεια μίας παγκόσμιας ’εκλογής’ κάθε δέκα περίπου λεπτά, επιτρέποντας έτσι στο αποκεντρωμένο δίκτυο να έρχεται σε συναίνεση (consensus) για την κατάσταση των συναλλαγών. Η καινοτομία αυτή λύνει κομψά το πρόβλημα του διπλοξοδέματος. Επίσης δίνει μία πρακτική λύση στο αλύτο πρόβλημα των ’Βυζαντινών Στρατηγών’ [32] το οποίο επιγραμματικά συνίσταται στην προσπάθεια να

συμφωνηθεί μια πορεία δράσης με ανταλλαγή πληροφοριών σε ένα αναξιόπιστο και δυνητικά παραβιασμένο δίκτυο. Με την απόδειξη εργασίας επιτυγχάνεται συναίνεση χωρίς την παρουσία μίας έμπιστης κεντρικής αρχής και αντιπροσωπεύει μια σημαντική ανακάλυψη στην επιστήμη των κατανεμημένη υπολογιστικών συστημάτων έχοντας παράλληλα ευρεία εφαρμοσιμότητα πέρα από μόνο το νόμισμα. Μπορεί να χρησιμοποιηθεί για την επίτευξη συναίνεσης σε αποκεντρωμένα δίκτυα για να αποδείξει την νομιμότητα εκλογών, μητρώων περιουσιακών στοιχείων, ψηφιακής επικύρωσης και αλλα.

Στα εξαιρετικά βιβλία των Andreas M. Antonopoulos [33, 34] και Imran Bashir [35, 36] δίνεται μία πολύ αναλυτική περιγραφή της λειτουργίας του bitcoin καθώς και της blockchain.

3.2.2 Λειτουργία του Bitcoin

Η ιδιοκτησία μίας αξίας σε bitcoin κατοχυρώνεται μέσω ψηφιακών κλειδιών, διευθύνσεων bitcoin και ψηφιακών υπογραφών. Η μεταφορά της από ένα ιδιοκτήτη σε έναν άλλον γίνεται μέσω των συναλλαγών (transactions).

Ιδιωτικά και δημόσια κλειδιά στο Bitcoin

Τα ψηφιακά κλειδιά δεν αποθηκεύονται στο δίκτυο αλλά σε μία απλή βάση δεδομένων που την καλούμε 'πορτοφόλι' (wallet). Τα ψηφιακά κλειδιά είναι ανεξάρτητα από το δίκτυο και το λογισμίκο του πορτοφολιού μπορεί να τα παράγει και να τα αποθηκεύει. Για να περιληφθεί στην blockchain μία συναλλαγή bitcoin απαιτείται μία έγκυρη υπογραφή η οποία παράγεται μόνο με την χρήση έγκυρων ψηφιακών κλειδιών. Έτσι, όποιος έχει τα κλειδιά αυτά, αυτομάτως έχει και τον έλεγχο του αντίστοιχου λογαρισμού bitcoin. Ενα ζευγάρι ψηφιακών κλειδιών αποτελείται από ένα ιδιωτικό και από ένα δημόσιο κλειδί. Μπορούμε να θεωρήσουμε το δημόσιο κλειδί σαν τον λογαριασμό IBAN και το ιδιωτικό κλειδι σαν το αριθμό PIN.

Σε μία συναλλαγή bitcoin, το δημόσιο κλειδί του παραλήπτη αντιπροσωπεύεται από την διεύθυνση του παραλήπτη και χρησιμοποιείται με τον ίδιο τρόπο που χρησιμοποιείται το όνομα του δικαιούχου μίας επιταγής. Στις περισσότερες περιπτώσεις, μία διεύθυνση bitcoin παράγεται από ένα δημόσιο κλειδί και αντιστοιχεί σε αυτό. Υπάρχουν όμως και περιπτώσεις που η διεύθυνση αυτή αντιστοιχεί σε άλλους δικαιούχους όπως τα λεγόμενα scripts.

Το ιδιωτικό κλειδί είναι ένας αριθμός μεταξύ του 1 και του $n-1$ όπου $n = 1.158 * 10^{77}$. Παράγεται από μία κρυπτογραφικά ισχυρή γεννήτρια ψευδοτυχαίων αριθμών (CSPRNG) μαζί με την χρήση μίας πηγής εντροπίας που μπορεί να είναι η κίνηση του ποντικιού ή τυχαία πληκτρολόγηση ή άλλη. Το δημόσιο κλειδί παράγεται από το ιδιωτικό κλειδί με την

χρήση κρυπτογραφίας ελλειπτικής καμπύλης όπως έχουμε αναφέρει προηγουμένως.

Διευθύνσεις Bitcoin - Bitcoin Addresses

Μία διεύθυνση bitcoin είναι συνήθως μία σειρά γραμμάτων και αριθμών που ξεκινάει από 1 η οποία μπορεί να μοιραστεί με οποιονδήποτε που θέλει να μας στείλει bitcoin. π.χ `16xTznL6ksTCCuyhSRMx7924Pd9KhB2tJd`. Μία διεύθυνση bitcoin παράγεται από ένα δημόσιο κλειδί μέσω των συναρτήσεων κατακερματισμού SHA-256 και RIPEMD-160.

$$A = RIPEMD160(SHA256(K)) \tag{3.1}$$

όπου η διεύθυνση A είναι ένας αριθμός 160 bit και K είναι το δημόσιο κλειδί. Από το δημόσιο κλειδί χρησιμοποιείται μόνο η τετμημένη του, x, γιατί κάθε σημείο της ελλειπτικής καμπύλης μπορεί να προσδιοριστεί μόναδικά από αυτή λόγω του ότι το αντίστοιχο συμμετρικό σημείο του δημοσίου κλειδιού διαφέρει μόνο στην τεταγμένη. Η τεταγμένη του δημόσιου κλειδιού μπορεί να είναι είτε y είτε $-y$ όταν πρόκειται για ελλειπτική καμπύλη πάνω στο σώμα των πραγματικών αριθμών ενώ πάνω σε πεπερασμένο σώμα έχουμε αντίστοιχα μονή ή ζυγή τεταγμένη. Για τον λόγο αυτό χρησιμοποιείται πριν τους επόμενους κατακερματισμούς το πρόθεμα (prefix) 02 όταν η τεταγμένη είναι y (even) ή το prefix 03 όταν η τεταγμένη είναι $-y$ (odd). Η θέση της τεταγμένης y αναγνωρίζεται, ελέγχοντας το τελευταίο ψηφίο της. Για παράδειγμα μία τεταγμένη y με δεκαεξαδική μορφή `B32E9ECC107CB7C23863EEF30266E0 4960250ECFE077BEB34208DF61DDA46B51` αντιπροσωπεύει τον αριθμό `810463708388727048025711853195902881625718206159773218245086886814320241160 49` στο δεκαδικό σύστημα. Όταν ξεκίνησε το bitcoin, δεν χρησιμοποιούνταν η παραπάνω συμπιεσμένη μορφή του δημόσιου κλειδιού αλλά γινόταν χρήση και των δύο συντεταγμένων. Έάν κάποιος θέλει να χρησιμοποιήσει την ασυμπίεστη μορφή του δημοσίου κλειδιού πρέπει να χρησιμοποιήσει το πρόθεμα 04. Λόγω του μεγάλου μήκους του δημόσιου κλειδιού (512-bit) στην ασυμπίεστη μορφή του και (256-bit) στη συμπιεσμένη μορφή και για επιπρόσθετη ασφάλεια, χρησιμοποιείται η συνάρτηση κατακερματισμού SHA-256 με την οποία μειώνεται το μήκος του στα 256 bit και κατόπιν με την χρήση της RIPEMD-160 το μήκος μειώνεται στα 160 bit. Το αποτέλεσμα είναι ουσιαστικά μία περισσότερο συμπιεσμένη μορφή του δημοσίου κλειδιού. Στη συνέχεια μπροστά από την νεοσυμπιεσμένη μορφή, συμπληρώνεται ένα prefix το οποίο για τις περισσότερες διευθύνσεις είναι το `00`. Υπάρχουν και άλλα προθέματα που χρησιμοποιούνται για διαφορετικές λειτουργίες, όπως το πρόθεμα `6f` για χρήση στο testnet κ.α. Στην συνέχεια, στην καινούργια συμβολοσειρά που δημιουργήθηκε, εφαρμόζεται δύο φορές ο SHA-256. Από την καινούργια σύνοψη λαμβάνουμε τα πρώτα 4 bytes (8 ψηφία στο δεκαεξαδικό σύστημα) τα οποία αποτελούν το λεγόμενο checksum που χρισιμεύει στην αναγνώριση λαθών. Το τε-

λευταίο βήμα είναι η χρήση της κωδικοποιήσης Base58Check. Το τελικό αποτέλεσμα είναι η διεύθυνση bitcoin.

Παράδειγμα 2. *(Παραγωγή διεύθυνσης Bitcoin)*

(i) Δημιουργία ιδιωτικού κλειδιού χωρίς χρήση κρυπτογραφικής γεννήτριας, με τυχαία πληκτρολόγηση. (Δεν συνίσταται παρά μόνο για εκπαιδευτικούς σκοπούς). Πληκτρολογείται η παρακάτω φράση:

ethnikokaikapodistriakopanepistimioathinon

(ii) Παραγωγή του ιδιωτικού κλειδιού με χρήση της SHA256

SHA256(ethnikokaikapodistriakopanepistimioathinon)=

38933DC9686793BB89CF8F0B1E361985CB61E61FE2A9C67A47EEBA7A1E6E09B0

(iii) Παραγωγή του δημοσίου κλειδιού με χρήση της ελλειπτικής καμπύλης secp256k1.

x = *518F2FB988CBD90A88067391F4D82563B6DA3FFB202881D1E695A94D9958 AFCB*

y = *B32E9ECC107CB7C23863EEF30266E04960250ECFE077BEB34208DF61DDA4 6B51*

(iv) Έλεγχος για τον τύπο του prefix. Η τεταγμένη της δυάδας του δημοσίου κλειδιού στην δεκαδική της μορφή είναι περιττός αριθμός, οπότε θα χρησιμοποιηθεί το prefix 03*. Εάν ήταν άρτιος αριθμός θα χρησιμοποιούσαμε το prefix* 02*. Το δημόσιο κλειδί θα παρασταθεί με την συμπιεσμένη του μορφή, ως εξής:*

03 *518F2FB988CBD90A88067391F4D82563B6DA3FFB202881D1E695A94D9958*

AFCB Το κενό μεταξύ του prefix και του κλειδιού υπάρχει εδώ μόνο για το σκοπό καλής ανάγνωσης.

(v) Με εφαρμογή διπλού κατακερματισμού RIPEMD160(SHA256(ΔΗΜΟΣΙΟ ΚΛΕΙΔΙ)) λαμβάνουμε την πρώτη μορφή της bitcoin διεύθυνσης:

41560AC990131A63380C981DD85FCD5665E5418B

(vi) Χρησιμοποιούμε το prefix 00 για μία συνηθισμένη διεύθυνση bitcoin και λαμβάνουμε την ακόλουθη συμβολοσειρά:

00 *41560AC990131A63380C981DD85FCD5665E5418B*

(vii) Εφαρμόζουμε διπλό κατακερματισμό SHA256D στην προηγούμενη συμβολοσειρά και λαμβάνουμε το ακόλουθο checksum 91F5F872

(viii) Χρησιμοποιούμε Base58 Encode για την ακόλουθη διεύθυνση στην οποία ένσωματώ-

νουμε το checksum στο τέλος 0041560AC990131A63380C981DD85FCD5665E5418B 91F5F872

και έχουμε την διεύθυνση Bitcoin 16xTznL6ksTCCuyhSRMx7924Pd9KhB2tJd που θέλουμε να χρησιμοποιήσουμε.

Για το παράδειγμα χρησιμοποιήθηκε ο υπολογιστής διεύθυνσης bitcoin στη διεύθυνση `https://bit.ly/37tWncp`. Τα αποτελέσματά του ελέγχθηκαν με χρήση του υπολογιστή ελλειπτικών καμπυλών στην διεύθυνση `https://bit.ly/3bwy6FM` καθώς και του υπολογιστή τιμών κατακερματισμού στη διεύθυνση `https://bit.ly/2vBrQwc`. Στον υπολογιστή τιμών κατακερματισμού θα πρέπει να επιλεχθεί η επιλογή "Hash hex bytes" ώστε να επιτευχθεί η σωστή hash value. Για την μετατροπή από το δεκαεξαδικό σύστημα στο δεκαδικό, χρησιμοποιήθηκε ο μετατροπέας στη διεύθυνση `https://bit.ly/37nbYKM`. Για την κωδικοποίηση Base58 Encode χρησιμοποιήθηκε ο κωδικοποιητής στη διεύθυνση `https://bit.ly/2Hnp2VV`. Αυτές οι διευθύνσεις λέγονται και **pay-to-public-key-hash (P2PKH)**.

Εκτός από τις κλασσικές διευθύνσεις που όπως είπαμε αρχίζουν από 1 υπάρχουν διευθύνσεις που αρχίζουν από 3 και τις ονομάζουμε **pay-to-script hash (P2SH)**. Αυτές ορίζουν ως δικαιούχο μίας συναλλαγής bitcoin την τιμή κατακερματισμού ενός script (δέσμη ενεργειών), αντί για τον ιδιοκτήτη ενός δημόσιου κλειδιού. Τα κεφάλαια που στέλνονται σε 3 διευθύνσεις χρειάζονται κάτι περισσότερο από την επίδειξη του hash ενός δημοσίου κλειδιού και της διεύθυνσης ενός ιδιωτικού κλειδιού σαν απόδειξη ιδιοκτησίας. Οι απαιτήσεις ορίζονται την στιγμή που δημιουργείται η διεύθυνση, μέσα στο script, και όλες οι εισροές σε αυτή την διεύθυνση θα επιβαρυνθούν με τις απαιτήσεις αυτές. Μία διεύθυνση P2SH δημιουργείται από ένα script συναλλαγής, το οποίο ορίζει το ποιός μπορεί να ξοδέψει μία συναλλαγή εκροής.

Η συνηθέστερη εφαρμογή της P2SH είναι οι λεγόμενες **multisignature υπογραφές**. Όπως υποδηλώνει το όνομα, το script επιβάλλει περισσότερες από μία υπογραφές για την απόδειξη της ιδιοκτησίας και επομένως για το ξόδεμα των κεφαλαίων. Το χαρακτηριστικό αυτό απαιτεί M το πλήθος υπογραφών από ένα σύνολο N το πλήθος κλειδιών, με $M \leq N$. Οι υπογραφές αυτές είναι το ανάλογο των υπογραφών που θα χρειάζονταν για να γίνει μία πληρωμή σε κάποιον προμηθευτή μίας εταιρείας από το λογιστήριο αυτής.

Πορτοφόλια- Wallets

Ένα πορτοφόλι bitcoin είναι απλά ένας αποθηκευτικός χώρος ζευγών ιδιωτικών και δημοσίων κλειδιών, ένα αρχείο που λέγεται "wallet.dat". Το αρχείο αυτό δεν περιέχει νομί-

σματα bitcoin. Τα bitcoin υπάρχουν καταγεγραμμένα στην blockchain στο δίκτυο bitcoin. Ο έλεγχος των νομισμάτων από τους χρήστες γίνεται υπογράφοντας τις συναλλαγές (transactions) με τα κλειδιά που έχουν στο πορτοφόλι τους. Οι χρήστες υπογράφουν τις συναλλαγές τους με τα κλειδιά και ως εκ τούτου αποδεικνύουν ότι έχουν στην κατοχή τους τις συναλλαγές εκροής (transaction outputs) δηλαδή τα νομίσματά τους. Τα νομίσματα αποθηκεύονται στην blockchain με την μορφή συναλλαγών εκροής.

3.3 Συναλλαγές - Transactions

Η συναλλαγή (transaction) είναι ο μηχανισμός με τον οποίο αποστέλονται και λαμβάνονται τα bitcoin. Με την συναλλαγή, ο ιδιοκτήτης κάποιας ποσότητας bitcoin μεταφέρει την κυριότητα που έχει σε αυτά, σε κάποια άλλη διεύθυνση.

Η συναλλαγή (transaction) είναι η βασική λειτουργία του οικοσυστήματος του Bitcoin. Μία transaction δεν μεταφέρει απλά μία ποσότητα από μία διεύθυνση bitcoin σε μία άλλη. Μία transaction μπορεί να μεταφέρει bitcoin μεταξύ πολλών εισροών (inputs) και εκροών (outputs). Κάθε input περιέχει μία συναλλαγή και μία διεύθυνση στην οποία αποστέλεται η ποσότητα των bitcoin ενώ κάθε output είναι μία διεύθυνση που λαμβάνει τα bitcoin μαζί με την ποσότητα των bitcoin που αποστέλονται σε αυτή τη διεύθυνση.

Η συναλλαγή είναι μία μεταφορά ποσότητας bitcoin που μεταδίδεται στο δίκτυο και συλλέγεται σε block. Η συναλλαγή αναφέρεται σε ήδη υπάρχουσες συναλλαγές εκροών (transaction outputs) και τις μετατρέπει σε καινούργιες συναλλαγές εισροών (transactions inputs). Οι συναλλαγές δεν είναι κρυπτογραφημένες και ο οποιοσδήποτε μπορεί να τις δει στο δίκτυο. Μετά από αρκετές επιβεβαιώσεις των συναλλαγών, αυτές μπορούν να θεωρηθούν αμετάκλητες.

Οι συναλλαγές λένε στο δίκτυο ότι ο ιδιοκτήτης ενός αριθμού bitcoin έχει εξουσιοδοτήσει την μεταφορά αυτών σε κάποιον άλλο χρήστη. Ο νέος ιδιοκτήτης μπορεί να δημιουργήσει μία νέα συναλλαγή και να μεταφέρει αυτά η μέρος τους σε κάποιον άλλο κτλ. Έτσι δημιουργείται μία αλυσίδα ιδιοκτησίας. Τις συναλλαγές μπορούμε να τις παρομοιάσουμε με εγγραφές σε ένα λογιστικό βιβλίο. Κάθε συναλλαγή αποτελείται από συναλλαγές εισόδου που εγγράφονται σαν χρεώσεις σε ένα υπάρχον λογαριασμό bitcoin και συναλλαγές εξόδου που εγγράφονται σαν πιστώσεις σε κάποιον άλλο λογαριασμό bitcoin. Η κάθε συναλλαγή περιέχει απόδειξη ιδιοκτησίας για κάθε συναλλαγή εισόδου που μεταβιβάζεται με την μορφή μίας ψηφιακής υπογραφής η οποία μπορεί να επαληθευτεί από οποιονδήποτε. Σε όρους bitcoin 'ξοδεύω' σημαίνει υπογράφω μία συναλλαγή που μεταφέρει αξία από μία προηγούμενη συναλλαγή σε ένα καινούργιο ιδιοκτήτη, ο οποίος αναγνωρίζεται από μία

διεύθυνση bitcoin.

Οι συναλλαγές είναι σαν εγγραφές σε ένα λογιστικό βιβλίο. Κάθε συναλλαγή περιέχει μία ή περισσότερες 'εισροές' (inputs), οι οποίες είναι χρεώσεις έναντι ενός λογαριασμού bitcoin. Από την άλλη πλευρά της συναλλαγής υπάρχουν μία ή περισσότερες εκροές (outputs), οι οποίες είναι πιστώσεις που προστίθενται σε ένα λογαριασμό bitcoin. Τον άθροισμα των εισροών και των εκροών δεν είναι πάντα ίσο με την συνολική αξία. Οι εκροές έχουν αθροισμα ελαφρώς μικρότερο από τις εισροές και η διαφορά τους είναι η λεγόμενη αμοιβή συναλλαγής (transaction fee) η οποία πληρώνεται στο εξορύκτη (miner).

Οι συναλλαγές μεταφέρουν αξία από συναλλαγές εισροής σε συναλλαγές εκροής. Μία εισροή δηλώνει από που προέρχεται η αξία, συνήθως από μία προηγούμενη εκροή. Μία εκροή εκχωρεί την αξία σε ένα καινούργιο ιδιοκτήτη συσχετίζοντάς τη με ένα κλειδί. Το κλειδί προορισμού λέγεται βάρος ή επιβάρυνση (encumbrance) και θέτει μία απαίτηση για υπογραφή ώστε η αξία ή μέρος της να μπορεί να εξαργυρωθεί σε μελλοντικές συναλλαγές. Εκροές από μία συναλλαγή μπορούν να χρησιμοποιηθούν σαν εισροές σε μία νέα συναλλαγή, δημιουργώντας έτσι μία αλυσίδα ιδιοκτησίας κατά την μεταφορά της αξίας από ιδιοκτήτη σε ιδιοκτήτη.

3.3.1 Εκπομπή και διάδοση των συναλλαγών στο δίκτυο bitcoin

Μία συναλλαγή πρέπει πρώτα να παραδοθεί στο δίκτυο bitcoin ώστε να διαδοθεί σε όλους τους κόμβους και κατόπιν να περιληφθεί στην αλυσίδα. Μία συναλλαγή bitcoin έχει μέγεθος περίπου 300 με 400 bytes δεδομένων και πρέπει να φθάσει σε οποιονδήποτε κόμβο από τους χιλιάδες του δικτύου. Οι αποστολείς των συναλλαγών δεν χρειάζεται να εμπιστεύονται τους κόμβους για την διάδοσή τους όσο χρησιμοποιούν περισσότερους από ένα κόμβους για να επιβεβαιώσουν ότι η συναλλαγή διαδίδεται. Οι κόμβοι από την άλλη πλευρά, δεν χρειάζεται να επμπιστεύονται τους αποστολείς των συναλλαγών ή να καθορίζουν την ταυτότητα των αποστολέων. Επειδή κάθε συναλλαγή υπογράφεται και δεν περιέχει εμπιστευτικές πληροφορίες σε αντίθεση για παράδειγμα με μία πιστωτική κάρτα, μπορεί να διαδοθεί στο δίκτυο χρησιμοποιώντας οποιοδήποτε κανάλι μεταφοράς, όπως WiFi, Bluetooth, barcodes, μέσω ιστοσελίδων, δορυφόρων, ραδιοσημάτων, μηνυμάτων σε κανάλια chat, Skype κ.α.

Από την στιγμή που η συναλλαγή στέλνεται σε οποιονδήποτε κόμβο του δικτύου, θα επικυρωθεί από αυτόν τον κόμβο. Εάν είναι έγκυρη, ο κόμβος αυτός θα την προωθήσει και στους άλλους κόμβους με τους οποίους είναι συνδεδεμένος και θα σταλεί ένα μήνυμα επιτυχίας στον δημιουργό της. Εάν είναι ακύρη ο κόμβος θα την απορρίψει στέλνοντας ταυτόχρονα μήνυμα αποτυχίας στον δημιουργό της. Κάθε έγκυρη συναλλαγή θα προωθηθεί σε τρεις ή τέσσερεις γειτονικούς κόμβους, κάθε ένας από αυτούς θα την στείλει αντίστοιχα

σε άλλους κόμβους και σε μερικά λεπτά η συναλλαγή θα διαδοθεί εκθετικά στο δίκτυο εώς ότου την λάβουν όλοι οι συνδεδεμένοι εκείνη τη στιγμή κόμβοι στο δίκτυο. Το δίκτυο bitcoin είναι σχεδιασμένο να διαδίδει τις συναλλαγές και τα blocks σε όλους τους κόμβους με τέτοιο τρόπο ώστε να είναι απρόσβλητο από επιθέσεις. Για αποφυγή spamming και επιθέσεων τύπου denial of service, κάθε κόμβος επικυρώνει ανεξάρτητα κάθε συναλλαγή, προτού την διαδόσει στο δίκτυο. Με αυτόν τον τρόπο, μία συναλλαγή που έχει παραμορφωμένα στοιχεία δεν μπορεί να διαδοθεί πέραν του πρώτου κόμβου που θα την ελέγξει.

