תמלול: האם בלוקצ'יין מממשת את ההבטחה?

הופק על ידי רשת, עושים היסטוריה.

יובל: ברוכים הבאים לנקודה IL, הפודקאסט של איגוד האינטרנט הישראלי שעוזר לנו להבין מה הן השפעות העומק של האינטרנט על החברה, הכלכלה, הפוליטיקה והתרבות. אני דוקטור יובל דרור. יש נושאים רבים, לא רבים, אבל יש כמה... שלא משנה כמה פעמים יסבירו לי אותם אני פשוט לא מצליח לקלוט אותם עד הסוף. אני חושב שאני מבין. ואז אני מבין שאני לא לגמרי מבין. ואחד הנושאים האלו הוא בלוקצ'יין, אני חושב שאני יודע מה זה. אבל אם תבקשו ממני הסבר, כנראה שמתישהו אחרי זמן לא ארוך, אני אחליף איכשהו נושא. העניין הוא שבלוקצ'יין הוא דבר שתוסף תאוצה. הישום שעליו כולנו שמענו הוא הביטקוין, אבל בלוקצ'יין הוא הרבה מעבר לביטקוין. ובשנתיים האחרונות נשמעים יותר ויותר קולות שקוראים לקחת תחומים נוספים ולהעביר אותם ל-בלוקצ'יין. מה זה אומר? מה זה אומר לקחת משהו ולשים אותו על ה-בלוקצ'יין? איך זה אמור לעבוד והאם זה בכלל רעיון טוב? כדי לענות על השאלות האלו, כי בואו, אני לא יודע לענות עליהן, אני מארח היום את פרופסור אור דונקלמן, מומחה לאבטחת מידע ואיש סגל באוניברסיטת חיפה, שהיה מעורב בכתיבת

מסמך מדיניות עבור איגוד האינטרנט הישראלי בנושא הזה.

בנושא של הבלוקצ'יין. אוק שלום.

אור: שלום יובל.

יובל: בתור התחלה, אני אבקש ממך להתמודד עם אתגר מאוד מסובך, לפחות בעיני. במשפט אחד, מה זה בלוקצ'יין?

אור: בלוקצ'יין זו מערכת שתפקידה להגיע להסכמה בין מספר גופים שונים על עובדות מסוימות. לדוגמא, אם אנחנו חושבים על ביטקוין, על מי מחזיק כמה כסף. או מי העביר כמה כסף למי ומתי. כאשר האמון בין אותם אנשים שמסכימים הוא קטן ככל האפשר.

יובל: אז המערכת הזאת מאפשרת לי ליצור את האמון?

אור: היא מאפשרת ליצור את ההסכמה, גם אם אתה לא סומך על מי שיושב בצד השני.

יובל: באיזה אופן היא מאפשרת את זה?

אור: אז כאן נכנס האמון במתמטיקה, באלגוריתמיקה. ישנן בעיות קשות, שאנחנו יודעים שהן בעיות מתמטיות קשות. או בהקשרים של ביטקוין, אז בעיות קרובות למתמטיות. שהפתרון שלהן הוא קשה ומי שפותר אותן הוא לכאורה וזה קשור, אנחנו נקרא בהמשך לנושא הכרייה, בעצם, מי שמצליח לפתור אותן הוא זה שמייצר את ההסכמה וכופה את ההסכמה

על כולם בעצם זה שהוא זה שפתר. העניין של מינימום האמון הוא שכל אחד יכול לפתור.

יובל: אז אני לא יכול לסמוך על ה... אם כל אחד יכול לפתור, אז כל אחד יכול לייצר אמון. אם כל אחד יכול לייצר אמון, אז אין בעצם אמון, כי כל אחד יכול לייצר אותו.

אור: זה היופי של הקריפטוגרפיה מאחורה.

יובל: תסביר לי.

אורי: הרעיון הוא כזה, נניח לרגע שאני נותן לך ספר טלפונים. ואני אומר לך, יובל, מצא בבקשה את מספר הטלפון של אדם מסוים, פלוני אלמוני. אתה פותח את ספר הטלפונים. ואני מזכיר, אנחנו מדברים על ספר טלפונים פיזי, לא אפליקציות ואתרים.

יובל: היה פעם אחד כזה.

אור: כן.

יובל: אוקי.

אור: לשומעינו הצעירים, תבקשו במוזיאון הקרוב למקום מגוריכם.

יובל: אז פתחתי את ספר הטלפונים ואני מחפש את השם שאתה ביקשת ממני.

אור: נכון. וזה בעיה יחסית פשוטה.

יובל: נכון.

אור: ועכשיו אני אשאל אותך את השאלה הבאה. למי יש את מספר הטלפון אפס ארבע, שמונה אחד שתיים שלוש ארבע חמש שש.

יובל: זאת אומרת לעשות חיפוש הפוך?

אור: כן.

יובל: זה הרבה יותר מסובך.

אור: זה הרבה יותר מסובך. אז זאת דוגמא לבעיה שקל לנו לחשב אותה לכיוון אחד בהינתן שם, למצוא את מספר הטלפון. וקשה לנו לחשב לכיוון ההפוך. הרעיון מאחורי כריית ביטקוינים או בכלל בבלוקצ'יין, יש שלושה סוגי בעיות מהצורה הזאת. זאת אומרת, זה דוגמא לבעיות שהן קשות בעבודה. נותנים מספר טלפון וצריך למצוא אחורה. צריך למצוא מי בעל מספר הטלפון. כאשר הרעיון הוא כזה, מכיוון שכולנו יכולים לנסות לפתור, הראשון שיצליח לפתור, כופה את דעתו. אבל אם הוא ינסה לעשות משהו שהוא יותר מדי אגרסיבי, הבא בתור שיפתור, יש בעצם רצף של בעיות. כל אחד בתורו מנסה לפתור את הבעיה הנוכחית. וכל פעם מישהו פותר חלק אחר של הבעיה. או בעיה אחרת קשורה. ואז מה שקורה, אם יש מישהו שמנסה להשתלט על המערכת, הוא לא יצליח לאורך זמן, כי הסיכוי שהוא יצליח לענות נכון גם על השאלה הנוכחית, גם על השאלה הבאה, גם על השאלה שאחריה, גם על... הוא מאוד

מאוד קטן. וככה, למרות העובדה שכל אחד, יש לו אינטרסים מאוד הפוכים מאחרים, בעצם מה שיוצא זה מערכת שבה קשה מאוד לגורם אחד להשתלט.

יובל: זאת הנקודה בעצם. המערכת מייצרת אמון מכיוון שאין שחקן אחד שיכול להשתלט עליה? זו בעצם הנקודה?

