מידע רדיו וטלויזיה

IFAT House
96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת
דרך מנחם בגין 96-98 , תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

לינק לקובץ : לחץ כאן
תוכנית : ג'יגה ב'
תאריך : 03/02/2016
שעה : 22:42:00
רשת : רשת ב

כותרת : ***ד"ר ערן טרומר, ביה"ס למדעי המחשב באוניברסיטת ת"א וממייסדי הZCASH -***

נפתלי מנשה : טוב, אנחנו עוברים לעניין הבא. על המטבע הווירטואלי ביטקוין סיפרנו לכם הרבה פעמים בעבר. הפעם נספר על מטבע וירטואלי חדש בפיתוח ישראלי-אמריקני שעולה ביתרונותיו על הביטקוין. קוראים ZCASH, שלום ל... או .ZCASH CASH. שלום לד"ר ערן טרומר מבית הספר למדעי המחשב באוניברסיטת תל אביב וממייסדי מטבע ה-ZCASH.

ד"ר ערן טרומר : ערב טוב.

נפתלי מנשה : אז מה מיוחד ב-ZCASH לעומת הביטקוין?

ד"ר ערן טרומר : ה-ZCASH דומה ביתרונות ובשימושיות שלו לביטקוין, אבל בניגוד לביטקוין הוא לא חושף את כל פרטי העסקאות של המשתמשים בו.

נפתלי מנשה : כלומר, ביטקוין חושף את הפרטים של העסקאות שלי, אני החלטתי לקנות איזה מוצר וכולם יודעים מה קניתי ואיך

מידע רדיו וטלויזיה

IFAT House
96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת
דרך מנחם בגין 96-98 , תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

עשיתי את זה?

ד"ר ערן טרומר : אכן. בביטקוין כאשר אתה מבצע רכישה כל אחד יכול לראות כמה שילמת, מתי ולמי. הסוחרים בשוק הביטקוין יכולים לראות מה יתרת המזומן בארנק שלך אם הם סקרנים. אתה סוחר, המתחרים יכולים לראות מה תזרים המזומנים שלך.

נפתלי מנשה : למה זה צריך להיות ככה?

ד"ר ערן טרומר : כל זה נובע מבעצם רעיון בסיסי, ולמעשה גאוני למדי, שבבסיס ביטקוין, רעיון של אותו סטושי נקמוטו, ... שמו האמיתי...

נפתלי מנשה : הוא עלום, עלום.

ד"ר ערן טרומר : והרעיון המפורסם שלו הוא כיצד למנוע שימוש באותו מטבע פעמיים. הרעיון הוא ליצור מן יומן פומבי של עסקאות שמפורסם לכל העולם וכך כאשר אם מישהו מנסה לבצע עסקה, הסחור בודק האם העסקה הזאת כבר משתמשת במטבע שכבר ביומן ואם כן, דוחה אותה. כך נשמר הערך הכלכלי של המטבע וזה עיקרון הפעולה הבסיס. אבל באותו יומם פומבי ניתן לראות את כל אותן עסקאות.

- נשמע כמו חדריה עצומה לפרטיות.

ד"ר ערן טרומר : אכן כך וזה באמת צוואר בקבוק בשימושיות של ביטקוין כפי שהוא היום, בין אם זה לאנשים שחרדים

מידע רדיו וטלויזיה

IFAT House
96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת
דרך מנחם בגין 96-98 , תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

מהפרטיות האישית שלהם, אבל בין אם לארגונים ולממשלות שלא היו רוצים שאחרים יוכלו להביט לתוך הארנק שלהם.

נפתלי מנשה : כן, אבל אני חושב שאנחנו חוטאים טיפה לדיוק. אין מאחורי המספר של הביטקוין, הרי לכל ביטקוין יש איזשהו מספר מזהה, לא יודעים מי אני, לא יודעים שאני זה עם השם שלי ומקום המגורים שלי והכל. אלא יודעים שהמטבע הספציפי הזה עבר מאדם אחד לאדם אחר. אבל לא... כל הקטע של ביטקוין הזה האנונימיות שלו שלא יודעים מי אני. אז מי זה שמחזיק את המטבע.

