ארכיטקטורה לוגית
למערכת השקל הדיגיטלי

בנק ישראל
מרץ 2024

ועדת ההיגוי של בנק ישראל
להנפקה אפשרית
של שקל דיגיטלי

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

מרץ 2024

כותבי המסמך:

אמיר משה – פרויקט השקל הדיגיטלי
יואב סופר - פרויקט השקל הדיגיטלי

תודתנו לעמיתים מחטיבת טכנולוגיית המידע בבנק ישראל, ממחלקת מערכות תשלומים וסליקה בבנק ישראל, מצוות העבודה בפרויקט השקל הדיגיטלי ולוועדת ההיגוי של הפרויקט על הליך החשיבה המשותף, איתגור הממצאים והסיוע בכתיבה ובעריכה של המסמך.

תוכן עניינים

04
רשימת מונחים וראשי תיבות

06
רקע ועיקרי המסקנות

07
הנחות ומתודולוגיה

08
סוגי המשתתפים במערכת

11
מסע משתמש הקצה והפונקציונאליות הנדרשת ממערכת השקל הדיגיטלי

13
מודל ההפצה

20
שכבת ה-"Back-end"

28
סוגיות נוספות

31
מסקנות והמלצות

רשימת מונחים וראשי תיבות

משתמשי קצה – אנשים פרטיים וארגונים (בתי עסק, עמותות משרדי ממשלה וכד') אשר יוכלו להחזיק יתרה ולבצע ביניהם פעולות תשלום בשקל הדיגיטלי.

משתתף - ארגון שממלא תפקיד במערכת השקל הדיגיטלי, ומחויב לכללי המערכת. בשונה מהגדרת משתתף על פי חוק מערכות תשלומים, משתתף במערכת השקל הדיגיטלי לא בהכרח יכול לתת הוראות תשלום. במסמך זה מוגדרים ארבעה סוגי משתתפים: בנק ישראל, ספק שירותי תשלום בשקל הדיגיטלי (DS-PSP), מנהל חשבון עו"ש (FI), ונותן שירותים נוספים (ASP).

מוסד המנהל חשבון עו"ש (Funding Institution, FI) - גופים פיננסיים המנהלים חשבונות עו"ש לציבור מחוץ למערכת השקל הדיגיטלי, ויאפשרו ללקוחותיהם להמיר כסף מהיתרה בחשבון אצלם לשק"ד (פעולת טעינה, funding) ולהיפך (פעולת פריקה, defunding). למשל - בנקים מסחריים, בנק הדואר, אגודות פיקדון ואשראי, גופים למתן שירותים בנכס פיננסי, וכדומה. חלק מהגופים האלה יתמכו גם בפעולת המרה של מזומן לשק"ד ולהיפך, עבור כלל משתמשי הקצה בשקל הדיגיטלי.

מטבע דיגיטלי קמעונאי של הבנק המרכזי (rCBDC) – מטבע דיגיטלי אשר מונפק על ידי הבנק המרכזי , מהווה התחייבות ישירה שלו ומיועד לשימוש הציבור הרחב ("מזומן דיגיטלי").

מודל דו נדבכי (Two tier) – מודל תפעול למערכת rCBDC ולפיו, גישת משתמשי הקצה אל המערכת תבוסס על התקשרות עם מתווכים אשר יספקו את המעטפת הטכנולוגית והעסקית הנדרשת לצורך חיבור זה.

Back-end – רכיבי המערכת הנדרשים לבנק המרכזי לצורך ביצוע תפקידיו במערכת השקל הדיגיטלי, כולל מאגרי המידע הנדרשים ו/או נגזרים מפעולות אלה. בפרט, ה-back end יכלול את "מנוע" הסליקה – הרכיב שמאפשר העברה של שקלים דיגיטליים במסגרת פעולת תשלום בין שני משתמשי קצה.

ספק שירותי תשלום בשקל הדיגיטלי (בקיצור - ספק תשלום. DS-PSP , Digital Shekel Payment Services (Provider, or PSP – משתתף מרכזי במימוש המודל הדו-נדבכי במערכת השקל הדיגיטלי. משתתף מסוג זה יהיה אחראי לספק את המעטפת הטכנולוגית והעסקית הנדרשת לצורך חיבור משתמשי קצה אל מערכת השקל הדיגיטלי (ביצוע הליך הכר את הלקוח, אספקה ושחזור של אמצעי גישה אל המערכת, שירות לקוחות, ועוד). ללא התקשרות עם ספק תשלום, משתמש קצה לא יוכל לפעול במערכת השקל הדיגיטלי.

נותן שירותים נוספים (ASP, Additional Services Provider) – גוף מסוג זה יוכל לספק שירותים נוספים אופציונאליים למשתמשי הקצה כגון: ניהול תקציב, שירותי אנליזה לבתי עסק, שירותי ניטור הונאות, יישומי תשלום חדשניים, וכד' .

טעינה/פדיון – המרה של כסף דיגיטלי שאינו מייצג התחייבות של הבנק המרכזי (למשל, פיקדון בבנק מסחרי או בגוף המנהל חשבון תשלום עבור הלקוח) לשקל דיגיטלי, או המרה של מזומן לשקל דיגיטלי. התוצאה של פעולת טעינה היא שהיתרה בארנק השקל הדיגיטלי של משתמש הקצה גדלה. פעולת פדיון היא הפעולה ההפוכה לפעולת טעינה.

RTGS (Real Time Gross Settlement) - מערכת לסליקה פרטנית, מיידית וסופית, לעסקאות בין בנקים וגורמים עסקיים כמו מסלקות אחרות, ובין לקוחות. במדינת ישראל מערכת ה- RTGS מכונה זה"ב (**ז**יכויים **ו**ה**ע**ברות **ב**זמן אמת) ומתופעלת על ידי בנק ישראל.

בנקאות פתוחה (Open Banking) – סטנדרטיזציה המאפשרת לגורמי צד ג' לגשת אל מידע פיננסי של לקוח המנהל חשבון אצל גורם אחר, או ליזום פעולות בחשבונו של הלקוח. הגישה של צד ג' מבוצעת על ידי שימוש ב APIs שמוחצנים על ידי הגורם המנהל את החשבון.

טוקן – ייצוג דיגיטלי של ערך בפלטפורמה הניתנת לתכנות. טוקן יכול להיות תוצאה של תהליך "טוקניזציה", כלומר, ייצוג של ערך שכבר קיים בשיטת רישום מסורתית (למשל – ייצוג של ניירות ערך שכבר רשומים למסחר במערכת קיימת), או שניתן להנפיק אותו ישירות לפלטפורמה מסוימת - למשל, טוקן של מטבע דיגיטלי.

Unspent Transaction Output (UTXO) – מודל למימוש סליקה מבוססת טוקנים. במודל זה, כל טרנסאקציה מורכבת מקלט של טוקן או טוקנים אשר משנים סטטוס ל "Spent Tokens" ובהם לא יכול משתמש הקצה לבצע יותר שימוש . במקביל, נוצר פלט של טוקנים בסטטוס של "Unspent Tokens" המונפקים אל הצד המוטב. במידת הצורך, יונפקו "Unspent Tokens" גם חזרה אל הגורם המשלם כעודף.

לדג'ר – ספר רישום או מסד נתונים דיגיטלי שבו כל העסקאות הפיננסיות נרשמות ומסוכמות. הוא משמש כרישום החשבונאי העיקרי של חברה או ישות, ומבטיח שכל הזיכויים והחיובים נרשמים ומאוזנים.

תשלום מותנה – פעולת תשלום אשר השלמתה מבוססת על קיומו של תנאי מסוים - למשל, קבלת חבילה בדואר (DvP) או קבלת תשלום במטבע אחר כנגד (PvP). קיימים מנגנונים טכנולוגיים ועסקיים שונים לניהול הליך עסקה מותנית. ברובם, נדרש לבצע נעילה של יתרה מסוימת בעת קשירת העסקה, ושחרורה אל הגורם המוטב בהתקיים התנאי או הטריגר.

Waterfall / מנגנון המפל – תהליך במסגרתו מתבצעת באופן אוטומטי פריקה של ארנק השקל הדיגיטלי במידה והיתרה בארנק עולה על הסכום המקסימלי המותר להחזקה בארנק (כתוצאה ממגבלת החזקה), או שהיתרה עולה על רף מסוים שמשתמש הקצה הגדיר. ההליך מבטיח פגיעה מינימלית בחוויית המשתמש משום שהוא מאפשר למשתמש לקבל תשלומים לארנק השקל הדיגיטלי גם אם קבלת התשלום מעלה את היתרה אל מעבר למגבלת ההחזקה.

