בנק ישראל
יוני 2022

שקל דיגיטלי

ועדת ההיגוי של בנק ישראל
להנפקה אפשרית של
שקל דיגיטלי

ניסוי על גבי פלטפורמה מבוזרת

בנק ישראל - ועדת ההיגוי של בנק ישראל להנפקה אפשרית של שקל דיגיטלי

יוני 2022

הניסויים המתוארים בנייר זה במסגרת עבודת הצוות הטכנולוגי של פרוייקט השקל הדיגיטלי.

לקחו חלק בעבודת הניסוי:
אייל זפרני, תומר מזרחי, נאורס דחלה, אביה הולנדר, אילן מתתיהו, דניאל סקוריקוב, גיל פולק – החטיבה לטכנולוגיית המידע.

כותבי הנייר:
אייל זפרני, תומר מזרחי – החטיבה לטכנולוגיית המידע, יואב סופר – מנהל פרויקט השקל הדיגיטלי.

תוכן עניינים

04
רקע

06
מבנה המערכת

09
התחברות לקוחות קצה למערכת וביצוע פעולת תשלום

11
יישומים אפשריים של חוזים חכמים במערכת השקל הדיגיטלי

16
פרטיות מוגבלת בתשלומים דיגיטליים

19
סיכום

21
ביבליוגרפיה

1. רקע

ועדת ההיגוי של בנק ישראל להנפקה אפשרית של שקל דיגיטלי בונה תכנית פעולה, כך שבמידה וייווצרו תנאים בעתיד שיביאו לכך שלהערכת בנק ישראל התועלות מהנפקת שקל דיגיטלי עולות על העלויות והסיכונים הפוטנציאליים, בנק ישראל יהיה ערוך ומוכן להוציא תכנית זו לפועל. במסגרת הפרויקט, מתבצעת גם למידה של החלופות הטכנולוגיות, וההזדמנויות והסיכונים שעשויים להיות גלומים בטכנולוגיות שונות ליישום מערכת השקל הדיגיטלי. למידה זו מתבצעת הן על ידי ניתוח תיאורטי, והן במסגרת ניסויים מעשיים בהם נבחנות טכנולוגיות שונות. ברקע הדברים, בנקים מרכזיים רבים בעולם עורכים ניסויים טכנולוגיים מגוונים בהיקפים שונים – חלקם בתנאי מעבדה בלבד (ניסויים אלה מכונים לעיתים PoC – Proof of Concept), וחלקם תוך שימוש בכסף "אמיתי" ובהשתתפות משתתפים - גופים פיננסיים, בתי עסק וצרכנים – "אמיתיים" (ניסויים המכונים לעיתים Pilot –). עם זאת, אף מדינה מפותחת עדיין לא החליטה על הנפקה של מטבע דיגיטלי של הבנק המרכזי, לא כל שכן בחרה את הטכנולוגיה עליו הוא יתבסס, מה שהופך את משימת הלמידה של החלופות הטכנולוגיות למאתגרת. הלימוד והחקירה באמצעות ניסוי מאפשרים לתת מענה לסוגיות טכנולוגיות בד בבד עם בחינה של היבטים עסקיים וסוגיות מדיניות.

מסמך זה מתאר את הניסוי הטכנולוגי הראשון שערך בנק ישראל במסגרת תכנית הפעולה של פרוייקט השקל הדיגיטלי. הניסוי נערך בתנאי מעבדה (PoC), ובמסגרתו, הוקמה בסביבת ניסוי תשתית מבוזרת (DLT – Distributed Ledger Technology) בענן, עליה מומשה מערכת Quorum Blockchain המבוססת על את'ריום (Ethereum). יודגש, שהעובדה שסביבה זו נבחרה לניסוי אין בה כדי להצביע על כך שבנק ישראל מתכוון לממש את מערכת השקל הדיגיטלי - ככל שיוחלט להנפיק אותו - על גבי סביבה מבוזרת, בכלל, או על גבי טכנולוגיית את'ריום בפרט. כמו כן, אין בכך כדי להצביע על כך שטכנולוגיה זו עדיפה על פני טכנולוגיות אחרות. בניסויים הנערכים על ידי בנקים מרכזיים בעולם נבחנת טכנולוגיה זו[1] לצד טכנולוגיות מבוזרות אחרות[2], ובמקביל נבחנות גם טכנולוגיות שאינן מבוזרות[3]. בנק ישראל בחר לערוך את הניסוי בסביבה טכנולוגית זו על מנת לאפשר לצוותים המקצועיים בבנק להתנסות בשימוש בטכנולוגיות מבוזרות בכלל ובטכנולוגיית

[1] ראו למשל, Bank of Thailand, 2021, Reserve Bank of Australia (2021)
[2] למשל, Sveriges Riksbank, 2022, Federal Reserve Bank of Boston (2022)
[3] למשל, Bank of Japan (2022)

את'ריום בפרט, לאור היותה של טכנולוגיה זו פלטפורמת קוד פתוח שמאפשרת בנייה של יישומים מגוונים. הבחינה של חלק מהיישומים האלה יכולה לתמוך בניתוח של היכולת של השקל הדיגיטלי לממש חלק מהמוטיבציות האפשריות להנפקתו, כפי שתוארו בדוח שפרסמה ועדת ההיגוי (בנק ישראל, 2021). הכוונה היא שהפלטפורמה שהוקמה תשמש כמעין אב טיפוס מתגלגל, שעל גביו ניתן יהיה לבחון בהמשך שאלות טכנולוגיות שונות תוך שינוי של התצורה בהתאם לצורך.

השלב הראשון של הניסוי כלל את הקמת הפלטפורמה, ובחינת היכולת לבצע בה את הפעולות הבסיסיות של הנפקת המטבע הדיגיטלי והעברתו מארנק לארנק (ביצוע פעולת תשלום). בנוסף, נבחנה היכולת להטיל מגבלות כמותיות על פעולות התשלום, ולעשות שימוש ב"חוזים חכמים" לצורך פעולת Delivery vs. Payment. יכולת זו עשויה לשמש כאחד הנדבכים לפוטנציאל של השקל הדיגיטלי ליצור תשתית חדשנית, שתבטיח את התאמת מערך התשלומים לצרכים של הכלכלה הדיגיטלית העתידית - אחת המוטיבציות שתוארו על ידי ועדת ההיגוי.

