

האוניברסיטה הפתוחה
המחלקה למתמטיקה ולמדעי המחשב

מימוש חיפוש טרנזקציות בבלוקצ'יין

דוח פרויקט מתקדם זה הוגש כחלק מהדרישות לקבלת תואר
"מוסמך למדעים" M.Sc. במדעי המחשב
באוניברסיטה הפתוחה
המחלקה למתמטיקה ולמדעי המחשב

על-ידי

נועם מימון

העבודה הוכנה בהדרכתו של פרופ' אהוד גודס

דצמבר 2019

תוכן עניינים

3.....	תקציר
5.....	מבוא
6.....	מטרת הפרויקט
6.....	חשיבות הפרויקט
7.....	מושגי יסוד
7.....	בלוקצ'ין
9.....	טרנזקציות
12.....	ניתוח מקוון
12.....	Web scraping
14.....	Transaction fingerprinting
15.....	מימוש הפרויקט
15.....	תכולת עבודה
15.....	סביבת פיתוח וכלי עבודה
16.....	Data set
16.....	ארכיטקטורה
18.....	קלט ופלט
19.....	דוגמאות הרצה
22.....	מגבלות התוכנה
22.....	אתגרים
23.....	תוצאות ומסקנות
24.....	Bibliography

רשימת איורים

7	איור 1- שרשרת הבלוקים
9	איור 2 - טרנזקציה עם קלט אחד
11	איור 3 - טרנזקציה עם מספר פלטים
12	איור 4 - כתובת ביטקוין נחשפת בשוגג על ידי משתמש
18	איור 5 - דיאגרמת המחלקות של ספריית Bitcoin
19	איור 6- זליגת כתובת משתמש ברשת הפייסבוק
20	איור 7- פרמטרים לחיפוש טרנזקציות בבלוקצ'יין
20	איור 8- מהלך החיפוש הטרנזקציות בבלוקים
21	איור 9 - תוצאת החיפוש

תקציר

רשת הביטקוין היא רשת מבוזרת שבה ניתן לבצע תשלומים בעזרת המטבע הדיגיטלי ביטקוין. כל עסקאות המטבע, דהיינו הטרוזקציות, נרשמות לפנקס ציבורי המכונה בלוקצין. לדוגמה כתובת X שלחה Y מטבעות לכתובת Z . הבלוקצין שומר את כל הטרוזקציות שנעשו במטבע מיום הקמת הרשת ב 2009. הטרוזקציות נשמרות לא מוצפנות ולכן כל אחד יכול לראות את כולן.

בעבודה המסכמת סקרנו מספר דרכים לחשוף פעילות משתמשים ברשת הביטקוין אשר כולן משתמשות בבלוקצין כבסיס לעבודתן. למשל ב [1] ראינו כיצד קוראים את הטרוזקציות ובונים ממנו גרף המתאר את זרימת המטבעות, כאשר הצמתים הם הכתובות אשר שולחות ומקבלות את המטבעות. בהמשך מסמנים צמתים בגרף על פי מידע שחושפים באינטרנט, למשל עבור משתמש אשר חשף את כתובת הביטקוין שלו בפורום באינטרנט נסמן את הכתובת התואמת בגרף עם שם המשתמש כפי שהופיע באינטרנט. דוגמה נוספת הייתה לחפש טרוזקציות בבלוקצין על פי מידע חלקי אודות הטרוזקציה. למשל פלוני שאמר לאלמוני שלחתי לך 10 ביטקוין אתמול בצהריים. ראינו כי ניתן לייצר טרוזקציות מועמדות עם הסתברות מסוימת.

בפרויקט המעשי מימשת 2 שיטות לחיפוש מידע בבלוקצין, כפי שעולה מ [1]. השיטה ראשונה הינה חיפוש מדויק של כתובת מסוימת. בשיטה זו מחפשים תחילה באינטרנט משתמש אשר חשף בטעות את כתובת הביטקוין שלו, ומחפשים בבלוקצין טרוזקציות אשר כתובת זו מופיעה בהן. באופן זה ניתן לדעת את הכתובת השולחת, את סכום המטבעות שנשלחו, הזמן בו התבצעה השליחה ועוד. החיפוש אותו בחנתי היה חיפוש אחר טרוזקציות של משתמש אשר חשף את כתובת הביטקוין שלו בפייסבוק. תוצאות החיפוש הראו את כל פרטי הטרוזקציה שתיאר המשתמש באינטרנט, ונתנו לנו מידע נוסף על הישות אשר שלחה את הטרוזקציה למשתמש אשר עליו התבצע החיפוש.

השיטה השנייה הינה חיפוש טרוזקציה על פי מאפיינים מסוימים. כאן הקלט הינו מידע חלקי אודות הטרוזקציה כגון טרוזקציה שנשלחה בתאריך מסוים בצהרי היום עם סכום מטבעות כלשהו. על פי פרמטרים אלה מחפשים את כל הטרוזקציות המועמדות להיות הטרוזקציה שאנו מחפשים. עבור כל טרוזקציות שנמצאות תואמת לפרמטרים שבחיפוש, מוצגים נתונים מתוך האובייקט של הטרוזקציה כמו גם מאובייקט הבלוק שבו נמצאה.

בדוח זה נתאר תחילה את מושגי היסוד הרלוונטיים לעבודה זו כגון טרוזקציות ובלוקים. בנוסף נתאר כיצד מורידים את הבלוקצין וקוראים את הטרוזקציות. בהמשך נתאר את שיטות החיפוש אשר אותן מימשנו בפרויקט. לאחר מכן נתאר את

ארכיטקטורת המערכת, גבולותיה ומאפייני האובייקטים מהם היא מורכבת. לבסוף נראה את דוגמאות ההרצה וננתח אותן.

רשת הביטקוין הינה אוסף מבוזר של מחשבים, על גבי רשת האינטרנט, אשר מאמתים ומתעדים את עסקאות המטבע.

כאשר שולחים ביטקוין בעזרת הארנק, לכתובת ארנק של מישהו אחר, נשלחת טרנזקציה לרשת הביטקוין. הטרנזקציה מגיעה לאחד מהכורים, אשר מוודא את תקינות הטרנזקציה. במידה שהטרנזקציה תקינה, הוא יצרף אותה לבלוק של טרנזקציות ויתחיל לבצע "הוכחת עבודה" זאת אומרת יחפש מספר אשר ה HASH שלו ושל כל הטרנזקציות בבלוק (ביחד עם המספר של הבלוק הקודם) יתחיל במספר ארוך של אפסים (מספר זה משתנה, בהתאם לכוח החישוב של הרשת). כאשר הוא ימצא את המספר (לאחר מעבר סידרתי על כל האפשרויות, ולכן פעולה זו נקראת הוכחת עבודה) הוא יכניס אותו לפנקס הציבורי שברשותו, וישדר את הבלוק לשאר הצמתים ברשת אשר יוודאו את תקינותו ויכניסו אותו לעותק של הפנקס הציבורי שברשותם. כך נשמרת הטרנזקציה באופן גלוי לכל וללא אפשרות לבטלה בשום צורה. הטרנזקציות מוכנסות לבלוק, עם ID ייחודי, בצורה מסודרת ואופטימלית לשליפה מהירה, למשל על מנת לוודא את סכום הביטקוין שיש לכתובת הארנק ואותו יוכל לבזבז.