3.3.2 Δομή της Συναλλαγής

Η συναλλαγή είναι μία δομή δεδομένων που κωδικοποιεί μία μεταφορά αξίας από μία πηγή κεφαλαίου (εισροή-input), σε κάποιο προορισμό (εκροή-output). Μία συναλλαγή περιέχει διάφορα πεδία, οπως φαίνεται στον επόμενο πίνακα:

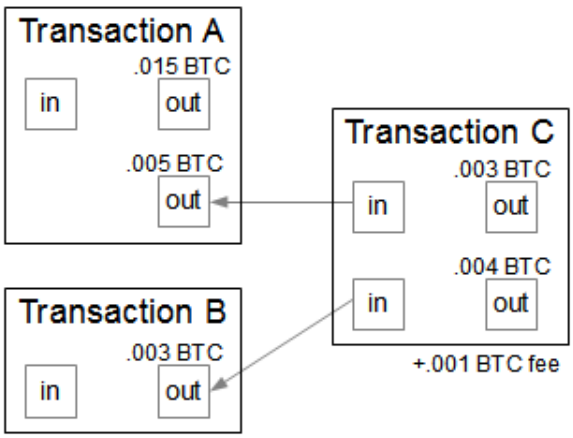
Πίνακας 3.3.1: Δομή μίας Συναλλαγής.

Μέγεθος	**Πεδίο**	**Περιγραφή**
4 bytes	Έκδοση Λογισμικού	Καθορισμός κανόνων της συναλλαγής
1–9 bytes (VarInt)	Μετρητής Εισροών	Πόσες εισροές περιλαμβάνονται
Variable	Εισροές	Μία ή περισσότερες συναλλαγές εισροών
1–9 bytes (VarInt)	Μετρητής Εκροών	Πόσες εκροές περιλαμβάνονται
Variable	Εκροές	Μία ή περισσότερες συναλλαγές εκροών
4 bytes	Locktime	A Unix time stamp ή αριθμός block

Στο σχήμα 3.1 φαίνεται το εσωτερικό κάποιων συναλλαγών. Κάθε συναλλαγή bitcoin μεταφέρει ποσότητα bitcoin μεταξύ μίας ή περισσοτέρων συναλλαγών εισροής ή εκροής. Κάθε εισροή είναι ταυτόχρονα και συναλλαγή και διεύθυνση που μεταφέρει bitcoin. Κάθε εκροή είναι μία διεύθυνση bitcoin που δέχεται bitcoins μαζί με την ποσότητα των bitcoin που πάνε σε αυτή τη διεύθυνση.

3.3.3 Συναλλαγές Εκροής και Εισροής

Το θεμέλιο μίας συναλλαγής bitcoin είναι η συναλλαγή εκροής (transaction output). Οι συναλλαγές εκροής είναι αδιαίρετα κομμάτια από bitcoin, καταγεγραμμένα στην blockchain, και αναγνωρισμένα σαν έγκυρα σε ολόκληρο το δίκτυο. Οι πλήρεις κόμβοι του bitcoin, ανιχνεύουν όλες τις διαθέσιμες εκροές, που είναι γνωστές ως **unspent transaction outputs, ή UTXO**. Το σύνολο των εκροών αυτών, λεγεται σύνολο UTXO και το πλήθος τους αυτή τη στιγμή είναι πολλά εκατομμύρια. Κάθε συναλλαγή αναπαριστά και μία αλλαγή στο σύνολο των UTXO.



Σχήμα 3.1: Απλή συναλλαγή Bitcoin

Όταν το πορτοφόλι ένός χρήστη δεχθεί ένα ποσό bitcoin, αυτό σημαίνει ότι το το πορτοφόλι ανίχνευσε μία UTXO η οποία μπορεί να ξοδευθεί με την χρήση των κλειδιών του συγκεκριμένου πορτοφολιού. Έτσι το υπόλοιπο σε bitcoin ενός πορτοφολιού είναι το άθροισμα όλων των UTXO που μπορεί να ξοδέψει το πορτοφόλι. Προφανώς αυτές οι UTXO είναι διασκορπισμένες ανάμεσα σε εκατοντάδες συναλλαγές και block της αλυσίδας. Εάν φανταστούμε τις UTXO σαν π.χ το χαρτονόμισμα των 5 ευρώ, γνωρίζουμε ότι μπορούμε να κάνουμε συναλλαγή με αυτό αλλά δεν μπορούμε να το κόψουμε στα δύο ή περισσότερο.

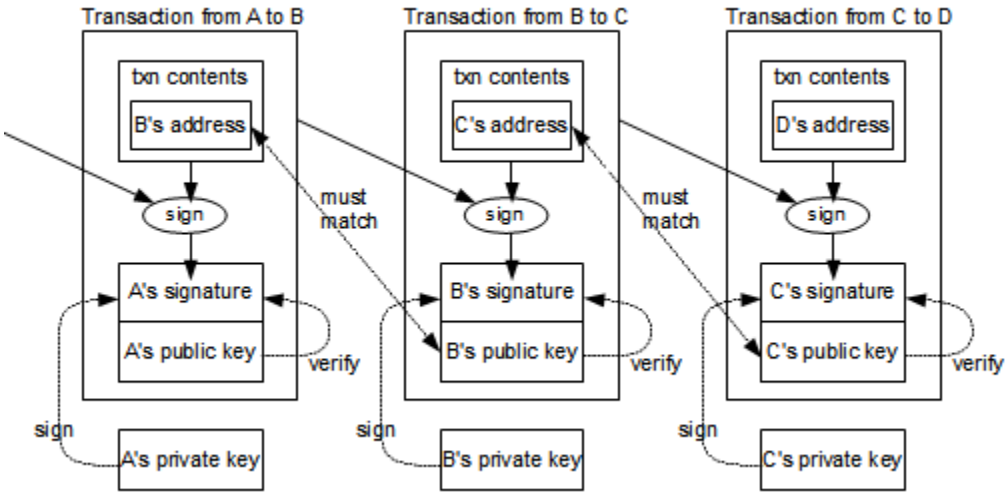
Οι εκροές αυτές από την στιγμή που δημιουργούνται είναι αδιαίρετες και μοναδικές. Μία UTXO (όπως ακριβώς και ένα συμβατικό νόμισμα ή χαρτονόμισμα) θα καταναλωθεί πλήρως από μία συναλλαγή. Αν είναι μεγαλύτερη από το ποσό συναλλαγής, πάλι θα καταναλωθεί πλήρως, αλλά όπως και σε μία εγχρήματη συναλλαγή θα δημιουργήσει ρέστα. Δηλάδή αν π.χ έχουμε μία UTXO 5-Bitcoin και πληρώσουμε για κάτι που αξίζει 1-Bitcoin, τότε η συναλλαγή θα καταναλώσει ολόκληρη την UTXO των 5-Bitcoin και θα παράξει δύο συναλλαγές εκροής: Μία αξίας 1-Bitcoin που θα πληρωθεί στον δικαιούχο της αμοιβής και άλλη μία αξίας 4-Bitcoin που θα επιστραφεί πίσω στο πορτοφόλι μας.

Παρόμοια μία συναλλαγή μπορεί να δημιουργηθεί από τις διαθέσιμες UTXO που έχει ο χρήστης στην κατοχή του, στην περίπτωση που το συνολικό ποσό δεν καλύπτεται από μία UTXO, όπως ακριβώς θα συνέβαινε αν θέλαμε να πληρώσουμε ένα ποσό συνδυάζοντας μικρότερες χρηματικές μονάδες μεταξύ τους. Το πορτοφόλι του χρήστη συνθέτει ένα ποσό από τις υπάρχουσες UTXO ίσης ή μεγαλύτερης αξίας από το ποσό που πρέπει να πληρωθεί. Όλα αυτά γίνονται αυτόματα από την εφαρμογή του πορτοφολιού χωρίς την ανάμειξη του χρήστη.

Μία συναλλαγή καταναλώνει προηγούμενες UTXO's και δημιουργεί νέες συναλλαγές εκροής οι οποίες μπορούν να χρησιμοποιηθούν σε μελλοντικές συναλλαγές. Με αυτόν τον τρόπο, μέρη bitcoin μεταφέρονται από ιδιοκτήτη σε ιδιοκτήτη σε μία αλυσίδα συναλλαγών, καταναλώνοντας και δημιουργώντας UTXO's.

Η μόνη εξαίρεση στην αλυσίδα αυτή είναι ένας ειδικός τύπος συναλλαγής που λέγεται **συναλλαγή βάσης νομίσματος** ή **coinbase transaction** και είναι η πρώτη συναλλαγή σε κάθε block. Η συναλλαγή αυτή τοποθετείται εκεί από τον "νικητή" εξορύκτη, σαν ανταμοιβή για την εξόρυξη. Αυτή η συναλλαγή δεν καταναλώνει UTXO's και είναι ο τρόπος με τον οποίον δημιουργούνται τα καινούργια bitcoin κατά την διάρκεια της εξόρυξης.

Υπογραφή, επικύρωση και σύνδεση των συναλλαγών



Σχήμα 3.2: Υπογραφή, επίκυρωση και σύνδεση συναλλαγών (απλή μορφή)

Στο σχήμα 3.2 βλέπουμε πως υπογράφονται, επαληθεύονται και συνδέονται οι συναλλαγές μεταξύ τους. Στην μεσαία συναλλαγή μεταφέρεται μία ποσότητα bitcoin από τον B στον C. Τα περιεχόμενα της συναλλαγής (συμπεριλαμβανομένης της τιμής κατακερματισμού - hash value της προηγούμενης συναλλαγής) μαζί με την διεύθυνση του C κατακερματίζονται και υπογράφονται με το ιδιωτικό κλειδί του B. Επιπλέον στην συναλλαγή αυτή περιέχεται και το δημόσιο κλειδί του B. Αυτό είναι αναγκαίο για να μπορέσουν οι κόμβοι του δικτύου να επικυρώσουν την συναλλαγή. Για την επικύρωση, λαμβάνει χώρα η ακόλουθη διαδικασία:

(i) Το δημόσιο κλειδί του Β πρέπει να αντιστοιχεί στην διεύθυνση του Β που βρίσκεται στην συναλλαγή από τον Α στον Β. Έτσι αποδεικνύεται ότι το δημόσιο κλειδί του Β είναι έγκυρο. Η διαδικασία αυτή περιγράφεται αναλυτικά στο παράδειγμα 2, βήματα (iv) έως και (vii).

(ii) Η υπογραφή του Β στην συναλλαγή (Β στον C) μπορεί να επικυρωθεί με χρήση του δημοσίου κλειδιού του Β που περιλαμβάνεται στην συναλλαγή. Η διαδικασία αυτή περιγράφεται αναλυτικά στο κεφάλαιο 2 (2.4.7).

Τα βήματα αυτά εξασφαλίζουν ότι η συναλλαγή είναι έγκυρη και ότι έχει εξουσιοδοτηθεί από τον Β. Για επιπρόσθετη ασφάλεια (παρά το γεγονός ότι η εύρεση του ιδιωτικού κλειδιού από το δημόσιο είναι πρακτικά αδύνατη) το δημόσιο κλειδί του Β δεν γίνεται γνωστό, παρά μόνο κατά την διαδικασία της συναλλαγής.

Με αυτή, την σαν αλυσίδα διαδικασία, γίνεται η μεταφορά bitcoin από διεύθυνση σε διεύθυνση.

Κεφάλαιο 4

Το δίκτυο Bitcoin

4.1 Αρχιτεκτονική δικτύου Peer-to-Peer

Ορισμός 4.1.1. ***Δίκτυο*** *(peer-to-peer network) Είναι ένα δίκτυο δύο ή περισσοτέρων υπολογιστών, που μέσω ενός πρωτοκόλλου επικοινωνίας τους επιτρέπει να μοιράζονται ισοδύναμα τους πόρους τους χωρίς την μεσολάβηση κάποιου κεντρικού εξηπηρετητή(server). Κάθε μέλος του δικτύου είναι ταυτόχρονα και εξυπηρετητής(server) και εξυπηρετούμενος(client).*

Ορισμός 4.1.2. ***Τοπολογία δικτύου*** *(network topology) Είναι η διάταξη των στοιχείων ενός δικτύου επικοινωνίας.*

Ορισμός 4.1.3. ***Πλεγματοειδές δίκτυο*** *(mesh network) Είναι μία τοπολογία δικτύου στη οποία οι κόμβοι επικοινωνούν άμεσα, δυναμικά και μη ιεραρχικά, με όσους το δυνατόν περισσότερους κόμβους του δικτύου γίνεται, με σκοπό την αποτελεσματικότερη δρομολόγηση των δεδομένων από και πρός τους εξυπηρετούμενους(clients).*

Το bitcoin είναι δομημένο σαν ένα δίκτυο ομότιμων συνδέσεων στην κορυφή του internet. Ο όρος peer-to-peer ή P2P σημαίνει ότι οι υπολογιστές που συμμετέχουν μέσω του πρωτόκολλου επικοινωνίας bitcoin(bitcoin protocol) μοιράζονται ισοδύναμα τους πόρους τους χωρίς την μεσολάβηση κάποιου κεντρικού εξηπηρετητή(server), δεν υπάρχουν κόμβοι με ειδικά προνόμια και όλοι οι κόμβοι μοιράζονται το φορτίο της παροχής υπηρεσιών δικτύου. Κάθε μέλος του δικτύου είναι ταυτόχρονα και εξυπηρετητής (server) και εξυπηρετούμενος (client). Όλοι οι κόμβοι επικοινωνούν μεταξύ τους σε ένα πλεγματοειδές δίκτυο (mesh network) με επίπεδη τοπολογία δικτύου.

Τα P2P δίκτυα είναι κληρονομικά ανθεκτικά, αποκεντρωμένα και ανοικτά. Η αρχιτεκτονική του bitcoin δεν είναι απλά μία επιλογή τοπολογίας. Το bitcoin είναι ένα P2P σύστημα ψηφιακού χρήματος και η αρχιτεκτονική του δικτύου του το θεμέλιο αυτού του χαρακτη-

ριστικού. Η αποκέντρωση του ελέγχου μπορεί να επιτευχθεί μόνο σε ένα επίπεδο αποκεντρωμενό συναινετικό P2P δίκτυο.

Ο όρος **bitcoin network** αναφέρεται στο σύνολο των κόμβων που τρέχουν το P2P πρωτόκολλο του bitcoin. Επιπλέον του πρωτοκόλλου bitcoin ύπάρχουν και άλλα, όπως το Stratum που χρησιμοποιείται για εξόρυξη και ελαφριά ή κινητά πορτοφόλια. Όλα αυτά τα πρωτόκολλα συνδέονται μεταξύ τους δημιουργώντας το εκτεταμένο δίκτυο bitcoin.

4.2 Τύποι Κόμβων - Node Types

Οι κόμβοι στο P2P δίκτυο του bitcoin είναι ισότιμοι, όμως μπορεί να έχουν διαφορετικούς ρόλους βασισμένους στην λειτουργικότητά τους. Ένας κόμβος bitcoin περιέχει διάφορες λειτουργείες: κόμβος δρομολόγησης δικτύου N (network routing node), πλήρης βάση δεδομένων της αλυσίδας B (full blockchain database), εξόρυξη M(mining) και υπηρεσίες πορτοφολιού W (wallet services), δρολογητής δεξαμενής P, δρομολογητής Stratum S.

Κάποιοι κόμβοι, λέγονται πλήρεις κόμβοι και περιέχουν ένα πλήρες αντίγραφο της blockchain. Είναι αυτόνομοι και μπορούν να επικυρώσουν κάθε συναλλαγή χωρίς εξωτερικές αναφορές. Κάποιοι κόμβοι διατηρούν ένα υποσύνολο της blockchain και επικυρώνουν τις συναλλαγές χρησιμοποιώνταις μία μέθοδο που λέγεται **απλοποιημένη επικύρωση συναλλαγής - simplified payment verification (SPV)**. Τέτοιο κόμβοι λέγονται κόμβοι SPV ή lightweight κόμβοι. Ακολουθούν διάφοροι τύποι κόμβων:

- **Reference Client(Bitcoin Core)**. Περιέχει τις ακόλουθες λειτουργίες W, M, B, N στο P2P δίκτυο bitcoin.
- **Full Block Chain Node**. Περιέχει τις ακόλουθες λειτουργίες B, N στο P2P δίκτυο bitcoin.
- **Solo Miner**. Περιέχει τις ακόλουθες λειτουργίες M, B, N στο P2P δίκτυο bitcoin.
- **Lightweight (SPV) Wallet**. Περιέχει τις ακόλουθες λειτουργίες W, N στο P2P δίκτυο bitcoin. Δεν περιέχει αντίγραφο της αλυσίδας.
- **Mining Nodes**. Περιέχει τις ακόλουθες λειτουργίες M, S ή M, P.
- **Lightweight (SPV) Stratum Wallet**. Περιέχει τις ακόλουθες λειτουργίες W, S. Δεν περιέχει αντίγραφο της αλυσίδας.

4.3 Πλήρεις Κόμβοι - Full Nodes

Οι πλήρεις κόμβοι είναι κόμβοι που διατηρούν ένα πλήρες αντίγραφο της blockchain με όλες τις συναλλαγές, το οποίο κατασκευάζουν και επικυρώνουν ξεκινώντας από το πρώτο block (genesis block) μέχρι το τελευταίο γνωστό στο δίκτυο block. Ένας πλήρης κόμβος μπορεί επικυρώσει οποιαδήποτε συναλλαγή ανεξάρτητα από κάθε άλλο κόμβο ή άλλη πηγή πληροφορίας. Με το που θα συνδεθεί ένας πλήρης κόμβος με τους ομότιμούς του στο δίκτυο θα προσπαθήσει να κατασκευάσει μία πλήρη blockchain. Έαν πλήρης κόμβος είναι καινούργιος τότε όλη η διαδικασία ξεκινάει από το μόνο γνωστό block, το γνωστό ως genesis block το οποίο είναι ενσωματωμένο στο client software. Ξεκινώντας με το block 0, ο καινούργιος κόμβος θα πρέπει να κατεβάσει εκατοντάδες χιλιάδες blocks για να μπορέσει να συγχρονιστεί με το δίκτυο και να εγκαταστήσει μία πλήρη αλυσίδα.

Η λειτουργία ενός πλήρη κόμβου σήμερα απαιτεί πολύ μεγάλο αποθηκευτικό χώρο για την αποθήκευση όλης της αλυσίδας. Για να συγχρονιστεί ο πλήρης κόμβος με το δίκτυο σήμερα, ο χρόνος που μπορεί να χρειαστεί εξαρτάται από τις προδιαγραφές του υπολογιστή και από το μέγεθος της αλυσίδας. Ο χρόνος μπορεί να κυμαίνεται από μερικές ημέρες έως κάποιους μήνες.

4.4 Simplified Payment Verification (SPV) Nodes

Δεν έχουν όλοι οι κόμβοι την δυνατότητα αποθήκευσης ολοκληρης της αλυσίδας. Και αυτό γιατί κάποιοι bitcoin clients είναι σχεδιασμένοι για συσκευές με μικρό αποθηκευτικό χώρο και ενεργειακούς περιορισμούς όπως tablets, κινητά τηλέφωνα κ.α. Για τέτοιες συσκευές χρησιμοποιείται η μέθοδος της απλοποιημένης επικύρωσης συναλλαγής ή simplified payment verification (SPV) method, η οποία τους επιτρέπει να λειτουργούν χωρίς την αποθήκευση ολόκληρης της blockchain. Τέτοιοι τύποι λέγονται SPV ή lightweight clients. Οι SPV κόμβοι κατεβάζουν μόνο τις επικεφαλίδες των block και όχι τις συναλλαγές που υπάρχουν σε κάθε block. Με αυτόν τον τρόπο η αλυσίδα των block είναι περίπου 1000 φορές μικρότερή από ότι η αλυσίδα σε ένα πλήρη κόμβο. Η επικύρωση των συναλλαγών γίνεται με διαφορετικό τρόπο που στηρίζεται στην αναζήτηση συγκεριμένων μερών της αλυσίδας στους ομότιμους κόμβους.

Ένας κόμβος SPV επικυρώνει συναλλαγές με αναφορά στο πόσο βαθιά είναι στην αλυσίδα. Ένας πλήρης κόμβος θα κατασκευάσει μία πλήρως επιβεβαιωμένη και επικυρωμένη αλυσίδα που αποτελείται από χιλιάδες block και συναλλαγές μέχρι το genesis block, ενώ ένας κόμβος SPV θα επικυρώσει την αλυσίδα των μπλοκ εκτός των συναλλαγών που περιέχονται σε αυτά, και θα συνδέσει αυτή την αλυσίδα με την συναλλάγή που τον ενδιαφέρει.

4.5 Δεξαμενές Συναλλαγών - Transaction Pools

Σχεδόν κάθε κόμβος στο δικτυο bitcoin διατηρεί μία προσωρινή λίστα ανεπιβεβαίωτων συναλλαγών που λέγεται δεξαμενή συναλλαγών. Οι κόμβοι χρησιμοποιούν αυτή τη δεξαμενή για να παρακολουθούν τις συναλλαγές που ναι μεν έχουν γίνει γνωστές στο δίκτυο αλλά δεν έχουν συμπεριληφθεί ακόμα στην αλυσίδα. Για παράδειγμα, ένας κόμβος πορτοφολιού θα χρησιμοποιήσει τη δεξαμενή για να ανιχνεύσει εισερχόμενες πληρωμές στο πορτοφόλι οι οποίες έχουν γίνει ήδη γνωστές στο δίκτυο αλλά δεν έχουν ακόμη επιβεβαιωθεί. Καθώς οι συναλλαγές λαμβάνονται και επαληθεύονται, προστίθενται στη δεξαμενή και μεταδίδονται σε γειτονικούς κόμβους για να διαδοθούν στο δίκτυο.

Κάποιοι κόμβοι διατηρούν μία δεξαμενή για ορφανές συναλλαγές, συναλλαγές των οποίων οι εισροές αναφέρονται σε συναλλαγές οι οποίες δεν έχουν γίνει ακόμα γνωστές στο δίκτυο, δηλαδή είναι αγνώστου γονέα. Αυτές μαζεύονται στη δεξαμενή ορφανών συναλλαγών έως ότου να εμφανιστεί η συναλλαγή γονέας στο δίκτυο. Όταν μία συναλλαγή προστεθεί στη δεξαμενή συναλλαγών, ελέγχεται η δεξαμενή των ορφανών συναλλαγών για οποιαδήποτε ορφανή συναλλαγή που αναφέρεται στην αρχική συναλλαγή. Αν βρεθεί αντίστοιχη ορφανή συναλλαγή ΄που έχει σχέση με αυτή τότε αφαιρείται από την δεξαμενή ορφανών συναλλαγών και προστίθεται στη δεξαμενή συναλλαγών, συμπληρώνοντας έτσι την αλυσίδα που άρχισε με την συναλλαγή γονέα. Η διαδικασία αυτή επαναλαμβάνεται αναδρομικά και αναζητούνται περαιτέρω απόγονοι μέχρι που να μην υπάρχουν πλέον άλλοι απόγονοι. Με αυτή τη διαδικασία ενώνονται οι ορφανές συναλλαγές με τους γονείς τους σε όλο το βάθος της αλυσίδας. Και οι δύο δεξαμενές αποθηκεύονται στην προσωρινή μνήμη και μπορεί να διαφέρουν στο περιεχόμενό τους από κόμβο σε κόμβο.