מוטיבציה נוספת שוועדת ההיגוי פירטה הנה שמירת האפשרות של הציבור לעשות שימוש באמצעי תשלום דיגיטלי תוך שמירה על רמה מסוימת של פרטיות, וזאת בתנאי שתובטח העמידה בכללים שקובעות רשויות המדינה בכל הנוגע לאיסור הלבנת הון ומימון טרור, ולגילוי הנדרש לרשויות המס. בהקשר זה, בשלב השני של הניסוי נבחנה טכנולוגיה חדשנית שפורסמה לאחרונה על ידי חוקרים מחברת VMware [4], המאפשרת לקובעי המדיניות להגדיר רף תקופתי מסוים של תשלומים דיגיטליים שניתן יהיה לבצע באופן אנונימי.

בנק ישראל ממשיך לחקור את האפשרויות הגלומות בטכנולוגיות חדשניות שפותחו בשנים האחרונות, ואת הישימות האפשרית של טכנולוגיות אלה לממש את המוטיבציות האפשריות להנפקה אפשרית של שקל דיגיטלי, ויעדכן את הציבור מעת לעת בדבר ממצאי הבחינה.

[4] Tomescu, et al. 2022

2. מבנה המערכת

לצורך הניסוי הוקמה תשתית DLT בענן של Microsoft Azure באמצעות השירות Azure Blockchain Services, המאפשר לממש Quorum Blockchain המבוסס על את'ריום (Ethereum). על פי טיוטת המודל שפרסמה ועדת ההיגוי, מערכת השקל הדיגיטלי בניסוי נבניתה במודל של two-tier (איור 1): בעוד שהשקל הדיגיטלי מהווה התחייבות של הבנק המרכזי כלפי ציבור המחזיקים בו, הציבור אינו ניגש ישירות אל הבנק המרכזי על מנת לקבל, לפדות, או לשלם בשקל הדיגיטלי. הגישה של הציבור מתאפשרת באמצעות "ספקי שירותי תשלום" - אלו יכולים להיות בנקים, גופים פיננסיים אחרים, חברות פינטק, ועוד. בסביבת הניסוי הוקמו ארבעה שרתים (Nodes) על הבלוקצ'יין, שמדמים מצב בו בנוסף לבנק המרכזי, מערכת השקל הדיגיטלי כוללת שלושה ספקי שירותי תשלום. כל ספק שירותי תשלום נוצר ב–Node נפרד ומתקיים ביזור מלא של הרשת. בנק ישראל הוא ה-Administrator של הרשת ומגדיר את ספקי שירותי התשלום כ-validators – מאשרי עסקאות. בנוסף, בנק ישראל הוא זה שמממש את החוזה החכם שמגדיר את המטבע הדיגיטלי והוא בעל ההרשאה היחידה להנפיק ולהשמיד (minting and burning) מטבעות. ספקי שירותי התשלום מספקים ללקוחות הקצה תשתית ושירות של ארנק דיגיטלי באמצעותו הלקוחות ניגשים לרשת השקל הדיגיטלי, והם אלו שמעבירים את פקודות העברת התשלום בין לקוחות הקצה. יודגש, שהספקים אינם מחזיקים את השקלים הדיגיטליים של לקוחות הקצה, הם רק מקנים ללקוח את הגישה הטכנולוגית אל רשת הבלוקצ'יין ומעבירים בשמו את הוראות התשלום.

ברשתות בלוקצ'יין מבוזרות לחלוטין, שכל גורם יכול לגשת אליהן (permissionless blockchain), אין אמון בין המשתתפים ברשת, והן מתבססות על מנגנוי קונצנזוס כדוגמת Proof of Work - מנגנון יקר ומסורבל שצורך כמויות גדולות של אנרגיה. לעומת זאת, מנגנון אישור העסקאות (מנגנון הקונצנזוס) בניסוי הוא מנגנון של Proof of Authority (PoA). במערכת CBDC האמון מבוסס על המוניטין של הבנק המרכזי, והעובדה שהבנק הוא זה שמחליט מי יכול לשמש כ-validator למעשה מאצילה את האמון ממנו נהנה הבנק המרכזי אל אותם validators, תוך שמירה על הביזור של המערכת, מה שמאפשר להשתמש במנגנון של PoA (וצריכת האנרגיה נמוכה באופן משמעותי - בדומה לזו של מערכות תשלומים סטנדרטיות).

בניסוי השתתפו שלושים "לקוחות קצה" – בפועל היו אלה עובדי בנק ישראל השותפים בצוותי העבודה של השקל הדיגיטלי, שדימו את הלקוחות בניסוי – וחולקו באופן רדנומלי בין שלושת ספקי שירותי התשלום. עבור כל המשתתפים ברשת (בנק ישראל, ספקי שירותי תשלום, ומשתמשי קצה) נוצרו שלושת הפרמטרים הבאים:

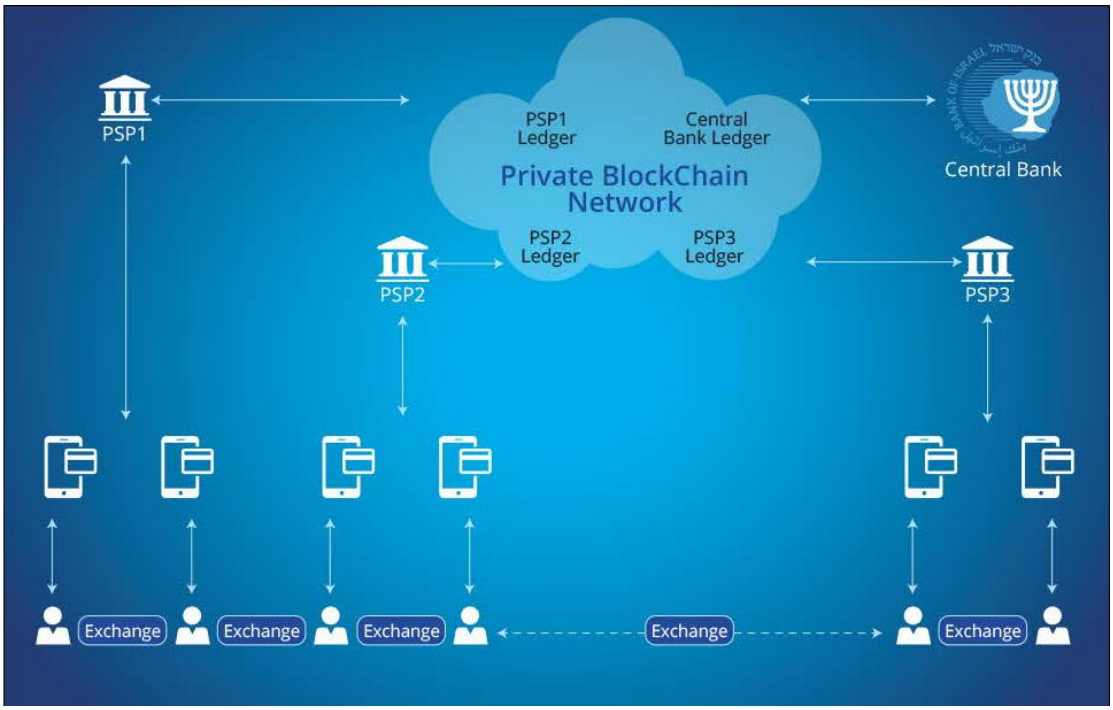
i. כתובת ציבורית ברשת הבלוקצ'יין (Address).

ii. מפתח פרטי (Private Key).

iii. זהות דיגיטלית מרכזית (Digital Identity).

