



מגמות כלליות
והתפתחותם של
סיכוני הלבנת
הון ומימון טרור
בעולם הנכסים
הוירטואליים

הרשות לאיסור הלבנת הון
ומימון טרור
דצמבר 2025





תוכן עניינים

3	תקציר מנהלים
5	שוק הנכסים הוירטואליים
6	מגמות פשיעה, הלבנה ומימון טרור
11	התפתחויות טכנולוגיות וסיכוני הלבנת הון ומימון טרור
19	האסדרה בעולם ובישראל
23	דגלים אדומים

תקציר מנהלים

שוק הנכסים הוירטואליים ('קריפטו') נמצא בעיצומה של תנופה מחודשת עם שווי שוק מוערך של טריליוני דולרים, מחזורי מסחר, המגיעים עד מאות מיליארדי דולר ביום, ואימוץ גובר מצד הציבור הרחב והמוסדות הפיננסים המסורתיים. שוק זה מאופיין בצמיחה מהירה, חדשנות טכנולוגית ומגוון רחב של יישומים, וטומן בחובו פוטנציאל מהותי לקידום יעילות והכלה פיננסית. התפתחויות אלו מלוות בסיכונים ייחודיים ובכללם סיכונים הלבנת הון ומימון טרור, אשר נובעים, בין היתר, ממאפייני הטכנולוגיה, היות והפעילות חוצת גבולות ולעיתים נטולת גבולות גיאוגרפיים וקצב השינויים המהיר.

בשנים האחרונות מסתמנות מספר מגמות ותופעות פשיעה משמעותיות בעלות השלכה ישירה על סיכונים הלבנת הון ומימון טרור באמצעות נכסים וירטואליים. אחת המגמות הרחבות היא מעבר גובר של גורמי פשיעה, מלבני הון ומממני טרור לשימוש במטבעות יציבים (Stable Coins), אשר מאופיינים בפונקציונליות דומה בהיבטי הסיכון להלבנת הון ומימון טרור של נכסים וירטואליים אחרים, אך מעניקים למחזיקים בהם הגנה מפני תנודתיות גבוהה במחיר.

הגידול העצום בהשקעות של הציבור בארץ ובעולם בנכסים וירטואליים הביא עמו גם גידול בהיקפי ההונאות המבוצעות כלפי ציבור המשקיעים. כמו כן, חל גידול בשימוש בנכסים וירטואליים כאמצעי להלבנת ההכנסות המופקות מן ההונאות. מתקפות כופרה ממשיכות להוות איום משמעותי בהקשר לשימוש בנכסים וירטואליים, לאור דרישות כופר גדלות בנכס וירטואלי. שינוי מגמה נוסף קשור לאמצעים המשמשים לריבוד הנכסים הוירטואליים שהתקבלו מן העבירה, ובראשם מעבר משימוש בשירותי "ערבול" ('Mixers') לגשרים בין-רשתות ('Cross-Chain Bridges').

בנוסף לעבירות שצוינו, הקלות שבהעלמת הכנסות שהופקו מרווח, המופק מפעילות בנכסים וירטואליים, כמו גם מורכבות האסדרה המיסויית של נכסים וירטואליים, הנובעת ממאפייניהם הייחודיים ומפערים רגולטוריים בתחום, מעלים את החשש להעלמות מס בהיקפים גדולים, תוך הסתייעות בזירות מסחר זרות או בעלות משטר פיקוח רופף, לצורך הסתרת הפעילות הפיננסית.

לצד זאת, זירות מסחר זרות בסיכון גבוה ושירותי הלבנת הון מקצועיים, כגון זירות מסחר "מקוננות" הפועלות כזירות משנה לא מפקחות בתוך זירות מסחר בינלאומיות גדולות יותר, מציעות מענה מתוחכם בעל פוטנציאל לפעילות עבריינית.

גם בתחום מימון הטרור נרשם שימוש גובר בנכסים וירטואליים, עם העדפה למטבעות יציבים ושיטות פעולה מתוחכמות יותר, הכוללות מעבר תכופ בין כתובות ארנק חדשות, פרסום כתובות ארנק בערוצי מדיה מגוונים ושיתוף ידע בין פעילים לגבי פלטפורמות מומלצות, שירותים ייעודיים והתפתחויות טכנולוגיות חדשניות, כדוגמת פלטפורמות מסחר בין עמיתים (P2P), יישומי כלכלה מבוססת (DeFi) ומסחר באמצעות בוטים בפלטפורמות חברתיות. היות ואלו, אינן חוסות בהכרח תחת משטרי איסור הלבנת הון ומימון טרור, הן בעלות פוטנציאל לניצול לרעה על ידי גורמים עברייניים ומציבות גם הן אתגרים משמעותיים, בפני רשויות החוק והאכיפה ברחבי העולם.

בעקבות האימוץ הרחב והתפתחות תחום הנכסים הוירטואליים בעשור האחרון, ארגון ה-FATF אשר אמון על קביעת הסטנדרטים הגלובליים במאבק בהלבנת הון ומימון טרור, עדכן את הסטנדרטים הבינלאומיים, על מנת להתמודד עם האתגרים הייחודיים שצמחו בתחום. בין השאר, הוחלו סטנדרטים בינלאומיים גם על נכסים וירטואליים ונותני שירותים בתחום זה, וכן הוחל עקרון ה-Travel Rule הקובע, כי על נותני שירותים בנכס וירטואלי (Virtual Asset Service Providers - VASPs) להעביר את פרטי המעביר והנעבר בכל עסקה. הארגון גיבש מפת דרכים לחיזוק

יישום ההמלצות ומעקב אחר הטמעתן והוא מפרסם דוחות תקופתיים על מנת לזהות אתגרים¹ ולשתף דרכי פעולה מומלצות.²

צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירות בנקסי פיננסי ונותני שירותי אשראי למניעת הלבנת הון ומימון טרור) התשע"ח - 2018, אשר חל על נותני שירותים פיננסיים ונכנס לתוקף בנובמבר 2021, מחיל חובות מפורטות על נותני שירות בנקסי פיננסי, ולראשונה גם על נותני שירות במטבע וירטואלי. חובות אלו הותאמו לסטנדרטים של ארגון ה-FATF ולפעילותם של נותני השירותים בנקסים וירטואליים. מדינת ישראל ממשיכה לעקוב אחר התפתחויות בתחום ופועלת לגבש אסדרה משלימה כמענה לצרכים הייחודיים של שוק הנכסים הוירטואליים.

הרשות לאיסור הלבנת הון ומימון טרור (להלן: "הרשות") רואה חשיבות רבה במעקב אחר המגמות בתחום והיכרות עמן, בזיהוי סיכונים הלבנת ההון ומימון הטרור הנובעים מהם, ובמתן כלים לניהול סיכונים הלבנת הון הכרוכים בתחום, בדגש על הגופים הפיננסיים המחויבים בזיהוי פעילות בלתי רגילה ודיווח בגינה לרשות. מסמך זה נועד לספק תמונת מצב עדכנית ולהנגיש ידע מקצועי בנושא זה, במטרה לסייע לגורמים רגולטוריים, רשויות אכיפה, מוסדות פיננסיים וגורמים עסקיים הפועלים בתחום.

בכל מערכת פיננסית ובכל פעילות באמצעות נכס או שירות פיננסי, בנוסף על הפעילות הכלכלית הלגיטימית, קיימים גם סיכונים הלבנת הון ומימון טרור. כך הדבר גם בכל הנוגע לפעילות באמצעות נכסים וירטואליים, קרי, הגם שמרבית הפעילות לגיטימית, היא כוללת בחובה סיכונים הלבנת הון ומימון טרור.

הסטנדרטים הבינלאומיים של ארגון ה-FATF אינם קובעים מראש כי תחום פעילות מסוים נמצא בסיכון גבוה להלבנת הון ומימון טרור, אלא דורשים לבחון ולזהות תחומי פעילות החשופים לניצול לרעה להלבנת הון ומימון טרור. זאת, על מנת שהסקטורים הציבורי והפרטי יפעלו להלבנת הסיכונים הכרוכים בפעילות ויבצעו הערכת סיכונים לפעילות הספציפית המתבצעת - הכוללת התייחסות לסוג השירותים, המוצרים, הלקוחות, המדינות או הטריטוריות מולם הם עובדים, איתנות משטר איסור הלבנת הון, הציות ומידת עמידת נותן השירות ברגולציה המקומית ובסטנדרטים הבינלאומיים בתחום איסור הלבנת הון ומימון טרור.

בהתאם לסטנדרטים של ה-FATF יש לפעול גם בתחום הנכסים הוירטואליים כבכל תחום פעילות אחר החשוף לסיכונים הלבנת הון ומימון טרור, קרי - נקיטה בגישה מבוססת סיכון בהתאם להיקף הסיכון הפרטי והייחודי שזוהה, וזאת בניגוד לגישה של התעלמות מהסיכון או הימנעות מסיכון (De-risking).

¹ FATF, יולי 2024, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*, [קישור](#).
² FATF, אוקטובר 2021, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, [קישור](#).

שוק הנכסים הוירטואליים

גידול בהיקפי הפעילות: שוק הנכסים הוירטואליים חווה בעשור האחרון תנודתיות רבה. לאחר תקופת צמיחה מהירה בשנים 2020-2021, השנים 2022-2023 אופיינו בירידות חדות בעקבות סדרה של משברים תאגידיים והונאות. החל מ-2024 ובמהלך שנת 2025, רשם שוק הנכסים הוירטואליים התאוששות מלווה בתנודתיות ובירידות חדות ברבעון האחרון של 2025. שווי השוק של המטבעות הוירטואליים הנסחרים נאמד כיום בטריליוני דולרים. עם זאת, שילובם בשירותים פיננסיים מרכזיים עדיין מוגבל.

התפתחות טכנולוגית: התפתחות טכנולוגיית של הבלוקצ'יין, ובעיקר פיתוח רשת אתריום והחוזים החכמים, הביאו למגוון עצום של יוזמות ופתרונות טכנולוגיים, רשתות נוספות, התפתחות תחום ה-DeFi וה-NFT, מנגנוני שליטה מבוזרים (DAO), בריכות נזילות וספקי נזילות (liquidity pools & liquidity providers) וככלל ליצירת תעשיה עולמית השוקדת על פיתוחים בלתי פוסקים ויצירה יומיומית של מטבעות וירטואליים.

צמיחת המטבעות היציבים (Stablecoins): מנוע משמעותי נוסף בצמיחתו ובהתרחבותו של שוק הנכסים הוירטואליים בשנים האחרונות, הוא האימוץ הגובר של מטבעות יציבים. מחירים של נכסים וירטואליים אלו מוצמד לערך מטבע שהנו הילך חוקי, כגון הדולר, או לנכס ממשי כלשהו. באופן זה פוחת הסיכון הכרוך בתנודתיות הגבוהה של נכסים וירטואליים אחרים, כגון ביטקוין או מטבעות אלטרנטיביים (altcoins). לאור עלויות השימוש הנמוכות של מטבעות אלו, בהשוואה למערכות העברת כספים מסורתיות, הפכו אלו לחלופה אטרקטיבית הן לצורך ניהול השקעות באופן שאינו מחייב מעבר להילך חוקי בעת קניה ומכירה של נכסים וירטואליים והן למגוון שימושים עסקיים ופרטיים.

מהלכים רגולטוריים בארה"ב: במהלך 2024 אישרה ארה"ב פעילות של קרנות סל ותעודות סל על נכסים וירטואליים. אישור זה היווה נקודת מפנה נוספת בשוק הנכסים הוירטואליים. קרנות אלו זכו להצלחה חסרת תקדים, לוו בהשקעות בהיקף של עשרות מיליארדי דולרים, ועקפו בביצועיהן השקות של קרנות סל מסורתיות. הצלחה זו הובילה גופים מוסדיים, בהם קרנות פנסיה וקרנות גידור, אשר קודם לכן היססו להיכנס לתחום, להשקיע בנכסים וירטואליים.³

צמיחת הפוטנציאל העסקי והפיננסי הגלום בענף והשתכללות השוק כרוכים במקביל בעליה בסיכונים הנשקפים מגורמים פליליים המבקשים לנצל לרעה את מאפייני השוק הייחודיים לצורך פשיעה פיננסית, הלבנת הון ומימון טרור, כפי שיפורט להלן.

³ להתייחסות נוספת ראו עמודים 11-12, בפרק אודות מטבעות יציבים.