Κεφάλαιο 5

Η Αλυσίδα Ομάδων Συναλλαγών - The Blockchain

5.1 Εισαγωγή

Η δομή δεδομένων της blockchain είναι μία διατεταγμένη, συνδεδεμένη προς τα πίσω λίστα, αλυσίδα ομάδων συναλλαγών (blockchain). Η αλυσίδα μπορεί να αποθηκευτεί σαν μία απλή βάση δεδομένων. Ο εξυπηρετητής Bitcoin Core αποθηκεύει τα μεταδεδομένα χρησιμοποιώντας την LevelDB βάση δεδομένων του Google. Οι ομάδες συναλλαγών (blocks) συνδέονται προς τα πίσω, με το κάθε block να αναφέρεται στο προηγούμενο block στην αλυσίδα. Η αλυσίδα απεικονίζεται συχνά σαν μία κάθετη στοίβα, με block στιβαγμένα το ένα πάνω στο άλλο έχοντας σαν θεμέλιο block το λεγόμενο **genesis block**. Λόγω αυτής της απεικόνισης χρησιμοποείται ο όρος **ύψος - height** ο οποίος αναφέρεται στην απόσταση από το πρώτο (genesis) block καθώς και ο όρος κορυφή - top/tip που αναφέρεται στο πιο πρόσφατα προστιθέν block στην αλυσίδα.

Κάθε block μέσα στην αλυσίδα αναγνωρίζεται από μια τιμή hash, που παράγεται χρησιμοποιώντας τον SHA256 στην επικεφαλίδα (header) του block. Επίσης κάθε block αναφέρεται στο προηγούμενό του block, γνωστό και ως **γονικό block - parent block**, μέσω του πεδίου 'previous block hash' που υπάρχει στην επικεφαλίδα του block. Για να γίνει πιο κατανοητό, κάθε block περιέχει την τιμή hash της επικεφαλίδας του γονικού block, μέσα στην δική του επικεφαλίδα. Αυτή η ακολουθία των τιμών hash συνδέουν κάθε block με το γονικό του, δημιουργώντας έτσι μία αλυσίδα που φθάνει πίσω μέχρι το πρώτο block που δημιουργήθηκε, γνωστό και ως genesis block.

Κάθε block έχει μόνο ένα γονέα, αλλά προσωρινά μπορεί να έχει πολλά παιδιά. Κάθε ένα από τα παιδιά, αναφέρεται στο ίδιο block σαν γονικό και περιέχει την ίδια τιμή hash στο πεδίο "previous block hash". Κατά την διάρκεια ταυτόχρονης ανακάλυψης διαφορετικών block από τους εξορύκτες, δημιουργείται μία προσωρινή κατάσταση η οποία λέγεται

φουρκέτα - fork της αλυσίδας, κατά την οποία δημιουργούνται πολλαπλά παιδιά. Τελικά, μόνο ένα παιδί γίνεται μέρος της αλυσίδας και έτσι η φουρκέτα επιλύεται. Καίτοι ένα block μπορεί να έχει περισσότερα από ένα παιδιά, κάθε block μπορεί να έχει μόνο ένα γονέα. Και αυτό γίνεται γιατί ένα block έχει μόνο ένα πεδίο "previous block hash" που αναφέρει τον μοναδικό του γονέα. Το πεδίο "previous block hash" βρίσκεται μέσα στην επικεφαλίδα του block οπότε και επηρεάζει την τιμή hash του block. Η ταυτότητα του παιδιού αλλάζει αν αλλάξει η ταυτότητα του γονέα. Εάν με οποιοδήποτε τρόπο τροποποιηθεί το block του γονέα, τότε αλλάζει και η τιμή hash του block αυτού. Η αλλαγή στην τιμή hash του γονέα, επιβάλλει αλλαγή στο πεδίο "previous block hash" του παιδιού. Αυτή με τη σειρά της προκαλεί αλλαγή στη τιμή hash του παιδιού, η οποία προκαλεί με τη σειρά της αλλαγή στο αντίστοιχο πεδίο του εγγονού κτλ. Αυτή η αλληλουχία γεγονότων διασφαλίζει ότι όταν ένα block έχει πολλές γενεές που το ακολουθούν, δεν μπορεί να αλλαχθεί χωρίς να προκαλέσει ένα επανυπολογισμό όλων των επόμενων μπλοκ. Επειδή κάτι τέτοιο θα σήμαινε τεράστια υπολογιστική προσπάθεια και επομένως τεράστια κατανάλωση ενέργειας, η ύπαρξη μίας μακριάς αλυσίδας block κάνει την αλυσίδα απρόσβλητη σε αλλαγές, το οποίο είναι και το βασικό χαρακτηριστικό της ασφάλειας του bitcoin.

5.2 Δομή ενός Block

Ένα block είναι μία δομή δεδομένων που συγκεντρώνει τις συναλλαγές ώστε να συμπεριληφθούν στο δημόσιο λογιστικό βιβλίο, το blockchain. Το block απαρτίζεται από μία επικεφαλίδα που περιέχει μεταδεδομένα, ακολοθούμενη από μία μεγάλη λίστα συναλλαγών. Στον παρακάτω πίνακα περιγράφεται η δομή ενός block.

Πίνακας 5.2.1: Δομή ενός block.

Μέγεθος	**Πεδίο**	**Περιγραφή**
4 bytes	μέγεθος του block	Το μέγεθος του block, μετά το πεδίο αυτό
80 bytes	επικεφαλίδα του block	Διάφορα πεδία σχηματίζουν την επικεφαλίδα
1–9 bytes (VarInt)	Μετρητής Συναλλαγών	Πόσες συναλλαγές ακολουθούν
Variable	Συναλλαγές	Εγγεγραμένες συναλλαγές στο block

5.3 Επικεφαλίδα του Block - Block Header

Η επικεφαλίδα του block αποτελείται από τρία σύνολα μεταδεδομένων. Στο πρώτο ύπάρχει αναφορά στην τιμή hash του προηγούμενο block, που συνδέει το παρών block με το

προηγούμενό του στην αλυσίδα. Το δεύτερο σύνολο μεταδεδομένων περιέχει την δυσκολία, την χρονοσήμανση και τον αριθμό nonce και συσχετίζεται με την εξόρυξη. Το τρίτο σύνολο μεταδεδομένων περιλαμβάνει την διάταξη Merkle tree root, μία δομή δεδομένων που χρησιμοποιείται για την αποτελεσματική περίληψη όλων των συναλλαγών. Στον παρακάτω πίνακα περιγράφεται η δομή της επικεφαλίδας ενός block.

Πίνακας 5.3.1: Δομή ενός block.

Μέγεθος	**Πεδίο**	**Περιγραφή**
4 bytes	Έκδοση	Αριθμός έκδοσης του λογισμικού/ για αναβαθμίσεις του πρωτοκόλλου
32 bytes	τιμή hash του προηγούμενου block	Αναφορά στην hash του προηγούμενου (γονέα) block
32 bytes	ρίζα Merkle	Η τιμή hash της ρίζας του δέντρου Merkle των συναλλαγών αυτού του block
4 bytes	Χρονοσήμανση	Ο χρόνος δημιουργίας του block
4 bytes	Στόχος Δυσκολίας	Ο στόχος δυσκολίας του αλγόριθμου απόδειξης εργασίας για το block αυτό
4 bytes	Αριθμός nonce	Ένας μετρητής που χρησιμοποιείται στο αλγόριθμο απόδειξης εργασίας

5.4 Αναγνωριστικά ενός Block - Block Identifiers

5.4.1 Block Header Hash and Block Height

Το αναγνωριστικό ενός block είναι η τιμή κατακερματισμού του (hash value). Δημιουργείται εφαρμόζοντας δύο φορές τον SHA256 στην επικεφαλίδα του block και ονομάζεται **block hash** ή **block header hash**.

$$BlockHeaderhash = SHA256(SHA256(blockheader)) \tag{5.1}$$

Το block hash προσδιορίζει μοναδικά ένα block και οποιοσδήποτε κόμβος μπορεί ανεξάρτητα να το επιβεβαιώσει κατακερματίζοντας την επικεφαλίδα του block. Το block hash δεν περιλαμβάνεται μέσα στα δεδομένα του block αλλά υπολογίζεται από κάθε κόμβο όταν το block μεταδίδεται στο δίκτυο. Ένας άλλος τρόπος για να αναγνωριστεί ένα block είναι από την θέση του στην αλυσίδα και λέγεται **ύψος του block - block height**. Το genesis block έχει ύψος 0. Η τιμή hash του block προσδιορίζεται μοναδικά για κάθε block, ενώ αντίθετα αυτό δεν συμβαίνει με το ύψος του block. Κατα το στάδιο της εξόρυξης, δύο ή και περισσότερα block μπορούν να διαγωνίζονται για το ποιό θα είναι το επικρατέστερο στην αλυσίδα, έχοντας έτσι το ίδιο block height. Αυτό οδηγεί στην δημιουργία διαφορετικών κλάδων της

αλυσίδας (forks) και η επίλυση του προβλήματος αυτού θα συζητηθεί στα επόμενα.

5.5 The Genesis Block

Το πρώτο block στην αλυσίδα ονομάζεται **genesis block** και δημιουργήθηκε το 2009. Είναι η αφετηρία όλων των επόμενων block στην αλυσίδα. Εάν ξεκινήσουμε από οποιοδήποτε block της αλυσίδα προς τα πίσω, θα φθάσουμε τελικά στο genesis block. Κάθε κόμβος ξεκινά με μία αλυσίδα που έχει ένα τουλάχιστον block, το genesis block, κωδικοποιημένο εξαρχής στο λογισμικό bitcoin Core χωρίς να μπορεί να αλλαχθεί. Κάθε κόμβος γνωρίζει την τιμή hash του genesis block, τον χρόνο δημιουργίας του καθώς και την πρώτη συναλλαγή μέσα στο genesis block. Κάθε κόμβος ξεκινά την κατασκευή της αλυσίδας από αυτό το block, του οποίου η τιμή κατακερματισμού του είναι η ακόλουθη:

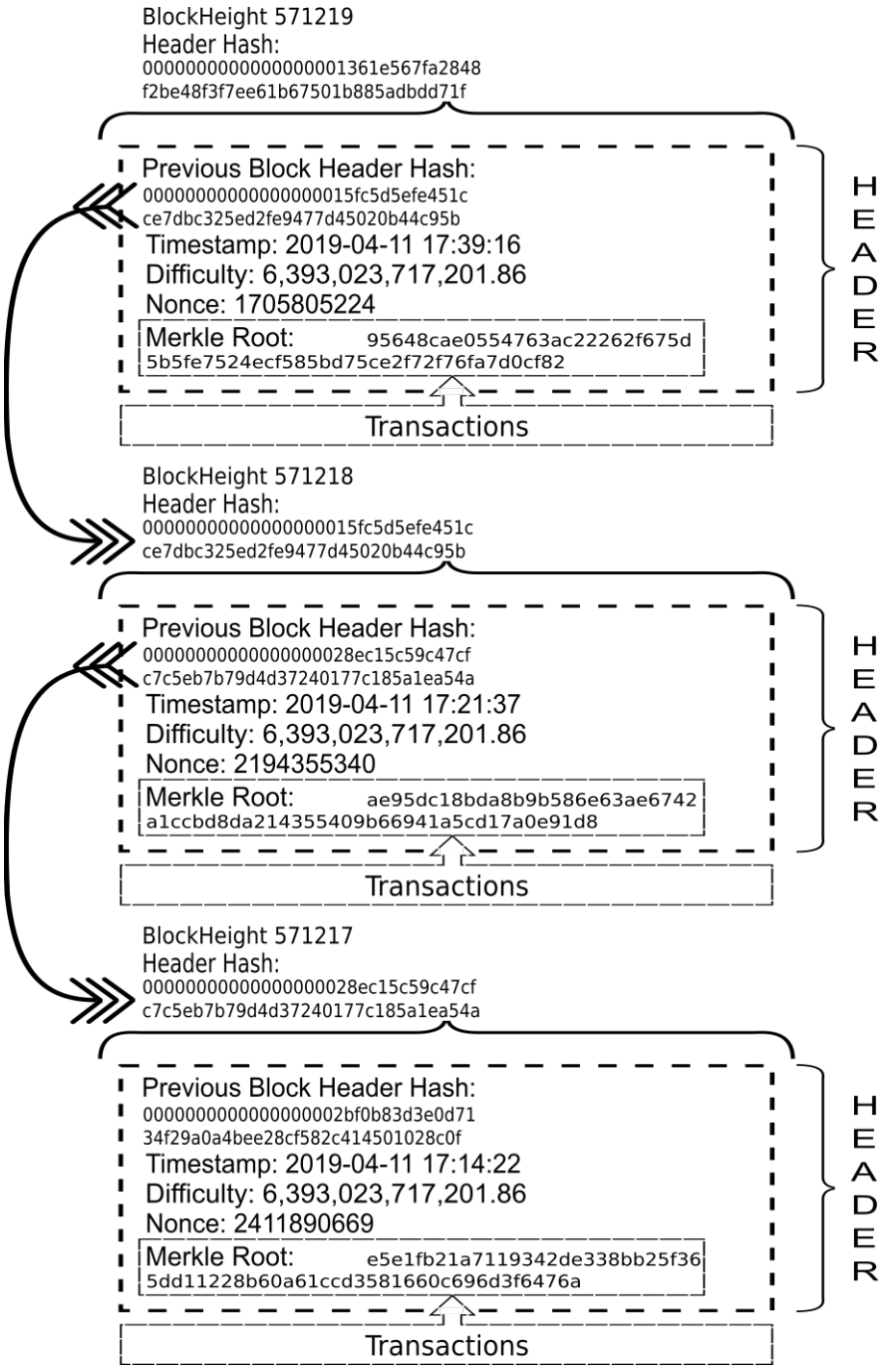
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`

5.6 Σύνδεση των blocks στην αλυσίδα

Όλοι οι πλήρεις κόμβοι του bitcoin διατηρούν τοπικά ένα αντίγραφο της αλυσίδα. Κάθε φορά που ένα νέο block προκύπτει από την εξόρυξη το αντίγραφο ανανεώνεται και η αλυδίδα επεκτείνεται. Καθώς ένας κόμβος λαμβάνει εισερχόμενα block από το δίκτυο, πρέπει πρώτα να τα επικυρώσει και έπειτα να τα ενσωματώσει στην προυπάρχουσα αλυσίδα. Για να συνδεθεί το νέο block στην αλυσίδα, ο κόμβος εξετάζει την επικεφαλίδα του block και διαβάζει το πεδίο “previous block hash”. Για παράδειγμα και χρησιμοποιώντας το σχήμα 5.1 υποθέτουμε ότι ένας κόμβος έχει $571,217$ blocks. Το τελευταίο block που γνωρίζει ο κόμβος είναι το block $521,217$, του οποίου η τιμή κατακερματισμού της επικεφαλίδας του (Header Hash) είναι η ακόλουθη:

`00000000000000000028ec15c59c47cfc7c5eb7b79d4d37240177c185a1ea54a`

Ο κόμβος λαμβάνει ένα νέο block από το δίκτυο και προσπελάζει κατά σειρά τα πεδία της επικεφαλίδας του καινούργιου block καθώς και τις συναλλαγές που αυτό περιέχει. Μέσα στην επικεφαλίδα υπάρχει το πεδίο ’previous block hash’ το οποίο είναι το γνωστό Header Hash του γονικού block, του μπλοκ $521,217$. Άρα το νέο block είναι το παιδί του τελευταίου block της αλυσίδας και επεκτείνει την υπαρχουσα αλυσίδα. Ο κόμβος προσθέτει το νέο block στο τέλος της αλυσίδας καθιστώντας την μακρύτερη, με νέο ύψος το $521,218$. Στο σχήμα 5.1 φαίνεται η αλυσίδα τριών block καθώς και οι συνδέσεις των πεδίων previous block hash και των Header Hash.



Σχήμα 5.1: Σύνδεση των block με αναφορά στην previous block header hash.

5.7 Merkle Trees

Κάθε block στην αλυσίδα περιέχει μία περίληψη όλων των συναλλαγών του block αυτού, χρησιμοποιώντας ένα **δέντρο Merkle (Merkle tree)**.

Τα Merkle trees, εφευρέθηκαν από τον Ralph Merkle to 1979 [37] και είναι μία δομή δεδομένων που χρησιμοποιείται για την περίληψη και την επιβεβαίωση της ακεραιότητας μεγάλων συνόλων δεδομένων. Είναι γνωστά και ως δέντρα δυαδικού κατακερματισμού (binary hash trees). Τα Merkle trees είναι δέντρα στα οποία κάθε κόμβος φύλλων είναι σημασμένος με την κρυπτογραφική τιμή κατακερματισμού (hash) των ετικετών των κόμβων παιδιών του. Τα δέντρα Merkle συνήθως παρουσιάζονται με ανάποδη μορφή δέντρου, ξεκινώντας από πάνω με την ρίζα και ακολουθώντας προς τα κάτω την κλαδική μορφή.

Τα δέντρα Merkle χρησιμοποιούνται στο bitcoin για την δημιουργία μίας περίληψης όλων των συναλλαγών που βρίσκονται σε ένα block. Με αυτό τον τρόπο δημιουργείται μία πολύ γρήγορη και αποτελεσματική διαδικασία επικύρωσης της ενσωμάτωσης ή όχι, μίας συναλλαγής μέσα σε ένα block.

Η κατασκευή ενός δέντρου Merkle έχει ως εξής: ζεύγη κόμβων κατακερματίζονται αναδρομικά έως ότου να μείνει μόνο μία τιμή κατακερματισμού που λέγεται ρίζα ή ρίζα Merkle. Για την κατασκευή αυτή στο bitcoin, χρησιμοποιείται ο κρυπτογραφικός αλγόριθμος κατακερματισμού SHA256 ο οποίος εφαρμόζεται δύο φορές (double SHA256).

Στο παράδειγμα που ακολουθεί (βλέπε σχήμα 5.2) ξεκινάμε με τέσσερεις συναλλαγές 1, 2, 3, 4, οι οποίες σχηματίζουν τα φύλλα ενός δέντρου Merkle. Οι συναλλαγές δεν αποθηκεύονται στο δέντρο Merkle αλλά τα δεδομένα τους κατακερματίζονται. Οι συνόψεις (hash values) τους αποθηκεύονται σε κάθε κόμβο φύλλου H_1, H_2, H_3, H_4 ως εξής:

$$H_N = SHA256(SHA256(Tx(N)) \qquad N = 1, 2, 3, 4 \tag{5.2}$$

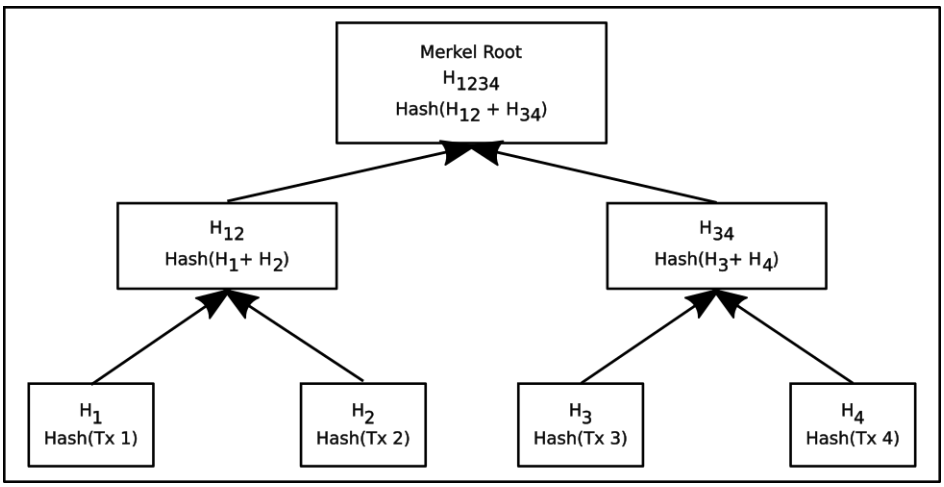
όπου με $Tx(N)$ συμβολίζεται η νιοστή συναλλαγή.

Διαδοχικά ζεύγη κόμβων των φύλλων συσσωματώνονται μαζί και κατακερματίζονται παράγοντας έτσι τον γονικό κόμβο. Για την κατασκευή του γονικού κόμβου H_{12}, οι 32-byte τιμές κατακερματισμού, συσσωματώνονται σε ένα string 64-byte το οποίο στη συνέχεια διπλοκατακερματίζεται για να παράγει τον γονικό κόμβο ως εξής:

$$H_{12} = SHA256(SHA256(H_1 + H_2)) \tag{5.3}$$

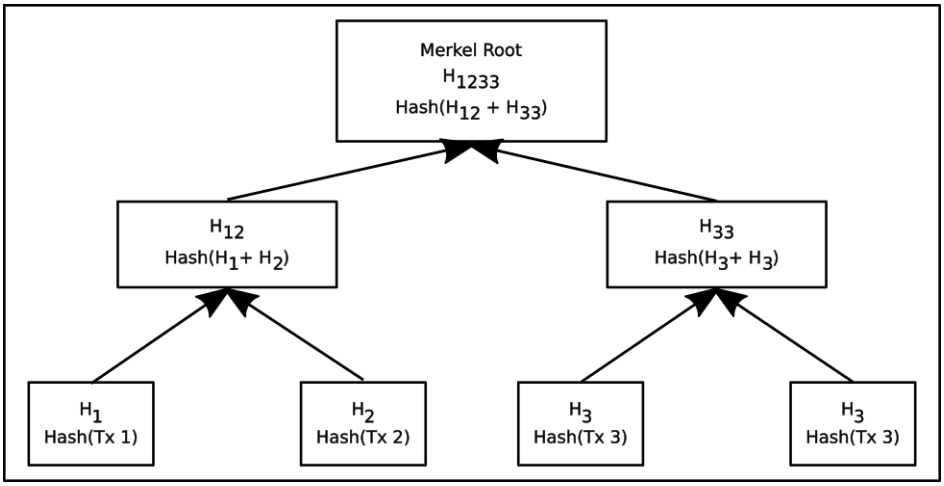
Η διαδικασία συνεχίζεται μέχρι να μείνει μόνο ένας κόμβος στην κορυφή, γνωστός ως ρίζα

Merkle. Η 32-bit τιμή κατακερματισμού αποθηκεύεται στην επικεφαλίδα του block και συνοψίζει όλα τα δεδομένα και στις τέσσερις συναλλαγές.



Σχήμα 5.2: Υπολογισμός άρτιων κόμβων φύλλων σε ένα δέντρο Merkle.

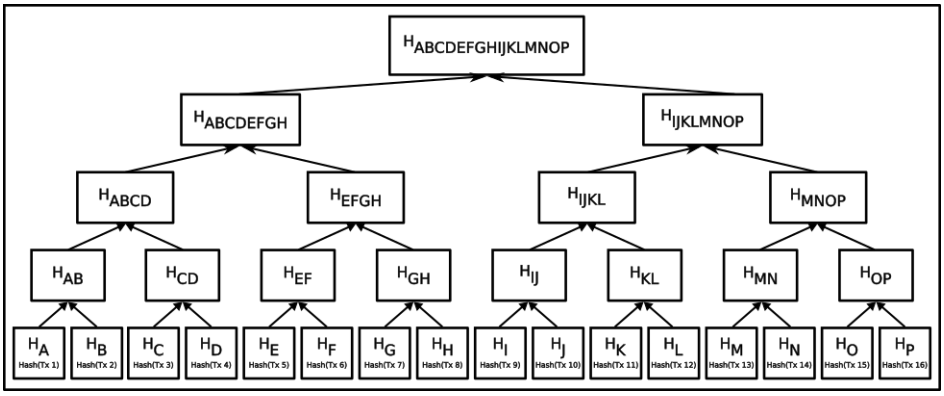
Επειδή τα δέντρα Merkle είναι δυαδικά, χρειάζονται άρτιο αριθμό κόμβο φύλλων. Για να συνοψιστεί περιττός αριθμός συναλλαγών (σχήμα 5.3), η τιμή κατακερματισμού της τελευταίας συναλλαγής αντιγράφεται δημιουργώντας έτσι άρτιο αριθμό φύλλων.