ספקי שירותי התשלום הם אלו שמחזיקים את המפתח הפרטי ואת נתוני ה-KYC של לקוחות הקצה.

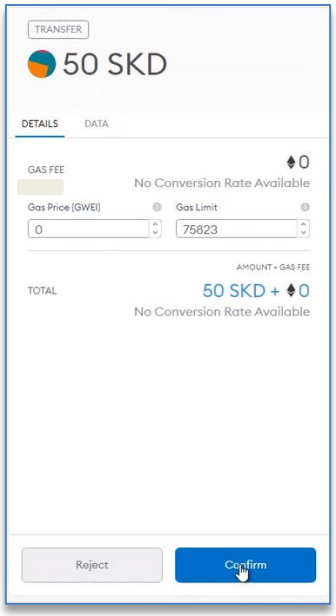
<u>איור 1: מבנה המערכת במודל Two-Tier</u>



לאחר הקמת המערכת, בנק ישראל "הנפיק" את ה"שקלים הדיגיטליים" באמצעות תקן ERC20. התקן כולל אופרציות להנפקת המטבע ולביצוע תשלומים על ידי משתמשי הקצה או ספקי שירותי התשלום.

השימוש בתקן ERC 20 על גבי בלוקצ'יין סטנדרטי של Quorum Ethereum מאפשר למעשה להחזיק את השקלים הדיגיטליים שהונפקו בניסוי בכל ארנק סטנדרטי שנמצא בשוק. על מנת לבחון את התאמת המערכת לסטנדרט בוצע חיבור של ארנק MetaMask[5], בסיטואציה המדמה מצב בו לקוחות הקצה מחזיקים את המפתח הפרטי בארנק הדיגיטלי שברשותם. הארנק זיהה את ה-Token שמייצג את השקלים הדיגיטליים בניסוי, וניתן היה לבצע העברה של שקלים דיגיטליים מלקוח אחד לשני (איור 2).

<u>איור 2 גישה לרשת הבלוקצ'יין והעברה ראשונית של שקלים דיגיטליים באמצעות ארנק סטנדרטי</u>



[5] ניתן היה להשתמש בכל ארנק שתומך בתקן ERC 20.

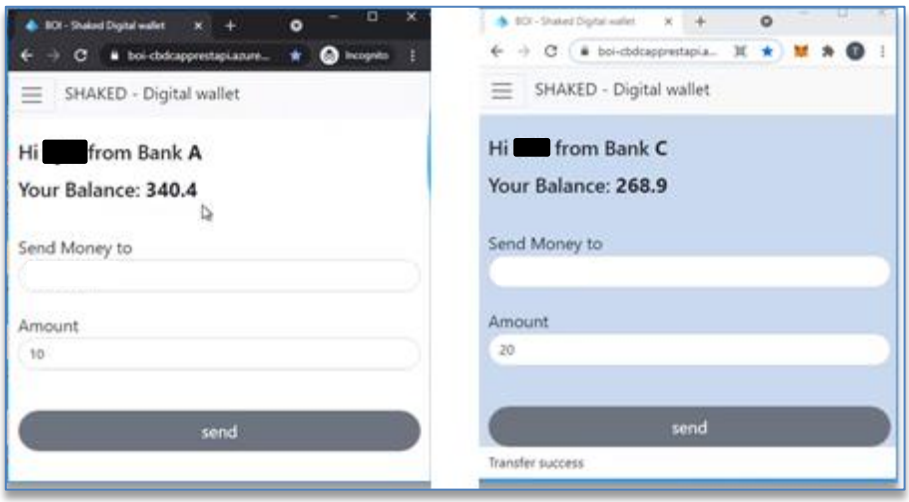
3. התחברות לקוחות קצה למערכת וביצוע פעולת תשלום

חלק מההיגיון שבסיס היישום של מטבע דיגיטלי של הבנק המרכזי במודל של two tier מתבסס על היתרון היחסי של המגזר העסקי ביחס לבנק המרכזי בכל הנוגע לביצוע הליכי "הכר את הלקוח" (KYC) הנדרשים מכוח כללי איסור הלבנת הון ומימון טרור. במסגרת הניסוי דימינו בצורה פשוטה מצב בו מתקיימת מערכת זיהוי לאומי, שממנה ספקי שירותי התשלום יכולים לשאוב מידע אודות הזהות של הלקוחות[6]. לאחר ההזדהות מול ספק שירותי התשלום, הלקוח מתחבר למערכת, ומקבל address בבלוקצ'יין המשויך לזהות שלו, שאליה משתמשים אחרים רשאים להעביר כסף דיגיטלי. לשם פשטות, במסגרת הניסוי לא נבחן אופן ה"רכישה" של שקל דיגיטלי על ידי הלקוח – כלומר, לא הודגמה העברה של כסף מחשבון הבנק או כסף מזומן אל ארנק השקל הדיגיטלי. במקום זאת, בתחילת הניסוי לקוחות הקצה קיבלו יתרת התחלתית של שקלים דיגיטליים שהונפקה על ידי בנק ישראל, על מנת שניתן יהיה להתנסות בביצוע פעולות תשלום.

על מנת לבצע תשלום ללקוח אחר, הלקוח בוחר את הכתובת להעברת התשלום, ואת הסכום שהוא מעוניין להעביר (איור 3). ספק שירותי התשלום מזהה את הלקוח ושולף את ה-address שלו ואת המפתח הפרטי שלו. הספק מתחבר לבלוקצ'יין, ומעביר לרשת את ה-address של המקבל ואת הסכום להעברה. הפקודה מתקבלת בבלוקצ'יין ומפעילה את פונקציית transfer מתוך החוזה החכם בתקן ERC 20. פעולה זו מאמתת את העובדה של-address של המשלם ישנה יתרה מספקת, וככל שזה המצב מתבצעת העברה של הסכום ל-address המקבל. מנגנון הקונצנזוס מוודא שהמצב החדש מסונכרן ב-ledger אצל כל שאר ה-nodes.

