ניתוח פיצולים במערכת בלוקצ'יין

יונתן בן צבי yonibz92@campus.tecnion.ac.il

אליעד בן ישי ebenyishay@campus.technion.ac.il

מנחה: איתי צברי

1.1.2020

מבוא

במערכות מרובות משתמשים, באופן אידאלי, כל המשתמשים רואים את אותה "המציאות", אך בחיים לא הכל תמיד אידאלי ובמערכות מבוזרות מרובות משתמשים, כדוגמת בלוקצ'יין, לכל משתמש יש את נקודת המבט שלו. דבר הנובע מקצב התפשטות המידע במערכת, שאינו מידי.

במערכת בלוקצ'יין, כתוצאה מהפרשי הזמנים בין רגע כריית בלוק חדש על ידי משתמש במערכת לבין רגע הגעת המידע על היווצרות הבלוק החדש למשתמש אחר, נוצר מצב שבכל רגע נתון במערכת לכל משתמש יש את נקודת המבט שלו ולאף משתמש אין גישה לנקודת מבט גלובלית על המערכת, מצב אליו המערכת שואפת להגיע. באומרנו נקודת מבט גלובלית בהקשר למערכת בלוקצ'יין, הכוונה היא לשרשרת בלוקים ראשית שאמורה להיות זהה עבור כל המשתמשים.

אחת מתופעות הלוואי שנולדו בשל נקודות המבט השונות של משתמשי מערכת בלוקצ'יין נקראת פיצולים (באנגלית: Forks). פיצול במערכת בלוקצ'יין הוא מצב שברגע נתון לשני משתמשים שונים יש שתי שרשראות בלוקים שונות שיש להן רישא משותפת, מצב שלא אמור להתרחש במערכת אידאלית בה המידע מגיע באופן מידי.

ישנם גורמים שונים שעשויים להשפיע על פיצולים במערכת בלוקצ'יין והגורמים אליהם בחרנו להתייחס בניתוח הבעיה הם: הטופולוגיה של המערכת, כוח הכרייה של משתמשי המערכת, גודל תקופה (epoch) וקצב יצירת הבלוקים הרצוי אליו המערכת שואפת להתנרמל.

בלוקצ'יין

בסיס נתונים מבוזר וסדרתי המכיל שרשרת בלוקים שמהווים את אבני היסוד בהן נשמר המידע.

כל בלוק מקושר לבלוק הקודם בשרשרת (ולא מקושר לבלוק הבא), מכיל את זמן היווצרותו, מזהה ייחודי ומידע נוסף.

כריית בלוק היא תהליך של פתירת חידה קריפטוגרפית ובאופן כללי, הסיכוי של כל משתמש לכרות את הבלוק הבא במערכת הוא היחס בין כוח הכרייה של המשתמש לבין סך כוח הכרייה של כל משתמשי המערכת.

כאשר משתמש כורה בלוק, המידע על כך נשלח ליתר המשתמשים. בלוק חדש מתווסף לשרשרת קיימת של משתמש במערכת רק אם אורך השרשרת אליה מחובר הבלוק שנוצר, ארוכה יותר מהשרשרת הנוכחית של המשתמש אליו הגיע המידע.

פיצולים במערכת בלוקצ'יין

מטרות עיקריות

מימוש

מימשנו את הקוד בשפת Python 3.7, בסביבת העבודה PyCharm, תוך שימוש ב-GitHub לשמירת הקוד וב-Git לבקרת גרסאות.

הסימולטור מבוסס תור עדיפויות של אירועים ומקבל כפרמטר מחלקה שהיא iterable, הנקראת SystemGenerator, ליצירת מערכות בלוקצ'יין עם פרמטרים שונים בהתאם לאתחולה.

SystemGenerator מאותחלת עם כל פרמטרי המערכת הרלוונטיים (מספר הבלוקים באפוק, קצב יצירת בלוקים רצוי, טופולוגיית המערכת, כוחות החישוב של משתמשי המערכת).

האירועים הרלוונטיים עבורנו היו יצירת בלוק חדש והגעת בלוק קיים למשתמש במערכת.

סימלוץ תהליך כריית הבלוקים מתבצע בסימולטור על ידי הגרלת זמני יצירתם לפי כוח החישוב של המשתמש וקושי שרשרת הבלוקים הרלוונטית עבורו, בדומה לאופן שבו עובד תהליך כריית בלוקים בביטקוין.

להלן נרחיב על מספר מחלקות עיקריות אותן מימשנו בכתיבת הסימולטור:

**Block:** מחלקה המתארת בלוק בשרשרת בלוקצ'יין. כל בלוק מצביע על הבלוק שקדם לו בשרשרת של מי שיצר אותו (חוץ מבלוק המקור במערכת) ומכיל מידע לגבי הבעלים שלו, זמן היצירה שהוגרל עבורו, אינדקסו בשרשרת אליה הוא התחבר, הקושי החישובי של השרשרת, מספר הבלוק באפוק (לצורך עדכון הקושי בתחילת כל אפוק), קצב יצירת בלוקים רצוי ואת מספר ההתחלות של פיצולים ממנו (כלומר, כמה בלוקים מצביעים עליו פחות אחד עבור המצב ה"תקין").