Reverse waterfall / מנגנון המפל ההפוך – תהליך במסגרתו מתבצעת באופן אוטומטי טעינה של ארנק השקל הדיגיטלי אם אין בארנק יתרה מספקת לביצוע פעולה, או אם היתרה בארנק ירדה מתחת לסף מסוים שהגדיר המשתמש. תהליך זה יכול לאפשר ביצוע פעולות תשלום בסכומים גבוהים ממגבלת ההחזקה, ולשפר באופן כללי את חווית המשתמש.

1. רקע ועיקרי המסקנות

בדומה לבנקים מרכזיים רבים בעולם אשר עוסקים בסוגיית העיצוב וההנפקה האפשרית של מטבע דיגיטלי קמעונאי של הבנק המרכזי (rCBDC), הצהיר בנק ישראל (בנק ישראל, 2021) כי המודל הנבחן לתפעול המערכת הפוטנציאלית הינו המודל הדו-נדבכי (Two- tier). במודל זה, הגישה של משתמשי הקצה אל המטבע הדיגיטלי של הבנק המרכזי תבוצע באמצעות גופים מתווכים מהמגזר הפרטי. נייר זה עוסק בבחינת החלופות הארכיטקטוניות למימוש המודל הדו-נדבכי.

נושא המימוש הארכיטקטוני של המודל הדו-נדבכי מקבל לאחרונה משקל משמעותי גם במשימות עבודה של בנקים מרכזיים נוספים הבוחנים הנפקה אפשרית של rCBDC. למשל, הבנק המרכזי האירופאי (ECB 2023) והבנק המרכזי של אנגליה (BIS 2023c) ביצעו ניסויים טכנולוגיים ושיתופי פעולה עם המגזר הפרטי לבחינת הנושא. גם בפרויקט "סלע" אשר הושלם לאחרונה ובו שיתף בנק ישראל פעולה עם מרכז החדשנות של הבנק הבינלאומי לסילוקין (BIS Innovation Hub) ועם הרשות המוניטרית של הונג קונג (HKMA), יושמה ארכיטקטורה מסוימת של המודל הדו-נדבכי בהתבסס על הטכנולוגיה שהוצעה על ידי הספק בפרויקט[1] והדרישות העסקיות שהוצבו על ידי השותפים לפרויקט (BIS 2023a).

בחינת החלופות בנייר נעשתה תוך מתן דגש ופירוט על מספר נושאים מרכזיים: סוגי המשתתפים במערכת; החלוקה הפונקציונאלית בין המשתתפים במסגרת מימוש הפתרון המלא; מודל ההפצה של השקל הדיגיטלי מהבנק המרכזי אל משתמשי הקצה, וחלופות שונות למימוש שכבת ה "back-end", או "מנוע" המערכת אשר יוקם וינוהל על ידי בנק ישראל (או מי מטעמו).

<u>עיקרי ההמלצות:</u>

מסמך זה נכתב כחלק מתהליך האפיון של השקל הדיגיטלי, והחשיבה שנערכה אודות הארכיטקטורה הלוגית המתאימה למערכת זו. בסעיף 8 בנייר מתוארות המסקנות העיקריות לגבי כמה היבטים מרכזיים של ארכיטקטורה לוגית למערכת rCBDC ובפרט למערכת השקל הדיגיטלי: סוגי המשתתפים במערכת – מעבר לספקי התשלום (PSP), הנייר מפרט סוגים שונים של מוסדות המנהלים חשבונות עו"ש ללקוחות אשר ידרשו לאפשר המרה מהחשבון אותו הם מנהלים, או ממזומן, אל השקל דיגיטלי. בנוסף, הנייר מתאר את האפשרות לשילוב סוג נוסף של משתתף במערכת, אשר יעניק שירותי ערך מוסף אופציונאליים; המלצה לשימוש במודל הפצה עקיף במסגרתו יפיץ בנק ישראל שקלים דיגיטליים אל המוסדות המנהלים חשבונות עו"ש, ואלה יתמכו בהפצה אל משתמשי הקצה; עקרונות לניהול שכבת ה back-end תוך הפרדה ברורה בין פעולת הסליקה לניהול המידע; ועקרונות ראשוניים לסוגיית האינטראופראביליות של המערכת עם תשתיות קיימות ועתידיות.

יודגש, כי הנייר כולו, ופרק המסקנות בפרט, נכתבו תוך גישה אגנוסטית ככל הניתן למימוש הארכיטקטורה. בשלב זה של הפרויקט, צוות הפרויקט אינו עוסק בבחירה בין טכנולוגיות שונות (למשל, טכנולוגיות רישום מבוזר או טכנולוגיות בסיסי נתונים מסורתיות). עם זאת, מטבע הדברים, המודעות לקיומן ומידת הישימות של טכנולוגיות כאלה או אחרות משליכות על אופן החשיבה אודות הארכיטקטורה הלוגית.

[1] יישום הטכנולוגיה בפרויקט בוצע על ידי חברת FIS וחברת M10.

2. הנחות ומתודולוגיה

2.1 הנחות מקדימות

תפקידה של הארכיטקטורה הלוגית בשק"ד הינו לתמוך באספקת הפתרון המלא למשתמשי הקצה לביצוע ההליכים והפעולות השונות בשקל הדיגיטלי, תוך התקיימות מספר הנחות והחלטות שהתקבלו בפרויקט עד כה ואשר יש להן השפעה מהותית על מאפייני החלופה הארכיטקטונית הנבחרת:

- הארכיטקטורה תציג מימוש למודל הדו-נדבכי (Two-tier);
- המערכת תתמוך בביצוע תשלומים מיידים וסופיים, 24/7;
- ספקי התשלום לא יפתחו חשיפה פיננסית במסגרת אספקת שירותים בשקל הדיגיטלי[2];
- על מנת להבטיח סביבה תחרותית, משתמש קצה יוכל לפעול באמצעות מספר ספקי תשלום בזמן נתון;
- המערכת תוכל לתמוך בהחלה ובאכיפה של מגבלות, למשל מגבלות על היתרה שיותר למשתמש להחזיק בשקל הדיגיטלי ;
- המערכת תתמוך באפשרות להחלת ריבית על השקל הדיגיטלי על ידי הבנק המרכזי;
- תתאפשר אינטראופראביליות עם פתרון שיאפשר שימוש בשקל הדיגיטלי באופן לא מקוון (אופליין);
- הארכיטקטורה תתמוך בכל החלטות העיצוב שהתקבלו עד כה בפרויקט. בפרט, בתחום הפרטיות, הארכיטקטורה תאפשר לבנק המרכזי כמנהל המערכת להגדיר מהם סוגי המידע הנדרשים לצורך התפעול, הבקרה והניטור של המערכת, אולם, לבנק המרכזי לא תהיה גישה למידע פרטני מזוהה אודות היתרות והטרנסאקציות של משתמשי הקצה, בנוסף, הארכיטקטורה תאפשר רמות שונות של פרטיות מול מאגר המידע המרכזי בהתאם לסוג המשתמש (פרטי, עסקי וכדומה), סוג הטרנסאקציה, ועוד.

2.2 מתודולוגיית העבודה

בליבת הנייר ניצבת שאלת החלוקה הפונקציונאלית הרצויה בין המשתתפים השונים כך שתתמוך במימוש הפתרון המלא הנדרש למשתמשי הקצה במערכת. חלוקה זו תקבע למעשה את אופן תמיכת המשתתפים בביצוע פעולות מסוגים שונים על ידי המשתמשים ועליה כמובן לעמוד בהנחות השונות שצוינו לעיל ולחתור גם להשגת היעדים העסקיים הרצויים מהמערכת המתגבשת. המתודולוגיה לאיתור הסוגיות השונות אשר הינן בעלות השפעה מהותית על החלוקה הפונקציונלית והארכיטקטורה הלוגית כללה מספר שלבים (כפי שמתוארים באיור 1).

[2] להרחבה בנושא ראו סעיף 3.2 בדו"ח פרויקט סלע (BIS 2023 a).

איור 1 – השלבים השונים במתודולוגיית העבודה

הסעיפים הבאים בנייר עוסקים בהרחבה בכל אחד מהשלבים המוצגים במתודולוגית העבודה אשר תוארה לעיל.

