ביטקוין: מערכת אלקטרונית לתשלומים ישירים (עמית לעמית)

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org
Translated in Hebrew from bitcoin.org/bitcoin.pdf
by Zeev Shilor

תקציר. מערכת מושלמת של גירסה של כסף אלקטרוני תאפשר העברה ישירה בין פרט אחד למשנהו ללא תיווך של מוסד פיננסי. חתימות דיגיטליות מספקות חלק מהפתרון אך התועלות העיקריות מוחמצות אם עדיין נדרש צד שלישי כדי למנוע הוצאה כפולה. אנו מציעים פתרון לבעית ההוצאה הכפולה דרך שימוש ברשת להעברה ישירה בין הצדדים. חותמות הזמן של עסקות הרשת עם המוצפנות ב"האשינג" לשרשרת מתמשכת של הוכחות עבודה, יוצרות תיעוד אשר אינו ניתן לשינוי ללא ביצוע מחדש של העבודה. השרשרת הארוכה ביותר לא רק משמשת כעדות לרצף האירועים שקרו, אלא גם שההוכחה הגיעה מהמאגר הגדול ביותר של כח המיחשוב (CPU). כל עוד מרבית כח המיחשוב נשלט ע"י צמתות אשר אינן מתאגדות לתקוף את הרשת, הן ייצרו את השרשרת הארוכה ביותר ויגברו על התוקפים. הרשת עצמה צורכת ארגון מינימלי. הודעות משוגרות על בסיס המאמץ המוצלח ביותר, וצמתות הרשת יכולות להתחבר ולהתנתק כרצונן, תוך קבלת שרשרת הוכחת העבודה הארוכה .ביותר כהוכחה למה שאירע ברשת בעת שהיו מנותקות.

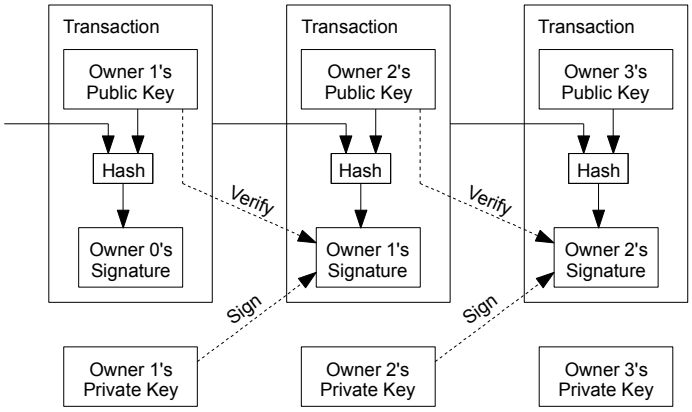
1. הקדמה

מסחר באינטרנט הגיע למצב בו נשען כמעט לגמרי על מוסדות פיננסים המשמשים כנאמן צד שלישי כדי לעבד תשלומים אלקטרונים. אמנם המערכת עובדת היטב עבור מרבית העסקות, אך היא עדיין סובלת מהחולשה המובנה של מודל מבוסס אמון. אין אפשרות אמיתית לעסקות ללא חזרה, כיון שהמוסדות אינם יכולים להמנע מהצורך לגשר בין מחלוקות. עלות התווך מעלה את עלויות העסקה, מה שמגביל באופן פרקטי את מינימום גובה עסקה ומנטרל את העסקות היומיומיות הזעירות, ויש גם עלות נרחבת יותר בחוסר היכולת לבצע תשלומים ללא חזרה לשרותים שלא ניתן לבטלם לאחר שהתבצעו. עם האפשרות להתחרטות, הצורך בשרותי אמון מתרחב. סוחרים צריכים להיות חשדנים לגבי לקוחותיהם ולהטריחם בדרישות מידע אשר במצב אחר לא היה נדרש. יש אחוז מסוים של הונאות אשר נתפס כבלתי ניתן למניעה. עלויות אלו ועלויות כתוצאה מחוסר ודאות ניתנות למניעה באופן ישיר בעת השימוש בכסף מזומן פיזי. אך אין מנגנון שמאפשר תשלומים כאלה דרך ערוץ תקשורת ללא אמון.

