

ביטקוין: הצעה לכלכלת העתיד

יעילותם ואמינותם של המטבעות הדיגיטליים, יחד עם בשורת החירות האישית שבכנפיהם, מאיימים על מוסדות המדינה המוכרים. גיבוש מדיניות כלכלית-טכנולוגית עדכנית אינו יכול להידחות עוד

אם אינכם יודעים מהו "ביטקוין" (bitcoin), או אם מעולם לא עלה על דעתכם לקנות אחד או יותר, הרגישו בנוח: לרבים, אולי לרובה המוחלט של אוכלוסיית העולם, אין מושג במה מדובר. ייתכן ששמעתם על הביטקוין אך תהיתם: האין זה כסף דמיוני שאין מאחוריו מאומה?

ובכן, הביטקוין הוא מציאות ממשית לחלוטין. הוא משגשג וגדל במהירות, ובדרכו מטלטל את השוק הפיננסי כולו טלטלה הגונה. הביטקוין כאן כדי להישאר, ונראה כי הוא עתיד לעצב את חיינו באופן עמוק ויסודי.

מהו ביטקוין ומהו כסף?

ביטקוין הוא המצאה חדשה ודרמטית, ומאז נולד ב-2009 הוא אינו חדל מלזעזע את אמות הסיפים של הכלכלה והטכנולוגיה. רבים אמרו אז, ועדיין אומרים היום, כי "זה רק משבר קטן וזה חולף", אולם כוחו של הביטקוין וערכו הולכים וגדלים והמשמעות שלו מרחיקת לכת. הוא אינו מכה קלה בכסף, אלא המצאה שעתידה להשפיע על כל היבט בחיינו.

בפשטות, אפשר לראות את הביטקוין כ"זהב דיגיטלי" שיש לו יתרונות רבים לעומת כסף מזומן או זהב, אבל חיסרון בולט אחד: אי אפשר לעשות ממנו עגילים...

הביטקוין בא לעולם כדי לפתור בעיה יסודית ועתיקה, והיא: כיצד לשמור על הכסף שלנו באופן מוחלט.

דעאל שלו הוא יום פינטק (הייטק פיננסי), בלוגר ("מר קדמוני"), מחבר הספר "הסוד הקדמוני" וממובילי קהילת הפליאו בארץ. ספרו החדש עומד לצאת בהוצאת כנרת זמורה ביתן.

לפני שנבין כיצד שומר הביטקוין על הכסף שלנו, כדאי שנבהיר מהו כסף בכלל ומה נותן לו את ערכו. נתחיל דווקא מהזהב, ידידנו הוותיק והמנצנץ, המשמש מטבע עובר לסוחר כבר אלפי שנים. הסיבה לכך היא שמאז ומתמיד ידעו בני האדם כי זהב הוא מצרך נדיר שאינו מתגלגל סתם כך ברחובות והמצאי שלו מוגבל למדי – ולכן ייחסו לו שווי. זהב אינו יודע לעשות שום דבר יותר מאשר כל חתיכת מתכת אחרת, או פיסת אבן, שגם מהם אפשר לעשות תכשיטים; ברור שהנדירות שלו והקושי לכרות זהב חדש, ומאידך פשטות המסחר בו, הם אלו שהעניקו לו את ערכו. המוסכמה העולמית קובעת כי אם מוצר מסוים הינו נדיר וקשה להשגה, אזי יש לו ערך או שווי – בדומה ליהלומים ולמחצבים נדירים או לקלפים עם חתימות של שחקני בייסבול. ואכן, הזהב הוא דוגמה טובה לכל התכונות הנדרשות מכסף עובר לסוחר: הוא מוגבל ואפילו נדיר, וזהו התנאי הראשון לכך שמשוה יוכל לשמש ככסף (אחרת, היינו סוחרים באבנים); הוא עמיד, שהרי אין לו תאריך תפוגה והוא נשמר אלפי שנים; הוא נייד, כלומר אפשר להעביר אותו מיד ליד בין אנשים, ולכן גם לסחור בו; הוא אחיד ובר-החלפה בכל מקום (גרם זהב הוא גרם זהב, ואין זה משנה באיזה גרם ספציפי מדובר); ולבסוף, הוא ניתן לחלוקה, כלומר אפשר לקנות אונקיית זהב, ואפשר גם יותר או פחות. כל התכונות האלה הופכות אותו גם למקובל, כלומר לכך שאנשים מקבלים אותו כשווה ערך.

מסיבות אלו, כבר לפני חמשת אלפים שנה החלו בני האדם להשתמש בזהב (ולעיתים גם במתכות אחרות) כאמצעי תשלום, ומטילי זהב במשקלים שונים שימשו מאז כאמצעי תשלום מקובל לכל סחורה. ההערכה הייתה פשוטה: ככול שמשקל הזהב גבוה יותר, כך ניתן לקנות בו סחורה בעלת ערך רב יותר. רק בשנת 600 לפני הספירה נוצרו המטבעות הראשונים, ואלו נטבעו בחותם מלכותי שהעיד על טוהר המתכת ומשקל המטבע. המטבעות הפחיתו מאוד את עלויות המסחר (לא היה עוד צורך לשקול מטילי מתכת או לחלק אותם לפיסות לצורך עסקאות קטנות כמו רכישת קילו תפוחים), הקלו על נידוד ההון ועל קביעת ערך לפריטים. המטבעות השתלטו על העולם, ומאז ועד לפני כמאתיים שנה העיקרון נותר זהה: המטבעות המשיכו לשמש לפי ערכם במשקל המתכת שבה נוצקו. הפני האנגלי היה עשוי מכסף עד שלהי המאה ה-18, ואילו הסנט האמריקני הראשון נטבע בנחישות.

במקביל, עם התפתחות המסחר והמצאת הדפוס, החלו להופיע אמצעים שהחליפו את השימוש הישיר במטבעות ממתכות יקרות. במקום להתמודד עם העלויות הנכבדות של הובלת מתכת או להסתכן בשוד דרכים, גופים שונים הנפיקו שטרי חוב שאפשרו לזכות בהון הזהב גם מבלי לשאת אותו באופן פיזי.

רק באמצע המאה ה-19 החל המסחר במטבעות ממתכות פשוטות, שערכם הנקוב גבוה ממחיר המתכת שהם עשויים ממנה – בדומה למטבעות שבהם אנו משתמשים כיום. המעבר בין סוגי המטבעות התרחש רק לאחר אלפי שנות מטבעות כי הוא דרש מההמון שינוי יסודי בתפיסת מהות הכסף. בעבר הכסף היה מוצר נדיר מטבעו, כמו



מתכות יקרות, ואילו המטבעות החדשים שהציעו המדינות הן מוצר נדיר רק בגלל החלטה שלטונית, שהרי אין כל בעיה לייצר אינסוף מטבעות ממתכות זולות. לכן הנפקת מטבעות פשוטים התרחשה רק לאחר ביסוס כוח שלטון מוחלט, ורכישת אמון הציבור בכוח המדינה ובהוגנות שלה. ללא יציבות שלטונית, מי יערוב בידי התושבים כי באמת יש ערך ממשי ממתכות נדירות במרתפי המדינה כנגד כל מטבע ממתכת זולה? רק כשהושג האמון, נוצרה קפיצת המדרגה.

היה זה שלב דרמטי בתהליכי ההפשטה שעבר הכסף ובהרחקתו מהבנתם של רבים מבני התמותה. למעשה הודיעה המדינה לתושבים כי מטבעות המתכת האפורים אינם אלא ייצוג של הזהב האמיתי הטמון במרתפיה; ובאותה הזדמנות הוסיפה והציעה: אם כבר ייצרנו מטבעות-כמו-זהב, הבה נדפיס גם שטרות-כמו-זהב, ומעתה ואילך רק המדינה תהיה רשאית להדפיס שטרי חוב. אף שהזהב אינו ניכר מן השטרות או מן המטבעות האפורים, עדיין כל מדינה החזיקה זהב פיסה כנגד המטבעות והשטרות שהיא הדפיסה (כלומר, הייתה ערובה שלמדינה יש יכולת לשלם בזהב אמיתי את הכסף שמצויר על השטר).

אולם בשנות השבעים של המאה הקודמת תקן הזהב ננטש. מאז ועד עתה, מטבעות ושטרות אינם מייצגים עוד זהב אלא אך ורק את הבטחתה של המדינה לכבד את הכסף ולא להדפיס ממנו כמויות גדולות מדי. כסף כזה נקרא "כסף פיאט" – על פי הביטוי הלטיני "פיאט" (Fiat) שמשמעו "[המלך אמר] שכך יהיה". כסף הפיאט כלל אינו מתיימר להיות מגובה בזהב, אלא הפך לכלי שלטוני המכוון ומרחיב את ההון לפי החלטת הריבון ולא לפי בוחן המציאות. למרות זאת, כל עוד כולנו מסכימים להחליף סחורה או שירות בתמורה לכסף כזה וכולנו סומכים על המדינה ומוסדותיה – לכסף פיאט יש ערך. אכן, כפי שנראה, כסף פיאט לא פתר את הבעיות המלוות את הכסף מראשית ימיו ואף יצר בעיות חדשות.

בעיות בשמירת ההון

כאשר יש לנו הון, אנו רוצים לשמור עליו, לטובתנו ולטובת הדורות הבאים. לשם כך נוכל לקנות בתיים, קרקעות או מניות, אבל אם אני רוצה לשמור חלק מההון בצורת כסף נזיל ועמיד, יש לי שלוש בעיות קשות ביותר: האחת, איך אני יודע שהכסף הוא אמיתי ולא מזויף. השנייה, איך אני מוודא שהכסף שלי יישאר רק שלי; כלומר, בעיית רישום הבעלות על הכסף. השלישית, איך אני יודע שהכסף שלי יהיה שווה גם בעתיד ולא יאבד את ערכו.

כדי לפתור את הבעיה הראשונה, בעיית הזיוף, מדינות משקיעות מאמצים רבים ביצירת כסף שקשה לזייף: סימני מים או חוטי כסף בשטרות, זיזים במטבעות ועוד

מיני המצאות. לפעמים הפתרונות הללו מועילים; לפעמים פחות.

הבעיה השנייה, בעיית רישום הבעלות על הכסף, קשה יותר. כדי לפתור אותה אנו מפקידים את כספנו בבנקים, כלומר במוסדות שאנחנו סומכים על מה שרשום אצלם "בספרים", ורואים ברישומים אלו את מה שקובע האם סכום כסף שייך לי או למישהו אחר. לדוגמה, אם בחשבון הבנק שלי רשומה יתרה חיובית של מאה אלף שקלים, זהו הכסף "שלי", ואני סומך על הבנק שיוודא כי אין בו פקיד (דוגמת אתי אלון) שירשום לי יתרה שלילית של מאה אלף שקלים. כלקוח, אין בידי כל יכולת לסתור את מצב החשבון המופיע בספרי הבנק, וכל זאת אף על פי שכספי אינו מוחזק באמת בבנק. למעשה, רק אחוז קטן מההון מוחזק על ידי הבנקים כמזומן, ובפועל אין אצלם לא מטבעות ולא שטרות, אלא רק רישומים, תדפיסים ועמלות שורה. הבנק מחזיק בעברנו רק ייצוג של הכסף.

