ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κρυπτονομίσματα
Τεχνικά χαρακτηριστικά και συγκριτική μελέτη

Γεώργιος Ι. Τραχανάς
Ιωάννα Κ. Βρεττού

Επιβλέπων: **Λάζαρος Μεράκος,** Καθηγητής

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2019

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κρυπτονομίσματα
Τεχνικά χαρακτηριστικά και συγκριτική μελέτη

Γεώργιος Ι. Τραχανάς

Α.Μ.: 1115201300178

Ιωάννα Κ. Βρεττού

Α.Μ.: 1115200700102

ΕΠΙΒΛΕΠΩΝ: **Λάζαρος Μεράκος,** Καθηγητής

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία παρουσιάζει τα τεχνικά χαρακτηριστικά επιλεγμένων κρυπτονομισμάτων και το μηχανισμό με τον οποίο αυτά λειτουργούν. Η εργασία μας επικεντρώθηκε στα εξής κρυπτονομίσματα: Bitcoin, Ethereum, Ripple, Dash, Namecoin και Libra. Σκοπός της εργασίας είναι να προχωρήσει σε μία αξιολόγηση και συγκριτική μελέτη των παραπάνω κρυπτονομισμάτων με βάση ένα σύνολο κριτηρίων της επιλογής μας, όπως την ανάγκη δημιουργίας τους, τον τρόπο με τον οποίο λειτουργεί το blockchain του καθενός, πως εισέρχονται νέα νομισμάτα στο δίκτυο, τον τρόπο με τον οποίο πραγματοποιούνται και πιστοποιούνται οι συναλλαγές, τους μηχανισμούς εξασφάλισης συναίνεσης, το τρέχον market capitalization και αν εξυπηρετούν smart contracts. Για το σκοπό της εργασίας έγινε λεπτομερής έρευνα και αξιοποιήθηκαν επιστημονικά άρθρα, τα whitepapers των εν λόγω νομισμάτων, καθώς και επιστημονικές μελέτες που έχουν πραγματοποιηθεί όσον αφορά τον τρόπο λειτουργίας τους.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Κρυπτονομίσματα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Blockchain, bitcoin, peer-to-peer σύστημα, ledger, mining, συναλλαγή, μηχανισμοί consensus

ABSTRACT

This BSc Thesis presents the technical characteristics of selected cryptocurrencies and how they are being used. Our research focused on the specific coins and altcoins: Bitcoin, Ethereum, Ripple, Dash, Namecoin and Libra. Our purpose is to evaluate and compare those coins, based on a set of criteria that we chose. Why they were invented and what was the purpose? How does their blockchain work and how new blocks are being added in the chain? How new coins are being minted? In which way transactions are performed and how they are validated? How consensus works? What is the current market capitalizaton and if they support smart contracts? In order to make this possible we utilized a lot of scientific articles, the whitepapers of the coins and scientific studies on the way that cryptocurencies are perfomed.

SUBJECT AREA: Cryptocurrencies

KEYWORDS: Blockchain, bitcoin, peer-to-peer system, ledger, mining, transaction, consensus mechanisms

Η εργασία αυτή αφιερώνεται στο σχήμα, στη Ρόζα και στο kung-fu panda.

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας πτυχιακής εργασίας, θα θέλαμε να ευχαριστήσουμε το Διονύση Ξενάκη για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωση της.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα πτυχιακή εργασία με τίτλο **"Κρυπτονομίσματα – Τεχνικά χαρακτηριστικά και συγκριτική μελέτη"** εκπονήθηκε από τους συγγραφείς της στα πλαίσια της ολοκλήρωσης των προυποθέσεων για τη λήψη πτυχίου από το τμήμα της Πληροφορικής και Τηλεπικοινωνιών της Σχολής Θετικών Επιστημών του ΕΚΠΑ. Η εργασία αποτελεί συνιδιοκτησία της σχολής και των φοιτητών, ο καθένας από τους οποίους έχει δικαίωμα να την αναπαράγει και να τη χρησιμοποιεί ελεύθερα για διδακτικούς και ερευνητικούς σκοπούς, αναφέροντας σε κάθε περίπτωση τον τίτλο, τους συγγραφείς, το τμήμα όπου εκπονήθηκε η εργασία καθώς και τους επιβλέποντες.

1. ΕΙΣΑΓΩΓΗ

Το χρήμα είναι το βασικό εργαλείο για να συνεχίζει να λειτουργεί η σύγχρονη οικονομία. Εάν σταματούσαν να πραγματοποιούνται πληρωμές, το σύγχρονο οικονομικό σύστημα όπως το ξέρουμε, θα σταματούσε να λειτουργεί. Τα τελευταία χρόνια, που βιώνουμε μια έκρηξη ανάπτυξης της επιστήμης των υπολογιστών και του Διαδικτύου, η ανθρωπότητα έπρεπε να προσαρμοστεί στη σύγχρονη τεχνολογία και καινοτομία. Την ίδια πορεία ακολούθησε και το χρήμα. Παρατηρείται μία αλλαγή στο πως οι άνθρωποι θέλουν να διεξάγουν τις συναλλαγές τους και κατά συνέπεια υπήρξε μια μετατόπιση από τα συμβατικά νομίσματα, όπως το ευρώ και το δολάριο, σε νέες μορφές χρήματος. Έτσι εμφανίστηκαν τα κρυπτονομίσματα, τα οποία έδωσαν λύση στα ζητήματα που θέτουν οι σύγχρονες παγκοσμιοποιημένες και ψηφιακές οικονομίες. Τα κρυπτονομίσματα δίνουν τη δυνατότητα για συναλλαγές ασφαλείς, χωρίς λάθη, με ελάχιστο κόστος και χωρίς σπατάλη χρόνου.

Τα κρυπτονομίσματα είναι μια μορφή ψηφιακού χρηματικού προϊόντος, και διαχειρίζονται από ένα P2P δίκτυο, χωρίς να απαιτείται προηγούμενη σχέση ή εμπιστοσύνη μεταξύ προσώπων και χωρίς την ανάγκη εμπιστοσύνης του αντισυμβαλλομένου ή μιας κεντρικής έμπιστης αρχής ως ρυθμιστής. Ο σχεδιασμός του μηχανισμού των κρυπτονομισμάτων είναι ο παράγοντας που εγγυάται και εξασφαλίζει την ακεραιότητα και την εγκυρότητα των κινήσεων και των συναλλαγών.

Το βασικό χαρακτηριστικό για την εξέλιξη της αγοράς των κρυπτονομισμάτων ήταν η απελευθέρωση των πληρωμών από οποιονδήποτε ενδιάμεσο ή αξιόπιστο κεντρικό φορέα. Η εισαγωγή του Bitcoin το 2009 ήταν η πρώτη υλοποίηση της ιδέας ενός αποκεντρωμένου αξιόπιστου ψηφιακού νομίσματος. Στη φύση του ανοιχτού κώδικα(*open-source*) του Bitcoin, στηρίχθηκαν πολλά νομίσματα που εμφανίστηκαν τα επόμενα χρόνια. Από το 2014, έχουν αναπτυχθεί πάνω από 275 κρυπτονομίσματα που διαφέρουν μεταξύ τους όσον αφορά την υλοποίηση και το σχεδιασμό. Τη στιγμή που γράφεται αυτή η εργασία το πλήθος τους έχει φτάσει τα 3000 κρυπτονομίσματα, πολλά εκ των οποίων τυγχάνουν της ευρείας αποδοχής του κοινου και άλλα έχουν υποπέσει σε αχρηστία. Ωστόσο, μοιράζονται την ίδια αρχή τεχνικού σχεδιασμού, που έχει στο επίκεντρο της την κρυπτογραφία, για να εξασφαλίσουν εμπιστοσύνη στις αποκεντρωμένες συναλλαγές όπως συμβαίνει και στο Bitcoin.

Υπάρχουν 4 βασικά χαρακτηριστικά που μοιράζονται όλα τα κρυπτονομίσματα:

1. Όλα αποτελούν ένα ψηφιακό μέσο ανταλλαγών τα οποία χρησιμοποιούν μεθόδους κρυπτογραφίας για να πραγματοποιήσουν συναλλαγές. Αξιοποιούν μορφές και παραλλαγές της τεχνολογίας blockchain για να αποκτήσουν αποκέντρωση και προστασία από επιθέσεις
2. Η ποσότητα των νομισμάτων που θα κοπούν είναι σταθερή, σε αντίθεση με την αξία τους που είναι μεταβλητή
3. Βασίζονται όλα σε ένα peer-to-peer δίκτυο υπολογιστών (P2P), το οποίο φιλοξενεί συναλλαγές οποιουδήποτε είδους. Οι συναλλαγές παραγματοποιούνται με το ελάχιστο κόστος, δίνοντας τη δυνατότητα στους χρήστες να αποφεύγουν το μεγάλο κόστος που επιβάλλεται από τους παραδοσιακούς οικονομικούς οργανισμούς.

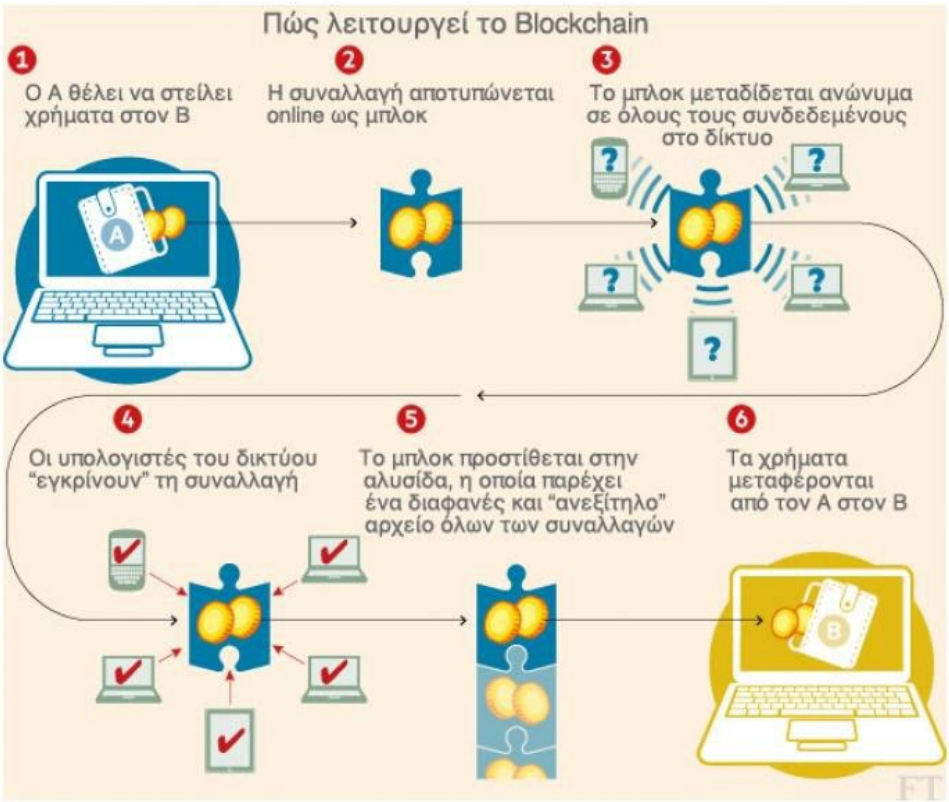
4. Δεν ελέγχονται από κάποια κεντρική αρχή, καθώς η αποκεντρωμένη φύση της τεχνολογίας blockchain προστατεύει τα κρυπτονομίσματα από τον έλεγχο από κυβερνήσεις και ενδιάμεσους φορείς, όπως τράπεζες.

Με βάση όλα τα παραπανω επιλέξαμε να μελετήσουμε μία σειρά κρυπτονομισμάτων, καθώς και το πρώτο alt-coin (Namecoin), τα οποία είτε έχουν ευρεία αποδοχή από τους χρήστες όπως το Bitcoin, το Ethereum, το Ripple ή το Dash, είτε είναι πολλά υποσχόμενα όπως το Libra. Ξεκινήσαμε με μία επισκόπηση των βασικών ορολογιών που χρησιμοποιούν τα κρυπτονομίσματα, ώστε να προχωρήσουμε στην λεπτομερή καταγραφή των τεχνικών χαρακτηριστικών που αυτά ακολουθούν και να καταλήξουμε στη μεταξύ τους σύγκριση.

1.1 Βασική ορολογία κρυπτονομισμάτων

1.1.1 Blockchain

Είναι ένα απλουστευμένο σύτημα που πιστοποιεί συναλλαγές και ανταλλαγές αξιών. Εντός του συστήματος του blockchain τόσο το συνάλλαγμα που χρησιμοποιείται όσο και τα στοιχεία που συναλλάσσονται και οι πληροφορίες των συναλλασσόμενων αποκτούν πλέον ψηφιακή μορφή. Η δομή και τα λειτουργικά στοιχεία αυτής της τεχνολογίας αλλάζουν ραγδαία τον τρόπο πραγματοποίησης των συναλλαγών. Πλέον δεν υπάρχει η ανάγκη για ενδιάμεσους φορείς, ενισχύεται η διαφάνεια, ενώ παράλληλα μειώνεται δραστικά το κόστος και ο χρόνος διεκπεραίωσης των διαδικασιών, και αντίστοιχα ο κίνδυνος μη ολοκλήρωσης τους.



Σχήμα 1: Τρόπος λειτουργίας Blockchain

Το Blockchain είναι ένα κατανεμημένο συναινετικό σύστημα που επιτρέπει την γρήγορη πιστοποίηση των συναλλαγών, και την ασφαλή διατήρηση και συντήρηση τους μέσω της κρυπτογραφίας, της υπολογιστικής ενέργειας και των ίδιων των χρηστών του δικτύου.

Το Blockchain είναι μια αλυσίδα από μπλοκ όπου το κάθε μπλοκ αποτελείται από μία σειρά ομαδοποιημένων συναλλαγών και των χαρακτηριστικών τους. Κάθε μπλοκ έχει ένα χαρακτηριστικό που ονομάζεται timestamp. Αποτελεί δηλαδή μια χρονολογική βάση δεδομένων των συναλλαγών οι οποίες καταγράφονται από ένα δίκτυο υπολογιστών. Το δίκτυο για να πιστοποιήσει την εγκυρότητα των συναλλαγών που προστίθενται στην αλυσίδα, στηρίζεται στο ιστορικό των προηγουμένων. Αυτό επιτυγχάνεται με την δημιουργία ενός hash για κάθε μπλοκ, δηλαδή ενός μαθηματικού αλγόριθμου που μετατρέπει την εισροή σε εκροή και παρουσιάζει την επεξεργασία των στοιχείων εισόδου σ' ένα μπλοκ. Η συνάρτηση κατακερματισμού (hash) στην ουσία είναι η υπογραφή ενός στοιχείου ή δεδομένου. Κάθε φορά που μια νέα συναλλαγή πιστοποιείται και προστίθεται στο δίκτυο, κάθε χρήστης του δικτύου αποκτά ένα νέο αντίγραφο αυτού. Με αυτό τον τρόπο δημιουργείται μια αλυσίδα συνδεδεμένων συναλλαγών, χρονικά συνδεδεμένων μεταξύ τους από το πρώτο μέχρι και το τελευταίο μπλοκ.

1.1.2 Nodes (κόμβοι)

Οι κόμβοι είναι το θεμέλιο του δικτύου των blockchain εφαρμογών, καθώς διασφαλίζουν τη λειτουργία και την επιβίωσή του. Ένας κόμβος μπορεί να είναι οποιαδήποτε ενεργή ηλεκτρονική συσκευή, συμπεριλαμβανομένου ενός υπολογιστή, ενός τηλεφώνου ή ακόμα και ενός εκτυπωτή, εφόσον είναι συνδεδεμένη στο διαδίκτυο και ως εκ τούτου έχει διεύθυνση IP. Ο ρόλος ενός κόμβου είναι να υποστηρίζει το δίκτυο διατηρώντας ένα αντίγραφο ενός blockchain και, σε ορισμένες περιπτώσεις, να επεξεργάζεται τις συναλλαγές. Κάθε κρυπτονόμισμα έχει τους δικούς του κόμβους.

Οι κόμβοι ως επιμέρους τμήματα του blockchain συνεισφέρουν τους υπολογιστικούς τους πόρους για την αποθήκευση και την επικύρωση των συναλλαγών τους. Η επεξεργασία αυτών των συναλλαγών μπορεί να απαιτεί μεγάλες ποσότητες υπολογιστικής και επεξεργαστικής ισχύος.

1.1.3 Transactions

Τα transactions είναι πακέτα δεδομένων τα οποία αποθηκεύουν πληροφορίες, οπως για παράδειγμα νομισματικές πληροφορίες για κρυπτονομίσματα ή για άλλες αποκεντρωμένες εφαρμογές. Η ακεραιότητα ενός transaction ελέγχεται από αλγοριθμικούς κανόνες και κρυπτογραφικές τεχνικές. Ένα transaction αποστέλεται σε έναν κόμβο που είναι συνδεδεμένος με το blockchain δίκτυο και έπειτα κάνει validate το transaction και προωθείται σε άλλους κόμβους του δικτύου. Επίσης, οι κόμβοι επικυρώνουν και προωθούν το transaction στους δικούς τους peers μέχρι αυτό να φτάσει στο σύνολο τον κόμβων του δικτύου.

1.1.4 Fees

Η επεξεργασία των transaction περιλαμβάνει ένα συγκεκριμένο τέλος συναλλαγής, το οποίο καθορίζεται από το κόστος το οποίο επιβάλεται στο δίκτυο και αποτελεί ένα επιπλέον κίνητρο ώστε οι κόμβοι να παραμένουν έμπιστοι.

1.1.5 Mining

Ο όρος mining αντιστοιχεί στη διαδικασία της πιστοποίησης των συναλλαγών και προσθήκης νέων μπλοκ συναλλαγών στη blockchain. Παράλληλα, είναι και ένας μηχανισμός, με τον οποίο εισέρχονται νέα νομίσματα στο δίκτυο. Η διαδικασία του mining δεν αφορά όλα τα κρυπτονομίσματα. Επίσης, δεν έχει ούτε τα ίδια χαρακτηριστικά σε κάθε κρυπτονόμισμα που υλοποιεί mining. Κεντρικό και καθοριστικό ρόλο στη διαδικασία αυτή αναλαμβάνουν συγκεκριμένοι κόμβοι, ο οποίοι ονομάζονται miners. Το δίκτυο κάθε κρυπτονομίσματος παρέχει κίνητρο για τη συμμετοχή περισσότερων miner με τη μορφή ανταμοιβής (reward) για τις πολύτιμες υπηρεσίες τους.

Η τεχνολογία του mining

Το τρέχον hash rate μόνο για τη περίπτωση του Bitcoin mining ανέρχεται σε 86.002.554 TH/s. Αναλογιζόμαστε το μέγεθος της υπολογιστικής ισχύος, η οποία έχει συσσωρευτεί στα δίκτυα, αν προσθέσουμε και τις περιπτώσεις όλων των κρυπτονομισμάτων. Βέβαια, οι ρυθμοί προέκυψαν μέσω της εκρηκτικής ανάπτυξης του εξοπλισμού για τη διαδικασία του mining, αλλά και της προσέλκυσης πολλών νέων χρηστών. Μπορούμε να καταγράψουμε 4 βασικές τεχνολογίες:

1. CPU: αποτελούν τη κλασσική κεντρική μονάδα επεξεργασίας (Central Processing Unit), η οποία είναι ενσωματωμένη σε υπολογιστές και άλλες συσκευές. Κατά την κυκλοφορία του Bitcoin, το mining υλοποιούνταν αποκλειστικά από CPUs. Άλλωστε, ήταν το μόνο κρυπτονόμισμα σε λειτουργία μέχρι τότε.
2. GPU: αποτελούν τη μονάδα επεξεργασίας γραφικών (Graphics Processing Unit). Η δομή τους και η δυνατότητα γρήγορης προσπέλασης δεδομένων λόγω παράλληλης εκτέλεσης, οδήγει στο να πάρουν προβάδισμα σε σχέση με τα CPUs.
3. FPGAs: αποτελούν ειδικά σχεδιασμένο υλικό, που εστιάζει στην εκτέλεση μίας συγκεκριμένης εργασίας. Ανταγωνίζονται σε hash rate τα GPUs, βέβαια έχουν τη δυνατότητα να καταναλώνουν λιγότερη ενέργεια.
4. ASICs: αποτελούν ειδικά σχεδιασμένο υλικό για τη διαδικασία του mining. Σχεδιάζεται με τέτοιο τρόπο, ώστε να παράγουν το μέγιστο δυνατό πλήθος από hashes μέσω παράλληλης εκτέλεσης hash function. Είναι ο μόνος τρόπος πλέον για να μπορέσει ένας χρήστης να υλοποιήσει επιτυχές mining.

Κάθε χρήστης, αν διαθέτει τον αντίστοιχο εξοπλισμό, έχει τη δυνατότητα να υλοποιήσει από μόνος του mining (αν υποστηρίζεται από το κρυπτονόμισμα). Η περίπτωση αυτή ονομάζεται **solo mining.** Ωστόσο, λόγω της συσσώρευσης τεράστιας υπολογιστικής ισχύος μέσα στο δίκτυο παγκοσμίως και συνεχούς ανανέωσης της τεχνολογίας, το mining ενδέχεται να γίνεται και οικονομικά ασύμφορο για μεμονωμένους χρήστες.

Για αυτό το λόγο, εμφανίστηκε το **pool mining.** Στη περίπτωση αυτή ένα σύνολο από miners συνεισφέρουν την υπολογιστική τους δύναμη στο pool, με σκοπό να μοιραστούν τα rewards, που θα αποφέρει η διαδικασία. Η κατανομή του reward σε κάθε χρήστη στο pool mining είναι ανάλογη της συνεισφοράς με hash rate στο pool. Παράλληλα, κάθε χρήστης για τη συμμετοχή του στο pool, είναι υποχρεωμένος να καταβάλλει ένα μικρό τέλος συμμετοχής στον διαχειριστή του.

1.1.6 DAG

Αντιστοιχεί στον όρο directed acyclic graph (κατευθυνόμενος ακυκλικός γράφος), δηλαδή αποτελεί ένα πεπερασμένο γράφο χωρίς κύκλους. Αναλυτικότερα, αποτελείται από ένα πεπερασμένο αριθμό από κορυφές (vertices) και ακμές (edges), με κάθε ακμή να κατευθύνεται από μία κορυφή σε άλλη με τέτοιο τρόπο, ώστε να μην υπάρχει κανένα μονοπάτι το οποίο ξεκινά από μία κορυφή v και να καταλήγει μετά από ορισμένα βήματα στην ίδια κορυφή. Ισοδύναμα. ένας DAG είναι ένας κατευθυνόμενος γράφος που έχει ταξινομηθεί τοπολογικά, δηλαδή είναι μία σειρά από κορυφές, τέτοια ώστε κάθε κορυφή να κατευθύνεται από προηγούμενη σε επόμενη.

1.1.7 Hash function

Με τον όρο hash function αναφερόμαστε γενικά σε μία ομάδα συναρτήσεων, οι οποίες συμπιέζουν δεδομένα εισόδου (αυθαίρετου μεγέθους) και παράγουν μία έξοδο (hash value σε μορφή string) σταθερού μεγέθους. Λόγω των ιδιοτήτων τους, αποτελούν ένα ισχυρό εργαλείο για τις εφαρμογές, οι οποίες αξιοποιούν κρυπτογραφία, όπως όλα τα κρυπτονομίσματα.

Οι ιδιότητες τους είναι οι εξής:

- **Pre-image resistance:** Δοσμένου ενός hash value πχ hash(m), είναι υπολογιστικά αδύνατο να βρεθεί η τιμή εισόδου m.
- **Second pre-image resistance:** Δοσμένης μίας τιμής εισόδου m_1, είναι υπολογιστικά ανέφικτο να βρεις μία διαφορετική τιμή εισόδου m_2, τέτοια ώστε να ισχύει ότι hash(m_1) = hash(m_2).
- Είναι υπολογιστικά αδύνατο να βρεις μία δύο διαφορετικά μηνύματα μεταξύ τους (m_1 και m_2), τέτοια ώστε hash(m_1) = hash(m_2). Η περίπτωση αυτή ονομάζεται hash collision

1.1.8 Merkle tree

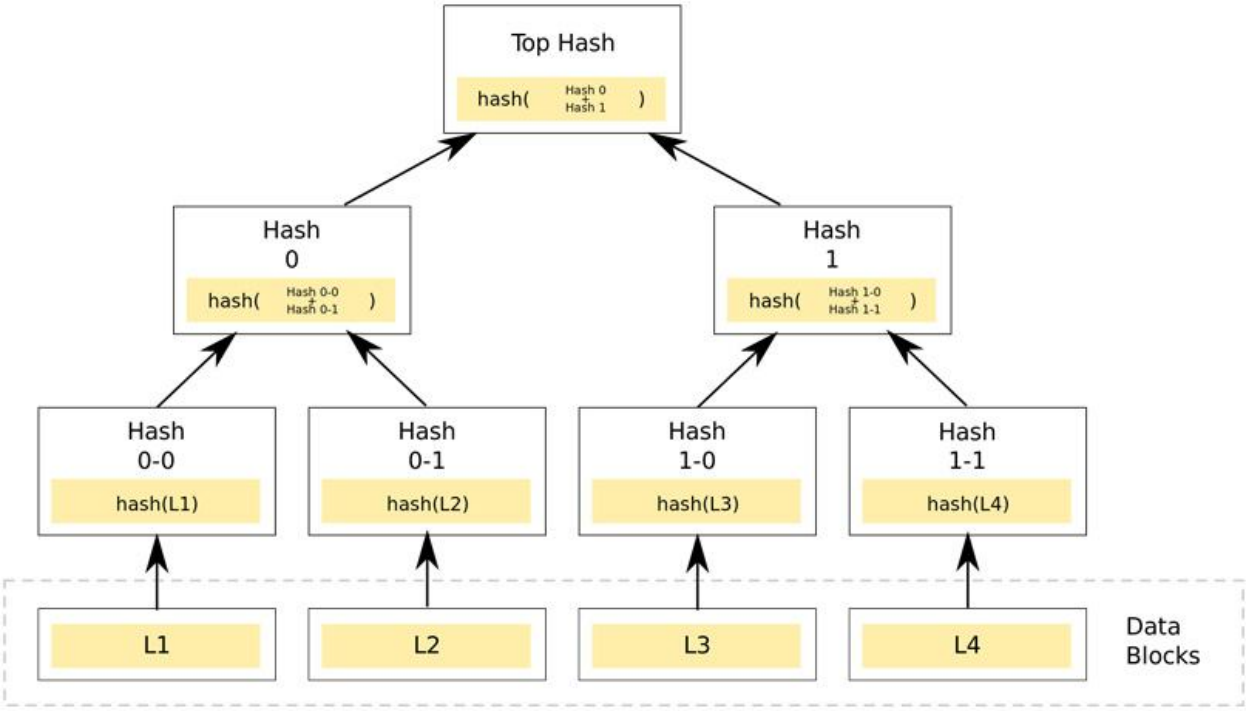
Το Merkle tree αποτελεί μία δομή δεδομένων τύπου tree (δέντρο), όπου κάθε leaf κόμβος αντιστοιχεί στο hash value ενός μπλοκ δεδομένων και κάθε non-leaf κόμβος περιλαμβάνει το hash value των σχετικών σε αυτόν child κόμβων.

Leaf κόμβος ονομάζεται ο κόμβος που δεν έχει καθόλου άλλους κόμβους ως απογόνους (descentants). Αντιστοιχούν στο τελεύταιο επίπεδο μίας δομής τύπου tree.

Non leaf κόμβος ονομάζεται ο κόμβος που διαθέτει τουλάχιστον έναν απόγονο κόμβο.

Όπως στην αρχή του παρόντος προτύπου. Δηλαδή με τη σειρά:

Στο σχήμα, παρατηρούμε μία αρκετά απλή μορφή ενός merkle tree. Κάθε επίπεδο αντιστοιχεί σε έναν αριθμό, με αφετήρια τον κόμβο ρίζα (root). Από πάνω προς τα κάτω, έχουμε αντίστοιχα τα επίπεδα 1,2,3,4. Οι leaf κόμβοι του σχήματος αντιστοιχούν στους L1, L2, L3, L4 (επίπεδο 4) και όλοι οι υπόλοιποι αντιστοιχούν στους non-leaf κόμβους (επίπεδα 1,2,3).



Σχήμα 2: Αναπαράσταση δομής Merkle tree

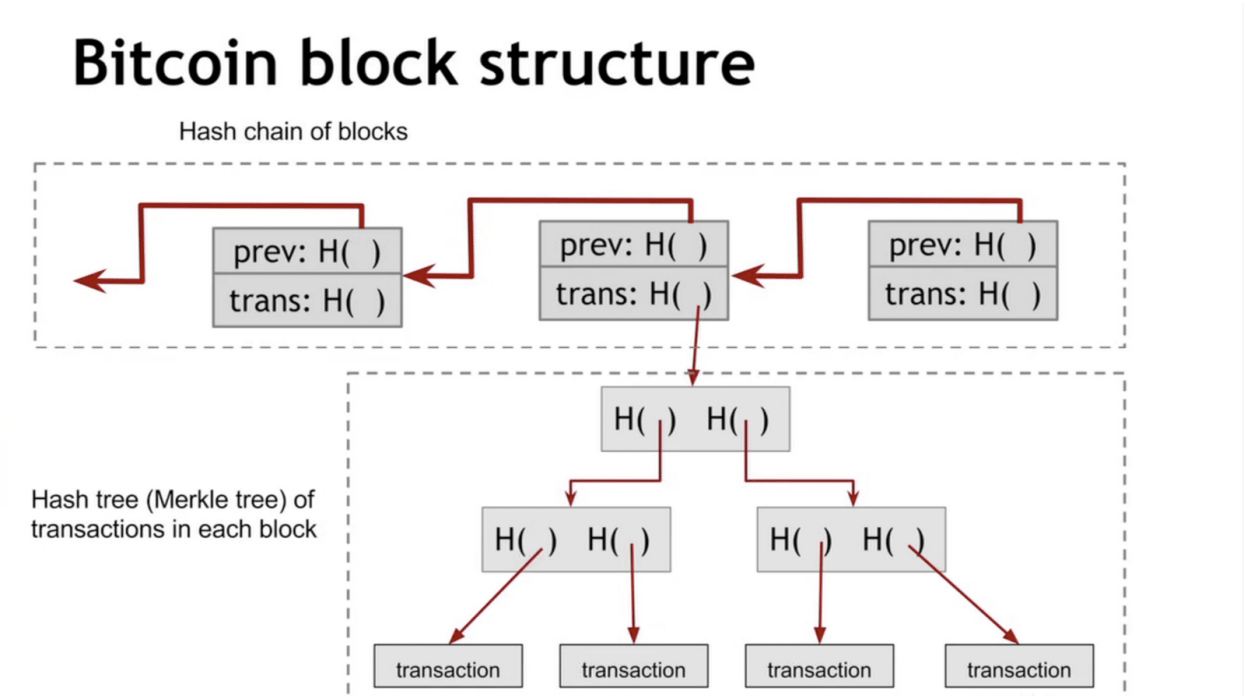
Παρατηρούμε, επίσης, ακριβώς στο επόμενο επίπεδο 3, υπάρχουν οι κόμβοι που περιλαμβάνουν τα hash values τους των κόμβων του επιπέδου 4. Η αντίστοιχη ροή συνθέτει συνολικά το merkle tree. Οι κόμβοι του επιπέδου i - 1 περιλαμβάνουν το hash value των κόμβων του επιπέδου i. Αν σημειωθεί η οποιαδήποτε αλλαγή στο περιεχόμενο ή στη διάταξη των δεδομενων που έχουν αποθηκευτεί στο Merkle tree, μεταβάλλεται και το Merkle root. Ουσιαστικά, η δομή merkle tree λαμβάνει ως δεδομένα έναν αριθμό n από hash values και τα αναπαριστά, συγχωνεύοντας τα με ένα απλό hash value.

Αξιοποιώντας την αντίστοιχη δομή ή παραλλαγές της (πχ patricia tree), δίνεται η δυνατότητα για αποτελεσματική διαχείριση των δεδομένων. Αυτό επιτυγχάνεται, καθώς υπάρχει διάκριση ανάμεσα στα αυτούσια δεδομένα και στα δεδομένα που είναι χρήσιμα για τις περιπτώσεις επιβεβαίωσης.

Παράλληλα, διαθέτει ορισμένα βασικά πλεονεκτήματα:

- Παρέχουν ένα αποδοτικό τρόπο για τη πιστοποίηση της εγκυρότητας και της ακεραίοτητας των δεδομένων.
- Αξιοποιούν μικρές ποσότητες μνήμης.

  Πολλές είναι οι περιπτώσεις των κρυπτονομισμάτων που χρησιμοποιούν αντίστοιχες δομές. Το hash value του Merkle Root συνήθως αποθηκεύεται στο block header των μπλοκ του blockchain. Μόνο έτσι δίνεται η δυνατότητα για πιστοποίηση του περιεχομένου πολλών μπλοκ. Δύο ή παραπάνω χρήστες του δικτύου, μπορούν να έρχονται σε συμφωνία (consensus) για την ταύτιση ή όχι ενός μπλοκ, απλά συγκρίνοντας τα hash value των merkle root.



Σχήμα 3: Bitcoin merkle tree

1.1.9 Fork

Τα γεγονότα τύπου fork δημιουργούν ένα εναλλακτικό στιγμιότυπο της παρούσας blockchain. Ανάλογα με τα χαρακτηριστικά τους και τη σημασία τους στη μορφή του blockchain, διακρίνονται στα εξής:

- (Temporary) fork: συμβαίνουν όταν προκύπτουν ταυτόχρονα ανταγωνιστικά (ως προς το ποιο θα ενσωματωθεί στο blockchain) μπλοκ από τη διαδικασία του mining, προκαλώντας έτσι τη διάσπαση του blockchain σε δύο ανταγωνιστικά στιγμιότυπα. Αυτή η περίπτωση των fork, επιλύεται από τα PoW συστήματα με την επιλογή του καταλληλότερου στιγμιοτύπου blockchain με βάση τη σύγκριση των timestamp ή του μήκους του αντίστοιχου στιγμιοτύπου.
- Soft fork: οδηγεί σε μόνιμες αλλαγές στους κανόνες του πρωτοκόλλου ενός κρυπτονομίσματος. Αναβαθμίζει το λογισμικό του πρωτοκόλλου με τέτοιο τρόπο, ώστε η νέα έκδοση να είναι συμβατή με τη παλαιότερη. Δεν απαιτείται η αναβάθμιση για όλους τους κόμβους για να υπάρχει συμφωνία στο δίκτυο, καθώς όλα τα μπλοκ υποστηρίζουν και το καινούριο και τον παλιό σύνολο κανόνων για συμφωνίας. Ωστόσο, αν κάποιο μπλοκ παραβιάζει του καινούριους κανόνες, είναι πολύ πιθανό να καταλήξει ως stale.
- Hard fork: οδηγεί σε μόνιμες αλλαγές στους κανόνες του πρωτοκόλλου ενός κρυπτονομίσματος. Ωστόσο, η διαφορά του με τη προηγούμενη περίπτωση, είναι το hard fork οδηγεί σε αναβάθμιση τέτοια, ώστε η νέα έκδοση να μην είναι συμβατή με τη προηγούμενη. Όλοι οι κόμβοι του δικτύου είναι υποχρεωμένοι να αναβαθμίσουν το πρωτόκολλο που τρέχουν, ώστε να συνεχίσουν να συμμετέχουν στο δίκτυο. Μπλοκ που έχει επιβεβαιωθεί η εγκυρότητα τους από κόμβους που δεν αναβαθμιστεί, θεωρούνται άκυρα. Η πρώτη περίπτωση αναφέρεται στη περίπτωση των blockchain και οι υπόλοιπες δύο αναφέρονται στη περίπτωση ενός λογισμικού.

1.2 Οι μηχανισμοί εξασφάλισης συναίνεσης (consensus)

1.2.1 Proof of Work (PoW)

Η ιδέα του PoW παρουσιάστηκε πρώτη φορά το 1993 (πολύ πιο πριν από την ανάπτυξη του Bitcoin) ως μία τεχνική για την αντιμετώπιση του spam στις υπηρεσίες email. Με λίγα λόγια απαιτούσε από τον αποστολέα του mail να υπολογίσει τη λύση ενός μαθηματικού puzzle, με σκοπό να αποδείξει πως έχει δαπανήσει ορισμένη υπολογιστική ισχύ για την ενέργεια αυτή. Το PoW προτάθηκε αυτοτελώς το 1997, μέσω του αλγορίθμου το hashcash, πάλι με σκοπό την αντιμετώπιση του spam. Στη περίπτωση του hashcash, το υπολογιστικό πρόβλημα περιελάμβανε την εύρεση ενός hash value (μέσω της συνάρτησης SHA-1), το οποίο θα ξεκινούσε από τουλάχιστον 20 συνεχόμενα μηδενικά. Αυτό προφανώς απαιτούσε συνεχόμενους υπολογισμούς με κόστος αρκετή υπολογιστική ισχύ. Το έγκυρο hash value θεωρείται πως ισοδυναμεί με το PoW.

Ο Satoshi Nakamoto, έτσι ώστε να εισαγάγει ένα consensus πρωτόκολλο, βασισμένο στη παραπάνω μεθοδολογία. Σε γενικές γραμμές, το πρωτόκολλο αυτό ορίζεται από 3 βασικές διαδικασίες.

1. Την επιβεβαίωση των μπλοκ και έτσι και του blockchain. Κατά τη διάρκεια της διαδικασίας αυτής ελέγχονται αν τηρούνται όλες οι προδιαγραφές για το δοσμένο στιγμιότυπο του blockchain. Ελέγχεται, δηλαδή, αν κάθε μπλοκ περιλαμβάνει ένα έγκυρο PoW και ότι δεν υπάρχει κάποια διχογνωμία ή ανάμεσα στις συναλλαγές.
2. Τη σύγκριση ανάμεσα στα στιγμιότυπα των blockchain και στην επέκταση της. Η διαδικασία αυτή περιλαμβάνει τη σύγκριση ανάμεσα στο μήκος ενός συνόλου από στιγμιότυπα blockchain, τα οποία λαμβάνονται από άλλους ομότιμους χρήστες. Μέσα από αυτό το στάδιο, υιοθετείται η μεγαλύτερη σε μήκος εκδοχή των προτεινόμενων blockchain.
3. Την αναζήτηση ενός έγκυρου PoW.

Η 3η παραπάνω βασική διαδικασία είναι η πιο απαιτητική από άποψη εργασίας και καθοριστική για τη λειτουργία του πρωτοκόλλου πολλών κρυπτονομισμάτων. Μία έγκυρη λύση PoW απαιτεί συνεχόμενους υπολογισμούς, έτσι ώστε να βρεθεί ένα hash value το οποίο θα ικανοποιεί μία συνθήκη του πρωτοκόλλου. Η μεθοδολογία αυτή μπορεί να συμπυκνωθεί ως εξής:

Δοσμένου ενός ρυθμιζόμενου παράγοντα difficulty h, η διαδικασία της εύρεσης μίας έγκυρης λύσης για το PoW στοχεύει στην αναζήτηση ενός string (γνωστό και ως nonce), τέτοιο ώστε για ένα δοσμένο μπλοκ δεδομένων x (οι συναλλαγές στη πλειονότητα των περιπτώσεων), το hash value του ζευγαριού nonce,data να είναι μικρότερεο από μία τιμή target D(h):

$$H(x \,||\, nonce) <= D(h)$$

όπου H αντιστοιχεί σε μία hash συνάρτηση

$$D(h) = 2^{L-h}, \text{ με L να αντιστοιχεί σε ένα σταθερό μήκος από bits}$$

Το παραπάνω πρωτόκολλο θεωρείται computation-intensive, καθώς για να ανταπεξέλθει κάποιος στον ανταγωνισμό για την εύρεση ενός έγκυρου PoW, χρειάζεται να διαθέτει όσο το δυνατό μεγαλύτερο hash rate. Αυτό το χαρακτηριστικό αποτρέπει τις επιθέσεις Sybil από κακόβουλους χρήστες. Από την άλλη μεριά, το οικονομικό κόστος μέσω της κατανάλωσης ισχύος, καθιστά αδύνατο για οποιοδήποτε κόμβο να συμμετάσχει στο δίκτυο χωρίς να επιβαρυνθεί με κάποιο κόστος. Ωστόσο, με σκοπό την

εξασφάλιση της λειτουργίας και τη σταθερή συμμετοχή των χρηστών στο δίκτυο, το πρωτόκολλο αυτό παρέχει κίνητρα όπως το reward ή τα transaction fees.

1.2.2 Proof of Stake (PoS)

Το PoS αποτελεί τη δεύτερη βασική κατηγορία αλγορίθμων consensus για blockchain. Οι χρήστες-κόμβοι σε αυτά τα συστήματα ονομάζονται validators. Βασίζονται στο απόθεμα νομισμάτων (stake) που επιλέγει να δεσμεύσει ένας validator στο δίκτυο. Κάθε validator εκτελεί μία ειδική συναλλαγή, που δεσμεύει ένα πόσο από κρυπτονομίσματα ως προκαταβολή. Μόνο οι validators έχουν τη δυνατότητα να δημιουργήσουν νέα μπλοκ και να αποφασίσουν μέσω του consensus ποιο θα συμπεριληφθεί στο blockchain. Στη διαδικασία του consensus, οι validators δε ψηφίζουν ισότημα, αλλά το «βάρος» της ψήφου εξαρτάται από το μέγεθος του stake που έχει θέσει ως προκαταβολή. Η πιθανότητα για έναν validator να είναι αυτός που θα λάβει το reward, είναι ανάλογη του κλάσματος του μεγέθους του stake (του δεσμευμένου ποσού) διαιρεμένου με το συνολικό αριθμό νομισμάτων σε κυκλοφορία. Όσο μεγαλύτερο ποσό θέτει ως προκαταβολή, τόσο αυξάνεται η πιθανότητα για επιτυχία. Όποιος validator παραβιάζει τους κανονισμούς του consensus, παρακρατείται το ποσό που έχει θέσει ως stake.

Στους συγκεκριμένους χρήστες αποδίδεται η δυνατότητα απόφασης μέσα στο δίκτυο. Παραπέρα, η πιθανότητα ένας validator να δημιουργήσει ένα νέο μπλοκ επιτυχώς εξαρτάται από τη ποσότητα των νομισμάτων που διαθέτει (από το μέγεθος του stake), και όχι από τη υπολογιστική ισχύ που δαπανά. Με αυτό το τρόπο, ελαχιστοποιείται το κόστος σε ενέργεια για κάθε συναλλαγή και μπλοκ.

Αποδίδει τη δυνατότητα απόφασης μόνο στους κόμβους όπου διαθέτουν stake μέσα στο δίκτυο. Δηλαδή, μόνο εάν ένας χρήστης διαθέτει ένα ποσό από νομίσματα μπορεί να συμμετάσχει στις διαδικασίες ενημέρωσης του blockchain (όπως ο έλεγχος της εγκυρότητας των συναλλαγών και η δημιουργία νέων μπλοκ). Αυτό έρχεται σε αντίθεση με τις περιπτώσεις του PoW, όπου κάθε χρήστης έχει τη δυνατότητα να αναλάβει το ρόλο του miner. Στη περίπτωση του PoS, δεν απαιτείται καθόλου υπολογιστική δύναμη για την επίλυση ενός ενός υπλογιστικού puzzle. Επίσης, δεν υπάρχουν rewards μέσα από τη μορφή της δημιουργίας χρήματος: οι κόμβοι (συχνά στο PoS ονομάζονται validators) συλλέγουν τα transaction fees. Από τη στιγμή που συμβαίνει κάτι τέτοιο, το ενδεχόμενο για τη δημιουργία κενών μπλοκ είναι σχετικά απίθανο, καθώς οι nodes έχουν ως κίνητρο τη ενσωμάτωση όσο το δυνατό περισσότερων transaction, ώστε να μεγιστοποιήσουν τα κέρδη τους.

1.2.3 Hybrid PoW / PoS

Τα συστήματα που αξιοποιούν hybrid PoW/PoS επιδιώκουν να συνδυάσουν τα πλεονεκτήματα κάθε σχεδιασμού. Σε αυτό το σχεδιασμό, η δημιουργία νέων μπλοκ, βασίζεται στο παράγοντα coinage. Το coinage στην ουσία αντιστοιχεί στο γινόμενο μίας ποσότητας νομισμάτων που διαθέτει ένας χρήστης επί το χρονικό διάστημα που βρίσκονται στην ιδιοκτησία του. Έτσι, η δημιουργία νέων μπλοκ πριμοδοτεί τα μπλοκ με το μεγαλύτερο coinage. Επίσης, τα νομίσματα μπαίνουν σε κυκλοφορία είναι το 1% των νομισμάτων που έχουν δαπανηθεί μέσα σε ένα coin-year. Το βασικό πλεονέκτημα είναι πως δεν απαιτείται μεγάλη κατανάλωση ενέργειας.

2. ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΤΩΝ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

2.1 Bitcoin (BTC)

2.1.1 Κίνητρα ανάπτυξης

Αν και δεν υπάρχουν αρκετά στοιχεία γύρω από το πρόσωπο και τη δραστηριότητα του δημιουργού του Bitcoin, έχουμε τη δυνατότητα να κάνουμε κάποιες ασφαλείς εκτιμήσεις για τα κίνητρα του. Βασικός μας οδηγός είναι το paper που δημοσίευσε ο ίδιος.

Ο συγγραφέας του paper περιγράφει πως το ηλεκτρονικό εμπόριο και οι συναλλαγές που πραγματοποιούνται σήμερα βασίζονται στο σύνολο τους σε τραπεζικά και οικονομικά ιδρύματα. Αυτά είναι υπεύθυνα για την επεξεργασία των συναλλαγών και τον έλεγχο της εγκυρότητας τους. Ακολουθούν το σχήμα client server με κάποιο διαμεσολαβητή, συνήθως κάποια κεντρική αρχή, η οποία είναι υπεύθυνη για τη διάδραση άναμεσα στους χρήστες. Και οι 2 χρήστες αρκεί να εμπιστεύονται τη κεντρική αρχή, ώστε το σύστημα να λειτουργεί αρμονικά.