אור: כן. תחת ההנחה, שאותה בעיה מתמטית היא באמת קשה.

יובל: בעצם העולם של הבלוקצ'יין מבוסס, למטה למטה יש קריפטוגרפיה, יש הצפנה, מה זה בעצם אומר?

אור: הצפנה התחילה בהגנה על מידע. אליס ובוב מדברים ביניהם בצורה כזאת שכל מי ששומע את התקשורת ביניהם לא יכול להבין מה נמצא בתוכה.

יובל: כי התקשורת מוצפנת.

אור: כי התקשורת מוצפנת, אחר כך זה עבר לתקשורת גם מוגנת. אי אפשר להחליף את המידע שעובר ביניהם. אף אחד לא יכול להזריק מידע. זאת אומרת, אליס פתאום שולחת הודעה לבוב, אני עוזבת אותך, למרות שבעצם זאת היתה איב ששלחה את ההודעה בשמה, אז גם הקריפטוגרפיה נותנת מענה לזה. עם הזמן עולם הקריפטוגרפיה התפתח ובעצם נותן שלל כלים להגן על מידע כנגד התנהגות, אנחנו קוראים לה עוינת.

יובל: אהה. זאת אומרת, יש כל מני כלים להגן על המידע. זה בעצם מה שהקריפטוגרפיה נותנת לעולם ולנו. אוקי, בסדר. בוא נלך

למקום שכולנו שומעים עליו, כל הזמן. וזה הביטקוין, איך זה עובד במקרה של הביטקוין. ביטקוין זה מטבע שיש לו ערך בעולם האמיתי. אני אפילו לא אגיד מה הוא, כי עד שאתם תשמעו אותו הוא יעלה וירד עד מיליון פעם. אבל אנחנו יודעים בגדול מה זה. איך הבלוקצ'יין עובד במקרה של הביטקוין, מה קורה שם?

אור: אז כעיקרון הבלוקצ'יין שיושב מאחורי הביטקוין, שזאת באמת הפעם הראשונה שהבלוקצ'יין מומש. הרעיון הוא כזה, לכל אחד יש חשבון. ומהחשבון הזה אתה יכול לקבל אליו כספים, לקבל אליו ביטקוינים. ולהוציא ממנו ביטקוינים.

יובל: חשבון הכוונה היא ארנק?

אור: ארנק.

יובל: אוקי.

אור: ארנק זה המימוש של החשבון. החשבון זה בעצם כתובת וירטואלית.

יובל: שזה החשבון שלי.

אור: כן.

יובל: שבפנים יש נניח ארבעה מטבעות ביטקוין.

אור: נכון.

יובל: סבבה. אוקי.

אור: ועכשיו בעצם כל פעם שמישהו מבצע העברה, הוא זורק, הוא מודיע לרשת הביטקוין, אני רוצה להעביר, מהחשבון של יובל לחשבון של אור, ביטקוין אחד. והרשת, זאת אומרת, אותם כורים, מה שהם עושים, הם אוספים את אותן טרנסאקציות. ומנסים לרשום אותן בתוך הבלוק. עכשיו, מה? מה הוא אותו בלוק? אפשר לחשוב על גושי חמר.

יובל: אוקי.

אור: אני לדוגמא, יש לי כרגע ארבעה ביטקוינים, אני רוצה להעביר לך אחד. אני מודיע לכולם, אני רוצה להעביר ליובל ביטקוין אחד. יושב מישהו וכותב על אותו גוש חמר, ביטקוין אחד עובר מאור ליובל. תהליך הכרייה, אותו פתרון של בעיה מתמטית זה בעצם לקחת את אותו לוח חמר ולשים אותו ולשרוף אותו, כדי שאי אפשר יהיה לשנות. זה הוא בעצם אותו רכיב, זה החלק של יצירת האמון. מכיוון שכל אחד יכול לקחת את הלוחות האלה ובצעם מה שעושים כל אחד מהכורים, הם לוקחים את כל אותם טרנסאקציות, את כל אותן בקשות העברה. רושמים אותם בלוח החמר הזה.

יובל: ושורפים אותם כך שאי אפשר יהיה לשנות אותם.

אור: כן. כמעט. למה? כחלק מהמנגנון, השריפה היא בעצם נעשית בשני חלקים. חלק ראשון אתה מקבע את הבלוק. ורק אחרי שעובר כמה זמן, זאת אומרת, רק אחרי שעברו כמה בלוקים

קדימה, בעצם שור... מקבעים סופית את הלוח הקודם. ואז אם במקרה... וזה באמת חלק מהמנגנון של ההגנה נגד מישהו שמנסה להשתלט על המערכת. מכיוון שאם מישהו מנסה לפתור את הבעיה ובעצם לייצר עולם שבו אני מעביר לך חמישה ביטוקוינים, למרות שיש לי בחשבון רק ארבעה, אז הוא אולי יוכל לייצר את הבלוק הראשון, את הלוח חמר הראשון אבל הלוחות חמר הבאים הוא כבר לא יוכל לייצר אותם, כי כל האחרים ינסו לייצר לוחות חמר מתחרים.

יובל: אז בעצם את האמון של מי אני מנסה להחליף?

אור: בבנק.

יובל: בבנק המרכזי?

אור: או במדינה.

יובל: תסביר, אם אני... בוא, בוא רגע ננסה להסביר את זה. אם אני רוצה להעביר אליך מאה שקל מהחשבון שלי לחשבון שלך, אני בעצם לא מעביר את זה ישירות אליך, אני מעביר את זה דרך הבנק. ואז לי ולך יש אמון בבנק, שכשאני אומר תעביר אליך מאה שקל, הבנק יעשה את מה שאני אומר. הוא יבדוק שיש לי מאה שקל וישים את זה בחשבון שלך. זאת אומרת, עניין מרכזי, בתוך כל המערכת הזאת, זה האמון שהבנק עושה את עבודתו.

אור: נכון.

יובל: מה עושה הבלוקצ'יין?

אור: הוא בעצם... אפשר לחשוב על זה בתור מאגר נתונים. בסופו של דבר אם אנחנו מדברים על הכסף, זה מאגר נתונים. יש לך בחשבון הבנק שלך היום איקס שקלים. לי יש וואי שקלים. ואתה אומר תעבירו מאה מפה לשם וזהו. בעצם הבלוקצ'יין מייצר את אותו דטא בייס. ופשוט במקום שיהיה מישהו מאחורה שאומר, אני בנק...

יובל: ערב לכך שיש לו.