מגמות פשיעה, הלבנה ומימון טרור

בשנים האחרונות גובר השימוש בנכסים וירטואליים במגוון תופעות פשיעה וכן כאמצעי להלבנת הון של תוצרי העבירה, בין אם הופקו בנכס וירטואלי ובין אם בנכס פיננסי אחר, וכאמצעי למימון טרור. גורמים עברייניים מנצלים את מאפייניהם, השירותים והכלים הייחודיים, שהתפתחו סביבם, לצורך העברת כספים מהירה, תוך הסוואה וטשטוש של העקבות המובילות לעבירות המקור. ככל שפעילות פלילית המערבת נכסים וירטואליים מתרחבת וכוללת מגוון רחב יותר של עבירות, כך ניכרת גם התמקצעות עבריינית גוברת.

על פי נתוני חברות לניתוח בלוקצ'יין⁴ שנת 2024 הייתה, ככל הנראה, שנת שיא בהיקף הנכסים הוירטואליים המעורבים בפעילות פלילית, כאשר בשנים האחרונות נרשם גידול שנתי ממוצע של כ- 25%. ההערכות הראשוניות נעות סביב היקף פעילות פלילית בסך 40 - 45 מיליארד דולר,⁵ אולם ניסיון השנים הקודמות מלמד, כי נתון זה צפוי להתעדכן כלפי מעלה עקב זיהוי בדיעבד של כתובות ארנק נוספות המשויכות לפעילות פלילית. רשתות הבלוקצ'יין המובילות בהיקפי הפעילות הפלילית הן TRON, ואחריה Ethereum ו-Bitcoin. נתונים אלו משקפים מגמת מעבר לרשתות התומכות במטבעות יציבים, עמלות נמוכות ושימוש בחוזים חכמים, לצד המשך דומיננטיות של ביטקוין בתחומי פשיעה מסוימים.

להלן מפורטת סקירה שערכה הרשות ביחס למגמות וההתפתחויות העיקריות של תופעות פשיעה פיננסית, הלבנת הון ומימון טרור המבוצעות באמצעות נכסים וירטואליים. תופעות פשיעה אלו מהוות מארג מורכב של פעילות בנכסים וירטואליים, המחייב התמודדות רגולטורית, מודיעינית ואכיפתית.

הונאות משקיעים

חלק ניכר מפעילות הפשיעה והלבנת הון המערבת נכסים וירטואליים מקושרת להונאות מסוגים שונים, כאשר במקרים מסוימים הפעילות בנכסים וירטואליים משמשת לביצוע ההונאה ואילו באחרים היא משמשת כאמצעי להלבנת ההון. [נתונים שפרסם](#) נאמדים בעשרות מיליארדי דולרים בשנים האחרונות ונמצאים במגמת עלייה. כך לדוג' על פי [נתונים שפרסם](#) ה-FBI היקף ההונאות בנכסים וירטואליים בארה"ב בלבד עמד על כ- 9 מיליארד דולר בשנת 2024, עלייה של 66% לעומת שנת 2023.

הונאות משקיעים צמחו במקביל להתרחבות שוק הנכסים הוירטואליים, לעיתים קרובות על רקע חוסר היכרות של הציבור עם התחום, לאור הקלות והמהירות בהן ניתן להעביר נכסים וירטואליים וכן עקב ההד התקשורתי סביב עליות חדות בשווי הנכסים והפיתוי להשיג תשואה מהירה וקלה.

בתרחיש טיפוסי של הונאה מסוג זה, נוכל יאתר קורבן פוטנציאלי ברשתות חברתיות, אפליקציות מסרים מידיים ופלטפורמות מקוונות באמצעות פרסומות המבטיחות הזדמנויות השקעה בעלות תשואה גבוהה. נוכלים מתחזים כמשקיעים מנוסים בתחום הנכסים הוירטואליים ואף יוצרים לשם כך זהות בדויה ברשתות החברתיות, לעיתים תוך שימוש בדמות פיקטיבית של גורם מפורסם, על מנת ליצור אמינות להצעת ההשקעה. לאחר ביסוס קשרי אמון עם הקורבן, ישכנע הנוכל את הקורבן להעביר סכומי כסף גדלים והולכים להשקעה בנכסים וירטואליים. **בשלב בו הנוכל פועל על מנת לבסס אמון, סכומי ההשקעה לכאורה יהיו לרוב נמוכים ויוצג לקורבן רווח מהיר ומשמעותי על מנת להביא להעברת כספים נוספת בסכומים משמעותיים יותר.**

⁴ Chainalysis, *2025 Crypto Crime trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized*, ינואר 2025, [קישור](#). TRM, *2025 Crypto Crime Report - Key trends that shaped the illicit crypto market in 2025*, פברואר 2025, [קישור](#).

⁵ היקפים אלו מהווים אחוז נמוך ביותר מכלל הפעילות הגלובלית בנכסים וירטואליים. מחזור המסחר היומי בנכסים וירטואליים עומד על עשרות עד מאות בודדות של מיליארדי \$ בשנה.

הקורבנות מונחים לרכוש נכסים וירטואליים בזירות מסחר מוכרות ולהעבירם לכתובות ארנק בשליטת הנוכל, אשר מוצגות כשייכות לפלטפורמת מסחר או כהשקעה לגיטימית. במקרים אחרים, כדי להימנע מחשיפה, יונחה הקורבן למשוך מזומן ולרכוש את הנכסים הוירטואליים באמצעות כספומט של נכסים וירטואליים.

על מנת לשמר את אמון הקורבן ולעודד "השקעות" נוספות, עשוי הנוכל להציג דיווחים ודפי חשבון כוזבים, המראים רווחים מההשקעות הפיקטיביות. בשלב מסוים, כאשר הקורבן מעביר סכומי כסף משמעותיים, לעיתים מאות אלפי ש"ח או מסרב להעביר כספים נוספים, הנוכל ינתק קשר וייעלם. במקרים אחרים ינסה לשכנע את הקורבן, שעל מנת לפדות את רווחי ההשקעה עליו להעביר סכום נוסף כתשלום מס. מוכרים מקרים נוספים בהם הנוכל יתחזה לגורם המציע סיוע בהשבת הכספים בתמורה לתשלום.

ניתוח של דיווחים על פעילות בלתי רגילה שהתקבלו ברשות מעלה כי תופעה זו של הונאות משקיעים בולטת גם בישראל. מדובר באחת מן התופעות המשמעותיות ביותר, הן לאור מספר הדיווחים המתקבלים בנושא בתחום הנכסים הוירטואליים והן בהיקף הכספים המעורבים. במקרים רבים, הנוכלים פועלים מול אוכלוסיות פגיעות יותר, כגון מבוגרים ועולים, ומנחים את הקורבנות לרכוש נכסים וירטואליים דרך זירות מסחר מוכרות, באמצעות העברות בנקאיות או תשלומי אשראי. עוד עולה, כי ישנם מקרים בהם הנוכל משתלט על המחשב או מכשיר הטלפון של הקורבן, מקבל באמצעותם גישה לחשבון הבנק או פרטי האשראי של הקורבן, ומבצע רכישות של נכסים וירטואליים המועברים לאחר הרכישה לכתובות ארנק של הנוכל.

מן הדיווחים עולה כי שיטות ההונאה משתכללות בין היתר על ידי ניצול טכניקות שונות של הנדסה חברתית ומצגי שווא, הנחייה והדרכה מפורטת של הקורבן כיצד לבצע את הפעילות באופן שלא יעורר את חשדם של הגופים המדווחים, זיוף מסמכים של מוסדות רשמיים לצורך יצירת מראית עין לגיטימית לפעילות וכן שימוש בכספומטים של נכסים וירטואליים כאמצעי להעברת הכספים מהקורבן לנוכל.

ראוי להדגיש כי קיימת מודעות מצד הגופים המדווחים לתופעה וכי הגופים פועלים לצמצום ניצול לרעה של השירותים הניתנים על ידם למטרות הונאה, תוך נקיטת צעדים להגנה על לקוחותיהם ודיווח לרשות על פעילות בלתי רגילה אשר זוהתה על ידם. עם זאת, נוכח התרחבותה המתמשכת של התופעה והתחכום ההולך וגובר של מבצעייה, נדרש להמשיך ולשמור על ערנות מרבית, לשכלל את כלי הניטור והאיתור של פעילות חריגה, וכן להגביר את המודעות הציבורית, ובפרט בקרב אוכלוסיות פגיעות לסיכונים אלו.

הונאות משקיעים של עשרות מיליוני דולרים

בשנת 2023, מנכ"ל בנק בקנוס נידון ל- 24 שנות מאסר לאחר שמעל ב- 47 מיליון דולר מכספי הבנק והעביר אותם לנוכלים במסגרת הונאת השקעה בנכסים וירטואליים.

חקירת הפרשה העלתה כי המנכ"ל, שעבד במשך 3 עשורים בבנק, החל לבצע השקעות בנכסים וירטואליים מכספו הפרטי לאחר שקיבל בדצמבר 2022 הודעה מגורם לא מזוהה באפליקציית מסרים מיידיים. הקשר, שהחל לכאורה בהודעה תמימה שנשלחה בטעות למען הלא נכון, התפתח במהרה ובתוך זמן קצר עברו הצדדים לדיונים על השקעות.

הנוכל הצליח לשכנע את המנכ"ל להשקיע סכומי כסף משמעותיים תוך הבטחה לתשואות גבוהות. בהמשך כשטען כי נדרשים כספים נוספים על מנת לשחרר את הרווחים, משך הבנקאי את כספי קרן החיסכון שהקים למימון לימודי בתו. הדרישות הכספיות המשיכו תחת טענות שונות כגון תשלום עמלות או מסים ובשלב זה הבנקאי כבר עבר לגניבת כספי הכנסייה המקומית. בשיאה של ההונאה במאי 2023 הוא הורה לעובדיו להעביר מיליוני דולרים מפיקדונות הבנק, כאשר במהלך תקופה קצרה יחסית של שמונה שבועות הוא הצליח להעביר עשרות מיליוני דולרים מכספי הבנק אל הנוכלים. המעילה הובילה לקריסתו של הבנק זמן קצר לאחר מכן ולפגיעה קשה בבעלי המניות ובחוסכים.

דיווח על פעילות בלתי רגילה לדוגמה

ברשות התקבל דיווח לגבי לקוח של VASP (נותן שירות בנכסים וירטואליים) שביצע מספר רכישות של נכסים וירטואליים. **הלקוח טען שגורמים שהציגו את עצמם כעובדים של אותו VASP הציעו לו להשקיע בנכסים וירטואליים תמורת תשואות גבוהות במיוחד. בתחילה ביקשו ממנו להעביר מספר אלפי ש"ח בודדים ובסמוך לאחר מכן דיווחו לו כי הרוויח סכום של עשרות אלפי ש"ח וכי על מנת למשוך את הכספים עליו להעביר סכום כסף נוסף באמצעות נכסים וירטואליים.** לאחר שהעביר את הסכום המבוקש שלחו לו תמונה של העברה כביכול וסיפרו לו שהרוויח עוד מאות אלפי ש"ח אך לצורך משיכתם עליו להעביר שוב סכום נוסף. בשלב זה ביקש הלקוח לראות שהכספים מתקבלים בפועל בחשבונו לפני שיבצע העברה נוספת. בתגובה אמר לו הגורם שתוך כשעה יראה את הכספים, אולם הכספים לא התקבלו.

כופרה

מתקפות כופרה ממשיכות להוות איום משמעותי, אף כי פעולות אכיפת חוק ברחבי העולם הצליחו במידה מסוימת בלום את התגברות התופעה. [על פי נתונים שפרסמה ממשלת ארצות הברית](#), בשנת 2024 נרשמה עלייה של כ- 15% במספר המתקפות ביחס לשנה הקודמת, עלייה מתונה יחסית ל- 77% עליה שנרשמה בשנת 2023. היקף המתקפות בארצות הברית היווה כ- 50% מהפעילות העולמית, ואילו המזרח התיכון היווה כ- 5% מהפעילות הגלובלית בשנת 2024, נתון שנותר ללא שינוי ביחס לשנה הקודמת. מרבית המתקפות התמקדו במגזרי השירותים המסחריים, הייצור, הטכנולוגיה והתקשורת.

