ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών

ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΤΑΝΕΜΗΜΕΝΟΥ ΚΑΘΟΛΙΚΟΥ

Distributed Ledger Techologies

1η Εργασία

Υλοποίηση Miner και Merkle Proof

Evagelia Chaniotaki
13442020108

Μάιος 24

Εισαγωγή

Στην παρούσα αναφορά παρουσιάζεται η υλοποίηση διαφόρων λειτουργιών τεχνολογίας blockchain χρησιμοποιώντας τη γλώσσα προγραμματισμού Python καθώς και οι βιβλιοθήκες hashlib(για την κρυπτογράφηση SHA-256) και time(για τον υπολογισμό χρόνου εκτέλεσης) . Η υλοποίηση αυτή περιλαμβάνει την κατασκευή ενός Merkle tree, την εξόρυξη νέων block (mining), καθώς και την εύρεση της απόδειξης ύπαρξης μιας συναλλαγής σε ένα Merkle tree.

Κατασκευή Merkle Tree

Αρχικά, χρησιμοποιήθηκε η συναρτηση **construct_merkle_tree** για τη δημιοργία ενός Merkle tree από μια λίστα συναλλαγών. Η συνάρτηση αυτή παράγει το Merkle tree χρησιμοποιώντας το hash συναλλαγών με αλγόριθμο SHA-256. Ενδεικτικά :

Args: transactions (list): Η λίστα των συναλλαγών.

Returns: list: Λίστα από λίστες που αντιπροσωπεύουν τα επίπεδα του Merkle tree.

Εξόρυξη Νέων Block (Mining)

Στη συνέχεια, αναπτύχθηκε η λειτουργία εξόρυξης νέων block στο blockchain με χρήση του αλγορίθμου proof of work. Οι εξόρυξη νέων block γίνεται μέσω του υπολογισμού ενός nonce που επιτρέπει την εύρεση ενός block hash με συγκεκριμένο αριθμό μηδενικών στην αρχή του. Ενδεικτικά :

Args: merkle_root_hash (str): Το hash του Merkle root.

previous_block_hash (str): Το hash του προηγούμενου block.

difficulty (int): Το επίπεδο δυσκολίας της εξόρυξης. Returns int : το nonce που βρέθηκε.

Αναζήτηση Απόδειξης Υπαρξης Συναλλαγής (generate proof)

Τέλος, υλοποιήθηκε η λειτουργία εύρεσης της απόδειξης ύπαρξης μιας συναλλαγής σε ένα Merkle tree. Αυτή η λειτουργία ελέγχει αν μια συναλλαγή υπάρχει στο Merkle tree . Εάν υπάρχει τότε επιστρέφει την απόδειξη της ύπαρξης της σε μορφή dictionary , περιλαμβάνοντας τα επίπεδα του δέντρου αλλα και τα αντίστοιχα ζεύγη.Ενδεικτικά:

Args: transaction (str): Η συναλλαγή που αναζητείται.

merkle_tree (list): Το Merkle tree.

Returns: dict: Το λεξικό με τα ζευγάρια που περιλαμβάνουν το επίπε

Αποτελέσματα

Στη διάρκεια της εκτέλεσης του κώδικα που αναπτύχθηκε, πραγματοποιήθηκαν αρκετές δοκιμές για την εξόρυξη νέων block, την κατασκευή του Merkle tree, και τη δημιουργία αποδείξεων ύπαρξης συναλλαγών. Τα αποτελέσματα καταδεικνύουν τη σωστή λειτουργία του κώδικα και την επιτυχή υλοποίηση των βασικών λειτουργιών της τεχνολογίας blockchain.

Ο κώδικας περιλαμβάνει αρκετά σχόλια για την ευκολότερη κατανόηση της λειτουργίας του. Επιπλέον, παραθέτω ένα απόκομμα από την τελική έξοδο.