Βέβαια, τα αντίστοιχα μοντέλα-σχήματα χαρακτηρίζονται από ορισμένα μειονεκτήματα λόγω της φύσης τους. Τα μειονεκτήματα ποικίλλουν. Για παράδειγμα, σε ένα ανάλογο διαδικτυακό μοντέλο, μία τράπεζα ή κάποιος άλλος οργανισμός (πχ κρατική υπηρεσία) διαμεσολαβεί για τη πραγματοποίηση συναλλαγών. Παράλληλα, οι συγκεκριμένοι θεσμοί διαθέτουν ισχύ για να επιβάλλουν τους κανόνες τους πχ πάγωμα της κίνησης του λογαριασμού, όριο στα ποσά που διακινούνται στις συναλλαγές, δημιουργώντας εμπόδια στους πελάτες-χρήστες. Επίσης, είναι υπόλογοι στη κρατική νομοθεσία πχ φόροι για τραπεζικές συναλλαγές, αλλά και ευάλωτοι σε αποσταθεροποιήσεις πχ κούρεμα καταθέσεων σε κρίσιμες καταστάσεις ή όρια στην πιστοληπτική ικανότητα. Επιπρόσθετα, ένα ανάλογο διαδικτυακό μοντέλο απαιτεί πληροφορίες για τους πελάτες, έτσι ώστε να εξασφαλίζεται η μετάκληση-αντιστροφή της συναλλαγής (η επιστροφή των χρημάτων) για τους χρήστες. Πολλές φορές αυτού του είδους οι συναλλαγές δημιουργούν διενέξεις ανάμεσα σε πωλητές και αγοραστές (πχ αγορά ενός προϊόντος που δεν έφτασε ποτέ στα χέρια μου-απάτη). Αυτό επιβαρύνει με επιπλέον κόστος τις συναλλαγές, πόσο μάλλον όταν θέλουμε να πραγματοποιήσουμε πολλές μικρές και έξυπνες συναλλαγές.

Έτσι, δημιουργήθηκε η ανάγκη για ένα σύστημα ηλεκτρονικών πληρωμών που θα βασίζεται στην κρυπτογραφικές τεχνικές απόδειξης, παρά στην αμοιβαία εμπιστοσύνη σε ένα κεντρικό διαμεσολαβητή. Με αυτό τον τρόπο επιτρέπεται σε οποιοδήποτε ζευγάρι χρηστών να συναλλάσεται απευθείας, χωρίς τη διαμεσολάβηση ενός τρίτου έμπιστου προσώπου (π.χ. μίας τράπεζας). Οι πωλητές-χρήστες θα προστατεύονται από απάτες, καθώς οι συναλλαγές δε θα μπορούν να αντιστραφούν, αλλά και οι αγοραστές-χρήστες θα προστατεύονται από μηχανισμούς χρηματικής εγγύησης.

Τα παραπάνω πλαίσιο αποτέλεσε το βασικό κίνητρο για τη δημιουργία του Bitcoin. Φαίνεται πως ο δημιουργός του Bitcoin να προσπαθούσε να φέρει ριζικές αλλαγές στη οικονομία με αυτό τον τρόπο, παρατηρώντας την αποτυχία και τις επικίνδυνες συνέπειες της κατάρρευσης του τραπεζικού συστήματος. Δεν είχε μάλλον πρόθεση να στοχοποιήσει ευθέως τους μεγάλους τραπεζικούς οργανισμούς, αλλά να τους

παρακάμψει, διαμορφώνοντας ένα δίκτυο γρηγορότερων, φθηνότερων και δίχως όρια συναλλαγών.

Δεν είναι τυχαία ούτε η ημερομηνία έκδοσης των πρώτων νομισμάτων ούτε και του paper. Το λογισμικό του bitcoin ήρθε στην πραγματικότητα στις 9 Ιανουαρίου του 2009, και το πρώτο μπλοκ δημιουργήθηκε στις 3/01/2009, ενώ το paper δημοσιεύθηκε στις 31 Οκτώβρη του 2008. Οι ημερομηνίες αυτές έρχονται μετά ακριβώς από το ξέσπασμα της παγκόσμιας χρηματοπιστωτικής κρίσης, που ξεκίνησε το 2007 στις ΗΠΑ, με αφετηρία την κατάρρευση του χρηματοπιστωτικού και τραπεζικού συστήματος.

Προς σε αυτή τη κατεύθυνση συνηγορεί και το περιεχόμενο της coinbase παραμέτρου στο genesis block που είναι η συγκεκριμένη: **The Times 03/Jan/2009 Chancellor on brink of second bailout for banks**

2.1.2 Στοιχεία για το δημιουργό

Ο δημιουργός του Bitcoin θεωρείται πως είναι ένα άτομο με το όνομα Satoshi Nakamoto. Πρόκειται για πρόσωπο αγνώστων λοιπών στοιχείων με αρκετές θεωρίες(πολλές από αυτές στα όρια της συνομωσίας) γύρω από τη πραγματική ταυτότητα του ατόμου. Είναι άγνωστη η εθνικότητα του, το πραγματικό του όνομα, οι σπουδές του και η επαγγελματική του δραστηριότητα. Σίγουρα το όνομα αυτό αποτελεί ψευφώνυμο για ένα ή περισσότερα άτομα.

Το όνομα Satoshi Nakamoto εμφανίζεται ως ο συγγραφέας μίας επιστημονικής έκθεσης (της πρώτης) για το πρωτόκολλο λειτουργίας του bitcoin. Στις 31/10/2008, κάποιος, με το συγκεκριμένο όνομα, ανακοίνωσε τη δημιουργία του Bitcoin σε διαδικτυακό φόρουμ. Ο ίδιος δημοσίευσε το γνωστό, πλέον, paper “Bitcoin: A Peer-to-Peer Electronic Cash System”, στη κρυπτογραφημένη mailing list του metzdowd.com

Έκτοτε, έφερε στη κυκλοφορία τη πρώτη έκδοση του λογισμικού για το bitcoin το 2009. Συγκεκριμένα, στις 03-01-2009 εμφανίστηκε και επίσημα το block 0(genesis block), ξεκινώντας έτσι τη blockchain του bitcoin. Το καιρό μετά από αυτό συμμετείχε με άλλους προγραμματιστές στη βελτίωση και τη συντήρηση του project. Όλη η επικοινωνία ανάμεσα στα μέλη της κοινότητας που δούλευαν στο project γινόταν μέσα από κρυπτογραφημένα μέιλ, προστατεύοντας έτσι κάθε πληροφορία που έχει σχέση με το πραγματικό πρόσωπό του. Στις πρώτες μέρες ύπαρξης και λειτουργίας του Bitcoin, υπήρχαν μόνο λίγοι χρήστες που συμμετείχαν στο δίκτυο, πραγματοποιώντας mining. Το difficulty (οι απαιτήσεις του mining) ήταν ακόμα αρκετά χαμηλό και έτσι ο κάθε χρήστης είχε τη δυνατότητα να συσσωρεύσει αρκετά νομίσματα. Ο ίδιος ο Satoshi φέρεται να έχει εξορύξει πάνω από 1 εκ νομίσματα. Ωστόσο, κανένα νόμισμα από αυτά δεν έχει ξοδευτεί. Ο επικρατέστερος λόγος σχετίζεται πως μία πιθανή σπατάλη ορισμένων νομισμάτων θα μπορούσε να οδηγήσει στο πραγματικό πρόσωπο, που κρύβεται πίσω από το ψευδώνυμο Satoshi Nakamoto.

Από τα τέλη του 2010, άρχισε να φθείνει η συμμετοχή του στην κοινότητα. Η τελευταία εμφάνισή του έγινε την άνοιξη του 2011, και έκτοτε δεν έχει απασχολήσει με τη δραστηριότητα του.

2.1.3 Το τρέχον market Capitalization

Σχήμα 4: Το Market Capitalization του Bitcoin

Η τρέχουσα ονομαστική αξία του Bitcoin είναι $8.866,41 και το συνολικό πλήθος των νομισμάτων σε κυκλοφορία είναι 17.954.887 BTC. Αυτό οδηγεί σε ένα τρέχον Market Capitalization της τάξης των $159.195.348.743.

Από την εμφάνιση του BTC σε κυκλοφορία μέχρι και τον Ιούλιο του 2017, η ονομαστική αξία του BTC και αντίστοιχα το Market Capitalization του κυμαίνονταν σε χαμηλά επίπεδα. Από τον Ιούλιο του 2017 μέχρι και τα μέσα του Δεκεμβρίου του 2017, παρουσιάστηκε μία ταχεία άνοδος στην ονομαστική του αξία. Ύστερα από αυτή τη περίοδο, παρατηρούμε σύντομες περιόδους συνεχών αυξομειώσεων.

Η ονομαστική αξία του BTC παρουσίασε:

- **ιστορικό υψηλό στις 17/12/2017, προσεγγίζοντας τα $ 20.089. Η αξία αυτή αντιστοιχούσε σε Market Cap της τάξης των $ 336.433.998.575.**
- **ιστορικό χαμηλό στις 05/07/2013, φτάνοντας τα $ 65,53. Η αξία αυτή αντιστοιχούσε σε Market Cap των $ 745.297.638.**

Το BTC διατηρεί εδώ και χρόνια τη υψηλότερη θέση στη κατάταξη των κρυπτονομισμάτων με βάση το Market Cap. Ανήκει στα large cap κρυπτονομίσματα.

2.1.4 Η νομισματική πολιτική

Όπως έχει αναφερθεί, το πρωτόκολλο του Bitcoin, αλλά και των υπόλοιπων κρυπτονομισμάτων, λειτουργεί αποκεντρωμένα, χωρίς την ύπαρξη και τη διαμεσολάβηση μίας κεντρικής αρχής.

Η νομισματική πολιτική του Bitcoin αποτελεί το σύνολο των κανόνων, με τους οποίους εισέρχονται νέα νομίσματα (BTC) στο δίκτυο. Αυτό αφορά και το ρύθμο παραγωγής(mining) νέων νομισμάτων. Κάθε νόμισμα που αδυνατεί να ακολουθήσει τους κανόνες που έχουν οριστεί για κάποιο λόγο (π.χ. ένας κακόβουλος χρήστης προσπαθεί να εισάγει "πλαστά" νομίσματα ως γνήσια) απορρίπτεται και έτσι δεν αποκτά καθόλου αξία.

Πίνακας 1: Βασικές νομισματικές μονάδες Bitcoin

Συντομογραφία	Κοινή ονομασία	Επίσημη ονομασία	Αξία σε BTC
BTC	bitcoin	bitcoin	1
mBTC		millibitcoin	0.001
μBTC	bit	microbitcoin	0.000001
	satoshi	satoshi	0.00000001

Το πρωτόκολλο του Bitcoin μπορεί να θέσει σε κυκλοφορία ένα πεπερασμένο πλήθος από νομίσματα. Αυτό έρχεται σε αντίθεση με το παραδοσιακό τραπεζικό συστήμα και τις νομισματικές πολιτικές που ακολουθούνται παγκοσμίως. Με βάση αυτές, δεν υπάρχει άνω όριο στη ποσότητα του χρήματος που κυκλοφορεί στην οικονομία. Βέβαια, και σε αυτή την περίπτωση, το χρήμα "δε κόβεται" αυθαίρετα και ανεξέλεγκτα, αλλά ο ρυθμός δημιουργίας ελέγχεται με βάση κάποιους κανονισμούς. **Ο μόνος τρόπος με τον οποίο τίθονται σε κυκλοφορία νέα νομίσματα είναι μέσω της διαδικασίας του mining.** Χρειάζεται να θέσουμε υπό εκτίμηση ορισμένους παράγοντες:

Κάθε φορά που επιβεβαιώνεται ένα μπλοκ συναλλαγών και εισέρχεται στο blockchain εισέρχονται στο δίκτυο νέα νομίσματα. Άρα ο χρόνος δημουργίας και "έκδοσης" ενός νέου μπλοκ σχετίζεται άμεσα με τα νομίσματα που τίθονται σε κυκλοφορία.

Το πρωτόκολλο του Bitcoin πρέπει να διατηρεί το ρυθμό δημιουργίας ενός νέου μπλοκ σταθερό στα 10 λεπτά περίπου, ανεξάρτητα από τη συνολική υπολογιστική ισχύ που υπάρχει στο δίκτυο. Αυτή η διαδικασία σταθεροποίησης του ρυθμού δημιουργίας νέων νομισμάτων αντιστοιχεί στην αναπροσαρμογή του difficulty για τη διαδικασία του mining. Ο ρυθμός δημιουργίας νέων μπλοκ ρυθμίζεται κάθε 2016 μπλοκ. Αυτό σημαίνει πως αν προστίθεται 1 μπλοκ κάθε 10 λεπτά στη blockchain, ο ρυθμός δημιουργίας νέων μπλοκ ρυθμίζεται κάθε 2 εβδομάδες.

Το πλήθος των bitcoin που δημιουργούνται ανά μπλοκ(και άρα το reward του miner για την αποτελεσματική δραστηριότητα του) είναι ρυθμισμένο να μειώνεται με ρυθμούς γεωμετρικής προόδου, με μείωση στο μισό κάθε 210.000 μπλοκ, ή κάθε 4 χρόνια προσεγγιστικά. Το ίδιο το πρωτόκολλο προφυλλάσεται από μία γρήγορη εξάντληση των αποθεμάτων του bitcoin και από φαινόμενα πληθωρισμού.

Οι παραπάνω κανόνες (πχ η μείωση του reward κάθε 4 χρόνια) αποτελούν απλά αυθαίρετες συμβάσεις. Ο ίδιος ο δημιουργός του Bitcoin ποτέ δεν εξήγησε ή δικαιολόγησε το μέγεθος αυτών των σταθερών. Διάφορες εκτιμήσεις που έχουν γίνει

γύρω από αυτές τις σταθερές καταλήγουν στο ότι με αυτό τον ρυθμό εξόρυξης, το συνολικό πλήθος των Satoshis που μπορούν να εξορυχθούν προσεγγίζει τη μέγιστη χωρητικότητα ενός 64-bit αριθμού κινητής υποδιαστολής. Βέβαια, αυτό παραμένει στο επίπεδο των εκτιμήσεων.

Επιπρόσθετα, έτσι ορίζεται και το άνω όριο των νομισμάτων που μπορούν να δημιουργηθούν. **Το σύνολο των bitcoin που μπορούν να τεθούν σε κυκλοφορία είναι προσεγγιστικά 21.000.000 BTC. Συγκεκριμένα, θα είναι 20.999.999,9769 BTC.** Από αυτά περίπου τα 17 εκ. βρίσκονται ήδη σε κυκλοφορία(έχουν γίνει mined). Συγκεκριμένα, τη στιγμή που γράφεται αυτό το κείμενο έχουν τεθεί σε κυκλοφορία πάνω από 17.768.988 BTC. Ο ακριβής ρυθμός μείωσης του reward του mining δε μπορεί να υπολογιστεί με ασφάλεια. Ο λόγος είναι οι μεταβολές στην συνολική υπολογιστική ισχύ του συστήματος (και άρα και στο difficulty του mining). Αυτό μας οδηγεί σε ορισμένες εικασίες. Αν η συνολική υπολογιστική ισχύ είχε παραμείνει σταθερή από τη στιγμή της εξόρυξης των πρώτων νομισμάτων, το τελευταίο νόμισμα θα έχει εξορυχθεί κάπου γύρω στις 8 Οκτωβρίου 2140. Από τη στιγμή που δε γνωρίζουμε ούτε μπορούμε να προβλέψουμε με σιγουριά τις μεταβολές που μπορούν να γίνουν στα τεχνικά δεδομένα του πρωτοκόλλου του bitcoin, είναι αδύνατο να υπολογίσουμε την ακριβή ημερομηνία εξόρυξης του τελευταίου νομίσματος. Τα νομίσματα που δεν έχουν ακόμα τεθεί σε κυκλοφορία βρίσκονται μέσα ένα χώρο(pool) και αναμένουν να αποτελέσουν reward για τους υποψήφιους miners.

Τι θα γίνει αν όλα τα νομίσματα εξορυχθούν;

Το μεγαλύτερο μέρος του reward που λαμβάνει ένας miner έχει σχέση με τη βασική ιδιότητα, να δημιουργεί νέα μπλοκ έγκυρων συναλλαγών και να τα τοποθετεί στη blockchain. Πέρα από αυτό, ένας miner ανταμοίβεται και από τα τέλη που συνοδεύουν τις συναλλαγές. **Στη συνθήκη, όπου έχουν εξαντληθεί όλα τα αποθέματα των νομισμάτων, τα τέλη συναλλαγών θα αποτελούν το βασικό κίνητρο για τους miners να συμμετέχουν στο δίκτυο και να συνεχίζουν τη δραστηριότητά τους.**

Επαναλαμβάνω πως ο εκτιμώμενος αριθμός των νομισμάτων που μπορούν να τεθούν σε κυκλοφορία για το Bitcoin προσεγγίζει τα 21 εκ. Βέβαια, αυτό δε σημαίνει πως αυτό το πλήθος των νομισμάτων μπορεί να ξοδευτεί στο σύνολο του. Το συνολικό απόθεμα των νομισμάτων που μπορούν να ξοδευτούν είναι πάντα μικρότερο σε σχέση με το συνολικό πλήθος των νομισμάτων που μπορούν να εξορυχθούν. Αυτό συμβαίνει για διάφορους λόγους όπως τεχνικές ανεπάρκειες και ζημιές πχ ολικές βλάβες σε σκληρούς δίσκους με απώλεια δεδομένων, σε κακόβουλες ενέργειες πχ κλοπή ζευγαριών δημόσιου-ιδιωτικού κλειδιού, αλλά και σε οικειοθελή καταστροφή.

Απώλεια νομισμάτων

Νομίσματα μπορεί να χαθούν αν οι συνθήκες των συναλλαγών πάψουν να είναι πλέον γνωστές. Για παράδειγμα, για να πραγματοποιηθεί μία συναλλαγή σε μία συγκεκριμένη διεύθυνση, απαιτείται ένα ιδιωτικό κλειδί. Αν αυτό χαθεί για οποιόδήποτε λόγο, τα νομίσματα που συμμετείχαν στη συναλλαγή θεωρούνται χαμένα. Είναι θεωρητικά αδύνατο να βρεθεί ξανά κλειδί που να ταιριάζει στην περίπτωση αυτή. Νομίσματα μπορούν να καταστραφούν οικειωθελώς. Για παράδειγμα, στοιχεία των νομισμάτων μπορούν να τροποποιηθούν ώστε να αδύνατο να τα ξοδέψουμε.

2.1.5 Τα χαρακτηριστικά των transactions

Κατ'αρχήν, υπάρχουν δύο τύποι από συναλλαγές στη περίπτωση του Bitcoin, οι coinbase transactions και οι regular transactions. Οι coinbase transactions είναι ειδικές συναλλαγές, στις οποίες νέα νομίσματα BTC εισέρχονται στο σύστημα. Περιλαμβάνονται σε κάθε μπλοκ ως η πρώτη ακριβώς συναλλαγή και σχετίζονται με το reward του επιτυχημένου miner. Από την άλλη, regular transactions σχετίζονται με τη μεταφορά υπαρχόντων νομισμάτων BTC ανάμεσα σε χρήστες του δικτύου. Οι διαφορές αυτές αποτυπώνονται και στην αντίστοιχη δομή τους.

2.1.5.1 Regular transactions

Όπως αναφέρθηκε παραπάνω, κάθε μπλοκ του blockchain περιλαμβάνει ένα σύνολο από transactions. Κάθε regular transaction αποτελείται από τους εξής παράγοντες.

Πίνακας 2: Η δομή μιας regular transaction στο Bitcoin

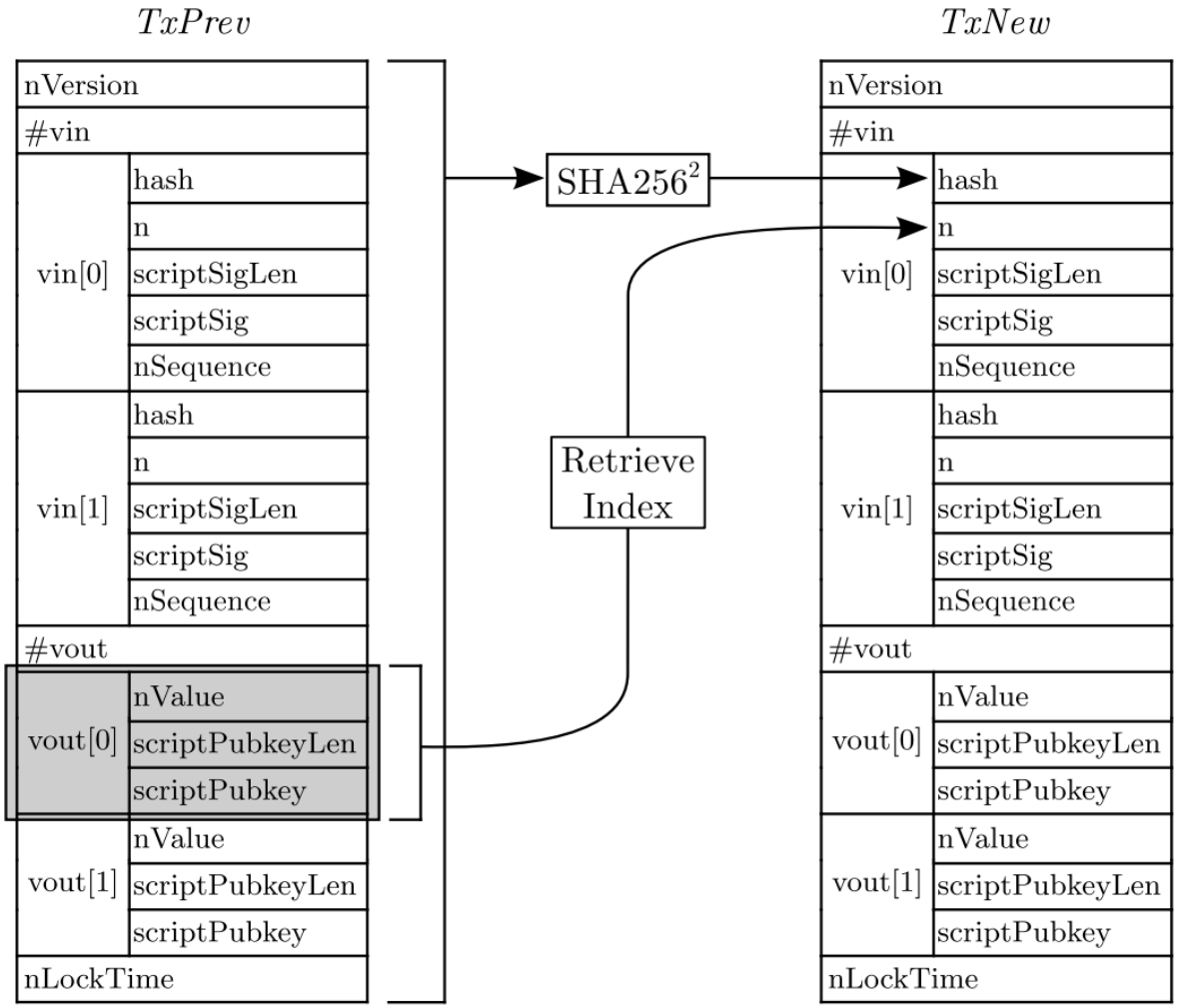
Πεδίο	Μέγεθος (byte)	Περιγραφή
nVersion	4	το τρέχον transaction version (με τιμή 1)
#vin	1-9	το πλήθος των δεδομένων εισόδου
hash	32	το hash value της προηγούμενης συναλλαγής
n	4	index της εξόδου της transaction που αναφέρεται το πεδίο hash
scriptSigLen	1-9	το μέγεθος του πεδίου scriptSig
scriptSig	δεν είναι σταθερό	το script που ικανοποιεί την συνθήκη ικανοποίησης της συναλλαγής
nSequence	4	Ο αύξων αριθμός της εισόδου της transaction
#vout	1-9	το πλήθος των δεδομένων εξόδου
nValue	8	ποσό εκφρασμένο σε 10^{-8} BTC (satoshis)
scriptPubkeyLen	1-9	το μέγεθος του scriptPubKey
scriptPubKey	δεν είναι σταθερό	το script το οποίο καθορίζει τις συνθήκες, στις οποίες η έξοδος μίας transaction μπορεί να διεκδικηθεί
nLockTime	4	timestamp του «κλειδώματος» της συναλλαγής

Το ζεύγος (hash,n) προσδιορίζουν μοναδικά την έξοδο της προηγούμενης transaction. Το πεδίο hash αναφέρεται και ως transaction ID (TxID). Υπολογίζεται από τη διπλή εφαρμογή του SHA256 στα περιεχόμενα της συναλλαγής.

$$\textbf{TxID} = \textbf{SHA256}^2\textbf{(Transaction's contents)}$$

Ως εκ τούτου, ενώ μία transaction αναγνωρίζεται μοναδικά από το hash value της, τα δεδομένα εξόδου μίας transaction αναγνωρίζονται από το πεδίο n.

Το πεδίο nLock, πιο αναλυτικά, περιγράφει το χρόνο κλειδώματος της transaction, δηλαδή το χρόνο που πρέπει να παρέλθει, έτσι ώστε να ενσωματωθεί στο σώμα του μπλοκ. Αν ο συγκεκριμένος χρόνος περάσει, η transaction θεωρείται «κλειδωμένη» και μπορεί πλέον να ενταχθεί στο υποψήφιο μπλοκ.



Σχήμα 5: Δομή μιας regular transaction

2.1.5.2 Coinbase transaction

Κάθε coinbase transaction αποτελείται από τα εξής πεδία:

Πίνακας 3: Δομή coinbase transaction

Πεδίο	Μέγεθος (bytes)	Περιγραφή
nVersion	4	το τρέχον transaction version (με τιμή 1)
#vin	1-9	το πλήθος των δεδομένων εισόδου
hash	32	hash value από τη διπλή εφαρμογή του SHA256
n	4	το index για τα δεδομένα εξόδου transaction

coinbaseLen	1-9	το μέγεθος του πεδίου coinbase
coinbase	δεν είναι σταθερό	κωδικοποίηση του block height και άλλων δεδομένων
nSequence	4	ο αύξων αριθμός των δεδομένων εισόδου της transaction
#vout	1-9	το πλήθος των δεδομένων εξόδου της transaction
nValue	8	ποσό εκφρασμένο σε 10^{-8} BTC (satoshis)
scriptPubkeyLen	1-9	το μέγεθος του πεδίου scriptPubkey
scriptPubkey	δεν είναι σταθερό	το script το οποίο καθορίζει τις συνθήκες, στις οποίες η έξοδος μίας transaction μπορεί να διεκδικηθεί
nLockTime	4	timestamp του «κλειδώματος» της συναλλαγής

Σε σχέση με τον πίνακα, πέρα από το μετονομασία του script πεδίου, από scriptSig σε coinbase, η δομή των συναλλαγών παραμένει η ίδια. Ωστόσο, υπάρχουν ορίσμενες ακόμα διαφορές.

Αναλυτικά:

1. Στη περίπτωση της coinbase transaction, νέα νομίσματα BTC εισέρχονται στο σύστημα, και ως εκ τούτου δεν υπάρχει αναφορά σε προηγούμενη συναλλαγή.

2.1.5.3 Μέγεθος transaction

Το μέγεθος μίας απλής συναλλαγής δε μπορεί να ξεπερνά τα 10000 bytes σε μέγεθος.

2.1.5.4 Final transaction

Μία συναλλαγή ονομάζεται final, εφ'όσον ικανοποιεί τουλάχιστον μία από τις παρακάτω συνθήκες:

2. Ο παράγοντας transaction lock time (το πεδίο nLockTime) είναι ορισμένο σε κατάσταση locked ή έχει παρέλθει το αντίστοιχο χρονικό διάστημα.
3. Όλα τα transaction input είναι final.

2.1.6 Το bitcoin block

Κάθε μπλοκ αποτελείται από ένα header και το payload. Το block header περιλαμβάνει τα εξής πεδία:

Πίνακας 4: Bitcoin block

Πεδίο	Μέγεθος(bytes)	Περιγραφή
nVersion	4	αντιστοιχεί στο τρέχουσα version του μπλοκ
HashPrevBlock	32	αντιστοιχεί στη hash value του block header, του αμέσως προηγούμενου μπλοκ

HashMerkleRoot	32	αντιστοιχεί στο hash value του root του Merkle tree που αξιοποιείται για τις συναλλαγές του blockchain.
nTime	4	το timestamp της δημιουργίας του μπλοκ
nBits	4	το target value για το proof of work
nNonce	4	ο παράγοντας nonce για το mining

Το payload περιλαμβάνει τα εξής πεδία:

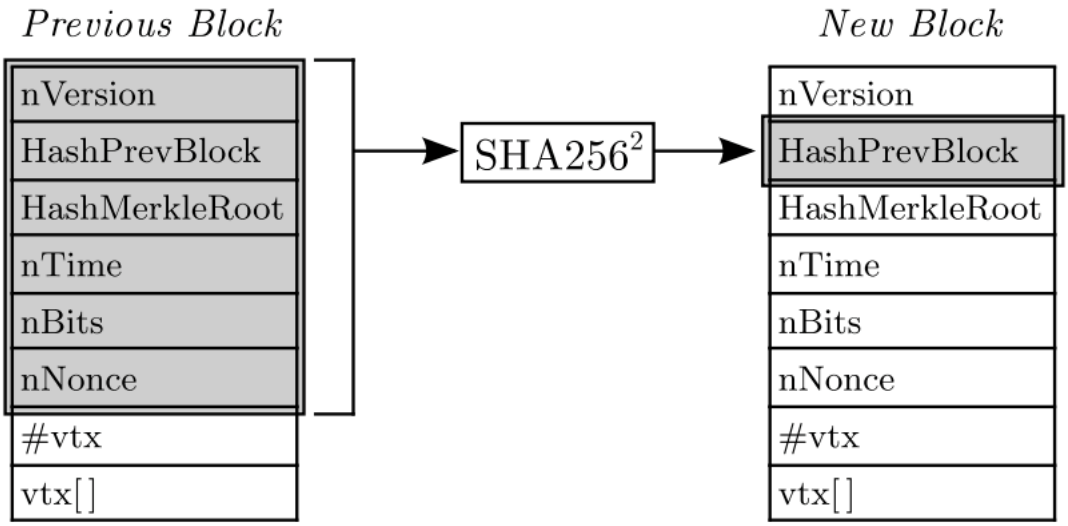
Πίνακας 5: Δομή payload

Πεδίο	Μέγεθος(σε bytes)	Περιγραφή
#vtx	1-9	το πλήθος των transactions
vtx	δε είναι σταθερό	οι συναλλαγές του μπλοκ

Αναλυτικά για τα πεδία του μπλοκ:

- Το transaction format version (το πεδίο nVersion) έχει τρέχουσα τιμή 2. Κάθε μπλοκ με διαφορετικό nVersion ούτε μπορεί να γίνει mined ούτε μπορεί να μεταδοθεί.
- Η σύνδεση με το προηγούμενο μπλοκ δεν είναι απλή, αλλά «αλυσιδωτή». Αυτό επιτυγχάνεται μέσω του πεδίου HashPrevBlock. Συγκεκριμένα, όλο το header του αμέσως προηγούμενου μπλοκ συγχωνεύεται και εισέρχεται ως είσοδος σε μία διπλή SHA256 συνάρτηση.

$SHA256^2$ (nVersion||HashPrevBlock||HashMerkleRoot||nT ime||nBits||nNonce) = HashPrevBlock(του επόμενου μπλοκ)



Σχήμα 6: Bitcoin block

2.1.7 Orphan μπλοκ

Orphan(ed) μπλοκ θεωρείται ένα μπλοκ, το οποίο δεν έχει γίνει δεκτό μέσα στη bitcoin blockchain. Ονομάζεται και stale μπλοκ. Περιλαμβάνει verified transactions και έχει θεωρηθεί έγκυρο μέσα από τη διαδικασία του mining. Η απόρριψη του από το δίκτυο σχετίζεται με την εξής εξέλιξη:

Κατά τη διάρκεια της διαδικασίας του mining, όλοι οι miners του δικτύου προσπαθούν να υπολογίσουν το σωστό proof of work. Υπάρχει το ενδεχόμενο, δύο miners να το πετύχουν και να δημιουργήσουν δύο έγκυρα μπλοκ σχετικά ταυτόχρονα. Το γεγονός αυτός οδηγεί σε fork, δηλαδή σε διάσπαση του blockchain. Στη περίπτωση αυτή, για να επιστρέψουμε σε μία blockchain, οι nodes του δικτύου επιλέγουν το μπλοκ που δημιουργήθηκε πρώτο(μέσα από τη σύγκριση του timestamp-πεδίο nTime) και συνεχίζουν την οικοδόμηση του blockchain από αυτό το σημείο. Το άλλο μπλοκ απομονώνεται στο δίκτυο και οι transactions που ενσωμάτωνε, επιστρέφουν στο pool των transaction σε αναμονή.

2.1.8 Genesis block

Το genesis block είναι το πρώτο μπλοκ σε ένα blockchain. Σύγχρονες εκδόσεις του bitcoin το αριθμούν ως το μπλοκ 0, σε αντίθεση με τις πρώτες εκδόσεις που το αριθμούσαν ως block 1. Όπως κάθε genesis μπλοκ, δεν υπάρχει καμία αναφορά σε κάποιο προηγούμενο μπλοκ.

Το hash value του genesis μπλοκ είναι:

019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Αν παρατηρήσει κανείς, περιλαμβάνει 2 παραπάνω μηδενικά σε hex στην αρχή, σε σχέση με όσα απαιτούσε ένα πρώιμο μπλοκ. Το coinbase του genesis block είναι hardcoded μέσα από λογισμικό του bitcoin.

Τα πρώτα 50 BTC κατευθήνθηκαν σε προορισμό με διεύθυνση το 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa (hex). Λόγω, όμως μίας ιδιομορφίας στο κώδικα του Bitcoin, το ποσό αυτό είναι αδύνατο να ξοδευτεί. Είναι ακόμα άγνωστο αν η συγκεκριμένη ιδιομορφία σχεδιάστηκε ακούσια ή εσκεμμένα από τον Satoshi Nakamoto. Άλλες συναλλαγές που είχαν ως προορισμό την ίδια διεύθυνση, θεωρούνται ότι μπορεί να ξοδευτούν. Είναι ακόμα άγνωστο αν η συγκεκριμένη διεύθυνση ανήκει στον ίδιο τον Satoshi.

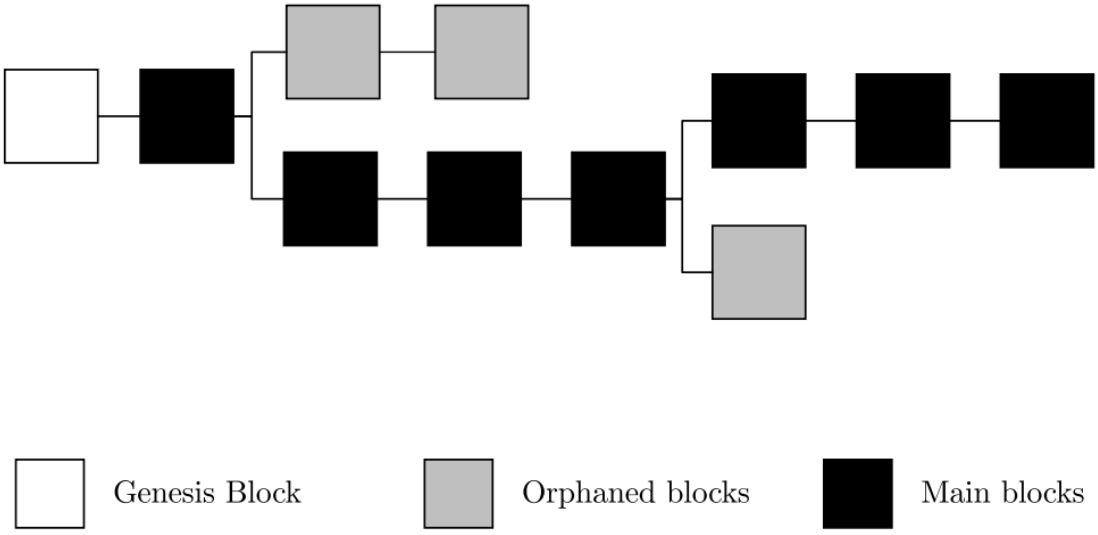
Στα μπλοκ των regular transactions, χρησιμοποιούμε ως δεδομένα εισόδου(transaction inputs) τα δεδομένα εξόδου(transaction outputs) της parent transaction. Βέβαια, όπως αναφέραμε προηγουμένως, το genesis block δεν έχει καμία αναφορά σε προηγούμενο μπλοκ συναλλαγών. Στην περίπτωση αυτή, το coinbase αποτελεί τα δεδομένα εισόδου για την πρώτη συναλλαγή.

Το coinbase μπορεί να περιέχει οποιαδήποτε αυθαίρετα ορισμένα δεδομένα. Στην περίπτωση του genesis block του bitcoin, το coinbase περιλαμβάνει ένα απόσπασμα από το πρωτοσέλιδο των FT: The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

2.1.9 Το blockchain

Η πλατφόρμα του Bitcoin αξιοποιεί τη τεχνολογία του Blockchain για την αποτελεσματική και αξιόπιστη λειτουργία της. Η αξιοποίηση της τεχνολογίας Blockchain

αποτέλεσε τομή σε σχέση με τις υπόλοιπες εφαρμογές ψηφιακών νομισμάτων, που είχαν κυκλοφορήσει παλαιότερα. Αποτρέπει από τη μία τη προσπάθεια για double-spending και από την άλλη παρέχει εγγυημένα τη δυνατότητα για χρονολογική κατάταξη των transactions.



Σχήμα 7: Το blockchain του bitcoin

Δομή

Σε γενικές γραμμές, η blockchain αποτελεί τη κατανεμημένη βάση δεδομένων των bitcoin transactions. Δηλαδή, από τη μία περιλαμβάνει όλες τις συναλλαγές που έχουν λάβει χώρα από την έναρξη λειτουργίας του δικτύου (την εξόρυξη του genesis block, ή Block #0) και από την άλλη κατανέμεται σε κάθε χρήστη του δικτύου.

- Βασικό συστατικό της Bitcoin blockchain του αποτελούν τα μπλοκ. Κάθε μπλοκ περιλαμβάνει μόνιμα καταγεγραμμένες πληροφορίες που σχετίζονται με τις transactions. Κατάσσονται σειριακά στην blockchain, με το τελευταίο μπλοκ να ονομάζεται block head.
- Η διαδικασία του mining οδηγεί στη προσθήκη νέων μπλοκ στη blockchain. Νέα μπλοκ δε μπορούν να υποβληθούν στο δίκτυο αν δε περιλαμβανουν το σωστό proof of work, που προκύπτει από το mining. Η διαδικασία αυτή επαναλαμβάνεται κάθε 10 λεπτά περίπου. Κάθε μπλοκ που “έρχεται στο φως” κυμαίνεται από 1 έως και 1.5 με MB δεδομένων. Μέχρι και τώρα το πλήθος των μπλοκ που είναι αποθηκευμένα στη blockchain είναι 596.344 μπλοκ. Το πλήθος αυτό ονομάζεται και block height. Αναφερόμαστε, δηλαδή, σε περίπου 595.344 MB με 894.516 MB αποθηκευμένης συνολικά πληροφορίας. Τα δεδομένα αυτά αφορούν κυρίως transactions ανάμεσα στους χρήστες της πλατφόρμας. Με αυτό το τρόπο, έχουμε πρόσβαση στα στοιχεία οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί ποτέ στη πλατφόρμα του Bitcoin. Δεν υπάρχει κάποιο όριο στο πλήθος των μπλοκ που μπορούν να εισέλθουν στη blockchain. Όσο πιο βαθιά εισχωρεί ένα μπλοκ μέσα στη blockchain, γίνεται ακόμα δυσκολότερο να μεταβληθεί ή να απομακρυνθεί, εξασφαλίζοντας έτσι τη μη αναστροφή των συναλλαγών.

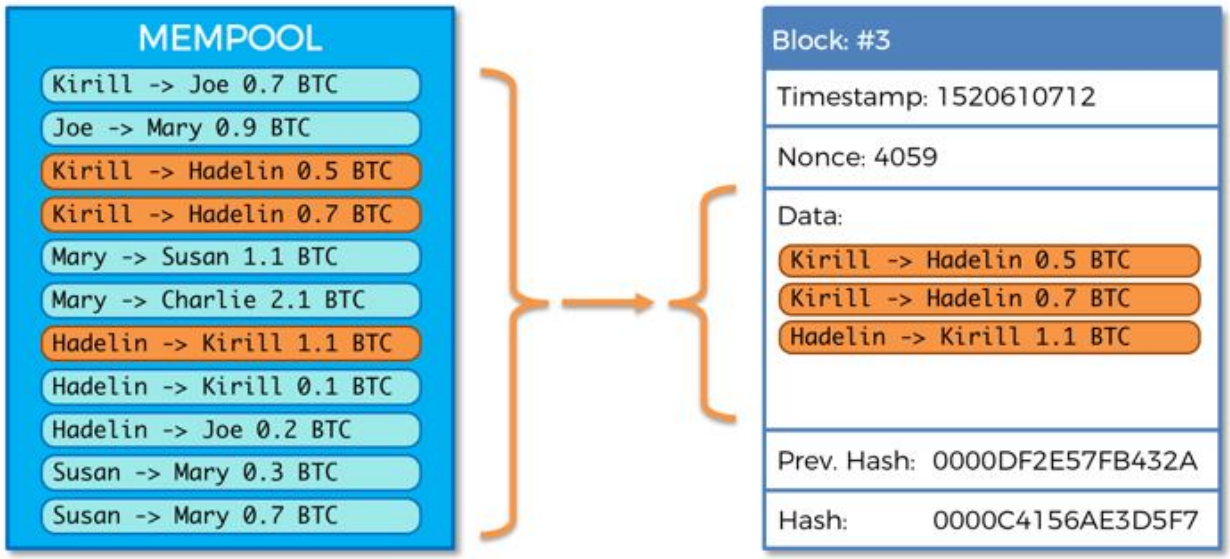
- Το Bitcoin blockchain ακολουθεί ένα συγκεκριμένο μοντέλο διακυβέρνησης, ώστε να αποφασίζονται “δημοκρατικά” οι μεταβολές εντός του δικτύου. Ο βασικός κανόνας αναφέρει πως “ό,τι θεωρεί η πλειοψηφία πως είναι αληθές”, αυτό καθορίζει σε γενικές γραμμές το ίδιο το δίκτυο. Κυριαρχεί, δηλαδή, η λογική του consensus. Πάντοτε, η blockchain με το μεγαλύτερο μήκος θεωρείται πιο έγκυρη, διότι υποτίθεται πως το συγκεκριμένο στιγμιότυπο της blockchain υποστηρίζεται από τη πλειονότητα. Πέρα από όλα αυτα, απαιτείται το μεγαλύτερο μέρος της υπολογιστικής ισχύος για τη δημιουργία της μεγαλύτερης σε μήκος έκδοσης της blockchain. Για αυτό και ένα αλλοιωμένο μπλοκ απορρίπτεται αυτόματα από την πλειονότητα του δικτύου, καθώς δε είναι πλέον “αλυσοδεμένο” με τη μακρύτερη blockchain.

Σχήμα 8: Δομή bitcoin blockchain

2.1.10 Η διαδικασία του mining

Οι mining nodes (ή απλά miners) του δικτύου εκτελούν τη παρακάτω διαδικασία συνεχώς:

1. Συλλογή όλων των transactions που έχουν μεταδοθεί στο δίκτυο. Στη συνέχεια, γίνεται έλεγχος της εγκυρότητάς τους. Τυπικά, κάθε transaction περιλαμβάνει ένα τέλος συναλλαγής(transaction fee), ως κίνητρο για το miner. Αν δεν υπάρχει κάτι τέτοιο, ο miner έχει την ελεύθερη, πλέον, επιλογή να απορρίψει τη transaction.
2. Επικύρωση όλων των transactions, που ενσωματώθηκαν στο μπλοκ.
3. Επιλογή του πιο πρόσφατου μπλοκ στο μεγαλύτερο σε μήκος μονοπάτι του blockchain. Εισαγωγή του hash value του block header του μπλοκ αυτού στο νέο μπλοκ.
4. Επίλυση του proof of work προβλήματος και μετάδοση της σωστής λύσης (αν βρεθεί) σε όλο το δίκτυο.
5. Έλεγχος της ορθότητας του proof of work από τους υπόλοιπους nodes του δικτύου. Συγκεκριμένα, ελέγχεται η εγκυρότητα του μπλοκ και των transactions που περιλαμβάνει. Συγκεκριμένα, υπολογίζεται το hash value του μπλοκ, με το παράγοντα nonce να έχει τροποποιηθεί από τη διαδικασία του mining. Αν το hash value αυτό ταυτίζεται με το proof of work που μετέδωσε ο miner, το νέο μπλοκ θεωρείται πλέον έγκυρο.



Σχήμα 9: Η διαδικασία του mining στο bitcoin

6. Αν υπάρχει consensus (συναίνεση) για την εγκυρότητα του μπλοκ από τους nodes του δικτύου, το μπλοκ εισέρχεται επιτυχημένα στο blockchain. Αν όχι, απορρίπτεται και τα δεδομένα του γίνονται null.

Μόλις τελειώσει η διαδικασία αυτή, επαναλαμβάνεται ξανά. Η διάρκειά της κυμαίνεται στα 10 λεπτά.

2.1.10.1 Proof-of-Work

Ο αλγόριθμος του proof of work του bitcoin βασίζονται στον αλγόριθμο του hashcash. Κατά τη διάρκεια του mining, κάθε miner επιχειρεί να υπολογίσει ένα hash value, το οποίο να είναι κάτω από ένα καθορισμένο από το δίκτυο όριο target value T.
Κατ'ουσίαν, το όριο αυτό εκφράζει τον αριθμό των συνεχόμενων μηδενικών που θα βρίσκονται στην αρχή του παραγόμενου hash value από το miner. Το Το όριο αυτό μεταβάλλεται με βάση το difficulty. Όσο περισσότερη υπολογιστική ισχύ συσσωρεύει το δίκτυο, τόσο αυξάνεται και το difficulty και αντιστροφώς. Η γραμμική σχέση αυτή υπάρχει, ώστε να παραμένει σταθερός ο χρόνος παραγωγής νέων μπλοκ στα 10 λεπτά.