אם כן, הבלוקצין הוא בסיס נתונים ציבורי המכיל את נתוני כל הטרנזקציות שנעשו אי פעם וממנו ניתן לדלות המון מידע. היתרון בעצם העובדה שהמערכת הינה מבוזרת הוא גם החיסרון שכן עותקי הטרנזקציות נשמרים אצל כל צומת ברשת וגלויים לכל. מצד אחד אין פרטים אישיים ברשת למעט כתובת ארנק, מצד שני אפשר לעקוב אחרי כל הטרנזקציות ממנה ואליה, ואם אי פעם מישהו חשף את הבעלים שלה אזי כל ההיסטוריה ועתיד התשלומים שלו מכתובת זו זה גם כן נחשפו.

כפי שמוזכר ב [1] ישנן מספר דרכים לקבל את הבלוקצין. בעבודה זו השתמשנו בתוכנה הרשמית של ארנק הביטקוין bitcoin core. מקור נוסף שבו השתמשנו הינו רשת האינטרנט. הרשת, ובייחוד אתרי פורומים בענייני ביטקוין מלאים במידע שאנשים חשפו אודות הטרנזקציות שביצעו וכתובות שהשתמשו.

כעת האתגר הוא להבין כיצד בנוי הבלוקצין, כיצד ניתן לקרוא ממנו את הטרנזקציות והאם וכיצד ניתן למצוא ולשייך טרנזקציות למשתמשים מסוימים או לאירועים כלשהם. כיוון שכמות הטרנזקציות היא עצומה, וכיוון שהטרנזקציות נשמרות רק עם הכתובת הציבורית של מבצע הטרנזקציה, אנו נדרשים לשביבי מידע נוספים כגון מידע שדלף לאינטרנט ומשייך בין משתמש לכתובת או מידע שהתגלה אודות פרטי טרנזקציה כגון תאריך שעה וסכום, בכדי להפיק מידע מהבלוקצין הציבורי שבידנו.

מטרת הפרויקט

מטרת הפרויקט היא לממש חיפוש מקומי נוח ואינטואיטיבי של טרנזקציות מהבלוקצ'יין, לפי השיטות שהוצגו ב [1], ולתת למשתמש כלי נגיש להתנסות בחקירת הבלוקצ'יין. התוכנה מאפשרת באופן מידי, וללא צורך בצעדים מקדימים כלשהם או אפילו חיבור לאינטרנט, לבצע חיפושים ספציפיים וכללים, לחקור את הטרנזקציות בבלוקצ'יין ולקבל מושג מוחשי אודות הטרנזקציות הבלוקים והבלוקצ'יין.

חשיבות הפרויקט

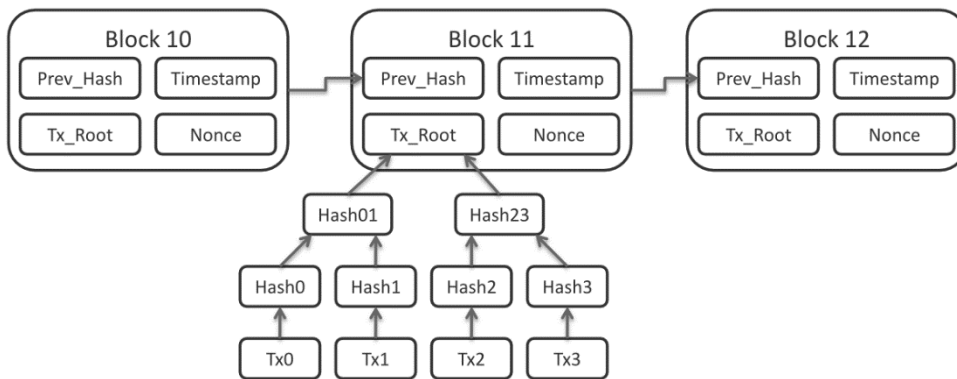
חשיבות הפרויקט היא להראות באופן אמפירי ונוח כיצד ניתן לבצע מגוון חיפושים בבלוקצ'יין ולהדגים פגיעה בפרטיות המשתמשים אשר חושפים את כתובות הביטקוין שלהם באינטרנט או בכל מדיה ציבורית כלשהי. אפילו השמעת מידע אודות טרנזקציה שמישהו ביצע בזמן מסוים יכולה לשמש כקלט עבור החיפוש בבלוקצ'יין וכתוצאה מכך להוביל לכך שנמצא את הטרנזקציה בהסתברות מסוימת.

בלוקצ'יין

הבלוקצ'יין הינו קובץ ציבורי המכיל את כל הטרנזקציות שנעשו במטבע. זהו למעשה ה Database של הטרנזקציות. המימוש של הבלוקצ'יין נעשה בעזרת רשימה מקושרת של בלוקים, כאשר כל בלוק מכיל טרנזקציות ביטקוין.

נכון להיום הבלוקצ'יין מכיל 602,158 בלוקים, כאשר בכל בלוק ישנן 2000 טרנזקציות בממוצע¹. הבלוקצ'יין מכיל את כל הטרנזקציות שהתבצעו במטבע מאז שנוצר.

דוגמא לשרשרת בלוקים המקושרים ביניהם ניתן לראות באיור 1.



איור 1- שרשרת הבלוקים

כפי שרואים ב- שרשרת הבלוקים, כל בלוק מכיל את הגובה שלו מהבלוק הראשון המכונה בלוק בראשית. זהו למעשה המספר הסידורי הייחודי של הבלוק. בנוסף כל בלוק מכיל את ה hash של הבלוק הקודם, עד לבלוק הראשון. כך ניתן למנוע זיוף בנוגע לאמינותם של הבלוקים הקודמים, שכן אם ישתנו הטרנזקציות בבלוק מסוים, אז גם ה hash של כל הבלוק ישתנה וכתוצאה מכך גם ה hash של כל הבלוקים בהמשך.

ה Timestamp משמש כמקור אימות עבור ה hash של הבלוק, ומצביע על הזמן הממוצע שבו נוצר כל בלוק. ברשת הביטקוין בכל 10 דקות בממוצע מתווסף בלוק. ברשת Ethereum זמן הבלוק הוא בין 14 ל 15 שניות.

¹ מתוך <https://www.blockchain.com/charts/>

Nonce הוא מספר רנדומלי באורך 32 ביטים. את המספר הזה מחפשים אלו שמתחזקים את הרשת המכונים כורים. על מנת למצוא את המספר הזה נדרש כוח חישוב גדול, המבצע brute force אך לאחר שהוא נמצא ניתן בקלות לאמת אותו בעזרת hash של תוכן הבלוק ביחד עם ה nonce שנמצא. כך למעשה מתבצעת הוכחת העבודה של הכורה, ולמעשה זוהי ההסכמה המבוזרת של כל הצמתים ברשת על אמינותו של הבלוק החדש. על עבודה קשה זו מתוגמל הכורה במספר ביטקוין וזהו התמריץ שלו לעיבוד הטרנזקציות החדשות לבלוק שיתווסף לבלוקציון ולהגנת הרשת.