ד"ר ערן טרומר : אז האנונימיות לכאורה של אותו מזהה מטבע נכונה רק עד הפעם הראשונה שבה אתה משתמש בו. מאותו רגע כל מי שסחרת איתו יודע לחבר בין אותו מספר אקראי לבין הזהות שלך.

נפתלי מנשה : איך הוא יודע?

ד"ר ערן טרומר : הוא רואה אות אותו מספר כחלק מהעסקה שהוא ביצע מולך וככה החברים שלך שפעם התחשבנתם איתם אחרי מסעדה יכולים לראות איזה קניות אתה עושה באינטרנט, השותפים העסקיים שלך יכולים לראות מה אתה עושה בבית וכן הלאה.

נפתלי מנשה : או־קיי. אז ספר לנו על היתרונות של ZCASH. מה מיוחד ב־ZCASH?

מידע רדיו וטלויזיה

IFAT House
96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת
דרך מנחם בגין 96-98 , תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

ד"ר ערן טרומר : אז הרעיון ב-ZCASH הוא לשמר את אותן תכונות שימושיות כל כך של ביטקוין אבל תוך שימור מלא של פרטיות כל המשתמשים. הרעיון הוא להשתמש בשיטת הוכחה מחזית המחקר של תרות ההצפנה, הוכחות שנקראת סנרק, שמאפשרות לנו לקחת טענות חישוביות ולהוכיח אותן מבלי לחשוף פרטים מיותרים. כדי לבצע תשלום, לדוגמה לסוחר, הקונה בודק בעצמו את התשלום מבלי לחשוף את הפרטים של עצמו ומבשר לסוחר שהתשלום תקין. כדי לשכנע את הסוחר שהבשורה הזאת אכן נכונה, הוא משתמש באותן הוכחות סנרק. ההוכחות האלה מעשיות ניתן לבדוק אותן תוך שבריר שנייה. הן משמרות לנו את כל התכונות המוניטריות של המטבע ועדיין מישהו שצופה מהצד לא יכול לדעת מי שילם למי, כמה הוא שילם ומתי. רק שותפים לעסקה יותר במה מדובר.

נפתלי מנשה : ואם השותפים האלו יהיו שותפים האלו יהיו שותפים לעסקה בעתיד? אז הם ידעו מי הוא מי ואיזה מטבע עבר ביניהם בעבר.

ד"ר ערן טרומר : הם עדיין לא יכולו לזהות חיבור בין העסקאות. ברגע שאחד מהשותפים האלה יבצע עסקה עם גורם שלישי, השותף האחר שיושב מהצד, כל מה שהוא ילמד זה שמישהו, איפשהו, ביצע איזושהי עסקה. הוא לא יכול לשייך אותה בשום צורה לעסקה הקודמת.

מידע רדיו וטלויזיה

IFAT House
96-98 Derech Menachem Begin, Tel Aviv
(formerly Derech Petach Tikva)
Tel 972-3-5635050, Fax 972-3-5617166
www.ifat.com

בית יפעת
דרך מנחם בגין 96-98 , תל אביב
(לשעבר דרך פ"ת)
טל 03-5635050, פקס 03-5617166
www.ifat.com

נפתלי מנשה : וכל זאת בזכות עולם הקריפטוגרפיה, היכולת להצפין מידע.

ד"ר ערן טרומר : להצפין, להוכיח. מדובר במחקר בחזית המחקר האקדמי. הוא התחיל כשיתוף פעולה בינלאומי של חוקרי אבטחת מידע אצלנו באוניברסיטת תל אביב עם פרופ' אלי בן ששון מהטכניון, עם שותפים מ-MIT ואוניברסיטת ג'ונס הופקינס בארה"ב, ובמשך השנים זה קרם עור וגידים מרעיון היפותטי, שאלה תאורטית לגמרי לגבי התכנות של שיטות הוכחה והפך למעשה לפני שבועיים למיזם חדש ופתוח שיאשר לציבור המשתמשים להשתמש במטבע הזה ולהגן על פרטיות העסקאות שלהם.

נפתלי מנשה : ד"ר ערן טרומר מבית הספר למדעי המחשב באוניברסיטת תל אביב וממייסדי מטבע ה-ZCASH, תודה רבה שבאמת לאלופן.

ד"ר ערן טרומר : תודה לכם.

נפתלי מנשה : הרבה הצלחה.