Η διαδικασία εύρεσης ενός σωστού proof of work περιλαμβάνει τα εξής βήματα από τη πλευρά του miner:

1. Ορίζει ελεύθερα τη τιμή του nonce(το πεδίο nNonce) και του coinbase(το πεδίο coinbase).
2. Υπολογίζει συνεχώς το hash value του block header μέσω της διπλής εφαρμογής του SHA256.
3. Ελέγχει αν το hash value που υπολογίστηκε είναι κάτω από το target value T
4. Αν είναι κάτω από το target value, ο miner έχει επιτυχώς υπολογίσει ένα proof of work και μεταδίδει το μπλοκ που συνθέτει, μαζί με το proof of work, στο υπόλοιπο δίκτυο.

2.1.11 Το δίκτυο του Bitcoin

Η πλατφόρμα του Bitcoin είναι δομημένη **ως ένα peer-to-peer δίκτυο.** Κάθε κόμβος συμμετέχει ισότιμα στο δίκτυο, έρχεται σε διάδραση με τους υπόλοιπους και δεν υπάρχουν "ειδικοί" κόμβοι. Όλοι μαζί μοιράζονται το φορτίο της παροχής των υπηρεσιών του δικτύου. Οι nodes του δικτύου διασυνδέονται μεταξύ τους σε ένα πλέγμα με "επίπεδη" τοπολογία. Δεν υπάρχει καμία κεντρική αρχή, κανένας server και καμία ιεραρχία μέσα στο δίκτυο. Οι nodes παρέχουν και καταναλώνουν υπηρεσίες ταυτόχρονα. Το δίκτυο του Bitcoin διαθέτει 3 συγκεκριμένα χαρακτηριστικά ως P2P δίκτυο:

1. Είναι **αποκεντρωμένο**, καθώς όπως έχουμε αναφέρει, δεν διαθέτει κάποιακεντρική αρχή που να το ορίζει ή να το διευθύνει.
2. Είναι **ανοικτό**, καθώς κάθε χρήστης έχει τη δυνατότητα να αποκτήσει πρόσβαση σε αυτό. Δεν απαιτεί από τους νέους χρήστες συμμόρφωση σε ένα σύνολο από κανόνες και περιορισμούς.
3. Είναι **ανθεκτικό σε επιθέσεις**, καθώς όσο περισσότεροι χρήστες παρέχουν υπηρεσίες στο δίκτυο, τόσο περισσότερη αντοχή υπάρχει σε κακόβουλες ενέργειες.

Θα μπορούσε κάποιος να ισχυριστεί πως το δίκτυο του Bitcoin παρουσιάζει αρκετές ομοιότητες με την αρχιτεκτονική του διαδικτύου στις πρώτες μέρες του. Ο αποκεντρωμένος έλεγχος πάνω στο δίκτυο αποτελεί τον πυρήνα του σχήματος του δικτύου και μπορεί να επιτευχθεί μόνο μέσα από ένα αποκεντρωμένο P2P δίκτυο συμφωνίας.

Με τον όρο δίκτυο του Bitcoin αναφερόμαστε σε ένα σύνολο από nodes, που εκτελούν το Bitcoin P2P πρωτόκολλο. Το πρωτόκολλο αυτό περιλαμβάνει τα εξής βήματα-γεγονότα:

1. Νέες transactions μεταδίδονται σε όλους τους κόμβους του δικτύου
2. Κάθε κόμβος επιλέγει ελεύθερα transactions από transaction pool και τις ενσωματώνει μέσα στο μπλοκ που συνθέτει.
3. Κάθε κόμβος υπολογίζει συνεχώς το proof of work για το δικό του μπλοκ.
4. Όταν ένας node βρίσκει ένα σωστό PoW, μεταδίδει το μπλοκ σε όλους τους υπόλοιπους nodes του δικτύου, μαζί με το PoW.
5. Οι κόμβοι δέχονται το μπλοκ ως έγκυρο, αν όλες οι συναλλαγές είναι έγκυρες.
6. Οι κόμβοι εκφράζουν την αποδοχή τους στο μπλοκ και ξεκινούν τη δημιουργία ενός νέου μπλοκ, χρησιμοποιώντας το hash value το πρόσφατα δημιουργημένου μπλοκ.

Πάραλληλα, με αυτό το πρωτόκολλο, υπάρχουν και εκτελλούνται και άλλα πρωτόκολλα, όπως το Stratum, που αξιοποιούνται για mining και εφαρμογές mobile wallet. Αυτά τα επιπρόσθετα πρωτόκολλα παρέχονται από ειδικούς servers, που δίνουν τη δυνατότητα πρόσβασης στο bitcoin δίκτυο. Με αυτό το τρόπο, δημιουργούν προϋποθέσεις για επέκταση του δικτύου. Χρησιμοποιούμε τον όρο διευρυμένο δίκτυο bitcoin για να αναφερθούμε στο συνολικό δίκτυο, στοιχεία του οποίου είναι το P2P bitcoin πρωτόκολλο, τα mining pools και κάθε είδους πρωτόκολλα που επιτρέπουν τη διασύνδεση όλων των συστατικών.Τύποι nodes και ο ρόλος του καθενός

Μπορεί όλοι οι κόμβοι του bitcoin δικτύου να είναι ισότιμοι μεταξύ τους, αναλαμβάνουν διαφορετικούς ρόλους. Οι ρόλοι αυτοί σχετίζονται με τη λειτουργικότητα που αυτοί υποστηρίζουν. Ένας bitcoin node υποστηρίζει μία σειρά από λειτουργίες: δρομολόγηση

δεδομένων και μπλοκ, συντήρηση, ανανέωση και συγχρονισμός του blockchain, mining και συμμετοχή σε υπηρεσίες για wallets.

2.1.11.1 Τύποι κόμβων (nodes) και ο ρόλος του καθενός

Full Node

Ένας full node υποστηρίζει όλες τις παραπάνω λειτουργίες. Όλοι οι nodes συμμετέχουν στο δίκτυο, επιβεβαιώνοντας την εγκυρότητα των συναλλαγών. Τα δεδομένα αυτά στη συνέχεια αναμεταδίδονται σε όλο το δίκτυο.

Παράλληλα, ορισμένοι κόμβοι, οι full nodes που έχουμε αναφέρει, διατηρούν ένα πλήρες και ενημερωμένο αντίγραφο του blockchain. Ένας full node έχει τη δυνατότητα αυτόματα και αξιόπιστα να επιβεβαιώνει συναλλαγές χωρίς τη παρέμβαση κάποιου άλλου node.

SPV Nodes

Ορισμένοι κόμβοι, επίσης, διαθέτουν μόνο ένα υποσύνολο από το ιστορικό της blockchain και επιβεβαιώνουν συναλλαγές μέσα από μία μέθοδο που ονομάζεται SPV(simplified payment verification). Οι κόμβοι αυτό για το συγκεκριμένο λόγο ονομάζονται SPV ή lightweight nodes.

Mining Nodes

Στο δίκτυο, καθοριστικό ρόλο αναλαμβάνουν οι mining nodes. Έχουν την ευθύνη να δομούν νέα μπλοκ, εκτελώντας τον proof-of-work αλγόριθμο. Οριμένοι mining nodes επεκτείνουν τη λειτουργικότητα τους, αποκτώντας τις αρμοδιότητες ενός full node.

Οι εφαρμογές των wallets αξιοποιούν τη λειτουργικότητα των full nodes, αλλά και των SPV nodes ειδικά στην περίπτωση των εφαρμογών σε κινητά τηλέφωνα.

2.1.11.2 Το διευρυμένο Bitcoin δίκτυο

Το κύριο bitcoin δίκτυο (αυτό δηλαδή που εκτελεί το Bitcoin P2P πρωτόκολλο) αποτελείται από περίπου 10.000 κόμβους (9623 nodes για την ακρίβεια τη στιγμή που γράφονται αυτά). Οι nodes αυτοί “ακούν” συνεχώς το δίκτυο και εκτελούν εκδοχές του Bitcoin Core. Αρκετές εκατοντάδες άλλοι κόμβοι υλοποιούν μία σειρά από άλλες εφαρμογές του Bitcoin πρωτοκόλλου, όπως το BitcoinJ, το Libbit-coin και το btcd. Ένα μικρό ποσοστό των nodes υλοποιούν mining. Ένα πλήθος από μεγάλες εταιρίες έρχονται σε επαφή με το δίκτυο του bitcoin, εκτελώντας full node λειτουργίες, χωρίς βέβαια να πραγματοποιούν mining ή υπηρεσίες wallet. Αυτού το είδους οι ειδικοί κόμβοι λειτουργούν ως δρομολογητές του δικτύου, επιτρέποντας τη διαμόρφωση ποικίλων υπηρεσιών.

2.2 Ethereum

2.2.1 Σκοπός δημιουργίας της πλατφόρμας του Ethereum

Προτού περιγράψουμε το σκοπό για τον οποίο σχεδιάστηκε η πλατφόρμα του Ethereum, και έτσι και το ether, χρειάζεται να ανατρέξουμε στον ίδιο το σκοπό ανάπτυξης του Bitcoin, αλλά και στα ίδια τα χαρακτηριστικά του διαδικτύου. Βασική επιδίωξη για το Bitcoin ήταν να δημιουργηθεί ένα peer-to-peer και ανοικτού κώδικα σύστημα το οποίο αξιοποιεί ψηφιακά νομίσματα με τη χρήση κρυπτογραφίας και κυρίως της τεχνολογίας Blockchain. Κύριο χαρακτηριστικό του είναι ο αποκεντρωμένος χαρακτήρας του. Δηλαδή, δεν υπάρχει ούτε κάποια κεντρική αρχή ή όργανο που να ρυθμίζει το δίκτυο των χρηστών και το σύστημα, ούτε κάποιος διαμεσολαβήτης για τις συναλλαγές των χρηστών. Με αυτό το τρόπο, δημιουργήθηκε μία “καθαρή” peer-to-peer εκδοχή ψηφιακών-ηλεκτρονικών νομισμάτων. Στο ιδανικό σενάριο της ευρύτατης χρήσης του Bitcoin, ως πλατφόρμα ηλεκτρονικών συναλλαγών, από τη πλειονότητα των χρηστών του διαδικτύου, θα είχαμε τουλάχιστον υποτίμηση ή ακόμα και παραγκωνισμό μέσων και εφαρμογών, όπως το PayPal ή το online banking των τραπέζων.

Το βασικό “αγκάθι” στο ζήτημα της ύπαρξης μιας κεντρικής αρχής ως διαμεσολαβητής στο client-server μοντέλο σχετίζεται με την εξουσία και την ισχύ που έχει πάνω στο δίκτυο, στους χρήστες και στα δεδομένα.

Από τη μία αξιοποιεί εξειδικευμένο προσωπικό και εξοπλισμό για την ποιοτική και άμεση εξυπηρέτηση των χρηστών. Από την άλλη, βέβαια, έχει τη δυνατότητα να μπλοκάρει ενέργειες των χρηστών, αλλά και να αποκτήσει πρόσβαση σε προσωπικά μας δεδομένα. Για παράδειγμα, μία τράπεζα, μπορεί να διατηρεί τα τραπεζικά αποθέματα ασφαλή, αλλά μπορεί ανά πάσα στιγμή να μπλοκάρει τις αναλήψεις ή να εκθέσει τα προσωπικά μας δεδομένα (πχ ιστορικό συναλλαγών) σε τρίτους.

Από τη στιγμή που θα επικρατούσε ένα “καθαρό” peer-to-peer σύστημα συναλλαγών, οι υπηρεσίες που βασίζονται σε μία κεντρική αρχή (πχ τραπεζικοί οργανισμοί) θα οδηγούνταν σταδιακά σε απαξίωση από το κοινό.

Εδώ εντάσσεται και η αντιπαράθεση για τον ίδιο των χαρακτήρα του διαδικτύου. Πολλοί είναι αυτοί που νομίζουν πως το διαδίκτυο έχει αποκεντρωμένο χαρακτήρα. Ωστόσο, κάτι τέτοιο δεν έχει καμία σχέση με την πραγματικότητα. Τεχνολογικοί κολοσσοί, όπως η Google, η Amazon το Facebook, και αρκετοί άλλοι διαθέτουν εκπληκτική ισχύ πάνω στο διαδικτύο. Όλα τα προσωπικά μας δεδομένα, κωδικοί, ιστορικά αναζήτησης, συναλλαγές, ιατρικές και προσωπικές πληροφορίες, βρίσκονται αποθηκευμένα σε clouds και servers που ελέγχονται από αυτή τη χούφτα των επιχειρήσεων. Έτσι, μπορεί να απολαμβάνουμε ποιοτικές υπηρεσίες και εφαρμογές, αλλά ελλοχεύει ένας βασικός κίνδυνος. Όλα αυτά τα δεδομένα μπορεί να αξιοποιηθούν με ή χωρίς τη συγκατάθεση μας για θεμιτούς και αθέμιτους σκοπούς (από στοχευμένες διαφημίσεις και προτάσεις μέχρι κλοπές, απάτες, χειραγώγηση κοινού). Έτσι, το διαδίκτυο έπρεπε να “αποκεντρωθεί”, ώστε να μην είναι υπόλογο σε αυτές τις επιχειρήσεις.

Αυτό αποτέλεσε το βασικό κίνητρο του δημιουργού του Ethereum. Δηλαδή, η ανάπτυξη μίας πλατφόρμας, στην οποία είναι δυνατή η σχεδίαση αποκεντρωμένων και

peer-to-peer εφαρμογών για οποιαδήποτε χρήση, στην οποία θα υπάρχει και το κίνητρο του αντίστοιχου νομίσματος.

Επόμενως, θα ήταν εφικτό να επαναπροσδιορίσουμε το μοντέλο client-server, καθιστώντας αχρείαστους τους διαμεσολαβητές και τα third parties. Στην ουσία αποτελεί μία γενίκευση της σκεπτικού που υπάρχει πίσω από το bitcoin. Θεωρητικά, υπάρχει συνδυασμός 2 παραγόντων: 1) Μόνο ο δημιουργός έχει έλεγχο(προσθήκη, επεξεργασία, διαγραφή) πάνω στα δεδομένα που δημιουργεί και εισάγει 2) τα δεδομένα αυτά μπορούν να ταξιδέψουν με τεράστιες ταχύτητες στο δίκτυο, ενημερώνοντας άμεσα όλους τους χρήστες.

2.2.2 Στοιχεία για τον δημιουργό

Το project του Ethereum επινοήθηκε και περιγράφτηκε από τον Vitalik Buterin (προγραμματιστής, με καταγωγή από τη Ρωσία και το Καναδά) (1994- τώρα), ο οποίος συνέγραψε και τη σχετική επιστημονική αναφορά. Ο ίδιος είναι συνεργάτης του περιοδικού Bitcon Magazine.

Στη διαδρομή της ανάπτυξης του Ethereum, μία σειρά από ερευνητές συνέβαλλαν καθοριστικά στην επιτυχία της πλατφόρμας. Ο Dr Gavin Good (θεωρείται συνιδρυτής) συνέγραψε το yellow paper για το ethereum. Συγκεκριμένα, περιέγραψε τις τεχνικές λεπτομέρειες για όλη τη λειτουργία του EVM (ethereum virtual machine) που διαχειρίχεται όλο το ledger και εκτελεί τα smart contracts. Ο Dr. Joseph Lubin (θεωρείται και συνιδρυτής) μέσω συγκεκριμένης start-up εταιρείας, που αξιοποιεί τη πλατφόρμα του Ethereum για τη σχεδίαση αποκεντρωμένων εφαρμογών, ώστε να διευρυνθεί το κοινό του Ethereum.

Πέρα από τους επώνυμους συνεργάτες, υπήρξαν αρκετοί υποστηρικτές που βοήθησαν στα πρώτα βήματα του project. Το εγχείρημα είχε ανάγκη από οικονομική στήριξη. Έτσι, διάφοροι ενδιαφερόμενοι συνεισέφεραν στο Ethereum με την αγορά Ether. Με αυτό το τρόπο συγκεντρώθηκαν πάνω από 18 εκ δολλάρια για να πάρει “σάρκα και οστά” η πλατφόρμα.

2.2.3 Στάδια ανάπτυξης

Η ανάπτυξη του δικτύου του Ethereum έχει περάσει από αρκετά στάδια, τα οποία είναι διακριτά μεταξύ τους. Κάθε στάδιο σηματοδοτούσε και την υιοθέτηση μία σειράς σημαντικών αλλαγών. Κάποιες από τις μεταβολές αυτές πήραν και τη μορφή hard fork, καθώς επηρέασαν καθοριστικά τη λειτουργικότητα του Ethereum.

Τα στάδια αυτά πήραν κωδικές ονομασίες και διάκριση μεταξύ τους ορίστηκε με βάση τον αριθμό των μπλοκ:

Block #0

Frontier: το αρχικό στάδιο του Ethereum, που διήρκησε από τις 30/07/2015 μέχρι και το Μάρτη του 2016

Block #200.000

Ice Age (Hard Fork): η αύξηση του difficulty υπολογίζεται πλέον εκθετικά, ώστε να έχουμε ομαλή μετάβαση στο PoS

Block #1,150,000

Homestead: το δεύτερο στάδιο του Ethereum, το οποίο ανακοινώθηκε το Μάρτιο του 2016

Block #1,192,000

DAO (Hard Fork): έλαβε χώρα, ώστε να αποζημιώσει τους θύματα ενός χακαρισμένου DAO contract. Υπήρξε η αφορμή για τη διάσπαση του Ethereum με το Ethereum Classic σε δύο διαφορετικά blockchain συστήματα.

Block #2,463,000

Tangerine Whistle(Hard Fork): μεταβλήθηκε ο τρόπος με τον οποίο γινόταν ο υπολογισμός του gas

Block #2,675,000

Spurious Dragon: έγινε εισαγωγή μηχανισμών για την αποτελεσματικότερη αντιμετώπιση των DoS επιθέσεων και του double-spend προβλήματος.

Block #4,370,000

Metropolis Byzantium: Το Metropolis είναι το τρίτο στάδιο του Ethereum, το οποίο ξεκίνησε τον Οκτώβριο του 2017. Περιλαμβάνει το hard fork Byzantium.

Block #7,280,000

Constantinople: αναπροσαρμόστηκε ο μηχανισμός του block reward

2.2.4 Το τρέχον market Capitalization

Η τρέχουσα ονομαστική αξία του Ether είναι $ 172.42 και το σύνολο των νομισμάτων που βρίσκονται σε κυκλοφορία είναι 108.045.965 Ether. Αυτό αντιστοιχεί σε ένα τρέχον Market Capitalization της τάξης των $18.683.665.710. Ανήκει στα large cap κρυπτονομίσματα.

Από την εμφάνιση της πλατφόρμας του Ethereum, η ονομαστική αξία του Ether βρισκόταν σε χαμηλά επίπεδα. Από την άνοιξη του 2017, άρχισε να παρουσιάζει σταδιακή αύξηση με αποκορύφωμα τον Ιανουάριο του 2018. Από εκεί και μετά, παρουσιάζει συνεχώς αυξομειώσεις σε χαμηλότερα επίπεδα.

Η ονομαστική αξία του Ether (ETH) παρουσίασε:

1. ιστορικό υψηλό, τα $1432,88, στις 13/01/2018. Η αξία αυτή αντιστοιχούσε σε $35.400.735.922 Market Capitalization.
2. ιστορικό χαμηλό, τα $0,420897, στις 21/10/2015. Η αξία αυτή αντιστοιχούσε σε $33.150.826 Market Capitalization.

Σχήμα 10: Το market Capitalization του ethereum

2.2.5 Η νομισματική πολιτική

Η νομισματική πολιτική του Ethereum περιλαμβάνει τους κανόνες έκδοσης νέων νομισμάτων και τις αλλαγές στο mining reward. Όπως όλα τα κρυπτονομίσματα, έτσι και στο δίκτυο του Ethereum υπάρχει μηχανισμός για την έκδοση νέων νομισμάτων(ether) μέσα στο δίκτυο. Βέβαια, ακολουθεί μία διαφορετική προσέγγιση στη διαδικασία αυτή.

Βασικές μονάδες του Ether είναι οι εξής:

Πίνακας 6: Βασικές νομισματικές μονάδες του Ethereum

Ονομασία	Αξία σε Ether	Αξία σε Wei
Ether	1	10^{18}
Finney	10^{-3}	10^{15}
Szabo	10^{-6}	10^{12}
Wei	10^{-18}	1

Το πλήθος των νομισμάτων που μπορούν να μπουν σε κυκλοφορία στο δίκτυο του Bitcoin έχει άνω όριο. Συγκεκριμένα, το άνω όριο αυτό προσεγγίζει τον αριθμό των 21 εκ νομισμάτων. Σε αντίθεση με αυτή τη λογική, το Ethereum δε θα διαθέτει τέτοιο όριο ακόμα. **Θεωρητικά, υπάρχει δυνατότητα να κυκλοφορήσουν άπειρα νομίσματα, όσο το σύστημα λειτουργεί άρτια.** Οι σχεδιαστές της πλατφόρμας προτίμησαν να χρησιμοποιήσουν μία πολιτική έκδοσης που να ενθαρρύνει τη συμμετοχή στο δίκτυο.

Τη χρονική στιγμή που γράφονται αυτά, το πλήθος των νομισμάτων ether που βρίσκονται σε κυκλοφορία είναι: 107,700,654.41 νομίσματα.

Βέβαια, δεν έχουν προκύψει όλα από τη διαδικασία του mining. Ένα σημαντικό κλάσμα προέκυψε από presale. Το πλήθος αυτών ήταν περίπου 60 εκ ether. Παράλληλα, περίπου 12 εκ ether συγκεντρώθηκαν από την Ethereum foundation, με σκοπό να ενισχυθούν οικονομικά όσοι συνεισέφεραν στο project και ο εξοπλισμός. Δηλαδή, κυκλοφορούν κατά προσέγγιση 72 εκ ether (72,009,990.50 για την ακρίβεια), τα οποία δεν έχουν προκύψει από τη διαδικασία του mining. Αναφερόμαστε στο 66.86 % της συνολικής κυκλοφορίας. Τα νομίσματα που έχουν προκύψει ως reward από τη διαδικασία του mining ανέρχονται σε 33 εκ ether περίπου (για την ακρίβεια 33,185,800.03) με ποσοστό 30.81 % επί της συνολικής κυκλοφορίας. Απομένει ένα ποσοστό της τάξης του 2.33 %(2,504,863.88) της συνολικής κυκλοφορίας, το οποίο αντιστοιχεί στο reward των miners, που ενώ κατάφεραν να βρουν την επιθυμητή λύση, το block τους δεν εισήχθη ποτέ στη blockchain. Η ανταμοιβή αυτή είναι γνωστή και ως uncle/aunt reward.

2.2.5.1 Οι μεταβολές στο reward του κάθε μπλοκ

Η ετήσια έκδοση νομισμάτων για το δίκτυο του Ethereum προσεγγίζει περίπου το 4,5% με 2 Ether ως reward για κάθε μπλοκ και ένα επιπρόσθετο 1,75 Ether για το uncle μπλοκ. Επίσης, προστίθονται και άλλα τέλη συναλλαγών στο reward ενός miner. Κάθε μπλοκ που παράγεται στο δίκτυο του Ethereum επιβραβεύει με ένα ποσό-reward τον επιτυχημένο miner. Επίσης ο ίδιος λαμβάνει περίπου 75% του reward του μπλοκ για κάθε uncle μπλοκ. Από τη λειτουργία του Ethereum, το reward έχει λάβει τις εξής τιμές:

Block 0 μέχρι και Block 4,369,999: 5 Ether

Block 4,370,000 μέχρι και 7,280,000: 3 Ether

Block 7,280,000 to now: 2 Ether

Οι μεταβολές δε προέκυψαν από κάποιο εσωτερικό κανονισμό του πρωτοκόλλου, όπως για παράδειγμα στη περίπτωση του Bitcoin. Αντιθέτως, προτάθηκαν για μία σειρά από λόγους και υιοθετήθηκαν εν τέλει. Ο ρυθμός έκδοσης νέων νομισμάτων επηρέασε και τη ταχύτητα παραγωγής των μπλοκ.

2.2.6 Transactions

2.2.6.1 Ορισμός

Με τον όρο transaction (συναλλαγή) στη πλατφόρμα του Ethereum αναφερόμαστε σε ένα πακέτο δεδομένων με ψηφιακή υπογραφή. Το πακέτο αυτό περιλαμβάνει ένα μήνυμα, το οποίο χρειάζεται να σταλεί σε έναν externally owned account.

2.2.6.2 Τα περιεχόμενα μιας transaction

Μία transaction περιλαμβάνει:

1. το αναγνωριστικό για τον παραλήπτη
2. μία υπογραφή, η οποία λειτουργεί ως αναγνωριστικό για τον αποστολέα
3. τη ποσότητα του ether που μεταβιβάζεται από τον αποστολέα στον παραλήπτη

4. ένα προαιρετικό data field
5. ένα παράγοντα με το όνομα STARTGAS, ο οποίος αντιστοιχεί στον μέγιστο αριθμό υπολογιστικών βημάτων που απαιτούνται για την εκτέλεση της συναλλαγής
6. ένα παράγοντα, με όνομα GASPRICE, ο οποίος αντιστοιχεί στο χρηματικό τέλος, το οποίο πληρώνει ο αποστολέας σε κάθε υπολογιστικό βήμα.

Οι 3 πρώτοι παράγοντες είναι κοινοί σε κάθε κρυπτονόμισμα. Το data field αξιοποιείται στις περιπτώσεις, όπου έχουμε υλοποίηση smart contract.

2.2.6.3 Η πολιτική τελών (transaction fees)

Οι 2 τελευταίοι παραπάνω παράγοντες εντάσσονται στη πολιτική, με την οποία το Ethereum εφαρμόζει τέλη στα transactions. Η πολιτική αυτή δεν είναι τόσο απλή, όπως στη περίπτωση του Bitcoin. Αντιθέτως, θεωρείται περισσότερο πολύπλοκη, καθώς λαμβάνει υπ'όψιν της το κόστος χρήσης του εύρους ζώνης(bandwith), το κόστος της αποθήκευσης και του υπολογισμού. **Ο λόγος της συγκεκριμένης επιλογής σχετίζεται με το γεγονός πως οι transactions του Ethereum αξιοποιούν bandwith, αποθηκευτικό χώρο και υπολογιστική ισχύ με βάση τις απαιτήσεις που υπάρχουν.** Κάτι τέτοιο σημαίνει πως δεν υπάρχει ούτε σταθερότητα ως προς τη χρήση αυτών των μεγεθών ούτε ικανότητα ασφαλούς πρόβλεψής τους.

Η πολιτική των τελών για τα transaction σκοπεύει κυρίως στην αντιμετώπιση των επιθέσεων τύπου DoS. Με σκοπό να εμποδίσουν τυχαία ή κακόβουλα infinite loops ή οποιαδήποτε άλλη μορφή υπολογιστικής εξάντλησης, για κάθε συναλλαγή απαιτείται ο ορισμός ενός ορίου υπολογιστικών βημάτων, τα οποία είναι απαραίτητα για την εκτέλεση του κώδικα.

Ο βασικός μηχανισμός πίσω από κάθε συναλλαγή ακολουθεί τα εξής βήματα:

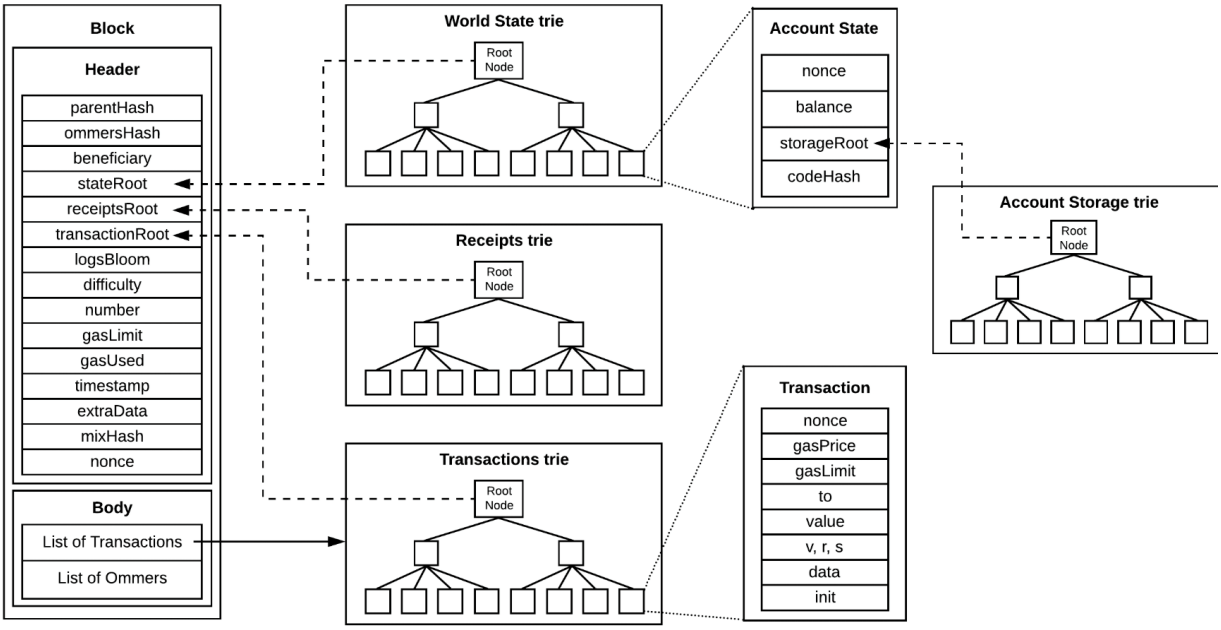
1. Κάθε συναλλαγή χρειάζεται να ορίσει ακριβώς τη ποσότητα του "gas" που έχει δυνατότητα να καταναλώσει (αντιστοιχεί στον παράγοντα STARTGAS). Επίσης, ορίζει το τέλος που επιθυμεί να πληρώσει ανά μονάδα gas (αντιστοιχεί στον παράγοντα GASPRICE). Στην αρχή της εκτέλεσης, ένα πόσο Ether (ίσο με το γινόμενο των STARTGAS και GASPRICE) αφαιρείται από τον λογαριασμό του αποστολέα της συναλλαγής.
2. Οποιαδήποτε λειτουργία κατά τη διάρκεια της εκτέλεσης της συναλλαγής, καθώς και κάθε υπολογιστικό βήμα καταναλώνει μία συγκεκριμένη ποσότητα από gas.
3. Αν μία συναλλαγή εκτελεστεί σωστά και πλήρως, καταναλώνοντας λιγότερο gas από το καθορισμένο όριο, αφήνει υπόλοιπο gas (αντιστοιχεί στο παράγοντα GAS_REM).
4. Στο τέλος της συναλλαγής, ο αποστολέας της συναλλαγής λαμβάνει ένα πόσο, ίσο με GAS_REM * GASPRICE και ο νικήτης miner λαμβάνει ένα επιπρόσθετο reward ίσο με (STARTGAS – GAS_REM) * GASPRICE.
5. Αν μία συναλλαγή δε έχει επαρκές gas κατά διάρκεια της εκτέλεσής της, τότε όλη η εκτέλεση αντιστρέφεται. Εντούτοις, η συναλλαγή θεωρείται έγκυρη και η μόνη επίδραση που έχει είναι να επιστρέψει τη ποσότητα startgas * gasprice στο miner.

2.2.7 Η δομή ενός μπλοκ

Ένα block στη περίπτωση του Ethereum blockchain αποτελείται από 17 διαφορετικά στοιχεία. Τα πρώτα 15 (παρουσιάζονται παρακάτω) συνθέτουν το block header. Τα υπόλοιπα συνιστούν την transaction list.

Το block header αποτελείται από τα εξής πεδία:

1. **Parent hash:** αποτελεί το hash value του parent block header
2. **Ommers/Uncle** hash: αποτελεί το hash value της λίστας των ommer/uncle μπλοκ
3. **Beneficiary:** αντιστοιχεί σε μία 20-byte διεύθυνση, στην οποία μεταφέρονται όλα τα block rewards
4. **State Root**: αποτελεί το hash value του root node του state trie, τα οποία υπολογίζονται από τη στιγμή που οι συναλλαγές ενός μπλοκ έχουν τελειώσει
5. **Transactions Root:** αποτελεί το hash value του root node της δομής trie, το οποίο περιλαμβάνει κάθε συναλλαγή του transaction list του μπλοκ
6. **Receipts Root:** αποτελεί το hash value του root node της δομής trie, το οποίο περιλαμβάνει τα αποδεικτικά στοιχεία για κάθε συναλλαγή του transaction list του μπλοκ
7. **Difficulty:** αποτελεί το difficulty κάθε μπλοκ. Η ποσότητα αυτή υπολογίζεται από το difficulty του προηγούμενου block και του δικού του timestamp
8. **Logs Bloom:** αντιστοιχεί σε ένα bloom filter
9. **Number:** αντιστοιχεί στον αριθμό των ancestor μπλοκ, τα οποία υπάρχουν πίσω από το τρέχον μπλοκ
10. **Gas Limit:** αντιστοιχεί στη τρέχουσα μέγιστη απαιτούμενη δαπάνη σε gas για το μπλοκ
11. **Gas Used:** αντιστοιχεί στη συνολική ποσότητα gas, που χρησιμοποιήθηκε στις συναλλαγές του μπλοκ
12. **Timestamp:** αντιστοιχεί στη χρονική στιγμή που δημιουργήθηκε το τρέχον μπλοκ σε ώρα Unix
13. **Extra data:** αποτελεί ένα byte-πίνακα, μεγέθους μέχρι και 32 bytes, ο οποίος περιλαμβάνει επιπρόσθετες πληροφορίες, σχετικά με το μπλοκ
14. **Mix Hash:** αποτελεί ένα hash value, μεγέθους 32 byte, το οποίο πιστοποιεί πως έχει ξοδευτεί μία επαρκής ποσότητα υπολογιστικής προσπάθειας μέσα στο συγκεκριμένο μπλοκ
15. **Ommer/Uncle Block Header:** αντιστοιχεί στο header των uncle μπλοκ



Σχήμα 11: Το ethereum μπλοκ

Παράλληλα, υπάρχει και ο παράγοντας Block Footer, το οποίο περιλαμβάνει το πεδίο Transaction Series

Για όλες τα παραπάνω hash values, η πλατφόρμα του Ethereum αξιοποιεί την κρυπτογραφική hash συνάρτηση Keccak-256.

Η Keccak-256 σχεδιάστηκε, ώστε να συμμετάσχει στον SHA-3 Cryptographic Hash Function Competition που πραγματοποιήθηκε το 2007 από το NIST (National Institute). Ο Keccak ήταν ο νικητήριος αλγόριθμος στη συγκεκριμένη διοργάνωση και ύστερα από τη προτυποίησή του, θα έπαιρνε το τίτλο του SHA-3. Ωστόσο, την περίοδο της ανάπτυξης του Ethereum, η προτυποποίηση του δεν είχε ακόμα ολοκληρωθεί. Το NIST προσάρμοσε ακόμα ορισμένες παραμέτρους του, κάτω από την πίεση της NSA. Κάτι τέτοιο, οδηγήγησε το Ethereum Foundation να υιοθετήσουν τον πραγματικό Keccak αλγόριθμο, όπως ακριβώς προτάθηκε από τους δημιουργούς του, παρά το SHA-3 standard που τροποποίησε το NIST.

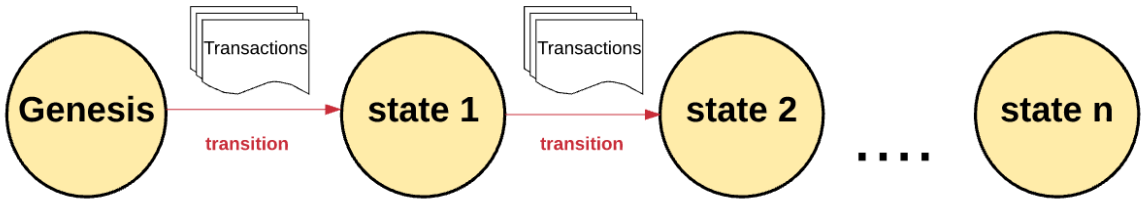
2.2.8 Το blockchain

Τη στιγμή που γράφονται όλα αυτά το blockchain του Ethereum μετρά 8,669,864 blocks.

2.2.8.1 Το ethereum blockchain ως state machine

Το blockchain του Ethereum ουσιαστικά λειτουργεί **ως transaction based state machine, δηλαδή οι αλλαγές στο state βασίζονται στις συναλλαγές.** Αφετηρία είναι η genesis state, και αντιστοιχεί στην απουσία κάθε αλλαγής μέσα το δίκτυο. Όταν μία συναλλαγή εκτελείται, από το genesis state μεταβαίνουμε σε ένα final state. Σε εκείνη τη χρονική στιγμή, το τρέχον state αναπαριστά το final state. Στα χαρακτηριστικά του κάθε

νέου state, χρειάζεται να συμφωνεί όλο το δίκτυο(να επιτυγχάνει consensus δηλαδή). Σε αντίθετη περίπτωση, πολλαπλά state ή ταυτόχρονες αλυσίδες θα οδηγούσαν σε σύγχυση. Προκειμένου να εμποδίζεται κάτι τέτοιο, το Ethereum αξιοποιεί ένα μηχανισμό, ο οποίος ονομάζεται GHOST("Greedy Heaviest Observed Tree"). Η λογική πίσω από το πρωτόκολλο ορίζει πως επιλέγουμε το μονοπάτι του blockchain, το οποίο αντιστοιχεί στα περισσότερα υπολογιστικά βήματα.



Σχήμα 12: Το blockchain του Ethereum

Κάθε state περιλαμβάνει χιλιάδες συναλλαγές, ο οποίες ενσωματώνονται σε μπλοκ.

Η blockchain του Ethereum παρουσιάζει αρκετά κοινά χαρακτηριστικά με τη περίπτωση του Bitcoin. Ωστόσο, παρουσιάζει ορισμένες διαφορές. Η βασική διαφορά σχετίζεται με την αρχιτεκτονική του blockchain. Στη περίπτωση του Bitcoin, το περιλαμβάνει μόνο ένα αντίγραφο της λίστας των συναλλαγών. Αντιθέτως, στο Ethereum περιλαμβάνει και αντίγραφο της λίστα των συναλλαγών και τη πιο πρόσφατη κατάσταση.

2.2.8.2 Ο αλγόριθμος για το validation του μπλοκ

Ο βασικός αλγόριθμος επιβεβαίωσης της εγκυρότητας ενός μπλοκ στο Ethereum ακολουθεί τα εξής βήματα:

1. Ελέγχουμε αν το αμέσως προηγούμενο μπλοκ υπάρχει και είναι έγκυρο.
2. Ελέγχουμε αν το timestamp του τρέχοντος μπλοκ είναι μεγαλύτερο από αυτό του αμέσως προηγούμενου και μικρότερο από μία χρονική στιγμή t (προκύπτει αν προσθέσουμε 15 λεπτά στο τρέχον timestamp).
3. Ελέγχουμε αν μία σειρά από παράγοντες του μπλοκ είναι έγκυροι (block number, difficulty, transaction root, uncle root, gasLimit).
4. Ελέγχουμε αν είναι έγκυρο το proof of work του μπλοκ.
5. Ορίζουμε ένα παράγοντα S_0, ο οποίος αντιστοιχεί στο state, όπως αυτό προέκυψε από το προηγούμενο μπλοκ.
6. Ορίζουμε τον παράγοντα TX, ο οποίος αντιστοιχεί στο transaction list του μπλοκ με n συναλλαγές. Για κάθε συναλλαγή, από το 0 μέχρι το n-1, ορίζουμε την επόμενη κατάσταση S_{i+1} ως αποτελέσμα του συνδυασμού της τρέχουσας κατάστασης S_i και της αντίστοιχης συναλλαγής TX_i, όπου i είναι αριθμός της συναλλαγής. Αν κάποιο βήμα από τα παραπάνω παρουσιάσει κάποιο λάθος ή το συνολικό gas που καταναλώθηκε είναι μεγαλύτερο από το gasLimit, επιστρέφεται error.

7. Αν δεν υπάρχει κάποιο error, ορίζουμε S_FINAL το S_n και αποστέλλουμε το reward στον επιτυχημένο miner.
8. Τέλος, ελέγχουμε αν το Merkle tree root του state S_FINAL είναι ίσο με το final state root, το οποίο παρέχεται από το block header. Αν ναι το μπλοκ θεωρείται έγκυρο. Διαφορετικά, θεωρείται άκυρο.

Η προσέγγιση αυτή μπορεί να φαίνεται αναποτελεσματική με τη πρώτη ματιά, καθώς απαιτεί την αποθήκευση ολόκληρου του state σε κάθε μπλοκ, αλλά στη πραγματικότητα τα αποτελέσματα είναι αρκετά γρήγορα. Αυτό προκύπτει από το γεγονός πως το state αποθηκεύεται σε μία δομή δέντρου (Patricia tree), και έτσι οι προσπελάσεις είναι πιο γρήγορες. Επιπρόσθετα, επειδή όλη η πληροφορία του state είναι μέρος του αμέσως προηγούμενου μπλοκ, δεν είναι απαραίτητη η αποθήκευση ολόκληρου του blockchain history σε ένα μπλοκ.

2.2.9 Η διαδικασία του mining

Το mining της πλατφόρμας του Ethereum, κατά τα πρώτα στάδια της ανάπτυξής του, παρουσίαζε αρκετά κοινά χαρακτηριστικά με τη περίπτωση του Bitcoin. Το σύστημα του Ethereum εξασφαλίζει μία σειρά από υπηρεσίες μέσα από τη διαδικασία του mining, όπως:

1. Έκδοση νέων νομισμάτων σε κυκλοφορία
2. Επιβεβαίωση των συναλλαγών
3. Ασφάλεια και ακεραιότητα στην υποδομή του δικτύου

2.2.9.1 Τα χαρακτηριστικά του Ethash

Το Ethereum αξιοποιεί ένα proof of work αλγόριθμο, ο οποίος ονομάζεται Ethash. Ο αλγόριθμος αυτός αποτελεί μία τροποποιημένη έκδοση του αλγορίθμου Dagger Hashimoto. Οι miners παράγουν νέα μπλοκ και το υπόλοιπο δίκτυο ελέγχει την εγκυρότητά τους. Ένα μπλοκ θεωρείται έγκυρο, αν και μόνο αν, ικανοποιεί τα κριτήρια του proof of work για μία δοσμένη τιμή του difficulty. Το πρωτόκολλο του Ethereum σκοπεύει να περάσει σε ένα νέο στάδιο και να αξιοποίησει νέο αλγόριθμο για το mining. Ο αλγόριθμος αυτός ονομάζεται Casper και ανήκει στην ομάδα των proof-of-stake.

Θα περιγράψουμε σε γενικές γραμμές τον αλγόριθμο Ethash και στην συνέχεια θα προχωρήσουμε σε ορισμένες εξειδικευμένες τεχνικές λεπτομέρειες για αυτόν. Η τιμή του difficulty προσαρμόζεται δυναμικά, έτσι ώστε να παράγεται ένα νέο μπλοκ κάθε 12 δευτερόλεπτα. Επομένως, το block time για τη περίπτωση ethereum επιδιώκεται να διατηρείται στα 12 λεπτά.

Ο Ethash ακολουθεί την εξής λογική:

1. Επιλέγει μία σειρά από τυχαία δεδομένα, τα οποία βρίσκονται αποθηκευμένα σε ένα μεγάλο dataset (με το όνομα DAG).
2. Επιλέγει τυχαία ορισμένες συναλλαγές από οποιοδήποτε μπλοκ.
3. Τα 2 παραπάνω δεδομένα αποτελούν είσοδο για τη κρυπτογραφική συνάρτηση Keccak-256, η οποία παράγει ένα hash value.

4. Το παραγόμενο hash value για να είναι έγκυρο(και άρα να είναι νικητής και ο αντίστοιχος miner), χρειάζεται να βρίσκεται κάτω από όριο που ορίζει το difficulty της διαδικασίας.
5. Ο πρώτος miner, ο οποίος καταφέρνει να βρει ένα “έγκυρο” hash value, είναι και αυτός που λαμβάνει το transaction reward και τα υπόλοιπα τέλη της συναλλαγής.