הבעיה השלישית, בעיית השמירה על שוויו של הכסף, היא החמורה ביותר וגם המוכחשת ביותר. כאמור, לא רק בבנק אין כסף אלא גם באוצר המדינה. מאחורי מטבעותיה ושטרותיה של המדינה אין מאומה מלבד הבטחת ה"פיאט": "שכך יהיה". ואכן, חסרונו העיקרי של כסף פיאט מוכר לכולנו: יש סיכוי כי יום אחד – מתוך משבר כלכלי, מצב לוחמה או חוסר אחריות – תבחר המדינה להנפיק מטבעות ושטרות רבים ולכן ערכם ירד בחדות. זה נקרא "אינפלציה".

הבטחתה או יציבותה של המדינה עלולות להיעלם כקיקיון, בן לילה. לעתים קורה כי למדינה אין כיסוי לכסף שהיא עצמה הדפיסה. בוווצואלה, למשל, התעוררו האזרחים בבוקר אחד וגילו שהמטבע שלהם לא שווה כלום, ושהבנקים סגורים בהוראת הממשלה ועל פתחיהם עומדים חיילים. זה קרה גם ביוון. לפני שנה זה קרה לאנשים בהודו, שמחקה מהמסחר חלק מהשטרות וסגרה את הבנקים. ממשלת קפריסין הלאימה חלק ניכר מהפקדונות הפרטיים לכיסוי גרעונותיה.¹ אולי זה יקרה מחר לגרמנים, שיתעוררו ויגלו שהצרפתים החליטו לפרוש מגוש האירו ובן לילה שווי המטבע שלהם, האירו, יימחק. גם מלחמה כוללת עלולה לערער את יציבותה של המדינה. האם מאומה מאלו לא יכול להתרחש גם בישראל?²

סיכום ביניים: הצגנו שלוש בעיות לגבי כסף – מניעת זיוף, רישום הבעלות על המטבע, ויציבות הגוף המנפיק את הכסף. בינואר 2009 קם סאטושי נאקמוטו (שם בדוי. עד היום אין איש אינו יודע מי הוא או היא) והמציא את הביטקוין, שפותר את שלוש הבעיות הללו באופן מדהים, על ידי מודל המבוסס על הרבה מתמטיקה וקריפטוגרפיה (מדע ההצפנה). למזלנו, לא צריך לדעת לא מתמטיקה ולא קריפטוגרפיה כדי ליהנות מההמצאה או להעריך את השלכותיה.

ביטקוין - פתרון אלגנטי לשלוש הבעיות

אז מה יצר אותו סאטושי נאקמוטו? ההמצאה שלו מורכבת מכמה רבדים השזורים זה בזה, ואנו ננסה לעבור על העיקריים שבהם בקצרה. בבסיס ההמצאה עומדת היכולת המהפכנית לייצר מוצר דיגיטלי שהוא נדיר, מוגבל ובלתי ניתן לשכפול או לזיוף. לכאורה, זהו דבר והיפוכו. אנו רגילים לחשוב על מידע דיגיטלי כמשהו שקל ופשוט ליצור ממנו עותקים. למשל שכפול תמונות, מסמכים, וכל מידע ששמור במחשב כלשהו. והנה בא סאטושי והציע מערכת אמינה המציעה מוצר דיגיטלי בעל כל התכונות הנדרשות לכסף: נדיר, עמיד, אחיד, ניתן לחלוקה, מאובטח, והיום גם מקובל לחלוטין.

הנה כך זה עובד:

סאטושי נאקמוטו הציע מנגנון שמייצר מוצר נדיר תמורת מאמץ חישובי משמעותי. ביטקוינים נוצרים בתהליך הנקרא כרייה, בדיוק כמו כרייה של זהב. אפשר לירות מטבעות ביטקוין חדשים על ידי השקעה של אנרגיה טהורה (כוח עיבוד של מחשבים) בפתרון "חידה" מתמטית. מכיוון שיקר וקשה מאוד לייצר את המטבעות הללו ובלתי ניתן מתמטית לזייף את תהליך ייצורם או לשכפל אותם, הם נדירים ולכן אנשים מעניקים להם ערך – בדיוק כמו לזהב. עוד עשה סאטושי בחוכמה והגביל את סך המטבעות העתידי, כדי שלא יהיה פיחות בשווי המטבעות. פרוטוקול הביטקוין קובע כי סך המטבעות האפשריים אי פעם יהיה 21 מיליון מטבעות. זהו. לצורך ההשוואה: איננו יודעים במדויק כמה זהב עדיין קבור במעמקי האדמה, ומובן שאיננו יודעים כמה דולרים יחליט הממשל האמריקני להדפיס השבוע. כמות הביטקוינים העתידיים, לעומת זאת, היא סופית ומוחלטת.

אבל, כמו לגבי כל כסף: כיצד נדע שכל ביטקוין הוא אמיתי ולא מזויף? ובאיזה אופן תירשם הבעלות על המטבע? סאטושי פתר את שתי בעיות היסוד הללו באופן אלגנטי, המחבר את מנגנון הכרייה של המטבעות למנגנון רישום הבעלות על המטבע.

אמר סאטושי: הבעלות על המטבע תיכתב ב"ספר עסקאות" (ledger) שיתופי ופומבי, ברשת; ובמקום שכל בנק ינהל רשומות משלו (בסגנון: "לפלוני, בעל מספר חשבון 123, יש מאה אלף שקל בבנק"), יהיה לנו "ספר ביטקוין" שיתופי, פתוח וציבורי. בספר זה, שיהיה זמין ופתוח באינטרנט, תירשמה כל העסקאות של כל האנשים, ועותקים ממנו יהיו ברשות כל מי שירצה. כך נפתרת הגדרת הבעלות על הכסף שכן אם לכולם יש עותק של אותו ספר ואצל כולם כתוב שיש לי עשרה ביטקוינים, כי אז אכן יש לי עשרה ביטקוינים: אי אפשר להתווכח על כך, ואף פקיד בנק אינו יכול לרמות אותי.

כאשר אני משלם עם ביטקוין, אני בעצם מעביר מטבע מהארנק שלי לארנק של מישהו אחר, בדומה להעברה מחשבון בנק אחד למשנהו; ובאותו רגע אני בעצם

מספר לעולם כי "ארנק מספר 987 העביר 1 ביטקוין לארנק מספר 543". כעת, עסקה זו צריכה להיכתב בספר השיטופי, הנקרא "בלוקצ'יין" (blockchain), שכאמור, חשוף בפני כולם. הבלוקצ'יין נמצא באינספור עותקים שכן כל אחד יכול להוריד אותו למחשב שלו, ומצויה בו ההיסטוריה של כל עסקאות הביטקוין שנעשו אף פעם. לאחר שנעשתה עסקה בביטקוין, היא משודרת מיד לרשת וכולם רואים אותה, אך כדי שהיא תהיה סופית ומוחלטת עליה להירשם בבלוקצ'יין – ומכאן ואילך זו תהיה ההוכחה הפומבית לבעלות על המטבע.³

אבל מי יכתוב זאת בבלוקצ'יין, וכיצד אוודא שהעסקה שלי אכן תירשם בו? ובכן, זהו לב העניין: לשם כך המציא סאטושי ידידנו מנגנון הכולל יצירת ביטקוינים חדשים, תמרוץ, חישוב מתמטי ופיקוח הדדי.

הכתיבה בבלוקצ'יין היא תהליך של רישום עסקאות, שבה בעת גם יוצר מטבעות חדשים בתהליך הכרייה הנוכרי. הכרייה תלויה ביכולתם של מחשבי הכורה לפתור מעין חידה שפתרונה מבטיח שני דברים: הכורה שמחשבו פתר את החידה הוא זה שיכתוב את העסקה בספר, והוא זה שירוויח מכך עמלה וביטקוינים חדשים.

מן הרגע שהעסקה משודרת אל הרשת (קרי: "א' קנה ביטקוין מ-ב'") היא פומבית וגלויה לכל מי שמחובר לרשת. בתוך כמה דקות מתחילה תחרות בין כל הכורים לרישום העסקאות שנוצרו בדקות האחרונות. כל אחד ממחשבי הכורים מנסה לייצר בלוק חדש ולכתוב אותו בבלוקצ'יין. הבלוק החדש כולל את כל העסקאות שנעשו בדקות האחרונות אך עדיין לא נרשמו בבלוקצ'יין; אולם כדי שכורה יוכל להוסיף את הבלוק החדש אל הבלוקצ'יין, וכך לרשום את העסקאות, עליו למצוא ביטוי מתמטי שייצג את הבלוק. מציאתו של ביטוי מתמטי כזה ("פתרון החידה") היא תהליך הדורש משאבי מחשוב רבים מאוד, משום שמדובר בחישוב מורכב אשר פתרונו דורש כעשר דקות בממוצע; וככל שהמחשבים נעשים חזקים יותר, גם האתגר הופך קשה יותר, כך שתמיד נדרשות כעשר דקות בממוצע כדי "לפתור" את האתגר ולייצר בלוק חדש. הכורה הראשון שמצליח במשימה כותב את הבלוק החדש, הכולל את כל העסקאות האחרונות, בבלוקצ'יין, וזוכה בעמלה וביטקוינים חדשים. במקביל, משודר הבלוק החדש לכל הכורים האחרים ברשת, וכולם מוסיפים אותו לעותקי הבלוקצ'יין הנמצאים אצלם – לאחר שווידאו שהבלוק אכן תקין. אפשר לחשוב על החישוב הנדרש כפתרון תשבץ: קשה מאוד לפתור אותו, אך אם מישהו כבר פתר את התשבץ, ניתן לוודא בקלות ובמהירות שהפתרון נכון.⁴

מנגנון התגמול הזה מבטיח תמרוץ חיובי לביצוע הכרייה, כלומר מתמרץ עוד ועוד שחקנים להשתתף במשחק וממילא יוצר בלוקצ'יין אמין ועמיד. המנגנון גורם גם לכורים להשקיע ערך אובייקטיבי, שהוא האנרגיה (חשמל) המושקעת במאמץ החישובי הנדרש לרישום הבלוק. ערך זה נקרא "הוכחת העבודה" (Proof of work)

כלומר הוכחה שהכורים השקיעו אנרגיה כדי לרשום את העסקה, ולכן גם אי אפשר להעתיק או לזייף ביטקוין. המנגנון עובד בצורה תקינה משום שיש בו פיקוח הדדי: אם הכורה "הזוכה" יצר בלוק לא תקין, הכורים האחרים יגלו זאת מיד, כאשר יודאו את תקינות הבלוק, והוא יפסיד את העמלה ואת הביטקוינים החדשים. לכן, על אף שישנה תחרות מובנית בין הכורים, ועל אף שאין שום גוף ריכוזי או מפקח, כולם פועלים תחת אותה חוקיות ובתוך אותה מסגרת.

השיטה הזו מבטיחה קונצנזוס מבוזר. אין אף גוף אחד שמרכז את העסקאות בבלוקצ'יין, וכל אחד יכול להשתתף ולכרות ביטקוין בעצמו או להוריד למחשב שלו עותק של הבלוקצ'יין, ועדיין כולם משחקים בכפוף לאותם הכללים. הביזוריות מבטיחה כי המערכת תהיה חזקה ובעלת שרידות עצומה, שכן אף אחד בעולם לא יוכל אי פעם לסגור אותה, בדיוק כשם שאי אפשר "לכבות את האינטרנט". הביטקוין הוא רשת עולמית פתוחה ומבוזרת לחלוטין שאינה מנוהלת על ידי איש.