למרות מאמצי האכיפה, סכומי הכופר שברו בשנת 2024 שיאים חדשים, כפי שממחיש התשלום חסר התקדים של כ- 75 מיליון דולר ששולם לקבוצת הכופרה Dark Angels.⁶ דרישות כופר הולכות וגדלות משקפות את העלייה בתעוזה ובתחכום של התוקפים, המנצלים כלים וטכניקות מתקדמות כדי להגביר את יעילות הסחיטה. **התשלום לתוקפים מבוצע באופן בלעדי באמצעות נכסים וירטואליים.**

בין המגמות שזוהו לאחרונה בתחום זה ניכר צמצום בשימוש במיקסרים להלבנת כספי כופרה, לצד מעבר לשימוש בגשרים בין-רשתיים (Cross-Chain Bridges) לשם טשטוש עקבות. השימוש בגשרים מאפשר העברה מהירה ויעילה יותר של כספים בלתי חוקיים. אף שביטקוין נותר המטבע העיקרי לתשלומי כופר ראשוניים, ממצאי המעקב אחר תנועת הכספים מצביעים על כך שחלק ניכר מהם מומר בהמשך לנכסים וירטואליים אחרים לצורך הסוואת מקורם.

דיווח על פעילות בלתי רגילה לדוגמה

בדיקה של מקור הנכסים של לקוחה שמכרה נכסים באמצעות VASP העלתה כי הם הגיעו מכתובת ארנק בעל היקף פעילות גבוהה ואשר **קיבל העברות מארנקים המשויכים לפעילות של מתקפות כופרה.**

תופעת מתקפות הכופרה ותשלומי דמי הכופר הנלווים אליה, סובלת מתת-דיווח משמעותי של קורבנות, אשר פוגמת ביכולת לגבש וליישם תוכנית פעולה אפקטיבית להתמודדות עימה. לאור זאת קיימת חשיבות רבה בהגברת המאמצים מצד הגופים המדווחים בזיהוי ודיווח על פעילות בלתי רגילה בתחום זה, על מנת לסייע לרשויות האכיפה והחוק במאבק בתופעה.

עבירות מס

היבטי המיסוי של נכסים וירטואליים מורכבים במיוחד, ובמדינות רבות, ישנם אתגרים בגיבוש מסגרת אסדרה ומיסוי אחידה וברורה לגביהם. המורכבות נובעת מאופיים המבוזר של הנכסים הוירטואליים, מהיעדר גורם מרכזי מדווח או אחראי לתשלום מס, מהאנונימיות היחסית שמאפשרת העברת נכסים בין ארנקים ומדינות, מהקושי לקבוע את שוויים בשל תנודתיות גבוהה, מהעובדה כי המודלים העסקיים משתנים במהירות ולאור היצירתיות הרבה במציאת דרכים ליצירת רווח באמצעות פעילות בנכסים וירטואליים.⁷ בשל מאפיינים אלו עלולים נכסים וירטואליים, להוות כלי אטרקטיבי עבור מעלימי מס המבקשים להסתיר את הונם תוך עקיפת המערכת הבנקאית המסורתית.

⁶ Forbes, יוני 2024, *Record-Breaking \$75 Million Ransom Paid To Dark Angels Gang*, [קישור](#).

⁷ רשות המסים פרסמה הנחיות בנוגע לדיווח על פעילות במטבעות וירטואליים ובקשה לתשלום מס המגיע במימוש מטבעות. השירות מאפשר תשלום מס ממנו **מטבעות וירטואליים**, בתנאי שהמערכת הבנקאית המסחרית בישראל סירבה לקבל את התשלום, כולל פתיחת חשבון. ראו [קישור](#).

הטיפולוגיות הנפוצות להתחמקות מדיווח לרשויות המס כוללות שימוש בזירות מסחר זרות הפועלות בתחומי שיפוט בהן הרגולציה אינה עומדת בסטנדרטים הבינלאומיים ו/או שרמת הפיקוח בהם רופפת, ניצול זהויות בדויות וניסיונות להסוות עסקאות בנכסים וירטואליים כהוצאה עסקית. בנוסף, נעשה שימוש בטכניקות מתקדמות להסתרת מקור הכספים, דוגמת שירותי ערבול (Mixers), וכן נרשמו מקרים של העלמות מס סביב רווחים מנכסים דיגיטליים ייחודיים דוגמת NFT.

בעקבות אתגרים אלו, מדינות רבות, ובכללן ישראל, פועלות לצמצום מרחב התמרון של משתמשים ונישומים, באמצעות הגברת חובת הדיווח על נכסים וירטואליים, חיזוק שיתופי פעולה בינלאומיים לאיתור פעילות חוצת גבולות, והטמעת כלים טכנולוגיים המאפשרים זיהוי של בעלויות בארנקים דיגיטליים וזיהוי זרימת כספים ברשתות בלוקצ'יין.

מימון טרור

על פי הערכות מודיעיניות של [רשויות חוק](#) וכן של חברות ניתוח בלוקצ'יין⁸ ישנו שימוש הולך וגובר בנכסים וירטואליים למטרות מימון טרור. בפרט, ישנה העדפה הולכת וגוברת של ארגוני טרור לשימוש במטבעות יציבים למימון פעילותם. המטבעות היציבים משמשים כאפיק מימון משמעותי, משום שהם משלבים נגישות ומהירות וכן לאור יציבות המחיר, תכונות המאפשרות לארגוני טרור להעביר ולשמור כספים תוך הפחתת הסיכון לזיהוי ולירידת ערך.

ניתוח דרכי הפעולה של גורמי טרור וקמפיינים לגיוס כספים, בין השאר באמצעות רשתות חברתיות, אפליקציות למסרים מיידיים, ואתרים ברשת מעיד על עלייה ברמת התחכום שלהם. דפוסי הפעילות שזוהו כוללים מעבר תכופ בין כתובות ארנק, פרסום ושיתוף כתובות ארנק בערוצי מדיה מגוונים, מעבר מהיר בין בורסות ופלטפורמות שונות בתחומי שיפוט בסיכון או ללא רגולציה מתאימה, שימוש גובר בארנקים פרטיים ובשירותי "ערבול", וכן שימוש בזהויות מזויפות כדי לעקוף בקורות KYC. גורמי טרור אף חולקים המלצות וטיפים מקוונים בנוגע לשיטות פעולה מומלצות ולפלטפורמות המספקות את רמת ההגנה הגבוהה ביותר.

המחשה לשימוש הגובר של ארגוני טרור בנכסים וירטואליים בעולם ובישראל בפרט ניתן לקבל על בסיס פירוט צווי התפיסה של כתובות ארנק המשמשים ארגוני טרור, כפי שהן מופיעות באתר של המטה ללוחמה כלכלית בטרור (המט"ל). ניתן לראות עלייה ניכרת במספר כתובות הארנק המזוהות לאורך השנים, כמו גם במגוון רחב יחסית של סוגי נכסים וירטואליים. כך לדוגמה [בנובמבר 2023 חתם שר הבטחון על צווי תפיסה](#) שהובילו להקפאת הפעילות של [כ-1,600 כתובות ארנק אשר זוהו כמשויכות לארגון טרור](#) [מוכרזאו ככאלו שנעברה בהן עבירת טרור חמורה](#)⁹ (כולן בזירת המסחר Binance). מעבר לעובדה שצווי תפיסה אלו פוגעים ביכולתם של בעלי כתובות הארנק להמשיך בפעילותם הסדירה הובילו הצווים [לתפיסה וחילוט של מיליוני ש"ח בנכסים וירטואליים](#)¹⁰.

על רקע התחכום העולה בפעילות של ארגוני הטרור, גובר הצורך בכלים ויכולות, אשר יאפשרו זיהוי אפקטיבי של פעילותם בנכסים וירטואליים כגון: מערך ניטור מתמשך, גיבוש תמונת מודיעין שוטפת ופיתוח יכולות טכניות מתקדמות.

⁸ TRM, 2025 Crypto Crime Report

⁹ ראה גם פרסום של צ'ינאליסיס המתייחס לתפיסות של המט"ל של ארנקים אשר החזיקו כ-1.7 מיליון דולר עבור חיזבאללה, רובם במטבע יציב USDT ברשת TRON. [קישור](#).

¹⁰ גלובס, ביהמ"ש: חמאס עושה שימוש במטבעות קריפטוגרפים להעברת כספים המבוצעות דרך חברות חלפנות הקשורות לארגון, ינואר 2025. [קישור](#).

שירותי הלבנת הון מקצועיים

מלביני הון מקצועיים מנצלים את האפשרויות המגוונות שמספקת פעילות בנקים וירטואליים כדי להלבין כספי פשיעה, בין אם הון שהופק בעבירות ומקורו בתווך המקוון ובין אם הון שהופק בתווך שאינו מקוון. גורמים עברייניים, כגון פושעי סייבר וסוחרי סמים ברשת האפלה, פונים בתדירות הולכת גוברת לשירותיהם של מלביני הון מקצועיים הפועלים בתחום הנכסים הוירטואליים, כדי לטשטש את עקבותיהם ולהסוות את מקור כספי הפשיעה. בין השיטות העיקריות של מלביני הון מקצועיים בתחום זה ניתן לראות ניצול זירות מסחר עם פיקוח רגולטורי לקוי או זירות זרות המשתפות פעולה עם גורמים פליליים, שימוש בטכנולוגיות מתקדמות להלבנה כגון מיקסרים וארנקים ייעודיים, המרה למטבעות יציבים לשמירה על ערך הנכסים וכן הפעלת רשתות בלדרים בשילוב שימוש בכספומטים לנכסים וירטואליים וכרטיסים נטענים. תופעה נוספת היא זירות מסחר "מקוננות" ('Nested Services'), שמלביני הון מקימים בתוך פלטפורמות מסחר בינלאומיות מרכזיות, אשר הופכות לכלי נפוץ להלבנת הון בהיקפים גדולים. מלביני ההון מפעילים מעין "זירות משנה" לא מפוקחות בתוך זירות מסחר בינלאומיות גדולות יותר, ומסווים את פעילותם הבלתי חוקית בתוך ים העסקאות הכשרות המתבצעות בזירה הראשית. באופן זה מנצלים מלביני הון את הנזילות הגבוהה והגישה לצמדי מסחר מגוונים של הזירות הגדולות לטובת הלבנת כספים שהופקו בעבירה.

התפתחויות טכנולוגיות וסיכוני הלבנת הון ומימון טרור

תחום הנכסים הוירטואליים מתאפיין בהתפתחות טכנולוגית בלתי פוסקת. ככל שהתחום צומח ומתמסד, כך הולכות וגדלות הקהילות המפתחות פרויקטים שונים, נכסים גופים עסקיים לרבות חברות ענק וגופים פיננסיים לתחום, כמו גם ציבור המשקיעים. מגמות אלו עיצבו בשנים האחרונות את התפתחות התחום וצפויות להמשיך ולעצב את פני הענף גם בשנים הקרובות. התפתחויות טכנולוגיות אלו מציבות במקביל אתגרים רגולטוריים ואכיפתיים במאבק בפשיעה פיננסית, הלבנת הון ומימון טרור.

מטבעות יציבים

המטבעות היציבים הפכו בשנים האחרונות לחלק אינטגרלי ומהותי בשוק הנכסים הוירטואליים, ומהווים את עיקר נפח העסקאות בעת הנוכחית.¹¹ ההיצע המצטבר של המטבעות היציבים במחזור גדל בשיעור שנתי ממוצע של כ-28% במהלך השנים האחרונות, [ונפח ההעברות הכולל באמצעותם הגיע בשנת 2024 לסך של כ-27.6 טריליון דולר](#), היקף הגבוה מסך העסקאות שבוצעו באותה שנה באמצעות חברות Visa ו-Mastercard גם יחד.

ייחודם של המטבעות היציבים, הצמודים לנכסי בסיס יציבים כגון מטבעות פיאט וסחורות, טמון ביכולתם לספק יציבות מחירים משמעותית, בניגוד לתנדבותיות הגבוהה המאפיינת נכסים וירטואליים אחרים. יציבות זו, בשילוב עם יעילותם הטכנולוגית, הניעה אימוץ גובר שלהם כאמצעי תשלום ואחסון ערך ברחבי העולם, בפרט באזורים המתמודדים עם חוסר יציבות מוניטרית ונגישות מוגבלת לדולר האמריקאי. עסקים, מוסדות פיננסיים ומשתמשים פרטיים מוצאים במטבעות היציבים פתרון יעיל לתשלומים בינלאומיים מהירים וזולים, ניהול נזילות משופר, וגידור סיכונים תנודות מטבע.