3. סוגי המשתתפים במערכת

מערכת השקל הדיגיטלי תתפקד כמערכת קמעונאית לביצוע תשלומים מידיים בין משתמשי הקצה (אנשים פרטיים, בתי עסק, ארגונים שונים ומשרדי ממשלה). בהתאם למודל הדו–נדבכי, באספקת הפתרון המלא למשתמשי הקצה יהיו מעורבים בנק ישראל והמתווכים. בשכבת המתווכים ניתן להבחין בין שני סוגי משתתפים מהם נדרשת פונקציונאליות שונה במימוש הפתרון: ספקי התשלום (PSPs) ומוסדות המנהלים חשבונות עו"ש (FIs). כמו כן, ייתכנו ספקי שירותים מתקדמים נוספים (ASPs) אשר משתמשי הקצה אינם חייבים להתקשר איתם לצורך הפעילות בשקל הדיגיטלי, אך הם יוכלו לאפשר למשתמשי הקצה ליהנות משירותים נוספים ככל שיחפצו בכך - שירותי מידע, תשלומים מותנים, או יישומי תשלום חדשניים אחרים.

הגדרת תפקידי המשתתפים השונים:

בנק ישראל – הגורם הבלעדי בעל הסמכות להנפקה/שריפה של שקל דיגיטלי, ואשר אמון על ניהול המערכת והפעלתה (באופן ישיר או על ידי מי מטעמו).

מוסדות המנהלים חשבונות עו"ש (FIs) - גופים פיננסיים המנהלים עבור הציבור חשבונות עו"ש בכסף שאינו השקל הדיגיטלי (בנקים מסחריים, בנק הדואר, אגודות פיקדון ואשראי, גופים למתן שירותים בנכס פיננסי, וכדומה) ויצטרכו לאפשר פעולת המרה

של משתמשי הקצה מהחשבונות אותם הם מנהלים, או ממזומן, אל השקל הדיגיטלי ולהיפך. כאמור, ייתכנו סוגים שונים של FIs כפי שיתוארו בסעיף 5 בנייר ובטבלה הבאה[3].

טבלה 1 – קונפיגורציות שונות לפעילות FIs

מחזיק שק"ד לטובת פעולת ההמרה		משתמש בשק"ד של גורם אחר[4]
מחובר ישירות ל RTGS	מיוצג על ידי משתתף אחר ב RTGS	
A	B	C

הבנקים המסחריים שאצלם מנוהלים מרבית חשבונות העו"ש של הציבור בוודאי יצטרכו לפעול כ-FIs נמנים על קבוצה A בטבלה לעיל. עם זאת, הארכיטקטורה המתגבשת תצטרך לאפשר גמישות וקיום גם של המודלים הנוספים בטבלה לעיל (למשל, גוף שאינו בנק המיוצג על ידי בנק מסחרי במערכת זה"ב).

<u>ספקי התשלום (PSPs)</u> – גופים אלה יהיו האחראים ליצירת הגישה הטכנולוגית של משתמשי הקצה אל מערכת השק"ד, ביצוע הליכי KYC ללקוחותיהם, אספקה ושחזור של אמצעי הגישה למערכת, שירות לקוחות, ועוד. ספקי התשלום לא יפתחו חשיפה פיננסית מאזנית בשום שלב במסגרת אספקת שירותי השקל הדיגיטלי וזאת, בהתאם להנחת העבודה בפרויקט השקל הדיגיטלי ואישוש ההיתכנות הטכנולוגית, העסקית והמשפטית של הנחה זו בפרויקט "סלע".

ייתכנו גם ספקי תשלום אשר אינם מחוברים אל המערכת באופן ישיר ומספקים שירותי שק"ד על בסיס חיבוריות אל ספק תשלום המחובר אל המערכת (משתתפים עקיפים).

<u>ספקי שירותים מתקדמים נוספים (ASPs)</u>[5] – גופים אלה יוכלו לספק שירותים נוספים **אופציונאליים** למשתמשי הקצה, כגון: ניהול תקציב, שירותי אנליזה לבתי עסק, שירותי ניטור הונאות, וכדומה. בנוסף, הם יוכלו גם לקחת <u>חלק</u> באספת שירותי תשלומים מותנים מתקדמים. למשל, הם יוכלו לשמש כצד שלישי האחראי על שליחת ה"טריגר" לנעילה או לשחרור של כספים בעסקת תשלום מותנה.

גופים אלה לא יוכלו לספק שירותי תשלום המבוססים על פנייה ישירה לבנק המרכזי (כפי ש PSPs יוכלו). עם זאת, לא מן הנמנע ש-ASPs יוכלו לספק שירותי ייזום תשלומים בשקל הדיגיטלי, דרך ה-PSP שאתו הלקוח בחר להתקשר. במסגרת הגדרת תפקידו של משתתף זה עולה השאלה האם נכון לאפשר לו גישה טכנולוגית ישירה אל מערכת הליבה של השקל הדיגיטלי בבנק המרכזי, או שמא להגביל את גישתו כך שהיא תתבצע אך ורק דרך ה-PSP בגישה דומה לזו המתפתחת ב- Open banking API (להרחבה בנושא התקשורת בין משתתפי המערכת ראו תיבה 1). כמו כן, קיימת שאלה גם לגבי ההשפעה של מעורבות משתתף זה על מבנה השוק (האם יהיו מספיק PSPs במידה וניתן יהיה לפעול כ- ASP? האם קיים מודל עסקי לסוג משתתף זה? ועוד). חלק מהסוגיות נוגעות בהחלטות מדיניות ורגולציה, ולא במימוש ארכיטקטוני.

הניתוח הראשוני שנערך במסגרת נייר זה העלה כי בהתחשב בכך שגישתו של ASP אל מערכת הליבה מוגבלת לביצוע פעולות מסוימות בלבד, ייתכן מצב בו היתרונות והיעילות באפשור הגישה הישירה אל הבנק המרכזי תעלינה על ההיבט השלילי של נטל הדרישות הרגולטוריות והטכנולוגיות לצורך חיבור זה. ולכן, בשלב זה בחרנו להניח קיומו של משתתף זה כחלק מהארכיטקטורה ועם חיבור ישיר למערכת הליבה של השקל הדיגיטלי ובכך להבטיח את הגמישות הארכיטקטונית. עם זאת, הערכה זו תצטרך

[3] יצוין כי מדובר בקונפיגורציות ארכיטקטוניות תיאורטיות והיתכנותן העסקית והרגולטורית תצטרך כמובן להיבחן.
[4] למשל, משתמש בשק"ד של FI אחר או על בסיס מודלים מתקדמים המתבססים למשל על יתרות משתמשי קצה במנגנון של Liquidity pools
[5] ה- Bank of England מכנה משתתף מסוג זה בשם ESIP (External Services Interface Provider). להרחבה ראו Bank of England (2023).

להיבחן שוב ולעמוד במבחן המציאות בהמשך לאור השאלות העסקיות והרגולטוריות שהוזכרו. בפרט, יהיה צריך להבין האם ניתן להשיג את אבן היסוד בקיומו של "שחקן" מסוג זה - נטל רגולטורי וטכנולוגי מופחת מזה הקיים ל- PSP.

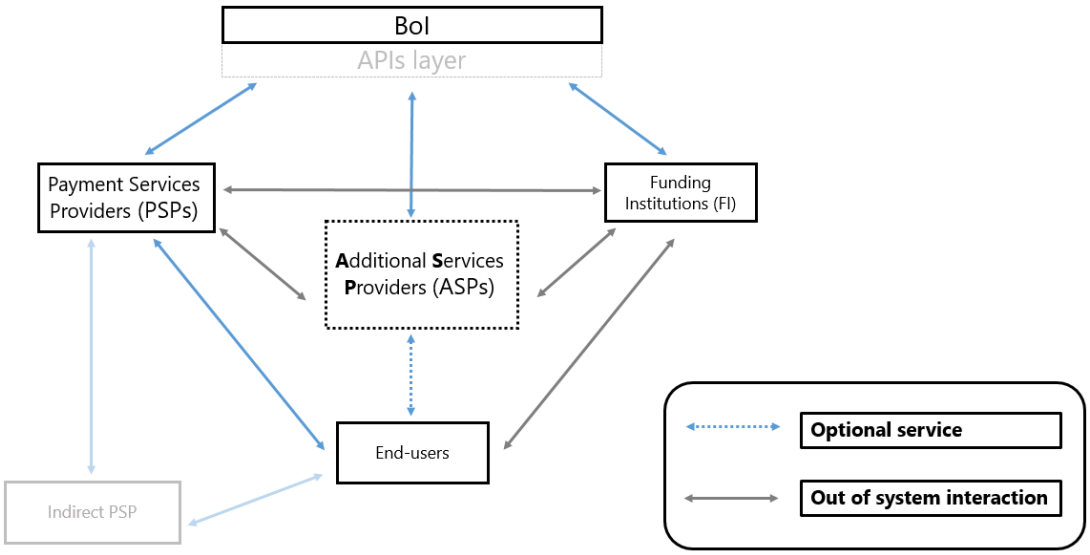
תיבה 1- התקשורת בין המשתתפים במערכת השקל הדיגיטלי