Σχήμα 5.3: Υπολογισμός περιττών κόμβων φύλλων σε ένα δέντρο Merkle.

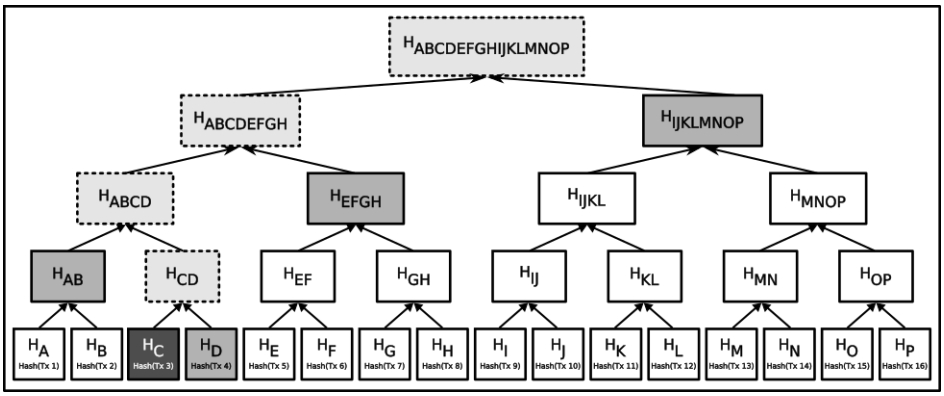
Με τον ίδιο τρόπο μπορεί να κατασκευαστεί ένα δέντρο οποιουδήποτε μεγέθους. Στο bitcoin είναι σύνηθες να έχουμε από εκατοντάδες έως πάνω από χίλιες συναλλαγές σε κάθε block. Αυτές οι συναλλαγές συνοψίζονται με τον ίδιο τρόπο όπως παραπάνω, δημιουργώ-

ντας τελικά μία τιμή κατακερματισμού, μήκους 32-byte.



Σχήμα 5.4: Ένα δέντρο Merkle που συνοψίζει πολλές συναλλαγές.

Για να αποδειχθεί ότι μία συγκεκριμένη συναλλαγή έχει συμπεριληφθεί σε ένα block, ένας κόμβος χρειάζεται να παράξει $log_2(N)$ το πλήθος τιμές κατακερματισμού μήκους 32-byte, συνιστώντας έτσι μια διαδρομή επαλήθευσης (merkle path) που συνδέει την συγκεκριμένη συναλλαγή με την ρίζα Merkle του δέντρου. Καθώς ο αριθμός των συναλλαγών αυξάνει, ο λογάριθμος με βάση το 2 του αριθμού των συναλλαγών αυξάνει με μικρότερο ρυθμό. Αυτό επιτρέπει στους κόμβους του bitcoin να παράγουν πολύ εύκολα διαδρομές των 10 ή 12 hashes, οι οποίες μπορούν να αποδείξουν την ύπαρξη μίας συναλλαγής στο block μέσα από χίλιες ή περισσότερες συναλλαγές του block.



Σχήμα 5.5: Η διαδρομή merkle που χρησιμοποιείται για την απόδειξη της περίληψης μίας συναλλαγής στο block.

Στο σχήμα 5.5, ένας κόμβος του δικτύου μπορεί να αποδείξει ότι η συναλλαγή (H_C) συμπεριλαμβάνεται στο block αυτό, παράγοντας ένα merkle path που έχει μήκος τέσσερεις

τιμές κατακερματισμού των 32-byte (σύνολο 128 byte). Η διαδρομή αυτή αποτελείται από τις ακόλουθες τέσσερεις τιμές κατακερματισμού: H_D, H_{AB}, H_{EFGH} και $H_{IJKLMNOP}$ (τα κουτάκια με το βαρύ γκρι χρώμα). Η επιβεβαίωση ότι η συναλλαγή $Tx\,1$ περιλαμβάνεται στο block χρειάζεται μόνο τον υπολογισμό των τιμών hash των H_C, H_{CD}, H_{ABCD} και $H_{ABCDEFGH}$ και όχι τον υπολογισμό όλων των hash τιμών των φύλλων του δέντρου. Η σημασία της αποδοτικότητας των δέντρων Merkle, φαίνεται όσο μεγαλώνει ο αριθμός των δεδομένων, εν προκειμένω, των συναλλαγών. Ο πίνακας 5.7.1 δείχνει τον όγκο των δεδομένων που χρειάζεται να συνδυαστούν για να αποδειχθεί ότι μία συναλλαγή είναι μέρος του block.

Πίνακας 5.7.1: Αποτελεσματικότητα των δέντρων Merkle.

Πλήθος Συναλλαγών	**Μέγεθος του block**	**Μέγεθος διαδρομής σε hashes**	**Μέγεθος διαδρομής σε bytes**
16 συναλλαγές	4 kilobytes	4 hashes	128 bytes
512 συναλλαγές	128 kilobytes	9 hashes	288 bytes
2048 συναλλαγές	512 kilobytes	11 hashes	352 bytes
65, 535 συναλλαγές	16 megabytes	16 hashes	512 bytes

Κεφάλαιο 6

Mining (Εξόρυξη)

6.1 Εισαγωγή

Η εξόρυξη (mining) είναι η δημιουργία (κοπή) νέων bitcoins. Παρότι θυμίζει την εξόρυξη πολύτιμων μετάλλων, στην πραγματικότητα είναι μία ανταμοιβή για τους εξορύκτες (miners) που επικυρώνουν τις συναλλαγές στο δίκτυο του bitcoin. Η λέξη εξόρυξη (mining) και εξορύκτης (miner) θυμίζει την εξόρυξη πολύτιμων μετάλλων. Ο σκοπός της εξόρυξης είναι να εξασφαλιστεί η ασφάλεια του δικτύου και να ενεργοποιηθεί η συναίνεση (consensus) μεταξύ των κόμβων του δικτύου ως προς την αυθεντικότητα της blockchain, χωρίς να χρειάζεται η επικύρωση της αλυσίδας και των συναλλαγών από μία κεντρική αρχή. Με την εξόρυξη επιτυγχάνεται η αποκέντρωση της ασφάλειας του δικτύου bitcoin.

Οι εξορύκτες επικυρώνουν νέες συναλλαγές και τις καταγράφουν στο δημόσιο λογιστικό βιβλίο (blockchain). Περίπου κάθε 10 λεπτά δημιουργείται ένα καινούργιο block που περιέχει συναλλαγές που συνέβησαν μετά το τελευταίο block. Έτσι οι καινούργιες συναλλαγές που προστίθενται στην αλυσίδα θεωρούνται πλέον ”επιβεβαιωμένες” και μπορούν να χρησιμοποιηθούν με ασφάλεια χωρίς κανείς να αμφιβάλλει για την εγκυρότητά τους. Για την παροχή της υπηρεσίας της ασφάλισης της αλυσίδας, οι εξορύκτες λαμβάνουν δύο τύπους ανταμοιβής. Καινούργιας κοπής νομίσματα (bitcoins) και αμοιβές συναλλαγών πάλι σε bitcoin. Για να λάβουν αυτές τις ανταμοιβές, οι εξορύκτες συναγωνίζονται μεταξύ τους για το ποιός θα καταφέρει πρώτος να λύσει ένα δύσκολο μαθηματικό πρόβλημα βασισμένο σε κρυπτογραφικές συναρτήσεις κατακερματισμού και συγκεκριμένα στην double hash SHA-256. Η λύση σε αυτό το πρόβλημα λέγεται ”απόδειξη εργασίας” (Proof of Work), συμπεριλαμβάνεται στο καινούργιο block και είναι η απόδειξη ότι οι εξορύκτες δαπάνησαν σημαντικό ποσό υπολογιστικών πόρων.

6.2 Αποκεντρωμένη Συναίνεση (Decentralized Consensus)

Συναίνεση (Consensus) είναι η διαδικασία συμφωνίας μεταξύ δύσπιστων (distrusting) συμβαλλόμενων κόμβων, όσον αφορά την τελική μορφή των δεδομένων. Συναίνεση μεταξύ δύο κόμβων (π.χ. client-server) επιτυγχάνεται εύκολα, όταν όμως συμμετέχουν πολλαπλοί κόμβοι είναι πολύ δύσκολο να επιτευχθεί. Η έννοια της επίτευξης συναίνεσης μεταξύ πολλαπλών κόμβων είναι γνωστή ως **κατανεμημένη συναίνεση (distributed consensus)**.

Η Κατανεμημένη Συναίνεση **Distributed Consensus** το θεμέλιο της blockchain. Επιτρέπει στην αλυσίδα να παράσχει μια ενιαία εκδοχή της αλήθειας η οποία συμφωνείται από όλα τα μέρη χωρίς την απαίτηση ύπαρξης μίας κεντρικής αρχής(central authority).

Η αποκεντρωμένη συναίνεση (consensus) του δικτύου αναδύεται από την ασύγχρονη αλληλεπίδραση χιλιάδων ανεξάρτητων κόμβων του δικτύου, που ακολουθούν απλούς γενικούς κανόνες:

- Ανεξάρτητη επικύρωση κάθε συναλλαγής, από κάθε πλήρη κόμβο (full node), η οποία βασίζεται σε συγκεριμένα κριτήρια.
- Ανεξάρτητη ενσωμάτωση των νέων πιθανών συναλλαγών σε καινούργια block, από κόμβους εξόρυξης, σε συνδυασμό με την επίδειξη της υπολογιστικής προσπάθειας μέσω του αλγόριθμου ”απόδειξης εργασίας”.
- Ανεξάρτητη επιβεβαίωση των καινούργιων block της αλυσίδας από κάθε κόμβο και συναρμολόγησή τους στην αλυσίδα.
- Ανεξάρτητη επιλογή (voting) από κάθε κόμβο, της αλυσίδας με την αποδεδειγμένη μέσω αλγόριθμου απόδειξης εργασίας μεγαλύτερης υπολογιστικής προσπάθειας.

6.3 Ανεξάρτητη Επικύρωση των Συναλλαγών

Το λογισμικό των πορτοφολιών δημιουργεί συναλλαγές με το να συλλέγει UTXO’s παρέχοντας τις απαραίτητες δέσμες ενεργειών ξεκλειδώματος (unlocking scripts), και να κατασκευάζει νέες εκροές που να τις εκχωρεί σε νέους ιδιοκτήτες. Η προκύπτουσα συναλλαγή αποστέλλεται στη συνέχεια στους γειτονικούς κόμβους του δικτύου του Bitcoin και στη συνέχεια εξαπλώνεται σε όλο το δίκτυο. Πριν όμως την διάδοση στους γειτονικούς κόμβους, κάθε κόμβος που λαμβάνει μία συναλλαγή, πρώτα θα την επικυρώσει και μόνο τότε θα την διαδώσει στο δίκτυο. Οι μη έγκυρες συναλλαγές απορρίπτονται από τον πρώτο κόμβο που θα τις συναντήσει.

6.4 Απόδειξη Εργασίας (Proof of Work - PoW)

Η απόδειξη εργασίας είναι η λύση του επόμενου μαθηματικό προβλήματος.

Ορισμός 6.4.1. ***Proof of Work*** *Εστω δεδομένα (data)* X*. Να βρεθεί αριθμός* n *τέτοιος ώστε η σύνοψη (hash) της ακόλουθης εισόδου* $(X||n||)$ *να είναι μικρότερη κάποιου δοσμένου αριθμού* Y*.*

Η απόδειξη εργασίας, χρησιμοποιείται για να εξασφαλιστεί ότι κάποιος έχει δαπανήσει ένα συγκεκριμένο ποσό υπολογιστικής εργασίας για να βρεί μία λύση, η οποία μπορεί να επαληθευτεί εύκολα από οποιονδήποτε.

6.4.1 Περιγραφή της απόδειξης εργασίας

Ας υποθέσουμε ένα πείραμα τύχης ως εξής: Ρίχνουμε δύο αμερόληπτα ζάρια και θέλουμε το άθροισμα των δύο ρίψεων να είναι μικρότερο από τον αριθμό-στόχο 12. Η μόνη περίπτωση να χάσουμε είναι να έρθει αποτέλεσμα $6 + 6$ το οποίο έχει πιθανότητα $1/36$. Στον επόμενο γύρο κατεβάζουμε τον στόχο στο 11. Η πιθανότητα τώρα να χάσουμε ανεβαίνει στο $3/36$. Συνεχίζουμε να ελαττώνουμε τον αριθμό στόχο. Έστω ότι σε κάποιο γύρο ο στόχος είναι ο 5. Η πιθανότητα να χάσουμε ανεβαίνει στο $31/36$. Βλέπουμε λοιπόν ότι όσο κατεβαίνει ο αριθμός στόχος, τόσο μειώνονται οι πιθανότητες νίκης μας στο παιχνίδι αυτό. Όταν ο αριθμός στόχος γίνει 3 τότε οι πιθανότητες νίκης είναι $1/36$.

Στα δεδομένα που ακολουθούν κάθε πρόταση παράγει μία διαφορετική τιμή hash με την χρήση της συνάρτησης SHA-256. Στο τέλος κάθε φράσης `my text_` συμπληρώνεται ενας αριθμός που λειτουργεί σαν αυθαίρετη μεταβλητή. Τον ονομάζουμε ”nonce” και γενικά η λειτουργία του είναι να αλλάζει την έξοδο μίας κρυπτογραφικής συνάρτησης. Εδω θέτουμε σαν στόχο, να βρεθεί μία φράση που η δεκαεξαδική τιμή κατακερματισμού της, να ξεκινάει με μηδέν.

```
my text0 => fc196ad25c24d1bc16a8b7960a56b232edcea0cd731a8a9d6199ac71.....
my text1 => bbae4e8daa04d179a1f1e49e6ba351eca1138a758870e32751da9508.....
my text2 => 33a0bb477555ebbce74711b9f22bbac59e5a7fb94b067c90953a9c9c.....
my text3 => a9d133db1cf0ae89cba848b0764332ace93a9cbb77f4457fa83ce0c4.....
my text4 => 32ed3183ebc55ca980ea10cb215c15beef7e4e2bc21af60326b6c9c9.....
my text5 => e9fd00cb6a7a113d0dae85fe8f187f156495d95140d7655d7e2ffe9c.....
my text6 => 3a4f2b6f937ee2b82a32928c7920aa471ceb7d8efeee91ff5c0c1597.....
my text7 => dbe79797bfe36bf98e003643aee0e7d3f76b99dbfb8e923732e1f092.....
my text8 => 5ffab77f595f10fa775658ad76619adfefa3fd3540f2ba6ca395d4e5.....
```

```
my text9  => 19904beb3d4f2a7cf6b425a9a7b5ea65f9f6e21ca1af8af313c1545c……
my text10 => 058de040bd790caaae51bcc1591d0c18a230775597e4cddd07eba1d9……
my text11 => 00f7e2326435f6ae03f1daad9abe7ea194e1cc5608baf41b9d4f877d……
my text13 => ed1719b7cc752fbe8bf16127e2e26c1ffeba37b1957f47c954c7b464……
my text14 => 248c991ffe2f506817fbadb9088a98c8ad7b9bbf8e44811f1247c4bd……
my text15 => 99f749a081cb2b9be19deaca67fad20e8aec9dd3b9e1e62b9acd26c0……
my text16 => d4aa47b98f13ca41861a23857af650b9f338e150e1dbfa5457bb586a……
```

Βλέπουμε ότι χρειάστηκαν μόνο 11 προσπάθειες, ώστε από την φράση `my text10` να προκύψει η hash `058de040bd790caaae51bcc1591d0c18a230775597e4cddd07eba1d937bcccef`.

Αν θεωρήσουμε ότι το αποτέλεσμα της συνάρτησης είναι ομοιόμορφα κατανεμημένο, τότε αναμένουμε να βρούμε ένα αποτέλεσμα με τον αριθμό 0 στην πρώτη θέση μία φορά για κάθε 16 προσπάθειες, δηλαδή μία τιμή hash μικρότερη του αριθμού `0x1000000000000000000000000000000000000000000000000000000000000000` οποιαδήποτε και αν είναι η φράση που θα κατακερματίσουμε. Αυτόν τον αριθμό τον λέμε στόχο (target) και ο σκοπός μας είναι να βρούμε κάποια τιμή hash μικρότερη από αυτόν. Για να βρουμε 00 στις δύο πρώτες θέσεις (δηλαδή να μικρύνουμε τον αριθμό στόχο περισσότερο) η πιθανότητα μικραίνει στο$1/2^8$ και συνεχίζει να μικραίνει όσο ζητάμε περισσότερα συνεχόμενα μηδέν να καλύπτουν τις θέσεις ξεκινώντας από αριστερά προς τα δεξιά, μειώνοντας παράλληλα τον αριθμό στόχο. Όσο μικραίνει ο στόχος βλέπουμε οτι η διαδικασία εύρεσης τιμής hash μικρότερης από τον αριθμό στόχο γίνεται ολενά και δυσκολότερη.

Η απόδειξη εργασίας που χρησιμοποιεί το bitcoin μοιάζει πολύ με το προηγούμενο παράδειγμα. Ένας εξορύκτης γεμίζει ένα υποψήφιο block με συναλλαγές. Κατόπιν υπολογίζει την hash τιμή της επικεφαλίδας του block και την συγκρίνει με την τιμή στόχο. Αν η hash τιμή δεν είναι μικρότερη από την τιμή στόχο τότε τροποποιεί την τιμή nonce (η nonce αυξάνεται κατά 1) και υπολογίζει ξανά την τιμή της επικεφαλίδας του block. Η διαδικασία συνεχίζεται μέχρι η τιμή hash να γίνει μικρότερη ή ίση με την τιμή στόχο. Ο αλγόριθμος που χρησιμοποιείται για τον κατακερματισμό της επικεφαλίδας του block είναι ο double SHA-256 και τον αριθμό στόχο τον συμβολίζουμε με T. Έστω η τιμή κατακερματισμού $H = SHA256(SHA256(bh||n))$ όπου $bh||n$ είναι η επικεφαλίδα του block bh και n ο αριθμός nonce. Η πιθανότητα εύρεσης ενός αριθμού nonce είναι:

$$P[H \leq T] = \frac{T}{2^{256}} \tag{6.1}$$

Ο αναμενόμενος αριθμός δοκιμών που πρέπει να εκτελέσει ένας εξορύκτης για να βρεί μία

απόδειξη εργασίας είναι κατά μέσο όρο

$$T[H \leq T] = \frac{1}{P[H \leq T]} = \frac{2^{256}}{T} \tag{6.2}$$

Η επιβεβαίωση από κάποιον τρίτο, του κατά πόσο ο αριθμός nonce που τη συνοδεύει είναι πράγματι μία έγκυρη απόδειξη εργασίας, γίνεται πολύ εύκολα, υπολογίζοντας απλά εάν ισχύει ότι

$$SHA256(SHA256(bh||n)) \leq T. \tag{6.3}$$

6.4.2 Επαναπροσδιορισμός της Στόχου

Ένα bitcoin block παράγεται κατά μέσο όρο περίπου κάθε 10 λεπτά. Για να παραμείνει ο χρόνος γέννεσης του block σε αυτό το μέσο όρο, πρέπει να αναπροσαρμόζεται η δυσκολία της εξόρυξης, κατά συνέπεια πρέπει να αναπροσαρμόζεται ο αριθμός στόχος. Η αναπροσαρμογή αυτή γίνεται αυτόματα και ανεξάρτητα σε κάθε κόμβο. Κάθε $2,016$ blocks όλοι ο κόμβοι αναπροσαρμόζουν τον στόχο με βάση την ακόλουθη εξίσωση.

New Target = Old Target * (Actual Time of Last 2,016 Blocks / 20160 minutes))

Εάν το δίκτυο βρίσκει τα blocks γρηγορότερα από 10 λεπτά, τότε η δυσκολία εξόρυξης αυξάνεται (ο αριθμός στόχος μειώνεται) ενώ αντίθετα αν ο χρόνος δημιουργίας των block είναι μεγαλύτερος από 10 λεπτά η δυσκολία εξόρυξης μειώνεται (ο αριθμός στόχος αυξάνεται).

6.4.3 Εξόρυξη και επικύρωση του νέου block

Μόλις ο εξορύκτης βρεί την τιμή hash που είναι μικρότερη από τον αριθμό στόχο, αμέσως το νέο block μεταδίδεται σε όλους τους κόμβους.

Οι κόμβοι λαμβάνουν, επικυρώνουν και διαδίδουν το νέο block στο δίκτυο προσθέτοντάς το ο καθένας στο δίκό του αντίγραφο της αλυσίδας. Όταν οι κόμβοι εξόρυξης λάβουν και επικυρώσουν (ακολουθώντας ένα συγκεκριμένο πρωτόκολλο) το νέο block, σταματούν τις προσπάθειες εξόρυξής του και ξεκινάνε την διαδικασία για την εξόρυξη ενός καινούργιου block χρησιμοποιώντας το προσφάτως δημιουργηθέν block σαν γονέα (parent). Ξεκίνωντας την διαδικασία πάλι από την αρχή, οι εξορύκτες ψηφίζουνε με την υπολογιστική τους ισχύ την εγκυρότητα του νέου block και ταυτόχρονα εγκρίνουν την αλυσίδα που επεκτείνεται από αυτό. Κάθε κόμβος επικυρώνει ξεχωριστά την αλυσίδα βάσει συγκεκριμένων κριτηρίων, όπως:

- Η δομή των δεδομένων του block είναι συντακτικά έγκυρη.
- Η τιμή hash της επικεφαλίδας του block είναι μικρότερη από τον αριθμό στόχο.
- Το μέγεθος του block είναι μέσα σε κάποια επιτρεπτά όρια.
- Η πρώτη συναλλαγή του block και μόνο αυτή είναι μία coinbase συναλλαγή.
- Όλες οι συναλλαγές του block έχουν επικυρωθεί σύμφωνα με συγκεκριμένα κριτήρια που διέπουν τις συναλλαγές.

Η ανεξάρτητη επικύρωση κάθε νέου block από κάθε κόμβο του δικτύου εξασφαλίζει ότι κανένας εξορύκτης δεν μπορεί να εξαπατήσει το δίκτυο δημιουργώντας πλαστό block.