אור: לא רק שיש לו. אלא גם לוקח. כשאני לקחתי ממנו מאה ושמתי פה מאה ולקחתי את העמלה המוסכמת וזהו, אלה חוקי המשחק. ועל הבנק יושבת רגולציה והחוקים וכל הדברים. בבלוקצ'יין בעצם יש תחרות בין מספר כורים. כאשר כל כורה, כל אחד מאותם מיינרים, בעצם מנסה לשמש בתפקיד הבנק.

יובל: אהה. זאת אומרת, כל אחד יכול לשמש בתפקיד הבנק. מה מקבל זה שפתר את הבעיה המתמטית?

אור: אז הוא מקבל שני תגמולים. תגמול ראשון, יש את תגמול הכרייה. התגמול הזה הולך ופוחת. זה התחיל פעם על כל בלוק מקבלים עשרים וחמישה ביטקוינים וזה הולך ופוחת כל כמה וכמה שנים, חלקי שתיים. ויש גם את עמלת השורה. כשאתה אומר אני רוצה להעביר למישהו ביטקוין, אתה אומר גם מה עמלת השורה שאתה מוכן לתת.

יובל: כל אחד יכול לקבוע את העמלה שלו?

אור: כל אחד קובע את העמלה כשהוא משלם.

יובל: אוקי.

אור: המיינר יכול להסכים כן לבצע את הטרנסאקציה או לא לבצע את הטרנסאקציה, בהתאם לעמלה.

יובל: אוקי.

אור: ואז בעצם מה שיקרה זה, אם הטרנסאקציה שלי מאוד חשובה לי שתקרה מהר, אני אשים עליה עמלה גבוהה.

יובל: אהה.

אור: ואם לא, אז לא.

יובל: זאת אומרת, לקחנו גוף אחד, בנק פועלים, בנק לאומי, בנק אוף אמריקה, זה בכלל לא משנה. והחלפנו אותו באין ספור בנקאים קטנים שכל אחד מהם רץ כדי לממש את האירוע הזה של העברת אותו ביטקוין ביני לבינך, כי הוא מקבל גם ביטקוין וגם עמלה, על עצם זה שהוא הסכים לשמש כבנקאי שלי ושלך.

אור: נכון.

יובל: שכנעת אותי שבעולם של הביטקוין, כל הסיפור הזה של הבלוקצ'יין הוא לגמרי הגיוני ועובד. תן לי דוגמא נוספת למקום שבו בלוקצ'יין עובד בצורה ככה מוצלחת.

אור: אז אני רגע רוצה לחזור טיפה לאמירה שזה עובד בצורה מוצלחת. צריך לזכור, כמות החשמל הנצרכת היום על ידי רשת הביטקוין היא אדירה. כדי להחליף את האמון באותו בנק, גורם מרכזי, מה שהיום אנחנו עושים בהעברה בנקאית שאפילו לא מורגשת מבחינת צריכת האנרגיה, כל בלוק ברשת הביטקוין, עולה בהמון חשמל.

יובל: אנחנו יודעים כמה?

אור: אני חושב שהסקר האחרון אמר שרשת הביטקוין ב-2018 או 19 צרכה כמות חשמל של 120 ג'יגה ואט שעה.

יובל: לשעה?

אור: לא, בשנה.

יובל: בשנה. 120 ג'יגה ואט.

אור: ג'יגה ואט שעה, שזה בערך פי אחד וחצי מהצריכה הישראלית, אם אני זוכר את הטבלאות ההמרה הנכונות.

יובל: זאת אומרת, רק כי רציתי להעביר אליך... אני רציתי. ועוד מישהו ועוד מישהו ועוד מישהו. כל הרשת הזאת, צריכת חשמל של מדינה.

אור: בסדר גודל של בינונית.

יובל: הבנתי. אבל טכנולוגית אור, טכנולוגית זה עובד ממש בסדר. תן לי דוגמא נוספת למקום שבו אתה כאיש שמתמחה בעולמות האלה אומר, וואלה, שם זה גם הגיוני.

אור: בעצם רגע, יש עוד מקום שזה קצת פחות עובד בו כשחושבים על זה. מכיוון שיש מגבלה לכמות הטרנסאקציות שיכולה להתבצע בביטקוין.

יובל: למה?

אור: מכיוון שגודל הבלוק הוא קבוע. גודל הבלוק הוגדר להיות מגה בייט.

יובל: מגה בייט אחד?

אור: אחד. וכל עשר דקות נוצר בלוק.

יובל: אוקי, בסדר.

אור: זה אומר שאם כמות הטרנסאקציות יותר גדולה ממה שנכנס לבלוק...

יובל: הוא צריך לחכות לבלוק הבא?

אור: כן.

יובל: ונוצר שם פקק כמו בתעלת סואץ?

אור: כן.

יובל: אהה... וזה פקק שאנחנו ממש רואים אותו שאתה מדבר איתי עכשיו ברמה התיאורטית?

אור: יש ימים ושעות שבהם רואים את זה.

יובל: ואז אתה פשוט מחכה?

אור: הטרנסאקציה שלך יכולה לחכות. כן. היא תהיה במצב פנדיג. כאילו במצב של עוד לא התבצעה. אבל יכול להיות מצב

שכתוצא המזה אני אגדיל את כמות עמלת השורה שאני מוכן לשלם כדי שהטרנסאקציה שלי כן תיכנס.

יובל: צריך להגיד, טרנסאקציה זה כמה ביטים. אבל כשעושים כל כך הרבה, אז גם המגה הזה נגמר.

אור: נכון.

יובל: אוקי. אז...

אור: אבל חוץ מזה זה עובד.

יובל: בדיוק. אז יש לנו חשמל. יש לנו מגבלת כמות. חוץ מזה זה עובד. תן לי דוגמא נוספת לאפליקציה, ליישום מוצלח נוסף של הבלוקצ'יין.

אור: דוגמא נוספת היא לא ביטקוין, כי ביטקוין הוא באמת רק מטבע קריפטוגפרי, יש את נושא הבלוקצ'יין ואולי שמעתם, אמנם זה מטבע קריפטוגרפי אחר, מה שקרוי האת'ריום.

יובל: כן.

אור: רשת האת'ריום בעצם נותנת לנו גם פונקציה נוספת שהיא חוזה חכם. לא רק שזה מטבע קריפטוגרפי, אלא יש, אפשר להצמיד אליו קוד מחשב, מותנה, שמבצע דברים.

יובל: תסביר.

אור: לדוגמא, אם אני רוצה להעביר לך כסף, בתמורה לזה שאתה תעביר לי בעלות על דירה. היום אנחנו פותרים את זה על ידי הליכה לעורכי דין, חשבונות נאמנות. שלל דברים כאלה. למה?