מערכת השקל הדיגיטלי תידרש לתמוך בפעילותם של גופים רבים מסוגים שונים, ולצורך תפקודה התקין, נדרשת תקשורת משני סוגים:

- **תקשורת בין משתתפי המערכת מהמגזר הפרטי לבין הבנק המרכזי** – מימוש אפשרי לתקשורת זו יכול להיות על ידי גישה ישירה של המשתתפים אל שכבת ה APIs אשר מוחצנת על ידי הבנק המרכזי מפלטפורמת השקל הדיגיטלי. (ראו למשל – BIS (2023 c). סביר להניח כי ל-FIs ול-PSPs תינתן אפשרות לתקשר באופן ישיר עם פלטפורמת השקל הדיגיטלי. למשל, לטובת שידור הוראה לביצוע תשלום עבור משתמש קצה או לצורך תמיכה בפעולת טעינה/פדיון. אגב, לא מן הנמנע שתתאפשר פעילות של גופים מסוגים אלה גם ללא חיבור ישיר אל המערכת בקונפיגורציה של משתתפים עקיפים, אך זו כמובן תלויה בקיומם של משתתפים המחוברים ישירות לפלטפורמה.
בשונה מ- FIs ו- PSPs, התקשורת הישירה של משתתף מסוג ASP מול הבנק המרכזי אינה הכרחית וככל שיוחלט בסופו של דבר שלא לאפשר למשתתף זה גישה ישירה, תהא פעילותו תלויה בתשתיות הקיימות במשק (למשל, התשתית הקיימת והמתפתחת לבנקאות הפתוחה).
- **תקשורת בין המשתתפים** - תידרש גם תקשורת בין המשתתפים במערכת לצורך תמיכה בפעולות מקדימות ו/או משלימות לפעולות המבוצעות על גבי פלטפורמת השקל הדיגיטלי. למשל, כאשר משתמש קצה יבקש לבצע פעולת טעינה מחשבונו אצל ה-FI אל ארנק השק"ד המנוהל על ידי PSP, ה- PSP יצטרך לבדוק האם ללקוח יש יתרה מספקת אצל ה-FI לצורך ביצוע הפעולה, כמו גם במקרה של פעולה המביאה להחזקה עודפת ולצורך השלמתה נדרשת הפעלה של מנגנון "Waterfall".
ניתן להניח שני מודלים מרכזיים ליצירת התקשורת בין המשתתפים:
  - שימוש בפלטפורמת ה CBDC כגורם המקשר בין המשתתפים
  - שימוש בתשתית הקיימת. למשל, Open banking API לתקשורת בין המשתתפים לצורך ביצוע ההליכים המקדימים והמשלימים לפעולה הרלוונטית.

משיקולים של ביצועי המערכת ושל אבטחת מידע יש עדיפות לכך שהתקשורת בין משתתפי המערכת לא תהיה תלויה בפלטפורמת השקל הדיגיטלי. כך, מערכת הפלטפורמה תוכל לעבוד במצב "Stateless" ולטפל בבקשת המשתתף לאחר שהליכי התקשורת המקדימים בין המשתתפים בוצעו, ותוך צמצום התלות בהליכים משלימים.

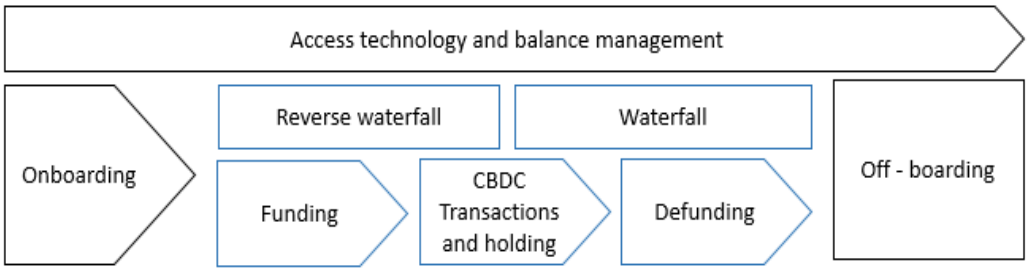
איור 2 - המשתתפים באספקת הפתרון למשתמש הקצה במערכת השקל הדיגיטלי .



4. מסע משתמש הקצה והפונקציונאליות הנדרשת ממערכת השקל הדיגיטלי

במסע משתמש הקצה בשקל הדיגיטלי ניתן להבחין בין שלבי הליבה, קרי, פעולות השימוש השוטף בשקל הדיגיטלי כאמצעי תשלום (מופיעות בכחול באיור להלן) לבין השלבים התומכים אשר נדרשים בכדי לאפשר את קיומן של פעולות הליבה, ואת שלמותו של מסע המשתמש (מופיעים בשחור באיור להלן).

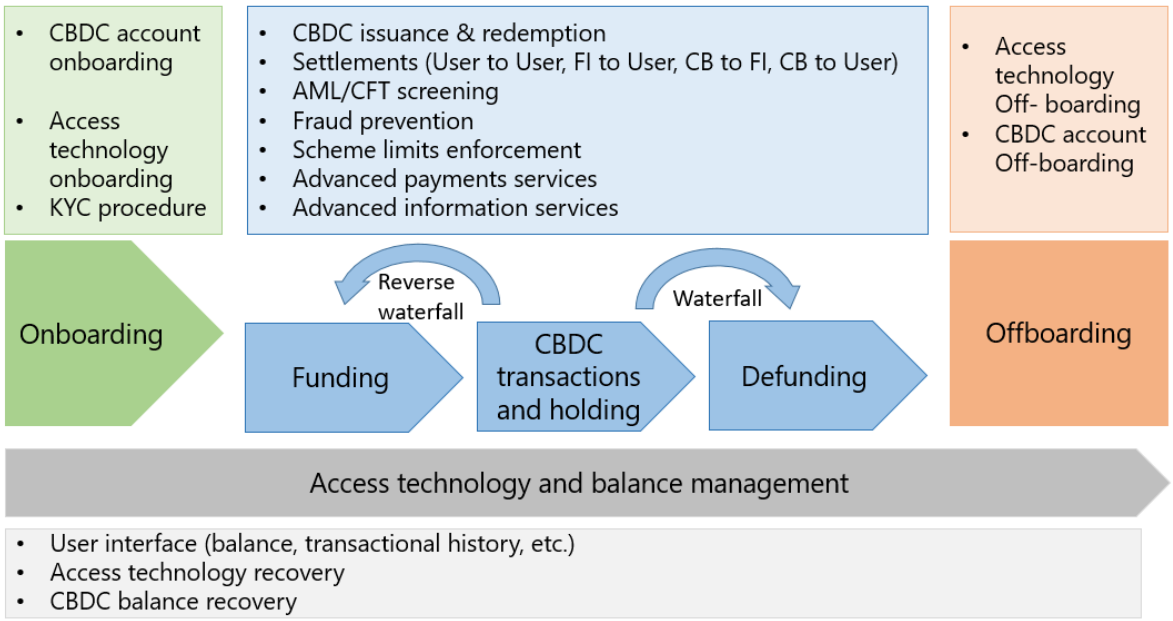
איור 3 – מסע משתמש הקצה בשקל הדיגיטלי



הארכיטקטורה הלוגית תידרש לתמוך באפשרות של משתמש הקצה לבצע כל אחד מההליכים המוצגים באיור.