מה שנחוץ הוא מערכת תשלומים אלקטרונית המבוססת על הוכחה קריפטוגרפית במקום מערכת מבוססת אמון, המאפשרת לכל שני צדדים שרוצים בכך, לבצע עסקות ישירות האחד עם השני ללא הצורך במעורבות נאמן צד שלישי. עסקות שחישובית אין אפשרות פרקטית להחזירן לאחור תבטחנה את המוכרים מהונאה, ומנגנוני נאמנות שוטפים יכולים להיות מיושמים בקלות לצורך הגנת הקונים. במאמר זה אנו מציעים פתרון לבעית ההוצאה הכפולה בעזרת שימוש בשרת חתימות זמן מבוזר להתקשרות ישירה המייצר הוכחה חישובית של הסדר הכרונולוגי של עסקות. המערכת הנה מאובטחת כל עוד מכלול הצמתות ההוגנות שולט בכח המיחשוב שגבוה יותר משל קבוצה כלשהי שאולי תחבור כדי לתקוף את הרשת.

2. עסקות

אנו מגדירים מטבע אלקטרוני כשרשרת של חתימות דיגיטליות. כל בעלים מעביר את המטבע לבא בתור בעזרת חתימה דיגיטלית של הצפנת ההאש של העסקה הקודמת והמפתח הציבורי של הבעלים הבא, והוספתם בסוף המטבע. המקבל יכול לאמת את החתימות כדי לודא את שרשרת הבעלות.

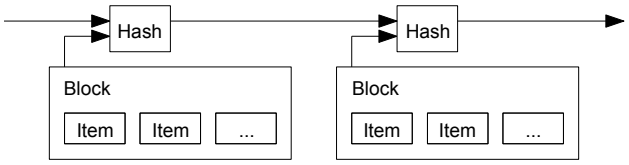


הבעיה היא כמובן בכך שהמקבל אינו יכול לודא שאחד מהבעלים הקודמים לא ביצע הוצאה כפולה של המטבע. הפתרון המקובל הוא לשלב רשות מרכזית נאמנה, או מטבעה, שתבדוק כל עסקה אם כבר הוצאה. אחרי כל עסקה, המטבע צריך לחזור למטבעה כדי ליצור מטבע חדש, ורק מטבעות אשר יוצרו ישירות על ידי המטבעה ניתן לסמוך עליהם שלא הוצאו פעמיים. הבעיה בפתרון זה היא שגורל כל המערכת הכספית תלוי בחברה שמבצעת את ההטבעה, כאשר כל עסקה עוברת דרכה בדיוק כמו בנק.

אנו זקוקים לאפשר למקבל לדעת שהבעלים הקודמים לא חתמו כבר על שום עסקה קודמת. מבחינתנו, העסקה המוקדמת ביותר היא הקובעת, כך שלא אכפת לנו מנסיונות מאוחרים יותר של הוצאה כפולה. הדרך היחידה שמבטיחה שאין עסקה קודמת היא לדעת על כל העסקות כולן. במודל מבוסס הטבעה, המטביע מכיר את כל העסקות ויכול להחליט מי היתה ראשונה. כדי להשיג זאת ללא צד שלישי, העסקות צריכות להיות מפורסמות לציבור [1], וצריך מערכת המאפשרת למשתתפיה להסכים על היסטוריה יחידה של הסדר בו העסקות התקבלו. המקבל צריך הוכחה שבעת שנכנסה העסקה, רוב הצמתות הסכימו שזו היתה הראשונה שהתקבלה.

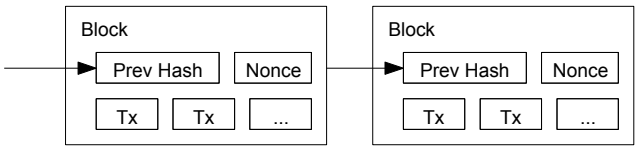
3. שרת חותמת זמן

הפתרון המוצע מתחיל בשרת חותמת הזמן. שרת חותמת זמן עובד ע"י לקיחת ההאש של בלוק של פריטים שיש להחתימם בזמן, ופרסום לציבור הרחב של ההאש, בדומה לעתון או בפוסט של יוזנט [2-5]. חותמת הזמן מוכיחה שמובן מאליו שהנתונים היו קיימים בעת החתימה כדי להכלל בהאש. כל חותמת זמן כוללת בהאש שלה את חותמת הזמן הקודמת, מה שיוצר שרשרת בה כל חותמת זמן נוספת מבססת את אלו שקדמו לה.



