מה זה מטבע וירטואלי?

מטבע שאין לו ביטוי פיזי, הוא משמש לסחר וקנייה כמו כל מטבע אחר אך עונה על 3 תנאים:

1. המטבע הוא אותנטי ואינו מזויף
2. מובטח שימוש יחיד בכל מטבע ללא קנייה או מכירה כפולה ("double-spend" problem)
3. הוכחת בעלות על המטבע – אף אחד לא יכול לטעון שהמטבע שלו.

על אף שבכל מטבע האתגרים האלו קיימים, במטבע וירטואלי קיימות התנאים האלו נעשית קשה לאין ערוך.

הצורך במטבע וירטואלי

"קפיצת דרך משמעותית בהיסטוריה אירעה כאשר המגעים החברתיים, התרבותיים והכלכליים באזור מסוים בנו די אמון שיאפשר להתחיל להשתמש בכסף חסר ערך אובייקטיבי, שקל לאגור ולנייד אותו." (קיצור תולדות האנושות, יובל נח הררי, עמ' 186)

היה צורך בפתרון להגבלות של כסף פיזי שמקשה על ניידות ואגירה, ניתן לזייף אותו וכן שווי המטבע ויצורו כפופים לממשל או לרגולציה.

בשנות ה80 המאוחרות, עם התפתחות הקריפטוגרפיה – נעשו מספר ניסיונות ליצור מטבע וירטואלי שיסמן בעלות על מטבע לאומי או משאב פיזי עם ערך כספי (כמו זהב) – כיוון שהמערכות האלה היו נתונות למרכז ניהול יחיד או שרת מרכזי – הן היו נתונות למתקפות של האקרים וממשלות. מערכות אלה היו דומות מדי לבנקים או כסף ממשלתי אחר ולכן גם לא החזיקו כשבעלי אינטרסים פגעו בדרכים שונות במקור המערכת.

מה זה ביטקוין?

ביטקוין הוא שם של אוסף טכנולוגיות שמהוות בסיס למערכת אקונומית של כסף.

ממציא המערכת הוא אדם (או קבוצה) בשם סאטוֹשי נַקאמוֹטוֹ (Satoshi Nakamoto) . אחרי מספר המצאות קודמות, סאטושי נקאמוטו פרסם ב2008 ברשימת תפוצה רעיון אחד המאגד את כל הרעיונות לכדי מערכת אחת, וב2009 פרסם את גרסת ביטקוין הראשונה וב3 בינואר 2009 ב18:15 נכרה על ידו הבלוק הראשון.

המערכת מנצלת טכנולוגיה וקריפטוגרפיה על מנת ליצור מטבע שאינו סובל מחסרונות של כסף פיזי או כסף דיגיטלי והיא מוגנת מפריצות, זיוף, אינפלציה ואינה כפופה לשום גוף ממשלתי או בעל כוח.

סחר וקנייה במטבע מתבצעים באמצעות פרוטוקול תקשורת של ביטקוין (peer-to-peer) שאינו מאוכסן ואינו תלוי בשום גוף מרכזי או שרת – מה שמעניק לביטקוין את יתרונו המרכזי.

למשתמשי ביטקוין יש מפתחות אישיים וייחודיים שמאוחסנים בארנק דיגיטלי במחשב המשתמש וע"י המפתחות המשתמשים יכולים להוכיח את בעלותם על המטבעות שאיתם הם סוחרים.

כריית המטבע הוירטואלי עצמו נעשית באמצעות חישוב מתמטי סזיפי ומורכב ("Proof-of-Work") אך כרייה כזאת יכולה להיעשות ע"י כל משתמש (בפרט - ע"י כל כח חישוב מתמטי – מחשב, פלאפון, GPU). פרוטוקול הביטקוין מבטיח שיווצר מטבע כל 10 דקות בממוצע ומרגע שנוצר מטבע כזה – כלל המשתמשים מסכימים על קונצנזוס באשר למצב ההעברות של המטבעות ומתחילה עבודת כרייה חדשה על המטבע הבא.

ביטקוין הוא פרויקט קוד פתוח ועקרונות הפרוטוקול פתוחים לכולם – מה שמקשה על התקפת האקרים (התקפה מחייבת הבנה עמוקה של התנהגות הפרוטוקול ולא חשיפת הפרטים – עקרון קרקהופס).