בהתאם למתודולוגיה שנקבעה לנייר, תחילה מיפינו את ההליכים בהם נדרשת המערכת לתמוך בכדי לאפשר את קיומו של כל אחד מהשלבים השונים במסע המשתמש:

איור 4 – הפונקציונאליות הנדרשת ממערכת השקל הדיגיטלי בכדי לתמוך במסע המשתמש (להסבר מפורט ראה טבלה 2 להלן):



טבלה 2 – הסבר על הפונקציונאליות הנדרשת ממערכת השקל הדיגיטלי

פונקציונאליות	הסבר
CBDC account onboarding	חיבור משתמש הקצה אל מערכת השקל הדיגיטלי
Access technology onboarding	אספקת אמצעי הגישה הטכנולוגי לביצוע פעולות בשקל הדיגיטלי (כרטיס חכם, אפליקציה בטלפון נייד, POS וכד')
KYC procedure	ביצוע הליך הכר את הלקוח בהקשר של משטר איסור הלבנת הון ומימון טרור
CBDC Issuance & redemption	הנפקה ושריפה של שקלים דיגיטליים על ידי הבנק המרכזי
Settlement	פעולות סליקה מסוגים שונים: העברה בין שני משתמשי קצה, העברה בין FI לבין משתמש קצה במסגרת פעולת Funding וכד'
AML/CFT screening	סט הפעולות שהמשתתף נדרש לבצע בכדי לעמוד בדרישות הרגולציה וכללי המערכת בכל הקשור לאיסור הלבנת הון ומימון טרור
Fraud prevention	סט הפעולות שהמשתתף נדרש לבצע בכדי לעמוד בדרישות הרגולציה וכללי המערכת בכל הקשור להגנה צרכנית
Scheme limits enforcement	אכיפת מגבלות בהתאם לכללי המערכת. בדגש על מגבלות על היתרה המקסימלית של שקל דיגיטלי שמשתמש יכול להחזיק
Advanced payments services	תמיכה ביכולת משתמש הקצה לבצע פעולות תשלום מתקדמות (תשלומים מותנים, הוראת תשלום חודשית, תשלום Batch וכד')
Advanced information services	תמיכה ביכולת משתמש הקצה לקבלת שירותי מידע מתקדמים : ניהול תקציב, אנליזה לבתי עסק וכד'
User interface	תמיכה ביכולת משתמש הקצה לנהל את פעילות השק"ד שלו (לראות יתרה, לראות את היסטוריית הפעולות וכד')
Access technology recovery	תמיכה ביכולת משתמש הקצה לשחזר את אמצעי הגישה הטכנולוגי (למשל, במקרה של אבדן כרטיס או מחיקת הטלפון הנייד)
CBDC balance recovery	מתן מענה לסיטואציה בה כלל אמצעי הגישה למערכת אינם זמינים יותר למשתמש הקצה. למשל, במצב בו PSP מסוים חדל לפעול והמערכת תצטרך לתמוך ביכולתו לשייך ספק תשלום חדש אל יתרתו
Access technology Off- boarding	ביטול הגישה של אמצעי גישה טכנולוגי מסוים אל המערכת
CBDC account Off-boarding	הסרה של משתמש הקצה ממערכת השקל הדיגיטלי, לבקשתו.

לאחר מיפוי כלל הפונקציונאליות הנדרשות ממערכת השקל הדיגיטלי, וזיהוי המשתתפים השונים שאמורים לחת חלק בכל פונקציונליות, מצאנו שיש לדון בשתי סוגיות ארכיטקטוניות מהותיות[6]:

- מודל ההפצה של השקל הדיגיטלי – כיצד יופץ השקל הדיגיטלי מבנק ישראל אל משתמשי הקצה? האם הפצה זו תבוצע ישירות מהבנק המרכזי אל משתמשי הקצה או שמא בצורה עקיפה לפיה הבנק המרכזי מפיץ את השקל הדיגיטלי אך ורק אל המוסדות המנהלים חשבונות עו"ש (ה – FIs) והם יפיצו את השק"ד אל משתמשי הקצה (בדומה להפצת מזומן). סוגיה זו מעלה מספר שאלות טכנולוגיות ועסקיות, בהן נדון בהרחבה בסעיף 5 להלן.

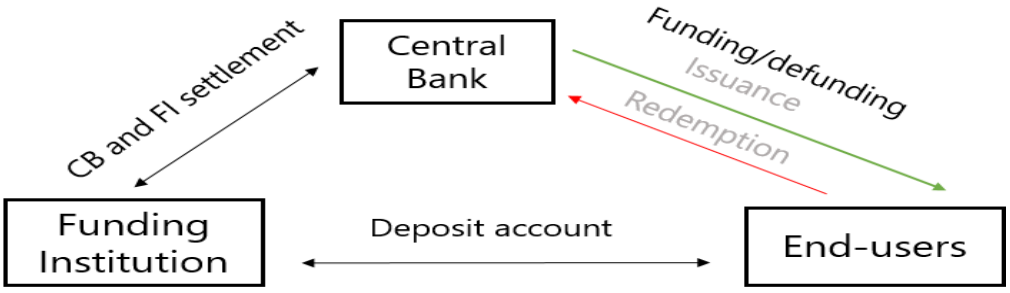
- מבנה שכבת ה- "Back-end" – כיצד תתבצע הסליקה של פעולות התשלום בשקל הדיגיטלי? ומה יהיה מבנה המידע הקיים ברשות בנק ישראל לצורך כך?
בסוגיה זה, מיפינו את הקונפיגורציות האפשריות השונות לניהול פעולת הסליקה ולבסיס המידע הקיים ברמת הבנק המרכזי תוך התייחסות ליתרונות והחסרונות בכל חלופה – נושא זה ידון בהרחבה בסעיף 6 להלן.

5. מודל ההפצה

ניתן להבחין בין שני מודלים קונספטואליים להפצת השקלים הדיגיטליים מהבנק המרכזי אל משתמשי הקצה:

- מודל ישיר – הנפקת השקלים הדיגיטליים מתבצעת ישירות אל חשבונות משתמשי הקצה. כל בקשה של משתמש קצה לביצוע פעולת טעינה (funding) או פדיון (defunding)[7] (כנגד כסף בחשבון אצל FI או כנגד מזומן) תגרור פעולת הנפקה או שריפה של שקלים דיגיטליים על ידי הבנק המרכזי (ובו זמנית, הקטנת/הגדלת הפיקדון של ה- FI בבנק המרכזי[8]).

איור 5 – מודל הפצה ישיר

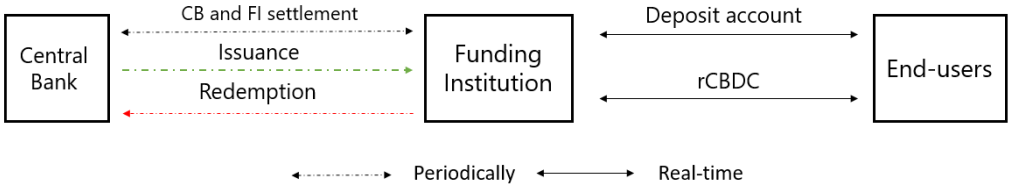


- מודל עקיף – הנפקת השקלים הדיגיטליים מתבצעת מול ה – FIs ופעולות הטעינה והפדיון של משתמשי הקצה מקטינות/מגדילות את המלאי של השקל הדיגיטלי אותו מחזיקים ה-FIs בכדי לתמוך בפעולה זו. בקונפיגורציה זו,

[6] ללא סוגיית פתרון האופליין אליו בחרנו להתייחס בשלב זה של הפרויקט כמעין רכיב חיצוני מולו תידרש אינטראופראביליות של המערכת.
[7] כולל פעולות טעינה ופדיון המוטמעות בפעולת התשלום – Waterfall/Reverse waterfall
[8] במצב הפשוט יחסית שבו ה- FI מנהל חשבון בבנק המרכזי. ייתכנו מצבים יותר מורכבים בהם ל-FI אין חשבון בבנק המרכזי אלא בבנק מסחרי (FI אחר). לעניין זה ראו סעיף 5.3.

הנפקה או שריפה של שקלים דיגיטליים מתבצעת אך ורק כאשר FI מבקש להגדיל או להקטין את מלאי השקלים הדיגיטליים שברשותו (בדומה למודל הפצת המזומן הקיים).

איור 6 – מודל הפצה עקיף



אם ניתן היה להניח שמערכת השק"ד תעוצב באופן שיוכל לתמוך בדרישות הטכנולוגיות של מודל הפצה ישיר אל משתמשי הקצה (הנפקה/שריפה של שק"ד וחיוב/ זיכוי כנגד כל פעולת טעינה/פדיון של משתמש קצה, 24/7), ובהתחשב בכך שבמודל עקיף ה-FIs נדרשים להחזיק מלאי של שקלים דיגיטליים בכל זמן נתון (דרישה בעלת השלכות עסקיות פוטנציאליות בדגש על אספקט הנזילות), נראה כי המודל הישיר יעיל יותר ולכאורה, נותרת פתוחה רק שאלת אופן ההתחשבנות בין הבנק המרכזי ל-FIs.