4. הוכחת עבודה

כדי לממש שרת מבוזר של חותמת זמן במערכת מבוססת עסקות ישירות, נצטרך מנגנון הוכחת עבודה הדומה לזה של ההאשקאש של אדם בק [6], ולא של עתון או פרסומי יוזנט. הוכחת העבודה כרוכה בחיפוש ערך אשר אם הוצפן האש, כמו למשל ב SHA-256 ההאש מתחיל במספר ביטים (סיביות) עם הערך 0. העבודה הממוצעת הנדרשת הנה בסדר גודל מעריכי של מספר האפסים הנדרש וניתן לאמת אותה בעזרת ביצוע האש יחיד. ברשת חותמת הזמן שלנו אנו מממשים את הוכחת העבודה בעזרת קידום ספרה (nonce) בבלוק עד אשר נמצא ערך אשר עונה על מספר הביטים המאופסים הנדרש. עם הצלחת התהליך של הוכחת העבודה והרחבת השרשרת, הבלוק אינו ניתן לשינוי מבלי לבצע את העבודה הזו מחדש. כיון שבלוקים מאוחרים יותר מתווספים בהמשכו, העבודה לשינוי הבלוק תחייב ביצוע עבודה לכל הבלוקים שהצטברו לאחר מכן. (בתרשים, Tx – טרנזקציה, עסקה)



הוכחת העבודה פותרת את בעית ההחלטה מי מייצג את דעת הרוב. לו קביעת הרוב היתה מבוססת על הצבעה של קול אחד לכל כתובות IP, היה הדבר מאפשר להטותה ע"י אלו שיכולים להקצות כתובות IP רבות. הוכחת עבודה בבסיסה היא קול אחד לכל CPU. החלטת הרוב מיוצגת ע"י השרשרת הארוכה ביותר, בה הושקע מאמץ הוכחת העבודה הגדול ביותר. אם מרבית כח מיחשוב נמצא בידי צמתות הוגנות, השרשרת ההוגנת תצמח מהר יותר ותשיג כל שרשרת מתחרה אחרת. כדי לשנות בלוק עתיק יותר, התוקף יצטרך לבצע תהליך הוכחת עבודה לבלוק ולכל אלו שבאו אחריו ואז להספיק להשלים גם אל כל מה שנוצר בינתיים ע"י הצמתות ההוגנות. נראה בהמשך שההסתברות שהיכולת של תוקף אטי יותר להשלים פערים יורדת אקספוננציאלית ככל שמתווספים בלוקים.

כדי לפצות על מהירות החישוב ההולכת וגדלה של חומרות, והענין המשתנה בהרצת צמתות על פני זמן, דרגת הקושי של הוכחת העבודה נקבעת ע"י ממוצע משוקלל אשר מתכנס למטרה של מספר הבלוקים בשעה. אם זו מהירה מדי, דרגת הקושי תעלה.

5. רשת

השלבים להרצת הרשת הנם כדלקמן:

1) עסקות חדשות משודרות לכל הצמתות.
2) כל צומת אוספת עסקות חדשות לתוך בלוק.
3) כל צומת עובדת על מציאת הוכחת העבודה הקשה עבור הבלוק שלה.
4) כאשר צומת מוצאת הוכחת עבודה, היא משדרת את הבלוק לכל הצמתות.
5) צמתות מאשרות בלוק רק אם כל העסקות שלו מאומתות וטרם הוצאו.
6) צמתות מביעות את הסכמתן לבלוק ע"י כך שעובדות על יצירת הבלוק הבא בשרשרת תוך שימוש בהאש של הבלוק המאומת כהאש הקודם בשרשרת.

צמתות מתיחסות תמיד לשרשרת הארוכה ביותר כנכונה וממשיכות לעבוד כדי להמשיכה. אם שתי צמתות משדרות גירסות שונות של הבלוק הבא בעת ובעונה אחת, יתכן שיהיו צמתות שיקבלו אחת או אחרת כראשונה. במצב כזה, הן עובדות על הראשונה שקיבלו, אך שומרות את השניה למקרה שהיא זו שתתקבל. השויון ישבר כאשר הוכחת העבודה הבאה תימצא וענף אחד יהיה ארוך יותר. במקרה זה הצמתות שעבדו על האחר יעברו לענף הראשי כדי להמשיך במלאכת העשייה.