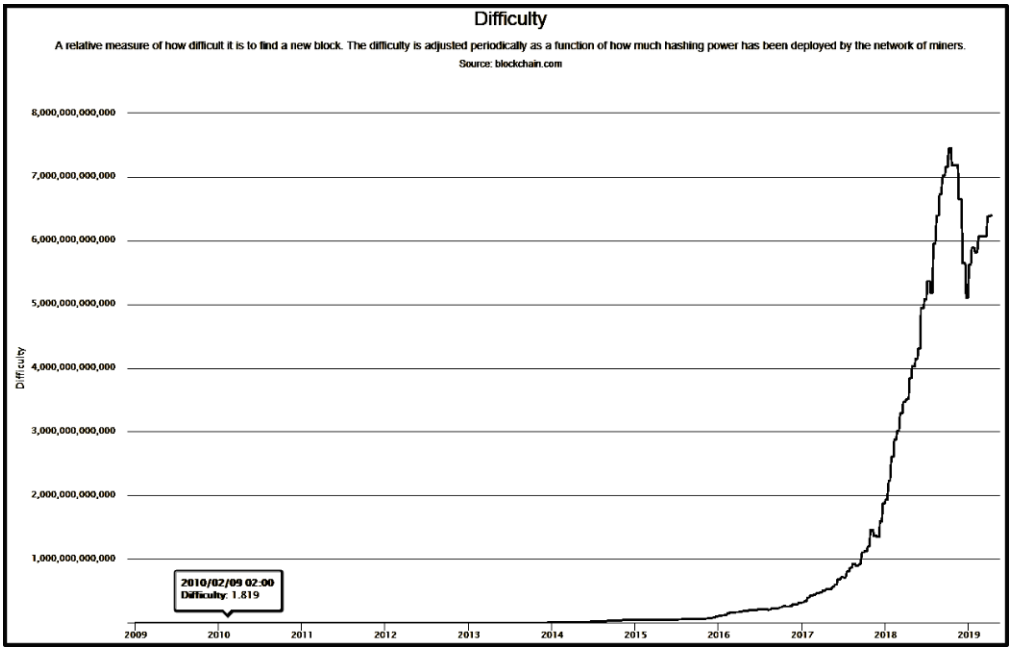
6.4.4 Συναρμογή και επιλογή της πιό έγκυρης αλυσίδας

Όταν ένας κόμβος επικυρώσει το νέο block, θα προσπαθήσει ακολούθως να δημιουργήσει μία αλυσίδα που θα περιέχει αυτό το block, προσθέτωντάς το στην ήδη υπάρχουσα αλυσίδα. Οι κόμβοι διατηρούν τρία σύνολα από block: αυτά που συνδέονται στην κύρια αλυσίδα, αυτά που δημιουργούν κλάδους εκτός της κύριας αλυσίδας (δευτερεύουσες αλυσίδες) και block που δεν έχουν γνωστό στο δίκτυο γονέα στις γνωστές αλυσίδες (ορφανά block). Blocks που δεν πέρασαν με επιτυχία κάποια από τα κριτήρια επικύρωσης, θεωρούνται άκυρα και δεν συμπεριλαμβάνονται σε καμμία αλυσίδα. Σαν Κύρια Αλυσίδα (main chain) οποιαδήποτε χρονική στιγμή, θεωρείται η αλυσίδα που σχετίζεται με την περισσότερη συσσωρευμένη απόδειξη εργασίας. Συνήθως είναι η αλυσίδα που έχει τα περισσότερα blocks, εκτός και εάν υπάρχουν δύο ίσου μεγέθους αλυσίδες και κάποια εξ αυτών έχει περισσότερη συσσωρευμένη απόδειξη εργασίας. Όταν ένα νέο block εμφανιστεί, ένας κόμβος θα προσπαθήσει να το εντάξει στην υπάρχουσα αλυσίδα. Ο κόμβος θα δει το πεδίο ”previous block hash” (είναι η αναφορά στο γονικό block) του υπό ένταξη block και θα προσπαθήσει να βρεί αυτόν το γονικό block στο δικό του αντίγραφο της αλυσίδας. Συνήθως ο γονέας θα είναι στο πάνω μέρος της αλυσίδας, οπότε το νέο block θα επεκτείνει αυτή την αλυσίδα. Επιλέγοντας την αλυσίδα με την περισσότερη συσσωρευμένη εργασία, τελικά όλοι οι κόμβοι επιτυγχάνουν την συναίνεση στο δίκτυο. Οι κόμβοι εξόρυξης ψηφίζουν με την υπολογιστική (εξορυκτική) ισχύ τους, επιλέγοντας ποιά αλυσίδα θα επεκτείνουν με το να εξορύξουν το επόμενο block που συνδέεται με την αλυσίδα αυτή. Στην ουσία το νέο block είναι η ψήφος τους.

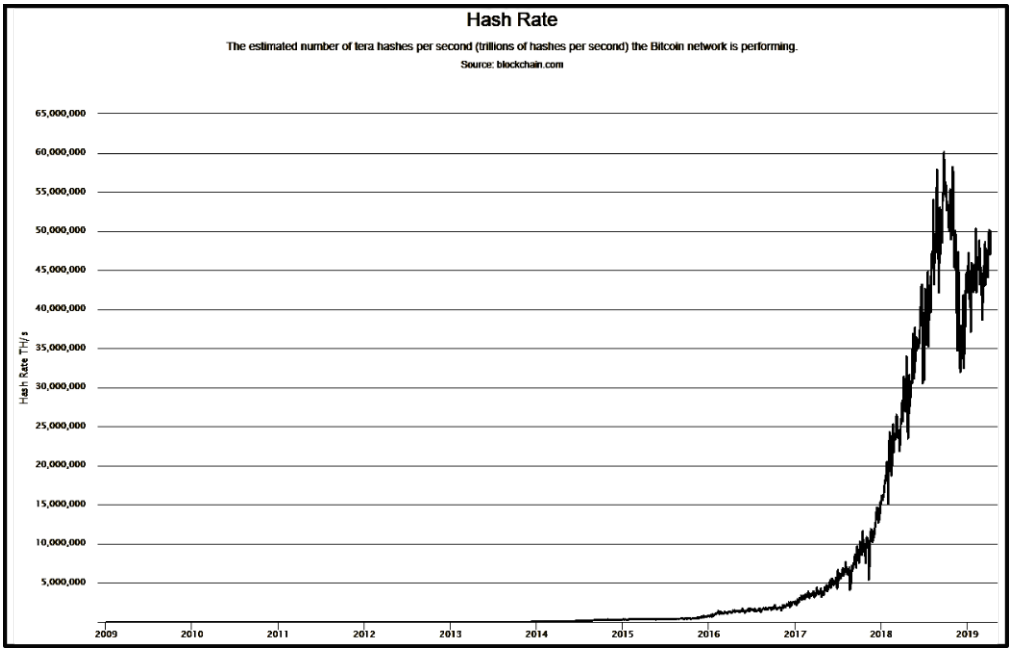
6.4.5 Εξόρυξη και Ρυθμός Κατακερματισμού

Η εξόρυξη Bitcoin είναι μία πολύ ανταγωνιστική βιομηχανία. Στα πρώτα χρόνια οι εξορύκτες χρησιμοποιούσαν την δύναμη των επεξεργαστών τους (CPU: central processing

unit) για τον υπολογισμό του στόχου, μέσω του αλγόριθμου SHA256. Αργότερα οι εξορύκτες άρχισαν να χρησιμοποιούν κάρτες γραφικών (GPU: graphics processing unit) που είχαν πολύ μεγαλύτερη υπολογιστική ισχύ καθώς και FPGA's (field programmable gate array). Το τεράστιο άλμα στην υπολογιστική ισχύ έγινε το 2013 με την εισαγωγή στην εξόρυξη των ASIC's (Application-Specific Integrated Circuit) στα οποία τυπώνεται απευθείας στα ολοκληρωμένα κυκλώματα η συνάρτηση SHA256 επιτυγχάνοντας έτσι τεράστια υπολογιστική ισχύ με πολύ μικρότερη κατανάλωση ενέργειας από τις προηγούμενες μεθόδους. Στα σχήματα (6.1) και (6.2) αποτυπώνεται η εξέλιξη της δυσκολίας (difficulty) καθώς και του ρυθμού κατακερματισμού (hashing rate) , από την γένεση του bitcoin έως σήμερα.



Σχήμα 6.1: Δυσκολία εξόρυξης Bitcoin από το 2009 έως σήμερα.



Σχήμα 6.2: Ρυθμός κατακερματισμού από το 2009 έως σήμερα.

Κεφάλαιο 7

Έξυπνα Συμβόλαια

Τα έξυπνα συμβόλαια (smart contracts) επινοήθηκαν από τον Nick Szabo [38] το 1997 και περιγράφονται ως υπολογιστικά προγράμματα που αντιπροσωπεύουν ένα πρωτόκολλο συναλλαγών το οποίο εκτελείται αυτόματα όταν πληρούνται οι συγκεκριμένοι όροι μίας σύμβασης.

Οι γενικοί στόχοι είναι να ικανοποιηθούν οι κοινοί συμβατικοί όροι όπως, οι όροι πληρωμής, τα εμπράγματα βάρη, η εμπιστευτικότητα ακόμη και η επιβολή των όρων αυτών, ελαχιστοποιώντας κακόβουλες ή τυχαίες εξαιρέσεις καθώς και την ανάγκη για αξιόπιστους διαμεσολαβητές. Οι οικονομικοί στόχοι της χρήσης των έξυπνων συμβολαίων περιλαμβάνουν τη μείωση οικονομικών απωλειών λόγω απάτης, μείωση του κόστους των διαιτητικών αποφάσεων και των δαπανών εκτέλεσης καθώς και άλλα κόστη συναλλαγών.

Χρειάστηκε να περάσουν 20 χρόνια για να φανούν οι δυνατότητες και τα οφέλη τους και αυτό οφείλεται στην εφαρμογή τους πάνω στην blockchain. Η εκτέλεση του κώδικα του έξυπνου συμβολαίου πάνω στην blockchain καθιστά αδύνατη την οποιαδήποτε παραποίησή του. Λόγω της ταυτόχρονης εκτέλεσης του έξυπνου συμβολαίου σε όλους τους κατανεμημένους κόμβους της αλυσίδας, όπως επίσης της χρήσης της συναίνεσης από τους κόμβους για την εκπλήρωση του συμβολαίου, μία λανθασμένη εκτέλεση από κάποιο κόμβο που έχει δεχθεί κυβερνοεπίθεση καθίσταται αδύνατη.

7.1 Πλεονεκτήματα των έξυπνων συμβολαίων

- **Πλήρης διαφάνεια**

  Τα έξυπνα συμβόλαια είναι απόλυτα διαφανή για όλα τα συμβαλλόμενα μέρη. Κάθε συμβαλλόμενο μέρος έχει πρόσβαση στους όρους και τις προϋποθέσεις του έξυπνου συμβολαίου, όπως και στα παραδοσιακά συμβόλαια.

- **Έλλειψη παρανοήσεων**

  Τα έξυπνα συμβόλαια εκτελούνται αυτόματα και περιέχουν με λεπτομέρεια όλες τις αναγκαίες πληροφορίες. Η οποιαδήποτε παρανόηση έχει μηδενική πιθανότητα να συμβεί.

- **Αποτελεσματική απόδοση**

  Ο συνδυασμός της ακρίβειας, της ταχύτητας και της αυτοματοποιημένης λειτουργίας ολοκληρώνει αποτελεσματικά ολόκληρη τη διαδικασία του συμβολαίου, χωρίς σφάλματα και μεσάζοντες ανεξάρτητα από τον όγκο των συναλλαγών.

- **Αντίγραφα ασφαλείας**

  Τα έξυπνα συμβόλαια έχουν πάντα αντίγραφα ασφαλείας, καταγεγραμμένα στην blockchain. Τα συμβόλαια καταγράφουν μόνιμα όλα τα βασικά έγγραφα με λεπτομέρειες. Η ανάκτηση οποιασδήποτε πληροφορίας είναι εύκολο να πραγματοποιηθεί σε περίπτωση απώλειας δεδομένων.

- **Εγγυημένα αποτελέσματα**

  Οι έξυπνες συμβάσεις επιτρέπουν στα συμβαλλόμενα μέρη να δημιουργούν οποιεσδήποτε συμφωνίες ακολουθώντας όμως συγκεκριμένους κανόνες παρόμοια με ένα παραδοσιακό συμβόλαιο. Κατά την εκτέλεσή τους το αποτέλεσμα δεν μπορεί να αμφισβητηθεί εκτός από ειδικές περιπτώσεις.

7.2 Μειονεκτήματα των έξυπνων συμβολαίων

- **Εμπιστευτικότητα**

  Ενώ η διαφάνεια είναι ένα από τα πλεονεκτήματα των έξυπνων συμβολαίων, μπορεί να οδηγήσει σε άρση της εμπιστευτικότητας. Για το λόγο αυτό, κάποιες blockchain που προσφέρουν έξυπνα συμβόλαια, παρέχουν στους χρήστες του ιδιωτικά έξυπνα συμβόλαια με πλήρη κάλυψη του απορρήτου.

- **Λάθη προγραμματισμού**

  Τα έξυπνα συμβόλαια είναι στην ουσία προγράμματα υπολογιστών. Ελοχεύει ο κίνδυνος ακούσιων ή εκούσιων σφαλμάτων στον κώδικα από τους προγραμματιστές. Ετσι εμφανίζεται η πιθανότητα ο κώδικας να έχει κάποια παραθυράκια ανοιχτά δημιουργώντας ζητήματα αξιοπιστίας.

- **Μη αξιόπιστες πληροφορίες**

Η πιθανότητα αποθήκευσης λανθασμένων ή ελλιπών ή και ψευδών πληροφοριών δεν μπορεί να αποφευχθεί. Χρειάζεται μεγάλη προσοχή στην σύνταξη αυτών των συμβολαίων. Χωρίς μία μορφή διαιτησίας και μεσεγγυούχου πάνω στην blockchain, η ταχύτατη εκτέλεσή τους δεν παρέχει δυνατότητα άρνησης του αποτελέσματος.

7.3 Παραδείγματα έξυπνων συμβολαίων

- **Υπηρεσίες υγείες**

  Ασθενής φορά ειδικό βραχιολάκι που μετράει τους χτύπους της καρδιάς και της πίεσής του. Οι μετρήσεις αυτές μεταφέρονται και καταγράφονται στην blockchain σε τακτά χρονικά διαστήματα. Όταν κάποιος ή κάποιοι από τους δείκτες ελέγχου υπερβούν συγκεκριμένα όρια, εκτελείται ένα έξυπνο συμβόλαιο που στέλνει ένα προειδοποιητικό μήνυμα στο τηλέφωνο του ασθενούς καθώς και στον θεράποντα ιατρό του, εξασφαλίζοντας έτσι κρίσιμο χρόνο για λήψη κάποιου φαρμάκου, αποσοβώντας έτσι μία πιθανή καρδιακή προσβολή ή/και επισπεύδοντας την επίσκεψη στον ιατρό. Παρόλο που τέτοια συμβαρικά συστήματα υπάρχουν ήδη, η ειδοποιός διαφορά είναι ότι οι μετρήσεις καταχωρούνται στην blockchain, εκμηδενίζοντας έτσι τις πιθανότητες κακόβουλης ή τυχαίας παραποίησής των μετρήσεων με αποτέλεσμα την απειλή της ζωής του ασθενούς.

  Η blockchain μπορεί επίσης να χρησιμοποιηθεί για την ασφαλή αποθήκευση των αποτελεσμάτων κλινικών εξετάσεων, καθώς εγγυάται την ιδιωτικότητα και το απόρρητο των ασθενών. Αν χρειαστεί να μελετηθούν τα αποτελέσματα από τον/τους θεράποντες ιατρούς μπορεί να δημιουργηθεί ένα έξυπνο συμβόλαιο με το οποίο ο ασθενής θα δίνει την συγκατάθεσή του αν εκπληρούνται συγκεκριμένοι όροι.

- **Εφοδιαστική αλυσίδα**

  Με την χρήση των έξυπνων συμβολαίων και με τη σύνδεσή τους με συσκευές IOT (π.χ αισθητήρες θερμοκρασίες, GPS για καταγραφή θέσης και ημερομηνίας) η ιχνηλασιμότητα των προϊόντων γίνεται πλέον αυτόματα και με διαφάνεια. Λόγω της καταγραφής όλων των σταδίων της εφοδιαστικής αλυσίδας στην blockchain, όπως τοποθεσίες, χρόνοι παραμονής σε κάθε μία από αυτές, όροι και συνθήκες αποθήκευσης και μεταφοράς σε όλα τα στάδια, οι περιπτώσεις μη τήρησης κάποιων από τους συμφωνημένους όρους του συμβολαίου μεταφοράς, όπως η διατήρηση της θερμοκρασίας σε συγκεκριμένα επίπεδα, σηματοδοτεί την έναρξη ενός έξυπνου συμβολαίου το οποίο καταγράφη την αλλαγή στην blockchain, επιτρέποντας έτσι στον τελικό παραλήπτη

να ασκήσει τις ποινικές ρήτρες του συμφωνημένου συμβολαίου. Οι καταγραφές στην blockchain αποτρέπουν οποιαδήποτε αλλοίωση από εξωτερικούς παράγοντες των εγγεγραμένων δεδομένων.

Κεφάλαιο 8

Άλλα Κρυπτονομίσματα

Τα κρυπτονομίσματα που διαμορφώθηκαν με πρότυπο το bitcoin λέγονται **altcoins** και παρουσιάζονται ως τροποποιημένες ή βελτιωμένες εκδόσεις του bitcoin. Ενώ ορισμένα από αυτά τα νομίσματα είναι ευκολότερο να εξορυχθούν από ότι το bitcoin, υπάρχουν διάφοροι συμβιβασμοί, όπως μεγαλύτερος κίνδυνος λόγω μικρότερης ρευστότητας, αποδοχής και διατήρησης αξίας. Αυτή τη στιγμή κυκλοφορούν πάνω από 1600 κρυπτονομίσματα και ο αριθμός τους μεγαλώνει συνεχώς. Τα σημαντικότερα είναι τα ακόλουθα:

1. **Litecoin (LTC)** Το Litecoin [39, 40], που ξεκίνησε το 2011, ήταν από τα πρώτα κρυπτονομίσματα που ακολούθησαν μετά το bitcoin και χαρακτηρίστηκε σαν το ”ασήμι αντί του χρυσού του bitcoin”. Μοιάζει πολύ στην αρχιτεκτονική με το bitcoin και χρησιμοποιεί σαν ”απόδειξη εργασίας” τον αλγόριθμο **scrypt** ο οποίος χρειάζεται μεγάλες ποσότητες RAM μειώνοντας έτσι την ανάγκη για εξειδικευμένα μηχανήματα εξόρυξης όπως τα ASIC’s. Η ενέργεια που καταναλώνεται για την διατήρηση του δικτύου είναι πολύ μικρότερη και η επικύρωση των συναλλαγών γίνεται γρηγορότερα από το bitcoin.
2. **Ethereum (ETH)** Το Ethereum [41, 42] είναι μια αποκεντρωμένη πλατφόρμα λογισμικού που επιτρέπει την κατασκευή και λειτουργία έξυπνων συμβάσεων (Smart Contracts) και κατανεμημένων εφαρμογών (Distributed Applications-DApps) χωρίς διακοπή, απάτη, έλεγχο ή παρεμβολές από τρίτους. Οι εφαρμογές στο Ethereum εκτελούνται με το δικό της νόμισμα που λέγεται Ether. Το Ether είναι σαν ένα όχημα μετακίνησης στη πλατφόρμα ethereum και επιδιώκεται κυρίως από προγραμματιστές που επιθυμούν να αναπτύξουν και να τρέξουν εφαρμογές στο εσωτερικό του ethereum ή τώρα από επενδυτές που επιθυμούν να κάνουν αγορές άλλων ψηφιακών νομισμάτων χρησιμοποιώντας ether. Κατά τη διάρκεια του 2014, η Ethereum ξεκίνησε μια εκ των προτέρων πώληση για το Ether, η οποία είχε μία συντριπτική ανταπόκριση. Έτσι ξε-

κίνησε η εποχή της αρχικής προσφοράς νομισμάτων (initial coin offering-ICO) [43]. Η Ethereum ισχυρίζεται ότι το Ether μπορεί να χρησιμοποιηθεί για να κωδικοποιήσει , αποκεντρώσει, ασφαλίσει και εμπορευτεί σχεδόν οτιδήποτε. Μετά την επίθεση κατά του DAO το 2016 [44, 45], το Ethereum χωρίστηκε σε Ethereum (ETH) και Ethereum Classic (ETC).

3. **Zcash (ZEC)** Το Zcash [46, 47] ξεκίνησε στο τέλος του 2016 και μία αναλογία του με το bitcoin είναι ότι "αν το bitcoin είναι το http για το χρήμα, τότε το Zcash είναι το https". Το Zcash προσφέρει ιδιωτικότητα και επιλεκτική διαφάνεια των συναλλαγών. Με αυτό τον τρόπο, όπως και με το https, το Zcash ισχυρίζεται ότι προσφέρει επιπλέον ασφάλεια και ιδιωτικότητα, όπου όλες οι συναλλαγές εγγράφονται και δημοσιεύονται στην αλυσίδα αλλά πληροφορίες όπως απόστολές, παραλήπτης και ποσά συναλλαγής παραμένουν ιδιωτικά. Το Zcash προσφέρει στους χρήστες του την επιλογή "θωρακισμένων" συναλλαγών, που επιτρέπουν κρυπτογραφημένο περιεχόμενο χρησιμοποιώντας μία τεχνική "απόδειξης μηδενικής γνώσης" που λέγεται **zk-SNARK** [48].
4. **Dash (DASH)** Το Dash [49] (αρχικά γνωστό και ως darkcoin) είναι μία πιο μυστική έκδοση του bitcoin. Το Dash προσφέρει περισσότερη ανωνυμία επειδή λειτουργεί σε ένα δίκτυο από dedicated servers που λέγονται masternodes το οποίο καθιστά τις συναλλαγές σχεδόν μη ανιχνεύσιμες. Ξεκίνησε το 2014 και μπορεί να εξορυχθεί χρησιμοποιώντας είτε CPU είτε GPU. Το 2015 μετονομάστηκε από darkcoin σε Dash (digital cash). Κάποια πολύ βασικά του χαρακτηριστικά είναι τα PrivateSend [50] και InstantX [51] που επιτρέπει την πραγματοποίηση συναλλαγών σε χρόνους όμοιους με αυτούς των πιστωτικών καρτών.
5. **Dash (Ripple (XRP))** Το Ripple Protocol [52] είναι ένα πρωτόκολλο που χρησιμοποιεί το νόμισμα Ripple (με το ίδιο όνομα) ή αλλιώς XRP δηλαδή ένα ακόμα κρυπτονόμισμα με στόχο την πραγματοποίηση συναλλαγών σε πραγματικό χρόνο. Έχει σχεδιαστεί για να χρησιμοποιείται από τις τράπεζες για την ανταλλαγή χρημάτων, εμβασμάτων και κάθε είδους συναλλαγών. Η βασική του ιδέα είναι οι τράπεζες να αντικαταστήσουν τα παλαιά συστήματα συναλλαγών όπως το SWIFT, που αναπτύχθηκε το 1972 και χρησιμοποιείται ακόμα και σήμερα από τις περισσότερες τράπεζες παγκοσμίως. Είναι αρκετά συχνό φαινόμενο να συγχέεται το πρωτόκολλο Ripple με το νόμισμα Ripple (XRP). Το κρυπτονόμισμα Ripple (XRP) έχει εκδοθεί από το Ripple Labs.Το XRP είναι ένα token που χρησιμοποιεί το Ripple δίκτυο και μπορεί να πραγματοποιήσει συναλλαγές πολύ γρήγορα και με χαμηλές αμοιβές. Το Ripple κυκλοφόρησε το 2012.
6. **Monero (XMR)** Το Monero (XMR) [53] είναι και αυτό ένα ανοικτού κώδικα κρυ-

πτονόμισμα το οποίο δημιουργήθηκε τον Απρίλιο του 2014 και είναι εστιασμένο στην ιδιωτικότητα, την αποκέντρωση και την επεκτασιμότητα. Αντίθετα με τα περισσότερα κρυπτονομίσματα που είναι εκδόσεις ή αντίγραφα του bitcoin, το Μονέρο είναι βασισμένο στο πρωτόκολλο Cryptonote [54] και διαθέτοντας ένα αδιαφανές blockchain σε αντίθεση με το διαφανές blockchain που χρησιμοποιείται από οποιαδήποτε άλλη κρυπτογράφηση που δεν βασίζεται στο CryptoNote, προσφέρει υψηλή ιδιωτικότητα στις συναλλαγές.