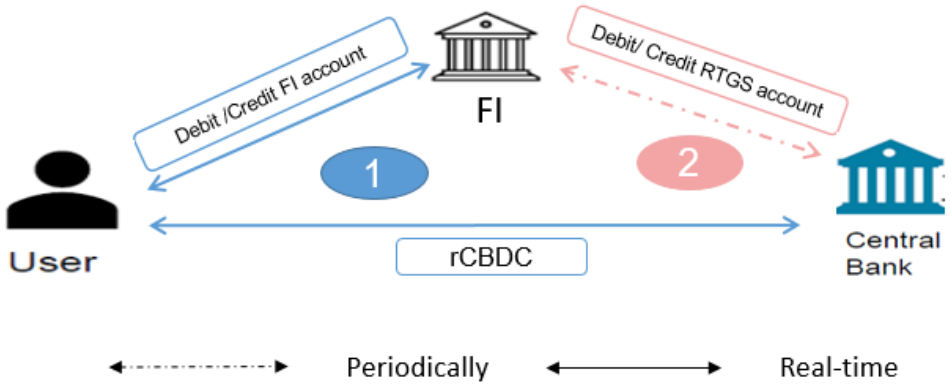
עם זאת, בהתחשב בכך שמערכות RTGS אינן זמינות 24/7 ואינן מתאימות לשימוש בעסקאות תדירות בסכומים קטנים ובתדירות גבוהה[9] **לא ניתן לממש את המודל הישיר תוך התחשבנות בין הבנק המרכזי אל הבנקים המסחריים על בסיס מערכת ה-RTGS**. לכן, בנייר זה, תוך התבססות על הארכיטקטורה שנבחנה בפרויקט "סלע", נבחנו פתרונות חלופיים למימוש מודל הפצה ישיר תוך בחינת היתרונות והחסרונות של הפתרונות המוצעים גם ביחס למודל הפצה עקיף.

5.1 פתרונות אפשריים להתחשבנות בין הבנק המרכזי לבנקים המסחריים במודל הפצה ישיר

- התחשבנות על בסיס תנועות נטו – בפתרון זה, בקשות של משתמשי הקצה לפעולות טעינה ופדיון יקבלו מענה 24/7, אך ההתחשבנות בין הבנק המרכזי לבין ה-FI תבוצע בחלונות הסליקה[10] (בדומה להתחשבנות המתקיימת כיום בין הבנקים המסחריים בארץ על בסיס קובץ תנועות נטו של מס"ב).

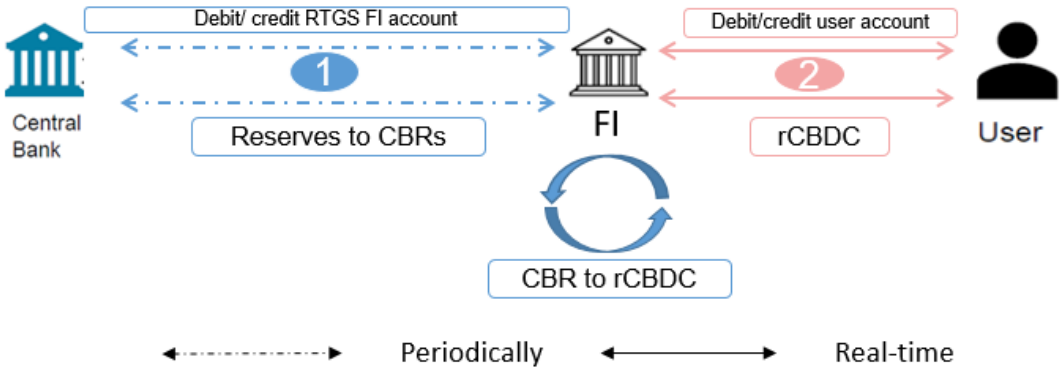
[9] Low value & high frequency transactions
[10] המרווח בין חלונות הסליקה מושפע כמובן מזמינות מערכת ה RTGS. למשל, בסופי שבוע וחגים הוא צפוי להיות ארוך יותר מאשר בימי עסקים רגילים.

איור 7 – פתרון ההתחשבנות נטו



- Central Bank Reserves Tokens (CBR tokens) – פתרון זה מאפשר להתגבר על חוסר הזמינות של מערכת ה RTGS על בסיס מנגנון לפיו:
  - FIs יכולים להמיר יתרות רזרבה ל- CBRs[11] בהתבסס על חלונות התחשבנות מוגדרים בין ה FIs לבנק המרכזי ותוך התחשבות בזמינות מערכת ה- RTGS (יתרת ההחזקה של הבנקים ב CBRs תוכל להשתקף גם בחשבון "צל" ב RTGS);
  - לצורך תמיכה בפעולת טעינה ופדיון של משתמשי הקצה ישתמשו ה – FIs ביתרות ה CBRs שלהם מול הבנק המרכזי אשר ישרוף CBRs וכנגד, ינפיק שקלים דיגיטליים ישירות למשתמשי הקצה.

איור 8 – פתרון ה- CBR Tokens



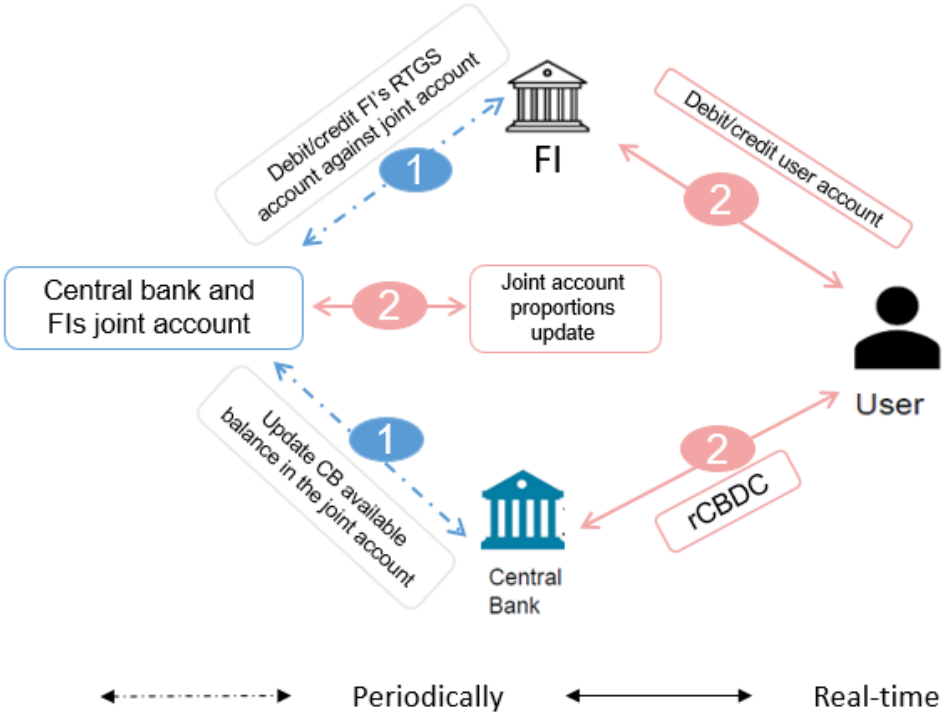
- Real time A2A (Account to account) – פתרון זה מתבסס על הפתרונות הקיימים היום במדינות מסוימות לתמיכה במערכות Fast payment. המשתתפים במערכת חולקים חשבון "משותף", ומבצעים העברות אליו בהתאם לזמינות מערכת ה-RTGS. כל פעולה בין לקוחותיהם של המשתתפים מקבלת ביטוי מידי בשינוי פרופורציות ההחזקה של המשתתפים בחשבון המשותף.

לדוגמא, נניח מערכת Fast Payment בה משתתפים שני בנקים וכל אחד מהם טוען את החשבון המשותף ב- 50 שקלים. בשלב הבא, נניח שמשתמש קצה שיש לו חשבון אצל משתתף א' מבצע העברה של 10 שקלים אל משתמש שיש לו

[11] ייצוג על ידי טוקניזציה של יתרות רזרבה של הבנקים בבנק ישראל.