[6] מאחר והלקוחות בניסוי הם עובדי בנק ישראל, ההזדהות בוצעה באמצעות מערכת ההזדהות הארגונית של בנק ישראל.

איור 3: תצוגת ארנק של לקוח אצל ספק שירותי תשלום. הארנק מציג את היתרה, ואת בקשת ההעברה לפי גובה הסכום ושם המקבל



איור 4: תיאור התנועות המוזנות במערכת

Transfer From	Transfer To	Amount
0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	0xebb4c6e6abb89ddec9c28265d02e89784342984	10
0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	0xe2aa67e6127f7d94cf7765f6417e301a098c4b	50
0xe2aa67e6127f7d94cf7765f6417e301a098c4b	0xcad739f1d9db299464f8685b4bd6d6d6b8835c148	2000

אחד הסיכונים הגלומים ביישום מטבע דיגיטלי של הבנק המרכזי הוא הסיכון ל-bank disintermediation – מצב בו הלקוחות ימשכו חלק גדול מחשבונות הבנק שלהם וימירו אותם לשקל הדיגיטלי. בהקשר זה, מדינות שונות בוחנות את הצורך בהגבלת השימוש ב-CBDC, על מנת למנוע פגיעה משמעותית במערכת הבנקאית[7]. במסגרת הניסוי, נבחנה היכולת להגביל את גובה העברה הבודדת, ומספר ההעברות הכולל ביום אחד, באמצעות כתיבת המגבלות בחוזה החכם[8].

[7] במטבע הדיגיטלי של הבנק המרכזי של הבהאמס, sand dollar, יש שתי רמות של ארנקים. בגבוהה מביניהן, ניתן להחזיק עד 8000 דולר וישנה מגבלת תשלום של 10,000 דולר, והארנק מחובר לחשבון הבנק של הלקוח, כך שסכום שמעבר ליתרה יעבור אוטומטית לחשבון הבנק. באירופה, ה-ECB ציין את הרף של 3000 אירו כרף אפשרי שמעליו לא ניתן יהיה להחזיק באירו הדיגיטלי.

[8] על מנת להשיג את המטרה של מניעת פגיעת המערכת הבנקאית נכון יותר להגביל את גובה היתרה שניתן להחזיק ולא את סכום ההעברה. אולם, יישום יעיל של מגבלה כזו מצריך חיבור ישיר אל חשבון הבנק, כך שיתרה עודפת תועבר לחשבון, ולא ניתן היה לבחון זאת בניסוי זה.

לקוח שניסה להעביר סכום גבוה מהיתרה שהוגדרה, או שניסה לבצע מספר העברות גבוה מהמותר ביום, קיבל הודעת שגיאה. יודגש, שלא מדובר בבחינה של ההיתכנות העסקית או ההשפעה הכלכלית של מגבלות כאלה – הבחינה הוגבלה ליכולת ליישם מגבלות אלה באמצעות הטוקן הסטנדרטי.

4. יישומים אפשריים של חוזים חכמים במערכת השקל הדיגיטלי

אחת המוטיבציות שתיארה ועדת ההיגוי להנפקה אפשרית של שקל דיגיטלי היא יצירת תשתית תשלומים שתתמוך באימוץ חדשנות, והתאמת מערך התשלומים לצרכים של הכלכלה הדיגיטלית. התפתחות ה- Distributed Ledger Technologies והקונספט של טוקניזציה דיגיטלית של הכסף הביאו רעיונות חדשים לפיתוח יישומי תשלום מתקדמים על בסיס שימוש בחוזים חכמים. כך, למשל, מטבע דיגיטלי יוכל לתמוך בשימושים של "אספקה תמורת תשלום" (Delivery versus payment), שיפשטו הליכי תשלום רבים במשק ויספקו ביטחון וודאות לשני הצדדים בעסקת התשלום. על פי טיוטת המודל שפרסמה ועדת ההיגוי, בנק ישראל אמור להעמיד את התשתית שתתמוך ביכולת של ספקי שירותי התשלום להציע ישומי תשלום מתקדמים.

האופן בו התבצע המימוש הטכנולוגי של השקל הדיגיטלי במסגרת הניסוי, כ-token בפלטפורמת DLT שתומך בחוזים חכמים, מאפשר למעשה לכל גורם שמחובר לבלוקצ'יין – ובמקרה שלנו, לספקי שירותי התשלום – לכתוב תכניות שיקבעו כללים על אופן העברת הכסף תוך שימוש בחוזה חכם שמשתמש ב-token באופן טבעי, מבלי שאותו גורם נדרש לכתוב תכנית יעודית על גבי מערכות הליבה שלו (חשיפה של API יעודי).

כמקרה בוחן, במסגרת הניסוי בחנו סיטואציה בה מתבצעת מכירה של רכב[9] תמורת שקלים דיגיטליים. במצב הקיים היום, פעולת העברת הבעלות מהמוכר לקונה ברשות הרישוי (למשל, בדלפק בסניף הדואר) ופעולת העברת הכסף מהקונה למוכר (למשל, באמצעות העברה במערכת זה"ב) אינן מסונכרנות זו עם זו, והצד הראשון שמבצע את הפעולה חשוף לסיכון שהצד השני לא

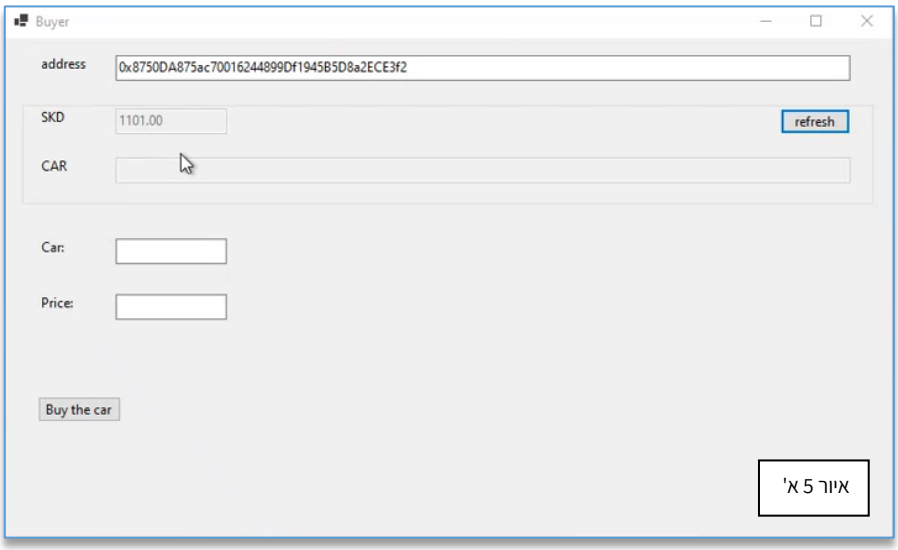
[9] הדוגמה של מכירת רכב היא קלה להבנה ומוכרת לכל קורא; הדוגמה רלוונטית לכל נכס שניתן לייצג אותו באופן דיגיטלי, החל משטר בעלות על נדל"ן וכלה בכרטיס להצגה או לסרט.

