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.

מחלקות חשובות:

**Block:** לךחכשד

**Node:** ךלח

**SystemEvent:** ךלחךל

**System:** חליל

**Simulator:** חליל

תוצאות

* בכל הגרפים להוסיף שם לגרף ומספר איטרציות (להסביר למה קראנו איטרציה...)!
* ציר y יהיה האינדקס הממוצע של הבלוק הזר הראשון (גרף עבור **כל** צומת) וציר x יהיה היחס בין קצב יצירת הבלוקים המצופה לבין ה"מרחק" בין כל שני משתמשים (**בלי** עדכון קושי!).
* מחייב קליקה עם קשתות שוות.
* להריץ עם טופולוגיה אחת: 2 צמתים. 2 תצורות כוח: כוח שווה, כוח שונה (למשל כפול).
* שני עמודים שונים בספר הפרויקט, אחד לכל תצורה.
* ציר y יהיה מספר הפיצולים הממוצע **בשרשרת** (גרף עבור **כל** צומת) וציר x יהיה היחס בין קצב יצירת הבלוקים המצופה לבין ה"מרחק" בין כל שני משתמשים (בלי עדכון קושי!).
* מחייב קליקה עם קשתות שוות.
* להריץ עם טופולוגיה אחת: 2 צמתים. 2 תצורות כוח: כוח שווה, כוח שונה (למשל כפול).
* שני עמודים שונים בספר הפרויקט, אחד לכל תצורה.
* ציר y יהיה מספר הפיצולים הממוצע **במערכת** וציר x יהיה היחס בין קצב יצירת הבלוקים המצופה לבין ה"מרחק" בין כל שני משתמשים (**עם** עדכון קושי!).
* מחייב קליקה עם קשתות שוות.
* להריץ עם טופולוגיה אחת: 2 צמתים. 2 תצורות כוח: כוח שווה, כוח שונה (למשל כפול).
* שני עמודים שונים בספר הפרויקט, אחד לכל תצורה.
* ציר y יהיה מספר הפיצולים הממוצע **במערכת** וציר x יהיה היחס בין קצב יצירת הבלוקים המצופה לבין ה"מרחק" בין כל שני משתמשים (**בלי** עדכון קושי).
* מחייב קליקה עם קשתות שוות.
* להריץ עם טופולוגיה אחת: "הרבה" צמתים. 2 תצורות כוח: כוח שווה, כוח שונה.
* שני עמודים שונים בספר הפרויקט, אחד לכל תצורה.
* ציר y יהיה מספר הפיצולים הממוצע **במערכת** וציר x יהיה היחס בין קצב יצירת הבלוקים המצופה לבין ה"מרחק" בין כל שני משתמשים (**עם** עדכון קושי).
* מחייב קליקה עם קשתות שוות.
* להריץ עם טופולוגיה אחת: "הרבה" צמתים. 2 תצורות כוח: כוח שווה, כוח שונה.
* שני עמודים שונים בספר הפרויקט, אחד לכל תצורה.
* ציר y יהיה

מסקנות ועבודה עתידית

* לבדוק עבור