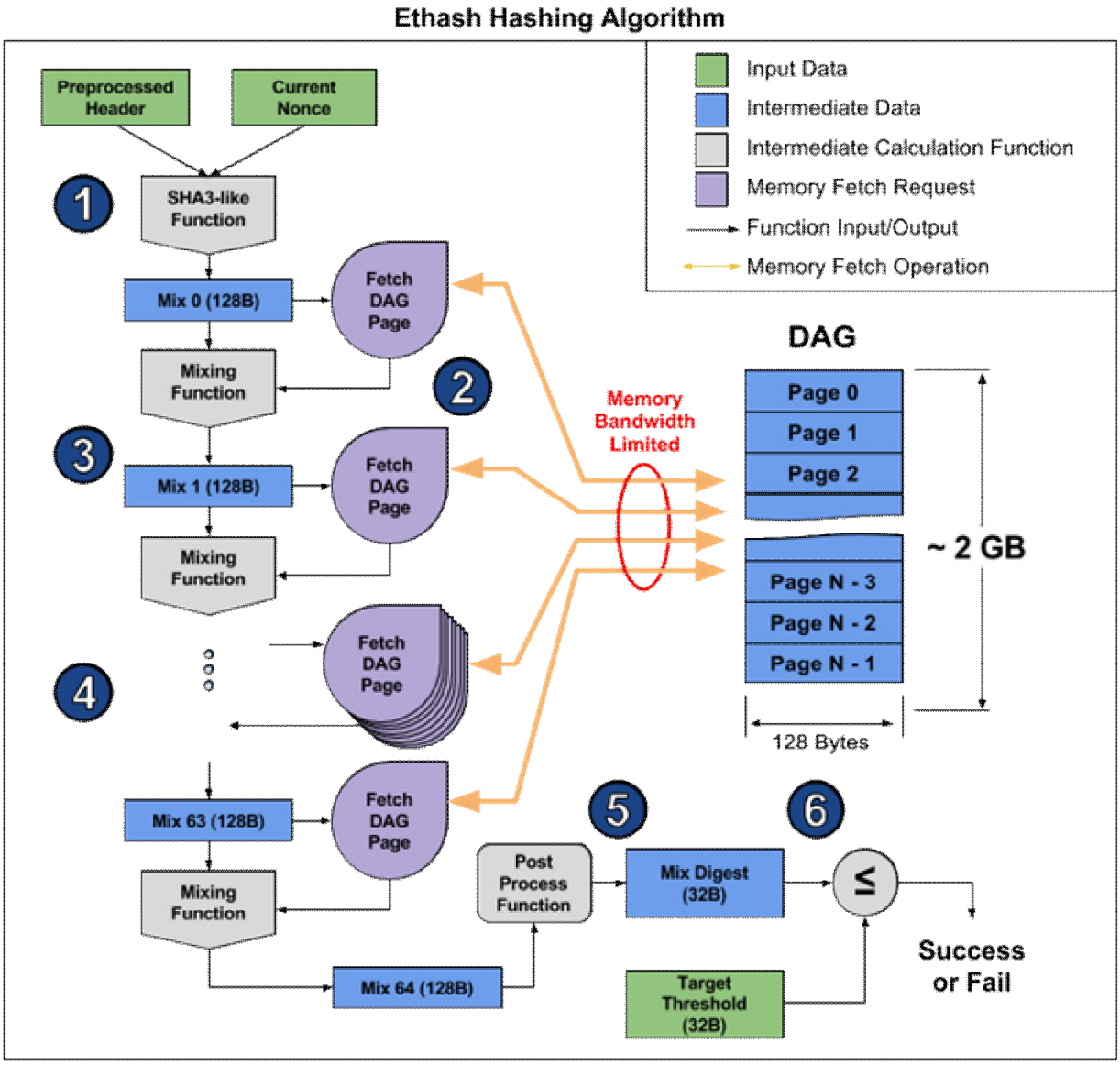
Η παραπάνω διαδικασία απαιτεί την αποθήκευση ολόκληρου του DAG, ώστε να είναι σε θέση κάθε φορά ο miner να επιλέγει τυχαία δεδομένα από αυτό. Αυτό σημαίνει πως το υπολογιστικό πρόβλημα το οποίο επιλύεται στον Ethash δεν απαιτεί μεγάλη υπολογιστική ταχύτητα(προερχόμενη από την αντίστοιχη υπολογιστική ισχύ). Αντιθέτως, εξαρτάται την απαιτούμενη ποσότητα μνήμης, η οποία χρησιμοποιείται για την αποθήκευση και ανάκτηση των δεδομένων. Ο αλγόριθμος Ethash, δηλαδή, θεωρείται memory-hard. Με λίγα λόγια, όσο περισσότερη μνήμη αξιοποείται από έναν miner, τόσο πιο εύκολα θα υπολογίσει το απαιτούμενο target.

2.2.9.2 Περιγραφή του Proof-of-Work Ethash

Η ροή του αλγορίθμου Ethash περιλαμβάνει τα εξής βήματα:

1. Από το πιο πρόσφατο μπλοκ, λαμβάνεται το προεπεξεργασμένο header και το τρέχον nonce. Οι δύο αυτοί παράγοντες συνδυάζονται και εισέρχονται στη κρυπτογραφική συνάρτηση Keccak-256. Παράγεται ένα αρχικό αποτελέσμα, μεγέθους 128 byte, το οποίο ονομάζεται Mix 0.
2. Με βάση το αποτέλεσμα Mix 0, επιλέγουμε μία σελίδα(μεγέθους 128 byte) από το DAG.
3. Το Mix 0 συνδυάζεται με την επιλεγμένη από το DAG σελίδα. Ο συνδυασμός αυτός αξιοποιείται για τη παραγωγή του επόμενου παράγοντα Mix, στη προκειμένη του Mix 1.
4. Τα βήματα 2 και 3 επαναλαμβάνονται 64 φορές, παράγοντας στη τελική το Mix 64.
5. Το αποτέλεσμα Mix 64 επεξεργάζεται περαιτέρω, ώστε να περιοριστεί στα 32 byte. Ο νέος παραγόμενος παράγοντας ονομάζεται Mix Digest.
6. Πραγματοποιείται σύγκριση ανάμεσα στο παραγόμενο Mix Digest και στο Target Threshold(το τρέχον με βάση το difficulty του mining). Αν το Mix Digest είναι μικρότερο ή ίσο του Target Threshold, τότε το τρέχον nonce θεωρείται επιτυχημένο. Το μπλοκ τώρα μπορεί να μεταδοθεί μέσα στο δίκτυο του ethereum. Σε αντίθετη περίπτωση, το τρέχον nonce θεωρείται άκυρο και ο αλγόριθμος εκτελείται ξανά με ένα διαφορετικό nonce (είτε αυξάνεται το τρέχον είτε επιλέγεται ένα νεό αυτή τη φορά)

Οι παράγοντες Mix της επαναληπτικής διαδικασίας προκύπτουν από τον αλγόριθμο Fnv (ακρωνύμιο για το Fowler–Noll–Vo). Ο αλγόριθμος fnv υλοποιεί μία μη-κρυπτογραφική hash συνάρτηση. Σχεδιάστηκε από τους Landon Curt Noll, and Kiem-Phong Vo.



Σχήμα 13: Υλοποίηση Proof-of-Work Ethash

2.2.9.3 Mining rewards

Ένας επιτυχημένος PoW miner λαμβάνει:

1. Ένα στατικό block reward για το “νικητήριο” μπλοκ της τάξης των 3.0 Ether ακριβώς.
2. Όλους τους παράγοντες gas, οι οποίοι έχουν ξοδευτεί για το συγκεκριμένο μπλοκ.
3. Ένα extra reward για τα Uncles, τα οποία περιλαμβάνεται στο νεόκοπο μπλοκ. Το reward για αυτή τη περίπτωση ανέρχεται στα 7/8 του στατικού block reward (συγκεκριμένα στα 2.625 ether). Επιτρέπονται μέχρι και 2 uncles για κάθε μπλοκ.

Ο Ethash αξιοποιεί ένα DAG(directed acyclic graph) για την υλοποίηση του. Ένα DAG παράγεται κάθε περίπου 100 ώρες(~5 ημέρες). Το χρονικό διάστημα αυτό ονομάζεται (mining) epoch για τη περίπτωση του ethereum και αντιστοιχεί σε 30000 νέα μπλοκ. Το DAG δε παραμένει σταθερό, αντιθέτως αυξάνεται σε κάθε mining epoch. Θεωρείται αρκετά σημαντικό να γνωρίζουμε το τρέχον και το μελλοντικό μέγεθος του DAG, καθώς

επιδρά καταλυτικά στη ταχύτητα του mining. Είναι προφανές πως αν η μνήμη του συστήματος του miner αδυνατεί να υποστηρίξει τις απαιτήσεις του DAG(δεν επιτρέπει τέτοια χωρητικότητα), καθίσταται στην ουσία άχρηστη.

Ο χρόνος αύξησης του DAG σχετίζεται απευθείας με το χρόνο δημιουργίας ενός νέου μπλοκ. Βέβαια, αυτό στη περίπτωση του Ethereum ποικίλλει. Η παραγωγή ενός νέου μπλοκ ενδέχεται να διαρκέσει από 10 έως 60 δευτερόλεπτα. Για το λόγο αυτό, η mining epoch αντιστοιχεί στον αριθμό των μπλοκ. Για το ethereum έχει υπολογιστεί πως γενικά το DAG αυξάνεται κατά 0,72 φορές το χρόνο. Η παραγωγή ενός νέου DAG διαρκεί ένα μεγάλο χρονικό διάστημα. Η παραγωγή του σχετίζεται με τον αριθμό των μπλοκ που έρχονται σε κυκλοφορία. Τη στιγμή που γράφονται αυτά, το μέγεθος του DAG ανέρχεται περίπου στα 3,26 GB. Βρισκόμαστε, επίσης, στη mining epoch #289, με τον αριθμό των μπλοκ να είναι στα 8676044. Ο μέσος χρόνος δημιουργίας ενός νέου μπλοκ είναι περίπου στα 13,36 s.

2.3 Ripple (XRP)

Υπάρχει μία σύγχυση γύρω από το Ripple, καθώς πολλές φορές το κρυπτονόμισμα, η πλατφόρμα, η εταιρεία που τη συντηρεί ταυτίζονται λανθασμένα. Αν θέλουμε να είμαστε αυστηροί στους ορισμούς μας, το Ripple αντιστοιχεί στην ονομασία της εταιρίας, που πάρεχει υπηρεσίες για την αποστολή χρημάτων παγκοσμίως.

Ο όρος XRP αντιστοιχεί στο ψηφιακό νόμισμα που υιοθετείται στις συναλλαγές. Το πρωτόκολλο που χρησιμοποείται από τους nodes του δικτύου ονομάζεται rippled. Πολλές φορές χρησιμοποιούμε καταχρηστικά τον όρο Ripple για τη περιγραφή είτε της πλατφόρμας δικτύου είτε του νομίσματος που αξιοποιεί. Αυτό δεν είναι σωστό, αν θέλουμε να κάνουμε χρήση αυστηρής ορολογίας.

2.3.1 Σκοπός δημιουργίας

Είναι γνωστό πως το πρωτόκολλο HTTP προσέφερε εκρηκτικές διαστάσεις στο διαδίκτυο, επιτρέποντας την αμεσότατη επικοινωνία ανάμεσα στους χρήστες. Ωστόσο, μία σειρά από άλλα συστήματα, όπως το τραπεζικό, δεν επιτρέπει τη ταχύτατη μετάδοση των συναλλαγών. Ένας βασικός λόγος σχετίζεται με τα απαρχαιομένα συστήματα που αξιοποιούν οι τραπεζικοί οργανισμοί για αυτή την συνδιαλλαγή. Παράλληλα, μία σειρά από εφαρμογές μεταφοράς χρημάτων, όπως το Swift, το MoneyGram και η Western Union παρέχουν αργές και ακριβές υπηρεσίες στους χρήστες.

Σε όλα αυτά έρχεται να προστεθεί και η ίδια η δομή του τραπεζικού συστήματος. Δεν υπάρχει ένα ενιαίο δίκτυο στο οποίο συμμετέχουν όλες οι τράπεζες και μέσω του οποίου πραγματοποιούν τις μεταξύ τους συναλλαγές. Έτσι, δεν υπάρχει ευθεία επικοινωνία ανάμεσα στους τραπεζικούς οργανισμούς. Αντιθέτως, η επικοινωνία αυτή συχνά απαιτεί μία σειρά από ενδιάμεσους κόμβους, ώστε να πραγματοποιηθεί με επιτυχία. Επαναλαμβάνουμε πως το “ταξίδι” αυτό είναι χρονοβόρο και δαπανηρό για τους χρήστες.

Ακόμα και να υπήρχε ευθεία επικοινωνία ανάμεσα στους τραπεζικούς οργανισμούς, δεν είναι εγγυημένο ότι υπάρχουν και τα ανάλογα αποθέματα για να πραγματοποιηθεί μία συναλλαγή. ‘Εστω ότι ο Γιώργος θέλει να στείλει 100 € από την τράπεζα Α στην Ιωάννα στο λογαριασμό της στη τράπεζα Β. Και οι 2 τράπεζες (Α και Β) διαθέτουν επαρκή αποθέματα σε € και έτσι διευκολύνεται η συναλλαγή. Τί γίνεται όμως αν μεταφέρω χρήματα από τη τράπεζα Α(με έδρα την Ιαπωνία) στη τράπεζα Β(με έδρα την Αλβανία); Αυτό σημαίνει πως η τράπεζα Α θα στείλει το ποσό σε Yen και τράπεζα Β θα πρέπει να λάβει το ποσό σε Λεκ. Χρειάζεται, δηλαδή, να έχουμε μετατροπή γιεν σε λεκ. Ωστόσο, συχνά κάτι τέτοιο δεν είναι εφικτό, καθώς είναι αδύνατο κάθε τράπεζα να διαθέτει επαρκές συνάλλαγμα για κάθε συναλλαγή. Με βάση τα παραπάνω, παρατηρούμε πως προκύπτει μία πολύπλοκη κατάσταση με κόστος χρόνου και χρήματος. Σε αυτήν, ακριβώς, την πολύπλοκη κατάσταση, ήρθε να απαντήσει το δίκτυο και το πρωτόκολλο του Ripple. Βασικό κίνητρο της ανάπτυξής τους ήταν:

1. Η απευθείας πραγματοποίηση συναλλαγών ανάμεσα στους τραπαεζικούς οργανισμούς.
2. Η μείωση των τελών ανάμεσα στις συναλλαγές.

Τα Ripple Labs, είχαν ως στόχο τη δημιουργία του “Internet of Value”, έναν τρόπο για να γίνονται συναλλαγές το ίδιο ταχύτατα, όπως μεταφέρεται η

πληροφορία. Μέσα από το RippleNet, ένας χρήστης ούτε θα περιμένει αρκετά για την πραγματοποίηση μίας συναλλαγής ούτε θα το κοστίσει και τόσο. Η φιλοσοφία γύρω από το RippleNet απέχει αρκετά από αυτή του Bitcoin. Στη περίπτωση του Ripple, δημιουργήθηκε ένα δίκτυο, ώστε να βελτιώσει την αποτελεσματικότητα του τραπεζικού συστήματος. Σε αντίθεση με τη περίπτωση του Bitcoin, όπου επιχειρείται η παράκαμψη του για τη πραγματοποίηση των συναλλαγών.

2.3.2 Στοιχεία για το δημιουργό

Η ανάπτυξη της πλατφόρμας και του δικτύου του Ripple πιστώνεται σε μία σειρά από πρόσωπα. Πρώτος, **ο Ryan Fugger** συνέλαβε την ιδέα το 2004, εργαζόμενος πάνω σε ένα σύστημα ηλεκτρονικών συναλλαγών στο Βανκούβερ. Στη συνέχεια, ανέπτυξε τη πρώτη εφαρμογή του συστήματος, το RipplePay.com.

Φτάνουμε μέχρι και το 2011, τον Μάιο, όταν ο Jed McCaleb ξεκίνησε την ανάπτυξη ενός συστήματος ψηφιακών νομισμάτων. Ωστόσο, ο έλεγχος για την εγκυρότητα των συναλλαγών θα βασιζόταν σε αλγόριθμο εξασφάλισης συναίνεσης(consensus algorithm), και όχι μέσα από τη διαδικασία του mining. Τον Αύγουστο του 2012, ο Jed McCaleb προσέλαβε Chris Larsen και μαζί προσέγγισαν τον Ryan Fugger, ώστε να αξιοποιήσουν την ιδέα του. Ήρθαν σε συμφωνία και οι 2 μαζί δημιούργησαν την εταιρεία OpenCoin. Η συγκεκριμένη εταιρεία ξεκίνησε την ανάπτυξη του πρωτοκόλλου του Ripple(RTXP) και του δικτύου των συναλλαγών. Στις 26 Σεπτεμβρίου 2013, η OpenCoin μετονομάζεται και επίσημα σε Ripple Labs. Την ίδια περίοδο, ο CTO της εταιρείας, Stefan Thomas, ανακοινώνει το source κώδικα για την υλοποίηση των κόμβων του P2P δικτύου.

Ο **Jed McCaleb** είναι Αμερικάνος προγραμματιστής και επιχειρηματίας. Μέχρι το 2013, διατήρουσε τη θέση του CTO της Ripple. Στη συνέχεια, συμμετείχε στην ίδρυση του Stellar. Ο ίδιος έχει υπάρξει δημιουργός της P2P εφαρμογής του eDonkey. Ο **Chris Larsen** είναι επιχειρηματίας. Αποτέλεσε συνιδρυτής μίας σειράς από start-ups, που σχετίζονται με P2P εφαρμογές δανεισμού. Ο ίδιος το 1996, συνίδρυσε την E-Loan, μία αρκετά επιτυχημένη επιχείρηση ηλεκτρονικών δανείων.

2.3.3 Το τρέχον market Capitalization

Η τρέχουσα ονομαστική αξία του Bitcoin είναι $8.866,41 και το συνολικό πλήθος των νομισμάτων σε κυκλοφορία είναι 17.954.887 BTC. Αυτό οδηγεί σε ένα τρέχον Market Capitalization της τάξης των $159.195.348.743. Η τρέχουσα ονομαστική αξία του XRP είναι $0.272118 και το συνολικό πλήθος των νομισμάτων σε κυκλοφορία είναι 43.121.735.112 XRP. Αυτό αντιστοιχεί σε ένα τρέχον Market Capitalization της τάξης των $ 11.734.178.900. Από την εμφάνιση του XRP μέχρι και το καλοκαίρι του 2017, η ονομαστική του αξία και αντίστοιχα το Market Cap του βρίσκονταν σε χαμηλά επίπεδα. Από εκεί και ύστερα μέχρι και το Δεκέμβρη του 2017, εκτινάχθηκε. Στη συνέχεια, παρουσίαζε αυξομειώσεις, σε χαμηλότερα όμως επίπεδα. Η ονομαστική αξία του XRP παρουσίασε:

1. ιστορικό υψηλό ($3,84) στις 04/01/2018. Αυτό αντιστοιχούσε σε 123.834.712.592$ Market Cap.
2. ιστορικό χαμηλό ($0.002802) στις 07/07/2014. Αυτό αντιστοιχούσε σε 24.096.300$ Market Cap.

Το XRP κατατάσσεται στα large cap νομίσματα.

Σχήμα 14: Το market Capitalization του Ripple

2.3.4 Η νομισματική πολιτική

Σε αντίθεση με άλλα κρυπτονομίσματα, τα Ripple Labs έχουν επιλέξει να τροφοδοτήσουν το δίκτυο του Ripple με ένα συνολικό απόθεμα 100.000.000.000 νομίσματα XRP. Το Ripple δε διαθέτει διαδικασία mining και όλο το απόθεμα αυτό έχει "κοπεί" από τους ιδρυτές πριν από τη κυκλοφορία της πλατφόρμας. Το πλήθος αυτό έχει κατανεμηθεί ως εξής:

- 20 δις νομίσματα XRP έχουν προσφερθεί του ιδρυτές Jec Macaleb, Chris Larsen και Arthur Britto.
- 7 δις νομίσματα XRP έχουν δωρηθεί στη Ripple Labs.
- 20 δις νομίσματα XRP έχουν αποτελέσει αντικείμενο αγοράς για εταιρίες και ιδιώτες.
- 55 δις νομίσματα XRP είχαν δεσμευτεί σε smart contract το 2017.

Με βάση το τελευταίο, κάθε χρόνο θα μεταφέρονται στο δίκτυο 1 δις νομίσματα XRP, έως ότου εξαντληθούν, προσεγγίζοντας τα 100 δις. Κάθε νόμισμα XRP έχει τη δυνατότητα να διαιρεθεί σε μικρότερες μονάδες, που φτάνουν μέχρι και τα 6 δεκαδικά ψηφία. Η μικρότερη δυνατή μονάδα είναι στα 0.000001 XRP.

Προκειμένου να αποφευχθεί η κακόβουλη συμπεριφορά του spam, απαιτείται ελάχιστη κατάθεση στα 20 XRP για κάθε νέο χρήστη. Με αυτό το τρόπο, έχει τη δυνατότητα κάποιος να εξασφαλίσει πρόσβαση σε wallet για το συγκεκριμένο κρυπτονόμισμα. Επαναλαμβάνουμε πως για κάθε συναλλαγή, καταστρέφεται ένα ποσό ως τέλος. Τα τέλη αυτά αντιστοιχούν πλέον σε νομίσματα, που δε μπορούμε να τα αξιοποιήσουμε ξανά. Θεωρητικά, όσο μειώνεται το πλήθος των νομισμάτων σε κυκλοφορία, τόσο μεγαλύτερη αξία θα αποκτήσουν με το πέρασμα του χρόνου. Ακόμα δεν έχει οριστεί κάποιος τρόπος για να κυκλοφορήσουν νέα και παραπάνω νόμισματα στο δίκτυο. Έχουν υπάρξει ορισμένες προτάσεις για αυτό το σενάριο, αλλά απέχουμε ακόμα από αυτό το σημείο.

2.3.5 Τα χαρακτηριστικά μιας XRP transaction

Μία συναλλαγή είναι ο μόνος τρόπος για να μεταβληθεί το XRP Ledger. Οι συναλλαγές είναι τελικές, μόνο αν έχουν υπογραφεί (ψηφιακά), υποβληθεί, γίνει αποδεκτές σε ένα validated ledger version (ακολουθώντας τους κανόνες της διαδικασίας του consensus). Οποιαδήποτε αλλαγή σε επίπεδο χρήστη στο ledger είναι αποτελέσμα κάποιας συναλλαγής. Η συναλλαγή στο δίκτυο του Ripple λαμβάνει ένα πιο αφηρημένο ορισμό, εκφράζοντας πληρωμές, μεταβολές σε στοιχεία χρηστών κα. Κάθε συναλλαγή εγκρίνει μία ή περισσότερες αλλαγές στο ledger και είναι υπογεγραμμένες ψηφιακά από ένα χρήστη. Ο μόνος τρόπος εισαγωγής νέων αλλαγών σε έναν λογαριασμό ή σε οτιδήποτε άλλο μέσα στο ledger, πραγματοποιείται μέσα από μία συναλλαγή.

Ορισμένα ledger έχουν τη δυνατότητα να επεξεργάζονται ψευδοσυναλλαγές (pseudo-transactions), οι οποίες δεν έχουν υπογραφεί ή υποβληθεί ακόμα και περιμένουν αποδοχή από το consensus. Οι αποτυχημένες συναλλαγές (απέτυχαν να γίνουν αποδεκτές) ενσωματώνονται επίσης στα ledgers, διότι προσαρμόζουν το υπόλοιπο των XRP, που είναι προορισμένα για τέλη anti-spam.

Οι συναλλαγές που ενσωματώνονται σε ένα validated ledger version, έχουν οδηγήσει επιτυχώς στην αλλαγή του ledger, ή έχουν επεξεργασθεί χωρίς να έχουν πραγματοποιήσει την απαιτούμενη ενέργεια τους. Επιτυχημένες συναλλαγές λαμβάνουν το tesSuccess result code, το οποίο δείχνει τις αλλαγές που εφαρμόστηκαν στο ledger. Οι αποτυχημένες συναλλαγές στο ledger λαμβάνουν το tec class result code.

Κάθε συναλλαγή που περιλαμβάνεται στο ledger history, καταστρέφει ένα πόσο XRP ως κόστος συναλλαγής, ανεξάρτητα αν έχουν λάβει ένα tes ή tec result code. Το ακριβές ποσό που οδηγείται σε καταστροφή προσδιορίζεται από το περιεχόμενο της συναλλαγής. Χρειάζεται, επίσης, να γίνει διάκριση ανάμεσα στις **υποψήφιες** και στις **valitaded** συναλλαγές: Οι μεν πρώτες εκφράζουν τις συναλλαγές που προτείνονται για εισαγωγή στο επόμενο ledger, ενώ οι δεύτερες εκφράζουν αυτές που έχουν ήδη εισαχθεί σε ένα validated ledger. Μόνο αν τα αποτελέσματα μίας συναλλαγής βρεθούν σε ένα validated ledger, μπορεί να θεωρηθούν μόνιμα.

Κάθε συναλλαγή διαθέτει ένα μοναδικό hash value ως αναγνωριστικό. Ο server παρέχει ένα hash value ως απάντηση στην υποβολή μίας συναλλαγής από ένα χρήστη. Το hash value της συναλλαγής θα μπορούσε να θεωρηθεί και ως απόδειξη πληρωμής - proof of payment(δε παραπέμπει σε κάποιον αλγόριθμο), καθώς κάθε χρήστης που συμμετέχει στο δίκτυο μπορεί να εντοπίσει τη συναλλαγή μέσω αυτού και να εστιάσει στις πληροφορίες της. Μέσω αυτής της διαδικασίας επιβεβαιώνεται ή όχι η τελική της κατάσταση.

Για τις **αποτυχημένες** συναλλαγές, χρεώνεται και σε αυτές τέλος. Μπορεί να φαίνεται άδικο, αλλά η ύπαρξη του είναι ωφέλιμη για τη πλατφόρμα:

1. Οι συναλλαγές που αποτυγχάνουν, δημιουργούν ζήτημα στην αρίθμηση των συναλλαγών. Η διατήρηση, έτσι, των αποτυχημένων συναλλαγών στο σύστημα, διορθώνει όποια προβλήματα προκύψουν στη διάταξη τους.
2. Η μετάδοση μίας συναλλαγής στο δίκτυο, αυξάνει το φόρτο του. Με τη προσθήκη αυτού του τέλους, καθίσταται ακόμα πιο δύσκολο σε οποιοδήποτε κακόβουλο χρήστη να γεμίσει το δίκτυο με αποτυχημένες συναλλαγές.
3. Το τέλος αυτό είναι σχετικά μικρό, ώστε να επιβαρύνει τους χρήστες, εκτός και αν μεταδίδουν ένα μεγάλο πλήθος από συναλλαγές.

2.3.5.1 Η διαδικασία του validation, της υπογραφής και της υποβολής μιας συναλλαγής

Σε ένα αποκεντρωμένο XRP Ledger, μία ψηφιακή υπογραφή αποδεικνύει πως μία συναλλαγή εγκρίνεται. Μόνο αυτές οι συναλλαγές έχουν τη δυνατότητα να υποβληθούν στο δίκτυο και να ενσωματωθούν σε ένα validated ledger. Μία υπογεγραμμένη συναλλαγή καθίσταται και αμετάβλητη και η υπογραφή αυτή δε μπορεί να συσχετισθεί με οποιαδήποτα άλλη συναλλαγή. Μία συναλλαγή μπορεί να εγκριθεί μέσα από μία σειρά υπογραφών:

1. Απλή υπογραφή με συσχέτιση του master private key με την διεύθυνση του αποστολέα, αξιοποιώντας μία AccountSet transaction
2. Απλή υπογραφή που σχετίζεται με ένα κανονικό private key και μία διεύθυνση, αξιοποιώντας μία SetRegularKey transaction.
3. Πολλαπλές υπογραφές, που αντιστοιχούν σε μία λίστα από αποστολείς, μαζί με μία διεύθυνση, αξιοποιώντας μία SignerListSet transaction

Η υπογραφή και η υποβολή μίας συναλλαγής

Η αποστολή μίας συναλλαγής στο XRP ledger περιλαμβάνει αρκετά βήματα:

1. Δημιουργία μίας μη υπογεγραμμένης συναλλαγής σε μορφή JSON.
2. Αξιοποίηση μίας σειράς από τις παραπάνω υπογραφές για την έγκριση της συναλλαγής
3. Υποβολή της συναλλαγής στο rippled server. Αν μία συναλλαγή είναι διαμορφωμένη σωστά, ο server εφαρμόζει τη συναλλαγή αυτή στο τρέχον ledger version που διαμορφώνει και την αναμεταδίδει στο P2P δίκτυο.
4. Η διαδικασία του consensus αποφασίζει αν αυτές οι προσωρινές συναλλαγές θα ενταχθούν στο επόμενο validated ledger.
5. Οι servers που εκτελούν το πρωτόκολλο rippled εφαρμόζουν τις συναλλαγές αυτές στο ledger.
6. Εάν υπάρχει επαρκής αριθμός από έμπιστους validators, που συνέθεσαν το ίδιο ledger, αυτό δηλώνεται ως validated.

2.3.6 Η περιγραφή ενός ledger version

Το blockchain του Ripple δεν παρουσιάζει την ίδια ακριβώς δομή με το αντίστοιχο άλλων κρυπτονομισμάτων. Δε διαθέτει διατεταγμένα μπλοκ με «αλυσιδωτή» σύνδεση μεταξύ τους. Αντιθέτως, μοιάζει πιο πολύ με λίστα, η οποία αποτελείται από **ledger version ή στιγμιότυπα ledger.** Τα ledger versions κατατάσσονται στη σειρά μέσα στο XRP Ledger.

Ενα απλό ledger version αποτελείται από τα εξής στοιχεία:

- Ένα **ledger header**: περιλαμβάνει το ledger index, το hash value των δεδομένων του ledger και άλλα metadata.
- Ένα **transaction tree**: περιλαμβάνει τις συναλλαγές που ενσωματώθηκαν στο προηγούμενο μπλοκ.
- Ένα **state tree**: περιλαμβάνει ledger αντικείμενα, με δεδομένα, υπόλοιπα, στοιχεία για το τρέχον ledger

Πιο αναλυτικά, το state tree, που διαθέτει κάθε ledger, είναι μία δομή δεδομένων με τη μορφή δέντρου. Κάθε αντικείμενο μέσα σε αυτή τη δομή αναγνωρίζεται από ένα 256 bit ID object. Το αντικείμενο αυτό συνήθως ονομάζεται **ledger node**, χωρίς να ταυτίζεται με τους nodes του P2P δικτύου. Αν το ID object το μετατρέψουμε σε JSON μορφή, θα λάβουμε ένα index 64 hex χαρακτήρων. Κάθε object στο state tree έχει ένα μοναδικό ID, ώστε να έχουμε πρόσβαση σε αυτό. Δε πρέπει να συγχέουμε το συγκεκριμένο index με το ledger index που χαρακτηρίζει κάθε ledger version (επί της ουσίας δείνει και την αριθμητική σειρά κατάταξης)

Κάθε συναλλαγή διαθέτει ένα μοναδικό hash, ώστε να την αναγνωρίζουμε στο transaction tree. Το αναγνωριστικό hash value σχετίζεται μόνο με τις συναλλαγές που έχουν υπογραφεί. Αντιθέτως, τα δεδομένα ενός transaction object, όπως τα metadata, δε περιλαμβάνονται στο hash.

2.3.7 Genesis ledger

Έχει αναφέρει πως στη πλατφόρμα του Ripple δεν υπάρχουν block με την ίδια έννοια που υπάρχουν και στις blockchain άλλων κρυπτονομισμάτων. Αντιθέτως, πολλαπλά στιγμιότυπα ledger, διατεταγμένα στη σειρά, συνθέτουν το XRP Ledger, με τη μορφή μίας λίστας. Επομένως, έχουμε τη δυνατότητα να αναφερόμαστε σε XRP genesis ledger.

Το πρώτο διαθέσιμο ledger version διαθέτει το index 32570 και όχι το 0. Αυτό δεν έχει προκύψει από κάποια σύμβαση του XRP, αλλά λόγω ενός τεχνικού λάθους. Τον Ιανουάριο του 2013, ένα bug στο server του Ripple προκάλεσε την απώλεια των ledger header. Μπορεί όλα τα δεδομένα να σώθηκαν, ωστόσο δεν ήταν εφικτή η ανασύνθεση των ledger. ‘Ετσι, οι συναλλαγές της προηγούμενης κατάστασης, διοχετεύτηκαν τυχαία σε άλλα ledger. Χωρίς τα ledger header, δεν υπάρχει η δυνατότητα για ανακατασκευή των ledger. Κάτι τέτοιο θα απαιτούσε τη γνώση του hash value του ledger N-1 για να δομήσεις ξανά το ledger N. Η διαδικασία αυτή, βέβαια, θεωρείται αρκετά πολύπλοκη.

Πίνακας 7: Genesis Ledger Ripple

Ledger summary

Ledger index:	GENESIS
Closed on:	Jan 01, 2013, 02:21:10 AM UTC
Total coins:	99,999,999,999.99632 XRP
Ledger hash:	4109C6F2045FC7EFF4CDE8F9905D19C28820D86304080FF886B299F0206E42B5
Parent hash:	60A01EBF11537D8394EA1235253293508BDA7131D5F8710EFE9413AA129653A2
Accounts hash:	3806AF8F22037DE598D30D38C8861FADF391171D26F7DE34ACFA038996EA6BEB
Transactions hash:	0000000000000000000000000000000000000000000000000000000000000000

2.3.8 Το XRP Ledger

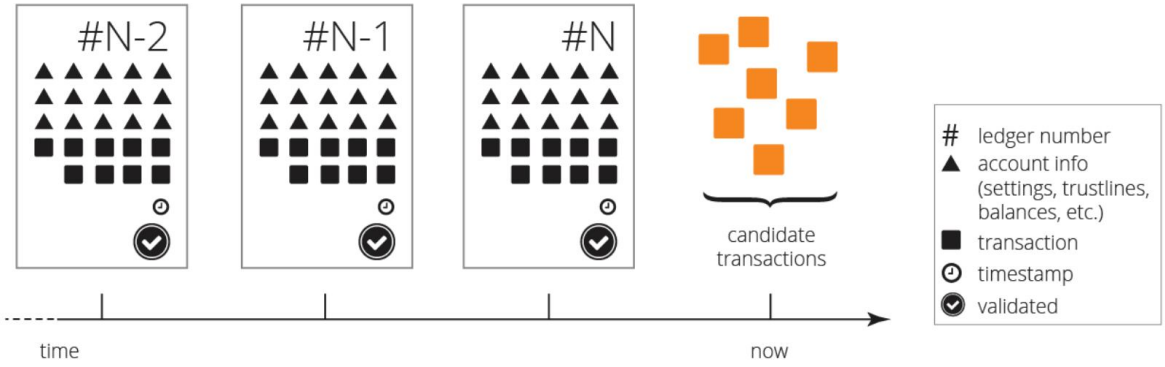
Το XRP Ledger αποτελεί, όπως έχουμε αναφέρει, **μία καθολικά κατανεμημένη βάση δεδομένων, ανοιχτή προς όλους τους νέους χρήστες**. Νέοι μεμονωμένοι χρήστες εμπιστεύονται την λειτουργία του ledger, χωρίς να διαμεσολαβεί κάποιος τρίτος ή κάποια κεντρική αρχή για τη πιστοποίησή της. Το πρωτόκολλο του rippled επιβάλλει στους servers του δικτύου συγκεκριμένη μεταχείριση στο ledger, βασισμένη σε κοινά συμφωνημένους κανόνες. Κάθε κόμβος, που εκτελεί το rippled πρωτόκολλο, διατηρεί ένα πλήρες αντίγραφο του ledger. Στο P2P δίκτυο των servers, μεταδίδονται ανάμεσα τους οι υποψήφιες συναλλαγές (candidate transactions). Η διαδικασία του consensus αποφασίζει για το ποιες συναλλαγές θα ενταχθούν στη νέα έκδοση του ledger.

Το καθολικά καταναμημένο XRP ledger αποτελεί στη πραγματικότητα μία σειρά από μεμονωμένα στιγμιότυπα του ledger. Ονομάζονται αλλιώς και ledger version. Το πρωτόκολλο του rippled διατηρεί τις ledger versions στο εσωτερικό του. Κάθε ledger version διαθέτει ένα ledger index, το οποίο βεβαιώνει τη χρονολογική σειρά με την οποία έχουν προκύψει τα διαφορετικά ledger versions. Σε κάθε δοσμένη χρονική στιγμή, υπάρχει ένα τρέχον open ledger, ένα πλήθος από closed ledgers, που δεν έχουν ακόμα γίνει αποδεκτά από τη διαδικασία του consensus και ένας αριθμός από ledgers, που έχουν γίνει αποδεκτά από το consensus. Μόνο τα ledgers που έχουν γίνει validated (επιβεβαιωθεί) είναι έγκυρα και αμετάβλητα.

Κάθε ledger στιγμιότυπο διαθέτει 2 αναγνωριστικά. Το πρώτο είναι το ledger index, το οποίο στην ουσία ταυτίζεται με τον αριθμό ακολουθίας. Τα ledger στιγμιότυπα κατάσσονται σε αύξουσα σειρά. Δηλαδή, αν το τρέχον ledger version διαθέτει το ledger index 100, το προηγούμενο διαθέτει το ledger index 99 και το επόμενο θα έχει ledger version 101. Το άλλο αναγνωριστικό είναι το hash value των περιεχομένων του ledger version.

Οι servers προτείνουν υποψήφιες συναλλαγές, ώστε να ενσωματωθούν στο ledger. Με αυτό το τρόπο, δημιουργούνται αρκετά υποψήφια ledger version με ελαφρώς

διαφορετικά περιεχόμενα. Αυτά τα υποψήφια ledger version, διαθέτουν το ίδιο index, αλλά διαφορετικό hash value. Από όλα τα υποψήφια version, μόνο ένα θα θεωρηθεί validated. Τα υπόλοιπα θα απορριφθούν. Επομένως, έχουμε ακριβώς ένα hash value για κάθε ledjer index στο ledger history.

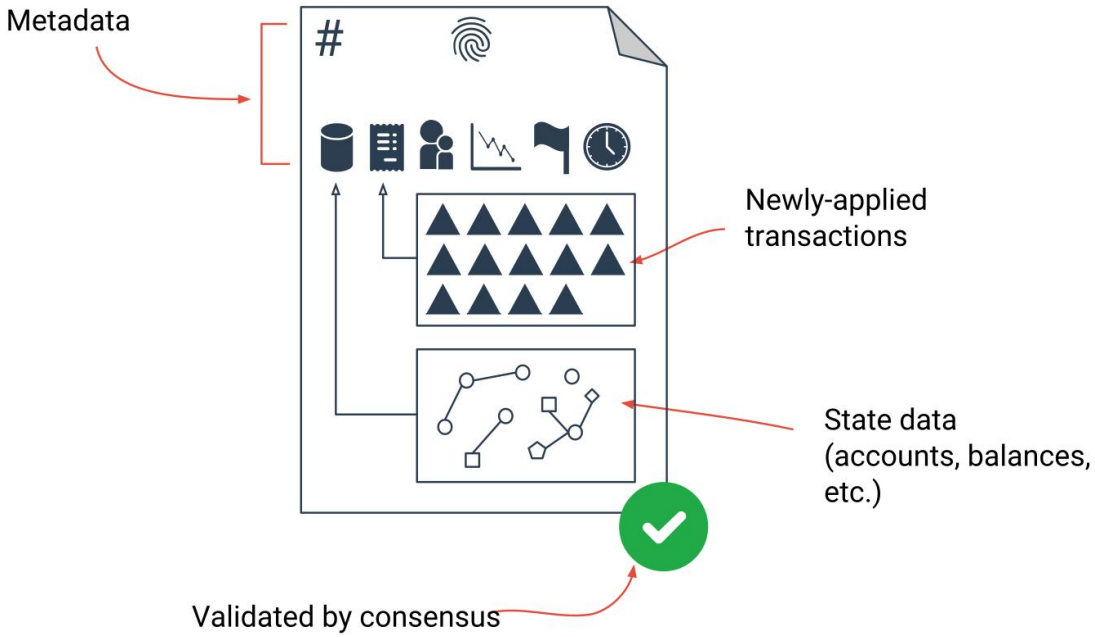


Σχήμα 15: Το XRP ledger history

Κάθε ledger στιγμιότυπο περιλαμβάνει επίσης και ένα σύνολο από συναλλαγές και metadata για αυτές. Το σύνολο των συναλλαγών που περιλαμβάνει ένα ledger στιγμιότυπο προσφέρει τη δυνατότητα αναδρομής σε οποιαδήποτε συναλλαγή στο ledger history. Αν, για παράδειγμα, το υπόλοιπο ενός λογαριασμού είναι διαφορετικό στο ledger N+1 από το ledger N, το ledger N+1 περιλαμβάνει τη συναλλαγή(ή συναλλαγές) που είναι υπεύθυνες για αυτή τη μεταβολή.

Το XRP Ledger ποτέ δε “κλείνει” ένα open ledger, ώστε να το μετατρέψει σε closed ledger. Αντιθέτως, ο server “πετάει” ένα open ledger και δημιουργεί ένα νέο closed ledger, εφαρμόζοντας συναλλαγές σε ένα προηγούμενο closed ledger. Στη συνέχεια, δημιουργεί ένα νέο open ledger, χρησιμοποιώντας ως βάση το πιο πρόσφατο closed ledger. Αυτή η πολύπλοκη συμπεριφορά αποτελεί συνέπεια του τρόπου επίλυσης του double-spend προβλήματος από τον αλγόριθμο του consensus.

Για ένα open ledger, οι servers τοποθετούν συναλλαγές με τη διάταξη με την οποία προέκυψαν, αλλά διαφορετικοί server μπορεί να παρατηρούν τις ίδιες συναλλαγές με διαφορετική διάταξη. Από τη στιγμή που απουσιάζει μία κεντρική αρχή, η οποία θα κρατά το χρόνο αυστηρά, οι servers ενδέχεται να διαφωνούν με την ακριβή διάταξη των συναλλαγών, που προέκυψαν περίπου την ίδια χρονική στιγμή. Επομένως, η διαδικασία υπολογισμού ενός closed ledger version, που θα επιλεγεί άμεσα για validation, είναι διαφορετική από τη διαδικασία σύνθεσης ενός νέου open ledger από τις προτεινόμενες συναλλαγές, όπως αυτές προκύπτουν χρονολογικά.



Σχήμα 16: XRP Ledger

Ένας server, για να δημιουργήσει ένα closed ledger, ξεκινά με ένα σύνολο από συναλλαγές και ένα προηγούμενο("parent") ledger version. Ο server τοποθετεί τις συναλλαγές σε κανονική διάταξη και στη συνέχεια εφαρμόζει σε αυτές το προηγούμενο ledger version.

2.3.9 Το XRP Ledger Πρωτόκολλο

Το P2P XRP Ledger δίκτυο αποτελείται από μία σειρά ανεξάρτητων XRP servers, που εκτελούν το πρωτόκολλο του rippled και λαμβάνουν και επεξεργάζονται συναλλαγές. Οι εφαρμογές που εκτελούν και αυτές το rippled πρωτόκολλο, υπογράφουν και στέλνουν ένα μεγάλο αριθμό συναλλαγών στους XRP servers. Με τη σειρά τους, οι servers αναμεταδίδουν τις συγκεκριμένες συναλλαγές μέσα στο δίκτυο για επεξεργασία. Τέτοιες εφαρμογές θα μπορούσαν να είναι mobile και web wallet, gateways σε τραπεζικούς οργανισμούς, πλατφόρμες ηλεκτρονικού εμπορίου κτλ.

Το XRP Ledger Consensus Protocol αποτελείται από 3 βασικά συστατικά στοιχεία:

- **Deliberation (διαβούλευση),** κατά τη διάρκεια της οποίας, κάθε κόμβος προτείνει ένα σύνολο από συναλλαγές για εισαγωγή στο ledger, βασισμένο σε προτάσεις που έχει λάβει από άλλους έμπιστους nodes. Όταν ένας node πιστεύει πως έχει αρκετές προτάσεις που συμφωνούν μεταξύ τους, εφαρμόζει τις αντίστοιχες συναλλαγές πάνω στο προγενέστερο ledger, με βάση τους κανονισμούς του πρωτοκόλλου. Στη συνέχεια, εφαρμόζει validation στο νέο ledger.
- **Validation (επικύρωση),** στην οποία οι κόμβοι αποφασίζουν αν θα επικυρώσουν πλήρως ένα ledger, βασιζόμενοι σε validations, που έχουν προκύψει από "έμπιστους" κόμβους. Όταν προκύψει απαρτία (quorum) από validations για το

ίδιο ledger, το συγκεκριμένο ledger και οι πρόγονοι του θεωρούνται πλήρως validated και η κατάστασή τους αξιόπιστη και αμετάκλητη.

- **Preferred branch,** στο οποίο οι κόμβοι αποφασίζουν το branch στο οποίο επιθυμούν να δουλέψουν στο ledger history. Στη περίπτωση, της συμφόρησης του δικτύου ή της αποτυχίας byzantine, οι nodes αρχικά μπορεί να μην επικύρωσαν το ίδιο ledger για ένα δοσμένο αριθμό ακολουθίας. Με σκοπό να υπάρξει περαιτέρω πρόοδος και πλήρης επικύρωση και άλλων ledger, οι nodes αξιοποιούν το ledger history των έμπιστων validations, για να συνεχίσουν τη διαδικασία.