אין הכרח ששידור עסקות חדשות יגיע לכל הצמתות. כל עוד הן מגיעות לצמתות רבות, הן תוכנסנה בסופו של דבר לבלוק. שידור בלוקים הנו גם כן סובלני להודעות שנשמטו. אם צומת לא קיבלה בלוק, היא תבקש אותו כאשר תקבל את הבלוק הבא ותגלה שהוא חסר לה.

6. תימרוץ

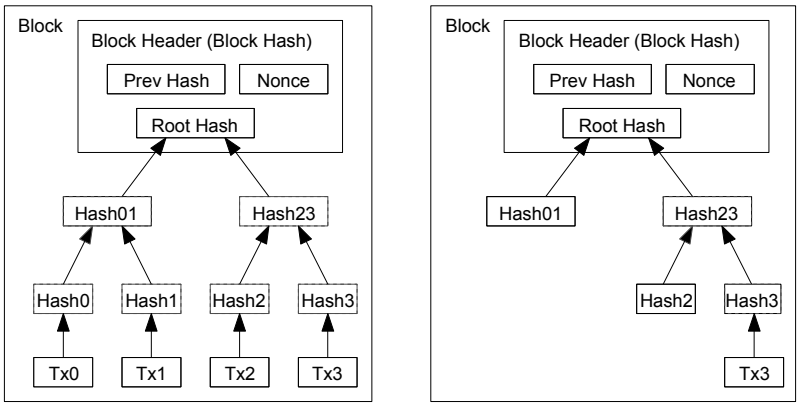
כנוהל, העסקה הראשונה בבלוק הנה עסקה מיוחדת אשר יוצרת מטבע חדש המוקצה ליוצר הבלוק. הדבר מספק תמריץ לצמתות לתמוך ברשת, ולספק אמצעי להפצה ראשונית של מטבעות לתוך המחזור, כיון שאין רשות מרכזית שתבצע זאת. התוספת היציבה והקבועה של כמות מטבעות דומה לזו של כורי הזהב אשר משקיעים משאבים כדי להוסיף זהב למחזור. במקרה שלנו זהו זמן CPU וחשמל שמהווים את העלות.

התמריצים יכולים גם להיות ממומנים ע"י עמלות עסקה. אם ערך הפלט קטן מערך הקלט, ההפרש הנו דמי עסקה שמתווספים לתמריץ של יצירת הבלוק המכיל את העסקה. ביום בו הכמות המוגדרת מראש של המטבעות תצטרף כולה למחזור, התמריץ יתבסס כולו רק על דמי העסקה ויהיה לגמרי מנוטרל ממרכיב האינפלציה,

התמריץ יכול לסייע בעידוד צמתות להשאר הוגנות. אם תוקף חמדן יכול לרכז יותר כח מיחשוב מאשר כל הצמתות ההוגנות, הוא יצטרך לבחור בין השימוש בו להונות אנשים ע"י גניבה בחזרה של תקבולים ששילם להם, או להשתמש בו כדי לייצר מטבעות חדשים. הוא אמור לגלות שיותר רווחי לדבוק בכללי המערכת, כללים אשר מתגמלים אותו ביותר מטבעות חדשים מאשר את כל האחרים יחדיו, מאשר לפגוע במערכת ובואלידיות של העושר האישי שלו.

7. שחרור שטח דיסק

כאשר העסקה האחרונה במטבע קבורה מתחת למספיק בלוקים, ניתן להתעלם מהעסקות הקודמות שהוצאו, וזאת כדי לחסוך בשטח דיסק. כדי לממש זאת מבלי לשבור את ההאש של הבלוק, עסקות מוצפנות האש של עץ מרקל [7][2][5], ורק שרש מרקל נכלל בהאש של הבלוק. בלוקים ישנים יכולים להתכווץ ע"י התנתקות מענפי העץ. . ההאשים הפנימיים אינם צריכים להשמר.