Tx_Root זהו השורש של עץ מרקל שנבנה על ידי ביצוע hash על כל זוג טרנזקציות בבלוק. זוהי למעשה חותמת קצרה וייחודית של כל הטרנזקציות בבלוק. אמנם ניתן ליצור חותמת ייחודית של כל הטרנזקציות בבלוק על יד חישוב hash אחד על כל הטרנזקציות ביחד, אבל אם זה היה המצב, אזי על מנת לבדוק האם טרנזקציה עם מזהה מסוים נמצאת בבלוק היה נדרש לדעת את כל המזהים של כל הטרנזקציות גם כן. השימוש בעץ מרקל נועד לבצע אופטימיזציה בתהליך החיפוש של טרנזקציה מסוימת בבלוק, מבלי לדעת את כל שאר הטרנזקציות. בעזרת מבנה הנתונים הזה נצרך לדעת רק את ה hash של הטרנזקציות הנמצאות בנתיב משורש העץ עד לטרנזקציה שאנו מחפשים.

טרנזקציות

הטרנזקציות הן אבני הבניין לכל מערכת הביטקוין. טרנזקציה היא העברה של סכום ביטקוין אשר משודרת לרשת ונאספת לתוך בלוק. בהמשך, הבלוק יקושר לשרשרת הבלוקים לאחר שיכיל מספר מסוים של טרנזקציות ובמוצע כ 10 דקות. טרנזקציה מורכבת מקלט ופלט. הקלט של הטרנזקציה הוא פלטים של טרנזקציות קודמות, והפלט שלה הוא סכום המטבעות בקלט. הטרנזקציות אינן מוצפנות ולכן ניתן למצוא ולראות כל טרנזקציה שאי פעם נאספה לתוך בלוק בבלוקצ'יין. באופן כללי, ניתן לראות את כל הטרנזקציות בבלוקצ'יין בעזרת דפדפן בלוקצ'יין² אשר יודע להמיר את הטרנזקציה לפרטים קריאים ומובנים. היכולת הזאת מהווה את הבסיס ל**שגיאה! מקור ההפניה לא נמצא.** ולחשיפת המשתמשים שנראה בהמשך בהרחבה.

דוגמה לטרנזקציה והשדות החשובים שהיא מכילה ניתן לראות באיור 2 מתוך [2]:

```
Input:
Previous tx:
f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig:
304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c
6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160
404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

איור 2 - טרנזקציה עם קלט אחד

כפי שרואים באיור, טרנזקציות מחולקות לשני חלקים, קלט ופלט. בקלט מתואר מהיכן אני לוקח את המטבעות ובקלט לאן אני רוצה לשלוח אותם. בדוגמה זו, בקלט לוקחים 50 מטבעות מטרנזקציה קודמת בעלת מזהה f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6 ובפלט שולחים את כל המטבעות לכתובת³ 404371705fa9bd789a2fcd52d2c580b65d35549d

זוהי טרנזקציה פשוטה עם קלט אחד ופלט אחד אך לעיתים ישנם מספר קלטים בטרנזקציה, כאשר כל הסכום שלהם נסכם וכולו מנוצל בפלט של הטרנזקציה, ולעיתים, כפי שנראה בהמשך ישנם גם מספר פלטים.

² דוגמה ל blockchain explorer ניתן למצוא ב <https://www.blockchain.com/explorer>
³ הפורמט כאן הוא hexadecimal.

כאשר מייצרים טרנזקציה מצרפים אליה script. ה script זהו אוסף פעולות אשר נדרשות על מנת להשתמש במטבעות שבטרנזקציה. מנגנון זה מספק גמישות ויכולת לשנות את מה שנדרש בכדי להשתמש במטבעות שבטרנזקציה⁴. זוהי למעשה הדרך להבטיח שרק מי ששלחו אליו את המטבעות יוכל להשתמש בהם בהמשך. בדרך כלל נדרשים להציג חתימה של המפתח הפרטי התואם למפתח הציבורי אליו שולחים את המטבעות.

באיור רואים את שני החלקים של script סטנדרטי :
scriptSig זוהי החתימה⁵ על ידי המפתח הפרטי שלי והיא מספקת הוכחה שאני הבעלים של המפתח הפרטי התואם למפתח הציבורי (כתובת הביטקוין) הרשום בטרנזקציית ה input שבה אני רוצה להשתמש. ההפניה לטרנזקציית ה input הזו היא על ידי השדה previous tx שבאיור. זהו למעשה מצביע לטרנזקציה בבלוקציין אשר נשלחה לכתובת הציבורית שלי, ובה אני רוצה להשתמש כעת (בסכום שנשלח בה או בחלק ממנו).
scriptPubKey זוהי הכתובת (שהיא המפתח הציבורי) שאליה אני רוצה לשלוח את המטבעות בטרנזקציה זו. שדה זה מכיל את כתובת הביטקוין בפורמט המוכר לנו, בצורה מקודדת.

אם כן, בשלב הראשון אליס שלחה לבוב מטבעות. היא יצרה טרנזקציה עם מקורות קלט ופלט. במקור הפלט היא כתבה בשדה scriptPubKey את כתובת הביטקוין – המפתח הציבורי של בוב. כאשר בוב רוצה לשלוח הלאה את המטבעות לצ'רלי, הוא מייצר טרנזקציה, ובמקור הקלט שלו הוא מצביע על טרנזקציית הפלט של אליס בשדה previous tx. בנוסף הוא מציג את החתימה של המפתח הפרטי שלו בשדה scriptSig, כהוכחה שהוא הבעלים אשר אליו נשלחה הטרנזקציה הקודמת ולכן הוא רשאי להשתמש במטבעות שהוגדרו בה. במקור הפלט של הטרנזקציה שבו מייצר הוא כותב את הכתובת של צ'רלי בשדה scriptPubKey ובנוסף כותב את סכום המטבעות אשר רוצה לשלוח בשדה value. לאחר מכן הוא משדר את הטרנזקציה לרשת. בצורה זו יוכלו הכורים לאמת את הטרנזקציה ולהכניסה לבלוק.

גם בפלט יכולים להיות מספר מקורות אשר חולקים את סכום הביטקוין בקלט. כל פלט של טרנזקציה יכול להיות בשימוש רק פעם אחת ולכן כל הסכום חייב להישלח כדי לא להתבזבז. כך למשל אם הקלט שווה ל 50 מטבעות אבל רוצים לשלוח רק 25, אזי המערכת תיצור שני פלטים של 25 מטבעות כל אחד כאשר אחד יהיה שייך לכתובת היעד אליה רצינו לשלוח ואחד בחזרה לשלוח בתור עודף אשר הוא שולח לעצמו. כל סכום קלט שלא משתמשים בו נחשב כעמלה לכורים אשר יאמתו את הטרנזקציה, יכניסו אותה לבלוק על ידי הוכחת עבודה וישדרו את הבלוק לרשת. כאשר הבלוק ישודר לרשת ויאומת על ידי הצמתים, יוכל המקבל לראות שאכן

⁴ למשל אפשר לדרוש שני מפתחות פרטיים על מנת להשתמש לקיים את ה script.
⁵ החתימה זוהי חתימת Elliptic curve על הטרנזקציה.

כתובת הביטקוין שלו זוכתה בסכום שנשלח ומאותו הזמן יכול גם לשלוח את הביטקוין הלאה לכתובת אחרת.

באיור 3 ניתן לראות דוגמה לטרנזקציה המייצרת 2 פלטים המסודרים לפי אינדקסים. הפלט הראשון הוא הסכום שרוצים להעביר, והפלט השני הוא העודף החוזר לכתובת חדשה של השולח.

