Δημήτριος Κυριακίδης

el17077

Κρυπτογραφία

Εξαμηνιαία Εργασία

«Τυχερά Παίγνια με Χρήση Τεχνολογίας Αλυσίδας Συναλλαγών»

Περιγραφή

Η εργασία αυτή βασίζεται στην ομώνυμη διπλωματική εργασία [1], στην οποία παρουσιάζεται ένα πρωτόκολλο υλοποίησης τυχερών παιγνίων, συγκεκριμένα της ρουλέττας, με χρήση blockchain. Η ιδέα αυτή έχει αξία διότι εξαλείφει τα προβλήματα εμπιστοσύνης που υφίστανται στις συμβατικές μεθόδους διεξαγωγής τέτοιων παιγνίων. Βασίζεται στην δημιουργία πλευρικής αλυσίδας για κάθε νέα υπόσταση του παιγνίου, και ως μέθοδοι κρυπτογράφησης - επαλήθευσης χρησιμοποιούνται το σχήμα κρυπτογράφησης El Gamal και η συνάρτηση κατακερματισμού SHA256. Στην παρούσα εργασία γίνεται μία πλήρως λειτουργική, απλοποιημένη εφαρμογή του πρωτοκόλλου αυτού σε γλώσσα Python.

Θεωρητική Θεμελίωση

Αρχικά θα δοθούν κάποιοι ορισμοί για τα βασικά θεωρήματα και μαθηματικά εργαλεία που χρησιμοποιούνται από το πρωτόκολλο και τις τεχνολογίες που αυτό προϋποθέτει.

Πρόβλημα Διακριτού Λογαρίθμου (DLP):

Έστω p πρώτος, g γεννήτωρ του δακτυλίου $\mathbb{Z}_p^*$ και y ένα στοιχείο του $\mathbb{Z}_p^*$. Το πρόβλημα του διακριτού λογαρίθμου είναι η εύρεση ακεραίου k τέτοιου, ώστε $g^k \equiv y \ mod \ p$.

Πρόβλημα Diffie-Hellman:

Έστω p ένας πρώτος και g ένας γεννήτωρ του δακτυλίου $\mathbb{Z}_p^*$. Αν δίνονται οι τιμές $g^a \ mod \ p$ και $g^b \ mod \ p$, χωρίς να είναι γνωστά τα a, b, τότε το πρόβλημα Diffie-Hellman είναι η εύρεση της τιμής $g^{ab} \ mod \ p$.

Το πρόβλημα DLP θεωρείται υπολογιστικώς δύσκολο, και το DHP ανάγεται σε αυτό (δηλαδή λύση του DLP συνεπάγεται και λύση του DHP). Η δυσκολία επίλυσης του DLP σχετίζεται με την ασφάλεια ιδιωτικών κλειδιών στο κρυπτοσύστημα El Gamal.

Κρυπτοσύστημα El Gamal:

- Δημιουργία κλειδιών
  Κάθε χρήστης ακολουθεί τα εξής βήματα για την παραγωγή δημοσίου και ιδιωτικού κλειδιού:
  1. Δημιουργεί μεγάλο πρώτο αριθμό p και γεννήτορα g του σώματος $\mathbb{Z}_p^*$.
  2. Επιλέγει έναν τυχαίο αριθμό α, $0 \leq a \leq p-2$ και υπολογίζει την τιμή $g^a \ mod \ p$.
  3. Το δημοσιο κλειδί του χρήστη είναι το (p, g, g^a) και το ιδιωτικό το α.
- Κρυπτογράφηση
  Ο χρήστης Α κρυπτογραφεί μήνυμα m και το στέλνει στον Β.
  1. Λαμβάνει το δημόσιο κλειδί (p, g, g^b) του Β.
  2. Μετατρέπει το μήνυμα m σε έναν ακέραιο στο διάστημα $\{0, \dots, p-1\}$.
  3. Επιλέγει τυχαίο ακέραιο k, $0 \leq k \leq p-2$.
  4. Υπολογίζει τις τιμές $\gamma = g^k \ mod \ p$, $\delta = m \cdot (g^b)^k \ mod \ p$ και στέλνει το κρυπτοκείμενο $c = (\gamma, \delta)$ στον Β.
- Αποκρυπτογράφηση
  Ο χρήστης Β αποκρυπτογραφεί το μήνυμα $c = (\gamma, \delta)$ που έλαβε από τον Α.
  1. Υπολογίζει την τιμή $\widehat{m} = \gamma^{p-1-b} \ mod \ p$.
  2. Ανακτά το αρχικό μήνυμα m υπολογίζοντας την τιμή $\widehat{m} \cdot \delta \ mod \ p$.

Συνάρτηση SHA256

Η συνάρτηση κατακερματισμού SHA256 (Secure Hash Algorithm-256) ανήκει στην γενικότερη οικογένεια συναρτήσεων SHA, και αντιστοιχίζει τμήματα μεγέθους 512 bits σε έξοδο μήκους 256.