חשבון אצל משתתף ב'. הביטוי של תנועה זו בחשבון המשותף תהיה בשינוי פרופורציות ההחזקה בין משתתפי המערכת מ – 50/50 ל- 60% בבעלות משתתף ב' ו -40% בבעלות משתתף א'. כך למעשה מתאפשרת סליקה סופית 24/7 בין משתתפי המערכת ללא תלות בזמינות מערכת ה RTGS.
שימוש בפתרון זה לטובת מודל הפצה ישיר של rCBDC משמעותו למעשה ניהול חשבון "משותף" לבנק המרכזי וה-FIs.
כל פעולת טעינה או פדיון של משתמש קצה תביא לשינוי הפרופורציות בחשבון המשותף בין הבנק המרכזי לבין ה-FI שממנו משתמש הקצה מבצע את הטעינה או הפדיון.

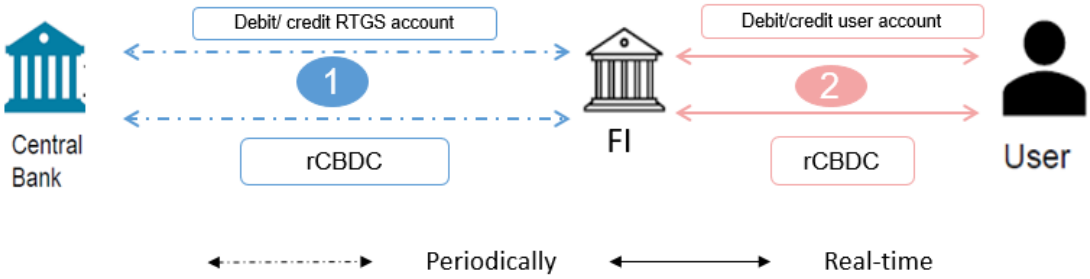
איור 9 – פתרון ה Real time A2A



5.2 מודל הפצה עקיף:

מול הפתרונות למימוש המודל להפצה ישירה, במודל להפצה עקיפה ה-FIs רוכשים שקלים דיגיטליים ומחזיקים מלאי של CBDC בכדי לתמוך בפעולות הטעינה והפדיון של משתמשי הקצה:

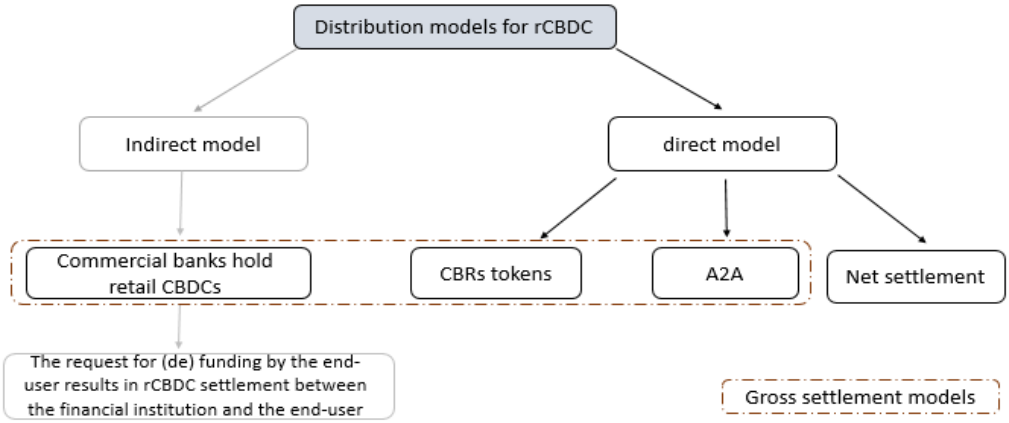
איור 10 – מימוש אפשרי למודל הפצה עקיף



5.3 שיקולים מרכזיים בהמלצה על הפתרון להפצת השקל הדיגיטלי:

- פתרון ההתחשבנות נטו יגרור אשראי תוך יומי בין הבנק המרכזי וה-FIs ולהפך. כתוצאה מכך, רק חלק מ"שרשרת" העסקה של פעולת טעינה/פדיון תהיה מיידית, שכן ההתחשבנות בין הבנק המרכזי ל FIs מבוצעת בדיעבד על בסיס חלונות סליקה מוגדרים מראש; בנוסף, חשיפת אשראי בין הבנק המרכזי ל-FI עשויה להעלות צורך במתן בטוחות, על כל המורכבות והעלויות הכרוכות בכך.
- פתרונות ה – A2A וה- CBRs ידרשו הקמה ותפעול של מערכת נוספת ולכך כמובן השלכות על המורכבות התפעולית והטכנולוגית. מעבר לכך, ניהול מאזן הבנק המרכזי עלול להפוך מורכב יותר עקב התחייבות מסוג נוסף (יתרות בחשבון המשותף/CBRs) וזאת, מעבר לתוספת הנובעת גם ככה מהוספת שקלים דיגיטליים למאזן הבנק;
- פתרונות ה – A2A וה-CBRs מתבססים על סליקה ברוטו ולכן, דורשים טעינה מראש של יתרה על ידי ה-FIs בהיקף הנדרש בכדי לתמוך בנקודת השיא ולא בהיקף התנועות נטו; גם המודל העקיף מתבסס על סליקה ברוטו (איור 11).

איור 11 – מיפוי הפתרונות השונים למימוש המודלים להפצת rCBDC



בבואנו להשוות בין שלושת המודלים המתבססים על סליקה ברוטו, יש לקחת בחשבון שבישראל, לבנקים המסחריים יש חובת נזילות כנגד עו"ש ופיקדונות ציבור לטווח קצר (עד חודש). יתרה זו אינה נושאת ריבית וכוללת את יתרת העו"ש של הבנקים המסחריים בבנק ישראל ואת המזומן המוחזק בכספות הבנקים. שקל דיגיטלי הינו התחייבות ישירה של הבנק המרכזי ועל כן, נכון שייכלל ביתרות המחושבות לצורך שקלול כרית הנזילות. בהתאם לכך, ההשפעה הנזילותית/ עסקית של הדרישה מהבנקים המסחריים להחזיק שקלים דיגיטליים כדי לתמוך במודל העקיף לא צפויה לגרור עלויות נוספות ביחס לשני המודלים האחרים[12];

- מעבר לפשטות היישום והסופיות בכל "שרשרת" הטרנסאקציה, המודל העקיף מציע שני יתרונות נוספים:
  - ביצועי מערכת – כמערכת קמעונאית, מערכת השקל הדיגיטלי תידרש לתמוך בתעבורה (throughput) גבוהה של עסקאות. על מנת שמשתמשי הקצה יוכלו לבצע פעולות טעינה ופדיון בכל עת, ובפרט על מנת לאפשר את מנגנוני ה-waterfall and reverse waterfall, גם מערכת ה-funding נדרשת לעמוד בתעבורה גבוהה. במודל העקיף, מנקודת המבט של מערכת השקל הדיגיטלי פעולת טעינה או פדיון שקולה לפעולת תשלום בין ה-FI למשתמש הקצה, כלומר, מתבססת על יכולת התעבורה הגבוהה של המערכת התומכת בפעולת תשלום, בעוד שבבנק המרכזי, המערכת שתפקידה להנפיק ולשרוף שקלים דיגיטליים יכולה לפעול במנות גדולות יותר ולכן בתעבורה נמוכה יותר. **כך או כך,**

[12] למעט מצבי קצה בהם כלל יתרות הנזילות שאינן נושאות ריבית בבנק המרכזי אינן מספקות בכדי לתמוך בפעולות הטעינה והפדיון של משתמשי הקצה לצד הפעילות השוטפת.

המערכות של ה-FIs תצטרכנה לתמוך בעדכון תדיר של חשבונות הלקוחות שלהם כנגד פעולות טעינה ופדיון, וזאת, ללא כל קשר לפתרון הנבחר.

- צעד בכיוון למטבע רב תכליתי – השימוש באותה מערכת על ידי המוסדות הפיננסיים ומשתמשי הקצה יכול לסלול את הדרך למטבע דיגיטלי רב תכליתי לשימושי Wholesale ו-Retail ולהיות צעד בכיוון פתרון בעיות של אינטראופראביליות בין הממד הקמעונאי לסיטונאי.