7. **Bitcoin Cash (BCH)** Το Bitcoin στις αρχές Αυγούστου 2017 υπέστη ένα γεγονός γνωστό ως ”hard fork”. Αυτό οδήγησε στη διάσπασή του σε δυο διαφορετικά κρυπτονομίσματα, το κλασικό Bitcoin και το Bitcoin Cash [55]. Η συζήτηση που οδήγησε στη δημιουργία της BCH είχε να κάνει με το ζήτημα της επεκτασιμότητας. Το bitcoin έχει ένα αυστηρό όριο στο μέγεθος των μπλοκ που είναι το 1 megabyte. Το BCH αυξάνει το μέγεθος του μπλοκ από 1 MB σε 8 MB, με την ιδέα ότι τα μεγαλύτερα μπλοκ θα επιτρέψουν ταχύτερους χρόνους συναλλαγής.
8. **NEO (NEO)** Το NEO [56] ξεκίνησε το 2014. Στην αρχή λεγόταν AntShares. Αυτή τη στιγμή είναι το μεγαλύτερο σε όγκο συναλλαγών κρυποτονόμισμα που ξεκίνησε από την Κίνα και λέγεται ότι είναι το κινέζικο ανάλογο του Ethereum λόγω της παρόμοιας χρήσης των έξυπνων συμβολαίων. Κλειδί της επιτυχίας του NEO είναι η δυνατότητα προγραμματισμού του σε διάφορες γλώσσες προγραμματισμού, όπως Go, Java, C++ κ.ά. Επίσης το NEO ωφελήθηκε από την θετική υποστήριξη που είχε από την κινεζική κυβέρνηση η οποία είναι γνωστή για την αντίθεσή της στα κρυπτονομίσματα.
9. **Cardano (ADA)** Το Cardano [57] ξεκίνησε από έναν από τους συνιδρυτές του ethereum τον Σεπτέμβριο του 2017. Ισχυρίζεται ότι προσφέρει όλα τα πλεονεκτήματα του etherium και περισσότερα. Εκτός των άλλων, το ADA στοχεύει στο να λύσει προβλήματα που μαστίζουν τα κρυπτονομίσματα, όπως η διαλειτουργικότητα και η επεκτασιμότητα. Επίσης ελπίζει ότι θα λύσει προβλήματα που αφορούν διεθνείς συναλλαγές οι οποίες είναι ακριβές και χρονοβόρες.
10. **EOS (EOS)** Ένα από τα νεότερα ψηφιακά νομίσματα, το EOS [58] ξεκίνησε τον Ιούνιο του 2018. Έχει σχεδιαστεί με βαση το etherium, άρα προσφέρει μία πλατφόρμα πάνω στην οποία μπορούν να δημιουργηθούν αποκεντρωμένες εφαρμογές. Ένας από τους κυρίους λόγος για την επιτυχία του είναι ότι είχε την μεγαλύτερη αρχική (ICO) προσφορά νομισμάτων στην ιστορία των κρυποτονομισμάτων. Επίσης το EOS προσφέρει έναν εξουσιοδοτημένο μηχανισμό απόδειξης συμμετοχής (Proof of stake (POS)), και ελπίζει ότι θα είναι σε θέση να προσφέρει μεγαλύτερη επεκτασιμότητα από αυτήν που είναι σε θέση να προσφέρουν οι ανταγωνιστές του. Στο EOS δεν

υπάρχει μηχανισμός εξόρυξης για την παραγωγή νομισμάτων. Αντ' αυτού, οι χρήστες που συγκροτούν και παράγουν τα block, ανταμοίβονται με νομίσματα EOS με βαση τον ρυθμό παραγωγής τους. Η ιδέα πίσω από αυτήν την λειτουργία είναι ότι τελικά το δίκτυο θα γίνει πιο δημοκρατικό και αποκεντρωμένο από ότι τα άλλα κρυπτονομίσματα.

Το Bitcoin συνεχίζει να οδηγεί το πακέτο των κρυπτονομισμάτων, από την άποψη της κεφαλαιοποίησης της αγοράς, της βάσης χρηστών και της δημοτικότητας. Παρόλα αυτά, νομίσματα όπως το etherium και το ripple, τα οποία χρησιμοποιούνται περισσότερο για επιχειρησιακές λύσεις, γίνονται δημοφιλή, ενώ ορισμένα altcoins θεωρούνται ότι έχουν ανώτερα ή προηγμένα χαρακτηριστικά έναντι των bitcoins. Η παρούσα τάση υποδεικνύει ότι τα κρυπτονομίσματα είναι εδώ για να παραμείνουν, αλλά πόσα από αυτά θα εμφανιστούν ως ηγέτες εν μέσω του αυξανόμενου ανταγωνισμού στο χώρο αυτό, θα αποκαλυφθεί μόνο με το χρόνο.

Κεφάλαιο 9

Εφαρμογές της Blockchain

Με την εφεύρεση του bitcoin έγινε γνωστή για πρώτη φορά η έννοια της blockchain. Μέχρι το 2013 δεν είχαν συνειδητοποιηθεί οι δυνατότητες αυτης της καινούργιας τεχνολογίας πέραν της εφαρμογής της στην δημιουργία ψηφιακών νομισμάτων. Με την εμφάνιση της Blockchain 2.0 που επέτρεπε **προγραμματιζόμενες συναλλαγές** (συναλλαγές που τροποποιούνται από μια συνθήκη ή ένα σύνολο προϋποθέσεων) φάνηκαν τα πραγματικά οφέλη από την εφαρμογή αυτής της τεχνολογίας σε πολλές διαφορετικές βιομηχανίες. Από το 2013 μέχρι τώρα έχουν προταθεί πολλές χρήσεις της τεχνολογίας blockchain σε διάφορους κλάδους οι οποίες περιλαμβάνουν, αλλά δεν περιορίζονται μόνο, τον χρηματοοικονομικό κλάδο, το IoT (Internet Of Things), τη διαχείριση ψηφιακών δικαιωμάτων, την ηλεκτρονική διακυβέρνηση, την υγεία, τις μεταφορές, το δίκαιο κ.α.

9.1 Internet of Things

Το Διαδίκτυο των Πραγμάτων (Internet of Things) μπορεί να οριστεί ως ένα δίκτυο υπολογιστικά ευφυών φυσικών αντικειμένων που είναι ικανά να συνδεθούν στο διαδίκτυο, να ανιχνεύσουν γεγονότα ή περιβάλλοντα του πραγματικού κόσμου, να αντιδράσουν στα γεγονότα αυτά, να συλλέξουν σχετικά δεδομένα και να επικοινωνήσουν μέσω του διαδικτύου. Ένα τυπικό IoT αποτελείται από πολλά φυσικά αντικείμενα που είναι συνδεδεμένα μεταξύ τους και όλα μαζί σε ένα κεντρικό εξυπηρετητή [59].

Για να περιγραφεί το IoT μπορεί να χρησιμοποιηθεί ένα μοντέλο πέντε επιπέδων, το οποίο αποτελείται από ένα επίπεδο φυσικών αντικειμένων (physical object layer), ένα επίπεδο συσκευών (device layer), ένα επίπεδο δικτύου (network layer), ένα επίπεδο υπηρεσιών διαχείρισης (management layer) και ένα επίπεδο εφαρμογών (application layer). Κάθε επίπεδο είναι υπεύθυνο για διάφορες λειτουργίες και περιλαμβάνει διάφορα στοιχεία.

- **Επίπεδο φυσικών αντικειμένων - (Physical object layer)**. Περιλαμβάνει όλα τα φυσικά αντικείμενα του πραγματικού κόσμου όπως ανθρώπους, ζώα, αυτοκίνητα, δέντρα, ψυγεία, τρένα, εργοστάσια, σπίτια. Οτιδήποτε μπορεί να παρακολουθηθεί και ελεγχθεί μπορεί να συνδεθεί με το IoT.
- **Επίπεδο συσκευών - (Device layer)**. Περιέχει αντικείμενα όπως αισθητήρες, μετατροπείς, ενεργοποιητές, έξυπνα τηλέφωνα και συσκευές και RFIDs (σημαντήρες ταυτοποίησης μέσω ραδιοσυχνοτήτων).
- **Επίπεδο δικτύου (network layer)**. Αποτελείται από διάφορες συσκευές δικτύου που χρησιμοποιούνται για την παροχή σύνδεσης μεταξύ συσκευών στο διαδίκτυο και για την σύνδεση τους με το υπολογιστικό νέφος ή τους διακομιστές που αποτελούν μέρος του οικοσυστήματος IoT.
- **Επίπεδο υπηρεσιών διαχείρισης (Management layer)**. Παρέχει τη διαχείριση για το IoT. Περιλαμβάνει πλατφόρμες που επιτρέπουν την επεξεργασία των δεδομένων που συλλέγονται από τις συσκευές IoT. Σε αυτό το επίπεδο περιλαμβάνονται επίσης η διαχείριση συσκευών, η διαχείριση ασφάλειας και η διαχείριση ροής δεδομένων καθώς και η διαχειρίση της επικοινωνίας μεταξύ των συσκευών και του επιπέδου εφαρμογών.
- **Επίπεδο εφαρμογών (Application layer)**. Περιλαμβάνει εφαρμογές που τρέχουν στην κορυφή του IoT. Ενδεικτικά περιλαμβάνει εφαρμογές για χρηματοοικονομικές υπηρεσίες, ασφάλιση, υγειονομική περίθαλψη, μεταφορές, διαχείριση αλυσίδων εφοδιασμού κ.α.

Το κανονικό μοντέλος IoT είναι κεντροποιημένο. Συσκευές IoT συνδέονται με μία υποδομή νέφους (cloud infrastructure) [60] η με κεντρικούς διακομιστές προκειμένου να αναφέρουν και να επεξεργαζονται τα σχετικά δεδομένα. Η κεντροποιημένη δομή είναι ευάλωτη σε hacking και σε κλοπή δεδομένων. Η απώλεια ελέγχου των προσωπικών δεδομένων σε ένα ενιαίο κεντρικό φορέα παροχής υπηρεσιών αυξάνει την πιθανότητα δημιουργίας ζητημάτων ασφάλειας και προστασίας της ιδιωτικής ζωής. Μολονότι υπάρχουν οι μέθοδοι και οι τεχνικές για την δημιουργία ενός πολύ ασφαλούς IoT, ένα μοντέλο IoT βασισμένο στη τεχνολογία της blockchain έχει πολλά περισσότερα οφέλη από το κανονικό μοντέλο IoT. Σύμφωνα με την IBM [61], το blockchain για το IoT μπορεί να συμβάλει στην οικοδόμηση εμπιστοσύνης, στη μείωση του κόστους και την επιταχύνση των συναλλαγών. Επιπλέον, η αποκέντρωση, η οποία βρίσκεται στον πυρήνα της τεχνολογίας blockchain, μπορεί να εξαλείψει μεμονωμένα σημεία αποτυχίας σε ένα δίκτυο IoT. Για παράδειγμα, ένας κεντρικός διακομιστής ίσως δεν είναι σε θέση να αντιμετωπίσει τον όγκο των δεδομένων που θα παρά-

γουν δισεκατομμύρια συσκευές IoT. Επίσης, η peer-to-peer επικοινωνία που παρέχεται από τη blockchain μπορεί να συμβάλει στη μείωση του κόστους, διότι δεν θα υπάρχει ανάγκη κατασκευής υψηλού κόστους κεντρικών δομών επεξεργασίας και αποθήκευσης δεδομένων ή η εφαρμογή πολύπλοκων υποδομών δημόσιου κλειδιού για ασφάλεια. Οι συσκευές μπορούν να επικοινωνούν μεταξύ τους απευθείας ή μέσω δρομολογητών.

Το με βάση την Blockchain IoT, μπορεί να δώσει λύσεις στα προβλήματα της επεκτασιμότητας, της ιδιωτικότητας και της αξιοπιστίας που υπάρχουν στο τρέχον μοντέλο IoT. Η τεχνολογία της blockchain επιτρέπει την άμεση επικοινωνία και συναλλαγή μεταξύ των ”πραγμάτων” και με την διαθεσιμότητα των έξυπνων συμβολαίων (smart contracts) η διαπραγμάτευση και οι οικονομικές συναλλαγές μεταξύ των συσκευών μπορούν να πραγματοποιηθούν χωρίς την ανάγκη κάποιου μεσάζοντα, μίας κεντρικής αρχής ή ανθρώπινης παρέμβασης. Μπορεί να υιοθετηθεί το μοντέλο IoT πέντε επιπέδων που αναφέραμε προηγουμένως, με την προσθήκη ενός επιπέδου blockchain μεταξύ του επιπέδου δικτύου και του επιπέδου υπηρεσιών διαχείρισης. Το επίπεδο αυτό θα εκτελεί έξυπνα συμβόλαια και θα παρέχει ασφάλεια, ιδιωτικότητα, ακεραιότητα, αυτονομία, επεκτασιμότητα και αποκεντρωμένες υπηρεσίες στο IoT. Το επίπεδο υπηρεσιών διαχείρισης θα αποτελείται μόνο από εφαρμογές που θα σχετίζονται με την ανάλυση και επεξεργασία δεδομένων, ενώ η ασφάλεια και ο έλεγχος θα μεταφερθούν στο επίπεδο blockchain.

9.2 Ηλεκτρονική Διακυβέρνηση

Υπάρχουν διάφορες εφαρμογές της blockchain στην ηλεκτρονική διακυβέρνηση, που ερευνώνται σήμερα. Η εφαρμογή της τεχνολογίας blockchain μπορεί να βελτιώσει τις ήδη υπάρχουσες κυβερνητικές λειτουργίες. Κάποιες από τις εφαρμογές αυτές, είναι η ψηφιακή ψηφοφορία, οι ψηφιακές ταυτότητες κ.α.

9.2.1 Ψηφιακή ψηφοφορία

Οι εκλογικές διαδικασίες σήμερα, σε διάφορες χώρες του κόσμου γίνονται με δύο τρόπους. Με τον κλασσικό τρόπο των χάρτινων ψηφοδελτίων και των φακέλλων και με ηλεκτρονικό τρόπο, όπου ο πολίτης ψηφίζει σε ειδικές μηχανές που καταμετρούν την ψήφο ψηφιακα. (π.χ Ηνωμένες Πολιτείες Αμερικής). Και τα δύο σύστήματα έχουν υποστεί σοβαρή κριτική, το πρώτο σε χώρες που οι δημοκρατικές διαδικασίες είναι υπό αμφισβήτηση και το δεύτερο λόγω του ότι η τεχνολογία που χρησιμοποιείται είναι πλέον παρωχημένη και ευάλωτη σε κυβερνοεπιθέσεις. Τα συστήματα ψήφου βασισμένα σε τεχνολογία blockchain μπορούν να επιλύσουν τέτοια προβλήματα, εισάγοντας ασφάλεια και διαφάνεια στην δια-

δικασία των ψηφοφοριών [62, 63, 64, 65, 66, 67] . Η ασφάλεια παρέχεται με την μορφή της ακεραιότητας και αυθεντικότητας των ψήφων, χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού η οποία είναι δεδομένη στην τεχνολογία blockchain. Επιπλέον, η τεχνολογία της blockchain μπορεί να εξασφαλίσει ότι μία ψήφος θα υπολογιστεί μόνο μία φορά και δεν θα μπορεί να ξαναμετρηθεί. Αυτό μπορεί να επιτευχθεί μέσω ενός συνδυασμού βιομετρικών χαρακτηριστικών(π.χ δακτυλικό αποτύπωμα) και ενός έξυπνου συμβολαίου το οποίο θα διατηρεί ένα κατάλογο των ψήφων που έχουν ήδη καταμετρηθεί. Για την προστασία της ιδιωτικότητας της ψήφου μπορούν να χρησιμοποιηθούν τεχνικές μηδενικής γνώσης στην blockchain.

9.2.2 Ψηφιακές ταυτότητες

Ψηφιοποιημένα δελτία ταυτότητας έχουν αρχίσει εδώ και καιρό να εκδίδονται από πολλές χώρες του κόσμου. Οι ταυτότητες αυτές διαθέτουν πολλά χαρακτηριστικά ασφαλείας που αποτρέπουν τις προσπάθειες αναπαραγωγής ή αλλοίωσης. Ωστόσο, με την τεχνολογίας blockchain μπορούν να γίνουν πολλές βελτιώσεις [68, 69]. Η ψηφιακή ταυτότητα δεν περιορίζεται μόνο στις κάρτες ταυτότητας που εκδίδονται από τις κυβερνήσεις. Είναι μια έννοια που μπορεί να εφαρμοστεί στα κοινωνικά δίκτυα και στα φόρουμ. Πολλαπλές ψηφιακές ταυτότητες μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς. Μια ηλεκτρονική ψηφιακή ταυτότητα βασισμένη στην blockchain επιτρέπει τον έλεγχο της ανταλλαγής προσωπικών πληροφοριών. Οι χρήστες μπορούν να δουν ποιος χρησιμοποίησε τα δεδομένα τους και για ποιο σκοπό και ποιος μπορεί να ελέγξει την πρόσβαση σε αυτά. Αυτό δεν είναι δυνατό με τις τρέχουσες υποδομές που είναι κεντροποιημένες. Το βασικό όφελος είναι ότι μια ενιαία ταυτότητα που εκδίδεται από την κυβέρνηση μπορεί να χρησιμοποιηθεί εύκολα και με διαφανή τρόπο για πολλαπλές υπηρεσίες μέσω μίας ενιαίας κυβερνητικής blockchain. Σε αυτή την περίπτωση, η blockchain θα χρησιμεύσει ως πλατφόρμα όπου η κυβέρνηση θα παρέχει διάφορες υπηρεσίες όπως οι συντάξεις, η φορολογία κ.α. Μία ενιαία ταυτότητα θα χρησιμοποιηθεί για την πρόσβαση σε όλες αυτές τις υπηρεσίες. Σε αυτήν την περίπτωση η blockchain θα παρέχει ένα αμετάβλητο αρχείο κάθε αλλαγής και συναλλαγής που πραγματοποιείται με την ψηφιακή ταυτότητα, εξασφαλίζοντας έτσι την ακεραιότητα και τη διαφάνεια του συστήματος. Επίσης οι πολίτες μπορούν να βεβαιώνουν, να λαμβάνουν και να χρησιμοποιούν, πιστοποιητικά γέννησης, γάμου, συμβολαιογραφικών πράξεων και πολλά άλλα έγγραφα που θα υπάρχουν στην κυβερνητική blockchain και θα συνδέονται με την ψηφιακή τους ταυτότητα. Επί του παρόντος, υπάρχουν επιτυχημένες εφαρμογές συστημάτων ταυτότητας σε διάφορες χώρες, οι οποίες λειτουργούν καλά και εδώ υπάρχει ένα επιχείρημα ότι ίσως δεν απαιτείται μία κυβερνητική blockchain στα συστήματα διαχείρισης ταυτότη-

τας. Παρόλο που η χρήση της τεχνολογίας blockchain μπορεί να δώσει πολλά οφέλη, όπως η προστασία της ιδιωτικής ζωής και ο έλεγχος της χρήσης των στοιχείων ταυτότητας, η τρέχουσα ανωριμότητα της τεχνολογίας blockchain είναι μεγάλος ανασταλτικός παράγοντας για την εφαρμογή της σε συστήματα ταυτοτήτων στον πραγματικό κόσμο. Ωστόσο, πραγματοποιούνται έρευνες από διάφορες κυβερνήσεις για τη χρήση της τεχνολογίας blockchain στη διαχείριση συστημάτων ταυτότητας.

9.2.3 Διάφορες κυβερνητικές υπηρεσίες

Η τεχνολογία blockchain θα μπορούσε να εφαρμοστεί στην φορολογία, στη διαχείριση των παροχών και στην εκταμίευσή τους, στη διαχείριση των αρχείων ιδιοκτησίας ακινήτων, στις διάφορες μορφές ληξιαρχικών πράξεων όπως γεννήσεις, γάμοι, θανάτοι, στις άδειες και μεταβιβάσεις αυτοκινήτων κ.α. Είναι προφανές ότι με την πάροδο του χρόνου πολλές κυβερνητικές υπηρεσίες και διαδικασίες θα μπορούσαν να προσαρμοστούν σε ένα μοντέλο που θα βασίζεται στην τεχνολογία blockchain. Τα βασικά πλεονεκτήματα του blockchain, όπως η μη αλλοίωση των εγγραφών,η διαφάνεια και η αποκέντρωση μπορεί να συμβάλουν στη βελτίωση των περισσότερων παραδοσιακών κυβερνητικών συστημάτων.

9.2.4 Υπηρεσίες υγείας

Ο τομέας της υγείας έχει χαρακτηριστεί ως ένας άλλος σημαντικός κλάδος που μπορεί να ωφεληθεί από την τεχνολογία blockchain [70, 71, 72, 73, 74]. Στην υγειονομική περίθαλψη, μεγάλα ζητήματα, όπως η παραβίαση της ιδιωτικότητας και των ιατρικών δεδομένων, απάτες και υψηλά κόστη μπορεί να προκύψουν απο την έλλειψη διαλειτουργικότητας και από υπερβολικά περίπλοκες διαδικασίες διαφάνειας και ελέγχου. Ένα άλλο πρόβλημα είναι τα πλαστά φάρμακα. Στις αναπτυσσόμενες χώρες, αυτό αποτελεί βασική αιτία ανησυχίας. Λόγω της προσαρμοστικότητας της blockchain μπορεί να προκύψουν οφέλη όπως εξοικονόμηση κόστους, αυξημένη εμπιστοσύνη, ταχύτερη διεκπεραίωση των απαιτήσεων, υψηλότερη διαθεσιμότητα των υπηρεσιών υγείας, εξάλειψη λειτουργικών λαθών λόγω της πολυπλοκότητας των επιχειρησιακών διαδικασιών και αποτροπή της διανομής πλαστών φαρμάκων.

9.3 Χρηματοοικονομικές υπηρεσίες

Οι εφαρμογές της blockchain στον τομέα των χρηματοοικονομικών υπηρεσιών είναι είναι το κύριο θέμα συζήτησης αυτή τη στιγμή. Τράπεζες και μεγάλοι χρηματοοικονομικοί

οργανισμοί έχουν ξεκινήσει έρευνες για να βρεθούν τρόποι προσαρμογής της τεχνολογίας blockchain κυρίως λόγω της δυνατότητας εξοικονόμησης κόστους που προσφέρει.

9.4 Ασφαλιστικές υπηρεσίες

Στον τομέα αυτό η τεχνολογία blockchain σε συνδυασμό με το IoT, μπορεί να επιταχύνει τις διαδικασίες διεκπεραίωσης των ασφαλιστικών αξιώσεων και να βοηθήσει στην ανίχνευση ασφαλιστικών απατών. Για παράδειγμα, όταν συμβεί ένα ατύχημα μπορεί μέσω έξυπνων συσκευών, έξυπνων συμβολαίων και εφαρμογών τηλεμετρίας, να καταγραφούν τα δεδομένα του ατυχήματος και βάσει αυτών αυτόματα να εκπληρωθούν οι όποιες αξιώσεις προκύψουν μεταξύ των συμβαλλομένων μερών.