לצד היתרונות הכלכליים והטכנולוגיים הגלומים בהם, המטבעות היציבים מעוררים דאגה רגולטורית גוברת, בעיקר בהקשר של סיכונים הלבנת הון ומימון טרור. האנונימיות החלקית, מהירות העסקאות ונגישותם הגלובלית של מטבעות אלו, עלולים לשמש גורמים עברייניים לביצוע העברות כספים בלתי חוקיות ולמימון פעילות טרור, תוך עקיפת מערכות פיננסיות מסורתיות ומנגנוני פיקוח. כתוצאה מכך, רגולטורים ברחבי העולם, החל מהונג קונג ויפן, דרך

¹¹ מרבית המסחר הינה במטבע היציב USDT.

האיחוד האירופי עם רגולציית MiCA, ועד ארצות הברית עם העברת חוק GENIUS, מגבירים את העיסוק במטבעות יציבים ופועלים לגיבוש מסגרות רגולטוריות מקיפות.¹²

ישראל פועלת גם היא לגיבוש מסגרת רגולטורית למטבעות יציבים. בהתאם להחלטת הממשלה בפברואר 2023¹³ הוסמכה רשות שוק ההון, ביטוח וחיסכון במשרד האוצר (להלן: "רשות שוק ההון") לשמש כגורם הרישוי, הפיקוח והאסדרה על גופים העוסקים בהנפקה והוצאה של מטבעות יציבים. במאי 2025 פרסמה רשות שוק ההון [קול-קורא לציבור](#)¹⁴ לקראת ניסוח תזכיר חוק חדש, שיקבע מסגרת רגולטורית כוללת להסדרת הנפקה והוצאה של מטבעות יציבים בישראל. תזכיר החוק מתבסס, בין היתר, על עקרונות שגיבש בנק ישראל [עקרונות שגיבש בנק ישראל](#)¹⁵ ועל רגולציות בין-לאומיות מקבילות במדינות מפותחות, תוך התאמתן לשוק הישראלי.

מטרת הרגולציה היא לאזן בין עידוד חדשנות טכנולוגית ומימוש הפוטנציאל הכלכלי של מטבעות יציבים, לבין הצורך הדחוף למנוע שימוש לרעה בהם למטרות פליליות, תוך שמירה על יציבות פיננסית והגנה על הצרכן.

זירות מסחר

זירות מסחר בנכסים וירטואליים מספקות נזילות חיונית לשוק ומשמשות כשערי מעבר בין העולם הפיננסי המסורתי והשימוש בפיאט לבין שוק הנכסים הוירטואליים. מסיבה זו, הן גם מהוות מטרות מרכזיות לניסיונות להלבנת הון.

זירות מסחר שאינן מפוקחות או שאינן עומדות בכללי הציות מציבות סיכון גבוה להלבנת כספים. ה-FATF מציין כי עברייניים מנצלים את הפערים הרגולטוריים ומעבירים כספי פשיעה ל-VASPs הפועלים במדינות בעלות משטר איסור ה"ה ומ"ט רופף.¹⁶ זירות מסחר בסיכון גבוה כוללות, בין השאר, זירות שמתעלמות במכוון מהדרישות הרגולטוריות; מאפשרות ללקוחות לפתוח חשבונות בלי או עם מעט מאוד מידע מזהה וכן זירות השוכנות במדינות המאופיינות כבעלות סיכון גבוה לה"ה ומ"ט. זירות מסחר לא מפוקחות או שאינן עומדות בדרישות הרגולטוריות מציבות סיכון מערכתי לשוק הנכסים הוירטואליים, בכך שהן מהוות פתח משמעותי להלבנת הון בהיקפים נרחבים ופוגעות בלגיטימיות של שחקנים אחרים הפועלים מולן. לאור זאת ישנה, חשיבות רבה למודעות לסיכונים הקיימים בפעילות מול זירות מסחר אלו.

בשנת 2025 רשות שוק ההון, הביטוח והחסכון שבה והזהירה את הציבור מפני קבלת שירותים במטבעות וירטואליים מידי גופים שאינם מפוקחים ושלא קיבלו רישיון מתאים, וכן הבהירה כי קיימים מקרים בהם בקשות של גופים מקומיים ובינלאומיים לקבלת רישיון נדחות, ולמרות זאת, וללא רישיון מתאים, הם ממשיכים להציע ולפרסם שירותים פיננסיים במטבעות וירטואליים בערוצים שונים. באותה שנה, הורה הממונה על שוק ההון, הביטוח והחיסכון על הפסקה מיידית של פעילות אתר בשם "Bitin", העוסק בתחום השירותים הפיננסיים בכלל ומתן שירותים במטבעות וירטואליים בפרט, לאחר שנמצא כי הוא אינו מחזיק ברישיון כנדרש בחוק הפיקוח על שירותים פיננסיים (שירותים פיננסיים מוסדרים), תשע"ו-2016 ומעניק שירותי קריפטו ללא רישיון. בעליו של האתר פנה בשנת 2022 לרשות שוק ההון על מנת לקבל רישיון ועל אף שבקשתו נדחתה הוא המשיך לעסוק במתן שירותים פיננסיים ולהציע שירותי קניה ומכירה של מטבעות וירטואליים בניגוד לחוק. בגין כך הודיעה רשות שוק ההון כי בכוונתה להטיל עיצום כספי של 1.7 מיליון ש"ח על בעלי האתר.¹⁷

¹² לקריאה נוספת, ראו: *World Economic Forum: The GENIUS Act is Designed to Regulate Stablecoins in the US, but How Will it Work?*, יולי 2025, [קישור](#). לקריאה נוספת בנושא חקיקת האיחוד האירופי בתחום הנכסים הוירטואליים, ראו: ESMA: *Markets in Crypto-Assets Regulation (MiCA)*, [קישור](#).

¹³ קידום האסדרה של הפעילות בנכסים דיגיטליים, החלטה מספר 204 של הממשלה. [קישור](#).

¹⁴ קול קורא לבחינת מדיניות נותן שירותים בנושא הנפקה והוצאה של מטבע דיגיטלי יציב, רשות שוק ההון, ביטוח וחיסכון. [קישור](#).

¹⁵ בנק ישראל, *העקרונות לפעילות "מטבעות דיגיטליים יציבים" בישראל*. [קישור](#).

¹⁶ FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, אוקטובר 2021, עמ' 88. [קישור](#).

¹⁷ לפרטי המקרה ולניק לקו החם של רשות שוק ההון, הביטוח והחיסכון : https://www.gov.il/he/pages/press_0058

זירות, שאינן מבצעות כנדרש תהליכי זיהוי לקוח (KYC), מאפשרות לעבריינים לפעול תחת מעטה אנונימיות מוגבר הנובע משילוב עם פסדו-אנונימיות שמקנים נכסים וירטואליים. לעיתים מאחורי זירות המסחר עצמן עומדים גורמים עבריינים, או לחלופין הן מעלימות עין מפעילותם או משתפות עמם פעולה.

יש לציין כי, בדומה למערכות פיננסיות לגיטימיות אחרות, גם זירות מסחר מפוקחות עלולות להיות מנוצלות להלבנת הון. זירת מסחר מוסדרת, אשר מהווה שער מעבר למערכת הפיננסית המסורתית, עלולה לשמש עבריינים בין היתר כמעין 'מערבלי', זאת מכיוון שבמקרים רבים הפעילות בזירה לרבות הפעילות הלגיטימית אינה מבוצעת בבלוקצ'יין (off-chain), וכתוצאה מכך אין תיעוד חיצוני של הפעולות המבוצעות במסגרת הזירה. בנוסף לכך מכיוון שזירות המסחר פועלות כמעט אך ורק בתווך המקוון, ליקויים בתהליך הזיהוי מרחוק, לצד התפתחויות טכנולוגיות, כגון היכולת לזייף מסמכים ברמה גבוהה או תהליכי הזדהות ויזואליים באמצעות כלי AI, הינם סיכונים נוספים המחייבים התייחסות ומענה ייעודי.

הלבנת הון באמצעות זירת מסחר בסיכון גבוה

זירת המסחר לשעבר BTC-e, שהוקמה ב- 2011 על-ידי אלכסנדר ויניק, נחשבת לדוגמה בולטת לזירה בלתי מפוקחת שהיוותה מוקד להלבנת הון בהיקפים נרחבים. לפי הערכות שונות, תשלומי כופר רבים ברחבי העולם הולבנו והומרו לפיאט דרך פלטפורמה זו במהלך פעילותה. הזירה אפשרה פתיחת חשבונות על בסיס כתובת דוא"ל בלבד, קבלת נכסים שעברו דרך מיקסרים וכן שימוש במטבעות פרטיות. לפי רשויות האכיפה בארצות הברית, הזירה הייתה יעד מועדף להלבנת כספים שהופקו במסגרת מגוון עבירות פליליות ובכלל זה מתקפות כופרה, הונאות, שחיתות ציבורית וסחר בסמים.

כיוון ש BTC-e פעלה בארה"ב ללא רישיון הרשויות האמריקאיות פתחו בחקירה בעניינה, אשר הובילה להטלת קנס של הרשות האמריקאית למודיעין פיננסי FinCEN בסך 110 מיליון דולר על הזירה ומייסדה. **החקירה התבססה במידה רבה על דיווחים בלתי רגילים מגופים פיננסיים**, שסיפקו מידע על הנהלים הסופיים ועל היקף הפעילות של הזירה.

לצורך הסוואת פעילותה הקימה BTC-e מבנה תאגידי מורכב שכלל רישום חברות קש במדינות שונות, מידע מטעה על מיקומה, וכן פתחה חשבונות בנק במקלטי מס. ויניק נעצר ביוון בשנת 2017, הוסגר לארה"ב ב- 2022 ובמאי 2024 הודה בקשירת קשר להלבנת הון. במסגרת הסדר טיעון חולטו למעלה מ- 100 מיליון דולר. בפברואר 2025 שוחרר במסגרת עסקת חילופי אסירים בין ארה"ב לרוסיה.

Decentralized Finance (DeFi)

כלכלה מבוזרת (DeFi) מייצגת מודל חדשני במערכת הפיננסית, הממנפת את מאפייניהם הייחודיים של נכסים וירטואליים וטכנולוגית הבלוקצ'יין, על מנת לספק גישה ישירה לשירותים פיננסיים מגוונים, אשר באופן מסורתי סופקו על ידי מוסדות פיננסיים מרכזיים. בבסיס DeFi עומד השימוש ב"חוזים חכמים", פרוטוקולים או תוכנות אוטונומיות הפועלות על גבי רשתות בלוקצ'יין בהתאם לתנאים מוגדרים מראש. באמצעות חוזים חכמים אלו, יישומי DeFi (DApps) מספקים שירותים פיננסיים מבוזרים, כלומר כאלה המתבצעים באופן אוטונומי וללא צורך בגורם מתווך, כגון בנק, ברוקר או מוסד אשראי המעניק את השירות הפיננסי או העסקי. המשמעות היא כי פעולות כמו הלוואה, מסחר או ניהול נכסים מתבצעות ישירות בין משתמשים (peer-to-peer), תוך הסתמכות על קוד פתוח ותשתית בלוקצ'יין המבטיחה את אמינות העסקאות במקום פיקוח אנושי או מוסדי.

אחת הדוגמאות הבולטות למימוש העקרונות של DeFi הינן זירות מסחר מבוזרות - Decentralized Exchanges (DEXs) המשתמשות בחוזים חכמים כדי לספק שירות של החלפות נכסים וירטואליים בזמן אמת למשתמשי הזירה.

בניגוד לזירות מסחר מרכזיות, הפועלות באמצעות גורם מתווך המנהל את העסקאות, בזירות DEX המסחר מתבצע ישירות בין המשתמשים, ללא שליטה של גוף מרכזי. בשנים האחרונות נרשמה עלייה חדה בהיקפי הפעילות בזירות אלו, שהגיעו בשיאם למחזורי מסחר של למעלה מ-30 מיליארד דולר בחודש.¹⁸ זירות מרכזיות בתחום הנכסים הוירטואליים, כמו Uniswap, מתחרות כיום בזירות המסחר הריכוזיות בהיקף הפעילות הכולל.