נוסף על כך, השיטה פותרת את בעיית הבעלות על המטבע. ספר העסקאות הוא מסמך ציבורי שכולם מסכימים עליו, ואף אחד אינו יכול לזייף אותו – משום שכל בלוק שנכתב חייב לצטט את הבלוק שהיה לפניו וכך היסטוריית העסקאות נעשית עמידה וסופית. זוהי הגנה על ידי מתמטיקה: ככל שנכתבות עסקאות נוספות, כלומר נוספים עוד בלוקים אל הבלוקצ'יין, המאמץ החישובי הנדרש כדי לשנות את הבלוקים הקודמים, או לזייף אותם, הוא בלתי אפשרי מעשית.⁵

כך נפתרו שתיים מתוך שלוש בעיות היסוד של הכסף: כיצד להבטיח שהמטבע שלי אינו מזויף וכיצד לאשרר מיהו הבעלים של הכסף בכל רגע ורגע. החישוב הנדרש לצורך רישום התנועה בבלוקצ'יין הוא ההוכחה שהמטבע אמיתי ולא מזויף, והעובדה שהעסקה רשומה בבלוקצ'יין מוכיחה מיהו הבעלים של המטבע בכל רגע נתון (מספר ארנק כך וכך).

כזכור, הבעיה השלישית שניצבה בפנינו הייתה כיצד נבטיח את אי-שחיקת הכסף ואת יציבות הגוף המנפיק את המטבע – כנגד משבר כלכלי או קטסטרופה פוליטית. בעיה זו נפתרת מאליה משום שבביטקוין אין כל גוף מרכזי המנפיק את המטבע. הביטקוין הוא תוכנה בקוד פתוח שאומצה על ידי מאות אלפי משתמשים ואשר פועלת רק על סמך המתמטיקה – ולכן בלתי ניתנת לסגירה כפויה ולעולם לא ניתן יהיה "לבטל את הביטקוין". אין זה משנה מה יהיו הלחצים הפוליטיים, מטבע הביטקוין חסין וימשיך לפעול כל עוד יהיו משתמשים המעוניינים בו ויש להם מחשבים (או טלפונים) המחברים לרשת האינטרנט. יתרה מזאת, הביטקוין עמיד לחלוטין בפני אינפלציה. כאמור, סך כל מטבעות הביטקוין העתידי מוגבל ל-21 מיליון מטבעות. כיום, יש כבר 16.5 מיליון מטבעות, ובכל עשר דקות מתווספים עוד מטבעות אל המחזור, כחלק מפעולת הכרייה. למעשה, אפשר לחשוב על זה כדופק: ליבו של הביטקוין פועם

בקצב של עשר דקות (שכן מדי עשר דקות בממוצע נכתב בלוק חדש בבלוקצ'יין). בכל פעימה כזו מתווספים מטבעות לשוק, והקוד מכתוב כי מדי ארבע שנים יורד קצב היצירה בחמישים אחוז: בהתחלה נוצרו חמישים מטבעות חדשים מדי עשר דקות; כעבור ארבע שנים ירד הקצב ל-25 מטבעות מדי עשר דקות; כיום, הקצב הוא 12.5 מטבעות (כלומר כ-1800 ביטקוינים חדשים מונפקים מדי יום); וביוני 2020 עתיד הקצב לרדת ל-6.725 מטבעות מדי עשר דקות, וכך הלאה בטור יורד. כרייתם של 21 מיליון המטבעות עתידה להסתיים בשנת 2140, ואז תמריץ הכתיבה בבלוקצ'יין יינתן רק תמורת עמלות הכורים ולא בעבור יצירת מטבעות חדשים – אך עם זאת יתמודדו רק נכדי נכדנו.

ביטקוין דומה לכסף מזומן, אבל אפשר להשתמש בו רק אם יש מפתח סודי. את המפתח מחזיקים בארנק. מפתח הוא מספר אקראי סודי וארוך. אם תטילו מטבע 256 פעמים ותורשמו בכל פעם את התוצאה, 0 או 1 (עץ או פלי), תקבלו מספר אקראי (רנדומלי) לחלוטין שאי אפשר לנחש אותו. המספר הזה הוא הבסיס למפתח הסודי שלכם, וממנו, על ידי עוד קצת מתמטיקה, נוצר גם מספר הארנק, שהוא הפומבי. בארנק שומרים את המפתח הסודי. בעולם הביטקוין, מי שמחזיק במפתח מחזיק בכסף; ולהפך, מי שרכש ביטקוין ואיבד את המפתח לא יוכל לעולם להשתמש בכספו. לשם הפשטות חשבו על חשבון הבנק שלכם: אם קרה ששכחתם את הסיסמה, אינכם יכולים לגשת לכסף שלכם. בבנקים "רגילים", אפשר ללכת לפקיד, להציג תעודת זהות ולשחרר את הכסף; אולם בביטקוין אין אפשרות כזו, שכן אין שום גוף מנהל, אין פקידים ואין ממשלות. ארנק הביטקוין הוא לכן המפתח, תרתי משמע, לכסף שלכם. המפתח הוא הכול, והמפתח הוא לעולם אישי ואנונימי.

יתרונות מפתיעים

אין די בפתרון הבעיות הקלאסיות של הכסף הישן כדי להסביר את זינוקו המטאורי של הביטקוין. הביזוריות שלו ומנגנון הפעולה השקוף הם הרקע לאחת מתכונותיו הבולטות: האנונימיות. בבלוקצ'יין אין חשבונות בנק ואין כתובות או שאר פרטים מזהים; מצויה בו רק שורה ארוכה של קודים במבנה קבוע וההעברות שבוצעו ביניהם. כך, באופן מפתיע, למרות פומביותו של ספר העסקאות, אף אחד מלבדכם אינו יכול לדעת מהו מספר הארנק שלכם וכמה כסף מסרתם או קיבלתם. בעולם הביטקוין אין אנשים, אין בנקים ואין ממשלות; יש רק ארנקים, מפתחות לפתיחתם וסכומי כסף המועברים ביניהם. אומנם, הביטקוין נחשב למטבע "אנונימי למחצה", שכן ניתן להתחקות אחר מסלול התנועה של הכסף בספר הפומבי. ניתן לנסות לעקוב אחר הכסף עד לאדם, אך מדובר בפרויקט מורכב: אין שום רישום הקושר בין זהות המשתמש לבין כתובת הארנק, ולכל אדם עשויות להיות אינספור כתובות ארנקים.⁷ אם לא סיפרתם לאיש מהו מספר הארנק שלכם, או כמה ארנקים יש לכם והיכן הכסף

שלכם שמור, נראה שתהיו היחידים שיִדעו את היתרה. יש להניח גם כי ככל שיחלוף הזמן, יתווספו אמצעי פרטיות ואנונימיות לעולמו של הביטקוין ושל המטבעות הדיגיטליים האחרים ("מטבעות קריפטו"), וכבר כיום ישנם מטבעות המציעים חומת אנונימיות מוחלטת. אנונימיות בתנועת ההון היא יתרון עצום לכל משתמש. המדינה יכולה שלא לאהוב זאת, אך אין לה יכולת לעשות הרבה בנידון.

מאז הומצא והתפרסם, התגלו מאפיינים וצרכים הייחודים לביטקוין, והצורך הוא אבי ההמצאה: מיד קמו חלפנים שהמירו כסף פיזי לביטקוין ולהפך; והוקמו בורסות קריפטו, שבהן ניתן לקנות ולמכור ביטקוין ומטבעות קריפטו נוספים. ככסף, הביטקוין נזיל וניתן בכל רגע להמירו למטבעות אחרים – מטבעות קריפטוגרפיים או מטבעות פיזי "רגילים". הבורסות פתוחות עשרים וארבע שעות ביממה, שבעה ימים בשבוע, ואין צורך לפתוח את בניין המסחר בוול-סטריט כדי לאפשר נגישות מלאה לקנייה ולמכירה. ישנם עשרות בורסות קריפטו, זירות "עמית לעמית" (Peer to Peer) פתוחות, ואינספור שירותים משלימים. שוק מטבעות הקריפטו הוא שוק משוכלל, זמין ונזיל.

יתרון נוסף של הביטקוין הוא היכולת לחלק אותו כמעט עד לאינסוף, אשר מאפשרת עקרונית גם מיקרו-תשלומים, שאינם אפשריים במטבעות אחרים. אינכם יכולים למשל לשלם אלפית הסנט תמורת מאמר שברצונכם לקרוא, במקום להתחייב על עשרה דולרים במינוי חודשי לאתר תוכן (שאת רוב התוכן בו לא תקראו, ככל הנראה). היחידה הקטנה ביותר של הביטקוין נקראת "סאטושי", והיא ממוקמת שמונה ספרות לאחר הנקודה העשרונית. זו יחידה כה קטנה, עד שגם אם יום אחד ביטקוין בודד יהיה שווה מיליון דולר, יחידת סאטושי תהיה שווה לסנט אחד בלבד – וגם יחידה זו תוכל להתחלק עוד, אם הקהילה תחפוץ בכך באותה עת.

אבל יתרוננו הגדול ביותר של הביטקוין סמוי מן העין וטמון דווקא במה שאין בו. הביטקוין הוא הכסף הראשון בהיסטוריה שהונפק ללא אישור משום גורם, שלא מתנוססת עליו חתימתו של נגיד, ושמרגע לידתו הוא תלוי אך ורק ברצונם הטוב של המשתמשים. בכך מדגים הביטקוין את אדישותו לכוח הממשל ואת אהבתו לעוצמת האדם הפשוט. כבר קרוב לעשור מתחזק הביטקוין, כנגד אזהרות "המומחים" והשלטונות. הוא כאן והוא מצליח רק משום שהמשתמשים בוחרים לשים בו את מבטחם.

קיבלנו, אם כן מוצר דיגיטלי נדיר (כלומר מוצר שכמותו מוגבלת וידועה מראש), בלתי ניתן לשכפול, שהבעלות עליו כתובה באופן שאינו ניתן לזיוף, וכל זאת במערכת פתוחה וציבורית, שאי אפשר לסגור אותה או לנטרל אותה. לפנינו גם מטבע אחיד שניתן לסחור בו או בחלקיקים ממנו, מיד ובכל מקום, ללא תלות בגבולות או ברגולציה, וכל זאת באנונימיות כמעט מוחלטת. זהו מטבע שלעולם לא יעבור פיחות

(כלומר לא יוכל להישחק עקב עודף הדפסה), והחשוב מכול: מטבע שאף מלחמה, פוליטיקה, משבר מדיני או חקיקה אינם יכולים לבטל או להכחיד. הביטקוין נוצר, מתקדם ונשמר על בסיס שיתוף חברתי, ובגיבוי חוקי הנצח של המתמטיקה הנעלים מכל משחק פוליטי או חקיקה.