Transactions Hashed in a Merkle Tree

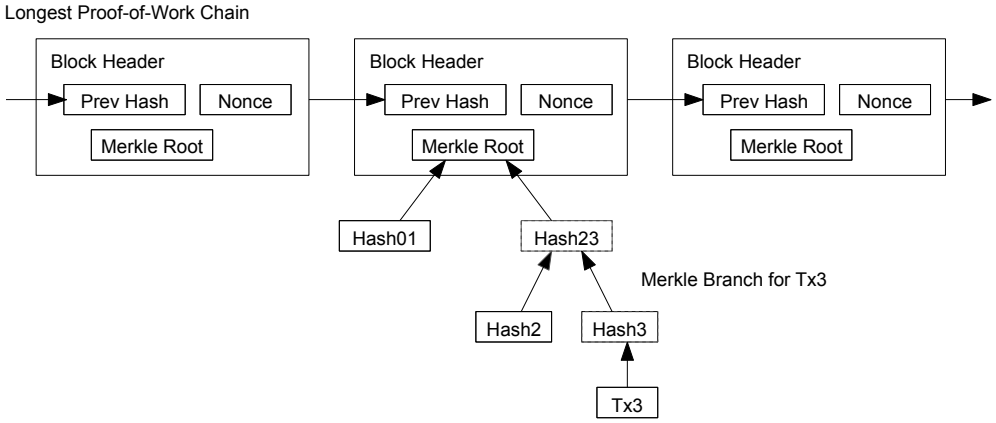
After Pruning Tx0-2 from the Block

כותרת בלוק ללא עסקות תופסת כ 80 בתים. אם נניח שבלוק נוצר כל 10 דקות, 80 בתים * 6 * 24 * 365 = 4.2MB בשנה. למחשבים שנמכרים בדרך כלל עם 2GB של RAM (שנת 2008) ולפי חוק מור הצופה גידול נוכחי של 1.2GB בשנה, שטח איחסון לא צריך להוות בעיה אפילו אם כותרות הבלוקים חייבות להשמר בזכרון.

8. אימות תשלומים מפושט

ניתן לאמת תשלומים ללא הרצה של צומת שלמה. משתמש צריך לשמור רק את כותרות הבלוקים של השרשרת הארוכה ביותר, אותה ניתן לבקש מהצמתות, עד מצב בו הוא משוכנע שמדובר בשרשרת הארוכה ביותר, ולקבל את ענף המרקל אשר קושר את העסקה לבלוק בו נחתם הזמן שלה. הוא אינו יכול לאמת את העסקה בעצמו, אך בעזרת הקישור שלה למקומה בשרשרת, הוא יכול לראות שהיתה צומת ברשת שאימתה אותה, ובלוקים נתווספו לאחר מכן מה שמוסיף משנה תוקף לאישור.

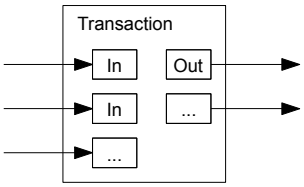
. ,,



לאור זאת, תהליך האימות הנו אמין כל עוד צמתות הוגנות שולטות ברשת, אך הנו פגיע יותר אם תוקף השיג עליונות ברשת. בעוד שצמתות הרשת יכולות לוודא עיסקות לעצמן, השיטה המפושטת מאפשרת הונאה ע"י תוקף שמפברק עסקות כל עוד התוקף יכול לנצח את הרשת בכח המיחשוב שלו. דרך אחת להגן נגד זאת היא לקבל אתראות מצמתות ברשת כאשר הן מגלות בלוק לא תקף, מה שיעודד את המשתמש להוריד את הבלוק כולו ואת העסקות החשודות כדי לאשר את אי התאימות. עסקים שמקבלים תשלומים שוטפים ירצו בדרך כלל להריץ את הצמתות שלהם כדי להשיג יותר עצמאות באבטחה ואימות מהיר יותר.