יובל: כי אני צריך לתת אמון בכך שכשאני אעביר לו את הכסף הוא יעביר לי את הדירה, זה עוד פעם אנחנו חוזרים לעניין האמון.

אור: נכון.

יובל: אוקי.

אור: ופה אני יכול במקום זה לעשות קוד, שאומר, אם אור מציג מסמך העברת בעלות תחת תנאים מסוימים ל-עד תאריך מסוים, אתה תעביר מהחשבון שלך לחשבון שלי כך וכך את'ריומים. ועכשיו, אנחנו בעצם מכניסים את אותו חוזה חכם לרשת האת'ריום. ורשת האת'ריום היא זאת שכופה עלינו, שוב, דרך אותו מנגנון של אמון. אנחנו סומכים שהכורים של את'ריום יעשו את עבודתם נאמנה. ובאמת מובטח לנו שהחוזה מתבצע בכללותו.

יובל: אני חייב להצמיד את זה לאת'ריום? אני לא יכול לשלם בדולרים? אני חייב בסוף לשלם באת'ריום?

אור: אתה יכול, כמו שהעברת הבעלות קורית בעולם האמיתי דרך מסמך אחר, יכול להיות שאתה יכול להגיד אני רוצה לראות תמורה מסמך אחר של העברת כספים.

יובל: אה, הבנתי. אבל בעצם מעצם העובדה ששמתי את החוזה על רשת שמתנהלת על הבלוקצ'יין יצרתי את אותו אמון שאנחנו מדברים עליו.

אור: נכון.

יובל: מה לגבי עוד יישום ששמעתי עליו בעולם של ראיות. ראיות דיגיטליות. מה זה אומר?

אור: אז כאן, בוא נחשוב רגע של משטרה שתופסת הארד דיסק של נאשם בפשע והיא רוצה להוכיח שזה ההארד דיסק שהיא תפסה. למה היא רוצה להוכיח? יבוא... נניח לרגע שמצאו שם אימיילים מרשיעים. והאדם הנאשם מגיע לבית משפט ואומר, המשטרה הכניסה את זה לשם. זה לא היה שם. אני נתתי להם הארד דיסק בלי זה.

יובל: אוקי.

אור: ולכן כל הנושא של ראיות דיגיטליות הוא נורא נורא מורכב. מכיוון שאנחנו רוצים בעצם לעשות איזה תצלום, תמונת מצב נוכחית ולדאוג שהיא לא השתנתה מהרגע שזה הגיע למשטרה עד הרגע שזה מגיע לבית המשפט. אז מה הרעיון? אם אותו בלוקצ'יין מייצר הסכמה בצורה מבוזרת, אנחנו ניקח את ההארד דיסק, נשים אותו באיזו שהיא צורה על הבלוקצ'יין והחל מרגע זה אף אחד לא יכול לשנות את ההיסטוריה.

יובל: אנחנו לא שמים את ההארד דיסק, אנחנו שמים את החתימה.

אור: נכון, אנחנו גם לא שמים את ההארד דיסק כי אין מקום בבלוקצ'יין.

יובל: בדיוק.

אור: אנחנו שמים איזה מאפיין. חתימה.

יובל: וזה סוג של האש?

אור: בדיוק. או שמים האש של ההארד דיסק ואז אם ההארד דיסק ישתנה מהרגע שהוא נתפס עד הרגע שמגיעים לבית משפט, יהיה אפשר להוכיח את זה די בקלות.

יובל: האש זה בעצם חתימה שמייצרת... זה מן איזה... זה קוד בעצם.

אור: תביעת אצבע. אפשר לחשוב על זה בתור תביעת אצבע של הנתונים. יש שקוראים לזה תמצית. יש כאלה שקוראים לזה גיבוב. אבל באמת האש, השם באנגלית, זה תביעת אצבע כזאת שבאמת מהרגע ששינית את הנתונים היא בהכרח תשתנה. אלה מכם שמורידים דיסקים חוקיים של לינוקס מהאינטרנט, יש שם בסוף איזה md5sum או sha1sum זה בדיוק אותו ערך. מספר קצר יחסית שמאמת שהמידע לא השתנה.

יובל: זה מקובל ברחבי העולם כפתרון שמקובל על בתי משפט? על משטרות? על עורכי דין, על נאשמים ועל מואשמים?

אור: בארצות הברית התחילו להיכנס לזה, חלק מהסטייטס כבר מקבלים את זה ובעצם אומרים, כל ראייה דיגיטלית צריכה לעלות אל הבלוקצ'יין. אבל כאן נכנסת בעיית האמון.

יובל: רגע. נכנסת בעיית האמון, אני לפני רגע פתרתי את בעיית האמון באמצעות הבלוקצ'יין, מה זאת אומרת נכנסת בעיית האמון?

אור: זוכר שאמרנו שהביטקוין עובד חוץ מ-ו... ו... ו...? אז אני שכחתי להגיד עוד משהו. אנחנו מאמינים שביטקוין עובד מכיוון שאין אף אחד שהוא חזק מספיק כדי לכרות את הבלוק הבא. מה זאת אומרת? אם יש מישהו שהוא תמיד כורה את הבלוק הבא, אותו מנגנון הגנה שאומר, מכיוון שיש לי הרבה שחקנים ויש להם אינטרסים סותרים ותמריצים סותרים, אם יש מישהו שהוא נורא חזק, במקרה של הביטקוין, מישהו שהוא שולט ב-51% מכוח הכרייה, הוא יכול לשכתב את כל רשת הביטקוין כרצונו.

יובל: אה... וואו... אה... פתאום הכנסת לי כאילו ג'וקר. עד עכשיו שיחקנו בקלפים והחוקים היו ברורים. פתאום שמת לי ג'וקר ואמרת רגע, בתוך המערכת הזאת, למי שיש 51% ממה בעצם?

אור: מכוח העיבוד.

יובל: מכוח העיבוד של הרשת, הוא יכול להשתלט עליה.

אור: נכון.

יובל: למה? למה שמישהו יכניס בכלל כזאת אופציה? למה זה שם בכלל?

אור: זה שם מכיוון שככה נבנתה רשת ה...

יובל: ככה היא נבנתה במקור?

אור: כן.

יובל: אז בעצם מה שאתה אומר, אני לא יכול לגמרי לסמוך על המערכת, על אותו האש, על אותה תביעת אצבע, כי מי יודע? אולי הנאשם השתלט על 51% מכוח המחשוב של הרשת, ילך וישנה את מה שכתוב בהארד דיסק ועכשיו אני לא יכול לסמוך עליו.

אור: או לחילופין המשטרה.

יובל: המשטרה...

אור: אם אתה דואג מהמדינה, הרי למי יש יותר כוח? חישוב.