צללים ופשעים

אנשים רעים אינה המצאה חדשה. הם תמיד היו, ולא סאטושי נאקמוטו ברא אותם. אבל הביטקוין בהחלט פתח דלת חדשה לפעילות פיננסית שמדינות אוסרות בדרך כלל; לדוגמה, תשלום לרוצח שכיר קל יותר, לשני הצדדים, כאשר הוא נעשה בעזרת ביטקוין. האופי הגלובלי והמיידני של הביטקוין והאנונימיות שלו מייטרים את הצורך להלבין את ההון, והופכים את הביטקוין לפתרון מוצלח לפעילות לא-חוקית. הימורים, סחיטה, כופר וזנות אסורים על ידי מדינות, ולכן בפועל מכריחות המדינות את העבריינים להשתמש בביטקוין. ככל הנראה, עבריינים היו מעדיפים דולרים, אך הביטקוין הפך את חייהם לפשוטים בהרבה: אין כל בעיה להעביר סכומים עצומים בין מדינות, אין רישום, אין פיקוח ואין רגולציה.

אלא שצידו המואר של הביטקוין חשוב לא פחות, והפוטנציאל שלו גדול בהרבה מזה של הצד האפל. הביטקוין הפך גן עדן גם, ובעיקר, לאנשים נורמטיביים וממושעמים להפליא⁸ שהמערכת הפיננסית דוחה מעליה. כך, לדוגמה, אם אין לך דירוג אשראי, לא תוכל לקבל חשבון בנק או כרטיס אשראי, אך תוכל בתוך כמה שניות לפתוח ארנק ביטקוין ולשלם ללא כל תעודה. נולדת במרכז אפריקה ואין לך בנקים או אשראי? הביטקוין הוא ידידך. את תושבת ונצואלה והמדינה סגרה לך את הבנקים? הביטקוין זמין לך.⁹ אתה פליט סורי שמדינתו נשרפת? אתה יכול לעבור למטבע לא-פוליטי שישמור על הונך, ולא להמשיך להחזיק במטבע שערכו פוחת והולך מיום ליום. כבר הזכרנו כי גם חברי הגוש האירופי היציב עלולים לגלות יום אחד שאיטליה וספרד פשטו את הרגל, והאירו שלהם נשחק עד עפר למימון חובותיהן של מדינות אחרות; גם להם עשוי הביטקוין לסייע.

הביטקוין מאפשר לאנשי העולם להמיר את הכסף המקומי והשביר שלהם בכסף שמאחוריו לא עומדת שום מדינה בזבזנית או שוחרת מלחמות, אלא חוקי הטבע של המתמטיקה. לכן, הביטקוין הוא האיום הגדול ביותר על מדינות בכלל, ועל מדינות המשתמשות במטבע כדרך להגבלת חירות אזרחיהן בפרט. מדינות כאלו מדפיסות כסף ומבזבזות אותו ללא כל אחריות, אך אומרות לאזרחיהן: "תסמכו עלינו! אנחנו הדבר האמיתי! אין יציב מן המטבע שלנו"; ואז הן משתתפות במלחמה נוראית, או "סתם" מגיעות לחדלות פירעון בשל נסיבות הגורל והאזרחים מאבדים את שארית הונם. כאשר מגלות המדינות שהכסף של אזרחיהן זולג מן הבנקים אל עולם הביטקוין, הן מיד מתחילות לצווח: "זהו כסף וירטואלי מזויף, זה לא אמין, זה כסף של פושעים".

אבל אנשים רבים יודעים כי מי שאינו אמין ולא ניתן לסמוך עליו הוא דווקא המדינה. בטווח הארוך, דווקא הכסף המצויר, על חוטי המתכת השזורים בו, הוא זה שאינו אמין.

הביטקוין אינו צד במלחמה הזו; הוא פשוט שם. הביטקוין הוא לא מטבע פוליטי, אלא בסך הכול טכנולוגיה עדיפה. טכנולוגיה עדיפה תמיד תנצח ותשרוד ותוציא לגמלאות ולמחסן הגרוטאות של ההיסטוריה את הטכנולוגיה הקודמת. כך קרה לווקמן בדור ה-CD, ול-CD כשהגיע ה-DVD, ולשניהם כשבא זיכרון המטמון. הטכנולוגיה של הביטקוין עדיפה על כסף בכל פרמטר: אי-פיחות, יציבות, מהירות, אנונימיות, ביזוריות, גלובליות ועלויות עסקאות נמוכות (חשבו כמה כסף לוקחים מאיתנו חברות האשראי והבנקים רק כדי שנוכל להעביר כסף זה לזה. שבריר האחוז מכך הוא עלות העסקאות בביטקוין); והטכנולוגיה תנצח.

העובדה שכיום הביטקוין מרכז אליו פעילות עבריינית רבה רק מדגימה ומחזקת את יתרונותיו. גם אל קפונה העדיף דולרים, אך זה לא מפריע לאף אחד לצבור דולרים עד היום. העבריינים פשוט היו הראשונים שזיהו את הפוטנציאל. אחריהם הגיעו הסינים, שקונים ביטקוין בהמוניהם, משום שהם מבינים כי הרגולציה הקשוחה וחוסר הדמוקרטיה במדינתם מעמידים את הסכונותיהם בסכנה. יחד איתם מגיעים אנשי העולם השלישי ואנשי העולם הראשון המודאגים. כולם כבר קנו ביטקוין, ונהירה זו אל המטבע עתידה להתעצם ככל שעוד ועוד אנשים יבינו כי יתרונות הטכנולוגיה לציידים וכי המערכת בלתי שבירה. בעוד עשור יהפוך הביטקוין לברירת המחדל של כל אדם המבקש לשמור על הונו, ואז תקבל הפעילות הבלתי חוקית את מקומה הטבעי.

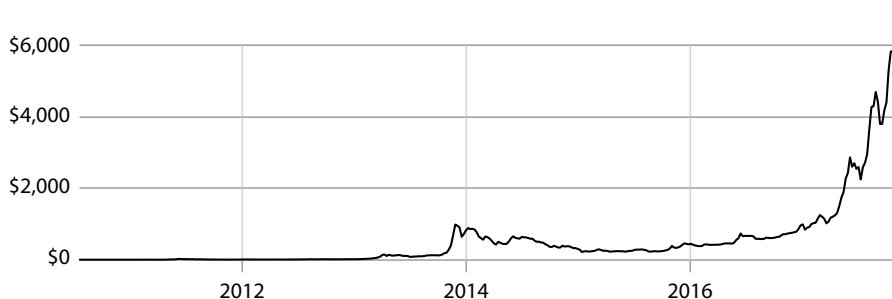
אך אם הביטקוין כה יעיל, מדוע עדיין איננו משלמים באמצעותו במכולת? שתי סיבות לכך: ראשית, עדיין אין צורך: השקל עושה זאת היטב; אולם מלבד זאת, פרוטוקול הביטקוין הנוכחי בנוי במתכוון להעברות הדורשות כעשר דקות, ולא לשם העברות מיידיות. איש אינו מתכוון לחכות עשר דקות אחרי קניית קרטיב רק כדי ששני הצדדים יודאו שההעברה הושלמה ונרשמה בבלוקצ'יין. לעומת זאת, אם המטרה היא שמירה על ההון, עשר דקות הן כלום. מלבד זאת, כיום ישנם פתרונות טכנולוגיים המאפשרים שימוש מלא וחופשי בביטקוין בחלקיקי שנייה ובעלות סליקה זניחה. פתרונות אלו מצויים הן בצד פרוטוקול הביטקוין והן בצד המוצרים המשלימים. למשל, חברת XAPO מנפיקה כרטיס אשראי רגיל המבוסס על ביטקוין באופן שקוף לחלוטין לחנויות ולצרכנים; ופתרונות כגון Segwit אשר התווסף לאחרונה לפרוטוקול הביטקוין, ו-Lightning Network, המאפשרים סליקה מיידית וזולה מאוד על גבי רשת הביטקוין. אפשרויות אלו ואחרות מתפתחות כל העת, מכיוון שפרוטוקול הביטקוין הוא פתוח ודינמי. כבר כעת אפשר לקנות עם ביטקוין בחנויות רבות בארץ ובעולם; וברחוב אחוזת בית בתל-אביב אפשר אפילו לקנות פלאפל עם הביטקוין שלכם.

עלייה מטאורית

כבר אמרנו שהביטקוין הוא מטבע עם מצאי מוגבל, ובדומה לכל סחורה אחרת אף הוא מתמודד עם כוחות ההיצע והביקוש של השוק. בתקופה הראשונה לאחר השקת המטבע, איש לא התעניין ברעיון המשונה הזה וערכו של המטבע היה בהתאם. העסקה הראשונה בהיסטוריה של קניית טובין באמצעות ביטקוין נערכה ב-22 במאי 2010, בלוס־אנג'לס: רכישת שני מגשי פיצה תמורת עשרת אלפים ביטקוין. שווי העסקה היה 25 דולר, כלומר כל ביטקוין היה שווה אז רבע סנט. כיום, עשרת אלפים ביטקוין שווים למעלה משלושים מיליון דולר! בדיעבד מסתבר כי הייתה זו הארוחה היקרה בהיסטוריה, אם אפשר לקרוא למגש פיצה ארוחה.

מאז זרמו הרבה ביטים בנהר הבלוקצ'יין, המטבע נחשף לעוד ועוד אנשים, והרעיון המשיך להתקבל ולהתבסס ובהתאם נולד מסחר פעיל ודינמי, וכיום ישנן בורסות קריפטו הפתוחות ללא הפסקה. כמו בעולם ניירות הערך, כל בורסה היא זירה תזזיתית התלויה בתנודות מצב הרוח של השוק. יש עיתות גאות ויש תקופות שפל, יש עליות וירידות, אופוריה ודיכאון, כל המצבים הרגילים שלנו, בני התמותה. אך בהסתכלות בתמונה הרחבה, המגמה ברורה וחד־משמעית: כמות המשתמשים וכמות האנשים הנחשפים לביטקוין גדלה בהתמדה, ולכן גם ערכו של הביטקוין מטפס משנה לשנה.

כך נראה גרף המחיר ההיסטורי של הביטקוין.



כפי שאפשר לראות בגרף, בסוף 2013 הייתה קפיצה אדירה בשווי הביטקוין וערכו גדל פי מאה בתוך כמה חודשים – מדולרים בודדים ל-1,200 דולר. קפיצה זו הונעה מחשיפת התקשורת הממסדית לביטקוין, יחד עם ציפיות לא־ריאליות של השוק על קצב ההתקבלות העתידי. לאחר תקופת האופוריה התרחש תיקון חד של השער ל-200 דולר (אולם גם לאחר הנפילה היה שווי המטבע גבוה פי עשרה משווי לפני העליות החדות); ומאז, במשך ארבע שנים רצופות, ממשיך הביטקוין לטפס בהדרגה ובנחישות בדרכו לכיבוש העולם. אכן, עדיין יש תנודתיות רבה בשער המטבע, הרבה יותר מכל מטבע אחר. קפיצה של מאות דולרים ביום, או ירידה של ארבעים אחוז

משווי המטבע בתוך ימים ספורים, נדמית כדרמה ענקית לעומת תנודות של אחוזים בודדים בשוק המטבעות המסורתי – אבל זהו חלק בלתי נמנע מתהליכי ההתבגרות של השוק. אחרי הכול, המחיר מבוסס על היצע וביקוש ובלבד, ואלו מושפעים מכותרות העיתונים, מחששות המשקיעים, מחקיקות חדשות ומתקופות של חוסר ודאות. בתחילת ספטמבר 2017, למשל, הודיעה סין על סגירת בורסות קריפטו בשטחה, ובתגובה נוצרה ירידה משמעותית בשווי המטבע; אך מגמת ירידה זו התהפכה בתוך ימים ספורים, ומרוץ חדש החל.