```
Input:
Previous tx:
325c9671dc2bb9e9481b4a1563d057e18df51321dce8c7d94b4a8bf7b2a6d69b
Index: 0
493046022100c5e80f170972f50bc7788b3db13d38558868ae4544227388f035c214
b9945be9022100e91bf1840e27cb1d78d9f8230d678a5be124d094f656db44b63763
4356e290000121032973cd63575a91d77cd586fc1b6294d04b1a93c2f0ef726ed25d
a95225edc4fa

Output:
Index: 0
Value: 2500000000
scriptPubKey: OP_DUP OP_HASH160
b3b7b5e6f37b4de1709d748aeb12576a0b82214d
OP_EQUALVERIFY OP_CHECKSIG

Index: 1
Value: 2500000000
scriptPubKey: OP_DUP OP_HASH160
c9571819a4612dc14300f4b908a074d1d55b57e3
OP_EQUALVERIFY OP_CHECKSIG
```

איור 3 - טרנזקציה עם מספר פלטים

ניתוח מקוון

כעת נסקור את 2 השיטות לחשיפת פעולות משתמשים ברשת הביטקוין, כפי שמובא ב [1]. אלו השיטות אשר נממש בפרויקט המעשי, ואת המימוש נתאר בפרק הבא.

השלב המקדים לשתי השיטות הינו עותק מקומי של הבלוקצ'יין הכולל את הבלוקים והטרנזקציות בתוכם. ההורדה נעשתה בעזרת תוכנת הארנק הרשמית של קהילת הביטקוין וביצוע סנכרון עם הרשת.

Web scraping

השיטה הראשונה הינה ניתוח on-line שנעזר ברשת האינטרנט ובמידע הציבורי באינטרנט בכדי למצוא כתובות ביטקוין שזלגו לרשת, ולאחר מכן מצליבה את המידע עם העותק המקומי של הבלוקצ'יין. שיטה זו מתבססת על העובדה שישנה גישה לכל המידע באינטרנט הכולל אתרי אינטרנט, פורומים, אתרי תרומות ורשתות חברתיות ובהם ניתן למצוא כתובות ביטקוין אשר פורסמו בכוונה או שלא בכוונה. כתוצאה מכך נוכל לשייך משתמש אמיתי⁶ לכתובת ציבורית. לדוגמה, אנשים אשר כתבו מדריכים בנושא הביטקוין ומשאירים את הכתובת שלהם מתוך כוונה לקבל טיפ. הם מעודדים את הקוראים שלהם לשלוח להם ביטקוין. כך ניתן לקשר בקלות בין המידע של המשתמש לבין הטרנזקציות בבלוקצ'יין.

באזור 4 מתוך המאמר, ניתן לראות דוגמה למשתמש אשר מבקש עזרה טכנית בפורום ביטקוין, ובטעות רושם את כתובת הביטקוין שלו.

altoid
Member

Activity: 48



Ignore



help with Bitcoin development in php (variable parameters)

April 25, 2011, 02:17:14 AM

Hi all, I have run into some trouble using the bitcoin api with php. When I issue a command like:

```
$bitcoin->sendfrom($userid, $receiving_address, $amount);
```

I get an error like:

```
fopen(http://...@localhost:8332/): failed to open stream: HTTP request failed! HTTP/1.1 500 Internal Server Error
```

But when I hard code in the parameters:

```
$bitcoin->sendfrom("1", "1LDNLreKJ6GawBHPgB5yfVLBERi8g3SbQS", 10);
```

איור 4 - כתובת ביטקוין נחשפת בשוגג על ידי משתמש

כפי שרואים באיור, כאשר מוצאים כתובת כזו בהקשר כזה, ניתן לשייך את הכתובת 1LDNLre.. למשתמש altoid. כפי שהזכרנו, שם זה יכול להיות אמיתי או כינוי לאותו משתמש. במקרה זה, המשתמש האמיתי היה Ross Ulbricht אשר הפעיל את

⁶ שם אמיתי יכול להיות השם האישי או שם משתמש מפורום או אתר אינטרנט.

אתר Silk Road למכירת סמים. ה-FBI אשר חיפשו אחריו בגין פעולות בלתי חוקיות שביצע, הגיעו אליו בעזרת המידע שפרסם בטעות כגון זו שראינו באיור.

לשם ביצוע שלב זה ביצעתי חיפוש של כתובות ביטקוין ברשת החברתית פייסבוק. חיפשתי קבוצות בנושאי ביטקוין ומטבעות קריפטוגרפים, ועברתי על הודעות של חברי הקבוצה במטרה למצוא כתובות ביטקוין שפורסמו. בנוסף נעזרתי בחיפוש המובנה בפייסבוק כדי לחפש את המילים "כתובת" ו"תרומה" מתוך כוונה למצוא חברים אשר מבקשים לגייס תרומה עבור מיזם כלשהו ומפרסמים את הכתובות שאליה הם מבקשים שישלחו את התרומה בביטקוין.

להפתעתי, ובהתאם למתואר במאמר, מצאתי לא מעט הודעות בהן חברים כותבים את כתובת הארנק שלהם בפומבי. סוגי ההודעות היו, כאמור, בקשה לגיוס תרומות לכתובות מסוימות, בקשה לקבל טיפ עבור כתיבת מדריך בנושא הביטקוין וכדומה.

בשלב הבא נשתמש בכתובת זו בכדי לבצע חיפוש בתוכנה שכתבנו, מתוך כוונה למצוא טרנזקציות המשויכות אליה. כך נוכל לדעת איזו כתובת שלחה לה מטבעות, כמה ומתי. בהמשך נוכל לבצע חיפוש נוסף עבור הכתובת השולחת וכן הלאה.

אם כן, בשיטה זו רואים שניתן לחפש ולמצוא באינטרנט מספר רב של מפתחות ציבוריים המשויכים למשתמשים מסוימים. מידע זה משמש כקלט בחיפוש הטרנזקציות בבלוקצ'יין המקומי שהורדנו. מציאת הטרנזקציות המקושרות לכתובת זו נותנת לנו מידע נוסף כגון עם מי משתמש זה התקשר ומתי, ויכולת להמשך החיפוש עבור כתובת המקור.

השיטה השנייה המוזכרת ב [1] מתמקדת ביכולת להתאים בין משתמשים לטרנזקציות על ידי מידע חלקי. מידע חלקי על טרנזקציה יכול להיות הסכום שלה, הזמן שנשלחה וכדומה. מידע חלקי יכול להיות "שלחתי לך 100 ביטקוין אתמול בצהריים". בהינתן מידע שכזה, מייצרים טרנזקציות מועמדות להיות אלו של המשתמש, בסבירות מסוימת. תוקף יכול להשיג מידע חלקי שכזה על ידי 'שמיעה במקרה' ממשמש מוכר וידוע. למשל להאזין לבוב שאומר לאליס שלחתי לך סכום כזה וכזה בביטקוין בזמן מסוים.

בשיטה זו לוקחים מידע מעורפל לגבי זמן הטרנזקציה וסכום הביטקוין שנשלח בה ומנסים למצוא את הטרנזקציה המקורית בבלוקצ'יין. למשל, נניח שתנודת ערך הביטקוין אל מול הדולר לא עלתה על דולר אחד⁷, ושזמן הצהריים המדובר מדויק ל 5 דקות. כעת ישנן מספר טרנזקציות מועמדות לבדיקה, והן כל הטרנזקציות שקרו בחלונות [11: 55 AM, 12: 05 PM] ו [99,\$101]\$. ניתן אף לבצע הכללה לדוגמא הנ"ל ולבדוק עבור חלונות בעלי מסגרת של 15 דקות ו 10 דולר, ולהראות כיצד כמות הטרנזקציות המועמדות עולה באופן ניכר. בדוגמא של בוב ואליס, הראו כותבי המאמר שניתן להגיע בהסתברות של 1/10 למפתח הציבורי שלו, בהנחה שהשיחה התקיימה בחודש מרץ 2012.

לשם מימוש שיטה זו בפרויקט, כתבתי ממשק משתמש המאפשר לקבל קלט עבור חיפוש טרנזקציה עם הפרמטרים של תאריך, שעה וסכום, וטווח החיפוש עבור הסכום והשעה. בהינתן קלט זה, יתבצע חיפוש בעותק הבלוקצ'יין המקומי, וישלפו ממנו רק אותן הטרנזקציות העונות על הפרמטרים של החיפוש. על מנת לבצע זאת נקרא את הטרנזקציות מהבלוקים, ועבור כל טרנזקציה נקרא את המאפיינים שלה כגון הזמן והכמות, נשווה אל מול מאפייני החיפוש ונחזיר רק את אלו העונות על הקריטריונים. החיפוש יוכל להתבצע בקלות פעמים נוספות, עם שינויים קלים בקלט, על מנת לבצע חיפוש גמיש ומדויק ולראות כיצד טווחי הקלט משפעים על גודל הפלט. גם בשיטה זו תינתן אפשרות לראות מידע מורחב עבור כל טרנזקציה שנמצאה בחיפוש, ואף לבצע חיפוש המשך עבור הכתובת המשויכת אליה.

⁷ ההמרה מביטקוין לדולר יכולה להיעשות לפי אתר blockchain.info ואחרים.

מימוש הפרויקט

בפרויקט המעשי מימשי חיפוש טרנזקציות בבלוקצ'יין והצגת המידע שנמצא. הרעיון הוא לעבוד עם המידע הגולמי ביותר – הבלוקצ'יין – בצורה לוקאלית, לממש אותו עם אובייקטים של שפת תוכנה כגון מחלקות Blockchain ו Transaction ולממש חיפושים לפי פרמטרים מסוימים, להציג את התוצאות בצורה מפורטת ומובנת ואפילו לאפשר לנווט בין הטרנזקציות.