יובל: זה תלוי אם אתה רמאי מסוג ג'יימס בונד, או זה. אבל אוקי, בדרך כלל למדינה יש יותר כוח.

אור: זאת אומרת, שאם היא שולטת ב-51% מכוח העיבוד. ויש כמובן גם התקפות יותר יעילות. יש את התקפת ה-33%. וכאן אנחנו לא נכנסים... גם ב-33% אפשר לעשות נזקים מעניינים. וכאן אנחנו קצת התעלמנו מזה שיש, כמו שאמרתי בהתחלה, שלוש שיטות שונות לכריית הבלוק הבא. אחת מבוססת על כוח חישוב. השנייה מבוססת על כמות זיכרון. והשלישית מבוססת על מה שקרוי proof of stake שזה בעיקר בהקשרים של דברים כספיים. ואז ככל שיש לי יותר כסף אני

מקבל יותר זכות לשלוט על מה שקורה. כמובן ברגע שעוברים את קו ה-51%, או כל רשת, יש איזה מספר אחר, המנגנון בעצם מפסיק.

יובל: זאת בעיה תיאורטית? או שזה אשכרה בעיה אמיתית?

אור: זה קרה פעם אחת כמעט ברשת הביטקוין, אחד מהכורים הגדולים הגיע לבין שלושים לארבעים אחוז והוא הפסיק להוסיף ציוד כרייה כדי לא לעבור את הקו הזה. כי זה היה מאוד פוגע באמון. בצד החיובי, וזה גם מביא אותנו לבעיות של סמארט קונטרקטס. אחד מהחוזים החכמים בתחילת רשת האת'ריום של דאו, נכתב עם באג.

יובל: עם באג בתוך התוכנה?

אור: כן, מכיוון שאנחנו כבני אדם יודעים לעשות חוזים שאי אפשר להפר אותם, לראייה בחירות שלישיות רביעיות. ומצד שני אנחנו כותבים תמיד קוד ללא באגים. ברור שהשילוב של חוזה בלי באגים עם קוד ללא באגים, ייצור משהו יציב.

יובל: אהה. אז היה שם באג?

אור: היה שם באג.

יובל: ואז מה זה אומר?

אור: שחמישים מיליון דולר נעלמו באוויר.

יובל: אהה.

אור: מישהו ניצל את הבאג כדי לגנוב.

יובל: זאת אומרת, בעצם מכיוון שזה עכשיו מבוסס על תוכנה, אז זה סובל מכל הבעיות של תוכנה.

אור: כן.

יובל: אוקי. רגע, אבל העברה בנקאית היא גם עניין של תוכנה, לא?

אור: נכון. אבל יש לה נקודה בודדת שצריך לאבטח אותה, זה אחד. ושתיים, זה קטע קוד מאוד מאוד פשוט. הקטע שמעביר כסף. חוזה חכם, הוא בעצמו מורכב, זאת אומרת, מישהו כותב תוכנה חדשה. ושם היתה הבעיה. העבירו מאה חמישים מיליון דולר, חמישים מיליון דולר נעלמו. ואז כל רשת האת'ריום היתה צריכה להחליט מה היא עושה. ואז הם החליטו, מכיוון שהם שולטים... זה לא כל רשת האת'ריום, אבל זה מרבית שחקני האת'ריום הגדולים, ישבו ואמרו, אתם יודעים מה? בואו נבטל את החוזה. בואו נשכתב את ההיסטוריה.

יובל: אהה. זאת אומרת מה שלכאורה אמור לא להיות משתנה, שונה.

אור: נכון.

יובל: בשיחה מקדימה בינינו, אמרתי לך, תראה, למרות כל ה-התקטננויות שלך, באמת התקטננויות, חמישים ואחד אחוז, עניינים, תוכנה. זה בסך הכל נראה לי פתרון די מהמם. זה נראה לי פתרון ממש מצוין. בוא נפתור עוד בעיות באמצעות

הבלוקצ'יין, לדוגמא, זכויות יוצרים של מוסיקה. מערכות להצבעה. בוא נשים עוד ועוד דברים על הבלוקצ'יין. ואתה אמרת לי, הלו, לא כל כך מהר. יש פה כל מני בעיות. אחת מהן היא שחלק גדול מהבעיות שאני למשל סתם עכשיו זרקתי אפשר לפתור סתם באמצעות הצפנה, לא צריך בלוקצ'יין. מה זה אומר?

אור: ענף הקריפטוגרפיה, שאנחנו רגילים לחשוב עליו כהצפנה באמת, מתעסק בהרבה דברים. ויש לנו כבר 40 שנה בערך פתרונות לביזור אמון. אפילו בארנקים הדיגיטליים של ביטקוין, את'ריום, מה שאתם משתמשים, יש שימוש באותם כלים לפיצול אמון, לדוגמא, כל מי שמכיר את הנושא של מולטי סיגנצ'רס. זאת אומרת, אני לוקח את הקוד ואני צריך כדי להעביר את הכסף, אני צריך לשים גם את הקוד מהסמארטפון וגם את הקוד שאני שמרתי במחשב וגם את הקוד שהדפסתי בכספת. ו... ו... ו... ו... זה מה שקרוי מולטי סיגנצ'ר. זה כלי קריפטוגרפי לביזור אמון. עכשיו, מה היתרונות של לעשות את כל הדברים הנפלאים שאמרת? הרי מה הבעיה? אני במקום לנהל את מאגר הפטנטים של מדינת ישראל בצורה סגורה ואף אחד לא יודע מי, מה... ופטנטים זה סך הכל דבר שהוא צריך להיות פומבי. בוא נשים את זה על הבלוקצ'יין. רעיון מצוין.

יובל: הינה, בבקשה, בוא נשים את זה על הבלוקצ'יין. מה הבעיה?

אור: אין שום בעיה. רק מה? האם זה הפתרון הנכון? מה קורה? היום להרבה מאוד דברים שצריכים שקיפות, שצריכים ביזור אמון, אומרים, בואו נזרוק את זה על הבלוקצ'יין. הינה, רשם הפטנטים, בואו נשים הכל על הבלוקצ'יין וככה נוכל לסמוך על זה שכשבאמת בקשת הפטנט שלי לבלוקצ'יין חדש חוסך באנרגיה ונפלא ומדהים הגיעה בראשון לינואר, היא באמת הגיעה בראשון לינואר. אבל כאן נכנס הנושא של האמון והנחות העבודה מלמטה. מה זאת אומרת? מישהו שולט בבלוקצ'יין.

יובל: אין מישהו, יש הרבה מאוד אנשים.