אומרים כי מיום שחרב המקדש ניתנה הנבואה לשוטים. איננו יודעים אם מחירו של הביטקוין ימשיך לטפס, כפי שאין איש יודע מה יעלה בגורלה של כלכלת ארצות הברית או של חברת גוגל. אנו יכולים רק לשער על סמך הנתונים והעובדות שיש בידינו, והללו מצביעים על אימוץ הולך וגובר של הביטקוין ועל צמיחה ופעילות מואצת זה תשע שנים. לכן, לא מופרך לשער שהביטקוין ימשיך להתחזק ולשמש פתרון ומקלט לעוד ועוד אנשים וגופים. שער הביטקוין צפוי להמשיך לטפס ולשבור שיאים חדשים, כי יש לו עוד מקום רב לצמיחה ולהתקדמות – כרגע מייצג הביטקוין רק שבריר זעום מהכלכלה העולמית. כדי לסבר את האוזן נאמר כי השווי הכולל של כל הביטקוונים הקיימים כיום הוא כ-60 מיליארד דולר, בעוד שווי הזהב הפיזי הקיים בעולם הוא כשבעה טריליון דולר (7,000 מיליארדי דולרים של זהב). 60 מיליארד דולר הם גם הרבה פחות משוויה של חברת אפל (המוערך בכ-800 מיליארד דולר) או מהונו האישי של ביל גייטס. נתונים אלה מדגימים כי לביטקוין יש עוד המון, המון מקום לצמוח. הערך המובנה הגלום בו, עדיפותו הטכנולוגית והגידול בכמות המשתמשים בו – כולם רומזים על עתיד ורוד ומסעיר. הכפלה בשווי השער, כלומר גידול בשיעור של מאה אחוזים, מדי שנה או פחות, היא תרחיש ריאלי לחלוטין. בעת כתיבת שורות אלה, שווי של ביטקוין יחיד הוא 3,000 דולר; בעוד שנה, ויש לשער שעוד קודם לכן, יהיה שווי 6,000 דולר; בעוד שנתיים, 12,000; בעוד עשור עשוי שוויו של הביטקוין לעמוד על מאות אלפי דולרים. וכל זה רק הביטקוין, לפני שדיברנו על שאר המטבעות, ועל האופן שבו תשנה טכנולוגיה זו כל ממד והיבט בחיינו.

לא בן יחיד

סאטושי נאקמוטו פרסם את המצאת הביטקוין כנייר עמדה פומבי, ללא סודות, כשהוא חשוף וגלוי לעין כול. באותו אופן גם הקוד של הביטקוין הוא ציבורי ופתוח. לכן, מיד לאחד השקת הביטקוין החלו יזמים להשתמש בטכנולוגיה כדי לייצר מטבעות נוספים וחדשים, המכונים בשם הכולל "טוקנים" (tokens), שכן במהותם הם לא בהכרח מטבעות. הרעיון שבבסיס הביטקוין, שנולד כדי לתת מענה לכסף דיגיטלי, הורחב וגדל לתחומים רבים חדשים, המציעים כל אחד שינוי פונקציונלי לעומת המטבע המקורי. חלק מהיוזמות הראשוניות היו ליצירת כספים אלטרנטיביים

נוספים, כגון מטבעות המציעים יכולת אבטחה גבוהה יותר או אנונימיות מוחלטת (כמו Monero ו-ZCASH), מטבעות המציעים מהירות עסקה גבוהה יותר, מטבעות ה"מוצמדים" לדולר, מטבעות שיש להם מנגנון או קצב כרייה שונה ועוד. כולם משתמשים בבלוקצ'יין כדי לרשום את העסקאות, ו"כולם היו בניו" של הביטקוין. אולם מטבעות קריפטוגרפיים אינם מוגבלים ליצירת "כסף" חדש. באמצעות טוקנים כאלו אפשר לייצג עניינים נוספים, כגון אחוז בעלות במיזם כלשהו או בטכנולוגיה חדשה (בדומה למניה); כמה מדינות החלו לבחון את השימוש בטוקנים כדי לאפשר בסיס נתונים ציבורי ופתוח לרישום בעלות בעסקאות נדל"ן; וניתן להשתמש בטוקנים גם כדי להשכיר שירותי מחשוב ענן או כוח עיבוד מחשבים. הנה דוגמה נוספת: הטוקן ETH (איתריום) מאפשר כתיבת "חוזה חכמים" הממומשים בקוד, וכך ניתן לקבוע תשלום ריבית בשיעור מסוים, ללא צורך בבנקאי או בבנק – שכן הקוד דואג לכל מה שצריך. יתרה מזאת, האיתריום הוא תשתית המאפשרת למפתחים אחרים לבנות על גבה יישומים ספציפיים, והטוקן של הפלטפורמה, ה-ETH, נסחר בשוק החופשי.

ישנם כבר מאות טוקנים קריפטוגרפיים, וטוקנים חדשים נוצרים מדי יום. המגבלה היחידה היא הדמיון שלנו. כך לדוגמה יכולים חברי קיבוץ ליצור "מטבע קהילתי" לשימוש בקיבוץ שלהם: החברים יקבלו תוספת מטבעות על עבודות קשות, כגון פלחה או תורנות מטבח, ויכולו להשתמש בהם לרכישת גזוז או לשם עדיפות בסבב הרכב. יצירתו של מטבע כזה דורשת שעות אחדות, לכל היותר, והשימוש בו או שוויו עתידים להיגזר מן הערך שיביא לחיי הקהילה.

גם חברות מסחריות, ואפילו מדינות, כבר עובדות על הנפקת מטבעות "שלהן". ואכן, מדוע צריכה רשת חנויות ליצור כרטיס מועדון, שהשימוש בו מסורבל למדי, אם היא יכולה להנפיק מטבעות משלה ולתת כמה מהם כתגמול על כל קנייה; להעניק הנחות ברכישה עתידית תמורת מטבעות ("קנייה במטבע שלנו זולה יותר לעומת קנייה בשקלים", תאמר הפרסומת); או לתת לנו קופונים בצורת מטבע הרשת? זה מחזק את הרשת, זה כלכלי יותר, זה קל יותר ללקוחות וזה זמין תמיד בטלפון.

כיום נסחרים באופן אקטיבי קרוב לאלף מטבעות. בדיוק כמו בביטקוין, גם שוויים של מטבעות אלו נקבע על ידי היצע וביקוש. אם המטבע החדש אינו מייצג שום ערך ממשי או תועלת, הוא יגוע מחוסר עניין ושימוש, וערכו ירד עד שהמטבע יעלם. אולם אם הוא פותר בעיה, או משמש תשתית טובה ליישומים נוספים, אזי סיכויי התקבלותו עולים ומסחר ער עשוי להתרחש סביבו.

השוק החופשי הופך לנגד עינינו מתיאוריה שניתן להתווכח על נכונותה, או לדון ביישומה בחיי המדינה, לעובדה גלובלית שאיננה תלויה במסד כלשהו. סחר חופשי לחלוטין שאיננו נתון להגבלות עומד מעבר לפינה.

העולם הוא שטוח

הקלות שבה ניתן לייצר מטבעות חדשים לשימושים שונים יצרה תופעה חדשה המכונה Initial Coin Offering ובקיצור ICO. אפשר לומר בפשטות שמדובר בהנפקה של טוקן חדש, המייצג טכנולוגיה או יישום חדש, ואשר מרגע שהוא בא לעולם ניתן לקנותו ולמוכרו והמסחר מתחיל. כדי להבין מדוע ה-ICO מצליחים ומהי הבשורה שהם מביאים לכלכלה העולמית, עלינו לעמוד על האופן שבו גויס עד היום הון לטובת יוזמות טכנולוגיות.

ב"עולם הישן", זה שהיה כאן עד אתמול, כסף הולך עם כסף, ומי שמתפס במעלה הסולם מושך את הסולם איתו למעלה, מרחיק את עצמו מן העדר, ומחזק את יתרונו. לדוגמה, כאשר הקים מרק צוקרברג את פייסבוק וביקש לגייס הון כדי לפתח את האפליקציה שלימים תשנה את העולם, הוא פנה למספר מצומצם מאוד של אנשים עשירים ומנהלי קרנות הון-סיכון היושבות בקליפורניה, והציע בפניהם את חזונו; כמה מהם ראו את הפוטנציאל, השקיעו מכספם, ולאחר כמה שנים הפכו לעשירים באופן אגדי. רק בשלב מאוחר הרבה יותר, זמן רב לאחר הקפיצה הגדולה בשווייה, הפכה פייסבוק לחברה ציבורית; ורק אז התאפשר גם לציבור לקנות מניות פייסבוק, כי עד היום לא הייתה ברירה אחרת. עד לאחרונה, סטארטאפים יכלו לגייס הון משמעותי רק מקרנות וממשקיעים גדולים, ולכן השמנת, מבחינת פוטנציאל צמיחה, שמורה הייתה תמיד לשמנת העסקית.

אבל אז בא סאטושי והשטיח את העולם במכה אחת.

בעולם הקריפטו, זכות הראשונים פתוחה לכולם. כל אחד מאיתנו יכול להיות המשקיע האגדי שהיה שם כבר ביום הראשון וגזר אחר כך קופון שמן; וכל אחד מאיתנו יכול גם לשים את כספו על קרן הצבי ולאבדו בן לילה. ה-ICO היא תופעה המאפשרת לכל אחד לגייס הון מהציבור, ולתת לציבור לשפוט בעצמו אם מדובר בטכנולוגיה ממשית, אם יש בה ערך ואם יש לה חזון; ובהתאם, להחליט אם לרכוש את הטוקן החדש בעת ההנפקה וכך להזרים כסף לקופת החברה ולהחזיק ב"מניה" בצורת טוקן שתקנה לו חלק בהצלחת המטבע החדש.

ואכן, לראשונים הקונים מטבע חדש בימיו הראשונים יש סיכויים לתשואות חסרות תקדים; וכמובן, גם סיכונים גבוהים מאוד. קנייה של האיתרום בימיו הראשונים, לפני כשנתיים וחצי, הביאה עד היום תשואה של כמאה אלף אחוזים. ייתכן שתשפשו את אוזניכם, אך זו אינה טעות: המשקיעים הרוויחו פי אלף! האם אתם מכירים מישהו במקום כלשהו שהשיג תשואות כאלו בעבר, באיזשהו תחום השקעה?

ה-ICO אינם מתרחשים הרחק מעבר לים; הם גם ממש כאן. חברת בנקור (Bancor) הישראלית, למשל, פיתחה טוקן בשם BNT המבוסס על איתרום, ומאפשר לחברות לייצר טוקנים משלהם במהירות ובקלות. במהלך יוני 2017 ביצעה בנקור הנפקה

של הטוקן החדש שלה; והרוכשים העבירו לארנק הדיגיטלי של בנקור טוקנים של איתרום, ובתמורה קיבלו טוקנים מסוג BNT (מאה BNT היו שווים ETH אחד ביום ההנפקה). בתוך שעותיים וחצי גייסה בנקור כספים בשווי של 143 מיליון דולר. בדיעבד התברר כי היה זה גיוס ההמונים הגדול בהיסטוריה.