כאמור בפרק הקודם, מימשי שני סוגי חיפושים. האחד הינו חיפוש מדויק עבור טרנזקציות אשר נשלחו לכתובת מסוימת אותה חשפתי באינטרנט. החיפוש אותו בחנתי היה חיפוש אחר טרנזקציות של משתמש אשר חשף את כתובת הביטקוין שלו בפייסבוק. תוצאות החיפוש הראו את כל פרטי הטרנזקציה שתואר המשתמש באינטרנט, ונתנו לנו מידע נוסף על הישות אשר שלחה את הטרנזקציה למשתמש אשר עליו התבצע החיפוש.

סוג החיפוש השני הינו חיפוש של כל הטרנזקציות העונות על פרמטרים מסוימים כגון תאריך, שעה וסכום, עם טווח שגיאה כלשהו שאף הוא פרמטר בחיפוש. כאשר נמצאו טרנזקציות לכל אחד מסוגי החיפוש, מוצגים נתונים מתוך האובייקט של הטרנזקציה כמו גם מאובייקט הבלוק שבו נמצאה.

תכולת עבודה

1. הורדת הבלוקצ'יין
2. parsing וטעינת הבלוקים.
3. עבור כל בלוק, מעבר על כל הטרנזקציות והשוואה לפרמטרים שבחיפוש.
4. הצגת מידע מורחב אודות הטרנזקציות שנמצאו.
5. במידת הצורך המשך החיפוש עם הכתובות שנמצאו בחיפוש.

סביבת פיתוח וכלי עבודה

סביבת התכנות בה השתמשתי היא IntelliJ. זוהי סביבת עבודה לפיתוח קוד ב Java ו Android. השתמשתי בגרסת Community מספר 2019.3.3. זוהי סביבת קוד פתוח אשר מציעה יכולות נוחות להוספת ספריות צד שלישי, ניהול קוד ו debugging.

בסביבה זו יצרתי פרויקט מסוג Java FX. זוהי פלטפורמה קוד פתוח לפיתוח תוכנות צד לקוח ל Desktop ו Mobile, על גבי Java. פלטפורמה זו מאפשרת יצירת UI נוח הכולל את כל רכיבי המשתמש כגון חלונות, רשימות וכפתורים. בנוסף ישנה אפשרות לסדר את הרכיבים באופנים שונים על המסך כגון לאורך לרוחב או בצורה של grid.

לפרויקט הוספתי את ספריית Bitcoinj. ספריית זו הינה ספרייה לעבודה עם פרוטוקול הביטקוין.

היכולות המרכזיות של הספרייה :

- יכולת לשלוח ולקבל טרנזקציות מבלי להוריד את כל הבלוקצייין.
- יכולת ניהול ארנק עם הצפנת המידע, עדכון והצגת מאזן המטבעות.
- ממשק משתמש פשוט עבור תצוגת הארנק, הכולל את היסטורית הטרנזקציות.

Data set

הורדת הבלוקצייין נעשתה בעזרת תוכנת Bitcoin core. לאחר סנכרון התוכנה, הורדת מעל 200 גיגה זיכרון אל המחשב ואינדוקס של כל קבצי הבלוקים – ניתן היה להשתמש בכל אחד מהקבצים. הקבצים הינם בעלי סיומת dat, ומכילים מספר כלשהו של בלוקים בתוכם.

על מנת לבצע parsing של הקבצים למידע אשר ניתן לקרוא ולהבין אותו, השתמשתי בספריית BitcoinJ⁸. זוהי ספרייה אשר נועדה לעבוד עם פרוטוקול הביטקוין. בין שאר היכולות שלה ניתן למצוא את האפשרויות לנהל ארנק לייט ולשלוח ולקבל טרנזקציות. ספרייה זו קראה את קבצי הבלוקצייין והמירה אותם לבלוקים המכילים טרנזקציות, וכך ניתן היה לעבור על כל הטרנזקציות ולבדוק אותן כנגד הפרמטרים של החיפוש.

ארכיטקטורה

ספריית BitcoinJ אחראית על טעינת קבצי הבלוקצייין והמרתם לאובייקטים המייצגים את פרוטוקול הביטקוין. זהו למעשה מימוש על הקונספט המופשט של הפרוטוקול על ידי Object Oriented Programming. להלן נתאר את המחלקות העיקריות במימוש ספציפי זה.

BlockChain

זהו מימוש של מצב SPV – simplified payment verification של פרוטוקול הביטקוין. מימוש זה מתאים לתוכנות הרצות עם משאבים מצומצמים כגון מכשירים ניידים. במצב זה לא נשמרים כל הבלוקים לדיסק.

⁸ <https://bitcoinj.github.io/>

מחלקה זו מחזיקה סדרה של בלוקים המקושרים ביניהם ויודעת לאמת שהם מקושרים ביניהם לפי חוקי הרשת. האימות מתבצע על ה headers בלבד ולא על התוכן של הבלוק, ז"א לא מאומתות חתימות הטרנזקציות.

מחלקה זו מכילה משתנה BlockStore שהוא אחראי לשמירת הבלוקים לדיסק. זהו Map המשייך בין Hash של ה headers של הבלוקים לאובייקטים של הבלוקים.

Block

בלוק מכיל רשימה של טרנזקציות, ובנוסף מספר משתנים אשר מקשרים אותו למקום המוחלט שלו בשרשרת הבלוקים, ומוכיחים שנעשתה הוכחת עבודה על התוכן שלו.

מחלקה זו מכילה את המשתנים הבאים:

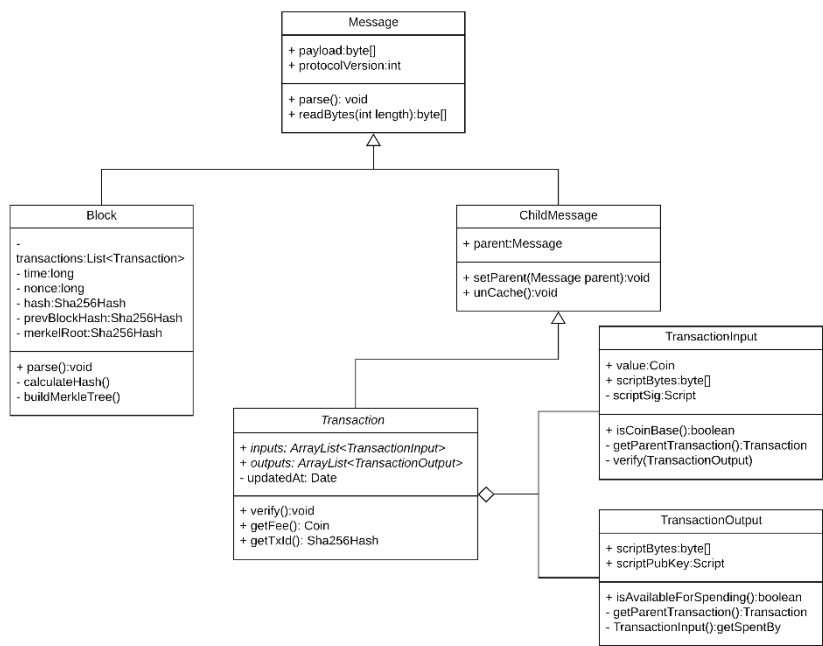
Sha256Hash של הבלוק הקודם, של שורש עץ מרקל המורכב מכל הטרנזקציות בבלוק, ושל הבלוק עצמו.
Long של הזמן שבו נוצר ושל ה nonce.

Transaction