במדינות רבות, עדיין קיימת אי בהירות בנוגע לשאלה האם זירות מסחר מבוזרות (DEXs) מצויות תחת הסמכות הרגולטורית של משטר איסור הלבנת הון ואיסור מימון טרור. זיהוי הגורמים והישויות האחראים לתפעול יישומי DeFi עלול להציב אתגרים משמעותיים בפני רשויות הפיקוח והרגולציה. חלק ממיזמי DeFi מצהירים כי מדובר בישות מבוזרת לחלוטין שבה אין לאף גורם יחיד שליטה משמעותית על פעילותה. עם זאת למרות טענות הביזוריות בתעשייה, לא אחת קיימות ישויות או יחידים השולטים בפועל על תפעול מיזמים אלה, בין היתר באמצעות תחזוקת פרוטוקולי DeFi. שליטה זו יכולה להיות מושגת על ידי יחידים או ישויות בעלי החזקות דומיננטיות של זכויות הצבעה או בהשפעה מכרעת על ביצוע שינויי ממשל מהותיים, לרבות הסמכות ליישם עדכוני פרוטוקול.¹⁹

אופיין המבוזר של פעילות DeFi וכתוצאה מכך היעדר פיקוח מרכזי ומנגנוני בקרה מקובלים כגון נהלי זיהוי לקוח (KYC), מקשים על זיהוי פעילות בלתי חוקית ומעקב אחר מקור הכספים ויוצרים פוטנציאל משמעותי לניצול לרעה לצורך הלבנת הון. בריכות נזילות, לשם דוגמה, מהוות מרכיב יסודי בזירות מסחר מבוזרות (DEXs) ומספקות נזילות למסחר בכך שמשתמשים מפקידים בהן זוגות של נכסים (כגון ETH ו-USDT) ומאפשרים ביצוע עסקאות אוטומטיות בין משתמשים אחרים. בתמורה, הם מקבלים חלק מעמלות המסחר הנגבות בזירה. מאגר משותף זה מאפשר מסחר רציף גם בהיעדר צד נגדי ישיר, אך מנגנון זה עצמו יוצר גם פוטנציאל לניצול לרעה: הפקדת נכסים שמקורם בעבירה בבריכת נזילות מאפשרת לרבד אותם עם נכסים אחרים ולמשוך לאחר מכן מטבעות "נקיים", תוך שטוש מקורם הבלתי חוקי או ליהנות מהכנסה חוקית שמקורה בעמלות. לציין, כי גם היכולת לרכוש את הטוקנים המקנים שליטה, יכולים להביא לשינוי באופן הפעילות של פרוטוקול DeFi מחד, ומאידך לשמש כאמצעי להלבנת הון.

¹⁸ Elliptic, *Preventing Financial Crime in Cryptoassets 2024*, עמ' 44.

¹⁹ **במסמך** שפורסם על ידי ה-Financial Stability Board (FSB) וקרן המטבע העולמית (IMF) מציעים הגופים כי לאור המגוון הרחב של מיזמי DeFi וההסדרים השונים על הרשויות לנתח את העובדות והנסיבות הרלוונטיות לזיהוי הגורמים והישויות האחראים. לאחר זיהוי הגורמים הטבעיים או הישויות (מאגדות או לא) השולטים בפרוטוקול DeFi, הרשויות יכולות להפעיל כלים רגולטוריים כדי להתמודד עם הסיכונים הכרוכים בפעילות. המסמך ממשיך ומציע דרכי התמודדות גם במקרים בהם הרשויות סוברות כי מדובר בגוף מבוזר לחלוטין. ראו שם, עמ' 13 ואילך.

כספומטים לנכסים וירטואליים

כספומטים למטבעות וירטואליים (Crypto ATMs) הם מכשירים פיזיים המאפשרים לציבור הרחב לרכוש או למכור נכסים וירטואליים באמצעות מזומן או כרטיס אשראי. בשנים האחרונות הפכו כספומטים אלו לנפוצים ברחבי העולם, והם מספקים שירות לרכישת נכסים וירטואליים לציבור הרחב. בד בבד הם מזוהים בעולם עם סיכוני הונאה, הלבנת הון ומימון טרור, עקב היכולת לפעול במזומן וכן לאור מקרים בהם השירות ניתן ללא הזדהות מלאה, ובאופן שאינו מחייב מעורבות של בנק או גוף פיננסי מפקח.

השילוב בין השימוש במזומן, קלות השימוש, מהירות העסקאות, היעדר הליכי זיהוי מחמירים ופיזור גיאוגרפי נרחב של המכשירים, מעלים את הסיכון שכספומטים ינוצלו למטרות פליליות והלבנת הון. נציבות הסחר הפדרלית בארה"ב (FTC) פרסמה סקירה [שקושרת בין כספומטים לבין הונאות בהיקפים של עשרות מיליוני דולרים](#), בעיקר בקרב אוכלוסיות מוחלשות. דוח זה מצביע על דפוסי פעולה שחוזרים על עצמם, ובהם התחזות לגורמים רשמיים (כגון רשויות ממשלה או גופי אכיפה), מצגי שווא של השקעות מהירות, ואף הונאות רומנטיות, במטרה לשכנע קורבנות לרכוש נכסים וירטואליים באמצעות כספומטים ולהעבירם לכתובות ארנק בשליטת עבריינים. [על פי נתונים שפורסמו ע"י יחידת הסייבר של ה-FBI בשנת 2024](#) דווחו בארצות הברית כ- 11,000 תלונות הקשורות להונאות שבוצעו באמצעות כספומטים לנכסים וירטואליים, עלייה של כ- 99% לעומת השנה הקודמת.

מדינות רבות ברחבי העולם נוקטות צעדים להגברת הפיקוח והאכיפה סביב פעילות כספומטים למטבעות וירטואליים מתוך הכרה בסיכונים הטמונים בהם. הגישות נעות בין איסור מוחלט על פעילות הכספומטים, דרך הטלת דרישות ציות חדשות ומחמירות, ועד אכיפה יזומה וחקיקה ייעודית שנועדה להגן על הציבור ולמנוע ניצולם לרעה.

בישראל, רשות שוק ההון בוחנת כיום את מדיניותה בנוגע להפעלת כספומטים למטבעות וירטואליים, זאת בין היתר על רקע בקשות חדשות לרישוי פעילות באמצעות כספומטים, כמו גם בקשות להרחבת פעילות מצד גופים מפקחים קיימים. על פי הערכותיה היקף העסקאות במזומן באמצעות כספומטים לנכסים וירטואליים בישראל עולה על 250 מיליון ש"ח בשנה ונמצא במגמת עלייה. במרץ 2025 פרסמה [קורא לשיתוף ציבור בנושא מתן שירותים פיננסיים במטבעות וירטואליים באמצעות כספומטים ייעודיים](#). הקול הקורא מתייחס, בין השאר, לסיכונים מוגברים להלבנת הון, מימון טרור והונאות צרכניות, בשל קושי בביצוע זיהוי, פיקוח ודיווח אפקטיביים.

נוכח האתגרים הייחודיים שמציבה פעילות זו, רשות שוק ההון ביקשה לבחון במסגרת הקול הקורא גיבוש מסגרת רגולטורית סדורה שתכלול, בין היתר: הגבלות על עסקאות במזומן, חיוב זיהוי מלא וביצוע KYC ללקוחות בכל סכום, הצבת המכשירים במתחמים מפקחים בלבד, שימוש בכלים טכנולוגיים לניטור עסקאות בזמן אמת, והטלת מגבלות על היקף הפעילות היומי והשנתי לכל לקוח. בנוסף, נבחנת האפשרות לחייב את המפעילים לספק גילוי נרחב לצרכנים ולוודא כי הכספים יוזרמו רק לחשבונות או ארנקים מזוהים של הלקוחות עצמם.

מיקסרים (מערבלים)

שירותי ערבול עסקאות ('Mixers', 'Tumblers'), פועלים באמצעות קבלת נכסים וירטואליים ממגוון משתמשים, ערבולם יחד, ושליחתם לכתובות ארנק חדשות. תהליך זה מקשה על הקישור בין מקור הכספים והנתיב שלהם בבלוקצ'יין ושיוכם למקורם ולפיכך על יכולת המעקב אחר הכספים, ומעניק מעטה אנונימיות מוגבר לפעילות הפיננסית בכנסים וירטואליים. למרות שמערבלים עשויים לשמש גם גורמים לגיטימיים המבקשים לשמור על פרטיותם, הרשויות ברחבי העולם מודאגות מהשימוש הנרחב שנעשה בהם על ידי גורמים עברייניים להלבנת הון שמקורו בפשיעה מקוונת ובעבירות אחרות.

במערכות פיננסיות מבוזרות (DeFi) בפרט, כלים לערבול עסקאות הפכו למכשיר משמעותי עבור גורמים עברייניים. ניטור פעילות של כתובות המזוהות כמשויכות לפעילות עבריינית בידי חברות לניתוח בלוקצ'יין מלמד כי הטלת סנקציות על שירות מערבל מוביל אמנם לירידה זמנית בשימוש בו, אך עד מהרה צצים שירותים חדשים כתחליף. הסתגלות מהירה זו של גורמי הפשיעה והיכולת שלהם למצוא פתרונות חלופיים מדגישה את הצורך במאמץ מתמשך ודינמי מצד רשויות האכיפה והרגולציה, כדי להתמודד עם אתגרי הלבנת ההון בזירת הנכסים הוירטואליים.

הלבנת הון באמצעות מיקסרים

באפריל 2024, הודיע משרד המשפטים האמריקאי (DOJ) כי הגיש כתבי אישום בגין הלבנת הון נגד המייסדים והמפעילים של שירות ארנק נכסים וירטואליים בשם 'Samurai Wallet'. השירות אשר הושק ב- 2015 הוצג כארנק אנונימי עבור החזקת נכסים וירטואליים. הארנק עשה שימוש במספר טכניקות מתקדמות להגברת האנונימיות ולטשטוש עסקאות של משתמשים. אחת מהטכניקות, 'Whirlpool', פעלה על ידי ערבוב כספי משתמשים שונים. טכניקה נוספת, 'Ricochet' אפשרה למשתמשי הארנק לבצע עסקאות דרך שרשרת של כתובות נכסים וירטואליים ("דילוגים"), במטרה להסוות את הקשר למקור הכספים הראשוני.

למרות ש-Samurai Wallet הוצג כשירות המבטיח אנונימיות למשתמשי לגיטימיים שחרדים לפרטיותם, ממשלת ארה"ב טוענת כי המייסדים והמפעילים ידעו היטב שהשירות משמש גורמים עברייניים, ובחרו שלא לנקוט כל צעד כדי למנוע זאת. לדוגמה, מפעילי השירות היו מודעים לכך שהארנק משמש משתמשים בשווקי הרשת האפלה, כגון Silk Road ו-Hydra Market להלבנת רווחי סחר בסמים. יתרה מזאת, התכתבויות שלהם חשפו כי היו שבעי רצון מהשימוש של גורמים עברייניים בארנק. במסגרת מאמצי אכיפת החוק כנגד השימוש בשירות נעצרו המייסדים והמפעילים, ורשויות אכיפה בארה"ב שיתפו פעולה עם מקביליהם באירופה כדי להחרים את שרתי Samurai Wallet וכתובת האינטרנט שלו. האפליקציה הוסרה מחנות האפליקציות של גוגל והגישה נחסמה למשתמשים מארה"ב.

דיווח על פעילות בלתי רגילה לדוגמה

לקוח ביקש למכור נכסים וירטואליים באמצעות VASP. בדיקה של מקור הנכסים העלה כי הם הגיעו מכתובת ארנק שמרבית הכספים שבו הגיעו ממיקסר וחלק נוסף משוק דארקנט.