Επεξήγηση Προγράμματος

Το πρόγραμμα έχει δομηθεί σε τέσσερα αρχεία κλάσεων, και ένα βοηθητικό που τρέχει το παίγνιο. Τα αρχεία του προγράμματος που περιέχουν την λογική του πρωτοκόλλου είναι τα Blockchain.py, Player.py και RouletteMaster.py.

Η κλάση Blockchain, χρησιμοποιώντας και την κλάση Block, υλοποιεί τις βασικές λειτουργίες μίας blockchain: εισαγωγή καταγραφών σε ένα block, σύνδεση νέων blocks παρεχομένης proof-of-work, επαλήθευση της απόδειξης αυτής. Κάθε block αφορά έναν γύρο του παιγνίου, και περιέχει πολλές καταγραφές - συναλλαγές. Όπως προβλέπεται από τους βασικούς κανόνες της blockchain, κάθε block επίσης περιέχει το hash του προηγούμενου. Κάθε μία συναλλαγή (transaction) είναι είτε ανακοίνωση ενός συμμετέχοντος, είτε ανακοίνωση ενός στοιχήματος, είτε μεταφορά πόρων από κάποιον εκ των συμμετεχόντων προς άλλον, ως αποτέλεσμα του παιγνίου. Για λόγους υπολογιστικής ευκολίας της προγραμματιστικής υλοποίησης, έχει χρησιμοποιηθεί μία απλοϊκή μέθοδος απόδειξης εργασίας. Σε πραγματικές συνθήκες φυσικά θα μπορούσε να αξιοποιηθεί καλύτερη μέθοδος, όπως η “Hashcash” του Bitcoin.

Η κλάση RouletteMaster υλοποιεί τον «επόπτη» του παιγνίου, ο οποίος, σύμφωνα με το πρωτόκολλο ([1], σελίδες 44-45), αρχικά πληροφορείται από όλους τους παίκτες για την πρόθεσή τους να συμμετέχουν, στην συνέχεια δημοσιεύει την πληροφορία αυτήν στην αλυσίδα, έπειτα δέχεται τα στοιχήματα όλων των συμμετεχόντων, δημοσιεύει και αυτά, και τέλος υπολογίζει τα αποτελέσματα και τα δημοσιεύει στην αλυσίδα.

Τέλος, η κλάση Player υλοποιεί τις ενέργειες ενός παίκτη: δήλωση συμμετοχής και στοιχήματος, και δημοσίευση αυτών στην αλυσίδα. Για λόγους απλότητας της εφαρμογής, κάθε παίκτης εκκινεί με ίδιο κεφάλαιο και στοιχηματίζει σταθερό ποσό σε τυχαίο αριθμό.

Με την εκτέλεση του αρχείου main.py μία φορά, παίζεται ένας γύρος του παιγνίου, και το αποτέλεσμα τυπώνεται στην γραμμή εντολών. Η αλυσίδα αποθηκεύεται στο σειριοποιημένο αρχείο blockchain.pkl, ώστε να μπορεί να ανακτηθεί και να εκτυπωθεί στο αρχείο chain.txt σε αναγνώσιμη μορφή.

Επίλογος

Είναι εμφανές ότι λόγω του δυσεπίλυτου χαρακτήρα του προβλήματος που βρίσκεται στο υπόβαθρο του συστήματος ασφαλείας των Blockchains, αυτές είναι ιδανικές για σχεδόν οποιαδήποτε εφαρμογή που εμπεριέχει συναλλαγές μεταξύ άγνωστων μερών. Μία από αυτές είναι και τα τυχερά παίγνια. Το πρωτόκολλο στο οποίο στηρίζεται η εργασία αυτή δεν θα επέτρεπε σε κακόβουλο παίκτη να αλλοιώσει την αλυσίδα προς προσωπικό χρηματικό όφελος, καθώς δεν θα μπορούσε να κατασκευάσει την πλειοψηφία των blocks. Καθώς πολλά τυχερά παίγνια ήδη διεξάγονται στο διαδίκτυο, η τεχνολογία Blockchain βρίσκει σε αυτά έξοχη εφαρμογή.

Βιβλιογραφία

Έντυπη

[1] Κουτσός, Βλάσιος. *Πρωτόκολλα Τυχερών Παιγνίων με Χρήση Τεχνολογίας Αλυσίδας Συναλλαγών (Blockchain)*. 2018. Εθνικό Μετσόβιο Πολυτεχνείο, Διπλωματική Εργασία.

[2] Burmester, Mike, et al. *Σύγχρονη Κρυπτογραφία*. Αθήνα, Παπασωτηρίου, 2011.

Ηλεκτρονική

[3] Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. N.p. Web. 24 Mar 2022. https://bitcoin.org/bitcoin.pdf.

[4] van Flymen, Daniel. “Learn Blockchains by Building One.” HackerNoon, 22 Sept. 2017, https://hackernoon.com/learn-blockchains-by-building-one-117428612f46. Accessed 22 Mar. 2022.