  Προχωράμε σε λεπτομερή περιγραφή των 3 αυτών βημάτων:

2.3.9.1 Deliberation

Το delibaration αποτελεί συστατικό στοιχείο της διαδικασίας του Ripple Consensus, στο οποίο οι κόμβοι επιχειρούν να συμφωνήσουν πάνω σε ένα σύνολο από συναλλαγές για τα ledger version που επικυρώνουν. Οι χρήστες της πλατφόρμας υποβάλλουν συναλλαγές σε ένα ή περισσότερους κόμβους μέσα στο δίκτυο, οι οποίοι με τη σειρά του αναμεταδίδουν τις συναλλαγές στο σύνολο του δικτύου. Κάθε κόμβος διατηρεί ένα σύνολο από συναλλαγές (που αναμένουν επιβεβαίωση) και δεν έχουν συμπεριληφθεί στο ledger. Έχοντας ως αφετηρία αυτό το σύνολο, κάθε κόμβος προτείνει επαναληπτικά νέα σύνολα από συναλλαγές. Η πρόταση αυτή λαμβάνει υπ'όψιν της μεμονωμένες συναλλαγές που προτείνονται από το UNL. Κάθε πρόταση $\mathbf{P_{T,r,L,i}}$ είναι ένα σύνολο από:

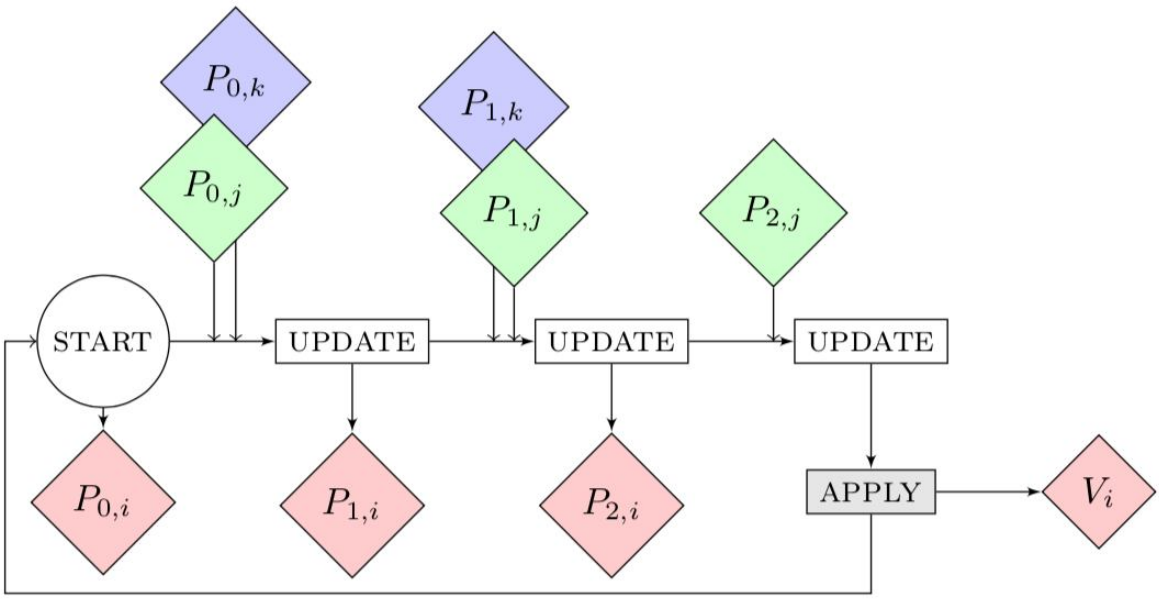
T, το προτεινόμενο από το node P_i σύνολο συναλλαγών

r, ο αριθμός του γύρου στον οποίο βρίσκεται η πρόταση

L, το προγενέστερο ledger στο οποίο θα εφαρμοστούν οι συγκεκριμένες συναλλαγές

i, το αναγνωριστικό του κόμβου P_i, που αναμεταδίδει την πρόταση

Όταν αρκετοί κόμβοι από το UNL προτείνουν το ίδιο σύνολο από συναλλαγές, ο κόμβος περνά στο βήμα του validation για το συγκεκριμένο σύνολο από συναλλαγές και ξεκινά τον επόμενο γύρο deliberation.



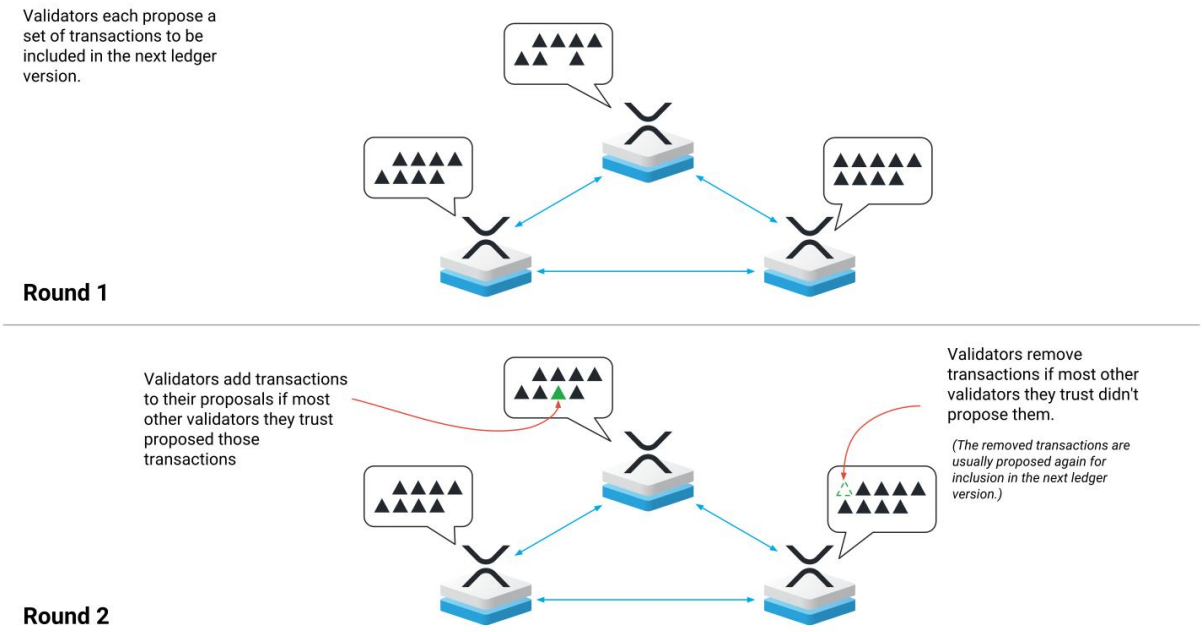
Σχήμα 17: Το XPR Ledger Consensus

Στο σχήμα παρουσιάζεται μία επισκόπηση της διαδικασίας του deliberation. Ένας node ξεκινά τη διαδικασία του deliberation, με τον πρώτο γύρο, και προτείνει ένα πρώτο σύνολο από συναλλαγές. Παράλληλα και ασύγχρονα, επεξεργάζεται νέες προτάσεις από "έμπιστους" κόμβου, διατηρώντας το σύνολο με τις πιο πρόσφατες από κάθε node. Οι προτάσεις που λαμβάνονται υπ'όψιν είναι μόνο αυτές που αναφέρονται στο ίδιο προγενέστερο ledger.

Ο κόμβος κανονικά ενημερώνει το προτεινόμενο σύνολο από συναλλαγές ως απάντηση στις πρόσφατα λαμβανόμενες προτάσεις. Η ενημέρωση γίνεται ως εξής: κάθε node ενσωματώνει τις προτεινόμενες συναλλαγές, που είναι παρούσες σε τουλάχιστον N από τις πιο πρόσφατες προτάσεις των nodes του UNL. Ο παράγοντας N είναι ένα κοινά συμφωνημένο κατώφλι, το οποίο αναπροσαρμόζεται σε κάθε γύρο. Ο παράγοντας αυτός ξεκινά από την απλή πλειοψηφία των nodes μέσα στο UNL, αλλά αυξάνεται όσο προχωρούν οι γύροι του deliberation. Αυτό εξασφαλίζει πως αργοί κόμβοι δεν θα μπορέσουν να εμποδίσουν στη τελική την επίτευξη σύγκλισης. Στην υλοποίηση του XRP Ledger, το κατώφλι (threshold) ακολουθεί την εξής πορεία 0.5 → 0.65 → 0.70 → 0.95, όσο αυξάνεται το r (οι γύροι του deliberation). Κάθε node ανακοινώνει την επίτευξη consensus όταν παρατηρεί την απαρτία από τους έμπιστους nodes να συμφωνούν σε ένα σύνολο από συναλλαγές. Στη συνέχεια, αξιοποιεί τις κοινά συμφωνημένες συναλλαγές για τη δημιουργία του επόμενου ledger, μεταδίδει το δικό του μήνυμα validation και ξεκινά ένα νέο γύρο deliberation.

Είναι σημαντικό να σημειώσουμε πως ένας node μπορεί να επικυρώσει μόνο ένα ledger με δοσμένο αριθμός σειράς. Στη πραγματικότητα, κάθε κόμβος μεταδίδει το validation μήνυμα στο δίκτυο για ένα συγκεκριμένο ledger, αν και εφόσον ο αριθμός ακολουθίας είναι μεγαλύτερος από κάθε ledger που επιβεβαιώθηκε προτύτερα από τον ίδιο node. Επομένως, αν κατά τη διάρκεια μίας διαδικασίας deliberation, ένας κόμβος αποφασίσει ότι δεν εργάζεται στο προτεινόμενο branch, θα το αλλάξει, ώστε να εργαστεί στο προτεινόμενο. Σε αυτό το σενάριο, ο node δε θα μπορεί να μεταδώσει ένα validation μήνυμα, αν δεν επιστρέψει στον αριθμό ακολουθίας που ήταν πριν την μεταβολή branch.

Στην υλοποιήση του deliberation στο XRP Ledger, το πρωτόκολλο ρυθμίζει χρονικές παραμέτρους για τις απαιτήσεις του συγχρονισμού και το τέλος της διαδικασίας. Επιπρόσθετες περίοδοι αναμονής ανάμεσα στους γύρους-φάσεις του deliberation εξισορροπούν τη διεκπεραιωτική ικανότητα και τη καθυστέρηση της επεξεργασίας των συναλλαγών, όπως επίσης και την επιβάρυνση του δικτύου από τις προτάσεις και τα σύνολα των συναλλαγών. Το πρωτόκολλο επίσης ρυθμίζει για το ποιες συναλλαγές θα είναι στην αρχική πρόταση, αλλά και την μεταχείριση των αποτυχημένων συναλλαγών, ώστε να συμπεριληφθούν σε επόμενο γύρο του deliberation.



Σχήμα 18: Η διαδικασία του validation στο XRP Ledger Consensus

2.3.9.2 Validation

Το Validation είναι το απλούστερο από τα 3 βήματα του consensus. Οι nodes του δικτύου ακούν μόνιμα το δίκτυο για νέα μηνύματα validation από τη λίστα με τους έμπιστους nodes(UNL). Αν ένας κόμβος P_i παρατηρήσει απαρτία από validations για ένα ledger, αποφασίζει τη τελική επικύρωσή του.

Το validation είναι το δεύτερο στάδιο της συνολικής διαδικασίας του consensus, όπου επιβεβαιώνεται ότι οι servers έχουν συμφωνήσει στα αποτελέσματα και δηλώνεται η τελική μορφή του νέου ledger στιγμιοτύπου. Στη σπάνια περίπτωση, όπου το πρώτο στάδιο του consensus αποτυγχάνει, το validation παρέχει μία ενημέρωση προς τους servers για το γεγονός αυτό, ώστε να πράξουν αναλόγως.

Το validation θα μπορούσε να χωριστεί σε δύο τμήματα:

- Υπολογισμός του τελικού ledger version με βάση το κοινά συμφωνημένο σύνολο συναλλαγών.
- Σύγκριση των αποτελεσμάτων και δήλωση του validated ledger στιγμιοτύπου, εάν έχει υπάρξει επαρκής αριθμός από έμπιστους validators που συμφωνούν.

Calculate and Share Validations

Όταν η διαδικασία του consensus φτάνει στο τέλος της, κάθε server ανεξάρτητα, αλλά ακολουθώντας τους ίδιους κανονισμούς, σχεδιάζει το νέο ledger version με βάση το κοινά συμφωνημένο σύνολο από συναλλαγές.

Οι κανόνες αυτοί είναι οι εξής:

- Ξεκινάμε από το άμεσως προηγούμενο validated ledger.

- Τοποθετούμε το κοινά συμφωνημένο σύνολο από συναλλαγές σε τέτοια διάταξη, ώστε κάθε server να το επεξεργάζεται με τον ίδιο τρόπο.
- Επεξεργαζόμαστε κάθε συναλλαγή με τη σειρά με βάση τις οδηγίες. Ενημέρωνουμε τα δεδομένα για το ledger state αναλόγως. Αν μία συναλλαγή δεν εκτελεστεί επιτυχώς, ενσωματώνεται σε αυτή ο κωδικός αποτελέσματος tec-class.
- Ενημερώνουμε το ledger header με τα ανάλογα metadata. Αυτό περιλαμβάνει τα δεδομένα όπως το ledger index, το αναγνωριστικό hash του άμεσως προηγούμενου validated ledger, το hash value των περιεχομένων του ledger.
- Υπολογίζουμε το αναγνωριστικό hash value για το νέο ledger version.

Σύγκριση των αποτελεσμάτων

Κάθε validator αναμεταδίδει τα δικά του αποτελέσματα με τη μορφή ενός υπογεγραμμένου μηνύματος. Το μήνυμα αυτό περιλαμβάνει το hash value του ledger version που μόλις υπολόγισαν. Τα μηνύματα αυτά ονομάζονται validations και επιτρέπει σε κάθε server να συγκρίνει το δικό του πρόσφατα υπολογισμένο ledger με αυτό που υπολόγισαν οι άλλοι.

Οι servers μέσα στο δίκτυο αναγνωρίζουν ως validated ένα ledger στιγμιότυπο αν υπάρχει μία ευρεία πλειοψηφία από ομότιμους χρήστες που έχουν και αυτοί μεταδώσει το ίδιο hash value. Προχωρώντας, οι συναλλαγές εφαρμόζονται σε αυτόν τον ενημερωμένο και επικυρωμένο ledger version με index N + 1 τώρα.

Στις περιπτώσεις, όπου ένας server αποτελεί μειοψηφία, δηλαδή έχοντας υπολογίσει ένα ledger version που διαφέρει από αυτά των άλλων ομότιμων, ο server αγνοεί το ledger version που υπολόγισε. Επαναλαμβάνει τον υπολογισμό ή ανακτά το σωστό ledger version από το δίκτυο.

Η αποτυχία εξασφάλισης ευρείας πλειοψηφίας ανάμεσα στα validations από το δίκτυο, υποδηλώνει πως ο όγκος των συναλλαγών είναι αρκετά υψηλός ή καθυστέρηση του δικτύου μεγάλη, ώστε να παραχθούν συνεπείς προτάσεις από τη διαδικασία του consensus. Όσο ο χρόνος περνά από την αρχή του consensus, γίνεται εξαιρετικά πιθανό ότι μία πλειοψηφία από servers έχουν λάβει το ίδιο σύνολο με συναλλαγές, όσο κάθε γύρος του consensus μειώνει τις διαφωνίες. Το XRP Ledger ρυθμίζει δυναμικά το κόστος των συναλλαγών και το χρόνο αναμονής για το consensus.

Μόλις φτάσουν σε ένα σημείο ευρείας πλειοψηφίας πάνω στα validations, οι servers πλέον ασχολούνται με το νέο validated ledger version me index N+1. Το consensus και το validation επαναλαμβάνεται, λαμβάνοντας υπ'όψιν νέες υποψήφιες συναλλαγές που δεν επιλέγησαν στον προηγούμενο γύρο.

2.3.9.3 Preferred Branch

Οι validators κανονικά επικυρώνουν μία λίστα-αλυσίδα από ledgers. Ωστόσο, κατά τη διάρκεια ασύγχρονων μεταδόσεων, συμφόρησης του δικτύου ή Byzantine αποτυχίας, δε λαμβάνονται επαρκείς validations για τη πλήρη επικύρωση ενός ledger με αποτέλεσμα να δημιουργούνται conflicts. Όταν συμβαίνει κάτι τέτοιο, ακολουθείται η στρατηγική της

προτεινόμενης αλυσίδας(preferred branch), ώστε να μπορούμε να συνεχίσουμε αποδοτικά προς τα εμπρός. Η διαδικασία αυτή βασίζεται σε ένα κοινό ιστορικό από τα πιο πρόσφατα validated ledgers.

Η διαδικασία-πρωτόκολλο του preffered branch ακολουθεί το εξής σκεπτικό: κάθε node θα πρέπει να λειτουργεί συντηρητικά και να αλλάζει branch μόνο αν γνωρίζει πως υπάρχουν αρκετοί κόμβοι που έχουν υποβληθεί στην αλυσίδα του ledger, ώστε καμία εναλλακτική αλύσιδα να μπορεί να τα υποστηρίξει. Το προτεινόμενο ledger εντοπίζεται, διατρέχοντας το ancestry tree (δομή δεδομένων με τη μορφή δέντρου), με αφετήρια το κοινό ancestor ledger από τα πιο πρόσφατα validated ledgers.

2.3.10 Το δίκτυο του Ripple

Το δίκτυο του Ripple αποτελείται από μία σειρά nodes, οι οποίοι εκτελούν το πρωτόκολλο rippled. Οι nodes, με βάση τη δραστηριότητά τους, διακρίνονται στις εξής κατηγορίες:

1) Validating nodes (ή απλά validator): οι συγκεκριμένοι κόμβοι παίζουν καθοριστικό ρόλο στη διαδικασία του consensus, καθώς αυτοί είναι που υπεύθυνοι για την επεξεργασία των υποψήφιων συναλλαγών και την απόφαση για τη σύνθεση των τελικών ledger version. Παράλληλα, οι validators αποφασίζουν μία σειρά άλλες παραμέτρους όπως για παράδειγμα το επιπρόσθετο κόστος των συναλλαγών.

Η λειτουργικότητα ενός validator απαιτεί περισσότερο φορτίο από έναν απλό κόμβο του δικτύου. Οι validators του δικτύου θα πρέπει να τηρούν ορισμένες προϋποθέσεις, ώστε να λειτουργούν ομαλά και αποτελεσματικά:

1. Συνεχής διαθεσιμότητα σημαίνει πως πρέπει να υπάρχει συνεχής πρόσβαση σε ένα τουλάχιστον validator. Κάτι τέτοιο προϋποθέτει συνεχή λειτουργία και προστασία από οποιονδήποτε παράγοντα μπορεί να τη διακόψει ή να τη παρεμποδίσει όπως διακοπές ρεύματος, κακόβουλοι χρήστες.
2. Συχνή ταύτιση και συμφωνία με το αποτέλεσμα της διαδικασίας του consensus. Αν αυτό δεν επιτυγχάνεται, σημαίνει πως ο validator εκτελεί ξεπερασμένο λογισμικό.
3. Ταχύτητα ως προς την μετάδοση των ψήφων, ώστε να καταφτάνουν σε όλους τους κόμβους πριν από τη λήξη κάθε γύρου του consensus.
4. Ο διαχειριστής του χρειάζεται να είναι σαφώς καθορισμένος και αναγνωρίζεται εύκολα από το δίκτυο.

Το πρωτόκολλο του rippled, προτείνει σε κάθε χρήστη μία λίστα από έμπιστους κόμβους, οι οποίοι αναλαμβάνουν το ρόλο του validator. **Η λίστα αυτή ονομάζεται UNL (unique node list) και περιλαμβάνει ένα υποσύνολο από validators του δικτύου.** Έχουν διατυπωθεί και προτάσεις, οι οποίες ισχυρίζονται πως κάθε χρήστης θα πρέπει να επιλέγει μόνος του τους validators που επιθυμεί, χωρίς τη διαμεσολάβηση του πρωτοκόλλου. Αυτή η πρόταση σκοπεύει στη μεγαλύτερη αποκέντρωση του δικτύου.

2) Stock nodes: γνωστοί και ως non-validating ή tracking nodes. Όπως φανερώνει και το όνομά τους, δε συμμέτεχουν στη διαδικασία του consensus ή στις διάφορες ψηφοφορίες που πραγματοποιούνται. Μπορεί κεντρικό ρόλο στο δίκτυο να έχουν οι

validators, ωστόσο οι stock nodes αναλαμβάνουν και αυτοί σημαντικές για το σύστημα υπηρεσίες όπως:

1. Προστασία από DoS επιθέσεις. Οι validators δημιουργούν ομάδες στο δίκτυο με τουλάχιστον 2 stock nodes, ώστε να υπάρχει επαρκής προστασία από κακόβουλες συμπεριφορές.
2. Παροχή πρόσβασης από εφαρμογές που εκτελούν το rippled
3. Αποθήκευση του XRP ledger history, ώστε να είναι διαθέσιμο σε όλο το ευρύ δίκτυο μέσω μίας διαδικασίας που ονομάζεται history sharding.

2.4 Dash (DASH)

2.4.1 Κίνητρα δημιουργίας

Μπορεί το Bitcoin να αποτελεί ένα ευρέως διαδεδομένο μέσο ηλεκτρονικών συναλλαγών (έχει το μεγαλύτερο Market Cap), ωστόσο διαθέτει ορισμένα μειονεκτήματα. Δύο χαρακτηριστικές του ελλείψεις είναι η αργή επεξεργασία των συναλλαγών και η απουσία πλήρους ανωνυμίας και ιδιωτικότητας, παράγοντες, που αποθαρρύνουν μία σειρά από χρήστες. Έτσι, δημιουργήθηκε η ανάγκη ανάπτυξης ενός νέου κρυπτονομίσματος ως μέσου ηλεκτρονικών συναλλαγών (στα πρότυπα του Bitcoin), το οποίο θα έλυνε τα ζητήματα αυτά. Από τη μία θα εξασφάλιζε τη δυνατότητα για άμεσες συναλλαγές με χαμηλά τέλη και από την άλλη θα αποτελούσε ένα ασφαλές περιβάλλον πλήρους ιδιωτικότητας για τους χρήστες. Με βάση αυτά τα χαρακτηριστικά αναπτύχθηκε το Dash.

2.4.2 Στοιχεία για το δημιουργό

Το Dash κυκλοφόρησε τον Ιανουάριο του 2014 από τον Evan Duffeld. Ο Evan Duffeld (1980-) είναι προγραμματιστής με καταγωγή από τις ΗΠΑ. Προτού ασχοληθεί με το Dash εργάστηκε σε πολλές εταιρείες, που δραστηριοποιούνται στον κλάδο της Πληροφορικής και στις τεχνολογίες αιχμής.

Η αρχική του ονομασία ήταν Xcoin. Ο ίδιος ο Duffeld είχε επισημάνει τα μειονεκτήματα στη χρήση του Bitcoin. Ωστόσο, γνώριζε πως δε θα μπορούσε να πείσει την ομάδα ανάπτυξης του Bitcoin για την εφαρμογή αυτών των αλλαγών. **Προέκυψε ως fork του Bitcoin πρωτοκόλλου και εντάσσεται στην ευρεία ομάδα των altcoins.** Τις πρώτες μέρες της κυκλοφορίας του υπήρξε δυσπιστία γύρω από τη χρήση του. Αναδιαμορφώθηκε και επανήλθε στη κυκλοφορία με το όνομα Darkcoin. Βέβαια, και πάλι αντιμετωπίστηκε με καχυποψία, καθώς γινόταν χρήση του στην αγορά του Dark Net. Το Μάρτιο του 2015, ανακατασκευάστηκε ξανά και επανακυκλοφόρησε με το όνομα Dash. Η ονομασία αυτή αποτελεί μία συντόμευση του όρου digital cash. Από τον Αύγουστο του 2016, το Dash αποσύρθηκε από τις συναλλαγές στο Dark Net.

2.4.3 Το τρέχον Market Capitalization

Το τρέχον Market Capitalization που παρουσιάζει το Dash ανέρχεται στα $661.174.669. Αυτό προκύπτει ως γινόμενο της τρέχουσας circulation supply που είναι 9.088.681 DASH και της τρέχουσας αξίας του, η οποία είναι $72.75

Η αξία του DASH παρουσίασε:

- ιστορικό υψηλό στις 20/12/2017, φτάνοντας στα $1.642,22. Αυτό αντιστοιχούσε σε market cap της τάξης των $638.744.422 USD.
- ιστορικό χαμηλό στις 14/02/2014, φτάνοντας στα $0,213899. Αυτό αντιστοιχούσε σε market cap της τάξης των $ 1.233.615 USD.

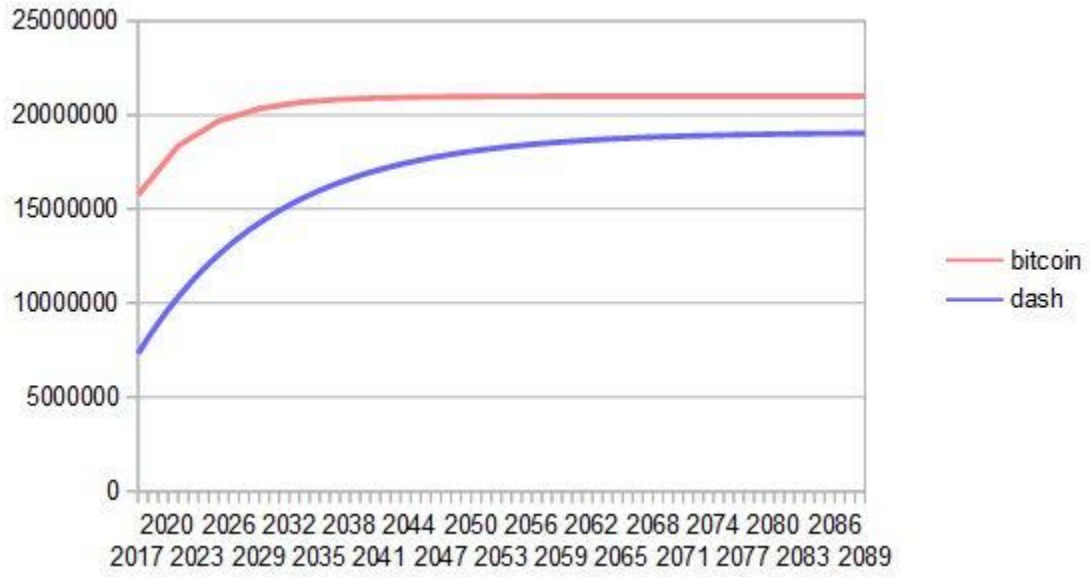
Το DASH, από τη κυκλοφορία του μέχρι και το Φεβρουάριο του 2017, παρουσιάζει χαμηλές πτήσεις, με χαμηλό market cap. Στη συνέχεια και μέχρι τα μέσα Δεκεμβρίου του 2017, παρουσιάζει ταχύτατα ανοδική πορεία, προσεγγίζοντας το ιστορικό υψηλό market cap του. Από εκεί και μετά παρουσιάζει συνεχείς αυξομειώσεις, χωρίς να έχει καταφέρει να προσεγγίσει ένα σταθερό ρυθμό αύξησης.

Σχήμα 19: Το Market Capitalization του Dash

2.4.4 Η νομισματική πολιτική

Μέσα από τη διαδικασία του mining παράγονται νέα νομίσματα Dash με τη μορφή **reward block**. Για να διασφαλιστεί ότι δε θα προκύψει μία γρήγορη εξάντληση, το reward του μπλοκ μειώνεται σταδιακά, όπως φαίνεται στο παρακάτω σχήμα. Το πρωτόκολλο του Dash ορίζει τον αντίστοιχο ρυθμό. Η γραφική παράσταση αυτών των δεδομένων οδηγεί σε μια καμπύλη που δείχνει τα συνολικά κέρματα που βρίσκονται σε κυκλοφορία (**coin emission rate)**.

Το Dash, κατά την ανάπτυξη του, παρείχε ένα reward των 5 DASH. Μειώνεται με ένα ρυθμό της τάξης του 7,14% για κάθε 210240 μπλοκ (περίπου 383,25 ημέρες). Το τρέχον reward είναι 3,10663 DASH. Διαπιστώνουμε ότι όταν η μείωση του reward είναι μικρή κάθε χρόνο, αυτό προσφέρει μια ομαλότερη μετάβαση σε ένα μοντέλο που βασίζεται στα τέλη των συναλλαγών.Τα συνολικά νομίσματα του Dash είναι το άθροισμα μιας γεωμετρικής σειράς (όπως και στη περίπτωση του Bitcoin), αλλά ο τελικός αριθμός κερμάτων που θα κυκλοφορήσουν είναι αβέβαιος. Με βάση τις μέχρι τώρα εκτιμήσεις, το **max supply** του Dash κυμαίνεται ανάμεσα στα 17.742.696 και 18.921.005 νομίσματα DASH.



Σχήμα 20: Καμπύλη νομισματικής πολιτικής του Dash

Το Dash θα συνεχίσει να κόβει νομίσματα για περίπου 192 χρόνια μέχρις ότου σε ένα πλήρες έτος εξορυχθεί λιγότερο από 1 DASH. Μετά το 2209 θα δημιουργηθούν μόνο 14 DASH. Η διαδικασία για να δημιουργηθεί το τελευταίο DASH θα διαρκέσει 231 χρόνια, αρχίζοντας από το 2246 και λήγοντας όταν η παραγωγή νέων νομισμάτων σταματήσει εντελώς το 2477. Με βάση αυτούς τους υπολογισμούς, το μέγιστο και το ελάχιστο πιθανό *coin supply* στο έτος 2254 μπορεί να υπολογιστεί ότι θα είναι μεταξύ:

Το **reward** για κάθε μπλοκ δε προορίζεται μόνο για τον miner, αλλά κατανέμεται ως εξής:

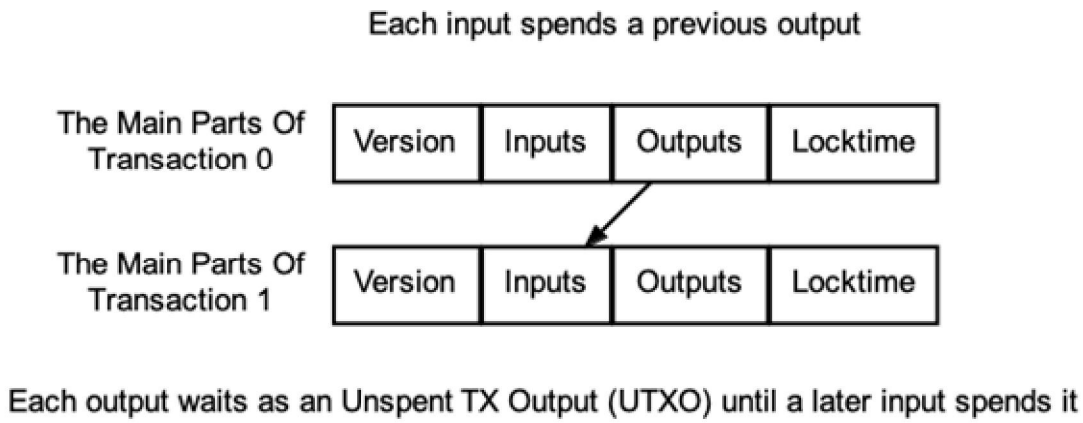
- Ο masternode και ο επιτυχών miner λαμβάνουν το 45% (δηλαδή περίπου 1,3995 DASH) του reward έκαστος.
- Το 10% του reward του μπλοκ προορίζεται για τις προτάσεις προϋπολογισμού. Η κοινότητα του Dash προσφέρει συμβουλές και προτάσεις. Πιο συγκεκριμένα, μέσω του Dash Forum, γίνονται προτάσεις για χρηματοδότηση, με σκοπό την περαιτέρω ανάπτυξη της πλατφόρμας. Οι masternodes ψηφίζουν πάνω στις προτάσεις αυτές («ναι», «όχι» ή αποχή). Εάν υπάρχει έγκριση, δηλαδή αν τα «ναι» είναι πάνω από 10%, το ποσό που έχει συγκεντρωθεί στο budget καταβάλλεται απευθείας από το blockchain.

Πίνακας 8: Νομισματικές μονάδες Dash

Ονομασία	Αξία (σε DASH)
DASH	1
duff	0,00000001

2.4.5 Τα χαρακτηριστικά των transactions

Τα transactions επιτρέπουν στους χρήστες να δαπανούν τα duffs. Κάθε transaction αποτελείται από ορισμένα στοιχεία που επιτρέπουν τόσο απλές άμεσες πληρωμές όσο και πολύπλοκες συναλλαγές.



Σχήμα 21: Dash transaction

Το σχήμα παρουσιάζει τα κύρια μέρη μίας Dash transaction. Κάθε transaction έχει τουλάχιστον μία είσοδο (transaction input) και μία έξοδο (transaction output). Κάθε transaction input περιλαμβάνει τα duffs που έχουν προκύψει ένα transaction output. Κάθε transaction output στη συνέχεια βρίσκεται σε αναμονή ως ένα Unspent Transaction Output (UTXO) μέχρι να το ξοδέψει μια επόμενη transaction input. Όταν το Dash wallet ενημερώνει κάποιον ότι έχει απόθεμα 10,000 duffs, σημαίνει ότι 10,000 duffs περιμένουν μέσα σε ένα ή περισσότερα UTXOs.

Κάθε συναλλαγή έχει έναν transaction version number, μεγέθους 4 bytes, ο οποίος υποδεικνύει στους miners και τους peer χρήστες του Dash το σύνολο απαραίτητων κανόνων για την επικύρωσή τους. Αυτό επιτρέπει στους προγραμματιστές να δημιουργούν νέους κανόνες για μελλοντικές συναλλαγές χωρίς να ακυρώνουν προηγούμενες συναλλαγές.

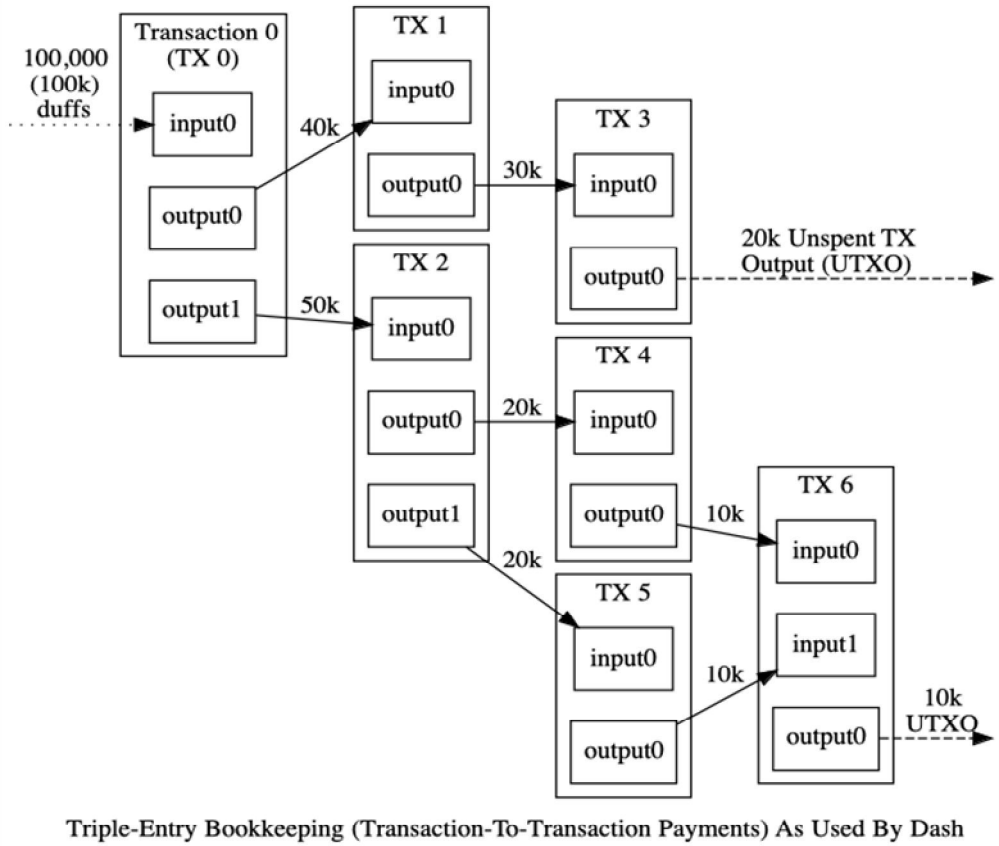
Μια transaction input έχει έναν αριθμό index, ο οποίος δείχνει τον αριθμό της συναλλαγής στην οποία είναι ενταγμένη η συγκεκριμένη έξοδος. Ο index αριθμός για την έξοδο της πρώτης transaction είναι μηδέν. Η έξοδος έχει επίσης ένα ποσό σε duffs το οποίο πληρώνει σε ένα pubkey script. Όποιος μπορεί να ικανοποιήσει τις προϋποθέσεις αυτού του pubkey script, μπορεί να ξοδέψει το ποσό duffs που αυτό διαθέτει.

Μια είσοδος χρησιμοποιεί ένα αναγνωριστικό συναλλαγής (txid) και έναν index αριθμό εξόδου για να ταυτοποιήσει μια συγκεκριμένη έξοδο που θα δαπανηθεί. Έχει επίσης ένα

signature script που της επιτρέπει να παρέχει παραμέτρους δεδομένων που ικανοποιούν τις προϋποθέσεις στο pubkey script.

Οι συναλλαγές συνδεδεμένες μεταξύ τους. Το λογισμικό wallet του Dash δίνει την εντύπωση ότι duffs στέλνονται από και προς τα wallets, αλλά στην ουσία η αξία του Dash μετακινείται από συναλλαγή σε συναλλαγή. Κάθε συναλλαγή ξοδεύει τα τελευταία duffs που έχει λάβει, έτσι ώστε η είσοδος μιας συναλλαγής να είναι η έξοδος της προηγούμενης.

Μια συναλλαγή μπορεί να έχει πολλαπλές εξόδους, όπως στην περίπτωση αποστολής σε πολλές διευθύνσεις, αλλά κάθε έξοδος μιας συγκεκριμένης συναλλαγής μπορεί να χρησιμοποιηθεί μόνο μία φορά ως είσοδος blockchain. Οποιαδήποτε μεταγενέστερη αναφορά αποτελεί προσπάθεια να ξοδευτούν τα ίδια duffs δύο φορές. Οι έξοδοι συνδέονται με τα transaction IDs (αναγνωριστικά των συναλλαγών), τα οποία είναι οι κατακερματισμοί των υπογεγραμμένων συναλλαγών. Επειδή κάθε έξοδος μιας συγκεκριμένης συναλλαγής μπορεί να δαπανηθεί μόνο μία φορά, οι έξοδοι όλων των συναλλαγών που περιλαμβάνονται στο blockchain χωρίζονται σε 2 κατηγορίες: τα **Unspent Transaction Outputs (UTXOs)**-που δεν έχουν ξοδευτεί, και τα **Spent Transaction Outputs**- που έχουν ξοδευτεί. Για να είναι έγκυρη μία πληρωμή, πρέπει να χρησιμοποιεί σαν είσοδο μόνο UTXOs.



Σχήμα 22: Transaction-To-Transaction

Εάν η αξία των εξόδων μιας συναλλαγής υπερβαίνει την αξία των εισόδων της, η συναλλαγή θα απορριφθεί - αλλά αν συμβαίνει το αντίθετο, οποιαδήποτε διαφορά στην

αξία μπορεί να θεωρηθεί ως τέλος συναλλαγής από τον Dash miner, ο οποίος δημιουργεί το μπλοκ που περιέχει αυτή τη συναλλαγή. Για παράδειγμα, στην εικόνα βλέπουμε, ότι κάθε συναλλαγή που ξοδεύει 10.000 duffs λιγότερα από όσα λαμβάνει από τον συνδυασμό των εισόδων της, καταβάλλει 10.000 duffs ως τέλος συναλλαγής.

2.4.5.1 Η δομή των transactions

Οι συναλλαγές Dash μεταδίδονται μεταξύ των χρηστών του δικτύου σε μορφή serialized byte, που ονομάζεται **raw format**. Όταν οι συναλλαγές βρίσκονται σε αυτή τη μορφή εφαρμόζεται διπλά η συνάρτηση κατακερματισμού SHA256, έτσι ώστε να δημιουργηθεί ένα μοναδικό αναγνωριστικό για τη συναλλαγή, το TXID και τελικά το merkle root ενός μπλοκ που περιέχει τη συναλλαγή. Με αυτό τον τρόπο το format της συναλλαγής παίζει ρόλο στο πως εφαρμόζεται το consensus πρωτόκολλο, ώστε να διασφαλιστεί η ασφάλεια των συναλλαγών εντός του Dash blockchain. Μία transaction στο δίκτυο του Dash έχει την ακόλουθη μορφή:

Πίνακας 9: Η δομή μιας raw transaction στο Dash

Όνομα	Bytes	Περιγραφή
version	2	Ο αριθμός της εκδοχής του version
type	2	*Ο τύπος της συναλλαγής*
tx_in count	*μεταβλητό*	Το πλήθος των δεδομένων εισόδου της συναλλαγής
tx_in	*μεταβλητό*	Τα δεδομένα εισόδου της συναλλαγής (transaction inputs)
tx_out count	*μεταβλητό*	Το πλήθος των δεδομένων εξόδου της συναλλαγής
tx_out	*μεταβλητό*	Τα δεδομένα εξόδου της συναλλαγής (transaction outputs)
lock_time	4	Ο χρόνος κλειδώματος της συναλλαγής
extra_payload size	*μεταβλητό*	*Το μέγεθος των επιπρόσθετων δεδομένων για τη συναλλαγή*
extra_payload	*μεταβλητό*	*Τα επιπρόσθετα δεδομένα για τη συναλλαγή*

Μια συναλλαγή μπορεί να έχει πολλαπλά inputs και outputs, έτσι ώστε οι δομές **txIn** και **txOut** να επαναλαμβάνονται μέσα σε μια συναλλαγή. Η δομή **txIn** αποτελεί ένα input μιας συναλλαγής και περιέχει 3 πεδία:

1. ένα outpoint (μία αναφορά σε προηγούμενο output)
2. ένα signature script (επιτρέπει στη συναλλαγή να ξοδέψει το outpoint)

3. έναν sequence αριθμό, ώστε να διατηρείται σωστά η διάταξή τους

Η δομή **txOut** αποτελεί ένα output μιας συναλλαγής και περιέχει 2 πεδία:

1. ένα value πεδίο, για να μεταφέρει 0 ή περισσότερα duffs
2. ένα pubkey script, που υποδεικνύει τις προϋποθέσεις που πρέπει να ισχύουν για να ξοδευτούν τα duffs

2.4.5.2 Η διαδικασία μιας transaction

Θα περιγράψουμε την αλληλουχία μιας transaction με Dash μέσα από ένα παράδειγμα. Ας υποθέσουμε ότι η Ιωάννα έχει στο Dash wallet της νομίσματα DASH. Υπάρχουν 2 βασικά χαρακτηριστικά του Dash wallet:

1. **Public address**: είναι κάτι αντίστοιχο με τον αριθμό τραπεζικού λογαριασμού που διατηρεί ένας χρήστης. Δημιουργείται τυχαία από έναν συνδυασμό γραμμάτων και αριθμών και πρέπει να δίνεται σε όποιον θέλει να μας στείλει μία πληρωμή.
2. **Private key**: Δημιουργείται από μία τυχαία ακολουθία χαρακτήρων και είναι απαραίτητος σε ένα χρήστη για να μπει στο Dash wallet του και να πραγματοποιήσει οποιαδήποτε transaction. Είναι αντίστοιχο με τον κωδικό ασφαλείας που χρησιμοποιεί κάποιος στο ATM και που δεν τον μοιράζεσαι με κανέναν.

Η Ιωάννα θέλει να στείλει στο Γιώργο 1 νόμισμα Dash. Η συναλλαγή ολοκληρώνεται μέσα από τα ακόλουθα βήματα:

1. Η Ιωάννα χρησιμοποιεί το private key της για να πραγματοποιήσει είσοδο στο Dash wallet της και στέλνει 1 Dash νόμισμα στην public address του Γιώργου
2. Οι miners του Dash θα προσθέσουν τη συναλλαγή μέσα στο μπλοκ Α, που είναι ένα γκρουπ συναλλαγών Dash που πραγματοποιούνται στο ίδιο χρονικό διάστημα.
3. Εάν η Ιωάννα διαλέξει την υπηρεσία InstantSend η συναλλαγή θα επιβεβαιωθεί από τον Masternode. Αλλιώς θα επιβεβαιωθεί από έναν απλό miner σε περίπου 2-3 λεπτά.
4. Όταν συμβεί αυτό, οι υπόλοιποι miners του δικτύου θα ενημερωθούν, θα ελέγξουν ξανά τα αποτελέσματα από τους miners που επικύρωσαν τη συναλλαγή για να βεβαιωθούν ότι δεν υπάρχουν λάθη και ότι η συναλλαγή είναι έγκυρη.
5. 1 Dash νόμισμα θα μεταφερθεί από το wallet της Ιωάννας στο Γιώργο.

2.4.5.3 Η πολιτική τελών

Ένα από τα κομβικά ζητήματα που έρχεται να λύσει το Dash είναι το κόστος της διεξαγωγής συναλλαγών. Το μέγεθος του κόστους των συναλλαγών με bitcoin καθορίζεται από μια πληθώρα παραγόντων, περιλαμβάνοντας το μέγεθος του block καθώς και το χρόνο (ώρα της ημέρας) που διεξάγεται η συναλλαγή. Το Dash από την άλλη ελαχιστοποιεί τα transaction fees που σύμφωνα με το μέσο όρο που το ίδιο το νόμισμα δημοσιοποίησε φτάνουν το 0,0264 δολάρια, ξεπερνώντας μάλιστα και άλλα κρυπτονομίσματα, όπως το Litecoin.

Οι συναλλαγές στο δίκτυο Dash εγγράφονται σε blocks στο blockchain. Το μέγεθος κάθε συναλλαγής μετράται σε bytes, αλλά δεν υπάρχει μια μοναδική συσχέτιση μεταξύ των συναλλαγών υψηλής αξίας και του αριθμού των bytes που απαιτούνται για την επεξεργασία της συναλλαγής**. Το μέγεθος της συναλλαγής επηρεάζεται από τον αριθμό των διευθύνσεων εισόδου και εξόδου που συμμετέχουν στη συναλλαγή.**

Κάθε νέο μπλοκ παράγεται από έναν miner, ο οποίος πληρώνεται με rewards για την ολοκλήρωση της εργασίας του. Για να αποφευχθεί το ενδεχόμενο να γεμίσει το δίκτυο με spam συναλλαγές, το μέγεθος κάθε μπλοκ περιορίζεται. Καθώς αυξάνεται ο όγκος συναλλαγών, ο ελεύθερος χώρος σε κάθε μπλοκ περιορίζεται. Επειδή οι miners δεν είναι υποχρεωμένοι να συμπεριλάβουν οποιαδήποτε συναλλαγή στα blocks που παράγουν, αφού τα blocks γεμίσουν, μπορεί να συμπεριληφθεί ένα προαιρετικό τέλος συναλλαγής ως κίνητρο στον miner για να επεξεργαστεί τη συναλλαγή. Τα περισσότερα wallets περιλαμβάνουν ένα προεπιλεγμένο μικρό τέλος, παρόλο που ορισμένοι miners επεξεργάζονται συναλλαγές ακόμη και αν δεν συμπεριλαμβάνονται τέλη.