גשרים בין רשתות בלוקצ'יין (Bridges)

עם פיתוחן של רשתות בלוקצ'יין רבות, צמח גם הסיכון להלבנת הון באמצעות גשרים בין רשתות (Cross-chain bridges). גשרים בין רשתות בלוקצ'יין מאפשרים העברת נכסים וירטואליים מרשת בלוקצ'יין אחת לשנייה באמצעות שימוש בחוזים חכמים. אפליקציות אלו פותחו לאור הצורך בפעולה הדדית בין בלוקצ'יינים שונים (Interoperability), על מנת לאפשר תקשורת בין הרשתות וחיבור קל ומהיר בין פרויקטים ויוזמות המפותחות בכל בלוקצ'יין בנפרד. תהליך זה מתבצע לרוב באופן מבוזר, וללא זירה ריכוזית וכן ללא תהליכי זיהוי והכרת לקוח (KYC), באופן המקשה על מעקב אחר הכספים.²⁰ גשרים פופולריים כוללים את RenBridge, VoltSwap ו-WanBridge.²¹

בנוסף על היכולת לחבר פעילות עסקית ופיננסית המבוצעת בבלוקצ'יינים שונים, המהווה נדבך קריטי בפיתוח התעשייה, הפכו בשנים האחרונות Cross-chain bridges לכלי משמעותי להלבנת הון. הלבנה באמצעות 'דילוג בין רשתות' ('Chain-hopping') הנה תופעה בה מבוצעת החלפה מהירה של נכסים וירטואליים בין רשתות בלוקצ'יין שונות ללא כל תכלית עסקית מלבד הרצון לטשטש את נתיב הכספים ולנתק אותם ממקורם. טיפולוגיה זו נועדה להקשות על התחקות אחר נתיב הכספים.²² סיבה נוספת לעלייה בשימוש בשיטה זו היא שחלק גדול והולך מכספי הפשיעה הוירטואליים מקורו בנכסים פחות נזילים, כמו טוקנים ייעודיים לפרוטוקולי DeFi, אשר המרתם למטבעות אחרים אפשרית רק באמצעות שירותים חוצי-רשתות. מגמת המעבר לשימוש ב-'Chain-hopping' הפכה לבולטת במיוחד בעקבות פעילות של רשויות אכיפה כנגד שירותי מיקסרים מרכזיים כדוג' Tornado Cash, Blender.io ו-ChipMixer.

מטבעות וירטואליים כאמצעי תשלום

התמסדות תחום הנכסים הוירטואליים והגידול העצום במסחר ובביקוש למטבעות מסוימים, כגון, ביטקוין, איתרום, USDT ו-USDC²³ הביאו לקבלה הולכת וגוברת של מטבעות אלו כאמצעי תשלום בכלכלה הפיזית והדיגיטלית. הגם שמדובר עדיין בתופעה מצומצמת יחסית, חיבור זה כולל בחובו סיכונים הלבנת הון בדמות היכולת להמיר באופן גלובלי, מהיר ומאובטח נכס וירטואלי לנכס אחר בעל סיכונים הלבנת הון נפרדים, כגון רכישת נדל"ן, רכבים, מוצרי יוקרה כגון שעונים ותכשיטים, מתכות יקרות, עסקים וכדומה. בנוסף, קיימות חברות פיננסיות בעולם שהחלו לקבל מטבעות קריפטוגרפים כאמצעי תשלום וכן ניתן להטעין כרטיסי מתנה בקריפטו. אם בעבר אחת מנקודות הסיכון העיקריות הייתה ביכולת להמיר מטבעות וירטואליים למטבע פיזי, הרי שהתפתחות הקריפטו כאמצעי תשלום הופכת כל מפגש עם נכס פיזי או דיגיטלי לבעל סיכון הלבנת הון נוסף.

פלטפורמות P2P (Peer to Peer)

פלטפורמות P2P משמשות להמרה בין נכסים וירטואליים שונים או בין נכסים וירטואליים לפיזי, ללא מעורבות של נותן שירות בנכסים וירטואליים (VASP) או גורם מפוקח אחר. עסקאות אלו מתבצעות בין שני ארנקים פרטיים, כאשר המשתמשים פועלים באופן עצמאי, והפלטפורמה משמשת רק כתווך מקוון המסייע בחיבור בין הצדדים, מבלי לקחת חלק פעיל בביצוע העסקה או בניהול הכספים. במקרים רבים פלטפורמות אלו אינן מחייבות הליכי זיהוי והכרת הלקוח ומאפשרות שימוש במגוון אמצעי תשלום ובכלל זה מזומן, כרטיסים נטענים וכרטיסי מתנה לטובת ביצוע

²⁰ ראו, FATF, Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers, יוני 2022, עמ' 25: "DeFi protocols can be used to perform 'chain-hopping' which can make the transactions more difficult to trace."

²¹ על פי דוח של חברת Elliptic, מאוגוסט 2022 הולבנו באמצעות RenBridge כ-540 מיליון דולר מתחילת 2020.
²² התחקות אחר נתיב הכספים מחייבת כלים לניתוח בלוקצ'יין, אשר כוללים יכולות לנתח מגוון רחב של רשתות בלוקצ'יין, כולל שימוש בגשרים, על מנת לאפשר מעקב כולל ורציף אחר המעבר של נתיב הכספים בין הרשתות.
²³ דוגמאות בלבד למטבעות העיקריים. בפועל ניתן לבצע תשלומים במגוון רחב מאוד של נכסים וירטואליים.

העסקאות. שימוש באמצעים אלו מעניק שכבת אנונימיות נוספת לרוכש, שכן הן אינן מתועדות בהכרח ברישומי הבנק או בפירוט חשבונות כרטיסי האשראי.

חובות משטר איסור הלבנת הון ומימון טרור הנגזרות מהמלצות ה-FATF אינן חלות באופן ישיר על עסקאות P2P, מאחר וחובות אלו מוטלות על גופים עסקיים מפקחים ולא על משתמשים פרטיים. מצב זה יוצר אתגר משמעותי עבור רשויות האכיפה והפיקוח, שכן עסקאות P2P מתבצעות ללא גורם מתווך שיבצע הליכי זיהוי לקוח (KYC), בדיקות נאותות (CDD) או דיווח על פעולות חשודות. שילוב זה של העדר גורם מפקח וחוסר בתיעוד נתיב הכספים מגביר את רמת הסיכון הנובע מפלטפורמות אלו בהיבטי הלבנת הון ומימון טרור.

קיים קושי להעריך את היקף השימוש בפלטפורמות P2P ובהתאם את רמת הסיכון הנשקפת מהן, אך ישנו חשש כי ככל שתתגבר הרגולציה על גופים מפקחים (VASPs), פעילות בלתי מפקחת תוסט בהדרגה לפלטפורמות אלו. [במסמך](#) של ה-FATF מיוני 2023, הבוחר את מידת היישום של המלצות הארגון בתחום הנכסים הוירטואליים, קורא ה-FATF להמשיך ולעקוב אחר מגמות השימוש באפיק זה ולפתח כלים וצעדים ייעודיים למיתון הסיכון.

כרייה של נכסים וירטואליים (Mining)

כריית נכסים וירטואליים היא מנגנון הפעולה של רשתות בלוקצ'יין המבוססות על הוכחת עבודה (Proof of Work - PoW), שבאמצעותן מעובדות עסקאות ונוצרים מטבעות חדשים. התהליך נשען על תחרות בין "כורים" המשתמשים במשאבי מחשב משמעותיים לפתרון "חידות" קריפטוגרפיות. הכורה הפותר ראשון מוסיף בלוק חדש לשרשרת ומקבל תגמול במטבעות חדשים או בעמלות משתמשים.

לצד תרומתה לאבטחת הרשת, הכרייה היא תהליך עתיר אנרגיה ויקר, המתבצע לרוב באמצעות בריכות כרייה (Mining Pools) המאחדות את כוח העיבוד של משתמשים רבים שחולקים את עלויות הכרייה ויכולים להשתתף באופן אנונימי בתהליך ולחלק את הרווחים המשותפים.

מבחינה רגולטורית, פעילות הכרייה אינה חוסה תחת משטר איסור הלבנת הון ומימון טרור ולכן מהווה אפיק פוטנציאלי לניצול עברייני. גורמים פוליטיים עשויים להשקיע כספי פשיעה בפעילות כרייה לגיטימית, לשלבם עם כספים ממקורות אחרים ולקבל תמורה שנראית "נקייה" כמקור ההכנסה. כך, בריכות כרייה עשויות לשמש כלי לריבוד והסוואת מקור הכספים.

באופן דומה פעולות כרייה עלולות לשמש לעקיפת סנקציות, כאמצעי ליצירת הכנסה שלכאורה נקייה משיוך למקור בעייתי.

מסחר באמצעות בוטים בפלטפורמות חברתיות

תופעה נוספת שצמחה במהירות בשנים האחרונות היא המסחר באמצעות בוטים אוטומטיים בנכסים וירטואליים בפלטפורמת טלגרם (Telegram). בוטים אלו מהווים כלי נגיש ופשוט למשתמשים, המאפשר ביצוע פעולות קנייה ומכירה של נכסים וירטואליים דרך ממשק צ'ט ידידותי. הפופולריות שלהם נובעת מהשילוב בין קלות השימוש, עמלות נמוכות, העניין הגובר במטבעות מם (Memecoins), שהפכו לקטגוריית מסחר בולטת בשוק הנכסים הוירטואליים וכן מהנגישות שהם מעניקים למסחר בזירות נכסים וירטואליים מבוזרות (DEXs). עיקר פעילות הבוטים מתרכזת כיום ברשתות בלוקצ'יין המאופיינות במהירות עסקאות גבוהה ודמי שימוש נמוכים, ובראשן רשת סולנה (Solana) שנחשבת לאחת הפלטפורמות המרכזיות בתחום. בוטי המסחר מפיקים הכנסות באמצעות גביית עמלה מכל פעולה, לרוב בשיעור של עד אחוז משווי העסקה והבולטים שבהם, כדוגמת Photon, גרפו הכנסות של מאות מיליוני דולרים.²⁴

לצד הפופולריות הגוברת, המסחר באמצעות בוטים בטלגרם טומן בחובו סיכונים הלבנת הון ומימון טרור ייחודיים. מאפייני טלגרם כפלטפורמת מסרים מוצפנת ומבוזרת מקשים על רגולציה ופיקוח, והעדר חובת זיהוי משתמשים (KYC) בבוטים רבים מאפשר אנונימיות כמעט מלאה. שילוב זה יוצר קרקע נוחה לניצול על ידי גורמים עברייניים המבקשים להסתיר את זהותם או את מקור כספם, במיוחד בעסקאות חוצות גבולות ובמטבעות בעלי נזילות נמוכה, אשר עלולים להיות יותר קשים למעקב ולניטור. בהיבט הרגולטורי, מרבית המדינות ובכללן ישראל טרם הסדירו במפורש את פעילות הבוטים למסחר בנכסים וירטואליים, מה שמקשה על אכיפה ומעקב אפקטיביים. לאור זאת, צפוי כי תחום זה ימשיך להוות אתגר גובר למערכות הפיקוח והאכיפה בשנים הקרובות.

האסדרה בעולם ובישראל

האסדרה בעולם

ב- 2019 במסגרת עדכון המלצה 15 ה-FATF את תחולת דרישות איסור הלבנת הון ומימון טרור כך שיחולו גם על נכסים וירטואליים.

בעקבות העדכון, כל המדינות חייבות לבצע הערכת סיכונים הלבנת הון/מימון טרור/מימון פרוליפרציה הנובעים מהשימוש בנכסים וירטואליים. כמו כן, הסטנדרטים הבינלאומיים דורשים החלה מלאה של משטר איסור הלבנת ההון ואיסור מימון הטרור גם על פעילות בנכסים וירטואליים (Virtual Assts - VAs) ועל נותני השירות בהם (Virtual Assets Service Providers - VASPs), כך שנותני שירות בנכסים וירטואליים יחויבו במשטר של רישום/רישוי ויוטלו עליהם החובות שמוטלות על נותני שירותים בנכסים פיננסיים ומוסדות פיננסיים אחרים, לרבות הכר את הלקוח, דיווח על פעולה חשודה, שמירת מסמכים וניהול סיכונים. בנוסף, נקבע כי בשל הסיכונים הטמונים בפעילות זו הסף לביצוע הליך הכרת הלקוח יהיה נמוך יותר מזה הקיים בסקטורים אחרים ועמוד על סך של 1,000 יורו/דולר.

במטרה להאיץ ולחזק את יישום המלצה 15 אימץ ה-FATF בשנת 2023 "מפת דרכים" מפורטת, שנועדה לספק מסגרת פעולה ברורה למדינות. כחלק ממפת דרכים זו, פורסם מיפוי מקיף המציג את סטטוס היישום של ההמלצות במדינות החברות ב-FATF ובמדינות נוספות בעלות פעילות משמעותית של נותני שירות בנכס וירטואלי (VASPs).