**Node:** מחלקה המתארת משתמש במערכת. כל משתמש מכיל את כוח החישוב שלו, את רשימת שכניו בטופולוגיית המערכת, את הבלוק האחרון בשרשרת הבלוקים שלו (מאפשר גישה סדרתית לכל בלוקי השרשרת), מזהה ייחודי ומצביע לאירוע יצירת הבלוק הבא.

**SystemEvent:** מחלקה אבסטרקטית המתארת אירוע במערכת. המחלקה מכילה את זמן יצירת האירוע, את מזהה המשתמש שיצר את האירוע ויורשות ממנה שתי המחלקות בהן נעשה שימוש בסימולטור.

מחלקה יורשת אחת נקראת BlockCreation. מתארת אירוע של יצירת בלוק ואין מוסיפה למחלקת האב.

מחלקה יורשת שנייה נקראת BlockArrival. מתארת אירוע של הגעת בלוק ומכילה בנוסף למחלקת האב גם את מזהה המשתמש ששלח את הבלוק וכן את הבלוק עצמו.

**System:** המחלקה המתארת את המערכת כולה. מכילה את כל המידע איתו מאותחלת המערכת (את הטופולוגיה, כוחות החישוב של המשתמשים, גודל כל אפוק, קצב יצירת בלוקים רצוי) בנוסף לרשימת משתמשי המערכת, אותם היא יוצרת באתחולה. כחלק מאתחול המערכת מתחיל תהליך יצירת האירועים והם נשמרים בתור עדיפויות.

מעבר למתודות סטנדרטיות, המחלקה מכילה מתודה חשובה, step, המשמשת לטיפול באירוע הנמצא בראש תור האירועים.

**Simulator:** להשלים עם אליעד...

תוצאות

הרצנו מספר ניסויים עם טופולוגיות ופרמטרי מערכת שונים על מנת לנתח היבטים שונים הקשורים לתופעת הפיצולים במערכת בלוקצ'יין ולהציג את פלט הסימולטור שכתבנו.

* להסביר למה בדיוק התכוונו באיטרציה...
* בכל הגרפים לא לשכוח להוסיף **שמות לצירים**, **מקרא** (במידת הצורך), **שם לגרף** (מתחת), **מספר** **איטרציות** (מתחת), **מספר ריצות** (מתחת. לפי מספר זה נלקח הממוצע)...

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| מספר גרף | טופולוגיה | ציר x | ציר y | מטרה | הערות |
| 1 | 2 צמתים מחוברים עם מרחק גדול ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | אינדקס ממוצע של הבלוק הזר הראשון (**המינימלי** מבין שני הצמתים) | בדיקה מתי לראשונה נשברת ה"הפרדה" | * **בלי** עדכון difficulty * power **שווה** |
| 2 | 2 צמתים מחוברים עם מרחק גדול ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | אינדקס ממוצע של הבלוק הזר הראשון (**המינימלי** מבין שני הצמתים) | להראות השפעה של ויסות קצב יצירת הבלוקים על התופעה | * **עם** עדכון difficulty * power **שווה** |
| 3 | 2 צמתים מחוברים עם מרחק גדול ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | המספר הממוצע של פיצולים **במערכת** | להראות שללא ויסות של קצב יצירת הבלוקים יש פיצולים רבים | * **בלי** עדכון   difficulty   * power **שווה** |
| 4 | 2 צמתים מחוברים עם מרחק גדול ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | המספר הממוצע של פיצולים **במערכת** | להראות השפעה של ויסות קצב יצירת הבלוקים על מספר הפיצולים | * **עם** עדכון   difficulty   * power **שווה** |
| 5 | קליקה של 10-20 צמתים עם מרחק 0 ביניהם | מספרי הצמתים | אחוז הבלוקים בבעלות הצומת מסך הבלוקים בשרשרת שלו | להראות תקינות של המערכת | * **עם** עדכון   difficulty   * לצומת ה-i יהיה power * דיאגרמת **עמודות** |
| 6 | קליקה של 10-20 צמתים עם מרחק חיובי ושווה ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | מספר הפיצולים הממוצע **במערכת** | להראות בתרחיש יותר "מציאותי" את השפעת היחס הנ"ל על מספר הפיצולים | * **עם** עדכון   difficulty   * power **שווה** |
| 7 | קליקה של 10-20 צמתים עם מרחק חיובי ושווה ביניהם | היחס בין קצב יצירת הבלוקים הצפוי לבין המרחק בין שני הצמתים | מספר הפיצולים הממוצע **במערכת** | להראות השפעת הויסות על מספר הפיצולים | * **בלי** עדכון   difficulty   * power **שווה** |

לבדוק עם איתי אם מספיק או שיש לו רעיונות לגרפים מעניינים נוספים.

מסקנות

להשלים לאחר שיהיו תוצאות...

עבודה עתידית

* להריץ ולנתח תרחישים נוספים.
* להשתמש בסימולטור כתשתית לניתוח תופעות נוספות המתרחשות במערכות בלוקצ'יין.