9. שילוב ופיצול ערך

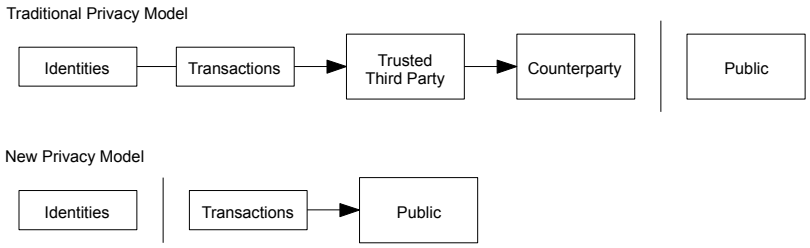
למרות שאפשרי לנהל מטבעות כל אחד בנפרד, יהיה מסורבל לבצע עסקה נפרדת לכל סנט שנמצא בתהליך העברה. כדי לאפשר לערך להתפצל ולהתאחד, עסקות כוללות קלטים ופלטים מרובים. באופן רגיל הן תכלולנה קלט יחיד עם סכום שגדול מהנדרש, או מספר קלטים עם סכומים הקטנים מהנדרש, ולכל היותר עם שני פלטים, האחד לתשלום והשני להחזרת היתרה. אם יש כזו, לשולח.



יש לציין שהרחבת המניפה, בה עסקה תלויה במספר עסקות, ואלו תלויות בעסקות רבות אחרות, אינה מהווה כאן בעיה. לעולם אין צורך לחלץ עותק מלא נפרד של היסטורית העסקה.

10. פרטיות

המודל הבנקאי המסורתי משיג רמה של פרטיות ע"י הגבלת הגישה למידע לצדדים המעורבים ולנאמני צד שלישי. הצורך בהכרזה ציבורית של כל העסקות מונעת שימוש בשיטה זו, אך פרטיות בכל זאת יכולה להשמר ע"י שבירת זרימת המידע במקום אחר, בעזרת השימוש במפתחות ציבוריים אנונימיים. הציבור יכול לראות שמישהו שולח סכום למישהו אחר, אך ללא מידע הקושר את העסקה למישהו מסויים. הדבר דומה לרמת המידע המסופק ע"י בורסות, שם מפרסמים את הזמן וגודל העסקה הספציפית אך ללא ציון מי היו הגורמים המעורבים.



כחומת הגנה נוספת, זוג חדש של מפתחות רצוי לכל עסקה כדי למנוע מהן להיות מקושרות לאותם הבעלים. קשירה מסוימת בכל זאת לא ניתן להתיר כאשר משתמשים בקלטים מרובים אשר בהכרח מגלים שיש להם בעלים אחד. הסיכון הנו בכך שאם בעל המפתח מתגלה, הקשר יוביל לעסקות נוספות שלו.

11. חישובים

נתייחס לתרחיש בו תוקף מנסה ליצור שרשרת חלופית מהר יותר מאשר השרשרת ההוגנת. אפילו אם הדבר מושג, הדבר אינו חושף את המערכת לשינויים מלאכותיים, כגון יצירת ערך יש מאין או לקיחת כסף אשר לעולם לא היה שייך לתוקף. צמתות לא יאשרו עסקות שגויות כתשלום, וצמתות הוגנות לעולם לא תקבלנה בלוק שכולל אותן. התוקף יכול רק לנסות לשנות אחת מהעסקות שלו כדי להחזיר לעצמו כסף שהוציא לאחרונה.

התחרות בין השרשרת ההוגנת והתוקפת יכולה להתאפיין כ"צעידה האקראית הבינומית" (Binomial Random Walk). אירוע ההצלחה הנו כאשר השרשרת ההוגנת הורחבה בבלוק אחד והגדילה את הפער ב 1+ וכשלון הנו כאשר התוקף הגדיל את השרשרת שלו בבלוק אחד, ובכך הפחית את הפער ב 1-.

ההסתברות לתוקף ליישר קו מפיגור נתון, אנלוגי לבעית "השברות המהמר" (Gambler's Ruin). נניח מהמר עם אשראי בלתי מוגבל אשר מתחיל עם פער ומנסה לסגור אותו במספר נסיונות אינסופי כדי להגיע לאיזון. נוכל לחשב את ההסתברות שהוא יגיע אי פעם לאיזון או שהתוקף יצליח להשתוות לשרשרת ההוגנת כדלקמן [8]:

$p =$ ההסתברות שהרשת ההוגנת תגלה את הבלוק הבא
$q =$ ההסתברות שהתוקף יגלה את הבלוק הבא
$qz =$ z ההסתברות שהתוקף יצליח אי פעם להשתוות מפיגור של כמות בלוקים

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

תחת ההנחה שלנו ש $p > q$ ההסתברות צונחת אקפוננציאלית ככל שמספר הבלוקים שהתוקף צריך להשלים גדל. עם הסיכויים נגדו, אם ההימור שלו לא מצליח מיד בהתחלה, סיכוייו מתמזערים והוא ממשיך להגדיל את הפער ולפגר מאחור.