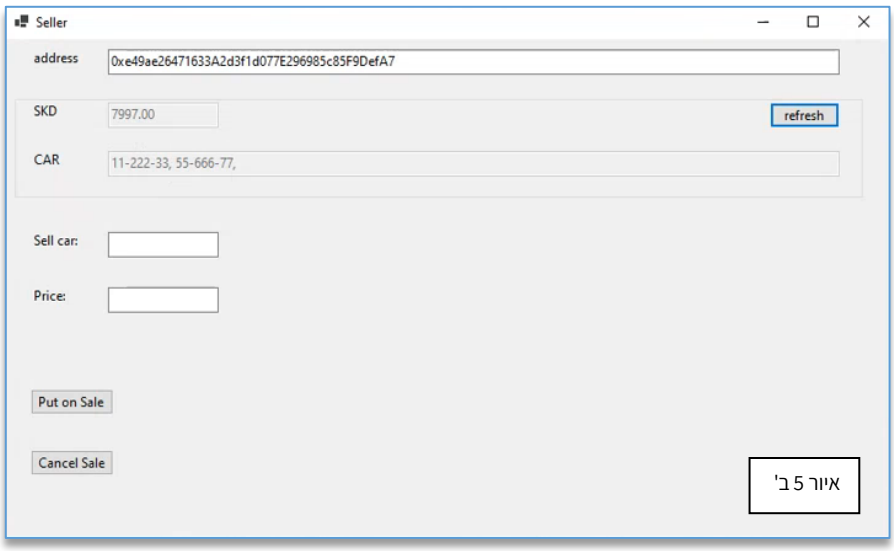
ישלים את חלקו בעסקה. בניסוי מומש תהליך בו העברת הבעלות על הרכב מתבצעת בו זמנית עם העברת התשלום. לשם-כך, הונפק Non Fungible Token (NFT) בסטנדרט ERC 721, שמייצג את הרכב הנמכר, ונכתב חוזה חכם שמפעיל שלוש פעולות בסיסיות:

1. הצעת הרכב למכירה: המוכר, הבעלים של ה-NFT שמייצג את הבעלות על הרכב, מציע את הרכב למכירה תמורת סכום כלשהו. ה-NFT עובר מהארנק של המוכר אל הארנק של החוזה החכם.
2. קניית הרכב: הקונה, שמחזיק שקלים דיגיטליים, מסכים לקניה של הרכב בסכום בו הציע המוכר.
3. ביטול: המוכר מבטל את המכירה במקרה בו התנאים לקיום העסקה לא התקיימו (למשל, הקונה הציע סכום נמוך מזה שהמוכר דרש), וה-NFT שמייצג את הבעלות על הרכב יוצא מהחזה החכם והמצב חוזר לקדמותו.

במידה והקונה הכניס לחוזה החכם את הסכום שהמוכר דרש, העסקה תתבצע- השקלים הדיגיטליים יעברו מהחוזה החכם אל המוכר, וה-NFT שמייצג את הבעלות על הרכב יעבור מחוזה החכם אל הקונה. בניסוי נכתבו שתי אפליקציות פשוטות לאינטראקציה עם החוזה החכם – אחת עבור המוכר ואחת עבור הקונה . איור 5 מציג את תמונת המצב שרואים הקונה (איור 5א) והמוכר (איור 5ב) לפני ביצוע העסקה. בארנק של הקונה יש 1101 שקלים דיגיטליים, ובארנק של המוכר יש 7997 שקלים דיגיטליים, ובנוסף בבעלותו שני כלי רכב, שמיוצגים על ידי מספר הרישוי שלהם.