Πίνακας 10: Τρέχουσα πολιτική τελών στο Dash

Τύπος συναλλαγής	Προτεινόμενο τέλος	Ανά μονάδα
Standard transaction	.00001 DASH	Ανά KB δεδομένων συναλλαγής
InstantSend autolock	.00001 DASH	Ανά KB δεδομένων συναλλαγής
InstantSend	.0001 DASH	Ανά transaction input
PrivateSend	.001 DASH	Ανά 10 γύρους mixing

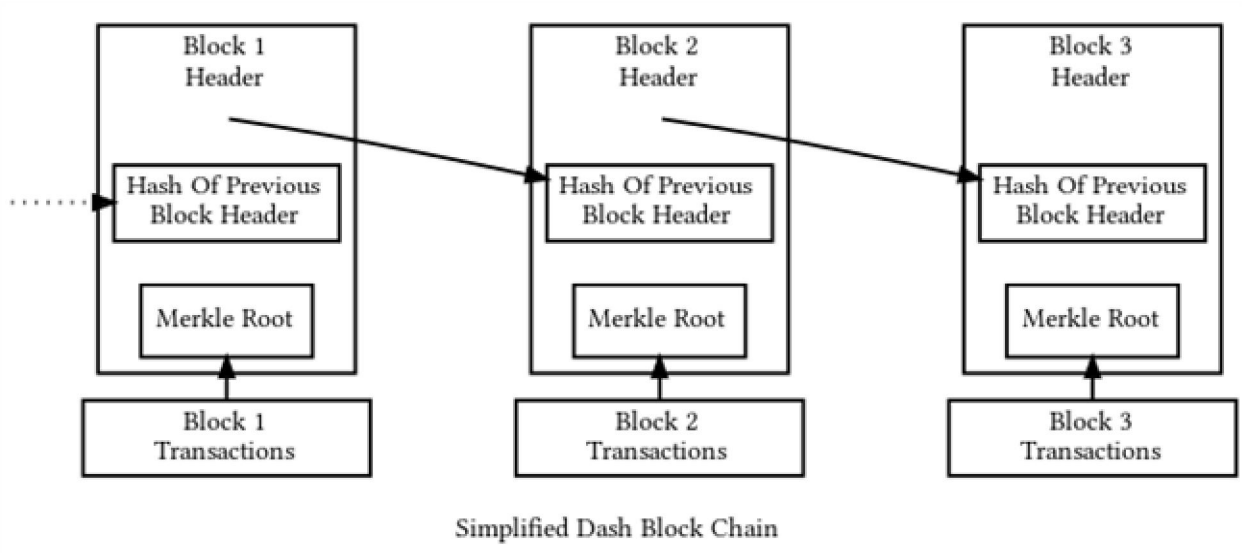
2.4.5.4 Ασφάλεια και προστασία μιας transaction

Το Dash μέσω της υπηρεσίας **PrivateSend** εγγυάται την ασφάλεια των συναλλαγών. Με τη χρήση της υπηρεσίας αυτής παρέχεται πλήρης ανωνυμία για τους συμμετέχοντες χρήστες σε μία συναλλαγή. Με αυτό το τρόπο, παρέχεται και πλήρης ιδιωτικότητα στη προέλευση των πόρων του χρήστη μέσω του mixing νομισμάτων, καθώς όλα τα νομίσματα Dash που έχει στην κατοχή του κάποιος αναγνωρίζονται ως μια διαφορετική "εισροή" (input), δηλαδή ως διακριτά και ξεχωριστά νομίσματα.

2.4.6 Το Blockchain

Το blockchain περιλαμβάνει το ledger του Dash, το οποίο αντιστοιχεί σε ένα ταξινομημένο και έγκυρο αρχείο των transactions. Το ledger έχει σχεδιαστεί με τέτοιο τρόπο, ώστε να εμποδίζει τις double spend επιθέσεις, καθώς και να διατηρεί αμετάβλητες τις transactions.

Κάθε full node του δικτύου του Dash διατηρεί ένα στιγμιότυπο του blockchain που περιέχει μόνο blocks, τα οποία έχουν επικυρωθεί από αυτόν τον κόμβο. Όταν ένας επαρκής αριθμός από κόμβους διατηρούν τα ίδια blocks στο blockchain τους, τότε αυτοί οι κόμβοι βρίσκονται σε συμφωνία(consensus). Οι κανόνες επικύρωσης που χρησιμοποιούν αυτοί οι κόμβοι προκειμένου να διατηρηθεί αυτή η συμφωνία ονομάζονται κανόνες συναίνεσης(consensus rules).



Σχήμα 23: Το blockchain του Dash

Η εικόνα παρουσιάζει μια απλοποιημένη έκδοση ενός blockchain. Ένα μπλοκ που περιέχει μια ή περισσότερες νέες transactions, εισάγεται στο τμήμα δεδομένων συναλλαγής του μπλοκ. Ύστερα, παράγεται το hash value για τα αντίγραφα κάθε συναλλαγής. Στη συνέχεια αυτά, τα hash value αυτά συγχωνεύονται. Με αυτό τρόπο δομείται το Merkle tree του Dash blockchain. Το merkle root αποθηκεύεται στο block header κάθε μπλοκ μαζί με το hash του block header του προηγούμενου μπλοκ. Με αυτό τον τρόπο συνδέονται τα μπλοκ στην αλυσίδα. Αυτό εξασφαλίζει ότι για να τροποποιηθεί μια συναλλαγή, πρέπει να τροποποιηθεί το μπλοκ που την περιέχει και όλα τα επόμενα μπλοκ.

2.4.6.1 Η δομή ενός μπλοκ

Κάθε μπλοκ στο Dash περιλαμβάνει το block header, το οποίο αποτελείται από τα εξής στοιχεία:

Πίνακας 11: Η δομή ενός μπλοκ στο Dash

Πεδίο	*Μέγεθος(σε bytes)*	*1.1 Περιγραφή*
version	*4*	*ο αριθμός του block version*
previous block header hash	*32*	*το hash value του block header του προηγούμενου μπλοκ*

merkle root hash	*32*	*το hash value του root του Merkle tree που αξιοποιείται για τις συναλλαγές του blockchain.*
time	*4*	*το timestamp δημιουργίας του μπλοκ*
nBits	*4*	*το target value για το mining*
nonce	*4*	*ο παράγοντας nonce για το mining*

Για τα πεδία ενός μπλοκ ισχύουν τα εξής:

1. το block version number υποδεικνύει το σύνολο των κανόνων, το οποίο θα αξιοποιηθεί στη διαδικασία του ελέγχου εγκυρότητας του μπλοκ.
2. το merkle root προέρχεται από τα hash value όλων των συναλλαγών, οι οποίες συμπεριλαμβάνονται μέσα στο μπλοκ. Με αυτό τρόπο, εξασφαλίζεται πως καμία από τις συναλλαγές δε μπορεί να τροποποιηθεί, αν δε τροποποιηθεί συνολικά το header.

2.4.7 Η λειτουργία του δικτύου στο Dash: Mining και Masternodes

Το δίκτυο του Dash, σε αντίθεση με άλλα κρυπτονομίσματα, διαθέτει δίκτυο με δύο επίπεδα. Το πρώτο επίπεδο περιλαμβάνει τους miners και τη δραστηριότητά τους, η οποία είναι ίδια με αυτή του Bitcoin. Οι miners και στη περίπτωση του Dash εκτελούν συνεχώς ένα Proof of Work αλγόριθμο, ώστε να πιστοποιήσουν συναλλαγές, να τις εντάξουν σε μπλοκ και να το εισάγουν με τη σειρά στο blockchain. Μέσω αυτής της διαδικασίας, οι miners λαμβάνουν μόνο ένα ποσοστό του block reward (το 45% συγκεκριμένα). Τα βήματα του PoW αλγορίθμου του Dash είναι παρόμοια με τη περίπτωση του Bitcoin. Περιγράφονται παρακάτω:

1. Κάθε miner συλλέγει συναλλαγές, οι οποίες έχουν μεταδοθεί στο δίκτυο.
2. Γίνεται επικύρωση όλων των συναλλαγών αυτών και εντάσσονται σε ένα υποψήφιο μπλοκ.
3. Το hash value του block header εισέρχεται στο υποψήφιο μπλοκ.
4. Κάθε miner προσπαθεί να επιλύσει το proof of work πρόβλημα. Αν υπάρξει επιτυχία, η λύση μεταδίδεται σε όλο το δίκτυο.
5. Το μεταδιδόμενο proof of work ελέγχεται ως προς την εγκυρότητα από το υπόλοιπο δίκτυο.
6. Αν υπάρχει consensus (συναίνεση) ως προς την εγκυρότητα του μπλοκ από τους κόμβους του δικτύου, το μπλοκ εισέρχεται επιτυχημένα στο blockchain.

Η διαδικασία του PoW του DASH είναι παρόμοια με αυτή του Bitcoin και ακολουθεί τα εξής βήματα:

- Ορίζεται μία τιμή για το nonce (το πεδίο nNonce).
- Ο miner υπολογίζει συνεχώς το hash value του block header μέσω της hash συνάρτησης X11.
- Ελέγχει αν το παραγόμενο hash value είναι κάτω από ένα όριο T.
- Αν είναι κάτω από αυτό το όριο, ο miner έχει επιτυχώς υπολογίσει ένα proof of work και μεταδίδει το μπλοκ που συνθέτει, μαζί με το proof of work, στο υπόλοιπο δίκτυο.

Σε κάθε μπλοκ, το δίκτυο χρησιμοποιεί το difficulty των τελευταίων 24 μπλοκ και τον αριθμό δευτερολέπτων που έχουν περάσει μεταξύ της δημιουργίας του πρώτου και του τελευταίου από αυτά τα 24 μπλοκς . Η ιδανική τιμή είναι 3600 sec (μία ώρα).

- Αν χρειαστεί λιγότερο από μία ώρα για να δημιουργηθούν τα 24 μπλοκ, η αναμενόμενη difficulty value αυξάνεται, έτσι ώστε τα επόμενα 24 μπλοκ να χρειαστούν ακριβώς μία ώρα για να δημιουργηθούν αν ελέγχονται τα hash values με τον ίδιο ρυθμό.
- Εάν χρειάστηκε πάνω από μία ώρα για να δημιουργηθούν τα blocks, η αναμενόμενη difficulty value μειώνεται για τον ίδιο λόγο.

Αυτή η μέθοδος υπολογισμού του difficulty (Dark Gravity Wave) γράφτηκε από τον δημιουργό του Dash, Evan Duffield, για να διορθώσει πιθανό exploit από τον προηγούμενο αλγόριθμο που χρησιμοποιούταν για τον υπολογισμό του difficulty (Kimoto Gravity Well). Το **Dark Gravity Wave** είναι ένας difficulty-adjusting αλγόριθμος ανοιχτού κώδικα για κρυπτονομίσματα που βασίζονται στο Bitcoin. Χρησιμοποιήθηκε για πρώτη φορά στο Dash και από τότε και σε άλλα ψηφιακά νομίσματα. Σε γενικές γραμμές, το DGW είναι παρόμοιο με το Kimoto Gravity Well, προσαρμόζοντας τα επίπεδα δυσκολίας σε κάθε μπλοκ (αντί για κάθε μπλοκ του 2016 όπως το Bitcoin) βάσει στατιστικών στοιχείων από πρόσφατα εντοπισμένα μπλοκ. Αυτό καθιστά δυνατή την έκδοση μπλοκ με σχετικά σταθερούς χρόνους, ακόμη και αν η hashing power έχει υψηλές διακυμάνσεις, χωρίς να υποφέρει από την time-warp exploit.

Το δεύτερο επίπεδο περιλαμβάνει τη λειτουργία των Masternodes. Οι masternodes δεν πραγματοποιούν mining, ούτε το υλικό του mining μπορεί να χρησιμοποιηθεί για τη λειτουργικότητα των Masternode. Υποστηρίζουν μία σειρά από πολύτιμες λειτουργίες μέσα στο δίκτυο όπως:

- Επιτρέπουν τη εκτέλεση άμεσων συναλλαγών. Παρέχουν, δηλαδή, το υπόβαθρο για τη υποστήριξη του Instant Send.
- Επιτρέπουν τη πλήρη ιδιωτικότητα στις συναλλαγές. Παρέχουν, δηλαδή, το υπόβαθρο για την υποστήριξη του Private Send.
- Αποφασίζουν μέσω ψήφων για βασικά ζητήματα του δικτύου. Κάθε masternode έχει δικαίωμα για μία ψήφο και μπορεί να αποφασίσει για τις προτάσεις που μπορεί να κάνει κάποιος χρήστης ή για τις προτάσεις ανάπτυξης του Dash.
- Έχουν τη δυνατότητα να απορρίψουν ένα κακοδιαμορφωμένο μπλοκ, όπως προέκυψε από έναν miner. Επίσης, αν ένας miner προσπαθήσει να λάβει όλο το reward για τον εαυτό του ή προσπαθήσει να λειτουργήσει με παλιά έκδοση του λογισμικού, το σύνολο των Masternode έχει τη δυνατότητα να αποτρέψει την προσθήκη του νέου μπλοκ στη blockchain.
- Προστατεύει το blockchain από τις 51% επιθέσεις.

Οι υπηρεσίες αυτές προσφέρουν το 45% του block reward σε έναν masternode. Το σύστημα των Masternode λειτουργεί με ένα τρόπο, ο οποίος ονομάζεται Proof of Service (PoSe). Κάθε χρήστης μπορεί να λάβει το ρόλο του Masternode, αρκεί να καταθέσει το ποσό των 1000 Dash. Το ποσό αυτό δε θεωρείται stake, καθώς δεν παρακρατείται αν λειτουργήσει κακόβουλα ο Masternode, ούτε κλειδώνεται επίσης. Κάθε χρήστης, ο οποίος λειτουργεί έναν masternode, έχει τη δυνατότητα κάθε στιγμή να

ξοδέψει μέρος αυτού του ποσού. Αν γίνει κάτι τέτοιο, ο σχετικός masternode απενεργοποιείται και παύει να λαμβάνει τα rewards.

Με βάση τα παραπάνω, καταλήγουμε πως το δίκτυο του Dash συνδυάζει τη λειτουργικότητα του Proof of Work και του Proof of Service. Το πρωτόκολλο του Dash αξιοποιεί τον αλγόριθμο X11 ως hash function, όπου μια είσοδος αυθαίρετου μεγέθους περνάει μέσα από 11 ανεξάρτητες hash functions σε έναν αλγόριθμο. Όταν υποβάλλεται μία τιμή, η πρώτη συνάρτηση παράγει ένα hash, το οποίο στη συνέχεια υποβάλλεται στην επόμενη συνάρτηση για να παράξει ένα άλλο hash. Αυτή η διαδικασία επαναλαμβάνεται μέχρι την τελευταία συνάρτηση που χρησιμοποιεί ο αλγόριθμος. Οι συναρτήσεις αυτές είναι οι:

1. BLAKE
2. BLUE MIDNIGHT WISH (BMW)
3. Grøsti
4. JH
5. Keccak
6. Skein
7. Luffa
8. CubeHash
9. SHAvite-3
10. SIMD
11. ECHO

και θεωρούνται από τις πιο ασφαλείς τεχνικές κρυπτογράφησης που υπάρχουν.

2.4.8 PrivateSend

Η υπηρεσία PrivateSend παρέχει πραγματική οικονομική ιδιωτικότητα στις συναλλαγές, καλύπτοντας την προέλευση των κεφαλαίων ενός χρήστη και του δίνει τη δυνατότητα να διατηρεί τον έλεγχο των χρημάτων του ανά πάσα στιγμή. Η διαδικασία PrivateSend λειτουργεί ως εξής:

- Το PrivateSend ξεκινά με τη μετατροπή των transaction inputs σε μικρές αξίες(denominations), όπως 0.001, 0.01, 0.1, 1 και 10 DASH (σαν τα πραγματικά χαρτονομίσματα).
- Η εφαρμογή wallet στέλνει κατόπιν αιτήματα στους masternodes. Οι masternodes ενημερώνονται ότι ο χρήστης ενδιαφέρεται να πραγματοποιήσει mixing συγκεκριμένων denominations, αλλά δεν λαμβάνουν καμία προσωπική πληροφορία για την ταυτότητα του χρήστη.
- Όταν δύο άλλοι χρήστες στείλουν παρόμοια μηνύματα, δηλώνοντας ότι επιθυμούν να πραγματοποιήσουν mixing των ίδιων denominations, ξεκινά μια mixing session. Ο masternode πραγματοποιεί mixing των transaction inputs και δίνει εντολή στα wallets των τριών χρηστών να πληρώσουν την μόλις μετασχηματισμένη input πίσω στον εαυτό τους.
- Το wallet πληρώνει αυτήν την ονομασία απευθείας στον εαυτό του, αλλά σε διαφορετική διεύθυνση (αποκαλούμενη διεύθυνση αλλαγής)

- Το wallet επαναλαμβάνει αυτή τη διαδικασία πολλές φορές με κάθε μονάδα denomination. Κάθε φορά που ολοκληρώνεται η διαδικασία, ολοκληρώνεται ένας γύρος. Σε κάθε γύρο του PrivateSend αυξάνεται ο βαθμός δυσκολίας για τον προσδιορισμό καταγωγής των κεφαλαίων. Ο χρήστης μπορεί να επιλέξει μεταξύ 1-16 γύρων mixing.
- Αυτή η διαδικασία mixing εκτελείται στο παρασκήνιο χωρίς καμία παρέμβαση από το χρήστη. Όταν ο χρήστης θέλει να πραγματοποιήσει μια ιδιωτική συναλλαγή, τα κεφάλαιά θα είναι έτοιμα να ξοδευτούν, χωρίς να απαιτείται επιπλέον αναμονή.

2.4.9 InstandSend

Τα παραδοσιακά αποκεντρωμένα κρυπτονομίσματα πρέπει να περιμένουν αρκετά (από 15 λεπτά έως μία ώρα) για να εξασφαλίσουν ότι μια συναλλαγή είναι μη αναστρέψιμη και δεν αποτελεί μια προσπάθεια για double-spend. Άλλα κρυπτονομίσματα επιτυγχάνουν ταχύτερο χρόνο επιβεβαίωσης συναλλαγών χρησιμοποιώντας μια κεντρική αρχή στο δίκτυο τους.

Το Dash αντιμετωπίζει αυτό το πρόβλημα χάρη στο 2ο επίπεδο του δικτύου του που αποτελείται από masternodes. Οι Masternodes μπορούν να κληθούν να σχηματίσουν voting quorums για να ελέγξουν την εγκυρότητα μια υποβαλλόμενης συναλλαγής. Εάν είναι έγκυρη, οι masternodes "κλειδώνουν" τα inputs για τη συναλλαγή και μεταδίδουν αυτή την πληροφορία στο δίκτυο, υποσχόμενοι ότι η συναλλαγή θα συμπεριληφθεί στα μεταγενέστερα mined blocks και δεν επιτρέπουν οποιαδήποτε άλλη δαπάνη αυτών των inputs κατά τη διάρκεια του validation.

Η τεχνολογία InstantSend επιτρέπει σε κρυπτονομίσματα όπως το Dash να ανταγωνίζονται συστήματα συναλλαγών όπως αυτό των πιστωτικών καρτών, ενώ δεν βασίζονται σε κεντρική αρχή.

2.5 Namecoin

2.5.1 Σκοπός δημιουργίας

Το Namecoin αναπτύχθηκε για να προστατεύσει το δημόσιο λόγο από κάθε είδους λογοκρισία και να βελτιώσει την ιδιωτικότητα των χρηστών του Διαδικτύου.

Ένας χώρος ονομάτων (***namespace***) είναι ένα ηλεκτρονικό σύστημα που αντιστοιχίζει ονόματα (***names***) σε τιμές (***values***). Μια υπηρεσία Ιστού, όπως το Twitter, που δίνει τη δυνατότητα δημιουργίας ονόματος χρήστη (*username*) και ηλεκτρονικού προφίλ (*profile*) είναι ένα παράδειγμα υλοποίησης namespace. Το **DNS** είναι το πιο εξέχον παράδειγμα. Το DNS είναι ο τηλεφωνικός κατάλογος του Διαδικτύου. Όταν κάποιος πληκτρολογεί μια διεύθυνση στον browser, το Διαδίκτυο δεν την αντιλαμβάνεται σαν κείμενο, γιατί στην πραγματικότητα λειτουργεί με αριθμητικές διευθύνσεις που ονομάζονται διευθύνσεις IP. Το πρόβλημα βέβαια είναι ότι οι αριθμοί δεν απομνημονεύονται εύκολα. Επομένως, δημιουργήθηκε ένα βιβλίο διευθύνσεων σε ολόκληρο το Internet, το οποίο ονομάζεται σύστημα ονομάτων τομέα (*DNS*), για να κάνει την πλοήγηση πολύ ευκολότερη. Το Namecoin είναι η βάση ενός αποκεντρωμένου συστήματος ονομάτων τομέα.

Το τελευταίο μέρος ενός τομέα, π.χ. .com, ονομάζεται τομέας ανώτατου επιπέδου (**top-level domain, TLD**). Το πρόβλημα είναι ότι τα TLDs ελέγχονται από κυβερνήσεις και μεγάλες εταιρείες (πχ ο .com TLD ελέγχεται από την ICANN - *Internet Corporation for Assigned Names and Numbers* στις ΗΠΑ), οι οποίες έχουν τη δυνατότητα να καταχράζονται τη δύναμή τους προκειμένου να λογοκρίνουν, να υφαρπάζουν προσωπικά δεδομένα ή να κατασκοπεύουν σχετικά με την προσωπική χρήση του Διαδικτύου που κάνει ο καθένας. Αυτό συμβαίνει σε τακτική βάση σε όλο τον κόσμο, ιδιαίτερα σε χώρες όπως η Κίνα και η Αμερική.

Οι ιστοσελίδες dot-bit (**.bit**) είναι ανθεκτικές σε τέτοιου είδους μεταχειρήσεις. Αυτό συμβαίνει γιατί ο ψηφιακός τηλεφωνικός κατάλογος δεν διαχειρίζεται από κάποια κεντρική αρχή (εταιρεία ή κυβέρνηση), αλλά βρίσκεται στον υπολογιστή του χρήστη. Η τεχνολογία Bitcoin εξασφαλίζει ότι κάθε χρήστης στον κόσμο έχει τα ίδια δεδομένα τηλεφωνικού καταλόγου στον υπολογιστή του, χωρίς κανείς να μπορεί να τα αλλάξει με παράνομο τρόπο.

2.5.2 Στοιχεία για το δημιουργό

Στις 18 Απριλίου του 2011 παρουσιάστηκε το Namecoin από τον Vinced (φήμες λένε ότι πρόκειται για τον Vincent Durham).

Δύο χρόνια αργότερα, τον Ιούνιο του 2013, παρουσιάστηκε η υπηρεσία NameID. Αυτή η υπηρεσία συσχετίζει πληροφορίες προφίλ με ταυτότητες στο blockchain του Namecoin και μια υπηρεσία-πάροχο OpenID, για να επιτρέψει τη σύνδεση σε υπάρχουσες τοποθεσίες Web με ταυτότητες Namecoin. Η ίδια η κύρια ιστοσελίδα συνοδεύεται από ένα ανοικτό πρωτόκολλο για έλεγχο ταυτότητας με ταυτότητες Namecoin χωρίς κωδικό πρόσβασης, μια αντίστοιχη εφαρμογή ελεύθερου λογισμικού και μια επέκταση υποστήριξης για το Firefox.

Τον Οκτώβριο του 2013, ο Michael Groager, κύριος προγραμματιστής του libcoin, βρήκε ένα ζήτημα ασφαλείας στο πρωτόκολλο Namecoin το οποίο επέτρεπε την τροποποίηση ξένων ονομάτων. Διορθώθηκε επιτυχώς σε σύντομο χρονικό διάστημα και δεν τέθηκε ποτέ ζήτημα exploit, εκτός από την περίπτωση του bitcoin.bit ως proof-of-concept.

Το Φεβρουάριο του 2014, κυκλοφόρησε μια προσθήκη για το Firefox συμβατή με τα Windows και Linux, με το όνομα FreeSpeechMe. Με τη βοήθειά της ήταν δυνατή η αυτόματη επίλυση ζητημάτων των διευθύνσεων .bit. Αυτό είναι διαθέσιμο με τη λήψη του blockchain του Namecoin και την εκτέλεσή του στο παρασκήνιο.

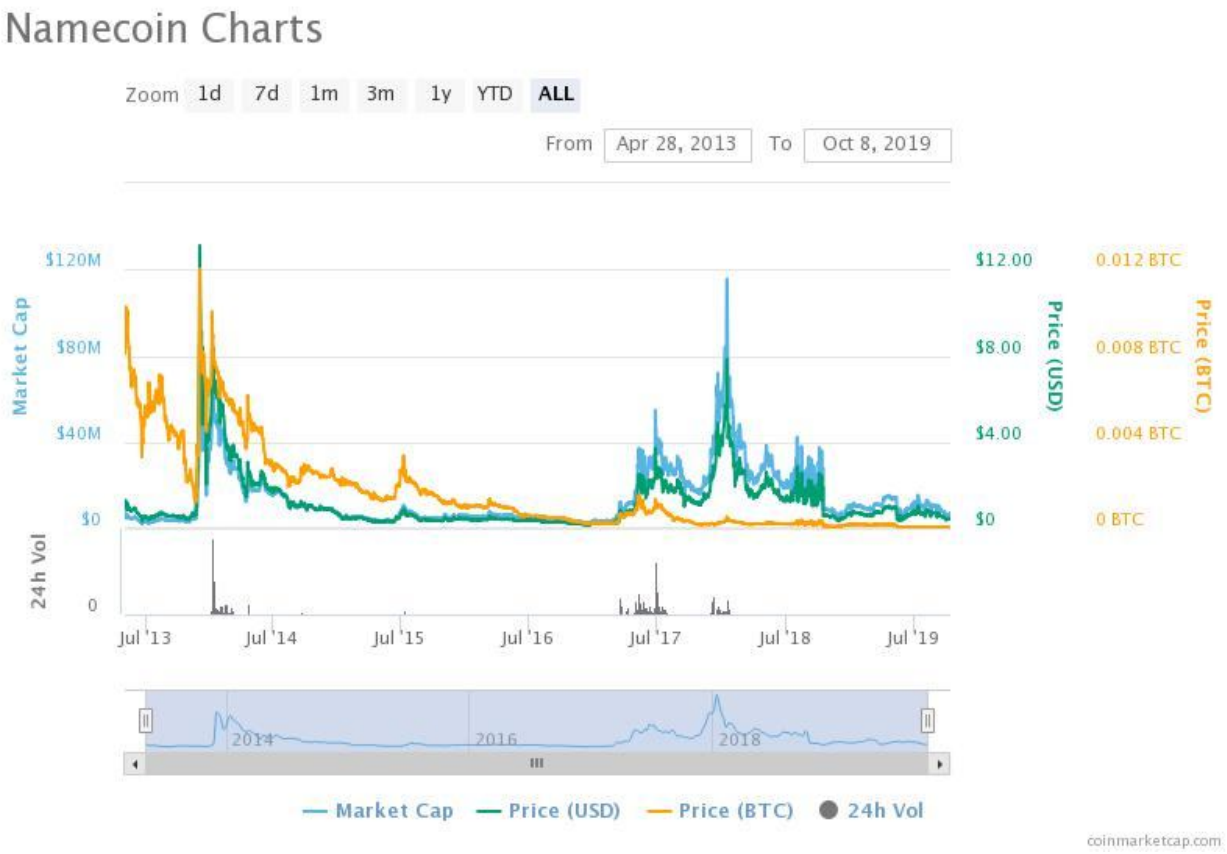
Ένα μήνα αργότερα, τον Μάρτιο του 2014, κυκλοφόρησε το Onename, ένα άλλο σύστημα ταυτοτήτων βασισμένο πάνω στο πρωτόκολλο Namecoin, που αποθηκεύει ονόματα χρηστών και προσωπικά δεδομένα προφίλ στο blockchain. Σε αντίθεση με το NameID, το Onename είναι κατασκευασμένο αποκλειστικά για πληροφορίες προφίλ και δεν υποστηρίζει έλεγχο ταυτότητας χωρίς κωδικό πρόσβασης ή σύνδεση.

Λίγο αργότερα, τον Σεπτέμβριο του 2015, το Onename άλλαξε προφίλ χρηστών από το blockchain του Namecoin σε αυτό του Bitcoin, επειδή το bitcoin είχε υψηλότερο *hash rate*

2.5.3 Το τρέχον Market Capitalization

Η τρέχουσα αξία του Namecoin σήμερα είναι $0,481523. Το σύνολο των νομισμάτων που βρίσκονται σε κυκλοφορία είναι 14.736.400 NMC. Αυτό αντιστοιχεί σε ένα market Capitalization της τάξης των $7.095.913. Η ονομαστική αξία του Namecoin παρουσίασε:

- ιστορικό υψηλό τα $10,80 στις 30/11/2013. Η αξία αυτή αντιστοιχούσε σε 80.223.550 $ Market Capitalization.
- ιστορικό χαμηλό τα $0.190262 στις 07/12/2016. Η αξία αυτή αντιστοιχούσε σε 2.496.788 $ Market Capitalization.



Σχήμα 24: Το Market Capitalization του Namecoin

2.5.4 Ο σχεδιασμός του Namecoin

Το Namecoin χρησιμοποιεί τεχνολογία ανοιχτού κώδικα (open-source) για την εγγραφή ονομάτων (names) και την αποθήκευση των συσχετισμένων values στο blockchain. Μπορεί κανείς να το περιγράψει ως μία διαμοιραζόμενη βάση δεδομένων που κατανέμεται από ένα peer-to-peer δίκτυο με ασφαλή τρόπο. Αυτά τα ονόματα αργότερα μπορούν να χρησιμοποιηθούν για την αναζήτηση στη βάση δεδομένων και την ανάκτηση των σχετικών δεδομένων. Για να κατέχει κάποιος ένα όνομα, πρέπει να κατέχει νομίσματα Namecoin και για να πραγματοποιηθεί αυτή η διαδικασία χρησιμοποιείται η κρυπτογράφηση δημόσιου κλειδιού (*public key cryptography*).

Το Namecoin έχει το δικό του blockchain στο οποίο εγγράφονται:

- transactions από NMC μεταξύ των χρηστών και
- domain names και σε ποιον ανήκουν.

Αποτελεί fork του bitcoin και χρησιμοποιεί τον ίδιο αλγόριθμο PoW που χρησιμοποιεί και αυτό. Λόγω των κοινών χαρακτηριστικών με το bitcoin, περιορίζεται και αυτό στα 21.000.000 νομίσματα, ενώ 50 νομίσματα NMC προκύπτουν ως reward από το mining.

Το μοντέλο του Bitcoin περιλαμβάνει ένα peer-to-peer σύστημα στο οποίο οι συμμετέχοντες επικυρώνουν συνεχώς μια σειρά συναλλαγών (transactions) χωρίς κεντρικό έλεγχο. Αυτό το μοντέλο εφαρμόστηκε στο DNS, τροποποιώντας το πρωτόκολλο του Bitcoin. Το αποτέλεσμα αυτής της διαδικασίας ονομάστηκε Namecoin (NMC). Αυτό που πραγματικά συνέβη είναι ότι δημιουργήθηκε ένα νέο genesis block, που αποτέλεσε τη βάση για τη δημιουργία ενός νέου blockchain. Αυτό διασφαλίζει ότι το Namecoin και το Bitcoin δεν αλληλεπιδρούν μεταξύ τους και δεν παρεμβαίνει το ένα στο blockchain του άλλου.

Τα επιπλέον στοιχεία σε σχέση με το πρωτόκολλο του bitcoin, εκτός από το διαφορετικό blockchain είναι τα εξής:

- διαφορετικό port, IRC bootstrap και message header
- νέοι τύποι transaction: new, first-update, update (NAME_NEW, NAME_FIRSTUPDATE και NAME_UPDATE.)
- Validation στους νέους τύπους transaction
- RPC calls για τη διαχείριση των names
- τέλη δικτύου για να μειωθεί το initial rush

2.5.4.1 Βασικές έννοιες και αρχές

- **Address**: ένα public key, που χρησιμοποιείται για τη λήψη των πληρωμών
- **Resource**: δεδομένα που κατανέμονται στο δίκτυο
- **Identifier**: ένα path προς το Resource.
- **Namespace**: μία ομαδοποιήση των Resources, περιγράφει τον τρόπο που τα Resources μεταφράζονται.

Κάθε resource στο Namecoin ΠΡΕΠΕΙ να βρίσκεται μέσα σε ένα namespace και ένα single resource ΔΕΝ ΠΡΕΠΕΙ να βρίσκεται μέσα σε πολλά namespaces.

Τα namespaces από μόνα τους δεν πρέπει να είναι χρησιμοποιήσιμα και εγγράψιμα. Κάθε namespace θα πρέπει να έχει το δικό του σκοπό και τη δική του χρήση. Δεν θα πρέπει να υπάρχουν διαφορετικά namespaces για τον ίδιο σκοπό. Τα resources πρέπει να αποθηκεύονται σε ένα block και συνεπώς στο blockchain. Το resource πρέπει να περιλαμβάνεται μέσα σε ένα block μόνο εάν η transaction που περιέχει το συγκεκριμένο resource είναι έγκυρη. Οι miners πρέπει να επιβεβαιώνουν πότε μία transaction είναι έγκυρη και πρέπει να φροντίζουν να μην συμπεριλαμβάνουν μέσα στα blocks όσες transactions δεν είναι έγκυρες.

Οι ομότιμοι χρήστες πρέπει να προωθούν τις transactions και τα blocks σε άλλους peers μόνο αν και τα 2 έχουν περάσει από τη διαδικασία του validation.

Πίνακας 12: Namecoin namespaces

Namespace	Application	Status
d/<domain>	Domain names for .bit TLD	active
id/<identity>	Public online identity system (e.g. addresses for BTC, NMC, email, ...)	active
p/<personal>	Personal namespace for PGP, SSL, identities, etc.	draft
m/<message>	Messaging system for Namecoin users	draft
a/<alias>	Alias system to map a name to another address	draft
tor/<domain>	Domain names for .tor TLD for onion websites	draft

2.5.4.2 Βασικές λειτουργίες

Οι βασικές λειτουργίες (key operations) του Namecoin εκτελούνται από transactions . Είναι οι εξής:

- name_new(hash(rand, name), value)
- name_firstupdate(name, rand, value)
- name_update(name, value)

Η μέθοδος που ακολουθείται είναι η εξής:

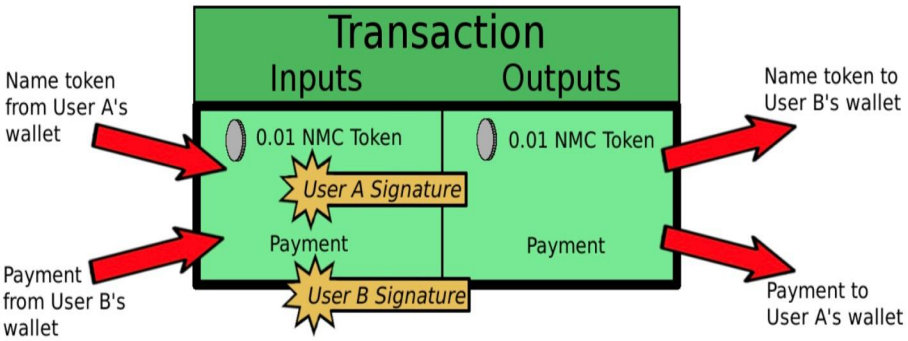
Κάθε key operation αντιστοιχεί σε μία transaction στο δίκτυο Namecoin. Μια λειτουργία μπορεί να δεσμεύσει (name_new), να αρχικοποιήσει (name_firstupdate), ή να ενημερώσει (name_update) ένα ζεύγος name/value.

Η name_firstupdate transaction απαιτεί ένα τέλος δκτύου. Τα τέλη δικτύου αναπαριστούν namecoins που έχουν καταστραφεί. Τα κρυπτονομίσματα που έχουν δημιουργηθεί στα πρότυπα του bitcoin έχουν ούτως ή αλλιώς ένα transaction fee που επιβάλλεται από τη διαδικασία του mining. Το τέλος δικτύου είναι μία επιπλέον χρέωση και όχι η ίδια.

2.5.5 Η διαδικασία των transactions

Στο Namecoin η εγγραφή ενός ονόματος είναι μια διαδικασία που εκτελείται σε 2 βήματα.

1. Ο χρήστης αρχικά προπληρώνει ένα όνομα σε μία νέα συναλλαγή *(pre-order transaction)* που περιλαμβάνει *hash(name)* μέσα στη συναλλαγή. Αυτή η διαδικασία δεν αποκαλύπτει το όνομα που προσπαθεί να εγγράψει η transaction. Αφότου η pre-order transaction επιβεβαιωθεί από το δίκτυο -επαρκής αριθμός blocks, συνήθως 10, προστίθενται στο blockchain για να είναι υπολογιστικά αδύνατο για έναν miner να ξαναγράψει το blockchain history και να αντιστρέψει τη συναλλαγή-, τότε ο χρήστης μπορεί να αποκαλύψει το όνομα που προσπαθούσε να εγγράψει.
2. Η αποκάλυψη του ονόματος γίνεται με την αποστολή μίας 2ης transaction στο δίκτυο που ολοκληρώνει το βήμα της εγγραφής. Ο χρήστης περιλαμβάνει στη 2η συναλλαγή το name/value ζευγάρι.



Σχήμα 25: Η ανατομία μιας Namecoin transaction

Η κρυπτογραφική διεύθυνση (δηλαδή το public key) που χρησιμοποιήθηκε για να υπογραφούν οι 2 συναλλαγές, γίνεται ο κύριος κάτοχος νέων εγγεγραμμένων ζευγαριών name/value. Ο μόνος τρόπος για να μπορέσει κάποιος άλλος χρήστης να αποκτήσει πρόσβαση σε αυτό το domain είναι μόνο αν ο κύριος κάτοχος μεταφέρει την κυριότητα στον άλλον χρήστη. Για να εγγράψει ένας χρήστης ένα domain στο blockchain το αντίτιμο είναι 0.01 NMC. Το τέλος συναλλαγής (transaction fee) καταστρέφεται από το ίδιο δίκτυο όταν η εγκυρόττητα του transaction επιβεβαιώνεται. Οι εγγραφές ονομάτων λήγουν μετά από συγκεκριμένο χρονικό διάστημα, συνήθως κάθε 36.000 blocks (περίπου κάθε 250 ημέρες), διαδικασία που δεν έχει τέλος συναλλαγής.

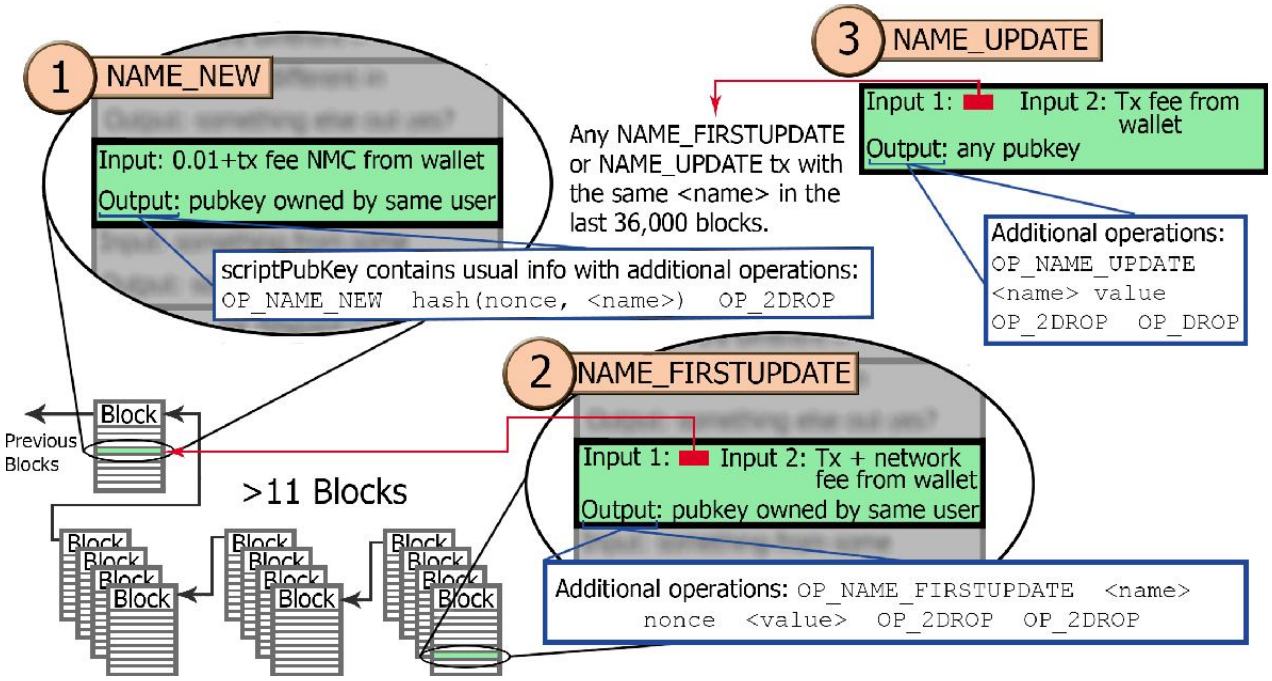
2.5.5.1 Τα χαρακτηριστικά των transactions

Για να γίνει κατανοητή η διαδικασία εγγραφής ενός domain name πρέπει να μελετηθούν οι τεχνικές λεπτομέρειες των βασικών λειτουργιών του Namecoin.

NAME_NEW: Για να ξεκινήσει κάποιος, θα πρέπει να επιλέξει ένα token που αναπαριστά ένα name και του οποίου το value μπορεί να αλλαχθεί από όποιον κατέχει το token. Το επόμενο βήμα για να καταχωρηθεί το όνομα είναι να κάνει ο χρήστης μια συναλλαγή που χρησιμοποιεί την script λειτουργία NAME_NEW. Χρησιμοποιώντας ο χρήστης τη λειτουργία NAME_NEW, δείχνει ενδιαφέρον για ένα name, δηλώνοντάς το σε hashed format στο scriptPubKey της transaction.

NAME_FIRSTUPDATE: Αφού πραγματοποιηθεί αυτό και ύστερα από αναμονή για 12 ή περισσότερα blocks επάνω σε αυτό που περιέχει την transaction NAME_NEW, ο ίδιος χρήστης μπορεί να χρησιμοποιήσει το output της NAME_NEW transaction ως input για τη NAME_FIRSTUPDATE transaction. Μόλις ολοκληρωθεί αυτή η διαδικασία, αυτό θα συνδέσει το επιλεγμένο όνομα (name) με την τιμή (value) που επιλέγεται από το χρήστη. Παρόμοια με το NAME_NEW, το NAME_FIRSTUPDATE επιτρέπει στα δεδομένα να καταχωρηθούν στο blockchain ως μέρος του scriptPubKey μιας ειδικής transaction. Για να δημιουργήσει κάποιος μια NAME_NEW transaction, θα επιλέξει ως input το output της NAME_NEW transaction. Στη συνέχεια, θα χρησιμοποιήσει μια άλλη διεύθυνση που ελέγχει ως output της συναλλαγής. Το scriptPubKey αυτής της transaction θα περιέχει ένα NAME_FIRSTUPDATE, το επιθυμητό name, το τυχαίο nonce που χρησιμοποιείται στο NAME_NEW hash commitment και την πρώτη value

που θα πάρει το name. Ένας miner επαληθεύει την εγκυρότητα της transaction. Το output αυτής της transaction περιέχει το token που αναπαριστά το ζεύγος name/value, και όποιος μπορεί να ξεκλειδώσει και να ξοδέψει το output, μπορεί να χρησιμοποιήσει την λειτουργία NAME_UPDATE



Σχήμα 26: Διαδικασία εγγραφής ενός ονόματος- βασικές λειτουργίες Namecoin

NAME_UPDATE: Η τρίτη και τελευταία λειτουργία στο Namecoin είναι η NAME_UPDATE. Και πάλι, τα ορίσματα αυτής της λειτουργίας (το name και το newValue) αποθηκεύονται στο scriptPubKey μια ειδικής transaction. Αυτή η transaction πρέπει να έχει ως input NAME_FIRSTUPDATE ή output NAME_UPDATE με το ίδιο name. Αυτή η λειτουργία έχει τρεις χρήσεις: ενημέρωση, ανανέωση και ανταλλαγή ενός name. Εάν ο χρήστης θέλει να αλλάξει την value που σχετίζεται με ένα name, θα ενημερώσει το name με αυτή τη λειτουργία, παρέχοντας μια newValue. Εάν τα ονόματα λήξουν, όπως κάνουν στο Namecoin, τότε αυτή η λειτουργία μπορεί επίσης να χρησιμοποιηθεί για την ανανέωση ενός name με την παροχή μιας newValue που είναι ίδια με την παλιά τιμή. Σε οποιαδήποτε από αυτές τις περιπτώσεις, ο χρήστης θα χρησιμοποιήσει μια address ως output της transaction. Ένας ακόμη λόγος για να κάνει ένας χρήστης μια NAME-UPDATE transaction είναι να ανταλλάξει το ειδικό νόμισμα με έναν άλλο χρήστη. Σε αυτή την περίπτωση, ο χρήστης θα θέσει ως output μια από τις addresses των άλλων χρηστών αντί για τις δικές του. Μόλις πραγματοποιηθεί η transaction, ο άλλος χρήστης θα έχει τον έλεγχο του ειδικού νομίσματος και μπορεί να αλλάξει την value του.