אחד הנושאים המרכזיים עליהם ארגון ה-FATF שם דגש הוא יישום המלצה 16 המכונה ה-"Travel Rule", הנחשב למרכיב קריטי בבקרה על מניעת הלבנת הון ומימון טרור. במסגרת זו, נדרשות כל מדינות העולם להטיל על נותני שירות בנכסים וירטואליים את החובה המוטלת על נותני שירותים בנכסים פיננסיים אחרים, לאסוף, לקבל, לשמור ולהעביר בצורה מאובטחת את פרטי המעביר והנעבר בכל העברה, יחד עם או במקביל למסר ההעברה. אימוץ של חובות ה-"Travel Rule" ויישומן מהווים נדבך מרכזי ביכולת של נותן שירותים פיננסיים לנהל ולצמצם את סיכונים הלבנת ההון ומימון טרור הנובעים מפעילות במטבעות וירטואליים, וביכולתם של גורמי האכיפה להתחקות אחרי מקורות ויעדי ההעברות לאחר מעשה במקרה הצורך.

מאז בוצעו עדכונים אלו עוקב ה-FATF אחר יישום ההמלצות ברחבי העולם ובתוך כך, מפרסם הארגון דוחות תקופתיים הסוקרים את סטטוס היישום במדינות שונות, תוך התמקדות בזיהוי אתגרים העומדים בפניהן, ניתוח התפתחויות של סיכונים חדשים, ושיתוף פרקטיקות מומלצות ליישום אפקטיבי של הרגולציה. דוחות אלו משמשים ככלי מרכזי להערכת ההתקדמות הגלובלית ולזיהוי נקודות תורפה הדורשות התערבות.

התמונה העולה מן הדוח התקופתי האחרון מורכבת.²⁵ אף שנרשמה התקדמות בהיקף המדינות שביצעו הערכות סיכונים בתחום הנכסים הוירטואליים, הערכה אפקטיבית של מידת הסיכון ויישום גישה מבוססת סיכון עדיין מהווים אתגר עבור מדינות רבות. כמו כן, אף שמדינות רבות יותר פועלות לגבש רגולציה ביחס לפעילות בנכסים וירטואליים, עדיין קיימים פערים ניכרים וטרם ברור עד כמה מסגרות אלו מיושמות בפועל. עוד נמצא כי חלה עלייה במספר המדינות שהסדירו בחקיקה את ה- 'Travel Rule', אולם מרביתן טרם נקטו פעולות פיקוח ואכיפה מהותיות בתחום זה.

עיכובים ואי-אחידות ביישום ה- Travel Rule במדינות שונות יוצרים את מה שמכונה ה- 'Sunrise effect'. הציות ל- Travel Rule מחייב את ספק שירותי הנכסים הוירטואליים (VASP) המעביר לספק מידע לגבי זהות המעביר והנעבר ל-VASP המוטב, אם אכן יש כזה; אחד האתגרים בתחום הנכסים הוירטואליים הוא לזהות האם כתובת היעד מתייחסת לארנק "מתארח" (hosted), לגביו חלה חובת העברת הפרטים, או לארנק Un-hosted שאז אין חובה להעביר את הפרטים. בשל מצב היישום הבלתי אחיד, ייתכן שלא תמיד שני ספקי השירות יידרשו על ידי הרשויות במדינותיהם לציית ל- 'Travel Rule', ואז או שקשה לזהות האם הארנק המוטב הוא hosted ואצל איזה VASP, או שה-VASP המעביר אינו נתון לחובת ההעברה. במצב זה, עד שכל ספקי שירותי הנכסים הוירטואליים (VASPs) יחויבו ליישם את ה- 'Travel Rule' באופן אחיד בכל העולם, יימשך אתגר ההתמודדות בביצוע ותיאום עסקאות מול גורמים מקבילים; גם כאשר שני ה-VASPs כפופים לחובות ה- Travel Rule עולה לעיתים קושי אם אינם מחוברים לאותה מערכת לזיהוי ארנקים והעברת מידע (אתגר ה- interoperability).

החדשנות וההתפתחויות המהירות המאפיינות את תחום הנכסים הוירטואליים מציבות אתגר מתמשך בפני הרשויות המאסדרות בבואן להתמודד עם הסיכונים הנובעים ממנו. שוק זה מאופיין בדינמיות רבה, ודפוסי השימוש בנכסים ובשירותים משתנים תדיר, בהשפעת גורמים מגוונים, ובהם העדפות צרכנים, תחרות, רגולציה, ספקולציה, התפתחויות טכנולוגיות ושיקולי פרטיות ואבטחת מידע. עם זאת, ה- FATF ממשיך לעקוב אחר סיכונים מתפתחים, ובהם השימוש הגובר ביישומי DeFi ובארנקים פרטיים לצורך הלבנת הון, תחומים שעשויים לדרוש בעתיד התאמות נוספות של המסגרת הרגולטורית.

האסדרה בישראל

מדינת ישראל מחויבת ליישום הסטנדרטים הבינלאומיים בתחום מניעת הלבנת הון ומימון טרור ובכלל זה ההנחיות הרלוונטיות לנכסים וירטואליים ולנותני שירותים בהם. בהתאם לכך, בעשור האחרון ננקטו בישראל הצעדים הנדרשים להסדרת הפעילות בתחום, במטרה להבטיח עמידה בהמלצות ה- FATF וליצור מסגרת רגולטורית ברורה המאזנת בין ניהול סיכונים לעידוד חדשנות.

חוק הפיקוח על שירותים פיננסיים שנחקק ב- 2016²⁶ הוסיף את סקטור נותני השירותים הפיננסיים לרשימת הגופים המנויים בתוספת השלישית לחוק איסור הלבנת הון ("החוק")²⁷ שחל עליהם משטר איסור הלבנת הון. מכוח החוק הוסמכה רשות שוק ההון כרגולטור של הסקטור ובהתאם הינה הגוף המפקח על פעילותם של נותני שירותים בנכסים וירטואליים. החוק הכניס את המטבע הוירטואלי להגדרה של נכס פיננסי ובכך החיל חובת רישוי ופיקוח על גופים פיננסיים העוסקים בפעילות במטבע וירטואלי עבור לקוחות, לרבות המרה, החלפה ושמירה.

צו איסור הלבנת הון העוסק בתחום²⁸ תוקן על מנת להחיל חובות איסור הלבנת הון ומימון טרור על נותני שירות בנכס פיננסי לרבות נותני שירות בנכסים וירטואליים ונכנס לתוקף בנובמבר 2021. הצו קבע חובות משטר איסור הלבנת הון

²⁵ Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2025

²⁶ חוק הפיקוח על שירותים פיננסיים (שירותים פיננסיים מוסדרים) התשע"ו 2016

²⁷ חוק איסור הלבנת הון, תש"ס-2000

²⁸ צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של נותני שירות בנכס פיננסי ונותני שירותי אשראי למניעת הלבנת הון ומימון טרור) תשע"ח-2018

ומימון טרור על נש"פים ונותני שירותי אשראי, ובכלל זה על נש"פים העוסקים במטבעות וירטואליים, בהתאם לנדרש בסטנדרטים הבינלאומיים.

סעיף 7א לצו, המתבסס על המלצה 16 של ארגון ה-FATF כולל הוראות לעניין רישום פרטי הצדדים בהעברות אלקטרוניות והעברות של מטבעות וירטואליים. עם זאת מכיוון שבמועד כניסתו לתוקף של הצו טרם היו זמינים פתרונות טכנולוגיים מתאימים, נדחתה באותה עת כניסתו לתוקף של חובה זו. ביוני 2024 פרסמה רשות שוק ההון טיוטת תיקון חוזר בו נקבע כי החובה נכנסה לתוקף החל מ-01.01.2025.

לאור כניסתו לתוקף של צו איסור הלבנת הון על נותני שירות בנקסי פיננסי, עדכן הפיקוח על הבנקים במאי 2022 את הוראת ניהול בנקאי תקין 29,411²⁹ העוסק בניהול סיכונים הלבנת הון ומימון טרור במערכת הבנקאית. העדכון מחייב את התאגידים הבנקאיים לנהל סיכונים הלבנת הון ומימון טרור גם בפעילות הקשורה לנכסים דיגיטליים, תוך יישום גישה מבוססת סיכון. כך, בין היתר, נקבע כי במקרים של היקף פעילות משמעותי (מעל 100,000 ש"ח בשנה), על התאגיד הבנקאי לפעול בהתאם לגישה מבוססת סיכון ולבחון את נתיב הכספים. יחד עם זאת, חל איסור על סירוב גורף לקבלת כספים שמקורם בפעילות בנקסית וירטואליים, בין אם ליחיד ובין אם לתאגיד, וזאת בתנאי שנותן השירות שמהווה צד בעסקה קיבל רישיון לפעילות בישראל.

בפברואר 2023, קיבלה ממשלת ישראל החלטה מספר 204 לקידום אסדרתו של שוק הנכסים הוירטואליים. החלטה זו נועדה ליצור ודאות רגולטורית, לנהל סיכונים, ולעודד חדשנות בתחום.

במסגרת ההחלטה הציבה הממשלה מספר יעדים מרכזיים:

- **ניהול מושכל של סיכונים:** הגנה על משקיעים, צרכנים ועסקים הפועלים בתחום הנכסים הדיגיטליים, תוך צמצום סיכונים פיננסיים, סיכונים הלבנת הון ומימון טרור, וסיכונים סייבר.
- **יצירת ודאות רגולטורית:** הגברת הודאות הרגולטורית עבור שחקנים בשוק המקומי, עידוד חדשנות וצמיחה של התעשייה, ומשיכת חברות ומשקיעים זרים.
- **ייעול השימוש במשאבי הפיקוח:** התאמת המסגרת הרגולטורית למאפיינים הייחודיים של נכסים דיגיטליים, ויצירת מנגנוני פיקוח יעילים ואפקטיביים.

לצורך הסדרת הפן המיסויי פרסמה רשות המסים [עמדות מקצועיות וחוזרים המבהירים את חובות המס והדיווח על פעילות בנקסים דיגיטליים](#). באפריל 2024 פורסמה הוראת שעה המאפשרת תשלום מס רווחי הון על נכסים דיגיטליים דרך חשבון בנק של רשות המסים בבנק ישראל, במקרים בהם הבנקים המסחריים מסרבים לקבל כספים אלו. בנובמבר 2024 פורסם תזכיר חוק ראשון שמגדיר "נכס דיגיטלי" בחקיקה וקובע כללים למיסוי רווחי הון בישראל מנכסים אלו. בינואר 2025 פורסמה טיוטת תקנות לפטור מדיווח שנתי על מכירת נכסים דיגיטליים דרך גורם מפוקח, במטרה להקל על הציבור וליצור ודאות רגולטורית.

²⁹ הוראות ניהול בנקאי תקין (נב"ת) חן הוראות שמפרסם המפקח על הבנקים הנוגעות לדרכי פעולתו וניהולו של תאגיד בנקאי.

מדיניות רשות שוק ההון, הביטוח והחסכון

במסגרת הרישוי והפיקוח של רשות שוק ההון ביטוח וחסכון על נותני שירותים פיננסיים בנכסים וירטואליים מיושמות בין היתר הנחיות שפרסם ארגון ה-FATF לעניין VASP'S ואימוץ של סטנדרטים בינלאומיים.

בהתאם לכך, הרשות שמה דגש רב על היבטים רבים ובכללם: מהימנותם ויושרתם של נושאי משרה ובעלי מניות, יכולת מקצועית מוכחת, הבנה רגולטורית ומדיניות וכלים טכנולוגיים לניטור וניהול הסיכונים המוגברים להלבנת הון ומימון טרור.

במסגרת בחינתה של בקשת הרישיון מושם דגש רב על סוג השירותים הפיננסיים שמבקש הרישיון מעוניין להציע ובפרט האם יש לו את היכולת ואת המשאבים להתמודד עם הסיכונים המאפיינים את הפעילות הפיננסית המבוקשת, לדוגמא ככל שמבקש הרישיון מעוניין להציע שירותי קנייה ומכירה של מטבעות וירטואליים אנונימיים או מטבעות אחרים שהנפיקו גורמים לא מזוהים, הרשות לא תאפשר זאת.