אור: אבל הינה, כמו שראינו באת'ריום, היתה קבוצה של אנשים, קבוצה של מספר מסוים של שחקנים, שבאו ואמרו, אתם יודעים מה? אנחנו מבטלים את החוזה החכם.

יובל: וזה קיים גם בבלוקצ'יין? סליחה, גם למשל בביטקוין זה קיים?

אור: זה קרה. זה הפיצול הגדול של הביטקוין לביטקוין וביטקוין קש.

יובל: זאת אומרת, מה שאתה אומר, שהאירועים האלה הם לא אירועים תיאורטיים, זה יכול לקרות. ואז בעצם אתה אומר לי, אי אפשר לתת אמון במערכות האלה?

אור: אז אפשר לתת אמון, כל עוד זה בעיה שהיא מאוד מוגדרת. כשאנחנו מבינים מי השחקנים, מי נגד מי. נגיד במקרה של כסף, ביטקוין. אנחנו מבינים. לך ולי יש אינטרס שלכל אחד יהיה יותר כסף ממה שיש לו קודם.

יובל: אוקי.

אור: והאינטרסים נורא ברורים. והאנליזת סיכונים היא נורא ברורה. אתה עשוי לאבד את הסיסמא. אתה עשוי לאבד את הארנק. יעשו לך תקיפת סייבר לארנק. יש אוסף סיכונים שהוא מאוד מאוד ברור.

יובל: אוקי.

אור: ככל שאנחנו מתרחקים מהדברים האלה, מעולמות התוכן האלה לעולמות תוכן כמו... רישום פטנטים, ראיות דיגיטליות, האיזונים משתנים. החששות משתנים.

יובל: ואז מה קורה? אני, מהרגע שאני לא יודע לזהות את האינטרסים זה יותר בעייתי? כי מה?

אור: כי אז אתה לא יודע כנגד מה אתה צריך להתגונן. בעצם החשיבה הקריפטוגרפית ושוב, יש לנו פתרונות לבעיה הזאת. אנחנו יודעים לקחת בעיה ולפצל את האמון בה. כמעט כל בעיה מעניינת אנחנו יודעים לעשות את זה. ואפילו בדרך כלל

בצורה יעילה. אבל כאן השאלה העיקרית, זה אם אנחנו מבינים מי נגד מי ולמה. וגם משהו שצריך לחשוב עליו, היום אנחנו מבינים המון מהדברים האלה שהם יחזיקו מעמד לשנים רבות. תחשוב רגע על תיק האימוצים של מדינת ישראל שדלף יחד עם אגרון, מי שזוכר את הסיפור. תיק אימוצים זה משהו שצריך להיות חסוי למאה שנה. אנחנו היום מבינים קריפטוגרפיה למאה שנה קדימה, זה תחום מדעי בן יותר משלושת אלפים שנה.

יובל: אוקי.

אור: לעומת זאת בלוקצ'יין זה טכנולוגיה חדשה.

יובל: אז רק בגלל שזה חדש זה מבהיל אותך?

אור: לא. זה לא מבהיל אותי החדש.

יובל: אלא.

אור: מבהיל אותי זה אנליזת הסיכונים והשינויים שצפויים עוד עשר שנים, עוד עשרים שנה. איך הרגולציה תיראה. איך השוק שעומד ממול ייראה. מדברים לדוגמא המון על בוא נעביר את כל הנכסים להיות נכסים דיגיטליים, אני לא מדבר אפילו על NFT, על הבלוקצ'יין המוזר הזה. אלא על דברים כמו בוא נעביר את הטאבו להיות על הבלוקצ'יין.

יובל: אוקי.

אור: כי השקיפות מלאה.

יובל: נכון.

אור: זה יהיה ברור. ואז אנחנו נוכל לעשות חוזים חכמים ונורא נוחים.

יובל: מה הבעיה?

אור: מי עושה לזה רגולציה?

יובל: אה... משרד הפנים, שעושה רגולציה למרשם הטאבו גם כך.

אור: איך הוא יעשה את זה?

יובל: מה זאת אומרת איך הוא יעשה את זה? באיך שהוא עושה רגולציה בדרך כלל, לא?

אור: כשזה מחשבים שלו נורא קל לו לעשות רגולציה.

יובל: אבל מכיוון שפיזרתי את זה, זה כבר לא בידיים שלו?

אור: נכון.

יובל: אהה.

אור: ואם עכשיו יבוא צו בית משפט? היה מקרה בישראל לפני כמה שנים, שמישהו מכר דירה שלא שייכת לו. זייף אישור, ייפויי כוח נוטריוני, מכר דירה שלא שייכת לו. איך אנחנו עושים ביטול של העסקה הזאת? במדינת ישראל. עכשיו, אם זה בלוקצ'יין שהוא רק של הטאבו הישראלי, של מנהל מקרקעי ישראל.

יובל: אז זה אפשרי.

אור: אז זה אפשרי. אבל אז למה מראש צריך את הבלוקצ'יין? שמהנהל ישים דטאבייס אונליין ונסגור עניין.

יובל: אהה. זאת אומרת, זה קצת לסבך משהו שאפשר לפתור אותו בצורה הרבה יותר פשוטה.

אור: נכון.

יובל: אתה גם אמרת שכל המערכת הזאת יוצאת מתוך נקודת הנחה שיש שם בעיה מתמטית שאי אפשר לפתור. אבל אולי יום אחד יפתרו אותה.

אור: נכון.

יובל: איבדת אותי. מה זה אומר? בעיה שאי אפשר לפתור אבל יום אחד יפתרו אותה, מה זה אומר?

אור: אוקי, אנחנו היום משתמשים בבעיות מתמטיות מסוימות כדי לייצר אבטחת מידע.

יובל: אוקי.

אור: אני מניח שחלקכם שמעתם על הצפנה פומבית, על RSA, שלוקחים זוג מספרים ראשוניים, כופלים אותם ועושים משהו עם המכפלה. והקושי הוא לקחת את המכפלה ולהוציא ממנה את הגורמים הראשוניים.

יובל: אוקי, זה בדיוק הבעיה ההפוכה שעליה דיברנו.

אור: נכון.

יובל: אוקי.

אור: יש לנו שלל בעיות מהצורה הזאת, שבהן משתמשים ברשתות בלוקצ'יין שונות, כל רשת בלוקצ'יין יש לה איזה בעיה מסוג דומה. דווקא האנשים הטכנולוגיים עכשיו יתלוננו שזה לא קשור בדיוק. משתמשים ב... אבל ברמת הקונספט זה מספיק קרוב. עכשיו, מה העניין? למה אנחנו משתמשים בהצפנה הזאת? עכשיו, שוב, בלי קשר לבלוקצ'יין. מכיוון שאנחנו מנסים לפתח שיטות למציאת הגורמים הראשוניים כבר מאתיים שנה.