2.5.5.2 Πώς γίνεται το validation σε μια transaction;

Μια transaction εισάγεται στο block αφού ακολουθηθεί η εξής διαδικασία validation:

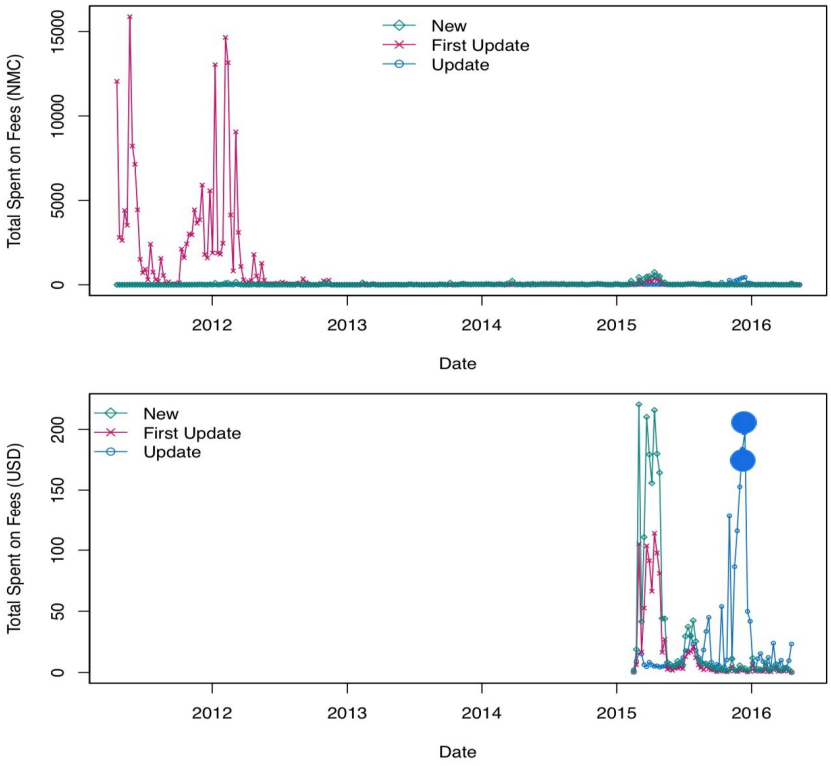
- Το validation pass που εκτελείται στο bitcoin

- εάν το transaction version δεν υποδεικνύει namecoin, τότε κανένα input δεν μπορεί να είναι namecoin output
- εάν το transaction version δεν υποδεικνύει namecoin, τερματίζει με επιτυχία
- Το transaction μπορεί να καταχωρηθεί σε ένα block όταν το παρόν τέλος δικτύου είναι μικρότερο από το τέλος δικτύου στο output της transaction
- εάν αυτό είναι ένα name_update λειοτυργία, ένα ακριβώς από τα inputs είναι name_update ή name_firstupdate και η δαιφορά σε αριθμό block είναι περίπου 12000. Επίσης κανένα άλλο input δεν είναι name operation.
- εάν αυτό είναι μία name_firstupdate λειτουργία, ένα ακριβώς από τα inputs είναι μία name_new λειτουργία με διαφορά block τουλάχιστον 12 αλλά όχι περισσότερο από 12000. κανένα άλλο input δεν είναι name operation.
- εάν αυτό είναι μία name_new λειτουργία, κανένα από τα inputs δεν είναι name operation.
- μία name_firstupdate λειτουργία πρέπει να εφαρμόζεται σε ένα εντελώς καινούριο όνομα ή ένα όνομα που έχει λήξει. Τα καινούρια ονόματα είναι valid μετα τη λειτουργία name_firstupdate
- Ένα όνομα λήγει 12000 blocks μετά από την τελευταία λειτουργία που πραγματοποιήθηκε σε αυτό.

2.5.5.3 Τα τέλη δικτύου

Ο σκοπός των τελών δικτύου είναι να ελαχιστοποιήσει το αρχικό rush.

- Τα τέλη δικτύου ξεκινούν από τα 50 NMC ανά λειτουργία στο genesis block.
- Σε κάθε μπλοκ τα τέλη δικτύου μειώνονται σε 10^{-8} NMC με βάση τον αλγόριθμο
  - res = 500000000 >> floor(nBlock / 8192), όπου >> δεξιά ολίσθηση και floor η συνάρτηση κατώφλι
  - res = res - (res >> 14)*(nBlock % 8192), όπου το % αντιστοιχεί στο ακέραιο υπόλοιπο της διαίρεσης.
- το nBlock είναι 0 στο genesis block
- Αυτό είναι μία μείωση της τάξης του 50% κάθε 8192 blocks (περίπου 2 μήνες)
- Σε κάθε μπλοκ δημιουργούνται 50 NMC αρχικά. Έτσι ο μέγιστος αριθμός registrations στα πρώτα 8192 blocks είναι τα 2/3 του 8192, δηλαδή 5461 registrations.
- Το difficulty ξεκινάει στο 512



Σχήμα 27: Το εβδομαδιαίο σύνολο των transaction fees για τις transactions new, first_update και name_update, src: https://www.poloniex.com/Poloniex

2.5.6 Το blockchain

Το blockchain του Namecoin ξεκίνησε στις 18 Απριλίου 2011 και από τότε περίπου κάθε 10 λεπτά προστίθεται ένα καινούριο μπλοκ. Αρχικά το reward προς τους miners για κάθε νέο μπλοκ ήταν 50 NMC. Στη συνέχεια, το reward μειωνόταν κατά το ήμισυ κάθε 210.000 blocks (περίπου κάθε 4 χρόνια). Για να συμμετέχει ένας κόμβος *(node)* στο δίκτυο του Namecoin, χρειάζεται να λειτουργήσει ένας Namecoin client που διατηρεί ένα ολόκληρο αντίγραφο του blockchain του Namecoin και να το συγχρονίσει με το P2P δίκτυο, προσθέτοντας και επικυρώνοντας νέα blocks από τους συνδεδεμένους peers του δικτύου.

Οι συναλλαγές με Namecoin απαιτούν την ψηφιακή υπογραφή του κατόχου ενός λογαριασμού για την αποτροπή κλοπής και κάθε συναλλαγή δημοσιεύεται στο blockchain. Το blockchain μπορεί να επεκταθεί με νέες συναλλαγές από οποιονδήποτε συμμετέχοντα, και οι συμμετέχοντες (miners) αποκτούν καινούριο νόμισμα namecoin και τέλη συναλλαγής από τις συναλλαγές για την εκτέλεση αυτής της λειτουργίας.

Οι επεκτάσεις του blockchain απαιτούν Proof Of Work που περιορίζει τη διαδικασία (σε περίπου μία επέκταση κάθε δέκα λεπτά), η οποία επιτρέπει σταθερό ρυθμό πληθωρισμού, επαρκή ανταγωνισμό μεταξύ των συμμετεχόντων για την επέκταση του blockchain και ικανοποιητικό χρόνο για την απόκτηση και την επαλήθευση του ιστορικού του blockchain για τους νέους συμμετέχοντες. Ανεπίσημα, το πρωτόκολλο του Proof Of Work στο Namecoin έχει σκοπό να διατηρήσει τις ακόλουθες δύο βασικές ιδιότητες του blockchain:

- Κάθε συμβαλλόμενο μέρος συμφωνεί με την εντολή και την ορθότητα των συναλλαγών στο blockchain.
- Κάθε συμβαλλόμενο μέρος μπορεί να δημοσιεύσει μια συναλλαγή, η οποία στη συνέχεια θα επικυρωθεί, και αν είναι έγκυρη, θα συμπεριληφθεί στο blockchain με μία μικρή καθυστέρηση.

2.5.7 Η διαδικασία του mining

Το Namecoin προέκυψε σαν fork του Bitcoin και η διαδικασία του mining σε αυτό λειτουργεί όπως στο bitcoin. Χρησιμοποιεί τον Proof-of-work αλγόριθμο SHA-256. Η διαδικασία του mining ακολουθεί τα εξής βήματα:

- αρχικά συλλέγονται όλες οι συναλλαγές που έχουν μεταδοθεί στο δίκτυο, για να πραγματοποιηθεί έλεγχος της εγκυρότητάς τους
- στη συνέχεια επικυρώνονται όλες οι συναλλαγές που συμπεριλήφθηκαν μέσα στο block
- ύστερα επιλέγεται από το blockchain το πιο πρόσφατο μπλοκ που βρίσκεται στο μεγαλύτερο σε μήκος μονοπάτι και το hash value που βρίσκεται στο block header του, εισάγεται και στο νέο μπλοκ
- μετά επιλύεται το proof-of-work πρόβλημα και η λύση του μεταδίδεται σε όλο το δίκτυο
- οι υπόλοιποι nodes του δικτύου ελέγχουν την ορθότητα του proof-of-work μάσα από την εξής διαδικασία: ελέγχεται το μπλοκ και τα transactions που περιλαμβάνει, δηλαδή υπολογίζεται το hash value του μπλοκ με τον παράγοντα nonce να έχει τροποποιηθεί από τη διαδικασία mining. Το νέο μπλοκ είναι έγκυρο, στην περίπτωση που το proof-of-work που μετέδωσε ο miner ταυτίζεται με το hash value
- αν οι κόμβοι (nodes) του δικτύου φτάσουν σε συναίνεση (consensus) για την εγκυρότητα του μπλοκ, τότε αυτό εισάγεται στο blockchain, αλλιώς απορρίπτεται και τα δεδομένα του γίνονται null.

Η διαδικασία διαρκεί περίπου 10 λεπτά και κάθε φορά που τελειώνει, επαναλαμβάνεται ξανά.

2.5.7.1 Proof-of-work

Η αξία και η σταθερότητα των κρυπτονομισμάτων συνδέονται άμεσα με την ποσότητα του Proof Of Work που εμπλέκεται στους υπολογισμούς των μπλοκ, επειδή αυτή η διαδικασία είναι που κρατά τα δεδομένα κατανεμημένα και ασφαλή μέσα στο blockchain. Τόσο για το Bitcoin όσο και για το Namecoin το PoW εμφανίζεται από τον υπολογισμό του κατακερματισμού ενός νέου block και μια τυχαία nonce ξανά και ξανά μέχρι ο υπολογισμένος κατακερματισμός να έχει έναν ορισμένο αριθμό από αρχικά μηδενικά. Ο αριθμός των κορυφαίων μηδενικών που απαιτούνται από το hash αναφέρεται ως difficulty.

Η εύρεση ενός σωστού PoW ακολουθεί μία διαδικασία από την πλευρά του miner.

1. Ορίζει ελεύθερα τα πεδία nNonce και coinbase

2. Εφαρμόζει 2 φορές τον αλγόριθμο SHA256 και υπολογίζει συνεχώς το hash value του block header
3. Ελέγχει αν το hash value είναι μικρότερο από το target value T

SHA2562 (nVersion||HashP revBlock||HashMerkleRoot||nTime||nBits||nNonce)

4. Αν ισχύει το βήμα 3, τότε σημαίνει πως ο miner έχει υπολογίσει με επιτυχία ένα proof-of-work. Τέλος, ο miner μεταδίδει στο δίκτυο το καινούριο μπλοκ μαζί με το proof-of-work.

Το Namecoin έχει υψηλό difficulty για το proof-of-work, επειδή είναι παρόμοιο με το Bitcoin και υποστηρίζει merged-mining με Bitcoin. Αυτό σημαίνει ότι οι miners που κάνουν εξόρυξη Bitcoin μπορούν επίσης να κάνουν εξόρυξη namecoin την ίδια ώρα χωρίς επιπλέον εργασία. Ουσιαστικά, αυτό συμβαίνει επειδή ο miner χρησιμοποιεί την υπολογιστική του ισχύ για την επίλυση ενός κρυπτογραφικού προβλήματος που ικανοποιεί το proof-of-work και για τα 2 blockchain ταυτόχρονα. Αυτό είναι επωφελές για τους miners, επειδή ανταμείβονται με νομίσματα και από τα δύο συστήματα και βοηθά το Namecoin επειδή το δίκτυο του αποκτά μια πολύ αυξημένη ποσότητα hash power που δεν θα είχε στην περίπτωση που δεν υποστήριζε merged-mining. Συμπεριλαμβανομένων και των merged miners, το Namecoin περιλαμβάνει το 1/3 του hash rate του Bitcoin. Αυτό παρέχει ανθεκτικότητα στις 51% επιθέσεις.

2.5.7.2 Merged-mining

Η διαδικασία του merge-mining ξεκίνησε στο μπλοκ 19200 του Namecoin. Αυτό που συνέβη είναι ότι το λογισμικό του Namecoin άλλαξε για να δεχθεί Bitcoin blocks ως έγκυρα. Οι miners που πραγματοποιούν merged-mining συλλέγουν Namecoin transactions, εφαρμόζουν hash functions και συμπεριλαμβάνουν τη hash value που προκύπτει σε ένα Bitcoin block. Εάν ο miner βρει ένα μπλοκ που συναντάει το όριο dfficulty του Namecoin ενσωματώνεται στο δίκτυο Namecoin μόνο. Εάν το block συναντήσει το όριο difficulty του Bitcoin, τότε το μπλοκ ενσωματώνεται και στα 2 δίκτυα και έτσι οι miners έχουν διπλό όφελος. Το δίκτυο Bitcoin αγνοεί τα επιπλέον δεδομένα, αλλά το blockchain του Namecoin αποθηκεύει δεδομένα Bitcoin.Το μειονέκτημα που μπορεί να προκύψει είναι η εξάρτηση του ενός blochchain από το άλλο.

Μόλις 1.7% (67,513) από το σύνολο των transactions βρίσκονται σε Namecoin blocks καθώς το υπόλοιπο 98.3% (3.9M) βρίσκεται σεωmerge-mined blocks. Όσον αφορά τις λειτουργίες του Namecoin, περισσότερρες από το 99% αυτών βρίσκονται σε merge-mined blocks.

Πίνακας 13: Η δραστηριότητα στο Namecoin διαχωρισμένη από το κριτήριο της απλής ή της συγχωνευμένης εξόρυξης

			Name operations		
	Blocks	Transactions	`new`	`firstupdate`	`update`
Normally mined	19,330	67,513	5484	2817	2624
Merge-mined	265,747 (93.2%)	3,900,753 (98.3%)	964,778 (99.4%)	867,733 (99.7%)	1,081,790 (99.8%)

2.6 Libra

2.6.1 Σκοπός δημιουργίας

Το Libra είναι ένα ψηφιακό κρυπτονόμισμα που βασίζεται σε permissioned Blockchain. Είναι stablecoin, δηλαδή βασίζεται σε περιουσιακά στοιχεία και έχει στόχο να κινείται γύρω από μια συγκεκριμένη τιμή, αποφεύγοντας τις διακυμάνσεις αξίας που παρουσίαζαν τα υπόλοιπα κρυπτονομίσματα.

Σύμφωνα με το whitepaper του Libra, υπάρχουν περίπου 1,7 δισεκατομμύρια ενήλικες σε όλο τον κόσμο χωρίς πρόσβαση σε παραδοσιακές χρηματοπιστωτικές υποδομές. Ωστόσο, το 1 δισεκατομμύριο από αυτούς έχει κινητό τηλέφωνο και περίπου τα 500 εκατομμύρια έχουν πρόσβαση στο Διαδίκτυο. Το Libra προσπαθεί να δημιουργήσει ένα παγκόσμιο κρυπτονόμισμα ικανό να προσφέρει ασφαλείς χρηματοπιστωτικές υπηρεσίες και χρηματοοικονομική υποδομή με χαμηλές αμοιβές για ανθρώπους που δεν έχουν χρήματα σε κάποια τράπεζα, αλλά έχουν πρόσβαση στο Διαδίκτυο και σε μια κινητή συσκευή.

Στις 18 Ιουνίου 2019 η Facebook ανακοίνωσε επίσημα με την έκδοση whitepaper τη δημιουργία του κρυπτονομίσματος, το οποίο στοχεύει στην αλλαγή των συναλλαγών μέσω Διαδικτύου. Η θυγατρική εταιρεία της Facebook, Calibra, μαζί με άλλες 22 εταιρείες κολοσσούς – ανάμεσά τους οι PayPal, Mastercard, Visa, eBay, Spotify, Uber, Vodafone- δημιούργησαν τον ανεξάρτητο μη κερδοσκοπικό φορέα Libra Association με έδρα τη Γενεύη, που θα έχει τον έλεγχο του νέου ψηφιακού νομίσματος και των συναλλαγών που θα πραγματοποιούνται με αυτό. Μέχρι σήμερα βρίσκεται σε στάδιο πρωτοτύπου, δεν υπάρχει ούτε το νόμισμα, ούτε το δίκτυο που θα το υποστηρίζει, παρά μόνο ο πρώτος πειραματικός κώδικας.

Η πρώτη έκδοση του Libra αναμένεται εντός του πρώτου εξαμήνου 2020. Τον πρώτο καιρό αναμένεται να έχει μικρό αριθμό χρηστών (100 μέλη έως το λανσάρισμα του νομίσματος), ο οποίος σταδιακά θα αυξάνεται. Κάθε μέλος θα έχει μία ψήφο σε ζητήματα που αφορούν το δίκτυο του κρυπτονομίσματος, ενώ μετά το τέλος του 2109 η Facebook σκοπεύει να μην έχει ηγετικό ρόλο στον οργανισμό. Οι συναλλαγές μεταξύ των χρηστών θα πραγματοποιούνται με το πορτοφόλι κρυπρογράφησης που θα παρέχει η εταιρεία Calibra. Το πορτοφόλι θα επιτρέπει στους χρήστες να στέλνουν το Libra μέσω της υπηρεσίας μηνυμάτων σε πλατφόρμες όπως το Facebook Messenger και το WhatsApp, ενώ για όσους δεν διαθέτουν λογαριασμό στο Facebook, η Calibra θα διαθέτει το πορτοφόλι ως εφαρμογή IOS και Android.

Το πορτοφόλι Calibra αν και θυγατρική του Facebook, δεν θα μοιράζεται κανένα οικονομικό στοιχείο με το Facebook ή τρίτους χωρίς τη συγκατάθεση του πελάτη. Η εταιρεία δηλώνει στο έγγραφο του Customer Commitment ότι τα δεδομένα της θα παραμείνουν τελείως ξεχωριστά από τα δεδομένα που προέρχονται από τις κοινωνικές πλατφόρμες του Facebook, εκτός εάν δοθεί συγκατάθεση από χρήστες που χρησιμοποιούν το πορτοφόλι Calibra.[2]

Αν και δεν υπάρχουν τράπεζες μεταξύ των αρχικών μελών, έχουν ήδη ξεκινήσει συζητήσεις με μια σειρά χρηματοπιστωτικών ιδρυμάτων προκειμένου να συμμετάσχουν, δήλωσε ο Τζον Λάμπερτ, εκτελεστικός αντιπρόεδρος ψηφιακών λύσεων στη

Mastercard. Έτσι λοιπόν η Libra Association σκοπεύει να αντλήσει χρήματα τους επόμενους μήνες μέσω ιδιωτικής τοποθέτησης τους.

2.6.2 Στοιχεία για το δημιουργό

Οι δημιουργοί του νομίσματος είναι οι Morgan Beller, David Marcus και Kevin Weil. Συγκεκριμένα ο Morgan Beller ήταν ο πρώτος άνθρωπος που εργάστηκε στην πρωτοβουλία του Facebook, όταν η εταιρεία ξεκίνησε τη διερεύνηση για το κρυπτονόμισμα και το blockchain του το 2017. Το Μάιο του 2018 ο David A Marcus, αντιπρόεδρος του Facebook, πήρε μετάθεση από το τμήμα Facebook Messenger στο νέο τμήμα του blockchain. Λίγες μέρες αργότερα δημοσιοποιήθηκαν οι πρώτες αναφορές για την πρωτοβουλία του Facebook να σχεδιάσει ένα κρυπτονόμισμα με υπεύθυνο τον Marcus, ενώ μέχρι το Φεβρουάριο του 2019, περισσότεροι από 50 μηχανικοί είχαν ξεκινήσει να εργάζονται στο καινούριο project

Ο David Marcus εξήγησε το πως η ονομασία «Libra» προήλθε από τη ρωμαϊκή ζυγαριά, που θεωρείται σύμβολο της δικαιοσύνης και τη γαλλική λέξη «liberte» που σημαίνει ‘ελευθερία’. Συγκεκριμένα δήλωσε: *«Ελευθερία, δικαιοσύνη και χρήματα, που είναι ακριβώς αυτό που προσπαθούμε να κάνουμε εδώ»*.

2.6.3 Η νομισματική πολιτική

Το Libra έχει σχεδιαστεί για να είναι ένα σταθερό ψηφιακό κρυπτονόμισμα που θα υποστηρίζεται πλήρως από ένα αποθεματικό πραγματικών περιουσιακών στοιχείων - το Reserve Libra - και θα υποστηρίζεται από ένα ανταγωνιστικό δίκτυο συναλλαγών που αγοράζει και πωλεί το Libra.

Τα χρήματα για το αποθεματικό θα προέρχονται από δύο πηγές: τα commitments των μελών και των χρηστών του Libra. Η ένωση θα καταβάλει τα κίνητρα σε νόμισμα Libra στα ιδρυτικά μέλη για να ενθαρρύνει τους χρήστες, τους εμπόρους και τους προγραμματιστές. Από την πλευρά του χρήστη, για να δημιουργηθούν νέα νομίσματα Libra, πρέπει να υπάρξει ισοδύναμη αγορά του Libra για το fiat και μεταφορά αυτού του fiat στο αποθεματικό. Ως εκ τούτου, το αποθεματικό θα αυξάνεται όσο αυξάνεται η ζήτηση των χρηστών για Libra. Εν ολίγοις, υπάρχει μόνο ένας τρόπος για να δημιουργηθεί περισσότερο Libra - αγοράζοντας περισσότερο Libra για fiat προκειμένου να αυξηθεί το απόθεμα.

Οι χρήστες του Libra δεν λαμβάνουν επιστροφή από το αποθεματικό. **Το αποθεματικό θα επενδυθεί** σε περιουσιακά στοιχεία χαμηλού κινδύνου που θα αποφέρουν κέρδος με την πάροδο του χρόνου. Τα έσοδα από αυτή τη διαδικασία θα διατεθούν πρώτα για τη στήριξη των λειτουργικών εξόδων της Libra Association - για τη χρηματοδότηση επενδύσεων για την ανάπτυξη του συστήματος, επιχορηγήσεων σε μη κερδοσκοπικούς οργανισμούς, στην έρευνα μηχανικής κλπ.

Τα πραγματικά περιουσιακά στοιχεία θα είναι μια συλλογή στοιχείων ενεργητικού χαμηλής μεταβλητότητας, συμπεριλαμβανομένων των τραπεζικών καταθέσεων και των κρατικών τίτλων σε νομίσματα από σταθερές και αξιόπιστες κεντρικές τράπεζες. Καθώς η αξία του Libra θα συνδεθεί αποτελεσματικά με νομίσματα fiat, θα υπάρξουν διακυμάνσεις στην αξία του. Η σύνθεση του αποθεματικού αποσκοπεί στο μετριασμό

της πιθανότητας και της σοβαρότητας αυτών των διακυμάνσεων, ιδιαίτερα αρνητικής κατεύθυνσης (δηλαδή ακόμη και σε οικονομικές κρίσεις).

Οι χρήστες δεν θα επικοινωνούν απευθείας με το απόθεμα. Αντίθετα, για να υποστηρίξει την υψηλότερη απόδοση, θα υπάρχουν εξουσιοδοτημένοι μεταπωλητές οι οποίοι θα είναι οι μόνες εξουσιοδοτημένες οντότητες από την ένωση να πραγματοποιούν συναλλαγές μεγάλων ποσοτήτων fiat και Libra μέσα και έξω από το αποθεματικό. Αυτοί οι εξουσιοδοτημένοι μεταπωλητές θα παρέχουν ρευστότητα για τους χρήστες που επιθυμούν να μετατρέψουν τα μετρητά σε Libra και αντίστροφα.

Η ένωση δεν θέτει νομισματική πολιτική. Θα κόβει και θα καίει νομίσματα μόνο ως απάντηση στη ζήτηση από εξουσιοδοτημένους μεταπωλητές. Για τα νέα νομίσματα που πρέπει να κοπούν, πρέπει να υπάρξει ανάλογη πληρωμή από τους μεταπωλητές στο αποθεματικό. Μέσω της αλληλεπίδρασης με εξουσιοδοτημένους μεταπωλητές, η Libra Association δημιουργεί αυτόματα νέα νομίσματα όταν η ζήτηση αυξάνεται και τα καταστρέφει όταν η ζήτηση μειώνεται. Επειδή το αποθεματικό δεν θα διαχειρίζεται ενεργά, οποιαδήποτε ανατίμηση ή υποτίμηση της αξίας του Libra θα προέλθει αποκλειστικά από τις κινήσεις της αγοράς συναλλάγματος.

Η ένωση θα ενθαρρύνει την εισαγωγή του Libra σε πολλές ηλεκτρονικές συναλλαγές σε όλο τον κόσμο. Αυτές οι συναλλαγές προσφέρουν τόσο δικτυακές πύλες όσο και εφαρμογές για τους χρήστες για να μπορούν να αγοράζουν και να πωλούν Libra. Η ένωση επιδιώκει σχέσεις με τις κύριες αγορές ανταλλαγής κρυπτονομισμάτων και τα κορυφαία τραπεζικά ιδρύματα ως εξουσιοδοτημένους μεταπωλητές για να επιτρέψουν στους ανθρώπους την ευκαιρία να ανταλλάξουν τα τοπικά νομίσματά τους για το Libra όσο το δυνατόν πιο εύκολα.

2.6.4 Τα χαρακτηριστικά των transactions

Οι χρήστες του Libra blockchain ενημερώνουν το ledger state μέσω της υποβολής συναλλαγών. Σε υψηλό επίπεδο (σε προγραμματιστικό), μια συναλλαγή αποτελείται από ένα **transaction script** (γραμμένο σε Move με μορφή bytecode) και ορίσματα για το transaction script (π.χ. μια διεύθυνση παραλήπτη ή το πλήθος των νομισμάτων Libra που αποστέλλει ένας χρήστης). Ένας **validator** εκτελεί τη συναλλαγή με τον εξής τρόπο: εκτελεί το script με είσοδο τα ορίσματα του και το τρέχον ledger state και παράγει μια έξοδο συναλλαγής. Το ledger state δεν αλλάζει μέχρι να γίνει commit η συναλλαγή στο στάδιο του consensus.

Κάθε συναλλαγή παράγει **ένα transaction output**. Εκτελώντας μίας συναλλαγή T_i παράγεται ένα νέο ledger state S_i, καθώς και ένα execution status code, το ποσό του gas που καταναλώθηκε (gas usage) και μία event list. Όλα μαζί συνιστούν ένα transaction output O_i. Το execution status code υποδεικνύει το αποτέλεσμα της συναλλαγής (πχ επιτυχία, αποτυχία, εξάντληση gas).

Μία **event list** αντιστοιχεί σε ένα σύνολο από γεγονότα, τα οποία όμως είναι δευτερεύουσας σημασίας. Η εκτέλεση Move scripts ενδέχεται να οδηγήσει Κάθε event σχετίζεται με ένα μοναδικό κλειδί, μέσω του οποίου προσδιορίζεται η προέλευση του (από ποιο δομικό στοιχείο προήλθε) και ορισμένες πληροφορίες για αυτό. Όταν μία συναλλαγή υποβάλλεται ως commited, γεγονότα, τα οποία προκαλούνται από μία συναλλαγή, προστίθονται στο κοινά συμφωνημένο ledger history και παρέχουν πληροφορίες για το αν μία συναλλαγή οδήγησε σε ένα συγκεκριμενο αποτελέσμα. Για

παράδειγμα, μία συναλλαγή πληρωμής οδηγεί σε ένα γεγονός που επιτρέπει στον παραλήπτη να επιβεβαιώσει πως έλαβε το ποσό.

2.6.4.1 Η δομή μιας transaction

Μια συναλλαγή αντιστοιχεί σε ένα signed message που περιέχει τα ακόλουθα δομικά στοιχεία:

- **Sender address**: Η διεύθυνση λογαριασμού του αποστολέα της συναλλαγής. Το VM διαβάζει τον αριθμό ακολουθίας, το κλειδί ελέγχου ταυτότητας(authentication key) και το υπόλοιπο από τον LibraAccount.T resource, που είναι αποθηκευμένος εντός αυτής της διεύθυνσης.
- **Sender public key:** Το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή της συναλλαγής. Το hash value αυτού του δημόσιου κλειδιού πρέπει να ταιριάζει με το κλειδί ελέγχου ταυτότητας που είναι αποθηκευμένο εντός του LibraAccount.T resource του αποστολέα.
- **Program**: Ένα transaction script σε γλώσσα Move προς εκτέλεση, μια προαιρετική λίστα δεδομένων εισόδων στο script και μια προαιρετική λίστα Move bytecode modules.
- **Gas price**: Ο αριθμός των Libra νομισμάτων που ο αποστολέας είναι διατεθειμένος να πληρώσει ανά μονάδα gas για να εκτελεστεί η συναλλαγή.
- **Maximum gas amount**: Ο μέγιστος αριθμός μονάδων gas που επιτρέπεται να καταναλώσει η συναλλαγή πριν σταματήσει να εκτελείται.
- **Sequence number:** Ένας unsigned ακέραιος αριθμός που πρέπει να είναι ίσος με τον αριθμό ακολουθίας από τον LibraAccount.T resource του αποστολέα. Μετά την εκτέλεση της συναλλαγής, ο αριθμός αυτός αυξάνεται κατά ένα. Δεδομένου ότι μόνο μία συναλλαγή μπορεί να πραγματοποιηθεί για έναν δεδομένο αριθμό ακολουθίας, οι συναλλαγές δεν μπορούν να επαναληφθούν.

2.6.4.2 Περιγραφή της διαδικασίας εκτέλεσης μιας transaction

Η εκτέλεση μιας συναλλαγής προχωρά μέσω μιας σειράς έξι βημάτων μέσα στο VM. Η εκτέλεση είναι ξεχωριστή από την επικαιροποίηση του ledger state. Πρώτον, μια συναλλαγή εκτελείται ως μέρος μιας προσπάθειας να φτάσει σε συμφωνία σχετικά με την σειρά εμφάνισης της. Σαν συνέχεια, εάν επιτευχθεί συμφωνία, η έξοδος της συναλλαγής εγγράφεται στο ledger history.

Η εκτέλεση μιας συναλλαγής περιλαμβάνει τα ακόλουθα έξι βήματα:

1. **Έλεγχος υπογραφής.** Η υπογραφή στη συναλλαγή πρέπει να ταιριάζει με το δημόσιο κλειδί του αποστολέα (sender public key) και τα δεδομένα συναλλαγής. Αυτό το βήμα είναι μια λειτουργία μόνο της ίδιας της συναλλαγής - δεν απαιτεί ανάγνωση των δεδομένων από τον λογαριασμό του αποστολέα.
2. **Εκτέλεση prologue.** Η διαδικασία prologue πιστοποιεί τον αποστολέα της συναλλαγής, εξασφαλίζει ότι ο αποστολέας διαθέτει επαρκές πλήθος από νομίσματα Libra, ώστε να πληρώσει το ποσό Maximum gas amount που προσδιορίζεται στη συναλλαγή, καθώς και ελέγχει ότι η συναλλαγή δεν είναι επανάληψη μιας προηγούμενης συναλλαγής (ώστε να αποφύγουμε φαινόμενα double spend). Όλοι αυτοί οι έλεγχοι υλοποιούνται στο Move μέσω της

διαδικασίας prologue του LibraAccount module. Η μέτρηση του gas διακόπτεται κατά την εκτέλεση του prologue. Συγκεκριμένα, η διαδικασία του prologue υλοποιεί τα εξής:

- Ελέγχει αν το hash value του sender public key ταυτίζεται με το κλειδί ελέγχου ταυτότητας που είναι αποθηκευμένο εντός του λογαριασμού του αποστολέα. Χωρίς αυτόν τον έλεγχο, το VM θα λάμβανε λανθασμένα μια συναλλαγή με μια κρυπτογραφικά έγκυρη υπογραφή, παρόλο που δεν υπάρχει καμία αντιστοιχία με το κλειδί που σχετίζεται με το λογαριασμό.
- Ελέγχει αν ο αποστολέας διαθέτει επαρκές απόθεμα από νομίσματα Libra, ώστε να καταβάλλει το απαιτούμενο ποσό για τη συναλλαγή σε gas. Ελέγχει, δηλαδή, αν ισχύει η σχέση **gas_price * max_gas_amount <= sender_account_balance.** Χωρίς τον έλεγχο αυτό, το VM θα εκτελούσε συναλλαγές, που θα μπορούσαν να οδηγηθούν σε αποτυχία στα παρακάτω βήματα, αν δεν υπήρχε το απαραίτητο gas.
- Βεβαιώνει ότι ο αριθμός ακολουθίας συναλλαγής ταυτίζεται με τον αριθμό ακολουθίας που είναι αποθηκευμένος εντός του λογαριασμού του χρήστη. Χωρίς αυτόν τον έλεγχο, ένας κακόβουλος χρήστης θα μπορούσε να επαναλάβει τις παλιές συναλλαγές.

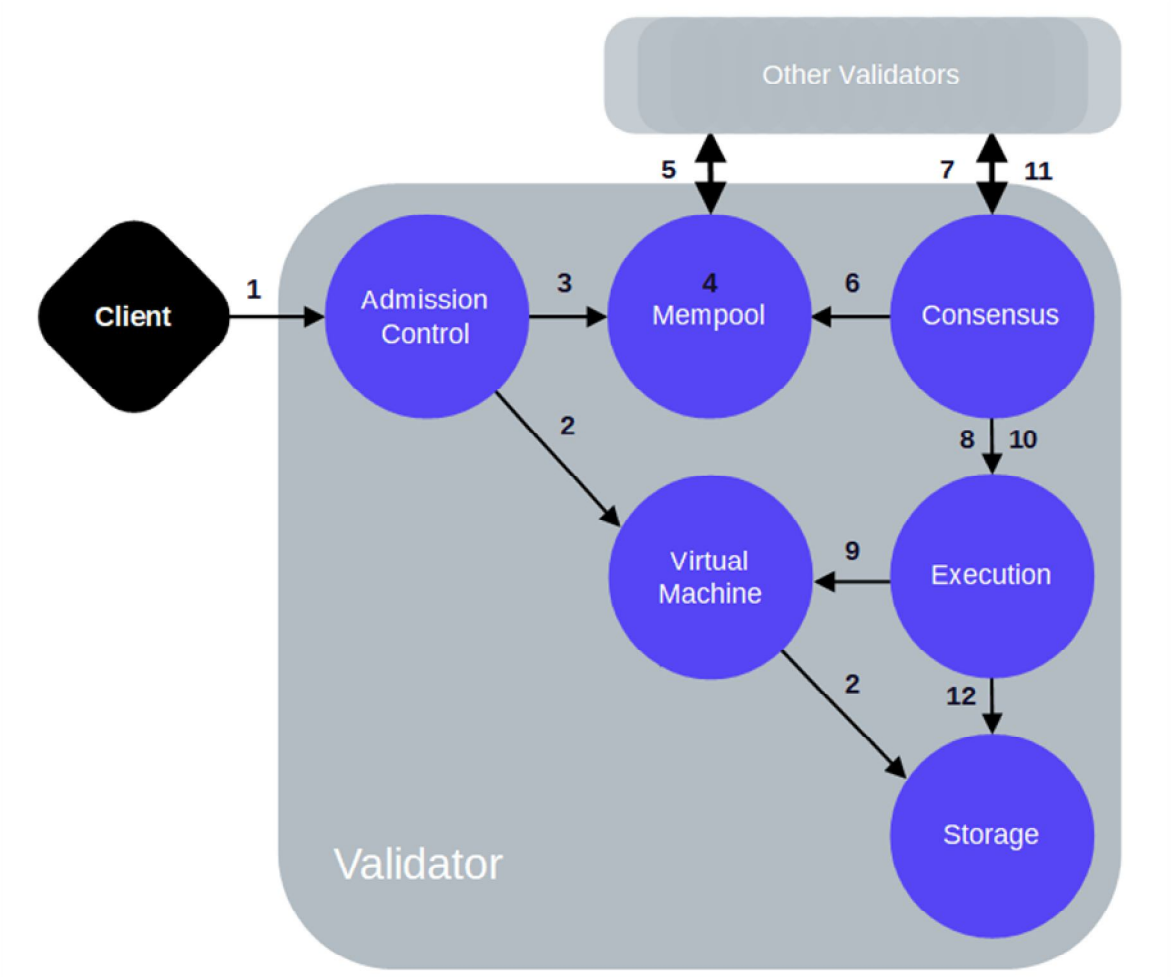
3. **Επιβεβαίωση του transaction script και των modules.** Μόλις ολοκληρωθεί με επιτυχία prologue διαδικασία της συναλλαγής, το VM εκτελεί ελέγχους καλής διαμόρφωσης/λειτουργίας στο transaction script και στα modules χρησιμοποιώντας τον Move bytecode verifier. Πριν από την εκτέλεση του script Move, ο bytecode verifier ελέγχει τις βασικές ιδιότητες για το transaction script.
4. **Δημοσίευση των modules.** Κάθε module στο πεδίο προγράμματος της συναλλαγής δημοσιεύεται από το λογαριασμό του αποστολέα. Διπλότυπα ονόματα modules δεν επιτρέπονται. Για παράδειγμα, αν η συναλλαγή επιχειρεί να δημοσιεύσει ένα module με όνομα M σε έναν λογαριασμό που περιέχει ήδη μια ενότητα με το όνομα M, το βήμα θα αποτύχει.
5. **Εκτέλεση transaction script.** Το VM συνδυάζει τα ορίσματα των συναλλαγών στις τυπικές παραμέτρους του transaction script και το εκτελεί. Εάν ολοκληρωθεί επιτυχώς, οι write λειτουργίες που εκτελούνται από το script και τα events που προκύπτουν από αυτό, εντάσσονται στο global state. Εάν η εκτέλεση του script αποτύχει (π.χ., εξαιτίας της εξάντλησης του gas ή μιας αποτυχίας εκτέλεσης), καμία από τις αλλαγές του script δεν εντάσσεται στο global state.
6. **Εκτέλεση epilogue.** Τέλος, ο VM τρέχει την epilogue διαδικασία συναλλαγής για να χρεώσει τον χρήστη για το χρησιμοποιούμενο gas και για να αυξήσει τον αριθμό ακολουθίας λογαριασμού του αποστολέα. Όπως η διαδικασία prologue, έτσι και η epilogue της συναλλαγής είναι μια διαδικασία του Move LibraAccount module. Η epilogue διαδικασία εκτελείται συνεχώς εάν η εκτέλεση ξεπεράσει το βήμα (2) και ταυτόχρονα τα βήματα (3), (4) ή (5) αποτυγχάνουν. Οι διαδικασίες prologue και epilogue δουλεύουν από κοινού για να διασφαλίσουν ότι όλες οι συναλλαγές που γίνονται δεκτές στο ledger history χρεώνονται για το gas. Συναλλαγές που δεν προχωρούν πέρα από το βήμα (2) δεν μπαίνουν στο ledger history. Το γεγονός ότι οι συναλλαγές αυτές εξετάστηκαν για εκτέλεση δεν καταγράφεται. Αν μια συναλλαγή προχωρά πέρα από το βήμα (2), η διαδικασία prologue έχει εξασφαλίσει ότι ο λογαριασμός έχει αρκετά νομίσματα Libra, ώστε να πληρώσει για το μέγιστο αριθμό μονάδων gas που επιτρέπονται για τη συναλλαγή. Ακόμη και αν η συναλλαγή εξαντλήσει το gas, η διαδικασία epilogue είναι σε θέση να το χρεώσει για αυτό το μέγιστο ποσό.

2.6.4.3 Ο κύκλος ζωής μιας transaction

Ένας χρήστης κατασκευάζει μία transaction T_5 για να μεταφέρει 10 LBR από το λογαριασμό της Ιωάννας στο λογαριασμό του Γιώργου. Η T_5 περιλαμβάνει τα πεδία που αναλύθηκαν στη δομή μιας συναλλαγής (μία account address της Ιωάννας, ένα program Move, gas price, max gas amount, το expiration της συναλλαγής και ένα sequence number πχ 5).

Ο client υπογράφει τη συναλλαγή T_5 με το private key της Ιωάννας. Η signed transaction T_5 περιλαμβάνει:

- την transaction
- το public key της Ιωάννας
- την signature *(υπογραφή)* της Ιωάννας



Σχήμα 28: Ο κύκλος ζωής μιας συναλλαγής στο Libra

Δεδομένα: Για να περιγράψουμε το κύκλο ζωής της συναλλαγής T_5, υποθέτουμε τα εξής:

1. Ο Γιώργος και η Ιωάννα διαθέτουν λογαριασμούς (accounts) στο blockchain του Libra.
2. Η Ιωάννα διαθέτει στο λογαριασμό της 110 LBR.
3. Ο τρέχων αριθμός ακολουθίας (sequence number) για το λογαριασμό της Ιωάννας είναι 5. Κάτι τέτοιο, υποδεικνύει πως ο λογαριασμός της Ιωάννας έχει λάβει ήδη 5 συναλλαγές.
4. Το δίκτυο του Libra Blockchain αποτελείται από 100 validators. (V_1 -V_{100}).
5. Ο αποστολέας υποβάλλει την συναλλαγή T_5 στο validator V_1.
6. Ο validator V_1 προτείνει για ένα leader/proposer στο τρέχον γύρο.

Βήματα

Αποδοχή της συναλλαγής

1. Ο client υποβάλλει τη συναλλαγή T_5 στον validator V_1. Το admission control (**AC**) component παραλαμβάνει τη συναλλαγή.

2. Το AC χρησιμοποιεί το Virtual Machine (**VM**) component για να πραγματοποιήσει validation ελέγχους.

3. Όταν η T_5 περάσει τους validation ελέγχους, το AC στέλνει τη συναλλαγή στο mempool του V_1.

Διαμοιρασμός της συναλλαγής με τους υπόλοιπους validators

4. Η mempool διατηρεί την T_5 σε ένα buffer. Η mempool μπορεί ήδη να περιέχει αρκετές συναλλαγές από τη διεύθυνση της Ιωάννας

5. Χρησιμοποιώντας το shared-mempool πρωτόκολλο, ο V_1 μοιράζεται τις συναλλαγές εντός του mempool του, με τους υπόλοιπους validators (V_2 έως V_{100}) και τοποθετεί τις συναλλαγές που έχει λάβει από τους υπόλοιπους validators μέσα στο δικό του mempool.

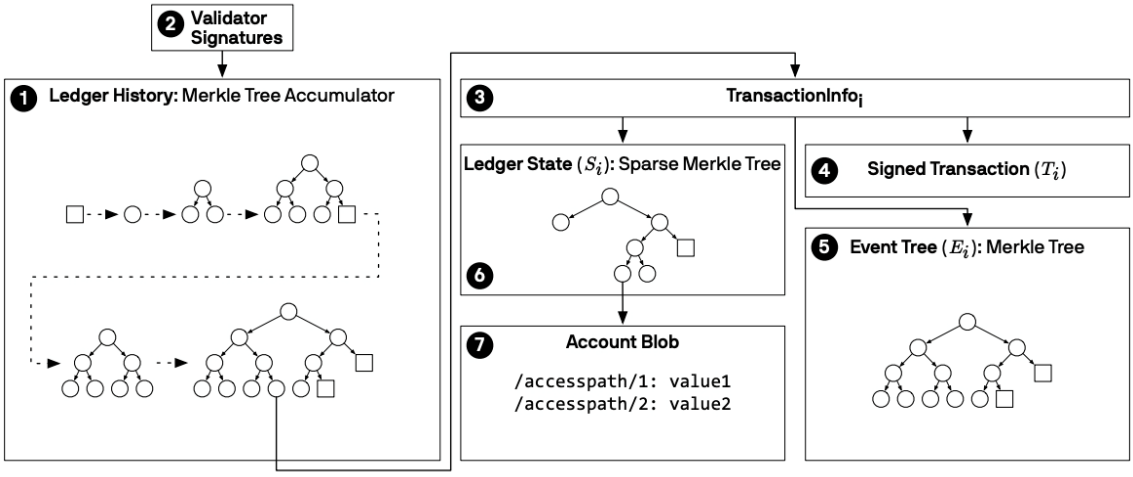
Πρόταση για το block που θα εισαχθεί η συναλλαγή

6. Ο V_1 λειτουργεί σαν proposer/leader. Τραβάει ένα μπλοκ συναλλαγών από το mempool του και δημιουργεί ένα αντίγραφό του σαν πρόταση προς τους υπόλοιπους validators μέσω του consensus component

7. Το consensus component είναι υπεύθυνο για να επέλθει συμφωνία μεταξύ όλων των validators για τη σειρά των συναλλαγών μέσα στο προτεινόμενο μπλοκ.

Εκτέλεση του block και επίτευξη consensus

8. Στα πλαίσια της διαδικασίας να επιτευχθεί συμφωνία μεταξύ των validators, το μπλοκ των συναλλαγών (συμπεριλαμβανομένης της T_5) περνάει στο execution component.



Σχήμα 29: Το Ledger History στο Libra

9. Το execution component είναι υπεύθυνο για την εκτέλεση των συναλλαγών στο VM component. Αυτό συμβαίνει πριν επιτευχθεί συμφωνία.

10. Αφού έχουν εκτελεστεί οι συναλλαγές μέσα στο μπλοκ, το execution component τις τοποθετεί (συμπεριλαμβανομένης της T_5) στον Merkle accumulator του ledger history. Αυτή η διαδικασία γίνεται στην προσωρινή μνήμη του merkle accumulator. Το αποτέλεσμα της εκτέλεσης επιστρέφεται στο consensus component.

11. Ο V_1 (ως consensus leader) επιδιώκει το αποτέλεσμα από την εκτέλεση του μπλοκ να φτάσει σε συναίνεση (*consensus*) με τους υπόλοιπους validators.

Εισαγωγή του block

12. Εάν το αποτέλεσμα της εκτέλεσης του μπλοκ έχει γίνει αποδεκτό και έχει γίνει signed από τους validators που έχουν την πλειοψηφία των ψήφων, το execution component του validator V_1 διαβάζει το αποτέλεσμα της εκτέλεσης και το τοποθετεί στο storage component.

13. Τώρα ο λογαριασμός της Ιωάννας θα έχει 100 LBR και ο sequence number θα είναι το 6. Εάν ο Γιώργος επιδιώξει να επαναλάβει την T_5 θα απορριφθεί γιατί ο sequence number του λογαριασμού της Ιωάννας είναι μεγαλύτερος από τον sequence number της συναλλαγής.

2.6.5 Το Ledger History

Στις περισσότερες εφαρμογές κρυπτονομισμάτων, όπως για παράδειγμα το Bitcoin, το blockchain παίρνει τη μορφή ενός μίας συνδεδεμένης λίστας, όπου κάθε μπλοκ συνδέεται με το αμέσως προηγούμενο του, όχι απλά, αλλά με το hash value του parent μπλοκ. Ωστόσο, το Libra δε διαθέτει αντίστοιχο blockchain, διότι χρειάζεται να αποφευχθεί η εξής ανεπάρκεια: αν ένας χρήστης θεωρεί έγκυρο ένα μπλοκ συναλλαγών Β και θέλει να επιβεβαιώσει τις πληροφορίες για ένα προηγούμενο μπλοκ Β', χρειάζεται να επεξεργαστεί όλα τα ενδιάμεσα μπλοκ.