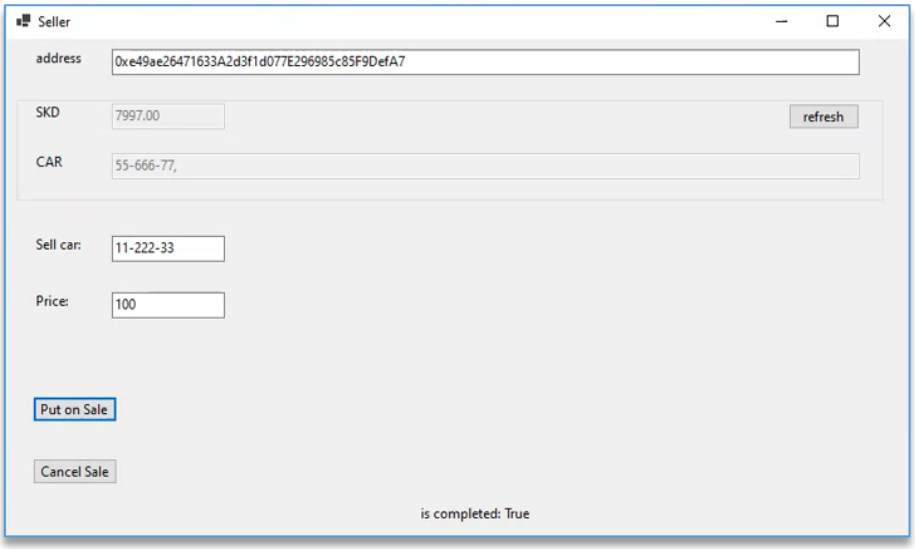
איור 5: תמונת המצב לפני ביצוע עסקת DvP





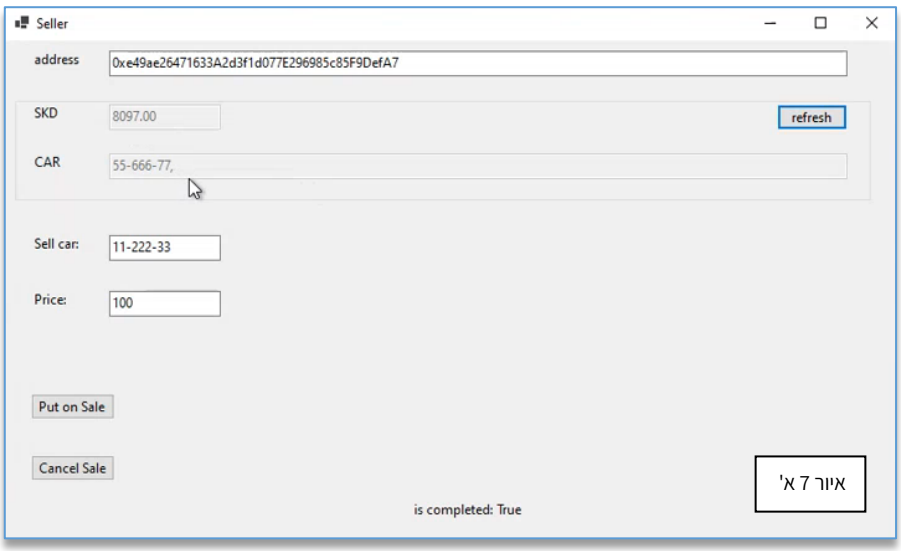
המוכר הציע את אחת המכוניות למכירה תמורת 100 שקלים. באיור 6 ניתן לראות שה-NFT שמייצג את המכונית נגרע זמנית מיתרת הנכסים הדיגיטליים של המוכר ועבר לחוזה החכם.

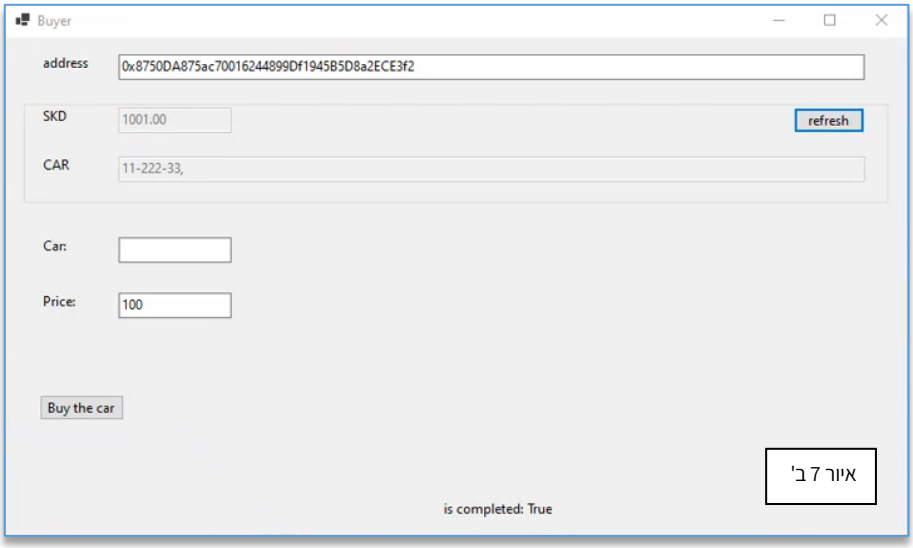
איור 6: הבעלות על הנכס הדיגיטלי מועמדת למכירה באמצעות חוזה חכם



לאחר שהקונה הציע את הסכום הנדרש על יד המוכר אל תוך החוזה החכם, העסקה מתבצעת באופן מיידי. באיור 7א ניתן לראות שיתרת השקלים הדיגיטליים של המוכר עלתה ב-100 שקלים, והרכב נגרע מבעלותו, בעוד יתרת השקלים הדיגיטליים של הקונה (איור 7ב) ירדה ב-100 שקלים, והבעלות על הרכב מיוצגת כעת בארנק שלו.

איור 7: תמונת המצב בתום ביצוע עסקת DvP





איור 7 ב'

ככל שהחוזה החכם נכתב על ידי גורם אמין ומתפקד כיאות, אף צד לא נחשף לסיכון בפרק הזמן שבין העברת הבעלות לבין ביצוע התשלום, זאת משום ששתי הפעולות תלויות זו בזו, ואם האחת אינה מתבצעת, גם השנייה מתבטלת. שאלה חשובה בהקשר זה הנה מיהו הגורם שבונה את החוזה החכם. בניסוי, החוזה למעשה נכתב על ידי ה-administrator של הרשת - בנק ישראל. במערכת השקל הדיגיטלי, לא סביר שבנק ישראל יכתוב אפליקציות לפעולות תשלום ספציפיות. מנגד, קשה להניח גם שיתאפשר לכל גורם לכתוב חוזה חכם על גבי הבלוקצ'יין עצמו, משום שהדבר עשוי להוות סיכון משמעותי למערכת כולה כתוצאה מבאגים בכתיבת הקוד של החוזה החכם, אם הקוד ייכתב בצורה לא יעילה שיגרום עומסים על המערכת כולה, או אם גורם עוין יכתוב חוזה חכם לא אמין, שיביא לאובדן כספים של הלקוחות. פתרון אפשרי הוא שספקי שירותי התשלום יהיו מורשים לכתוב חוזים חכמים. אם כך, עולה השאלה באיזו מידה יידרש פיקוח על סוג החוזים, האמינות של הקוד של החוזה, וכו'[10].

[10] חוקרים בבנק המרכזי של קנדה דנו בתועלות והסיכונים לגבי אופן השימוש בחוזים חכמים במערכת CBDC (Usher et.al, 2021). הבנק המרכזי של אנגליה ניתח את האפשרויות השונות לגבי אופן היישום של חוזים חכמים וכסף מתוכנת ב-CBDC: בליבת הרשת, כמודול נפרד, או כפונקציה שתסופק על ידי ספקי שירותי התשלום (Bank of England, 2020).