9.5 Διάφορες εφαρμογές

Η τεχνολογία blockchain θα μπορούσε να εφαρμοστεί στην διαχείριση των πνευματικών δικαιωμάτων, στην αυτοκινητοβιομηχανία, στο leasing αυτοκινήτων, στην παρακολούθηση εταιρικών στόλων, στην κτηματαγορά καθώς και σε στρατιωτικές εφαρμογές [75].

Κεφάλαιο 10

Stablecoins

Τα Stablecoins είναι μια ειδική κατηγορία κρυπτονομισμάτων, τα οποία συνδεόνται με κλειδωμένη ισοτιμία με κάποια περιουσιακά στοιχεία σταθερής, με την έννοια της όχι ιδιαίτερα ευάλωτης σε μεγάλες μεταβολές, αξίας, όπως κάποιο ισχυρό νόμισμα ή ο χρυσός.

Δημιουργήθηκαν για να λύσουν το πρόβλημα της υψηλής μεταβλητότητας των τιμών των κλασσικών κρυπτονομισμάτων, η οποία έχει σαν αποτέλεσμα την μεγάλη δυσκολία υιοθέτησης αυτών από το ευρύτερο κοινό ως μέσο πραγματοποίησης καθημερινών συναλλαγών.

Τα Stablecoins ενσωματώνουν τα καλύτερα χαρακτηριστικά των κλασσικών κρυπτονομισμάτων, έτσι η χρήση τους ποικίλει από την πραγματοποίηση καθημερινών συναλλάγων με ελάχιστες έως σχεδόν μηδενικές αμοιβές συναλλαγής καθώς και εξαιρετικά γρήγορη διευθέτηση αυτών σε σχέση με τις κλασσικές μεθόδους όπως τραπεζικές συναλλαγές και χρήση πιστωτικών ή χρεωστικών καρτών, την αποθήκευση μίας αξίας καθώς και για την παροχή ενός λιγότερου ευμετάβλητου περιβάλλοντος για διαπραγματευτές χονδρικής (wholesale traders), λιανικής (retail traders) και μεσιτών (brokers) που δραστηριοποιούνται στην αγορά των κρυπτονομισμάτων, κατά τις περιόδους υψηλών διακυμάνσεων της αγοράς αυτής.

Στον παραδοσιακό κόσμο του συναλλάγματος, δεν υπάρχει ένα πραγματικά σταθερό νόμισμα. Αυτό οφείλεται στο γεγονός ότι όλα τα νομίσματα fiat, όπως το δολάριο ΗΠΑ και το ευρώ, υπόκεινται σε κυμαινόμενες συναλλαγματικές ισοτιμίες και σε πληθωρισμό. Αυτές οι διακυμάνσεις είναι συνήθως αρκετά μικρές ώστε να μην τα εμποδίζουν να είναι τα κύρια μέσα συναλλαγής σε καθημερινή βάση.

Στον ψηφιακό κόσμο, έχουμε δει ότι τα κρυπτονομίσματα υπόκεινται σε τεράστια μεταβλητότητα. Για ένα μικρό μέρος των ατόμων, που συχνά αναφέρονται ως κερδοσκοπικοί επενδυτές, η αστάθεια αυτή υποστηρίζει το προτιμώμενο επίπεδο κινδύνου. Αλλά για την

πλειονότητα των βασικών καταναλωτών, αυτή η αστάθεια δεν αποτελεί ελκυστική επιλογή και δεν είναι πρακτική λύση για τις καθημερινές συναλλαγές τους ή για μακροπρόθεσμες επενδύσεις.

Προκειμένου ένα Stablecoin να είναι επιτυχημένο, πρέπει να προσφέρει προστασία από πολλούς παράγοντες που προκαλούν μεταβλητότητα στην τιμή του, είτε τώρα είτε έπειτα από 100 χρόνια.

Ανεξάρτητα από τον τύπο του νομίσματος, η σταθερότητα είναι ζωτικής σημασίας για την προστασία των αγοραστών και των πωλητών από την απώλεια αξίας κατά τη διάρκεια μιας συναλλαγής ή κατά τη διάρκεια μιας επένδυσης. Χωρίς κάποια σταθερότητα, είναι μάλλον απίθανο να υιοθετηθούν είτε ως ένα κύριο σύστημα πληρωμών είτε ως επενδυτική επιλογή. Κατά τη διάρκεια μιας κρίσης στην αγορά των κρυπτονομισμάτων ακόμη και οι κερδοσκοπικοί επενδυτές πρέπει έστω και προσωρινά να επενδύσουν τα χρήματά τους σε κάποιο Stablecoin έτσι ώστε να αποφύγουν τυχόν απώλειες. Με τα Stablecoins εμφανίζεται μία νέα ευκαιρία που μπορεί να παράσχει προστασία από την υψηλή μεταβλητότητα των κλασσικών κρυπτονομισμάτων.

10.1 Πλεονεκτήματα των Stablecoins

Τα Stablecoins αντιμετωπίζουν τα παρακάτω μειονεκτήματα των κλασσικών κρυπτονομισμάτων:

(i) **Διακύμανση τιμών**: Τα κρυπτονομισμάτα έχουν υψηλή μεταβλητότητα και οι τιμές τους υπόκεινται σε μεγάλες διακυμάνσεις,

(ii) **Τιμή που εξαρτάται από την κερδοσκοπία**: Οι τιμές της πλειοψηφίας των κρυπτονομισμάτων βασίζονται στην κερδοσκοπία και για αυτό το λόγο και δεν έχουν ακόμη αποδειχθεί αποτελεσματικά για ευρύτερες εμπορικές χρήσεις,

(iii) **Εμπορικός κίνδυνος**: Οι επιχειρήσεις είναι απρόθυμες να αναλάβουν τον κίνδυνο των μεγάλων διακυμάνσεων των τιμών,προκειμένου να αποδεχθούν τα κρυπτονομίσματα ως επιλογή πληρωμής,

(iv) **Έλλειψη εμπιστοσύνης των επενδυτών**: Υψηλή μεταβλητότητα που μπορεί να οδηγήσει, λόγω έλλειψης εμπιστοσύνης των επενδυτών, σε μεγάλη έξοδο αυτών από τα διάφορα project με αποτέλεσμα να προκληθούν ζημιές στις επιχειρήσεις που ασχολούνται με αυτά,

(v) **Αμοιβές δικτύου**: Μεγάλες διαφορές στα τέλη συναλλαγών και αργοί χρόνοι επεξεργασία των συναλλαγών στα αντίστοιχα δίκτυα.

10.2 Μέθοδοι ευστάθειας των Stablecoins

Σήμερα υπάρχουν τρείς μέθοδοι που προσπαθούν να δώσουν λύση στο πρόβλημα της ευστάθειας των τιμών των Stablecoins με αντίστοιχα πλεονεκτήματα και μειονεκτήματα:

(i) **Μέθοδος 1: Centralized and Fiat or asset-collateralized** (Συγκεντρωτική και εξασφαλισμένη απο χρήμα αναγκαστικής κυκλοφορίας ή επενδυτικά αγαθά): Stablecoins που υποστηρίζονται από χρήμα αναγκαστικής κυκλοφορίας ή παραστατικό χρήμα (Fiat money) όπως το δολάριο ή το ευρώ, από πολύτιμα μέταλλα ή από άλλα επενδυτικά αγαθά ή περιουσιακά στοιχεία. Απαιτείται εμπιστοσύνη σε ενα κεντρικό και αδιαφανές συμβαλλόμενο μέρος (συνήθως μια ιδιωτική εταιρεία) που θα εγγυάται την αξία τους.

Το πρωτόκολλο αυτό είναι απλό και μπορεί να περιγραφεί ως συναλλαγή 1:1. Ένας χρήστης καταθέτει ένα ευρώ ή δολλάριο σε μία εταιρεία χαρτοφυλακίων που ενεργεί ως κεντρικό συμβαλλόμενο μέρος. Σε αντάλλαγμα ο χρήστης λαμβάνει ένα Stablecoin αξίας ενός ευρώ ή ενός δολλαρίου. Θεωρητικά, ο χρήστης μπορεί οποιαδήποτε στιγμή να επιστρέψει το stablecoin στην εταιρεία και να λάβει πίσω την αξία του σε ευρώ ή δολλάριο. Η μεθοδος αυτή είναι πολύ απλή και θεωρητικά πολύ ισχυρή. Όμως η εταιρεία που ενεργεί ως το κεντρικό συμβαλλόμενο μέρος μπορεί να μην μπορέσει να επιστρέψει τα κεφάλαια όταν της ζητηθούν ή μπορεί να δημιουργήσει περισσότερα stablecoins από τα κεφάλαια τα όποια έχει σε πραγματικό συνάλλαγμα. Επίσης ελοχεύει ο κίνδυνος της αστάθειας και μεταβλητότητας των τιμών του FIAT χρήματος ή των τιμών των άλλων περιουσιακών αγαθών που είναι συνδεδεμένα με το εκδοθέν stablecoin.

Σε αυτή την κατηγορία ανήκουν τα stablecoins **USD Coin, tether, GEMINI dollar, TrustToken** τα οποία είναι εξασφαλισμένα με fiat νομίσματα, καθώς και τα **DGX, ONEGRAM, HelloGold, SendGold** που είναι εξασφαλισμένα με επενδυτικά αγαθά όπως ο χρυσός και άλλα.

(ii) **Μέθοδος 2: Decentralized and Crypto-Collateralized** (Αποκεντρωμένη και εξασφαλισμένη με κρυπτονομίσματα): Σε αντίθεση με την πρώτη μέθοδο οι χρήστες κάνουν την αρχική τους κατάθεση με κάποιο κρυπτονόμισμα. Αυτό επιτρέπει την διαχείριση της συναλλαγής με τη χρήση κάποιου έξυπνου συμβολαίου, επιτυγχάνοντας έτσι την αποκεντρωμένη διαχείριση.

Το πρωτόκολλο αυτό λειτουργεί με τρόπο παρόμοιο με τα ενυπόθηκα δάνεια. Οι χρήστες καταθέτουν τα κρυπτονομίσματά τους και δανείζονται έναντι αυτών stablecoins.

Επειδή οι εξασφαλίσεις βασίζονται σε κρυπτονόμισμα και πρέπει να αντέχουν την αστάθεια των τιμών, το πρωτόκολλο πρέπει να διαχειριστεί μία αναλογία δανείου προς αξία με λόγο 1:2. Το πρωτόκολλο αυτό είτε δουλεύει είτε αποτυγχάνει πλήρως.

Για παράδειγμα, εάν η αξία της εξασφάλισης με κρυπτονομίσματα πέσει περισσότερο από 50% (κάτι που έχει συμβεί πολλές φορές στο παρελθόν με τις τιμές των κρυπτονομισμάτων) τα κεφάλαια εξασφάλισης δεν θα μπορέσουν να υποστηρίξουν αυτή τη μεταβλητότητα. Το stablecoin δεν θα μπορέσει να διατηρήσει την ευστάθεια της τιμής του και θα υπάρξει μεγάλος κίνδυνος κατάρρευσης της τιμής του. Σε αυτό το σημείο, η εταιρεία που διαχειρίζεται το stablecoin θα απαιτήσει από τους χρήστες να επιστρέψουν τα stablecoins εάν η αξία των εξασφαλίσεων έχει πτώση κάτα 25% και ο λόγος δανείου προς αξία γίνει 1:1.5. Εάν οι χρήστες αρνηθούν, τότε η εταιρεία θα προχωρήσει σε πλειστηριασμό των εξασφαλίσεων και θα τις παραχωρήσει στον υψηλότερο πλειοδότη, όπως ακριβώς μία τράπεζα θα προχωρούσε στον εκπλειστηριασμό ενός ακινήτου του οποίου οι ιδιοκτήτες δεν πλήρωναν την υποθήκη τους στον απαιτούμενο χρόνο.

Σε αυτή την κατηγορία ανήκουν τα stablecoins **MAKER, Huobi, ALCHEMINT** και άλλα.

(iii) **Μέθοδος 3: Decentralized and Non-Collateralized**(Αποκεντρωμένη και όχι εξασφαλισμένη): Η μέθοδος αυτή δεν επαφίεται σε σύνδεση της τιμής του stablecoin με κάποιο fiat νόμισμα, με κρυπτονόμισμα ή κάποιο περιουσιακό αγαθό. Υποστηρίζεται μόνο από την ισχυρή εμπιστοσύνη στην ευστάθεια της τιμής του νομίσματος. Για να μπορέσει να λειτουργήσει αυτή η μέθοδος απαιτούνται δύο συνθήκες:

Η πρώτη, πρέπει να εξασφαλίζει ότι το σύστημα δεν θα αφήνει την τιμή του stablecoin να αυξηθεί πέραν του ενός ευρώ ή δολλαρίου. Αυτό μπορεί να γίνει εύκολα. Εάν η τιμή αυξηθεί πάνω από ένα ευρώ η δολλάριο, το σύστημα δημιουργεί επιπλέον stablecoins ούτως ώστε η τιμή να ισορροπήσει.

Η δεύτερη, πρέπει να εξασφαλίζει ότι το σύστημα δεν θα αφήνει την τιμή του stablecoin να μειωθεί κάτω από ένα ευρώ ή δολλαρίου. Όταν ξεκινήσει η μείωση της τιμής, το σύστημα πρέπει να μειώσει την ποσότητα των κυκλοφορούντων stablecoins και εδώ δημιουργείται το ακόλουθο πρόβλημα. Για να αφαιρεθούν stablecoins από την κυκλοφορία, θα πρέπει οι χρήστες που τα έχουν στην κατοχή τους να συμφωνήσουν να τα ανταλλάξουν στο σύστημα με αντάλλαγμα ένα ομόλογο που θα τους εξασφαλίζει οτι θα μπορούν να ξαναπρομηθευτούν τα νομίσματά τους σε μία μειωμένη τιμή στο μέλλον. Δηλαδή εάν η τιμή του stablecoin ανέβει ξανά πάνω από την τιμή του ενός

ευρώ ή δολλαρίου ανάλογα, το σύστημα θα δημιουργήσει επιπλέον νομίσματα και οι χρήστες που έχουν το ομόλογο, θα προμηθευτούν τα νομίσματα σε μειωμένη τιμή.

Υπάρχει ένα σκεπτικισμός όσον αφορά τη μέθοδο αυτή καθώς αυτή εξαρτάται από την εμπιστοσύνη και αφήνει ανοιχτό το ενδεχόμενο πανικού. Ο πανικός μπορεί εξαιρετικά γρήγορα να μειώσει ανεπανόρθωτα την τιμή του νομίσματος. Για παράδειγμα, τι θα γινότανε εάν το σύστημα χρειαζόταν να μειώσει την τιμή των stablecoins σε κυκλοφορία ώστε να εξισορροπήσει την τιμή και δεν υπήρχαν αρκετοί χρήστες πρόθυμοι να συμμετάσχουν στο μελλοντικό ομόλογο; Ή τι θα γινόταν εάν ενα stablecoin ήταν τόσο δημοφιλές (πολλοί χρήστες) ώστε η οργάνωση μίας επαναγοράς έπαιρνε μέρες;

Τα παραπάνω σενάρια μπορούν δυνητικά να δημιουργήσουν αστάθεια στην αξία ενός stablecoin. Η αβεβαιότητα αυτή θα ενίσχυε την δημόσια ανησυχία, τις φήμες και φυσικά τον πανικό. Αυτό θα είχε σαν αποτέλεσμα την δημιουργία ενός φαινομένου ντόμινο, οδηγώντας έτσι τους χρήστες σε μαζικές πωλήσεις με σκοπό την ελαχιστοποίηση των απωλειών τους. Έτσι θα υπήρχε μία ανατροφοδότηση του φαινομένου με αποτέλεσμα την συντριβή της αξίας του stablecoin.

Σε αυτή την κατηγορία ανήκουν τα stablecoins **Karbo, Terra** και άλλα.

10.3 ELEMENT ZERO platform

Στην τρίτη μέθοδο, ανήκει η πλατφόρμα **ELEMENT ZERO** χωρίς όμως, κατά τη γνώμη μας τα μειονεκτήματα, των με αλγοριθμική προσέγγιση stablecoins. Η πλατφόρμα αυτή δίνει την δυνατότητα σε εταιρείες, οργανισμούς είτε σε μεμονωμένα άτομα να δημιουργήσουν το δικό τους stablecoin, βασισμένο σε μία νέα αλγοριθμική μεθοδολογία ευστάθειας που κατ' αρχήν εξαφανίζει πλήρως την πιθανότητα μεταβλητότητας της τιμής του νομίσματος.

Το Element Zero προσπαθεί να δώσει λύση στο πρόβλημα της απώλειας αγοραστικής δύναμης και του πληθωρισμού καθώς και στις βίαιες μεταβολές των τιμών στην αγορά των stablecoins.

Θεωρητικά, κάθε EZcoin (Element Zero stablecoin) θα έχει ονομαστική αξία 100 δολλαρίων ΗΠΑ και θα παραμένει αμετάβλητο ως προς την αγοραστική αξία αυτών και μετά από 10, 20 ή και 30 χρόνια γιατί ο αλγόριθμός που το διέπει, το προστατεύει από τον πληθωρισμό και τις βίαιες μεταβολές του δολλαρίου. Αυτό θα επιτυγχάνεται μέσω ενός μηχανισμού μηχανικής μάθησης ο οποίος θα εξασφαλίζει ότι θα υπάρχουν αρκετά κεφάλαια στο αποθεματικό ρευστοποίησης του νομίσματος (liquidity reserve).

Το πρωτόκολλο του EZ είναι έτσι σχεδιασμένο ώστε να αυξάνει την τιμή του νομίσματος με τέτοιο τρόπο ώστε να εξισορροπεί την αγοραστική του αξία σε σχέση με τον πληθωρισμό. Αυτό επιτυγχάνεται ακολουθώντας αυτόματα τον δείκτη τιμών καταναλωτή καθώς και τον δείκτη τιμών ιδιωτικής κατανάλωσης, αναλόγως με το ποιός εκ των δύο είναι μεγαλύτερος.

Για να εξασφαλιστεί ότι η αξία του EZ λαμβάνει υπ' όψιν της τον πληθωρισμό, κάθε φορά που το σύστημα θα παράγει νέα νομίσματα, αυτά θα βασίζονται στην νέα τιμή του νομίσματος η οποία θα περιέχει μέσα της το αντίστοιχο ποσοστό του πληθωρισμού. Για παράδειγμα, εάν το νόμισμα αξίζει σήμερα 100 δολλάρια ΗΠΑ και ένα χρόνο μετά το σύστημα παράξει νέα νομίσματα στην τιμή των 102 δολλάρίων, οι χρήστες που θα θέλουν να εξαργυρώσουν τα νομίσματά τους θα λάβουν πίσω 102 δολλάρια ανα νόμισμα.

Για να εξασφαλιστεί ότι τα EZ δεν θα χάσουν την αξία τους λόγω της όποιας μεταβλητότητας του δολλάρίου ΗΠΑ, το σύστημα θα μετράει τον δείκτη SDR (Special Drawings Reserve) του Διεθνούς Νομισματικού Ταμείου και θα αναπροσαρμόζεται αυτόματα.

Το πρωτόκολλο αλγοριθμικής ευστάθειας που προτείνεται, δεν χρησιμοποιεί την σύνδεση του νομίσματος με FIAT χρήμα, αλλά βασίζεται σε ένα αλγόριθμο έξυπνων συμβολαίων που για πρώτη φάση είναι σχεδιασμένος έτσι ώστε να εξαλοίφει εντελώς την πιθανότητα βίαιης μεταβολής του νομίσματος. Σε αντίθεση με τα άλλα κρυπτονομίσματα που επεξεργάζονται μονόδρομες συναλλαγές, το πρωτόκολλο αυτό είναι σχεδιασμένο να επεξεργάζεται αμφίδρομες συναλλαγές. Έτσι λοιπόν, κατά την εκτέλεση μίας συναλλαγής, ένας αποστολέας μπορεί να στείλει μία ποσότητα EZ σε κάποιον παραλήπτη αλλά ο παραλήπτης πρέπει να στείλει στον αποστολέα είτε κρυπτονόμισμα είτε απόδειξη ή τιμολόγιο παροχής υπηρεσιών ή πώλησης αγαθών ίσης αξίας με την ονομαστική αξία των EZ. Εάν η αξία των συναλλαγών διαφέρει, τότε επεμβαίνει αυτόματα το έξυπνο συμβόλαιο και εξισορροπεί την ονομαστική αξία μεταξύ των δύο μερών, στέλνοντας την διαφορά σε όποιο από τα δύο μέρη την δικαιούται. Ο αμφίδρομος αυτός τρόπος λειτουργίας του έξυπνου συμβολαίου εξασφαλίζει οτι το EZ δεν μπορεί να δεχθεί κερδοσκοπική πίεση, αφού η σταθερή του αξία επιβάλλεται από το σύστημα.

Για παράδειγμα, ένας χρήστης Α πληρώνει 80 δολλάρια χρησιμοποιώντας κάποιο κρυπτονόμισμα όπως το Bitcoin ή το ETH, για να αγοράσει από κάποιο χρήστη Β, EZ νομίσματα, ονομαστικής αξίας 100 δολλαρίων. Το έξυπνο συμβόλαιο αυτόματα θα στείλει στον χρήστη Α μόνο το 80% των EZ νομισμάτων. Τα εναπομείναντα 20 θα επιστραφούν στον χρήστη Β αυτόματα.

Τα έξυπνα συμβόλαια θα ενεργήσουν με τον ίδιο τρόπο όταν η συναλλαγή αφορά προιόντα ή υπηρεσίες. Τα τιμολόγια ή οι αποδείξεις θα πρέπει να είναι ίσης αξίας με την ονομα-

στική αξία των EZ νομισμάτων. Διαφορετικά, αυτόματα το έξυπνο συμβόλαιο θα φροντίσει να ταιριάζουν.

Ένα επιπλέον πλεονέκτημα που προσφέρει η προσέγγιση αυτή, είναι ότι τα EZ προσφέρουν υπηρεσίες μεσεγγύησης και διαιτησίας. Το έξυπνο συμβόλαιο θα δίνει την δυνατότητα να μπορεί να δεσμευτεί το ποσό της αγοράς για κάποιο διάστημα που θα ορίζει ο χρήστης και θα το απελευθερώνει μετά την διαβεβαίωση από κάποιο τρίτο μέλος (πχ μία εταιρεία μεταφορών) ότι το προιόν παραδόθηκε στον παραλήπτη. Σε περιπτώσεις που ο αγοραστής υποστηρίξει ότι το προιόν δεν έχει τις προδιαγραφές που είχαν συμφωνηθεί, το έξυπνο συμβόλαιο θα συνεχίσει να δεσμεύει το ποσό, έως ότου μία επιτροπή αποτελούμενη από χρήστες που θα λειτουργεί σαν σώμα ενόρκων και έναντι κάποιας αμοιβής, αποφασίσει βάσει στοιχείων, για το ποιός από τα δύο συμβαλλόμενα μέρη έχει δίκιο. Η απόφαση θα λαμβάνεται πλειοψηφικά και κατόπιν το ποσό θα απελευθερώνεται από το έξυπνο συμβόλαιο στον δικαιούχο. Για να εξασφαλιστεί ότι το σύστημα αυτό θα είναι το δικαιότερο δυνατόν, η αμοιβή θα δίνεται μόνο στα μελη που η γνώμη τους ήταν σύμφωνη με την πλειοψηφία. Προφανώς η ψηφοφορία θα είναι ανώνυμη και απόρρητη. Με τον καιρό, κάθε χρήστης που θα προσφέρει τις υπηρεσίες του ως ένορκος, θα δημιουργήσει ένα ιστορικό με τις αποφάσεις του. Εάν το ιστορικό του δείχνει ότι έκανε περισσότερες επιλογές σύμφωνα με την πλειοψηφία τότε θα αυξάνονται οι πιθανότητες επιλογής του σε καινούργια σώματα ενόρκων που θα δημιουργούνται.