נבחן כעת כמה צריך לחכות המקבל של עסקה חדשה לפני שהוא מספיק בטוח שהשולח לא יכול לשנות את העסקה. נניח שהשולח הנו התוקף שרוצה שהמקבל יאמין לזמן מה שקיבל תשלום ואז הוא פונה לשלם לעצמו לאחר שזמן זה עבר. המקבל יקבל אתראה על כך, אך התוקף מקווה שהדבר יהיה כבר מאוחר מדי.

המקבל יוצר זוג מפתחות חדש ומספק את המפתח הציבורי לשולח זמן קצר טרם החתימה. כך נמנע מהשולח להכין מראש שרשרת בלוקים ע"י עבודה מתמשכת עד אשר הוא בר מזל להתקדם מספיק רחוק ואז הוא מבצע את העסקה. ברגע שהעסקה נשלחה, השולח הרמאי עובד בחשאי על שרשרת מקבילה אשר כוללת גירסה אחרת של העסקה.

המקבל ממתין עד שהעסקה נתווספה לבלוק ו z בלוקים נקשרו לאחר מכן. הוא לא יודע את המספר המדויק של התקדמות התוקף, אך נניח שהבלוקים בשרשרת ההוגנת התקדמו בזמן הממוצע הצפוי לבלוק, הפוטנציאל של התוקף להתקדם יהיה התפלגות פואסון עם ערך צפוי:

$$\lambda = z\frac{q}{p}$$

כדי לקבל את ההסתברות שהתוקף יוכל עדיין להשלים כעת את הפער, אנו כופלים את צפיפות פואסון לכל כמות של התקדמות שהוא יכול היה לבצע עם ההסתברות שהוא יכל להשלים את הפער מאותה הנקודה

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{Bmatrix}(q/p)^{(z-k)} & if\,k\le z\\ 1 & if\,k>z\end{Bmatrix}$$

ובארגון מחדש כדי להמנע מהזנב האינסופי של ההתפלגות ...

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

ובהמרה לקוד C...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

בהרצה של כמה מהתוצאות, ניתן לראות שההסתברות צונחת בקצב אקספוננציאלי עם z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

פותרים עבור P הקטן מ 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. סיכום

הצענו מערכת לעסקות אלקטרוניות ללא השענות על נאמן צד ג'. פתחנו עם המסגרת הרגילה של מטבעות הנוצרים מחתימות דיגיטליות, אשר מספקות בקרה חזקה על הבעלות, אך אינה שלמה ללא פתרון לבעית ההוצאה הכפולה. כדי לפתור זאת, הצענו רשת עמית לעמית ישירה המשתמשת בהוכחת עבודה כדי לתעד ציבורית את היסטורית העסקות אשר די מהר גורמת לאי כדאיות חישובית לתוקף שמנסה לבצע שינוי במצב בו לשרשרת הוגנת יש רוב של כח המיחשוב. הרשת הנה איתנה מתוך הפשטות הבלתי מובנית שלה. צמתות עובדות במקביל עם צורך מועט של תיאום. הן אינן זקוקות להזדהות כיון שמסרים אינם מנותבים ליעד ספציפי, אלא רק צריכים להשלח על בסיס המאמץ הגדול ביותר. צמתות יכולות להתנתק או להתחבר לרשת כרצונן, ומקבלות את הוכחת העבודה של שרשרת כהוכחה למה שקרה בעת העדרן. הן מצביעות על פי כח המיחשוב שלהן ומביעות את אישורן לבלוקים מאומתים ע"י כך שפועלות לבנות את הבלוק הבא מעליהם ולמנוע בלוקים לא תקניים ע"י סירוב לעבוד עליהם. כללים נדרשים כלשהם ותמריצים יכולים להיות מוכתבים במסגרת מבנה הקונצנזוס הזה.

הפניות

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *In Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. *1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.