להבדיל מגיוס הון בבורסה, גיוס זה התבצע בעבור סטארטאפ חסר היסטוריה, ללא תשקיף, ללא פיקוח של רשות ניירות הערך (בשלב זה), ובעיקר: כגיוס הפתוח לעולם כולו ולא לשוק מקומי. ה-ICO מייצגים את השלב הבא באבולוציה של גיוס הון והקמת יוזמות טכנולוגיות; ונוסף על כך, הטכנולוגיה שבבסיס מאפשרת, לראשונה, הקמה של ארגונים מבוזרים לחלוטין, אשר ניהולם וכלכלתם מבוססים על טוקנים סחירים ולא על מניות היזמים. זהו מבנה השונה ב-180 מעלות ממבנה החברות המסורתיות והריכוזיות. עולם שלם של אפליקציות וארגונים מבוזרים עומד על פתחנו.

מובן שאלה וקוץ בה. הציבור נוהר אחר ההנפקות החדשות אבל ישנם ICO רבים, ואולי אף רובם, שאינם מייצגים כל ערך אמיתי או טכנולוגיה ואינם אלא אשליה שתתגלה מיד לאחר שהיזמים יקבלו את הון ההמון. אולם בנוכלים וברמאים כבר עסקנו: הם אינם משנים את מהות הדברים. בפועל, המבנה המבוזר, הלא-ריכוזי, הפתוח והחופשי של מטבעות הקריפטו פותח דלתות חדשות ליזמות ולתנועת הכסף, מהאדם הקטן לכל יום, והוא מאפשר לכל אחד סולם משלו בדרך אל העצמאות. לא רק מסלול חדש אל הכסף נסלל כאן: לראשונה בהיסטוריה, כל אחד מאיתנו, מכל מקום על גבי הגלובוס, יכול להפוך בעצמו לענק עולמי. אפשר לפתח מטבעות וכלכלה, להפוך לבנק, להציע מוצרים ושירותים, לגייס הון ולפתור בעיות למיליוני אנשים. כדי לעשות את כל זאת לא נדרש יותר מאשר טלפון נייד. העולם בכף ידנו.

תנו לקיטר את אשר לקיטר?

נראה כי לא תיפלו מהכיסא אם אומר כי העולם הפיננסי הקלאסי אינו עתיד לפרוס שטיח אדום לרגלי הביטקוין; וברור כי הביטקוין ושוק הקריפטו כולו מאיימים על הכלכלה המסורתית ועל רבים מסדרי העולם. נתחיל מהכסף עצמו.

מטבע אינו רק ערך ומכשיר פיננסי; לעיתים הוא גם זהות. רבים מאיתנו מתגאים בשקל החזק ומרוצים ממנו בנסיעות לאירופה. ואכן, ערך המטבע הלאומי הוא נגזרת של עוצמתה הצבאית והכלכלית של המדינה. כך למשל כאשר מחיר חבית נפט ירד משמונים דולר לארבעים, כלכלות מבוססות נפט קרסו, ואילו המטבע של יצרנית הנפט ונצואלה (שמונהג בה משטר סוציאליסטי קיצוני) התמוטט כליל. בתגובת נגד טיפוסית הפכה ונצואלה את המסחר בביטקוין לבלתי חוקי; וכיום אסור להחזיק או לכרות ביטקוין בוונצואלה. למותר לציין כי צעד זה לא שינה דבר וההמונים ברחו וממשיכים לברוח מהבוליבר, אשר מודפס ללא אחריות וללא קשר ליכולת הפירעון

של המדינה, אל מטבעות דיגיטליים דוגמת הביטקוין – שחוקי המתמטיקה מנהלים אותן, ולא גחמה של רודן, משאבי טבע או שר אוצר סהרורי.

העולם החדש מציע לנו להיפרד משטרות התקפים ביחידה גיאוגרפית ספציפית ונתונים לחסדי שמיים או לחסדיו של שלטון מתחלף וקפריזי, ותחתייהם לרכוש מטבע דיגיטלי ונצחי, בעל זהות אוניברסלית ואוטונומית שאינה כפופה למדינה, לשפה או לחוק מקומי. את זהותנו הלאומית נשמר עם המנון ודגל, אך את זהותנו הכלכלית נגבש כפרטים באוטונומיה מלאה. אגב, שינוי כזה קרה כבר לא אחת: האיטלקים ויתרו על הלירטה לטובת האירו, והצרפתים והגרמנים על הפרנקים ועל המרקים. הוויתור על המטבע המקומי אינו מוביל בהכרח לויתור על גאווה או זהות לאומית.

לא כל המדינות מבינות זאת, אבל הכלכלה הדיגיטלית החדשה, הביטקוין ועמו שלל מטבעות הקריפטו, מהווים איום אסטרטגי על עצם מוסד המדינה ובעיקר על הבנק המרכזי. למעשה, המילה איום היא מטעה, כי היא מניחה שיש רק סיכון אפשרי, ואם המדינה תתנגד בנחרצות מספקת, היא תשכיל להדוף אותה. האמת היא שמטבעות הקריפטו אינם עוד בגדר איום אלא בבחינת עובדה סופית: העתיד כבר נגזר, הפור נפל והוא בלתי ניתן לשינוי. נותר רק לשאול כמה זמן ייקח למדינות להפנים כי העולם הפיננסי השתנה לבלי שוב.

הסיבה העיקרית שבעטיה מטיל הביטקוין צל כבד גם על מדינות היא שאלת המיסים. גביית מיסים היא בסיס הכוח של המדינה המודרנית, וממשלה או צבא אינם יכולים להתקיים ללא תקצוב ממשלתי. אולם ממשלה כידוע איננה מייצרת סחורות ומוצרים, אלא רק שירותים שעולים כסף – המגיע מכיסיהם של האזרחים. יכולתה הכמעט-טוטאלית של המדינה לגבות מיסים תלויה לא מעט ביכולתה להציץ אל תוך חשבון הבנק שלנו, לחלט כספים ואף לגבות "מלווה מרצון". המיסים אינם תרומה של התושבים אלא חובה הנאכפת באמצעות מנגנוני בקרה ושליטה: רואי חשבון, דיווחי בנקים, רשויות המיסים וההוצאה לפועל. לכן שקלו כמה מדינות לבטל כליל את המטבעות והשטרות ולהוציא את התשלום במזומן אל מחוץ לחוק – שכן עסקה במזומן היא בלתי אפשרית לניטור ולכן מעודדת כלכלה שחורה ואי-תשלום מס. אך בעולם החדש משימות הפיקוח והגבייה הופכות לקשות יותר ויותר: למדינה קשה מאוד להציץ את תוך "חשבון" הבנק הקריפטוגרפי שלנו, דהיינו אל הארנקים הדיגיטליים שלנו; המטבעות הדיגיטליים הופכים את הכלכלה כולה למרחב שבו הדיווח הופך לוולונטרי. כך, ככל שהשימוש במטבעות הקריפטו יהיה נפוץ יותר, יהפכו המטבעות המדינתיים רלבנטיים פחות, והכסף יזלוג החוצה – מן הבנקים והמוסדות הרשמיים אל הכלכלה האלטרנטיבית, הבינלאומית והבלתי מפוקחת.

שיעורי המס הנוכחיים יהיו חייבים להשתנות אל מאזן כוחות חדש, שבו המס יהיה נמוך בהרבה, כך שיהיה כדאי לתושבים לשלם ומאידך גיסא תהיה למדינה יכולת

להתקיים. יהיה צורך למצוא מאזן חדש בין עוצמתו של השלטון ובין חופש הפרט שמאפשרת הטכנולוגיה.

* * *

המעבר מכלכלה ישנה לכלכלה המבוססת על מטבעות דיגיטליים צפוי להיות רצוף קשיים ומהמורות, וכסף פינט וביטקוין יתקשו מאוד לדור בכפיפה אחת. מוקדי הכוח של מטבעות הפינט ייאהזו בקרנות המזבח של ריבית, שליטה ומיסוי; ועולם הקריפטו צפוי להתקל בניסיונות נואשים לעצירת השטף. ניתן לשער שמומחים מטעם הממסד יקבעו כי "הביטקוין הוא הונאה" ותופיע חקיקה פרועה כנגדו. אנו עתידים לראות מדינות המחרימות את הביטקוין לחלוטין, אוסרות את המסחר בו, או מבטלות את האפשרות להנפקת מטבעות או להקמת בורסות קריפטוגרפיות; אולם ניסיונות אלו לא יצלחו, ומטבע דיגיטלי חברתי ללא גבולות ישרוד, יקום ויתחזק כעוף החול. הטכנולוגיה חזקה מהמחוקק, ורצון האזרחים הוא הכוח המניע את המהפכה.¹⁰ הביטקוין לא ביקש רשות כדי להיוולד, וולא עתיד לבקש רשות כדי לשרוד ולשגשג.

זו הסיבה שהביטקוין עדיין איננו מוכר כמטבע עובר לסוחר בכל מדינות העולם. בשווייץ, באוסטרליה ובארה"ב כבר זכה הביטקוין למעמד, אך בישראל הוא עדיין נחשב לעוף מוזר. מעמדו עדיין לא ברור והוא אינו מוגדר כמטבע אלא כ"נכס" החייב במיסוי רווחי הון שמטבעות רגילים פטורים ממנו.¹¹ מדוע זה כך? התשובה פשוטה: כדי שרשות המיסים תוכל לגבות על מכירתו מיסים לא-מוצדקים. המדינה מערימה קשיים נוספים על רוכשי הביטקוין, וכמה בנקים ישראלים חסמו לאחרונה את חשבונות לקוחותיהם מפעולות הקשורות בצורה כלשהי למטבע הדיגיטלי. ביפן, אגב, הביטקוין הוא כבר "הילך חוקי", ונראה שמדינות רבות אחרות יצעדו בעקבותיה. בסופו של יום, לא תהיה להן ברירה אחרת.

הביטקוין ושוק הקריפטו יצרו, דה-פקטו, כלכלה שבה הסמכות שלי כפרט זהה לסמכותו של כל פרט אחר; ואילו בכלכלה הישנה, הנוכחית, מצויים פרטים הקובעים בשביל כולם. נגיד הבנק המרכזי אינו נבחר ציבור אלא אדם מן השורה, ובכל זאת הוא יכול להחליט על מחיר הכסף לכולנו: על גובה הריבית, על שיעור האינפלציה, ועל קצב ההדפסה. בעולם הקריפטו אין נגיד כזה; המתמטיקה וחוקי הפרוטוקול הציבורי הם הקובעים היחידים ואיש אינו חזק מחברו. אין כאן מדינות, לא קטנות ולא מעצמות; אין כאן יחסי הון-שלטון; אין איפה ואיפה; אלא רק כלכלה טהורה שנחתמה בקוד ומונעת על ידי הערך שהיא מביאה לעולם. והכלכלה הזו שווה בפני כולם ומציעה אינספור הזדמנויות לכל אדם.