Ένα άλλο σημαντικό πλεονέκτημα είναι ότι το σύστημα έξυπνων συμβολαίων θα είναι πολύ απλό, δίνοντας έτσι στον οποιοδήποτε χρήστη να δημιουργήσει το δικό του έξυπνο συμβόλαιο σε ελάχιστο χρόνο.

Ο τρόπος με τον οποίο η πλατφόρμα Element Zero θα εξασφαλίσει την ρευστότητα του νομίσματος σε περιόδους οικονομικής κρίσης στις αγορές των κρυπτονομισμάτων, είναι η αγορά ομολόγων ακίνητης περιουσίας η οποία μετά την οικονομική κρίση του 2009 είναι αυτή τη στιγμή η πιο σταθερή αγορά μετά την αγορά κρατικών ομολόγων και από τις πιο ελεγχόμενες κρατικά αγορές στις ΗΠΑ.

Το Element Zero, εκτός από τους αλγοριθμικούς μηχανισμούς στήριξης της τιμής του, βασίζεται επίσης και σε δύο αποθεματικά. Το αποθεματικό ρευστότητας (liquidity reserve) το οποίο θα λειτουργεί ως μία δεξαμενή κεφαλαίων ικανή να υποστηρίζει τις τρέχουσες συναλλαγές και το αποθεματικό αξιών (holding reserve) το οποίο θα αποτελείται από επενδύσεις σε επενδυτικά αγαθά μακροπρόθεσμης αξίας και απόδοσης, με ικανοποιητικά σταθερό χαρακτήρα στην μεταβλητότητα των τιμών, όπως η αγορά ακινήτων. Τα δύο αποθεματικά θα αλληλοδανείζονται κεφάλαια αυτόματα, προκειμένου να εξασφαλίζεται συνεχώς η ευστάθεια του νομίσματος.

Οποιαδήποτε κυβέρνηση, οικονομικός οργανισμός ή εταιρεία μπορεί να εκδόσει κάτω από την σκέπη της πλατφόρμας Element Zero, το δικό της stablecoin.

Το EZ επίσης είναι σχεδιασμένο έτσι ώστε να επιτυγχάνεται πλήρης αποκεντρωμένος έλεγχος. Σε περιπτώσεις που θα χρειαστεί να ληφθούν όχι ιδιαίτερα σημαντικές αποφάσεις αυτές θα λαμβάνονται από το συμβούλιο των διευθυντών στο οποίο θα μετέχουν οι εκδότες των EZ νομισμάτων, όπως κυβερνήσεις, χρηματοοικονομικοί οργανισμοί και άλλες εταιρείες, ενώ στην περίπτωση που πρέπει να ληφθούν σημαντικές αλλαγές όπως αλλαγές στο πρωτόκολλο και άλλα, τότε θα λαμβάνουν μέρος όλοι οι χρήστες τους συστήματος.

10.3.1 Η άποψη της παγκόσμιας οικονομικής κοινότητας

Σύμφωνα με το τελευταίο Σημείωμα του Συμβουλίου Χρηματοπιστωτικής Σταθερότητας (‘FSB’) [76] και την έκθεση της Ομάδας Έργου των ‘G-7’ [77] για τα “stablecoins” στις 24 Οκτωβρίου 2019 αναγνωρίζεται ο ρόλος και η ταχύτατη εξάπλωση των Stablecoins και προτείνονται μέτρα εφαρμογής ρυθμιστικών κανόνων για την αντιμετώπιση τυχόν οικονομικών κινδύνων που μπορεί να προκύψουν από τη συνεχομένη ανάπτυξη αυτών, όσο και σκέψεις για τρόπους υιοθέτησής των από τους χρηματοπιστωτικούς οργανισμούς παγκοσμίως.

Κεφάλαιο 11

Περαιτέρω Έρευνα

Εισαγωγή

Όπως αναφέραμε σε προηγούμενα κεφάλαια, στην blockchain κάθε block περιέχει την κρυπτογραφική σύνοψη του προηγούμενου, τη χρονοσήμανση και τα δεδομένα των συναλλαγών που αναπαρίστανται από τις συνόψεις που προκύπτουν με την χρήση των Merkel trees. Με αυτόν τον τρόπο καθίσταται σχεδόν αδύνατο να παραποιηθούν τα περιεχόμενα των blocks. Καθώς όμως τα δεδομένα των συναλλαγών είναι δημόσια δημοσιευμένα στην blockchain, ένα επιτιθέμενος μπορεί να έχει στη διάθεσή του όλες τις πληροφορίες των συναλλαγών, καθιστώντας έτσι το απόρρητο του συναλλασόμενου ευάλωτο. Επιπλέον λόγω του ορίου του 1M-byte αποθήκευσης στην περίπτωση του Bitcoin καθώς και του μικρού αριθμού συναλλαγών ανα δευτερόλεπτο, περίπου 7 συναλλαγές ανα δευτερόλεπτο, αυτό οδηγεί σε προβλήματος ταχύτητας του δικτύου, περισσότερο χρόνο επιβεβαίωσης των συναλλαγών κτλ. Για την αντιμετώπιση αυτού του προβλήματος έχουν γίνει διάφορες προτάσεις, πολλές εκ των οποίων έχουν υλοποιηθεί σε διάφορες blockchain χωρίς όμως να αντιμετωπίζονται πλήρως τα προβλήματα. Ο Yuan et al. [78] πρότεινε ένα σχήμα προστασίας του απορρήτου για τις blockchains, βασισμένο σε συγκεντρωτικές υπογραφές (aggregate signatures) [79], [80], το οποίο συγκεντρώνει πολλαπλά υπογεγραμμένα μηνύματα σε μία υπογραφή, μειώνοντας έτσι τον αποθηκευτικό χώρο που απαιτείται για τις υπογραφές, το εύρος ζώνης του δικτύου καθώς και το φορτίο λόγω επαλήθευσης των υπογραφών. Έπειδή όμως το σχήμα που προτείνεται βασίζεται σε κατασκευή μέσω διγραμμικών απεικονίσεων [81], [82], [83], [84], δημιουργείται πρόβλημα στην υπολογιστική αποδοτικότητα.

Παράλληλες Συγκεντρωτικές υπογραφές (Parallel Aggregate signatures)

Η συγκεντρωτική υπογραφή (Aggregate Signature) είναι μία παραλλαγή ψηφιακής υπογραφής η οποία έχει συγκεντρωτικά χαρακτηριστικά.

Η συγκεντρωτική υπογραφή παράγεται από μία τετράδα τεσσάρων αλγορίθμων: *KeyGen, Sign, Combine και Verify*. Έστω n ο αριθμός χρηστών με $u_i \in U(1 \leq i \leq n)$, όπου U είναι το σύνολο των χρηστών και n το πλήθος των μηνυμάτων με $m_i \in M(1 \leq i \leq n)$, όπου M είναι το σύνολο των μηνυμάτων. Οι αλγόριθμοι *KeyGen* και *Sign* είναι οι ίδιοι που χρησιμοποιούνται σε κάθε σχήμα ψηφιακής υπογραφής.

Ο αλγόριθμος *Keygen* παράγει τα ζεύγη ιδιωτικών και δημόσιων κλειδιών ενώ ο *Sign* παράγει μία ψηφιακή υπογραφή για κάθε χρήστη u_i.

Ο αλγόριθμος *Combine* δέχεται σαν είσοδο ένα διάνυσμα n τριάδων (pk_i, m_i, σ_i), όπου $(pk_i$ το ιδιωτικό κλειδί του χρήστη u_i, m_i το αντίστοιχο μήνυμα και σ_i η αντίστοιχη ψηφιακή υπογραφή του και παράγει μία μοναδική υπογραφή σ που λειτουργεί σαν υπογραφή για όλα τα μηνύματα.Η υπογραφή σ λέγεται **(Aggregate Signature)** και το μήκος της είναι ίσο με το μήκος μίας απλής ψηφιακής υπογραφής.

Ο αλγόριθμος *Verify* δέχεται σαν είσοδο ένα διάνυσμα n δυάδων (pk_i, m_i) και την συγκεντρωτική υπογραφή σ. Το αποτέλεσμα της εξόδου είναι "έγκυρο (valid)" μόνο αν η σ παράχθηκε από την συγκέντρωση n έγκυρων απλών υπογραφών.

Δοσμένης της συγκεντρωτικής υπογραφής, το αρχικό μήνυμα m_i το οποίο χρησιμοποιήθηκε για την παραγωγή της ταυτότητας u_i του συγκεντρωτικού υπογράφοντα (aggregate signer) καθώς και της υπογραφής του σ, ο επαληθεύων (verifier) μπορεί να επιβεβαιώσει ότι ο χρήστης u_i έχει υπογράψει το μήνυμα m_i.

Η διαδικασία της συγκέντρωσης μπορεί να γίνει από τον οποιονδήποτε χωρίς ν απαιτούνται επιπλέον μυστικά κλειδιά.

Σειριακές συγκεντρωτικές υπογραφές (sequential aggregate signatures)

Το παραπάνω σχήμα συγκεντρωτικών υπογραφών λέγεται και "παράλληλες συγκεντρωτικές υπογραφές (parallel aggregate signatures)". Υπάρχει και μία άλλη μορφή που λέγεται "σειριακές συγκεντρωτικές υπογραφές" [85], [86]. Σε αυτές ακολουθείται η εξής διαδικασία:

Ο χρήστης u_1 με την χρήση του αλγόριθμου *Combine* υπογράφει το μήνυμα m_1 με την υπογραφή του σ_1 και παράγει την μοναδική συγκεντρωτική υπογραφή Σ_1. Ο χρήστης u_2 χρησιμοποιεί την υπογραφή Σ_1 μαζί με το μήνυμα του m_2 και παράγει την συγκεντρωτική υπογραφή Σ_2 κτλ. Η τελική υπογραφή Σ παράγεται από τον χρήστη n ο οποίος συνδέει το μήνυμα του m_n με την υπογραφή σ_{n-1}. Η τελική υπογραφή θα έχει το ίδιο μήκος με μία απλή υπογραφή σε κάποιο μήνυμα. Η επαλήθευση της τελικής σειριακή συγκεντρωτικής υπογραφής γίνεται όπως και στην περίπτωση των παράλληλων συγκεντρωτικών υπογραφών. Στον επαληθευτή (verifier) δίνεται μόνο η τελική υπογραφή μαζί με τα μηνύματα και

δημόσια κλειδιά. Οι μερικώς συγκεντρωτικές υπογραφές που περνάνε απο χρήστη σε χρήστη, είναι άγνωστες στον τελικό επαληθευτή.

Οι σειριακές συγκεντρωτικές υπογραφές, επιτυγχάνουν το ίδιο επίπεδο ασφάλειας με τις παράλληλες, αλλά απαιτούν την συγκέντρωση των απλών υπογραφών με προκαθορισμένο τρόπο επιτυγχάνοντας έτσι αποτελεσματικότερη εφαρμογή.

Μελλοντική Έρευνα

Με βάση όλα τα παραπάνω προτείνεται για μελλοντική έρευνα η βελτιστοποίηση υπαρχόντων blockchain και bitcoin συστημάτων με τη χρήση σύγχρονων δέντρων κατακερματισμού [16], [17], συστημάτων μηδενικής γνώσης [12], [13] και καινοτόμων μεθόδων υπολογισμού αλγορίθμων δημόσιας κλείδας [59], [60] για εφαρμογές σε πραγματικό χρόνο και με υπολογιστές με περιορισμένους υπολογιστικούς πόρους.

Επίσης προτείνεται για μελλοντική έρευνα η κατασκευή ενός νέου σχήματος ψηφιακής υπογραφής βασισμένο στις **σειριακές συγκεντρωτικές υπογραφές** [87], τέτοιο ώστε να μπορεί να εφαρμοστεί στις συναλλαγές που εκτελούνται στην blockchain, με στόχο την μεγιστοποίηση του αριθμού των πληροφοριών που μπορούν να αποθηκευθούν σε κάθε block. Προφανώς ένα τέτοιο σχήμα θα επιτρέψει μία πιο συμπαγή αναπαράσταση των υπογραφών μειώνοντας έτσι τον όγκο των πληροφοριών σε όλο το δίκτυο της blockchain και θα αυξήσει σημαντικά την ταχύτητα επαλήθευσης των συναλλαγών. Ο κύριος σκοπός ενός τέτοιου σχήματος θα είναι να συγκεντρωθούν οι υπογραφές όλων των συναλλαγών μέσα σε κάθε block της blockchain ενώ παράλληλα θα επιτευχθεί και η ανωνυμία των συναλλασσομένων. Εάν μία τέτοια σειριακή συγκεντρωτική υπογραφή είχε την επιπλέον ιδιότητα μικροτέρου μήκους δημοσίου κλειδιού αυτό θα βελτίωνε ακόμα περισσότερο την ταχύτητα των συναλλαγών στην blockchain.

Βιβλιογραφία

[1] Δ. Βάρσος, Δ Δεριζιώτης, Γ. Εμμανουήλ, Μ. Μαλιάκας, and Ο. Ταλλελη. *Μία Εισαγωγή στην Άλγεβρα*. Εκδόσεις Σοφία, 2005.

[2] John B Fraleigh. *First Course in Abstract Algebra, A: Pearson New International Edition*. Pearson Higher Ed, 2013.

[3] Andreas Enge. *Elliptic curves and their applications to cryptography: an introduction*. Springer Science & Business Media, 2012.

[4] Alasdair McAndrew. *Introduction to Cryptography with open-source software*. CRC Press, 2016.

[5] William Fulton. Algebraic curves: an introduction to algebraic geometry. 2008. *Author's version*, 258.

[6] Νικόλαος Μπάρδης. Σημειώσεις μαθήματος: Κρυπτογραφία και Συστήματα Ασφάλειας Πληροφοριών. *ΠΜΣ Τμήμα Μαθηματικών ΕΚΠΑ, 2017.*

[7] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[8] C Kerry and P Gallagher. Fips pub 186-4: Digital signature standard (dss). *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. National Institute of Standards und Technology*, 2013.

[9] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[10] Neal Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. In *Annual International Cryptology Conference*, pages 327–337. Springer, 1998.

[11] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[12] Peter Stavroulakis, Oleksandr P Markovskyi, Nikolaos G Bardis, and Nikolaos Doukas. Efficient zero—knowledge identification based on one way boolean transformations. In *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, pages 275–280. IEEE, 2011.

[13] Nikolaos G Bardis, Nikolaos Doukas, and Oleksandr P Markovskyi. Zero-knowledge identification method based on block ciphers. In *2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)*, pages 307–311. IEEE, 2017.

[14] Kristian Bjoernsen. Koblitz curves and its practical uses in bitcoin security. *order (ε (GF (2k)*, 2(1):7, 2009.

[15] Alan G Konheim. *Hashing in computer science: Fifty years of slicing and dicing*. John Wiley & Sons, 2010.

[16] Nikolaos G Bardis, Nikolaos Doukas, and Oleksandr P Markovskyi. Hash addressing of the quasi-permanent key arrays in multilevel memory. *Journal of Applied Mathematics and Bioinformatics*, 3(4):91, 2013.

[17] Nikolaos Doukas, Oleksandr P Markovskyi, and Nikolaos G Bardis. Hash function design for cloud storage data auditing. *Theoretical Computer Science*, 800:42–51, 2019.

[18] Fips pub 180-4. secure hash standard (shs). `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`.

[19] Descriptions of sha-256, sha-384, and sha-512. `http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf`.

[20] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. Ripemd-160: A strengthened version of ripemd. In *International Workshop on Fast Software Encryption*, pages 71–82. Springer, 1996.

[21] Bart Preneel, Antoon Bosselaers, and Hans Dobbertin. The cryptographic hash function ripemd-160, 1997.

[22] Gaoli Wang, Yanzhao Shen, and Fukang Liu. Cryptanalysis of 48-step ripemd-160. *IACR Transactions on Symmetric Cryptology*, pages 177–202, 2017.

[23] Ronald L Rivest. Md4 message digest algorithm. 1990.

[24] Burt Kaliski and Matt Robshaw. Message authentication with md5. *CryptoBytes, Sping*, 1995.

[25] R. Rivest. The md5 message-digest algorithm. *MIT Laboratory for Computer Science and RSA Data Security Inc.*, 1992.

[26] Thai Duong and Juliano Rizzo. Flickr's api signature forgery vulnerability. `https://vnhacker.blogspot.com/2009/09/flickrs-apisignature-forgery.html`.

[27] Ron Bowes. Everything you need to know about hash length extension attacks. `https://blog.skullsecurity.org/2012/everything-you-need-to-knowabout-hash-length-extension-attacks`.

[28] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. Cryptography engineering. *Design Princi*, 2010.

[29] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[30] Wei Dai. b-money. `https://nakamotoinstitute.org/b-money/`, 1998.

[31] Adam Back et al. Hashcash-a denial of service counter-measure. 2002.

[32] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[33] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[34] Andreas M Antonopoulos. *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.", 2017.

[35] Imran Bashir. *Mastering blockchain*. Packt Publishing Ltd, 2017.

[36] Imran Bashir. *Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd, 2018.

[37] Ralph C Merkle. A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques*, pages 369–378. Springer, 1987.

[38] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[39] litecoin: The cryptocurrency for payments. `https://litecoin.org`.

[40] investopedia: Litecoin. `https://www.investopedia.com/terms/l/litecoin.asp`.

[41] ethereum: Blockchain. `https://www.ethereum.org/`.

[42] investopedia: Etherium. `https://www.investopedia.com/terms/e/ethereum.asp`.

[43] Yannis Bakos and Hanna Halaburda. The role of cryptographic tokens and icos in fostering platform adoption. 2019.

[44] Deloitte: The dao attack. `https://www2.deloitte.com/ie/en/pages/technology/articles/DAO-Attack-Analysis.html`.

[45] coindesk: Understanding the dao attack. `ttps://www.coindesk.com/understanding-dao-hack-journalists`.

[46] zcash :zcash is a privacy-protecting, digital currency built on strong science. `https://z.cash/`.

[47] investopedia: What is zcash? `https://www.investopedia.com/tech/what-zcash/`.

[48] zcash: What are zk-snarks? `https://z.cash/technology/zksnarks/`.

[49] dash : Your money, your way... `https://www.dash.org/`.

[50] dash : Privatesend. `https://docs.dash.org/en/latest/wallets/dashcore/privatesend-instantsend.htm`.

[51] Dash : Instantsend. `https://docs.dash.org/en/latest/introduction/features.html`.

[52] wikipedia: Ripple(payment protocol). https://en.wikipedia.org/wiki/Ripple.

[53] Monero: Private digital currency. https://www.getmonero.org/.

[54] Nicolas van Saberhagen. Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf, 1985.

[55] Bitcoincash: Peer-to-peer electronic cash. https://www.bitcoincash.org/.

[56] Neo: An open network for the smart economy. https://neo.org/.

[57] Cardano: Home of the ada cryptocurrency and technological platform. https://www.cardano.org/en/home/.

[58] Eos: Blockchain software architecture. https://eos.io/.

[59] Nikolaos G Bardis, Nikolaos Doukas, Vyacheslav Kharchenko, Vladimir Sklyar, and Svitlana Yaremchuk. Approaches and techniques to improve iot dependability. *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*, page 307, 2018.

[60] Nikolaos Bardis. Secure, green implementation of modular arithmetic operations for iot and cloud applications. In *Green IT Engineering: Components, Networks and Systems Implementation*, pages 43–64. Springer, 2017.

[61] Trusting the transaction of things: Iot and blockchain intersect. https://www.ibm.com/downloads/cas/E6LEKG31.

[62] Clement Chan Zheng Wei and Chuah Chai Wen. Blockchain-based electronic voting protocol. *JOIV: International Journal on Informatics Visualization*, 2(4-2):336–341, 2018.

[63] Bin Yu, Joseph K Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. Platform-independent secure blockchain-based voting system. In *International Conference on Information Security*, pages 369–386. Springer, 2018.

[64] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.

[65] Raghavendra Ganji and BN Yatish. Electronic voting system using blockchain. 2018.

[66] Mahmoud Al-Rawy and Atilla Elci. A design for blockchain-based digital voting system. In *The 2018 International Conference on Digital Science*, pages 397–407. Springer, 2018.

[67] Friðrik Þ Hjálmarsson, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. Blockchain-based e-voting system. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986. IEEE, 2018.

[68] Montes D Juan, Rincón P Andrés, Páez M Rafael, Ramírez E Gustavo, and Pérez C Manuel. A model for national electronic identity document and authentication mechanism based on blockchain. *Int. J. Model. Optim*, 8(3):160–165, 2018.

[69] K Wagner, B Némethi, E Renieris, P Lang, E Brunet, and E Holst. Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead. *Identity Working Group of the German Blockchain Association (https://jolocom. io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf*, 2018.

[70] Cornelius C Agbo, Qusay H Mahmoud, and J Mikael Eklund. Blockchain technology in healthcare: a systematic review. In *Healthcare*, volume 7, page 56. Multidisciplinary Digital Publishing Institute, 2019.

[71] Anuraag A Vazirani, Odhran O'Donoghue, David Brindley, and Edward Meinert. Implementing blockchains for efficient health care: Systematic review. *Journal of medical Internet research*, 21(2):e12439, 2019.

[72] Yu Rang Park, Eunsol Lee, Wonjun Na, Sungjun Park, Yura Lee, and Jae-Ho Lee. Is blockchain technology suitable for managing personal health records? mixed-methods study to test feasibility. *Journal of medical Internet research*, 21(2):e12533, 2019.

[73] Edward Meinert, Abrar Alturkistani, Kimberley A Foley, Tasnime Osama, Josip Car, Azeem Majeed, Michelle Van Velthoven, Glenn Wells, and David Brindley. Blockchain implementation in health care: Protocol for a systematic review. *JMIR research protocols*, 8(2):e10994, 2019.

[74] O Williams-Grut. Estonia is using the technology behind bitcoin to secure 1 million health records. business insider inc, 2016.

[75] Kannan Subbiah, Benno Ferrarini, Julie Maupin, Marthe Hinojales, Rahul Guhathakurta, S. Kulshrestha, and Danika Wright. The age of blockchain: A collection of articles, 2018.

[76] Financial Stability Board. Regulatory issues of stablecoins, 2019.

[77] G7 Working Group on Stablecoins. Investigating the impact of global stablecoins, 2019.

[78] Yumin Yuan, Qian Zhan, and Hua Huang. Efficient unrestricted identity-based aggregate signature scheme. *PloS one*, 9(10):e110100, 2014.

[79] Henk CA Van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[80] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 416–432. Springer, 2003.

[81] Alfred Menezes. An introduction to pairing-based cryptography. *Recent trends in cryptography*, 477:47–65, 2009.

[82] Tatsuaki Okamoto. Cryptography based on bilinear maps. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 35–50. Springer, 2006.

[83] Noel Michael McCullagh. *Crytographic applications of bilinear maps*. PhD thesis, Dublin City University, 2005.

[84] Mehmet Sabir Kiraz and Osmanbey Uzunkol. Still wrong use of pairings in cryptography. *arXiv preprint arXiv:1603.02826*, 2016.

[85] Xuhua Zhou, Junzuo Lai, Shengli Liu, and Kefei Chen. Sequential aggregate signatures and multisignatures in the plain public key model. *Chinese Journal of Electronics*, 24(2):338–342, 2015.

[86] Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham. Sequential aggregate signatures from trapdoor permutations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 74–90. Springer, 2004.

[87] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures and multisignatures without random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 465–485. Springer, 2006.