Για αυτό το λόγο, το Libra αξιοποιεί ένα Merkle tree, έτσι ώστε να διατηρεί μία δομή δεδομένων, στην οποία θα είναι αποθηκευμένα τα στοιχεία των συναλλαγών. Με αυτό

το τρόπο, έχουμε ένα πιστοποιημένο ledger history. Στην εικόνα **ταδε,** παρουσίαζεται η δομή του Ledger history.

Στο ledger history αποθηκεύεται η ακολουθία των συναλλαγών που έχουν δεσμευθεί ή εκτελεστεί, καθώς και τα events που αναδύονται από αυτή τη διαδικασία. Το ledger history διατηρεί εγγραφές $TransactionInfo_i$, - οι οποίες με τη σειρά τους περιέχουν πληροφορίες για τα states του Libra, για τα events και για τα accounts.

Η δομή **$TransactionInfo_i$**, η οποία αντιστοιχεί στις πληροφορίες για μία transaction, αποτελείται από:

1. μία transaction T_i με υπογραφή
2. έναν authenticator για το state αφού εκτελεστεί η T_i,(το S_i του σχήματος)
3. έναν authenticator για τα events που δημιουργούνται από την T_i, (το E_i του σχήματος)

Μέσω της δομής τύπου Merkle tree, έχουμε αποτελεσματικότερη προσπέλαση δεδομένων για τη πιστοποίηση των transaction. Ένας client θέλει να αναζητήσει για την έκδοση *i* του state ή να ψάξει ένα event που δημιουργήθηκε στην έκδοση i εκτελεί μία αναζήτηση της $TransactionInfo_i$, μαζί με μία αναζήτηση που χρησιμοποιεί το state που ήδη υπάρχει ή τον authenticator της λίστας με τα events.

Το ledger history, ειδικότερα, αξιοποιεί ένα Merkle tree accumulator, το οποίο χρησιμοπιείται για προσθήκη νέων δεδομένων στο merkle tree. Όπως βλέπουμε και στο σχήμα, το Merkle tree μεγεθύνεται προοδευτικά με νέα TransactionInfo. Μέσω του hash value του root του ledger history, μας δίνεται η δυνατότητα για χρήση Merkle accumulator. Με αυτό το τρόπο, έχουμε πρόσβαση σε όλα τα δεδομένα για κάθε state του blockchain.

Παρόλο που ένας validator δεν χρειάζεται να ξέρει ολόκληρο το ledger history για να εκτελέσει νέες συναλλαγές, ένας client μπορεί να υποβάλλει authenticated ερωτήματα στο ledger history και να το χρησιμοποιήσει για να πραγματοποιήσει έλεγχο πάνω στην εκτέλεση μίας συναλλαγής.

2.6.6 Το Ledger State

Το blockchain του Libra δεν παρουσιάζει την ίδια ακριβώς δομή με το αντίστοιχο άλλων κρυπτονομισμάτων. Δε διαθέτει διατεταγμένα μπλοκ με «αλυσιδωτή» σύνδεση μεταξύ τους. Η έννοια του μπλοκ στο Libra είναι περισσότερο μία εικονική λογική δομή που χρησιμοποιείται από τους validators για να συγχρονίζουν τα επιβεβαιωμένα στιγμιότυπα του ledger state. Το blockchain του Libra μοιάζει πιο πολύ με τη δομή που ακολουθούν το Ethereum και το Ripple. Όλα τα δεδομένα στο blockchain του Libra αποθηκεύονται σε μία **single-versioned** βάση δεδομένων. Ένας version αριθμός είναι ένας unsigned 64-bit ακέραιος που αντιστοιχεί στον αριθμό των transactions που έχει εκτελέσει το σύστημα. Η versioned βάση δεδομένων επιτρέπει στους validators:

- να εκτελούν μία transaction έναντι της τελευταίας version του ledger state

- να απαντούν στα ερωτήματα των clients για το τρέχον ledger history αλλά και το ledger history προηγούμενων version.

Το ledger state ή global state του Libra Blockchain αποτελείται από ένα στιγμιότυπο όλων των transactions που έχουν εγγραφεί στο δίκτυο, και συμπεριλαμβάνει επίσης και την ποσότητα Libra που κατέχει κάθε χρήστης. Το πρωτόκολλο Libra χρησιμοποιεί ένα μοντέλο δεδομένων βασισμένο σε accounts για να κωδικοποιήσει το ledger state. Το state είναι μία key-value δομή αποθήκευσης, που αντιστοιχίζει account address keys σε account values. Μία account value στο ledger state είναι μία συλλογή από Move resources και modules. Οι Move resources αποθηκεύουν data values και τα Move modules αποθηκεύουν κώδικα.

2.6.6.1 Genesis Ledger State

Με έναν τρόπο που μοιάζει πολύ με το πως το Bitcoin δίκτυο παράγει το genesis block, έτσι και στο Libra το αρχικό σετ των accounts και των αντιστοιχισμένων values τους καθορίζει το **genesis ledger state**.

2.6.6.2 Η λογική λειτουργία του Ledger State

Όπως αναφέρθηκε πιο πάνω όλα τα δεδομένα στο blockchain του Libra αποθηκεύονται σε μία **single-versioned** βάση δεδομένων και ένας version αριθμός αντιστοιχεί στον αριθμό των transactions που έχει εκτελέσει το σύστημα.

Σε κάθε version ***i*** η versioned database περιλαμβάνει ένα σύνολο (T_i, O_i, S_i), όπου:

- T_i: *η transaction i*
- O_i: *το output της transaction i*
- S_i: *το ledger state*

Χρησιμοποιώντας μια ντετερμινιστική συνάρτηση Apply ισχύουν τα εξής για το παραπάνω σύνολο: εκτελώντας την transaction Ti έναντι του ledger state S_{i-1} παράγεται ένα output O_i και ένα καινούριο ledger state S_i . Αυτό γράφεται ως εξής:

$$\mathbf{Apply}(S_{i-1}, T_i) \rightarrow \langle O_i , Si\rangle$$

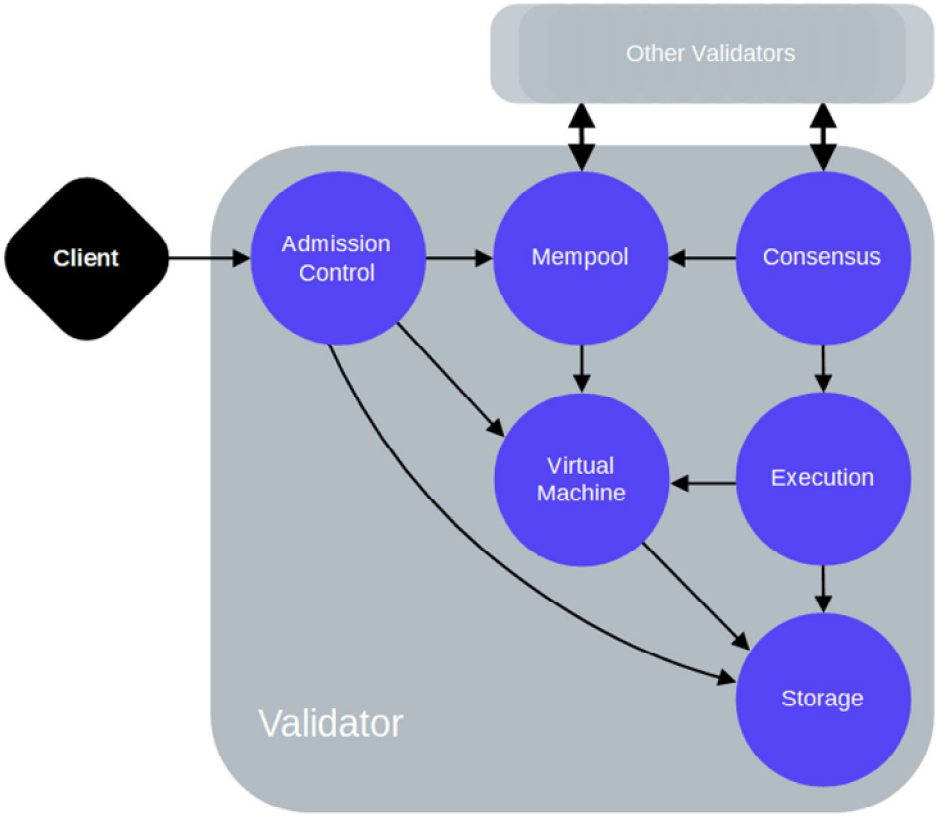
Το Libra χρησιμοποιεί την γλώσσα Move για να υλοποιήσει τη ντετερμινιστική συνάρτηση Apply.

2.6.7 Το συναινετικό πρωτοκόλλο Consensus LibraBFT

Γενικά, το consensus πρωτόκολλο που χρησιμοποιεί το Libra επιτρέπει σε ένα σύνολο από validators να δημιουργούν μία στιγμιότυπο ενός database. Το πρωτόκολλο δημιουργεί μία σειρά από αντίγραφα των συναλλαγών που έχουν υποβληθεί. Τα αντίγραφα αυτά μοιράζονται ανάμεσα στους validators, οι οποίοι εκτελούν τις συναλλαγές. Στη συνέχεια, συφωνούν στη διάταξη των συναλλαγών, καθώς και στο αποτέλεσμα της εκτέλεσης. Ως αποτέλεσμα, οι validators διατηρούν πανομοιότυπα στιγμιότυπα για το database με τις συναλλαγές για ένα δοσμένο version number.

Το πρωτόκολλο που χρησιμοποιείται ονομάζεται LibraBFT. Το πρωτόκολλο αυτό έχει σχεδιαστεί με τέτοιο τρόπο, ώστε να είναι Byzantine Fault Tolerant. Το consensus ανάμεσα στους χρήστες για το state του database, πρέπει να εξασφαλίζεται ακόμα και με ύπαρξη Byzantine faults.

Για το σκοπό αυτό, το LibraBFT υποθέτει πως το δίκτυο αποτελείται από μία ομάδα από κόμβους. Στην ομάδα αυτή, δίνεται η δυνατότητα για 3f + 1 ψήφους. Το πρωτόκολλο λειτουργεί ασφαλώς, εμποδίζοντας double spend και forks, όταν το πολύ f ψήφοι ελέγχονται από κανονικούς και έμπιστους χρήστες. Το πρωτόκολλο, επίσης, παραμένει ενεργό όσο υπάρχει ένα χρονικό διάστημα (που ονομάζεται global stabilization time-GST), μετά από το οποίο όλα τα μηνύματα ανάμεσα σε έμπιστους κόμβους δρομολογούνται σε όλους τους υπόλοιπους κόμβους, με μέγιστη καθυστέρηση ενός μεγέθους δ.



Σχήμα 30: Το LibraBFT

Οι validators λαμβάνουν transactions από τους χρήστες και τις μοιράζονται μεταξύ τους μέσω ενός διαμοιραζόμενου mempool πρωτοκόλλου. Το LibraBFT πρωτόκολλο επεξαργάζεται τις συναλλαγές σε μία σειρά από γύρους (rounds). Ο validator node εκτελεί ένα πρωτόκολλο συναίνεσης (μαζί με άλλους κόμβους επικύρωσης), εκτελεί τις συναλλαγές και τις αποθηκεύει μαζί με τα αποτελέσματα της εκτέλεσης τους στο blockchain. Ένας validator έχει την ακόλουθη δομή:

1. **Admission (AC)**
2. **Mempool**

3. **Consensus**
4. **Execution**
5. **Virtual Machine (VM)**
6. **Storage**

Το LibraBFT πρωτόκολλο λειτουργεί προοδευτικά σε γύρους, όπου σε κάθε γύρο επιλέγεται ένας leader μεταξύ των validators. Οι leaders είναι υπεύθυνοι για:

- την υποβολή προτάσεων για νέα μπλοκ συναλλαγών προκειμένου να επεκταθεί μιά συγκεκριμένη αλυσίδα από blocks που περιέχει όλο το ιστορικό των συναλλαγών και
- τη λήψη ψήφων με υπογραφή από τους validators σχετικά με τις προτάσεις τους.

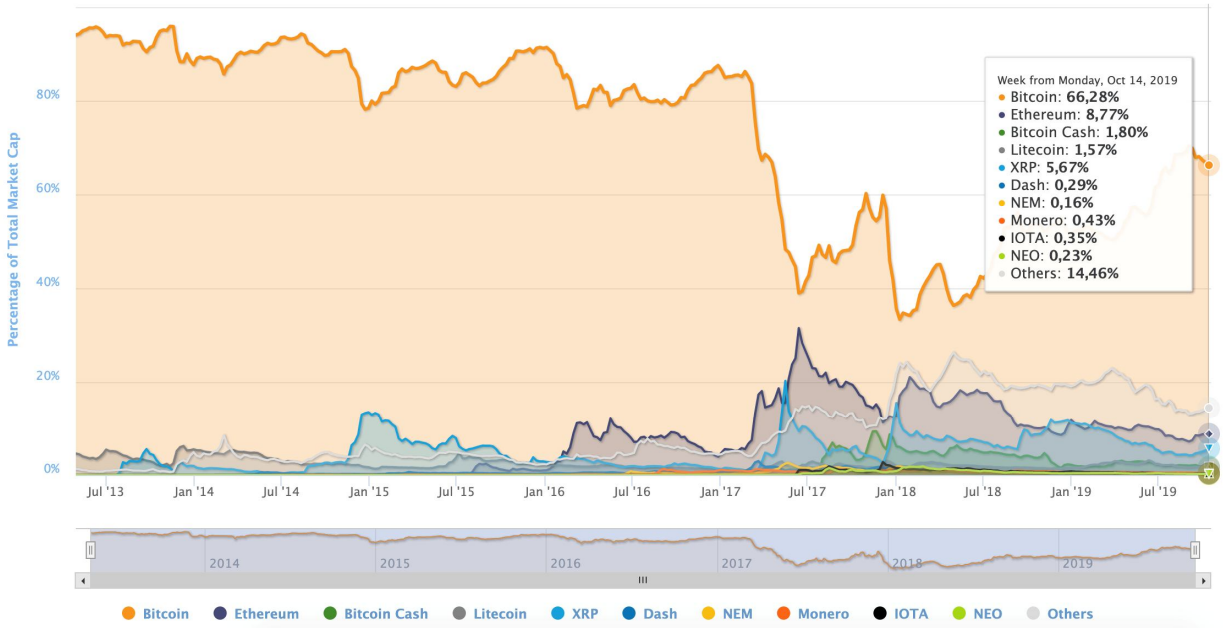
Το LibraBFT ακολουθεί και υλοποιεί τα εξής βήματα:

1. Ένας γύρος είναι μια φάση επικοινωνίας με έναν μόνο καθορισμένο leader, και οι προτάσεις του leader οργανώνονται σε μια αλυσίδα χρησιμοποιώντας κρυπτογραφικά hashes.
2. Κατά τη διάρκεια ενός γύρου, ο leader προτείνει ένα μπλοκ που επεκτείνει τη μεγαλύτερη αλυσίδα που γνωρίζει.
3. Εάν η πρόταση είναι έγκυρη και έγκαιρη, κάθε honest κόμβος θα την υπογράψει και θα στείλει μια ψήφο στο leader validator.
4. Αφού ο leader λάβει αρκετές ψήφους για να φτάσει σε συμφωνία, συγκεντρώνει τις ψήφους στο Quorum Certificate (QC) που επεκτείνει ξανά την ίδια αλυσίδα. Για να γίνει αυτό πρέπει το QC να παρέχει αποδείξεις *>=2f+1* των ψήφων γι' αυτό το μπλοκ.
5. Το QC μεταδίδεται σε κάθε κόμβο.
6. Αν ο leader δεν συγκεντρώσει ένα QC, ενεργοποιείται ένας μηχανισμός time-out για να ξεκινήσει ένας νέος γύρος και επιλέγεται ένας καινούριος leader από τους validators.
7. Όταν ένα μπλοκ θα συναντήσει έναν 3-chain commit κανόνα του πρωτοκόλλου LibraBFT, το μπλοκ εισάγεται. Ένα μπλοκ στο γύρο k εισάγεται εάν έχει ένα QC και έχει επιβεβαιωθεί από 2 επιπλέον μπλοκς και Qcs στους γύρους k+1 και k+2. Ο commit κανόνας επιτρέπει στους honest validators να εισαγάγουν ένα μπλοκ. Το LibraBFT εγγυάται ότι όλοι οι honest validators θα εισαγάγουν το μπλοκ και την αλυσίδα που δημιουργείται από αυτό το μπλοκ και κάθε προηγούμενό του. Όταν εισάγεται μια ακολουθία από blocks, το state που προκύπτει από την εκτέλεση των συναλλαγών τους μπορεί να δημιουργήσει μία replicated βάση δεδομένων.

3. ΣΥΜΠΕΡΑΣΜΑΤΑ

Με βάση τη μελέτη των βασικών χαρακτηριστικών των παράπανω κρυπτονομισμάτων, έχουμε τη δυνατότητα να εξάγουμε ορισμένα ασφαλή συμπεράσματα, με βάση ορισμένα κριτήρια. Η μη κυκλοφορία του Libra (LBR) δε μας προσφέρει τη δυνατότητα να εκτιμήσουμε σωστά την αποδοχή του από το κοινό και την χρησιμότητα που προσφέρουν τα ξεχωριστά χαρακτηριστικά του.

3.1 Market Capitalization



Σχήμα 31: Συμμετοχή κάθε κρυπτονομίσματος στο συνολικό Market Capitalization

Το Bitcoin (BTC) σταθερά βρίσκεται στη 1η θέση και χωρίς κανέναν ανταγωνισμό, καθώς καταλαμβάνει το 66,28 % του συνολικού Market Cap. Ακολουθούν το Ethereum (ETH), το XRP και το DASH με 8,77%, 5,67% και 0,29% αντίστοιχα. Το Namecoin (NMC) καταλαμβάνει ένα αρκετά χαμηλό ποσοστό της τάξης του 0,000031%. Το Libra (LBR) δεν εντάσσεται στη σύγκριση αυτή, καθώς δε βρίσκεται ακόμα σε κυκλοφορία.

Πίνακας 14: Ποσοστα συμμετοχής του Market Capitalization κάθε κρυπτονομίσματος στο συνολικό Market Capitalization

Κρυπτονόμισμα	Ποσοστό στο συνολικό Market Cap
BTC (Bitcoin)	66,28 %
ETH (Ethereum)	8,77 %
XRP (Ripple)	5,67 %
DASH (Dash)	0,29 %
LBR (Libra)	-

NMC (Namecoin)	0,000031%

3.2 Δυνατότητα υποστήριξης smart contracts

Η πλατφόρμα του Ethereum αποτελεί ξεκάθαρα το πρωτόπορο στην υποστήριξη smart contracts, μέσω της γλώσσας προγραμματισμού Solidity. Το Bitcoin, αρχικά, δεν υποστήριζε smart contracts, αλλά μέσω αναβαθμίσεων εξοπλίστηκε με τη γλώσσα Script για αυτό το λόγο. Ωστόσο, τα αποτελέσματα είναι αποθαρρυντικά, καθώς η χρησιμότητά τους είναι περιορισμένη, λόγω δύσχρηστης λειτουργικότητάς τους. Στα ίδια επίπεδα κινείται και το XRP με περιορισμένη υποστήριξη smart contracts. Το Namecoin (NMC), όπως και το Dash (DASH) δε παρέχουν αντίστοιχη υποστήριξη. Τέλος, το Libra προσφέρει τη δυνατότητα υλοποίησης smart contracts, με τη μορφή Move modules, μέσω της γλώσσας Move.

Πίνακας 15: Δυνατότητα υλοποίησης smart contracts

Κρυπτονόμισμα	Υλοποίηση smart contracts
BTC (Bitcoin)	ναι -- Περιορισμένη χρήση
ETH (Ethereum)	ναι -- Ευρεία χρήση
XRP (Ripple)	ναι – Περιορισμένη χρήση
DASH (Dash)	όχι
LBR (Libra)	ναι
NMC (Namecoin)	όχι

3.3 Συναλλαγές (transactions)

Μπορούμε να διακρίνουμε τις εξής διαφορετικές περιπτώσεις:

1. Όσον αφορά **το transactions per second (TPS)** έχουμε:

Το μέγεθος TPS εκφράζει θεωρητικά το μέγιστο αριθμό των συναλλαγών (transactions) ανά δευτερόλεπτο (sec) και υπολογίζεται προσεγγιστικά. Το XRP διαθέτει την υψηλότερη διεκπεραιωτική ικανότητα (transaction throughput) σε σχέση με τα υπόλοιπα κρυπτονομίσματα τα οποία μελετάμε, στις 1500 transactions/sec. Ακολουθεί το Libra με 1000 transactions/sec. Ύστερα, για τα υπόλοιπα, η διεκπεραιωτική ικανότητα πέφτει κατακόρυφα με 28, 15 , 7 και 7 transactions/sec για το DASH, το Ethereum, το Bitcoin και το Namecoin αντίστοιχα.

Πίνακας 16: Μέγιστος αριθμός συναλλαγών ανα δευτερόλεπτο

Κρυπτονόμισμα	TPS
BTC (Bitcoin)	7
ETH (Ethereum)	15
XRP (Ripple)	1500
DASH (Dash)	28

LBR (Libra)	1000
NMC (Namecoin)	7

2. Όσον αφορά το **reward** έχουμε:

Το Bitcoin και το Namecoin διαθέτουν το υψηλότερο reward (12.5 BTC) σε σχέση με τα υπόλοιπα. Ακολουθεί το Dash με 3.11 DASH και το Ethereum με 2 Ether. Για το Libra και το Ripple δεν είναι σταθερό για κάθε συναλλαγή.

Πίνακας 17: Πολιτική reward για κάθε νόμισμα

Κρυπτονόμισμα	Τρέχον reward	Αρχικό reward	Ρυθμός μείωσης
BTC (Bitcoin)	12,5 BTC (100.467 $)	50 BTC (401.600 $)	κάθε 2016 μπλοκ ~ 4 χρόνια
ETH (Ethereum)	2 Ether (347,07 $)	5 Ether (867,37 $)	ορίζεται από τις ενημερώσεις της πλατφόρμας
XRP (Ripple)	ορίζεται σε κάθε συναλλαγή	ορίζεται σε κάθε συναλλαγή	-
DASH (Dash)	3,11 DASH (211,01 $)	5 DASH (339,19 $)	7.14 % για κάθε 210240 μπλοκ ~ 383.25 ημέρες
LBR (Libra)	ορίζεται σε κάθε συναλλαγή	ορίζεται σε κάθε συναλλαγή	-
NMC (Namecoin)	12,5 NMC (5,64 $)	50 NMC (22,57 $)	κάθε 2016 μπλοκ ~4 χρόνια

3. Όσον αφορά το **blockchain** έχουμε:

Το Ethereum διαθέτει το μεγαλύτερο σε μέγεθος και πλήθος μπλοκ blockchain, με 436.85 GB και 8.772.8087 μπλοκ αντίστοιχα. Ακολουθεί το Bitcoin, το Dash και το Namecoin. Το XRP και το Libra δεν εντάσσονται στη συγκεκριμένη σύγκριση, καθώς δε διαθέτουν κάποια μορφή blockchain στην πλατφόρμα τους.

Πίνακας 18: Μέγεθος blockchain κάθε νομίσματος

Κρυπτονόμισμα	Πλήθος μπλοκ	Μέγεθος σε GB
BTC (Bitcoin)	600.092	285.99
ETH (Ethereum)	8.772.087	436.85
XRP (Ripple)	-	-
DASH (Dash)	1.156.173	16.73

LBR (Libra)	-	-
NMC (Namecoin)	475.934	6.04

3.4 Μηχανισμοί consensus

Συγκρίνοντας τους μηχανισμούς consensus που χρησιμοποιεί κάθε κρυπτονόμισμα, διακρίνουμε τα εξής κριτήρια σύγκρισης:

1. Όσον αφορά **το ρυθμό παραγωγής μπλοκ (block production rate),** έχουμε τα εξής:

Το Ethereum βρίσκεται στην πρώτη θέση με 264 μπλοκ ανά ώρα. Ακολουθεί το Dash με 23 μπλοκ/ώρα, το Namecoin με 7 μπλοκ/ώρα και το Bitcoin με 6 μπλοκ/ώρα. Το Libra και το XRP δε διαθέτουν μπλοκ στη δομή τους και δεν τίθονται προς σύγκριση.

Πίνακας 19: Ρυθμός παραγωγής μπλοκ στο blockchain

Κρυπτονόμισμα	Μπλοκ ανά ώρα
BTC (Bitcoin)	6
ETH (Ethereum)	264
XRP (Ripple)	-
DASH (Dash)	23
LBR (Libra)	-
NMC (Namecoin)	7

2. Όσον αφορά τις **hash συναρτήσεις** που χρησιμοποιούν και τους mining αλγορίθμους, έχουμε τα εξής:

Πίνακας 20: Hash συναρτήσεις και mining αλγόριθμοι που χρησιμοποιούνται από τα επιμέρους κρυπτονομίσματα

Κρυπτονόμισμα	Hash συναρτήσεις	Τύπος mining αλγορίθμου
BTC (Bitcoin)	SHA 256	Proof of Work
ETH (Ethereum)	Keccak 256	Proof of Work μετάβαση σε Proof of Stake
XRP (Ripple)	SHA 256	Ripple Consensus Protocol
DASH (Dash)	X11	Proof of work
LBR (Libra)	SHA3 256	LibraBFT Consensus Protocol
NMC (Namecoin)	SHA 256	Proof of Work

3. Όσον αφορά την **κατανάλωση ενέργειας**, συγκρίνουμε μόνο τα 3 μεγαλύτερα από άποψη Market Capitalization, δηλαδή το Bitcoin, το Ethereum και το Ripple. Νομίσματα όπως το Dash και το Namecoin, έχουν μικρότερη αποδοχή από το κοινό, γεγονός που μας οδηγεί στο συμπέρασμα ότι το ποσοστό της ενέργειας που καταναλώνουν είναι αμελητέα. Για το Libra δεν υπάρχουν ακόμη στοιχεία, γιατί αναμένεται να κυκοφορήσει στην αγορά των κρυπτονομισμάτων εντός του 2020.

Πίνακας 21: Κατανάλωση ενέργειας

Κρυπτονόμισμα	Κατανάλωση ενέργειας
BTC (Bitcoin)	Δαπανηρό
ETH (Ethereum)	Δαπανηρό
XRP (Ripple)	Περιορισμένη κατανάλωση ενέργειας

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

51% attack (51% επίθεση)	Βασική απειλή για το δίκτυο ενός κρυπτονομίσματος. Αντιστοιχεί στο εξής σενάριο: αν ένας χρήστης ή μία ομάδα χρηστών συσσωρεύσει πάνω από το 50% της υπολογιστικής ισχύος του δικτύου, έχει τη δυνατότητα να αποκτήσει πλήρη έλεγχο στο blockchain. Κάτι τέτοιο, θα έδινε τη δυνατότητα σε αυτούς τους χρήστες να αλλάξουν δεδομένα, προσθέσουν συναλλαγές, να ξοδέψουν χρήματα που δεν ανήκουν σε αυτούς. Όλα τα κρυπτονομίσματα διαθέτουν δομικά στοιχεία και μηχανισμούς, ώστε να την αποτρέπουν.
alt-coins	Γενικότερη ομαδοποίηση όλων των κρυπτονομισμάτων, τα οποία αναπτύχθηκαν με την εμφάνιση του Bitcoin. Αποτελούν εναλλακτικές (alternative) στο τρόπο με τον οποίο λειτουργεί το Bitcoin
Byzantine Generals' Problem	Σενάριο, όπου μία ομάδα κόμβων χρειάζεται να επικοινωνήσουν και να συμφωνήσουν στη στρατηγική που θα ακολουθήσουν. Ωστόσο, ενδέχεται να υπάρχουν κόμβοι οι οποίοι αντιστοιχούν σε κακόβουλους χρήστες ή οι πληροφορίες που ανταλλάσονται μπορεί και να αλλοιωθούν, οδηγώντας σε αποτυχία (Byzantine fault ή failure). Το σενάριο αυτό υπάρχει στα κατανεμημένα δίκτυα κόμβων και επιλύθηκε από τον Satoshi Nakamoto, μέσω του PoW. Αποτελεί μία αλληγορία του εξής προβλήματος: μία ομάδα από στρατηγούς, καθένας από τους οποίους ελέγχει και ένα τμήμα του στρατού, πρέπει να συνεργαστούν για μια επιτυχημένη επίθεση μέσω μηνυμάτων. Επειδή οι στρατηγοί βρίσκονται σε εχθρικό περιβάλλον, τα μηνύματα μπορεί να μη φτάσουν ποτέ στον προορισμό τους (όπως οι κόμβοι ενός κατανεμημένου δικτύου μπορεί να αποτύχουν ή να στείλουν αλλοιωμένα μηνύματα). Μία επιπλέον πτυχή έχει να κάνει με το γεγονός πως κάποιος στρατηγός είναι προδότης και προσπαθεί να υπονομεύσει την επιτυχία του σχεδίου (όπως και οι κακόβουλοι χρήστες σ'ένα κατ/μο δίκτυο).

Byzantine Fault Tolerance (BFT)	Σύστημα, το οποίο μέσω διαφόρων μηχανισμών, προστατεύεται από Byzantine Failures.
Block (μπλοκ)	Δομικό στοιχείο κάθε blockchain. Περιλαμβάνει συγκεκριμένα δεδομένα (διάφερουν ανάλογα με το κρυπτονόμισμα), τα οποία θεωρούνται αμετάκλητα μετά την εισαγωγή του μπλοκ στη blockchain.
centralized	Δομή, όπου ένας μικρός αριθμός από κόμβους έχουν απόλυτο έλεγχο και ισχύ επάνω σε όλο το δίκτυο συνολικά.
Circulating supply	Ο συνολικός αριθμός νομισμάτων που μπορούν άμεσα να χρησιμοποιοηθούν σε συναλλαγές δημόσια. Ορισμένα νομίσματα, είτε δεν είναι διαθέσιμα άμεσα, λόγω δέσμευσης ή κλειδώματος, είτε έχουν καταστραφεί από διάφορους παράγοντες. Τα νομίσματα αυτά δε λαμβάνονται υπ'όψιν στον υπολογισμό του circulating supply.
Block height	Το ύψος του blockchain, το οποίο αντιστοιχεί στο πλήθος των block που αυτό περιέχει. Για παράδειγμα, αν το Block Height είναι #100, σημαίνει πως η blockchain περιλαμβάνει μόνο 100 block
Decentralized (αποκεντρωμένο)	Δομή, όπου όλοι οι κόμβοι ή χρήστες λειτουργούν συντονισμένα και με κατανεμημένο τρόπο, ώστε να πετύχουν ένα συνολικό σκοπό.
Digital signature (ψηφιακή υπογραφή)	Μαθηματικό σχήμα, σκοπός του οποίου είναι η πιστοποίηση της αυθεντικότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μία έγκυρη ψηφιακή υπογραφή, όταν ικανοποιούνται όλες οι απαιτήσεις, προσφέρει ένα αδιάσειστο επιχείρημα στον παραλήπτη πως όντως ο αποστολέας είναι έγκυρος και όχι κάποιος (αυθεντικοποίηση) και ότι το μήνυμα δεν έχει αλλοιωθεί κατά τη μεταφορά (ακεραιότητα).
Double spend	Βασικό πρόβλημα που αντιμετώπισαν τα πρώτα κρυπτονομίσματα. Αντιστοιχεί στο σενάριο όπου ένας χρήστης επιχειρεί να ξοδέψει το ίδιο ποσό δύο φορές. Ενώ κάτι τέτοιο, στη κανονική ζωή εμποδίζεται

	εύκολα, στο ψηφιακά νομίσματα η απειλή είναι κάτι παραπάνω από πιθανή, καθώς κάθε χρήστης μπορεί να δημιουργήσει νομίσματα από το μηδεν και να αξιοποιήσει κατ'αυτό το τρόπο. Η 51% attack επιτρέπει στους χρήστες, αν είναι επιτυχημένη, να ξοδέψουν το ίδιο ποσό παραπάνω από μία φορά. Τα κρυπτονομίσματα διαθέτουν μηχανισμούς για την ικανοποιητική προστασία τους από το πρόβλημα αυτό.

DoS επίθεση	Cyber επίθεση, όπου ο επιτιθέμενος επιδιώκει να καταστήσει τους πόρους ενός μηχανήματος ή ενός δικτύου μη διαθέσιμους για τους χρήστες. Επιτυγχάνει κάτι τέτοιο μέσω μαζικής αποστολής request αιτημάτων στο μηχάνημα-στόχο, έτσι ώστε να υπάρξει υπερφόρτωση. Το γεγονός αυτό οδηγεί σε προσωρινή ή μόνιμη διακοπή των υπηρεσιών στη πλευρά του στόχου.
Gas	Όρος, ο οποίος αντιστοιχεί στην πλατφόρμα του Ethereum και αναφέρεται στη μονάδα μέτρησης της υπολογιστικής προσπάθειας που καταναλώνεται για την εκτέλεση συναλλαγών ή smart contracts ή dApps στο δίκτυο του.
Genesis block	Το πρώτο μπλοκ, από το οποίο ξεκινά το blockchain.
Hash rate	Μονάδα μέτρησης της ποσότητας υπολογιστικής ισχύος που καταναλώνεται σε ένα δίκτυο συνεχώς. Εκφράζει ρυθμό κατανάλωσης υπολογιστικής ισχύος και μετριέται σε kH/s, MH/s, GH/s, TH/s και άλλα.
Ledger	Λίστα, όπου καταγράφονται οι συναλλαγές, οι οποίες είναι αμετάκλητες. Ενημερώνεται μόνο με νέες συναλλαγές.
Market capitalization	Το γινόμενο ανάμεσα στο συνολικό αριθμό νομισμάτων σε κυκλοφορία επί την ονομαστική τους αξία.
Max supply	Η καλύτερη δυνατή προσέγγιση του μέγιστου αριθμού των νομισμάτων που έχουν υπάρξει στο χρονικό διάστημα που υπάρχει ένα κρυπτονόμισμα.
Memory hard function	Συνάρτηση, η οποία απαιτεί μεγάλη ποσότητα μνήμης για την αποθήκευση και την ανάκτηση δεδομένων.
Open source	Είδος λογισμικού με άδεια, στην οποία ο κάτοχος των πνευματικών δικαιωμάτων παρέχει στους χρήστες τα δικαιώματα να μελετούν, να αλλάζουν και να διανέμουν το λογισμικό σε οποιονδήποτε και για οποιονδήποτε σκοπό. Αντιστοιχεί επίσης σε μία λογική, όπου οι χρήστες συμβάλλουν στην ελεύθερη και ανοιχτή

	ανταλλαγή πληροφοριών και δεδομένων για την επιδίωξη του «ευρύτερου καλού».

Orphan block	Έγκυρο μπλοκ μίας blockchain, το οποίο δεν είναι μέρος της κύριας αλυσίδας. Ενδέχεται να προκύψει όταν δύο miners παράγουν μπλοκ σχεδόν ταυτόχρονα ή όταν ένας επιτιθέμενος προσπαθεί να αντιστρέψει συναλλαγές. Είναι γνωστό και ως “detached block”.
Parent block	Το αμέσως προηγούμενο μπλοκ του τρέχοντος. Η σύνδεση δεν είναι απλή, αλλά περιέχει το hash value του προηγούμενου μπλοκ.
Pre-sale	Χρονική περίοδος στην οποία γίνονται αρχικές προσφορές για ένα νόμισμα από ιδιώτες επενδυτές ή μέλη της κοινότητας, προτού αυτό βγει στην αγορά. Βασικός σκοπός είναι η εξασφάλιση πόρων για τα πρώτα βήματα της πλατφόρμας του νομίσματος
Pre-mine	Όταν μερικά ή όλα τα νομίσματα του αρχικού αποθέματος, δημιουργούνται κατά τη διάρκεια ή πριν ακόμα την εκκίνηση ενός νομίσματος. Αυτό διαφέρει από τη δημιουργία νομισμάτων μέσω του mining.
Scripting (scripting language)	Γλώσσα προγραμματισμού, η οποία υποστηρίζει την εκτέλεση scripts ή προγραμμάτων, τα οποία είναι σχεδιασμένα για run-time περιβάλλοντα. Εκτελούν εργασίες αυτόνομα και έτσι μειώνεται η ανθρώπινη διαμεσολάβηση. Αξιοποιούνται ευρέως στη συγγραφή smart contracts.
Selfish mining	Σενάριο, στο οποίο ένας miner δημιουργεί ένα νέο μπλοκ στη blockchain και δεν ενημερώνει για αυτή την αλλαγή το ίδιο το δίκτυο.
SHA-256	Κρυπτογραφική hash συνάρτηση, της οικογένειας SHA (Secure Hash Algorithm), η οποία χρησιμοποιείται στο Bitcoin και σε άλλα κρυπτονομίσματα. Παράγει μία σταθερού μεγέθους (256 bits) έξοδο από αυθαίρετου μεγέθους εισόδους. Σχεδιάστηκε από τη NSA.
Stale block	Μπλοκ, το οποίο έχει εξορυχθεί επιτυχώς, αλλά δεν ενσωματώθηκε στη μεγαλύτερη τρέχουσα blockchain, συνήθως διότι ένα άλλο μπλοκ με το ίδιο block height

	ενσωματώθηκε στην αλυσίδα πρώτα.
State machine	Μαθηματικό μοντέλο, όπου δέχεται ως είσοδο μία σειρά από δεδομένα τα επεξεργάζεται και με βάση την επεξεργασία αυτή μεταβαίνει σε μία νέα κατάσταση.
Test net	Όταν ο δημιουργός ενός κρυπτονομίσματος θέλει να ελέγχει μία νέα έκδοση για το blockchain, πραγματοποιεί τον έλεγχο αυτό μέσα σε ένα test net. Αυτό λειτουργεί σαν μία δεύτερη εκδοχή του blockchain, η οποία βέβαια δεν επηρεάζει την ενεργή blockchain.
Timestamp	Παράγοντας, ο οποίος αξιοποιείται για την εξακρίβωση του χρόνου, στο οποίο πραγματοποιήθηκε ένα συμβάν. Στις περισσότερες περιπτώσεις αξιοποιείται το Unix timestamp, το οποίο εκφράζει τον αριθμό των δευτερολέπτων που έχουν περάσει από τη 1/01/1970.
Total supply	Το συνολικό πλήθος από νομίσματα, τα οποία υπάρχουν τώρα, χωρίς τα νομίσματα που έχουν καταστραφεί αποδεδειγμένα.
Cryptocurrency wallet	Ψηφιακό πορτοφόλι, το οποίο χρησιμοποιείται για την αποθήκευση, αποστολή και παραλαβή ψηφιακών νομισμάτων. Διακρίνονται σε δύο κατηγορίες: hosted και cold wallets.
Επίθεση Sybil (sybil attack)	Επίθεση όπου ένα κακόβουλος χρήστης έχει τη δυνατότητα να χρησιμοποιήσει πολλαπλές ταυτότητες. Στο συγκεκριμένο σενάριο, ο επιτιθέμενος έχει τη δυνατότητα να εισάγει πλαστούς χρήστες στο δίκτυο υπό τον έλεγχο του. Αξιοποιεί ένα αριθμό από πλαστούς χρήστες, τόσο μεγάλο ώστε να έχει τη δυνατότητα να ελέγξει όλο το δίκτυο σε βάρος των γνήσιων χρηστών.

ΑΝΑΦΟΡΕΣ

[1] Wai Yan Maung Maung Thin, Naipeng Dong, Guangdong Bai, and Jin Song Dong, *Formal Analysis of a PoS Blockchain,* 2018.

[2] Rajeev Sobti, G. Geetha, *Cryptographic Hash Functions: A Review,* 2012

[3] Arati Balinga, *Understanding Blockchain Consensus Models*, 2017

[4] Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks, *A Brief Survey of Cryptocurrency Systems.*

[5] anonymous*, Market capitalization of cryptocurrencies, https://coinmarketcap.com/, 2019*

[6] anonymous*, Block, https://en.bitcoin.it/wiki/Block, 2019*

[7] anonymous*, Double spending, https://en.bitcoin.it/wiki/Double-spending, 2019*

[8] Lotte Fekkes, *Comparing Bitcoin and Ethereum*, 2018

[9] Florian Tschorsch and Björn Scheuermann, *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,2016*

[10] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008

[11] Krzysztof Okupski, *Bitcoin developer Reference. Available at* https://enetium.com/resources/Bitcoin.pdf, 2014.

[12] Vitalik Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2013

[13] anonymous, Ethash, https://github.com/ethereum/wiki/Ethash, 2014.

[14] URL: https://kauri.io/collection/5bb65f0f4f34080001731dc2/ethereum-101

[15] URL: https://ethereum.stackexchange.com/questions/1993/what-actually-is-a-dag

[16] URL: https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial#introduction

[17] URL: https://docs.ethhub.io/

[18] URL: https://github.com/ethereum/wiki/wiki/Mining

[19] URL: https://arvanaghi.com/blog/explaining-the-genesis-block-in-ethereum/

[20] Gavin Wood, *Ethereum: A secure decentralized generalized transaction ledger.*

[21] Brad Chase, Ethan MacBrough, "Analysis of the XRP Ledger Consensus Protocol", 2018.

[22] URL: https://xrpl.org/concepts.html

[23] URL: https://www.vijaypradeep.com/blog/2017-04-28-ethereums-memory-hardness-explained/

[24] David Schwartz, Noah Youngs, and Arthur Britto, "The Ripple protocol consensus algorithm", Ripple Labs, 2014.

[25] Evan Duffield, Daniel Diaz, *Dash: A payments-focused cryptocurrency*

[26] anonymous, Dash Developer Reference. URL: https://dash-docs.github.io/en/developer-reference

[27] anonymous, Dash Features. URL: https://docs.dash.org/en/stable/

[28] anonymous*, What's DNS? And why does Dot-Bit matter?,* URL: https://bit.namecoin.org/

[29] Harry Kalodner, Miles Carlsten, Paul Ellenbogen, Joseph Bonneau, Arvind Narayanan, *An empirical study of Namecoin and lessons for decentralized namespace design,* Princeton University

[30] Merged-mining. URL: https://www.binance.vision/glossary/merged-mining

[31] What is Namecoin? Future of NMC Cryptocurrencyand know how to buy NMC. URL:https://coinswitch.co/info/namecoin/what-is-namecoin

[32] Vinced, Namecoin design, URL: https://github.com/vinced/namecoin/blob/master/DESIGN-namecoin.md

[33] Tomas Melin och Tomas Vidhall, *Namecoin as authentication for public key cryptography*, Institutionen för datavetenskap Department of Computer and Information Science , 2014-06-15

[34] Luke Anderson , Ralph Holz , Alexander Ponomarev , Paul Rimba , Ingo Weber, *New kids on the block: an analysis of modern blockchains,* University of Sydney, Australia, 21-06-2016

[35] Tao Hung Chang, Davor Svetinovic, Data analysis of Digital Currency Networks: Namecoin case study,21st International Conference on Engineering of Complex computer Systems, November 2016

[36] Muneeb Ali , Jude Nelson , Ryan Shea , Michael J. Freedman, *Blockstack: Design and Implementation of a Global Naming System with Blockchains,* Princeton University , February 2016

[37] Andreas Loibl , *Namecoin* , Seminars FI / IITM SS 2014 , Technische Universität München , August 2014

[38] Jiaqi Liang, Linjing Li, Daniel Zeng, *Evolutionary dynamics of cryptocurrency transaction networks: An empirical study* , Research article, 17 August 2018

[39] Zachary Amsden, Ramnik Arora, Shehar Bano, Mathieu Baudet, Sam Blackshear, Abhay Bothra, George Cabrera, Christian Catalini, Konstantinos Chalkias, Evan Cheng, Avery Ching, Andrey Chursin, George Danezis, Gerardo Di Giacomo, David L. Dill, Hui Ding, Nick Doudchenko, Victor Gao, Zhenhuan Gao, François Garillot, Michael Gorven, Philip Hayes, J. Mark Hou, Yuxuan Hu, Kevin Hurley, Kevin Lewi, Chunqi Li, Zekun Li, Dahlia Malkhi, Sonia Margulis, Ben Maurer, Payman Mohassel, Ladi de Naurois, Valeria Nikolaenko, Todd Nowacki, Oleksandr Orlov, Dmitri Perelman, Alistair Pott, Brett Proctor, Shaz Qadeer, Rain, Dario Russi, Bryan Schwab, Stephane Sezer, Alberto Sonnino, Herman Venter, Lei Wei, Nils Wernerfelt, Brandon Williams, Qinfan Wu, Xifan Yan, Tim Zakian, Runtian Zhou, *The Libra Blockcain,* September 2019, URL: https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf

[40] Shehar Bano, Mathieu Baudet, Avery Ching, Andrey Chursin, George Danezis, François Garillot, Zekun Li, Dahlia Malkhi, Oded Naor, Dmitri Perelman, Alberto Sonnino , *State Machine Replication in the Libra Blockchain* , URL: https://developers.libra.org/docs/assets/papers/libra-consensus-state-machine-replication-in-the-libra-blockchain.pdf

[41] Libra Protocol. URL:https://developers.libra.org/docs/libra-protocol

[42] Life of a Transaction. URL:https://developers.libra.org/docs/life-of-a-transaction

[43] The Libra Reserve URL: https://libra.org/en-US/about-currency-reserve/#the_reserve

[44] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis, *SoK: Consensus in the Age of Blockchains,2017*

[45] Ryan Farrel, *An Analysis of the Cryptocurrency Industry, 2015*

[46] L.M.Bach, B.Mihaljevic, and M.Žagar, *Comparative Analysis of Blockchain Consensus Algorithms,* 2018

[47] Lara Mauri, Stelvio Cimato, and Ernesto Damiani, *A comparative analysis of current cryptocurrencies*

[48] Martin Garriga, Maxmiliano Arias, Alan De Renzis, *Blockchain and Cryptocurrency: A comparative framework of the main Architectural Drivers, 2018*