דוגמה נוספת לאבסורד הנזכר: במשך עשרות שנים הונהג ברוסיה הקומוניסטית "מחירון" מפוקח לכל שירות או מוצר: נעליים למשל עלו כך וכך רובל בכל מקום,

וזהו; הפרולטריון קבע את המחיר לכולם. האמריקנים גיחכו על היוזמה הקומוניסטית הזו, המונעת שוק חופשי ותחרות, אולם דבר אחד שכחו באמריקה: כי את המחיר למוצר החשוב מכולם, מחיר הכסף עצמו, קובע אדם יחיד, הלוא הוא נגיד הבנק המרכזי. נגיד הבנק קובע את הריבית, דהיינו את מחיר הכסף, ואנו נתינים וצמיתים של החלטתו – ללא יכולת ערעור או בחירה ישירה. כיום למשל הריבית הנהוגה במשק היא הנמוכה ביותר באלף השנים האחרונות (!), ועובדה זו מוכתבת לאורח מלמעלה ללא כל יכולת לשנותה. לעומת כל אלו, הביטקוין הפך את המשוואה על ראשה, העניק לעולם מטבע שקצב ההנפקה שלו קבוע מראש, ויצר מציאות שבה כל אחד יכול לייצר מטבע אלטרנטיבי במחיר אחר. כולנו הפכנו לנגידים בפוטנציה.

הביטקוין ושאר המטבעות מערערים כבר עכשיו את יציבות המערכת הבנקאית, שבה כל העברת כספים בינלאומית לוקחת מספר ימים ועולה כסף רב. הביטקוין מדלג מעל הגבולות ומאפשר העברה מיידית, תוך דקות, אל כל פינה בגלובוס, ללא צורך במערכת פקידותית, בחתימות, בחשבון מוגבל ועוד. יתרה מזאת, הביטקוין וחבריו מבטלים את הצורך בבנקים ממוסדים. הבנקים באו לעולם כארגונים שמטרתם לאחסן את כספם של האזרחים ולשמור עליו, אולם מעת שהכסף היה בידיהם, החלו הבנקים להלוות אותו לאחריים ולסחור בו. בעולם החדש אין בנקים ואין צורך בהם, שכן כל אדם מחזיק בעצמו את המפתחות לכסף שלו בארנק פרטי (או בכמה מהם). מעתה, כל אחד מאיתנו הוא הוא הבנק: בלי צורך ברישיון לפתיחת בנק ובלו הון מחייב. למעשה, כבר היום יש לי בנק משלי ואני יכול לאגור בו כסף, להלוות ממנו, לסחור בו ולפתוח חשבונות תחת החשבון הראשי (כלומר ארנקי משנה תחת ארנק ראשי אחד). לכן, הכסף יחל לזלוג החוצה, מהבנקים אל ארנקים פרטיים ואנונימיים, שיציעו את כל השירותים שמציעים הבנקים אך בזול יותר, מהר יותר, עשירים וארבע שעות ביממה, ובפרטיות מוחלטת. זה יקרה לאט לאט, אך יום אחד יתעוררו הבנקים ויגלו שכיסיהם ריקים.

לפנינו כלכלה חדשה לחלוטין, והיא אינה שואלת לגילך, לשמך, או להיסטוריה שלך; וכדי להנפיק בה מטבע או לסחור בו אינך צריך לקבל רשות מאיש. כל אחד בעולם יכול להיות חבר בכלכלה זו ולרכוב על גבה אל מרחבים חדשים ומסעירים. כיום, לדוגמה, לשלושה מיליארד בני אדם – באפריקה, במזרח, ובדרום אמריקה – אין כל גישה למערכת הבנקאית; הם חסומים בפני הכלכלה, ומבחינה כלכלית נעדרים מן העולם. כיום, אין להם שום סולם לטפס עליו אל רווחה ועצמאות, אך עולם הקריפטו מעניק לכל אחד מהם מפעל לסולמות. מיליארדי אנשים יוצרים כלכלה חדשה שאינה מבקשת רשות מאף מדינה, שלא יכולה להיעצר על ידי אף גורם, ואשר מפיתה תקווה והזדמנויות אינספור. זוהי כלכלה מבוזרת, שטוחה, שוויונית ודינמית המונעת בכוחם ובתעוזתם של הפרטים – ולא ברצונן הטוב של המדינות.

ברוכים הבאים לממלכת האפשרויות הבלתי מוגבלות.

עולם חדש מופלא

מדינות רבות השכילו זה כבר להבין את הפוטנציאל, והן מתחרות ביניהן על זכות הראשונים להוביל את העולם בתחום הקריפטו: שווייץ חוקקה חוקים שמאפשרים ליזמי קריפטו רבים לפעול ממנה; פוטין הודיע כי הוא רוצה להפוך את רוסיה למעצמת כרייה; אוסטרליה נתונה במרוץ לקריאת הפיכתו של הביטקוין למטבע חוקי; וכך גם לטביה ומדינות אחרות – כולם רוצים חלק מן העוגה הצומחת הזו. ובכל זאת, ועל אף הבהלה לזהב הדיגיטלי, נוהגות המדינות בעיוורון גמור בכל הנוגע למשמעויות מרחיקות הלכת של התבססות שוק המטבעות הקריפטוטוגרפיים.

הנה תסריט דמיוני לשיפוטכם. ככל שעובר הזמן, עוד ועוד אנשים מצטרפים למעגל המשתמשים במטבעות הקריפטו, עד שהחזקתם הופכת לחלק מההון והנכסים של רבים. כל מי שנכנס לכלכלה זו מעוניין ביציבות שלה, בהתפתחותה ובשמירת הערך של נכסיו; והוא גם מבין במהירות את יתרונותיו של הון פרטי לחלוטין, העמיד בפני פחות, וגלובלי מטבעו; וכך נוצר גלגל תנופה המחזק את עצמו. האדם גם מבין כי המדינה מוגבלת מאוד ביכולתה להציץ אל תוך הארנק הפרטי שלו; ובעיקר, כי המטבע המקומי נשחק מדי יום באינפלציה ובהדפסת כסף, ואילו החלופה הדיגיטלית מוגנת מכל שחיקה. לכן, לאדם הסביר יהיו עוד ועוד תמריצים להמרת נכסי הפיאט שלו בנכסים עמידים ודיגיטליים. בעוד עשור, האופציה המועדפת לקבלת תשלום תהיה כסף חזק ודיגיטלי (כמו הביטקוין) ולא כסף רעוע ופיזי (שקל).

המטבעות הדיגיטליים מאפשרים לנו להקים ישויות שאינן קיימות בשום מדינה. אלו חברות מתפקדות המגייסות מיליונים, ובכל זאת הן אנונימיות לחלוטין – ללא רישום, ללא מספר ח"פ וללא מס. חברות מעין אלו מכונות DAO (Decentralized Anonymous Organization), ולא מעט כאלו כבר קיימות; וככל שיעבור הזמן, הן עתידות להתרבות. אין סיבה שאת חברת פייסבוק (או גוגל) הבאה לא יקימו כ-DAO, דהיינו כחברה אמיתית לחלוטין שאין לה לא גוף, לא שם, ולא תיק מע"מ באף מדינה. את התמורה לשירותיה תגבה חברה זו במטבעות שהיא עצמה תייצר ותמיר במטבעות דיגיטליים אחרים.

כאשר הכלכלה תעבור לשם, אל מרחב גלובלי, אנונימי ומבוזר, הכסף הישן של המדינה לא יהיה מופקד עוד בבנקים בהיקפים המוכרים לנו כעת. המוסדות הפיננסיים הלא-יעילים, הבוזזים והבירוקרטיים, יהיו הראשונים להיפגע בגל ההדף העצום של היעילות והפרטיות המגיע אל חופינו. רוב ההון הפרטי יהפוך לטוקנים דיגיטליים ויהיה מוסתר תחת חומות הצפנה בלתי חדירות. כאשר עוד ועוד אנשים ישימו את מבטחם במתמטיקה ולא בפוליטיקה, יתרחש המהפך: המדינה תגלה שכיסיה מתרוקנים וכי אין לה סנקציות משמעותיות כלפי התושבים וכלפי העסקים הווירטואליים הפועלים (גם) בשטחה. המדינה תציע לאזרחים בקשה לגילוי מרצון

של נכסי קריפטו כדי להבטיח גביית מיסים. כמה אומללים עלולים להיזרק לכלא על העלמת מס, למען יראו וייראו, אך תחתיים יבואו עשרות, ואלפים ומיליונים שידעו כי למדינה יש יכולת מועטת לפקח על מהלך העניינים. מיסי ההון יהפכו למצומצמים יותר, או לזולטריים, ובמקומם יעלו מיסי תושבות מסוגה של הארנונה.

אם איש לא יאמין עוד לחתימת הנגיד המתנוססת על השטרות, לא תהיה עוד תועלת רבה בהנפקתם. תקציב המדינה יוגדר מחדש, בביטקווינים בשילוב המטבע המקומי או במטבעות נוספים שיהיו באותו זמן. התקציב יצטמצם באופן דרמטי, שכן אכיפת המיסים תרד; השלטון יהפוך לרזה ויעיל, כי יעילותו תימדד תמיד באלטרנטיבה דיגיטלית; והיבטים של חירות הפרט, אשר מתקיימים כיום בעיקר במאמריהם של "ניאו-שמרנים", יהפכו לברירת המחדל של כל אדם. כולם יבקשו לשמר את ההון שלהם בדיהם, וישמרו מכל משמר על המפתחות הפרטיים שלהם. נכדינו יוולדו לעולם שבו איש אינו נזקק למתווך כדי לשמור על הונו: "באמת סבא, היית עומד בתור לבנק? מה זה בנק? ומה זאת אומרת שהוא היה סגור בצהריים?"

לכשיתממש התסריט הזה, הוא עלול להתרחש בהפתעה גמורה, בדומה לקריסת חומת ברלין או להפיכת אוקטובר במצרים. יום אחד נתעורר לעולם חדש, שבו המוסדות הפיננסיים נעלמו והופשטו מנכסיהם; והמדינות יגלו כי כלכלתן השתנתה לחלוטין וכי תושביהן הפכו באחת אזרחי העולם. משוואת הכוחות תתהפך. עולם חדש של פרטים עצמאיים ושל מדינות רזות עומד בפתח.

המדינה הרזה

הבה נדמיין לרגע את העולם הזה, שבו כל הכסף גלובלי ודיגיטלי (כמו אירו, אך בכל מקום ובלי נגיד בנק). זהו עולם ללא בנקים, במובן המסורתי של המילה, שבו ישנן אינספור זירות המפגישות אנשים זה עם זה לטובת הלוואות, פיקדונות, השקעות וכדומה.

המדינה תיפרד מחלק ניכר מבסיסי הכוח שלה, ואלו יעברו לידי האזרחים. הרגולציה הנוגעת לכספים ולניהולם תתמוסס ותשתנה. בעולם שבו כל אדם הוא הבנק של עצמו, אין משמעות לתקנות ולחוקים הנדרשים להקמת מוסד פיננסי, שהלוא כולנו מוסדות פיננסיים; ואין צורך לקבל רשות מהמחוקק, כשם שאין לרשות יכולת לפקח על מסחר בין אנשים או לעצור אותו – לא רק בתוך תחומי המדינה, אלא בין כל שני אנשים, בכל מקום על הגלובוס. העולם הופך להיות קטן, שטוח ומייד. כל אחד רשאי יהיה לעשות עסקים עם כל אדם אחר, ללא הבדלי דת או לאום, וגם ללא הבדלי מין (במובן species) – משום שנוכל לנהל עסקים, מסחר ותנועת הון גם מול ישויות דיגיטליות לחלוטין שאינן אנשים. ניתן לכתוב תוכנה שתחזיק מטבעות, תסחור, תלווה אותם לפי אלגוריתמי סיכון, תשקיע את הכסף בחזרה במקומות נושאי

תשואה, וכך הלאה, ללא מגע יד אדם, כמערכת אוטונומית לחלוטין.