יובל: ועוד לא הצלחנו?

אור: ולא הצלחנו.

יובל: מה יקרה אם יום אחד נצליח?

אור: שאלה טובה. אההה!!!

יובל: ממש ככה?

אור: בערך.

יובל: כי כל המערכות מבוססות על אותה בעיה שאף אחד לא הצליח לפתור?

אור: אז כל מערכת מבוססת על בעיה מסוג קצת שונה, אבל כן. הרבה מהאינטרנט לדוגמא, אמנם היום בעיית הפירוק לגורמים היא קצת פחות דומיננטית, אבל בעיות דומות הן מהוות את עיקר התעבורה המוצפנת, המוגנת. דברים דומים יכולים להיאמר על הבסיסים של רשתות בלוקצ'יין שונות. זאת אומרת, מחר מישהו ימצא דרך לפתור, שם במקרה, במקרה של ביטקוין נגיד, זו פונקציית תמצות שנקראת שם sha256 מישהו יצליח לשבור אותה. יכול להיות שזה יקרה.

יובל: איך ישראל בהקשר הזה? דיברת קודם על הרגולטור, בוא רגע, אנחנו בכל זאת כאן נמצאים. איך הרגולטור הישראלי

מתייחס לסוגית הבלוקצ'יין? מתייחס לסוגיות שעולות כתוצאה מהשימוש בטכנולוגיה הזאת?

אור: קשה לו.

יובל: מאיזו בחינה?

אור: רשות המיסים מתייחסת לזה במובן של השקעות שהם עוד לא ממש יודעים מה לעשות איתן. זה כמו שחקני פוקר. שחקני פוקר כשהם רוצים לשלם מיסים על הרווחים שלהם, יש להם בעיה, כי במדינת ישראל אסור להמר. אז הם עושים איזה תרגיל כדי לשלם מיסים. אותו דבר עם אנשים שעושים רווחים מהפרשי השערים. קנו ביטקוין במחיר אחד ומכרו במחיר אחר, למרות שמדינת ישראל ממש לא תומכת בזה. זאת אומרת, הבנק ישראל לא שש, והוא עכשיו עדיין לא סיים את העבודות הפנימיות שלו למיטב ידיעתי, סביב מה לעשות עם זה. דברים אחרים אנחנו יחסים לא רצים אחרי העולם. בדברים האלה, שוב, לשים את הטאבו, לשים את הבורסה, מי מחזיק איזה מניות. נגיד בהקשר של הבורסה, אחד החששות הגדולים, מכיוון שזה הכל מבוזר ויש גם בלוקצ'יינים יותר אנונימיים מאחרים, יש שוב בעיית רגולציה, אם אני בעל עניין בחברה, יש דברים שאסור לי לעשות, או מותר לי לעשות. ברגע שאני יכול לבזר את האחזקה שלי, להחזיק אותה תחת מספר שמות

שונים, הרגולציה כבר לא יכולה לתפוס את זה בקלות. ולכן יש הרבה בעיות בהתאמה של העולם הרגולטורי החוקי הישראלי, לעולם התוכן הזה.

יובל: אנשי ההייטק המקומיים קצת מתלוננים על האובר רגולציה הזאת? או על היעדר הרגולציה המתאימה לעידן הזה?

אור: זה מורכב. אנשי ההייטק בדרך כלל אוהבים רגולציה.

יובל: נכון.

אור: ובכלל כל רשת הביטקוין היא מאוד ליברטיאנית במובן הזה של...

יובל: בדיוק.

אור: לא צריך רגולציה. מצד שני, יש גם בארץ חברות שמתעסקות ספציפית עבור את'ריום, חברה כמו סטארקוור, שעוזרת בלייצר עוד שכבת אנונימיזציה. והם מבינים את הבעייתיות שגלומה שם. אז יש אנשים שכן מבינים שהעולם, וזה אחד הדברים שעולה בדו"ח שלנו, זה באמת הניסיון לגשר בין עולם התוכן הרגולטורי החוקי לעולם הטכנולוגי. כי בסופו של דבר, וזה נכון לכל טכנולוגיה, אנחנו רואים את זה גם עכשיו עם פייסבוק, וכל סוגיית טראמפ.

יובל: אהה.

אור: יש רגולציה, הטכנולוגיה לא יכולה להתקיים בלעדיה. תוך התעלמות ממנה. היא יכולה להשפיע. אבל היא לא יכולה להתעלם.

יובל: אז בוויכוח הזה בין אותן חברות שרוצות לרוץ קדימה, לבין המדינה שאולי קצת מחזיקה אותן, איפה אתה עומד ב...?

אור: אני יותר נוטה לכיוון של המדינה פה, פשוט כי בלוקצ'יין, ברוב המקרים יש לנו פתרונות יותר טובים. אבל כאן הנקודה המהותית. זה נורא קשור לחסמים הלוקאליים, זאת אומרת, יכול להיות מצב שמישהו בא ואומר, כרגע יש לי בעיית חסמים מאוד מאוד מסוימת שאותה שקיפות או אותה פומביות של המידע יכולה להיפתר על ידי הבלוקצ'יין. יכול להיות שהפתרון הוא בוא נשים את המידע פומבי, לא על הבלוקצ'יין. וכאן צריך נורא להיות זהירים, מכיוון שנגיד אם מעבירים את כל הטאבו להיות על הבלוקצ'יין. החזרה אחורה היא בעייתית.

יובל: יכולה להיות בעייתית. איפה זה נכנס בעולם?

אור: אז בעולם באמת רואים בלוקצ'יינים שמנסים לפתור, נגיד, הנושא של... בהקשר של ספנות זה בעיקר חוזים חכמים, באמת שחרור, אני שילמתי את הכסף לפני שאני מקבל את

מסמכי השחרור מהמכס. מה שהיום עושים דרך עמילים ודרך כל מני מנגנוני נאמנות. אז אפשר לעשות את זה על הבלוקצ'יין. יש ניסיונות לשים מידע רפואי על הבלוקצ'יין. גרמניה עכשיו מנסה לעשות לדוגמא את האפליקציית רמזור, התו הירוק שלהם, על חמישה בלוקצ'יינים. לא אחד, חמישה בלוקצ'יינים, כדי שהמידע יהיה נגיש מכל מקום בעולם, תמיד איך שהוא בצורה מסוימת.