טרנזקציות הן אבני היסוד של פרוטוקול הביטקוין. הן מייצגות דרישה של סכום מסוים, ואת התנאים הנדרשים בכדי שהסכום הנוכחי יפדה בהמשך. מחלקה זו מאפשרת serialization של טרנזקציות כמו גם בניה שלהן ובדיקת תקינותן. בנוסף המחלקה מאפשרת לעקוב אחר מידע נוסף אודות הטרנזקציה כגון באיזה בלוקים היא נמצאה, ומהי מידת הביטחון שלא ישתמשו בטרנזקציה זו בשנית?⁹

את דיאגרמת המחלקות ניתן לראות באיור 5

⁹ דבר זה יכול לקרות במתקפת הבזבז הכפול.



איור 5 - דיאגרמת המחלקות של ספריית BitcoinJ

קלט ופלט

מקור הקלט ההכרחי והחשוב ביותר הינו קובץ המכיל בלוקים של הבלוקצ'יין. לא ניתן לבצע כל פעולה ללא קלט זה, והודעת שגיאה תינתן במקרה שכזה. כבר בשלב זה נוכל להריץ את התוכנה על מנת לספור את הבלוקים ואת סך כל הטרנזקציות בבלוקים. בנוסף נוכל לראות את המידע אודות הבלוקים והטרנזקציות כגון תאריכים ומזהים אחרים בבלוקצ'יין כגון ה Hash של שורש עץ המרקל. עבור הטרנזקציות נוכל לראות את מקורות הקלט והפלט שלהן כמו גם נתונים נוספים אודות הפרוטוקול. נוכל להוסיף עוד קלט שהוא נתונים עבור חיפוש עם סינון, כגון כתובת מסוימת או טווח תאריכים או ערכים של טרנזקציות. הפלט עבור קלט זה יהיה כל הטרנזקציות התואמות את מאפייני החיפוש שהוכנסו.

על מנת לבצע חיפוש מקורי הייתי צריך להשתמש בכתובת ביטקוין ללא ידע מוקדם לגבי טרנזקציות שביצעה כגון זמנים מסוימים או כמות מטבעות מסוימת. דרישה נוספת היא היכולת למצוא את הכתובת באופן לגיטימי וחופשי ברשת. זהו למעשה חיפוש של תוקף אשר רוצה לחפש מידע על כתובת מסוימת ולחשוף את פעולות המשתמש כגון למי שלח ומתי, ממי קיבל וכדומה.

כפי שמובא במאמרים שסקרתי, ובפרט ב [1], פורומים לענייני ביטקוין הם מקור שכיח למקרים בהם משתמשים חושפים את כתובת הביטקוין שלהם. בהמשך לכך, חיפשתי בפייסבוק קבוצות העוסקות ודנות בענייני ביטקוין. מצאתי מספר קבוצות ובחרתי את הגדולה מבניהן. כיוון שקבוצה זו הייתה קבוצה סגורה, ותוכן התכתובות היה גלוי רק לחבריה, ביקשתי להצטרף לקבוצה וכך יכולתי לראות את כל היסטוריית ההודעות בקבוצה. חיפוש קצר אשר נפרש על תקופת זמן לא ארוכה הניב מספר ההודעות שהכילו כתובת ביטקוין. לדוגמה, משתמשים וותיקים, כנראה ממנהלי הקבוצה, אשר רצו לעודד את השימוש בביטקוין בקרב משתמשים חדשים בכלל ובקרב בנות בפרט, הודיעו שכל מי שהוא חדש בתחום הביטקוין מוזמן לקבל תשלום סמלי בביטקוין בתור התנסות ראשונית ובכדי ללמוד כיצד לשלוח ולקבל מטבעות. כל מה שהיה נדרש מהמשתמשים החדשים הוא לפתוח ארנק ולכתוב את כתובת הארנק כדי שלשם יעבירו את הביטקוין. התגובות לביטקוין בחינם, אם כי מדובר היה בסכום קטן מאוד, היו רבות וכולן כללו את כתובות המשתמשים. מתוך רשימת הכתובות בחרתי אחת ובה השתמשתי כפרמטר בחיפוש.

את הכתובת שזלגה לרשת הפייסבוק ועבורה חיפשתי טרנזקציות בבלוקצ'יין ניתן לראות באיור 6:

ביטקוין ישראלי
August 16, 2017 at 12:29 AM · 🌐

ג'רל פאוור! ביטקוין במתנה לנשים: הדגמה חיה ואינטראקטיבית לכל מי שעוד לא התעסקה עם ביטקוין: אם את מתעניינת בביטקוין אך עוד לא החזקת ביטקוין ביד – את מוזמנת לפתוח בחינם ארנק... ביטקוין ולהדביק בתגובה את הכתו...

👍❤️😲 225

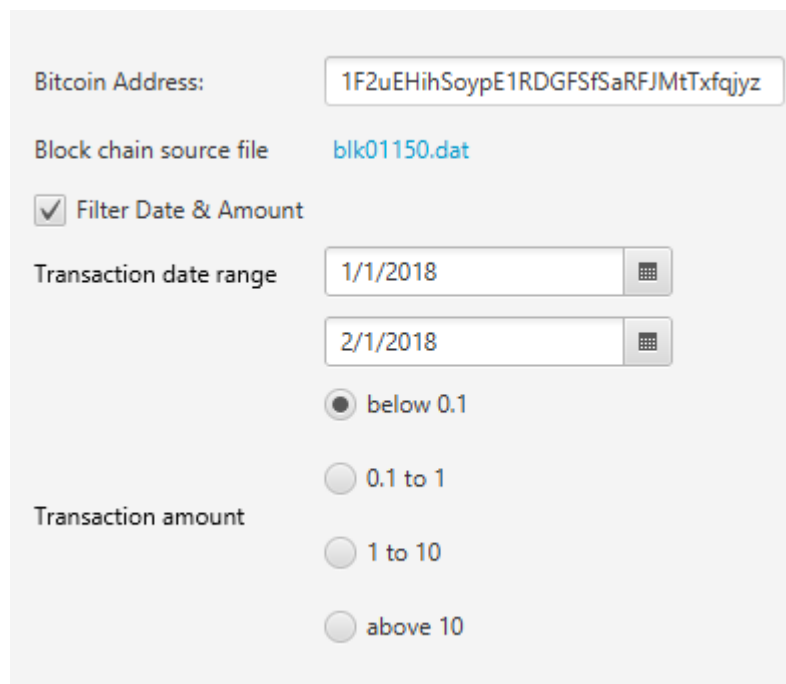
798 Comments 35 Shares

1F2uEHihSoypE1RDGFSfSaRFJMtXfqjyz

איור 6- זליגת כתובת משתמש ברשת הפייסבוק

באיור רואים כיצד משתמש תמים מפרסם את כתובת הארנק שלו על מנת לקבל סכום ביטקוין סמלי בחינם. כאמור זוהי דוגמה אחת מני רבות. רק להודעה זו היו מעל 10 כתובות שפורסמו, ובחיפוש פשוט ניתן למצוא עוד דוגמאות רבות.

תוכנת החיפוש שכתבתי מאפשרת להזין פרמטרים עבור החיפוש הכוללים כמובן את הכתובת עבורה נחפש טרנזקציות ובנוסף פילטרים לחיפוש כגון סכום הטרנזקציה והתאריך שבו התבצעה. בממשק זה הזנתי את הכתובת שמצאתי בפייסבוק כמו גם תאריכים התואמים לתקופה זה התפרסמה ההודעה בפייסבוק. את כלל הפרמטרים ויכולות החיפוש ניתן לראות באיור 7:



איור 7- פרמטרים לחיפוש טרנזקציות בבלוקצ'יין

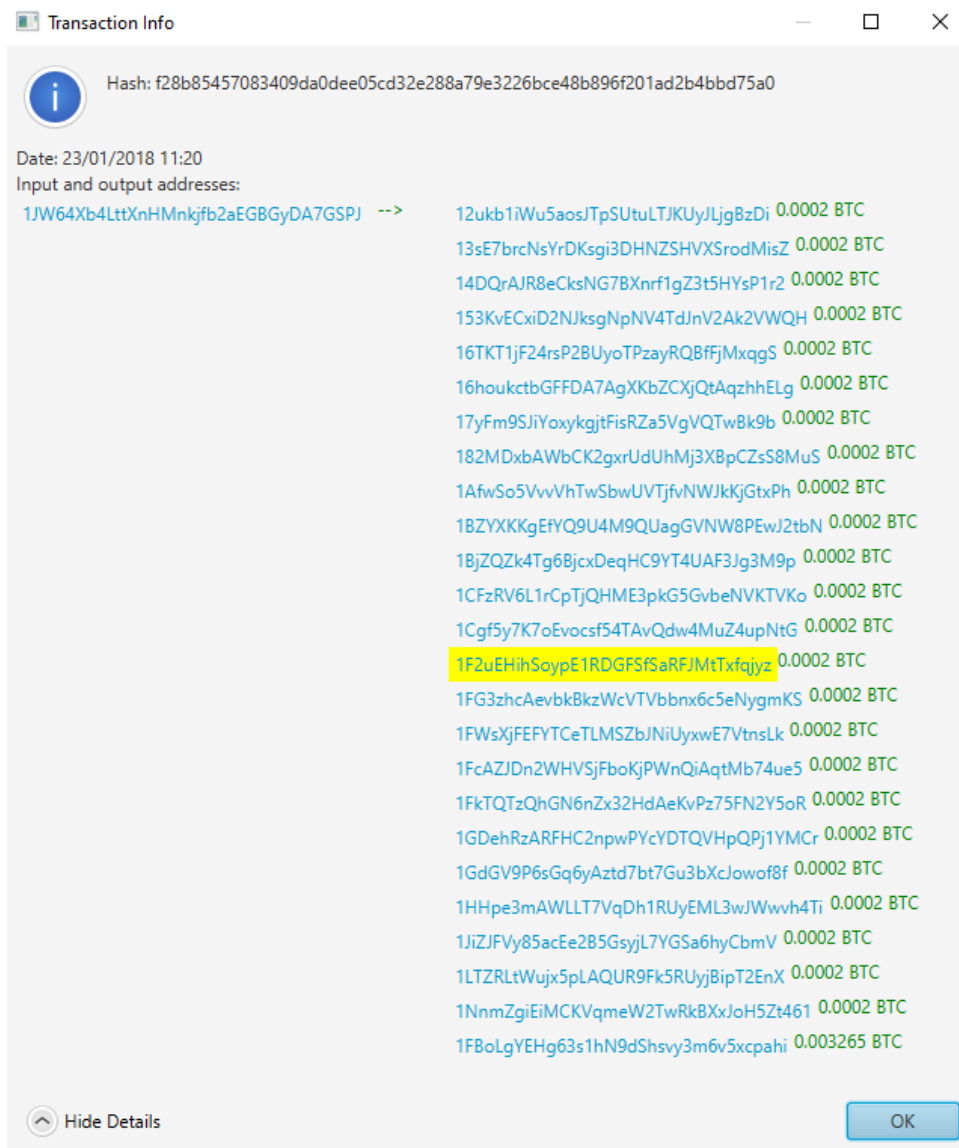
בעת לחיצה על הכפתור "Search in Blockchain" מתחיל תהליך טעינת הבלוקים מתוך הקובץ ומעבר על הטרנזקציות שבתוך הבלוקים בכדי לחפש התאמה לפרמטרים שהוגדרו בחיפוש. את מהלך החיפוש ומעבר על כל הטרנזקציות בבלוקים ניתן לראות באיור 8:

```
Block details:
Block time: 2018-01-23
Block Hash: 0000000000000000000000001635c2b1ebb05dae50a507d2063bb9327dd90eccd966c59
Total block scanned: 38

Transaction Details:
Transaction ID: b7cc4ea4e2a1f32ef59567a5e91c5c24306ce5ec3bc17efe5712c26dc875732f
Block Hash: Thu Jan 01 02:00:00 IST 1970
Total transaction scanned: 45958
```

איור 8- מהלך החיפוש הטרנזקציות בבלוקים

כאשר נמצאת התאמה בחיפוש, זאת אומרת שנמצאה טרנזקציה אשר אחד ממקורות הפלט שלה הכיל את כתובת היעד של החיפוש, אוספים את כל המידע הרלוונטי על מנת להבין את המקור ממנו הגיעו המטבעות ומציגים אותו ב UI, תוך מתן אפשרות נוחה להמשיך ולבצע חיפוש המשך עבור הכתובות המעניינות. את תוצאת החיפוש והמידע הנוסף ניתן לראות באיור 9:



איור 9 - תוצאת החיפוש.

באיור רואים את פרטי הטרנזקציה שנמצאה בחיפוש. בטרנזקציה זו היה מקור קלט אחד, ומספר מקורות פלט – זאת אומרת שבטרנזקציה אחת מבצע הטרנזקציה שלח מטבעות למספר רב של אנשים בו זמנית. דבר זה תואם למה שפרסם המשתמש בפייסבוק שכל מי שמעוניין ישלח את כתובת הביטקוין שלו ויקבל סכום קטן בכדי להתנסות בפלטפורמה, ושאכן מספר רב של אנשים פרסמו את הכתובת שלהם.

הכתובת שאותה חיפשנו, 1F2uEHihSoypE1RDGFSfSaRFJMtTxfqjyz, הינה רק אחת ממקורות הפלט של אותה טרנזקציה, והיא מודגשת בצהוב. הפרטים הנוספים שהסקנו מתוצאת החיפוש הם כתובת המקור אשר שלח את הטרנזקציה - 1JW64Xb4LttXnHMnkjfb2aEGBGyDA7GSPJ, התאריך בו הטרנזקציה נשלחה – 23 לינואר 2018, וכמות המטבעות שנשלחה – 0.0002 ביטקוין. בנוסף ניתן להסיק שכתובת הביטקוין במקור הפלט האחרון – 1FBoLgYEHg63s1hN9dShsvy3m6v5xcpahi הינה הכתובת אליה נשלח העודף מהסכום שהיה במקור הקלט, ושהוא שייך למשתמש אשר שלח את הטרנזקציה 1JW64Xb4LttXnHMnkjfb2aEGBGyDA7GSPJ. שהוא בעל כתובת הביטקוין

מגבלות התוכנה

כפי שכתבנו בעבודה המסכמת גודל הבלוקצין הינו עצום. כאמור, כל הטרנזקציות מאז הקמת והפעלת הרשת נשמרות בו, ללא כל אפשרות למחוק אפילו טרנזקציה אחת. נכון לזמן כתיבת העבודה גודל הבלוקצין הינו 250 גיגה בייט. נכון להיום כמות זו דורשת דיסק גדול במיוחד על מנת לשמור את כולו, וללא ספק אינו מתאים לטלפון חכם או מחשב נייד. אם כן בתוכנה הורדתי מספר קבצים המכילים כמות מצומצמת יחסית של בלוקים ובכל בלוק מספר טרנזקציות כלשהו.

אתגרים

האתגרים היו למצוא דרך להוריד רק חלק מהבלוקצין באופן שבו ניתן יהיה לקרוא את הבלוקים והטרנזקציות מבלי לפגוע בשלמותם. חיפוש משתמשים אשר חשפו את כתובת הביטקוין שלהם היה פשוט יחסית כיוון שלפייסבוק יש חיפוש מובנה באפליקציה וכל חיפוש בקבוצת הביטקוין עם מילות החיפוש 'תרומה' או 'כתובת' הניב תוצאות. עבור הכתובת שבחרתי חיפשתי בכעשרה קבצים של בלוקים עד שהגעתי לתאריך המקורב לזה שבו התפרסמה ההודעה בפייסבוק. עבור קובץ זה סרקתי 41 בלוקים ו 46,451 טרנזקציות עד שנמצאה הטרנזקציה. בחיפוש אחר טרנזקציות עם מאפיינים מסוימים בחרתי קובץ בלוקים אחר ובו סרקתי 118 בלוקים ומצאתי 2484 טרנזקציות העונות על מאפייני החיפוש. כל סריקה התבצעה בממוצע כמה שניות.

תוצאות ומסקנות

בעבודה זו ראינו בפועל כיצד ניתן להוריד את הבלוקצ'יין ולקרוא את היסטוריית הטרנזקציות שבו. ראינו את פרטי הטרנזקציה ופרטי הבלוק וממה הם מורכבים. ראינו דוגמאות של טרנזקציות עם מספרים שונים של מקורות קלט ופלט. בנוסף ראינו כיצד מתבצע חיפוש של טרנזקציות התואמות לכתובות ביטקוין מסוימת כמו גם תוצאות המסננות טרנזקציות לפי פרמטרים מסוימים כגון כל הטרנזקציות אשר התבצעו בתאריך כלשהו בטווח דקות כלשהו ועם סכום מטבעות כלשהו.

Bibliography

- [1] M. S. K. S. P. Michael Fleder, "Bitcoin Transaction Graph Analysis," *CoRR abs/1502.01657*, 2015.
- [2] "<https://en.bitcoin.it/wiki/Transaction>," [Online].
- [3] S. K. E. C. L. a. S. R. M. Conti, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.
- [4] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," <http://www.bitcoin.org/bitcoin.pdf>, 2009.
- [5] A. S. Dorit Ron, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *Financial Cryptography : 6-24*, 2013.
- [6] K. Krombholz, A. Judmayer, M. Gusenbauer and E. Weippl, "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy," *Financial Cryptography and Data Security*, pp. 555-580, 2016.
- [7] Y. Liu, X. Liu, C. Tang, J. Wang and L. Zhang, "Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin," *IEEE Access 6: 23261-23270*, 2018.
- [8] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," *arXiv preprint arXiv:1410.6079*, 2014.
- [9] A. Gervais, . G. O. Karame, D. Gruber and S. Capkun, "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients," *proceed. of ACSAC*, pp. 326-335, 2014.
- [10] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," *in Proceed. of PASSAT/SocialCom, IEEE Third International Conference on Social Computing (SocialCom), Boston, MA, USA*, 2011.
- [11] Q. ShenTu and J. Yu, "Research on Anonymization and De-anonymization in the Bitcoin System," *CoRR abs/1510.07782*, 2015.
- [12] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in bitcoin," *Proceed of. 2nd Workshop Bitcoin Res.*, pp. 127-141, 2015.
- [13] A. Gervais, . G. O. Karame, D. Gruber and S. Čapkun, "Gervais_ACSAC2014_Slides.key," [Online]. Available: https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2014/acsac_gervais_slides.pdf.