בנוסף, כאמור, הרשות בוחנת היבטים הנוגעים למהימנותם של נושאי משרה ובעלי מניות במבקש הרישיון וזאת במטרה למנוע את כניסתם של גורמים עבריינים לתחום של מטבעות וירטואליים. זאת ועוד, באשר לספקי נזילות - מבקשי רישיון רבים מסתמכים על התקשרות עם זירות מסחר בחו"ל, על מנת שאלו ישמשו ספקי נזילות, ויתמכו ביכולת של מבקש הרישיון לבצע פעילויות של קנייה ומכירה של מטבעות וירטואליים עבור לקוחותיו. הרשות בוחנת את מעמדו של ספק הנזילות במדינה בה הוא פועל, את המוניטין שלו וכן את מקום התאגדותו והיכן הוא מפוקח. היה ומבקש הרישיון התקשר עם ספק נזילות הפועל ללא פיקוח, ואז פועל תחת משטר רגולטורי רופף, הרשות לא תאשר זאת ובהיעדר יכולת להתקשר עם ספק נזילות מפוקח, לא ניתן יהיה להתקדם עם הבקשה. מלבד האמור, רשות שוק ההון בוחנת האם מבקש הרישיון מכיר את הסיכונים הייחודיים שמלווים את פעילותו העסקית והאם יש לו את המשאבים ואת היכולת המקצועית לנהל את הסיכונים. הרשות בוחנת את מעמדם של קציני הציות, את מקצועיותם של נושאי המשרה וכן את המשאבים הטכנולוגיים שעומדים לרשות מבקש הרישיון על מנת שהוא יוכל לעמוד בהוראות צו איסור הלבנת הון ובהוראות הממונה. ככל שאין למבקש הרישיון את היכולות הטכנולוגיות המתאימות ואת המשאבים הנדרשים לכך, הבקשה עלולה להידחות.

כפועל יוצא של מדיניות הרישוי, דחתה הרשות בקשות רבות של מבקשי רישיון ממגוון סיבות: עשרות בקשות של מבקשי רישיון בשל היבטי יושר ויושרה, אחרות נדחו על בסיס מהותי, לאחר ניתוח הבקשה וזיהוי פעילות בעלת סיכון גבוה וסיכוני סייבר, כמו כן, נדחו בקשות רישיון של מבקשי רישיון, שלא עמדו בסטנדרט הנדרש בהיבטי מקצועיות, הכרת הרגולציה הנדרשת ובנוסף, נדחו כאלו אצלם התגלה מחסור מהותי בכלים הנדרשים כדי לזהות ולהתמודד עם הסיכונים המוגברים להלבנת הון ומימון טרור.

דגלים אדומים



מטרתם של הדגלים האדומים היא לחזק את המודעות הציבורית לסיכוני הלבנת הון ומימון טרור הנובעים מפעילות בנכסים וירטואליים ואת היכולת של המגזר הפיננסי לזהות ולהתריע אודות הפעילויות המפורטות ברשימה.

יובהר, כי דגל אדום מהווה אינדיקציה אשר עשויה לסייע בזיהוי פעילות חריגה. אין בקיומו של דגל אדום בודד בפני עצמו כדי להעיד בהכרח על סיכון להלבנת הון או מימון טרור, ובלבד שקיים הסבר מניח את הדעת לפעילות זו.

ככל שקיימים דגלים אדומים רבים יותר בפעילות, כך מתגבר החשש כי מדובר בפעילות בעלת זיקה להלבנת הון או מימון טרור.

דגלים אדומים אלו יכולים לשמש עילה לבחינה של הפעילות והעברת דיווח בלתי רגיל לרשות בגינה. חשוב להבהיר כי הרשימה שלהלן אינה מהווה רשימה מלאה או סגורה.

הרשות פרסמה בעבר רשימות מפורטות של דגלים אדומים בתחום הנכסים הוירטואליים על סמך דוחות מקצועיים של ה-FATF שבהם ניתן לעיין בקישורים מטה. להלן מפורטים דגלים נוספים בתחומים ממוקדים המבוססים, בין היתר, על דוח מחקר של חברת ניתוח בלוקצ'יין.³⁰

אינדיקטורים לגבי הפעולה בנכס וירטואלי

- פעילות בהיקף גבוה, אשר לאחר מכן נותרת בארנק לתקופה ארוכה ללא ביצוע פעולות נוספות (מאפיין מקרים של תשלום בגין מתקפת כופרה).
- פעילות מורכבת בהיקפים גבוהים, המבוצעת במהירות ובמספר רב של כתובות ארנק, באופן הנראה כי ההוראות ניתנות באופן אוטומטי.
- העברות רבות מבוצעות ל-VASPs שונים במהירות, בייחוד כאשר מדובר בזירות בחו"ל בהן הרגולציה חלשה.
- הפקדה של כספים או מטבעות לזירה מסחר, קניה של מטבעות ומיד העברתם לארנק פרטי (שימוש בזירה כ"מיקסר").

אינדיקטורים לגבי זירות מסחר זר בלתי מפקחות/משטר ציות לקוי

- הזירה אינה מבצעת הליכי זיהוי לקוח, מאפשרת פתיחת חשבון עם מידע בסיסי בלבד, כגון כתובת אימייל וסיסמה.
- הזירה מאפשרת ללקוחות לממן את חשבונם גם אם קיבלו נכסים וירטואליים ישירות ממערבלי מטבעות.
- אין מידע משמעותי באתר הזירה לגבי נהלי הציות שלה, מבנה הניהול או רישום העסק.
- היקף משמעותי של העברות נכסים וירטואליים המגיעות לזירה מכתובות הקשורות למקורות פליליים, כגון התקפות כופרה, הימורים, הונאות, מימון טרור ושווקי רשת האפלה.
- אתר האינטרנט של הזירה מזהיר לקוחות לא להזכיר נכסים וירטואליים כאשר הם מדברים עם גורמים חיצוניים כמו בנקים.
- הזירה מנחה לקוחות להזין מידע מעורפל או מטעה בשדות הודעות העברה בנקאית בעת העברת כספי פינט לבנק או ממנו.

- הזירה נרשמה רק לאחרונה ואין לה היסטוריה קודמת ומבוססת של מסחר בנכסים וירטואליים.
- הזירה מוזכרת במסגרת פורומים/צ'טים בעלי זיקה לפעילות פלילית באינטרנט/ברשת האפילה.
- הזירה מפרסמת שהיא מאפשרת ללקוחות להחליף מזומן בנכסים וירטואליים.

אינדיקטורים לגבי זירות מסחר הפועלות במדינות בעלות סיכון גבוה

- זירת המסחר רשומה במדינה הנמצאת תחת סנקציות בינלאומיות.
- זירת המסחר מבצעת מסחר בהיקף גבוה במטבעות פיאט ממדינות הנתונות לסנקציות.
- זירת מסחר הפועלת במדינה בה משטר איסור הלבנת הון ומימון טרור חלש.
- מיקום זירת המסחר לא ידוע או אין כמעט מידע ממקורות גלויים לגבי המיקום גיאוגרפי של זירת המסחר.
- מבנה הבעלות (של הזירה) סבוך או מורכב וכולל חברות הרשומות במקלטי מס.
- מידע הרישום או המעמד המשפטי של זירת המסחר לא ברור, סותר או חסר הסבר (לדוגמה, מטה בבולגריה, אך כפוף לחוקי קפריסין).
- זירת המסחר מציעה צמדי מסחר במטבעות פיאט שאינם הגיוניים עסקית (לדוגמה, בורסה בפינלנד מציעה מסחר בפזו קולומביאני).
- זירת המסחר רשומה במדינה בסיכון נמוך, אך בעלי השליטה והדירקטורים מגיעים ממדינות בסיכון גבוה.
- על בעלי השליטה בבורסה ישנו סיקור תקשורתי שלילי.
- בעלי השליטה בבורסה הינם אנשי ציבור (PEPs).
- פרטי הקשר של הבורסה הנם של מדינה בסיכון גבוה, אך היא בבעלות חברות רשומות במדינות אחרות ללא סיבה ברורה.
- זירת המסחר משתמשת במעבדי תשלומים ממדינות בסיכון גבוה ללא סיבה נראית לעין.
- נציגי זירת המסחר משתמשים בדומיינים של אתרי אינטרנט ממדינות בסיכון גבוה, ללא קשר ברור למקום העסק הרשמי.

נסיבות המפחיתות סיכון

מטרתו של חלק זה לסייע למוסדות הפיננסיים בניהול הסיכונים הכרוכים בפעילות בנכסים וירטואליים. בדומה לדגלים אדומים, אין די בקיומה של נסיבה אחת כדי לבסס מסקנה בדבר סיכון נמוך של אותה פעילות, ויש לבחון בכל מקרה האם ישנם תסמינים אחרים העלולים להעיד על פעילות חריגה. רשימת הנסיבות מפחיתות הסיכון רלוונטית ככל שמדובר בנכס וירטואלי שמקורו בנותן שירותים בנכסים וירטואליים בעל רישיון שניתן במדינה בעלת רמת סיכון נמוכה מבחינת הלבנת הון ומימון טרור:

- פעילות מול זירות ישראליות בעלות רישיון מרשות שוק ההון למתן שירות פיננסי במטבע וירטואלי.
 - פעילות מול זירות מפוקחות במדינות העומדות בסטנדרט הבינלאומי החל על פעילות בנכסים וירטואליים.
- ביוני 2020 פרסמה הרשות [מסמך](#) אשר כותרתו "יישום גישה מבוססת סיכון בתחום הנכסים הוירטואליים". במסמך זה פורסמה רשימה נוספת של נסיבות מפחיתות סיכון (עמ' 8-9) והן עומדות בתוקפן גם כיום:
- פעילות בהיקף נמוך שייקבע על ידי הגורמים הרלוונטיים, בשים לב ליישום מנגנון לבחינת היקף הפעולות בסכום נמוך, על בסיס מצטבר, כדי לוודא שלא מתקיים פיצול עסקאות ולראייה של תמונת ההיקפים הכוללת.
 - נכסים וירטואליים שהתקבלו באופן ישיר מפעילות כרייה – כאשר ניתן לזהות את מקור הכספים למימון פעילות הכרייה, בהיקף מתאים לסכומים שהתקבלו;



- נכסים וירטואליים שנרכשו ונמכרו אל או מאותה כתובת ארנק אלקטרוני (address Wallet) עבור אותו לקוח, כאשר לא היו בכתובת הארנק האלקטרוני הספציפית תנועות נוספות (העברה אל או ממקורות אחרים זולת הלקוח);
- נכסים וירטואליים שנרכשו ונמכרו אל או מאותה כתובת ארנק אלקטרוני (address Wallet) עבור אותו לקוח, גם אם כאשר הנכסים הוירטואליים נקנו ומומשו באמצעות אותה כתובת ארנק אלקטרוני אך בוצעו באותה הכתובת תנועות נוספות מגופים או לגופים אחרים ככל שמדובר בפעולות "חלפנות" מול גופים מפוקחים הנמצאים במדינות בסיכון נמוך להלבנת הון, שביצעו זיהוי ללקוח או שהמימוש נעשה באמצעות הגופים המפוקחים האמורים;
- אישור מרשויות המס על תשלום מס בגין רווחים או הכנסות מפעילות בנכסים וירטואליים – נסיבה זו עשויה להצטרף לנסיבות אחרות ולהעיד על סיכון מופחת, אך לא כנסיבה חלופית העומדת בפני עצמה.



להרחבה וקריאה נוספת ראו להלן:

- הרשות לאיסור הלבנת הון ומימון טרור, [דגלים אדומים בתחום הנכסים הוירטואליים](#), דצמבר 2019.
- הרשות לאיסור הלבנת הון ומימון טרור, [יישום גישה מבוססת סיכון בתחום הנכסים הוירטואליים](#), יוני 2020.
- FATF, [Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing](#), ספטמבר 2020.
- FATF, [מדריך ליישום גישה מבוססת סיכון בנוגע לנכסים וירטואליים ולגותי שירות בנקס וירטואלי](#) (תקציר בעברית, כולל הפניה למדריך המלא באנגלית), אוקטובר 2021.
- הרשות לאיסור הלבנת הון ומימון טרור, [תקציר סקירת ה-FATF - בתום שנה מתיקון הסטנדרטים הבינלאומיים למאבק בהלבנת הון ובמימון טרור בתחום הנכסים וירטואליים](#), יולי 2022.
- הרשות לאיסור הלבנת הון ומימון טרור, [ניצול של המערכת הפיננסית לטובת העברת תשלומים בגין מתקפות כופרה](#), פברואר 2022.