5. פרטיות מוגבלת בתשלומים דיגיטליים

5.1 רקע

במערך התשלומים הקיים היום, ישנם שני מצבים דיכוטומיים בכל הנוגע לשמירה על הפרטיות בעת ביצוע עסקת תשלום. המזומן הוא אנונימי לחלוטין; התשלום במזומן אינו נושא עמו כל מידע לגבי זהות המשלם, גובה התשלום, מועד ומיקום ביצוע פעולת התשלום, או זהות המקבל. מנגד, בעת ביצוע פעולת תשלום בכל אמצעי התשלום הדיגיטליים – כרטיס חיוב, העברה בנקאית, אפליקציית תשלום, וכדומה, הגופים הפיננסיים שמתפעלים את אמצעי התשלום מחזיקים במידע מלא אודות כל הפרטים הללו. לשני ההיבטים יש יתרונות וחסרונות: לאזרח יש זכות בסיסית לפרטיות, וככל שהתשלום והעסקה בגינה הוא בוצע הם חוקיים, אין סיבה לפגוע בזכות זו. עם זאת, לאנונימיות המוחלטת הגלומה בתשלום במזומן יש השלכות מדיניות רחבות היקף, משום שהיא מאפשרת התחמקות מתשלום מס, הלבנת הון ומימון טרור. למידע שהגופים הפיננסים מחזיקים יש ערך מבחינת הצרכן – המידע הזה מאפשר לגופים הפיננסיים להציע הצעות ערך שונות לצרכן, להעריך את יכולתו לעמוד בהחזרי אשראי ולהציע אשראי בהתאם, וכדומה. מנגד, המידע עלול להיות מנוצל גם לרעת הצרכן. כך או כך, בפני הצרכן עומדות כאמור שתי אפשרויות דיכוטומיות, ובפרט, היכולת לשלם תוך שמירה על פרטיות מתקיימת רק בעת תשלום פיזי; תשלומים מרחוק, שהולכים ונעשים יותר ויותר נפוצים ככל שהכלכלה הופכת להיות יותר דיגיטלית, יכולים להתבצע רק באמצעי תשלום המופעלים על ידי גופים פיננסיים, שאוצרים כאמור את המידע הגלום בפעולת התשלום.

שמירת האפשרות של הציבור לעשות שימוש באמצעי תשלום דיגיטלי תוך שמירה על רמה מסוימת של פרטיות הנה אחת המוטיבציות שזוהו על ידי ועדת ההיגוי להנפקה אפשרית של שקל דיגיטלי, וגם בעולם מתקיים שיח נרחב אודות הפוטנציאל של CBDC לאפשר תשלומים במידה מסוימת של פרטיות. למשל, בשימוע הציבורי שערך הבנק המרכזי האירופאי לגבי הנפקה אפשרית של אירו דיגיטלי, עלה שהפרטיות היא המאפיין החשוב ביותר של האירו הדיגיטלי בעיני אלו שהשיבו לשימוע (ECB, 2021).

בשלב השני של הניסוי הטכנולוגי שערך בנק ישראל, נבחן מודל שפורסם לאחרונה על ידי חוקרים מחברת VMware המאפשר תשלום בפרטיות בשקל דיגיטלי באופן מוגבל. הרעיון בבסיס המודל הוא שבכל ארנק ניתן להחזיק שקלים דיגיטליים "רגילים", שהעברתם נרשמת ב Ledger - כפי

שתואר באיור 4, וגם שקלים דיגיטליים "פרטיים", שפרטי ההעברה שלהם אינה נרשמת בגלוי, ושני הצדדים לפעולת התשלום נהנים מפרטיות מוחלטת כמו בעת תשלום במזומן. קובע המדיניות יכול להגדיר "תקציב" תקופתי לתשלום בשקלים פרטיים - למשל, ניתן לקבוע שמכל ארנק ניתן לשלם עד 1000 שקלים בחודש באופן פרטי, ומעבר לכך כל פעולת תשלום תירשם ב- Ledger.

5.2 תיאור המודל

לצורך השלב השני של הניסוי הוקמה תשתית VMware Blockchain בענן של AWS , התומכת בטכנולוגיות הוכחה באפס ידיעה (Zero Knowledge Proof) עבור פרטיות מוגבלת. גם כאן המערכת נבנתה במודל של two-tier , עם מערכת הסכמה ביזנטית המבוססת על VMware Blockchain ומנוע תשלומים VMware Decentrlized eCash Infrastructure. הוקמו 4 שרתים (Nodes) שמנהלים את הבלוקצ'יין של הבנק המרכזי באופן מבוזר, וגם שלושה ספקי שירותי תשלום (Payment Service Providers) שמתקשרים ישירות עם הבלוקצ'יין של הבנק המרכזי, ומתווכים בין הארנקים של המשתמשים לבין הבלוקצ׳יין של הבנק. הארנקים הדיגיטליים שספקי שירותי התשלום מספקים ללקוחות הקצה מכילים שקלים דיגיטליים "רגילים" , שקלים דיגיטליים "פרטיים", ותקציב פרטיות.

מנגנון אישור העסקאות (מנגנון הקונצנזוס) בניסוי הוא מנגנון של Permissioned Byzantine Agreement[11], שמאפשר לרשת להתמודד עם התנהגות ״ביזנטית״ של אחד השרתים - נפילה של השרת (חשמל, דיסק תקול, ושאר מיני תקלות רגילות), או השתלטות עוינת על השרת שכתוצאה ממנה השרת מנסה לכתוב לבלוקצ׳יין מידע שגוי. באופן כללי, מספר הצמתים n צריך להתאים לנוסחה: n=3f+1, כאשר f הוא מספר הצמתים שהמערכת יכולה לספוג נפילה שלהם (או התנהגות ביזנטית שלהם). לדוגמה, מערכת בלוקצ׳יין עם 10 צמתים יכולה להתגונן מפני התקפה של אויב על 3 צמתים. המערכת מבטיחה Safety, Liveness, ו-Security כל עוד האויב משתלט על לא יותר מ- f צמתים. מנגנון הפרטיות המוגבלת בניסוי מבוסס על הרחבה של טכנולוגית eCash [12] תוך שימוש

[11] Gueta, et al. 2019
[12] Chaum, 1983

בכלים של הוכחות האפס ידיעה בכדי לוודא את ההגבלה על הפרטיות, באופן המשמר פרטיות מלאה לתשלומים שהם בתוך תקציב הפרטיות התקופתי[13].

בניסוי התקיימה הדמיה של עשרה לקוחות קצה. לאחר הקמת המערכת, בנק ישראל "הנפיק" שקלים דיגיטליים רגילים, שקלים דיגיטליים פרטיים, ותקציב פרטיות. על מנת לבחון את המערכת, נבדקו הפעולות הבאות:

1. תשלומים משמרי פרטיות בעזרת שקלים דיגיטליים פרטיים מתוך תקציב הפרטיות, המשמרים פרטיות מלאה ואינם נרשמים באופן גלוי על הבלוקצ'יין.
2. תשלומים בעזרת שקלים דיגיטליים רגילים הנרשמים באופן גלוי על הבלוקצ'יין.
3. המרה משקלים דיגיטליים רגילים לשקלים דיגיטליים פרטיים, ולהיפך (פעולה כזו אינה משנה את גודל תקציב הפרטיות; היא מאפשרת, למשל, להמיר שקלים פרטיים לשקלים רגילים אם תקציב הפרטיות התקופתי נגמר).
4. עמידות המערכת כאשר שרת אחד של הבלוקצ'יין נופל ומאבד את כל המידע; המערכת ממשיכה לפעול כרגיל, וכאשר השרת חוזר הוא מסתנכרן עם יתר חלקי המערכת וחוזר לפעול.
5. עמידות המערכת כאשר ספק שירותי תשלום נופל ומאבד את כל המידע. כאשר ספק שירותי תשלום חלופי עולה הוא משחזר את כל הארנקים (כולל החלוקה בין שקלים דיגיטלית פרטיים ורגילים ותקציב הפרטיות התקופתי).