המדינה תיאלץ להמציא את עצמה מחדש, ובעיקר את היחס שבינה לבין האזרח. בעולם פתוח כלכלית, ללא גבולות מסחר, יריבו המדינות על ליבם של התושבים, שכן קל מאוד יהיה להגר ולעבור למקום אחר. המקומות הראשונים שישגשו יהיו אלה שיפתחו עוד את השערים בפני כלכלה חופשית ודיגיטלית. הם ימשכו אליהם את המתעשרים החדשים, שצברו הון דיגיטלי ניכר ואינם מעוניינים לשלם ממנו מיסים ישנים. במדינה הזו, היא שמה "ביטקוניה", ייגבו מהם רק מס תושבות ומס הכנסה שיבוסס על דיווח עצמי בלבד וישולם גם הוא במטבע דיגיטלי. בתהליך שמחזק את עצמו תהפוך מדינה זו להיות אחת המדינות העשירות בעולם. ביטקוניה תהיה החלוצה, ושכנותיה יבינו באיחור את הפספוס שלהן וינסו לשחזר את הצלחתה. לאחר ביטקוניה החלוצה, עוד ועוד מדינות תהיינה אנוסות לקבל עליהן את הדין הדיגיטלי.

סדר עולמי חדש עומד לקום.

כיום, הדולר חזק משום שמאחוריו עומדים הרבה אנשים עם הרבה רובים. מאחורי הביטקוין אין אף רובה, נושאת מטוסים או צוללת גרעינית, ולמרות זאת הוא עמיד, חזק ובלתי ניתן להשמדה. הוא עובדה קיימת; שד שיצא מהבנק ואינו יכול להידחס שוב פנימה.

אם הביטקוין ישתלט על מפת העולם, מדינות קטנות עשויות להתגלות כמעצמות חדשות והמעצמות הישנות עלולות לפשוט רגל ולהיקבר תחת חולותיה הנודדים של ההיסטוריה. ממלכת הדולרים הירוקים עלולה להתגלות כחסרת ערך, ובמקומה עשויה לקום ולפרוח מדינה נידחת שהחלה לצבור ביטקוינים לפני שנים. אולי תהיה זו איסלנד, שבה עלויות ייצור החשמל נמוכות מאוד וחלק ניכר מהכרייה העולמית מתרחש בה, ואולי סין, ואולי היתרון הכלכלי של מדינה ייקבע לפי איכות כוח האדם והיזמות הקריפטוגרפית של תושביה.

בשיחת סלון שגרתית, המשפט "הביטקוין ישתלט על מפת העולם" נשמע מופרך ודמיוני; אולם בפועל, זהו תסריט ריאלי לחלוטין. הבנק המרכזי של קנדה פרסם השנה ניתוח שבחן מה יהיו שיעורי הריבית בעולם כאשר יהפוך הביטקוין לסטנדרט העולמי החדש, כך שמתבעות שונים יונפקו כנגדו כשם שהונפקו בעבר כנגד זהב.¹² נראה כי במחלקת המחקר של הבנק של קנדה הפסיקו לטמון את הראש בחול. מובן שאין בידינו כל ערובה כי אחד מן התסריטים הללו יתממש, אולם ברור כי עצם קיומם של הביטקוין ושל יתר המטבעות הקריפטוגרפיים – כטכנולוגיה, כגשר חברתי וכערוץ לשמירה על ההון – סולל חלופות ממשיות לסדרי בראשית של הכלכלה העולמית.

למדינת ישראל, עולם הקריפטו הוא איום אך גם הזדמנות אדירה. מקובל לומר כי במדינת ישראל מצוי ריכוז מוחות מהטובים בעולם (לפי פרסומים זרים), שפע יצירתיות, יוזמה וגם צבא חזק. ככל שמדינת ישראל תשכיל לאמץ את כלכלת

הקריפטו מהר יותר, כך יהיה לה יתרון יחסי נוסף על שכנותיה הקרובות והרחוקות. כבר כיום ישנן חברות קריפטו ישראליות רבות, אך בהשקעה מיידית נוכל להפוך למעצמה המובילה בעולם בתחום זה, לאבן שואבת ליזמים ולמקור אנרגיה כלכלית בלתי נדלית, שרק החלה את צעדיה הראשונים. עכשיו הוא הזמן, כשהתחום עודנו בראשית פריחתו ושחקנים רבים טרם נכנסו לִמְרוֹץ.

מדינת ישראל אינה יכולה להרשות לעצמה לומר "לי זה לא יקרה". נציב מס הכנסה אינו יכול לנוח בכיסאו ולחשוב שבסופו של דבר תימצא דרך לחייב את כולם בתשלום מיסים בדיוק כמו היום; שר הביטחון אינו יכול להניח שתקציבו יתפח לנצח; נגידת בנק ישראל אינה יכולה עוד להרשות לעצמה להחזיק יתרות מטבע זר בדולרים בלבד. הביטקוין כבר מזמן אינו מטבע דמיוני.

אם מדינת ישראל תיערך לכך כעת, יש לה סיכוי טוב להצליח.

אני שם על זה ביטקוין.

4. הרצות רבות מאוד של הפונקציה. מכיוון שמהירות המחשבים עולה בהתמדה, הפתרון עשוי להפוך קל ומהיר יותר לעומת פרוטוקול הביטקוין המחייב פתרון רק כל עשר דקות במוצע. לכן, הפונקציה נעשית קשה יותר ככל שהמחשבים נעשים מהירים יותר (נבדק אוטומטית ומתעדכן כל שבועיים). יעד זה נקרא ה־target כך שתוצאת ה־Hash תהיה נמוכה מהמטרה. כדי שיעד זה יושג, נדרש רצף ארוך יותר של אפסים, וכך במקום אפס אחד בהתחלה, נצטרך למצוא טקסט שייתן תוצאה שתתחיל בשני אפסים, שלושה אפסים וכן הלאה. כיום, פתרון החידה מחייב מציאת רצף של 18 אפסים לפחות. פתרון כזה זה מצריך טריליוני חישובים, לא פחות, כלומר אנרגיה רבה נדרשת כדי לכרות כל בלוק ולרשום אותו בבלוקצ'יין.

שימו לב כי ברגע שהחידה נפתרה, קל מאוד לוודא את נכונותה: כל אחד יכול להריץ את פונקציית ה־Hash על הבלוק האחרון ולוודא שקיבל רצף מתאים של אפסים בהתחלה.

5. כיום, למעשה, כוח החישוב של רשת הביטקוין גדול יותר מכל מחשבי העל גם יחד.

6. המונח "ארנק" מעט מטעה. להבדיל מארנק כסף "רגיל", המכיל מטבעות ושטרות, ארנק הביטקוין מכיל רק מפתחות. נכון יותר לחשוב על ארנק הביטקוין כעל מחזיק מפתחות. כמו במחזיק מפתחות אמיתי, אם מישהו שכפל עותק מהמפתח שלכם ללא רשותכם, הוא יוכל להיכנס אליכם הביתה. לכן יש לשמור על הארנק, כלומר על מחזיק המפתחות שלכם, היטב. וכך איש לא יוכל לפתוח את הדלת אל כספכם ללא רשות.

1. באפריל 2013 מחקו הבנקים בקפריסין כ־15 אחוז מהפיקדונות הפרטיים של לקוחות הבנק כדי לשלם את חוב המדינה.

2. לספקנים נוכרי כי בשנות השמונים האינפלציה השנתית בישראל הגיעה לכדי 445 אחוז.

אף שכלכלתה של מדינת ישראל חזקה לעת עתה, יצירת אינפלציה של שני אחוזים בשנה היא יעד מוצהר של בנק של ישראל. זו אינה טעות: שחיקת כוח השקל היא מדיניות!

3. למתקדמים, הנה הסבר מוקצר של "החידה". ישנה פונקציה מתמטית ידועה בשם Hash שמקבלת כקלט כל רצף של טקסט (לא משנה אם זו אות אחת או ספר שלם) ומחזירה תמיד ערך בן 32 ספרות ואותיות (למשל: e9b93a9e85). כאשר רוצים לכתוב בלוק חדש בבלוקצ'יין, הכורים כותבים את הבלוק, שהוא כאמור רצף העסקאות שנוצרו בעשר הדקות האחרונות, ומחשבים לו את פלט ה־Hash המתאים, כאשר כדי לכתוב את הבלוק בבלוקצ'יין חייבים לקבל תוצאה שמתחילה ברצף של אפסים. אולם בפונקציית Hash אי אפשר לדעת מראש מה תהיה התוצאה – לפעמים היא מתחילה באפס ולפעמים לא (בדוגמה לעיל היא מתחילה דווקא בשבע). כדי לגרום לתוצאה להתחיל במספר אפס עלינו להוסיף טקסט כלשהו בסוף הטקסט המקורי של הבלוק (למשל סימן קריאה בסוף הטקסט), להריץ את הפונקציה שוב ולבדוק אם קיבלנו תוצאה טובה. אם לא קיבלנו אפס, עלינו להוסיף עוד סימן קריאה ושוב לבדוק, וכך שוב ועד שנקבל אפס כספורה ראשונה. תהליך כזה זה עלול לדרוש

7. מה גם שרוב תוכנות הארנק מייצרות כתובת ביטקוין חדשה בכל העברה כספית, ולכן לכל משתמש יש כתובות רבות מאוד, גם אם יש לו רק ארנק אחד. ממילא, המעקב אחרי הכסף ושיוכו לאדם פלוני קשה ביותר.
8. יש בביטקוין מיליוני משתמשים. רק אל ה-coinbase מצטרפים כמיליון משתמשים חדשים (עם שם משתמש וסיסמה) מדי חודש. לא מתקבל על הדעת שכל המשתמשים הללו, או רובם, עבריינים.
9. בוונצואלה, בהודו ובמקומות אחרים שבהם שולטת המדינה על ההון באופן הדוק, הביטקוין יקר מאוד לעומת מחירו בכל מקום אחר. מבחינת המקומיים, יש לו ערך רב יותר מזה של המטבע המקומי – שאינו יכול לצאת מהמדינה או להציל אותם ביום סגריר.
10. ואכן, ההצפנה מכחישה את יכולתה של המדינה לסגור מוסדות ולאנוף את חוקיה. במדינת ישראל נאסר הסחר בסמים, אולם בפועל, בסיוע מערכת ההצפנה של אפליקציית טלגרם, קמה לאחרונה בארץ רשת משלוחי קנביס המונה כבר אלף סוחרים ו-70 אלף לקוחות. כשטכנולוגיה מאפשרת פוגשת קהילה דורשת, המדינה והאכיפה נותרות מחוץ לתמונה.
11. אלה לוי-וינריב, "המטבעות הווירטואליים עלו על הכוונת של רשות המסים", גלובס, 1.8.2017.
12. <http://www.bankofcanada.ca/wp-content/uploads/2016/03/swp2016-14.pdf>
- 85 בוימבואה, הביטקוין נסחר כעת בפרמיה של 85 אחוזים! ראו <https://www.techjuice.pk/zimbabwe-one-bitcoin-worth-7200/>