יובל: אני חושב שבדקות האחרונות אני הבנתי למה בלוקצ'יין הוא מעניין, אבל גם למה הוא בעייתי. ומצד שני נראה שיש המון המון התלהבות מהדבר הזה. יותר ויותר נושאים ותחומים רוצים להעביר לבלוקצ'יין, אתה יכול להסביר את פשר ההתלהבות בהינתן כל הבעיות שעכשיו דיברנו עליהן?

אור: זה יותר קשור שוב לנושאים של הייפ במובנים מסוימים. זה קשור לרצון להיראות חדשני. אם אנחנו עכשיו נשים את כל המידע הרפואי של אזרחי ישראל על הבלוקצ'יין, איזה חדשניים אנחנו.

יובל: יש מקום מסוים שאתה עוד לא רואה את העולם של הבלוקצ'יין, אתה לא רואה את היישום עושה שימוש בבלוקצ'יין ואתה אומר, רגע, זה דווקא כדאי לשים על הבלוקצ'יין? או שאין איזה שהוא מקום כזה שאתה מאתר?

אור: אז במקומות שבהם ברור לנו מי נגד מי. באותם מקומות שברור לנו שאין לנו צורך ברגולציה יוצאת דופן. זה דרישה ראשונה. ומקומות שבהם באמת אין על מי לסמוך.

יובל: בכל שאר המקרים אתה אומר, או שיש פתרונות אחרים, או שתעזבו אתכם מהבלוקצ'יין, זה פתרון לא מתאים.

אור: כנראה שיש פתרון יותר יעיל ויותר בטוח.

יובל: רגע לפני שאנחנו נפרדים, אני רוצה לשאול אותך שאלה שבעיני היא אולי קצת פילוסופית אפילו. אנחנו, במרכז הדיון שלנו נמצאת המילה אמון, כן? הרבה אמון, אין אמון בכלל. וכדומה. השאלה האם הבלוקצ'יין בעצם לא מחליף אמון בדבר אחד וגורם לי לתת, מחייב אותי, לתת אמון בדבר אחר. זאת אומרת, אני מחליף את האמון במוסדות, במס הכנסה, בביטוח לאומי, בטאבו, בבנק. ובמקום זה, אני עכשיו צריך לתת אמון בשרתים, בתוכנות. בקוד מחשב. בסך הכל החלפתי משהו במשהו. לא?

אור: זו אבחנה נהדרת, מכיוון שזה בעצם הבק סטייג', מאחורי הקלעים של בלוקצ'יינים. תחשוב לדוגמא על הצבעות. הינה, עשינו לא מזמן מערכת בחירות. מערכת הבחירות הישראלית, אנחנו סטארט אפ ניישן, כל הזמן אומרים, בואו נעבור

לבחירות אלקטרוניות. אפשר לשים את זה על הבלוקצ'יין. בשיטה הישראלית, היא נורא פשוטה. אתם באים, מצביעים, יוצאים, בסוף היום סופרים את הקולות בקלפי.

יובל: יש פתקים. יש נייר.

אור: יש. יש פתקים, יש נייר. כל ילד בכיתה ד' ידע לעשות את הסכימה של כמות הקולות במדינת ישראל.

יובל: ופה תוכנה תדע לעשות את הסכימה, מה הבעיה?

אור: אבל מי כתב את התוכנה?

יובל: זאת אומרת, אני צריך לתת אמון במי שכתב את התוכנה.

אור: כתב את הקוד. ואתה צריך לתת אמון במי שנתן לו את החומרה. ואתה צריך לתת אמון, בסופו של דבר בפרוטוקולים. ואתה צריך לתת אמון שאף אחד לא בודק מי הצביע מה. זאת אומרת, אם בהצבעה בפתק נייר שמים את זה בתוך מעטפה ומנערים את הקופסא ואז אי אפשר לדעת מה אתה הצבעת. בהצבעה אלקטרונית יש בוודאי איזה לוג שאומר, יובל הצביע בשמונה וחצי ובשמונה וחצי מישהו הצביע לאיגוד האינטרנט הישראלי. היכולת של מישהו לבוא אחר כך ולעשות בדיקה מאוד מאוד פוחת. ואז מה שקורה, במקום שכל אחד יוכל לבדוק את הבחירות וכל אחד יכול להיות משקיף. יש איזה

אסופת מכשפים, מומחי קריפטוגרפיה ואבטחת מידע, שנכנסים מאחורי הפרגוד ובאים ואומרים, הבחירות האלה היו בסדר. אותו דבר בביטקוין ובבלוקצ'יין, המרנו באמת את האמון באותם גופים שאני יכול לבדוק ואנחנו מכירים ומבינים אותם. ספיצית נגיד במקרה של ביטקוין, מסתמכים נורא על פונקצית התמצות sha256 למי שלא יודע, sha256 תוכננה על ידי ה-NSA, נשיונל סקיוריטי אייג'נסי, בסוף שנות ה-90.

יובל: בין בנק לביטקוין, מה ההעדפה האישית שלך? על מי אתה סומך יותר?

אור: אני שמעתי על ביטקוין כשזה היה שווה סנט.

יובל: אוקי. ולא קנית?

אור: ולא קניתי. כשזה היה מאה דולר, גם לא קניתי. גם עכשיו טרם קניתי.

יובל: כי אתה לא סומך? כי אתה לא נותן בו אמון?

אור: לא, כי בניהול הסיכונים שלי אני יותר מדי מושקע בטכנולוגיה, אז אין לי צורך להוסיף. אבל יש לי חבר שצוחק עלי כל הזמן, כי הוא קנה את זה כשזה היה שווה ארבעים דולר וטרם מכר.

יובל: פרופסור אור דונקלמן תודה רבה לך. אני חושב שיצאתי קצת יותר חכם לגבי הבלוקצ'יין. אני לא יודע כמה זמן אני אצליח להחזיק את ההסבר הזה בתוך הראש שלי, כי זה מסוג הדברים שבאים ואז נעלמים. אבל אני חושב שהיום יצאתי יותר חכם. עד כאן נקודה IL. הפודקאסט של איגוד האינטרנט הישראלי שעוזר לנו להבין מה הן השפעות העומק של האינטרנט על החברה, הכלכלה, הפוליטיקה והתרבות. אני דוקטור יובל דרור. נשתמע בפעם הבאה. אם אתם רוצים לדעת עוד על הנושא שעליו דיברנו וגם על נושאים אחרים, היכנסו לאתר האינטרנט של איגוד האינטרנט.

www.isoc.org.il. זה www.isoc.org.il. באמצעות האתר תוכלו גם להצטרף לקהילת החברים של איגוד האינטרנט הישראלי ולתמוך בהמשך עבודת האיגוד לשמירה על אינטרנט בטוח, חופשי ושוויוני לכלל החברה בישראל.

סיום הקלטה