[13] Tomescu, et al. 2022

סיכום

הניסוי המתואר במסמך זה מהווה התנסות טכנולוגית ראשונה של צוותי העבודה של בנק ישראל במסגרת פרוייקט השקל הדיגיטלי. בנקים מרכזיים רבים בוחנים שימוש בטכנולוגית מבוזרות כפלטפורמה אפשרית להנפקה של CBDC, על אף העובדה שמטבע דיגיטלי של בנק מרכזי, מעצם טבעו, יונפק על ידי גורם מרכזי. מאפיינים מסויימים של טכנולוגיות מבוזרות בכלל וטכנולוגיית בלוקצ'יין בפרט עשויים להוות יתרון בהנפקה של CBDC, וחלקם נבחנו במסגרת הניסוי שבנק ישראל ערך. אין להסיק מהבחירה בטכנולוגיה זו לצורך הניסוי, שזו הטכנולוגיה המתאימה להנפקה של שקל דיגיטלי בעתיד, ככל שיוחלט להנפיק כזה. הניסוי נגע גם בשתיים מהמוטיבציות שזיהתה ועדת ההיגוי להנפקה אפשרית של שקל דיגיטלי - ליצור תשתית חדשנית שתבטיח את התאמת מערך התשלומים לצרכים של הכלכלה הדיגיטלית העתידית, ומתן האפשרות לציבור לעשות שימוש באמצעי תשלום דיגיטלי תוך שמירה על רמה מסוימת של פרטיות.

בשלב א' של הניסוי, הוקמה תשתית נסיונית על גבי בלוקצ'יין של את'ריום. השימוש בטכנולוגיה זו על גבי פלטפורמת ענן והיישום של Token סטנדרטי איפשרו התנסות פשוטה יחסית בטכנולוגיה, ללא צורך בהקמת שרתים יעודיים ובכתיבת קוד החל מרמה בסיסית. כמו כן, הטכנולוגיה אפשרה בחינה של היכולת לעשות שימוש בחוזים חכמים ולייצר תשתית לעסקאות DvP, כאשר בנוסף ל-Token שמייצג את הכסף, Non Fungible Token מייצג בעלות על נכס המחליף ידיים בתמורה לכסף.

על אף שהשימוש בטכנולוגיה הסטנדרטית איפשר הנגשה של המטבע הדיגיטלי ל"לקוחות" באמצעות ארנק סטנדרטי, בניסוי בוצעה הדמיה של ארנק יעודי שמפותח על ידי המתווכים במודל של two-tier, תוך מתן פיתרון בסביבת ניסוי לביצוע תהליך KYC בהסתמך על מאגר זהויות מרכזי. הדמיה זו חידדה את הצורך ביצירת תשתית נוחה ויעילה לביצוע הזדהות על מנת שהמתווכים יוכלו להנגיש את שירותי השקל הדיגיטלי ללקוחות תוך עמידה בדרישות החוק.

בשלב ב' של הניסוי נבחנה היכולת לאפשר תשלום במטבע דיגיטלי תוך שמירה על פרטיות מוגבלת, בהתאם לכללים שיגדירו קובעי המדיניות. הניסיון לייצר פתרון לסוגיה זו בסביבת הניסוי הראה כי בארכיקטורה מבוזרת קיים קושי להשתמש במפתחות הצפנה, ולכן נדרש לעבוד עם מנגנונים אחרים שקשורים לטכנולוגיות של "הוכחה אפס ידיעה". בחינה של פיתוח חדשני של טכנולוגיה זו הראתה שניתן ליישם מדיניות על פיה לכל לקוח ברשת השקל הדיגיטלי יוקצה תקציב תקופתי של שקלים

דיגיטליים "פרטיים", איתם יוכל הלקוח לשלם מבלי שיישמר כל תיעוד של פעולם התשלום. הניסוי והדיונים שנערכו בעקבותיו חידדו את העובדה שעל אף הוכחת ההיתכנות הטכנולוגית, שאלות מדיניות רבות מצריכות עדיין בחינה ודיון. למשל, מהו תקציב הפרטיות ה"נכון", והאם לכל סוג של ארנק (פרטי, עסקי וכדומה) נכון להקציב את אותו סכום? האם עלולים להתפתח תמריצים כלכליים לשימוש לא נאות בשקלים ה"פרטיים"? ועוד.

התשתית שהוקמה לצורך הניסוי תוכל לשמש את בנק ישראל לבחינה של ישומים וסוגיות מדיניות נוספים בעתיד, ככל שהדבר יידרש. בנק ישראל ימשיך לבחון סוגיות טכנולוגיות שונות הקשורות בהנפקה אפשרית של שקל דיגיטלי.

ביבליוגרפיה

1. בנק ישראל, 2021: "שקל דיגיטלי של בנק ישראל – מוטיבציות אפשריות, טיוטת מודל וסוגיות לבחינה".
2. Bank of England, (2020): Central Bank Digital Currency: Opportunities, Challenges and Design
3. Bank of Japan, (2022): Central Bank Digital Currency - Results and Findings from "Proof of Concept Phase 1"
4. Bank of Thailand, (2021): Central Bank digital Currency: The Future of Payments for Corporates
5. Chaum, D. (1983): eCash, Blind Signatures for Untraceable Payments
6. ECB, (2021): Results of the Public Consultation on the Digital Euro
7. Federal Reserve Bank of Boston, (2022): Project Hamilton Phase 1
8. Gueta, G, et al. (2019): SBFT: a Scalable and Decentralized Trust Infrastructure
9. Sveriges Riksbank, (2022): E-krona pilot, phase 2
10. Tomescu, A, et al. (2022): UTT: Decentralized Ecash with Accountable Privacy
11. Usher, A., E. Reshidi, F. Rivadenyera, and S. Hendry. (2021): The positive case for a CBDC. Bank of Canada Staff Discussion Paper, 2021-11.