לסיכום, השיקולים השונים לבחירת מודל ופתרון כזה או אחר נוגעים בסוגיות הקשורות לסופיות הפעולה, הפשטות הטכנולוגית והנזילות שהינה הסוגיה המרכזית ביותר. בהתחשב בכך שהבנקים המסחריים בישראל מחויבים כבר היום בכרית נזילות אשר איננה נושאת ריבית, ותוכל לכלול גם את יתרות השקלים הדיגיטליים שהם יצטרכו להחזיק, **ניכר כי קיים יתרון מובהק למודל ההפצה העקיף בפעולות טעינה ופדיון.**

עם זאת, תיתכן פעילות של FIs גם ללא החזקה ישירה של שקלים דיגיטליים (קונפיגורציה C בטבלה 1 לעיל) למשל, על ידי שימוש במלאי השקלים הדיגיטליים המוחזקים על ידי FI אחר. לדוגמא, במצב בו מוסד מסוג e-Money מחזיק את כספי לקוחותיו בפיקדון אצל בנק מסחרי ויוכל לתמוך בפעולת הטעינה/פדיון של לקוחותיו על בסיס יתרת השק"ד המוחזקת על ידי הבנק המסחרי (לתיאור מלא של פעולת ההפצה ראה תרשימי רצף לפעולות השונות בנספח 2) . ייתכנו מודלים מתקדמים נוספים בהם ה-FI משתמש ביתרה מסוימת מתוך יתרת השקלים הדיגיטליים של לקוחותיו כ "Liquidity Pool", כמובן על בסיס התקשרות עסקית מוגדרת בין ה-FI ללקוחות, וכתלות ברגולציה שתאפשר מנגנון פעילות זה.

5.4 ביצוע פעולות טעינה ופדיון כנגד מזומן[13]:

בנוסף ליכולת של משתמשי הקצה לטעון ולפרוק את ארנק השקל הדיגיטלי כנגד חשבון שהם מנהלים בבנק מסחרי או במוסד אחר, חשוב מאוד לייצר גם פתרון שמאפשר המרה קלה ונוחה בין שקל דיגיטלי מזומן. לו היינו מסתפקים בפתרון שמאפשר למשתמש קצה להמיר שק"ד במזומן אך ורק באמצעות הבנק המסחרי בו מנוהל חשבון העו"ש של משתמש הקצה, פעולת ההמרה הייתה פשוטה וכוללת למעשה שני שלבים:

- הפקדה או משיכה של מזומן בחשבון הבנק על בסיס התשתית הקיימת – פעולה שאיננה קשורה באופן ישיר למערכת השקל הדיגיטלי, וכוללת התחשבנות של משתמש הקצה מול הבנק המסחרי בדומה למבוצע היום;
- ביצוע פעולת טעינה/פדיון כנגד חשבון הלקוח בבנק מסחרי (כפי שתואר בהרחבה בסעיף הקודם).

עם זאת, **ככל שחפצים באפיון מערכת אשר תוכל לתמוך בפעולות ההמרה של השק"ד מ/אל מזומן בצורה נגישה יותר, ושאיננה מוגבלת להתנהלות מול המוסד הפיננסי בו מנהל משתמש הקצה את חשבונו, ויכולה לתמוך גם במשתמשי קצה שאין להם חשבון בנק, יש צורך בעיצוב פתרון ייעודי.** להלן תוצג קונפיגורציה אפשרית (איור 12):

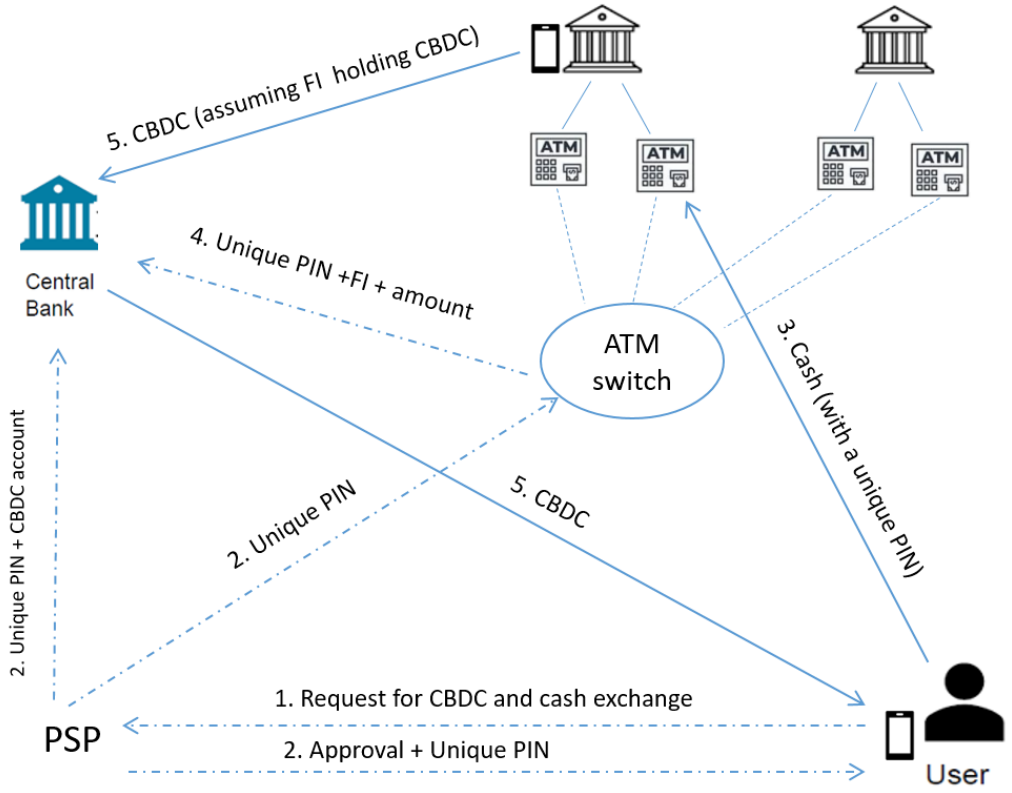
- הגורמים המעורבים בהליך ההמרה: ה-FIs בעלי מכשירי ATMs הפרושים ברחבי הארץ, ומכשירי ה- ATMs עצמם; מתג ה–ATM ; הבנק המרכזי; ספק התשלום (PSP) ומשתמש הקצה;

[13] על בסיס עקרונות מרכזיים מהפתרון שעוצב במסגרת פרויקט סלע.

- השלבים המרכזיים[14] בפתרון[15]:

1. משתמש הקצה מבקש (באמצעות ארנק השק"ד שסופק לו על ידי ספק התשלום) לבצע הפקדה של מזומן כנגד זיכוי בשקלים דיגיטליים;
2. ספק התשלום מבצע את ההליכים התפעוליים הנדרשים כדי לאפשר את הפעולה, ובפרט, בדיקות ככל שנדרשות מכוח כללי איסור הלבנת הון. עם השלמת הבדיקות, ישלח ספק התשלום הודעת אישור למשתמש הקצה, יחד עם קוד ייחודי אותו ישלח ספק התשלום במקביל גם אל הבנק המרכזי ואל מתג ה-ATM.;
3. משתמש הקצה יוכל לגשת (בטווח זמן שיוגדר מראש) לכל מכשיר ATM בארץ אשר מחובר אל מתג ה–ATM (ותומך בהפקדת מזומן) ולבצע הפקדה של מזומן תוך שימוש בקוד הייחודי שנמסר לו מספק התשלום[16].
4. מתג ה–ATM יפיץ את הפרטים הנדרשים לבנק המרכזי לצורך השלמת הפעולה: קוד ייחודי, ה-FI באמצעותו בוצעה ההפקדה והסכום. יודגש כי כיום לא מתקיימת קישוריות טכנולוגית ישירה בין בנק ישראל למתג ה- ATM ולא ניתנת תמיכה בהליכים דומים - תידרש חיבוריות ויצירה של הפרוטוקולים הנדרשים לצורך תמיכה בשלב זה;
5. היות ולא נדרשת הכרות מקדימה או התקשרות בין משתמש הקצה אל ה- FI, הבנק המרכזי יהווה חוצץ בין שני הגורמים ויבצע את פעולת חיוב ארנק השקל הדיגיטלי של ה–FI ומנגד, את פעולת זיכוי ארנק השקל הדיגיטלי של משתמש הקצה. מאחר וההנפקה של השקלים הדיגיטליים מבוצעת ישירות מהבנק המרכזי אל ארנק משתמש הקצה, **מצב זה יחרוג ממודל ההפצה העקיף שהוזכר בפרק הקודם**. לחילופין ניתן לשקול שההתחשבנות תבוצע כפעולת העברה של שקלים דיגיטליים בין ה FI למשתמש הקצה, מבלי לערב כלל את הבנק המרכזי, אך קונפיגורציה זו יכלה להעלות סוגיות של פרטיות ומחויבות (לא רצויה) של ה-FI לסוגיות AML.

איור 12 - תהליך אפשרי לתמיכת המערכת בהמרה ממזומן לשק"ד ולהיפך



[14] ייתכנו מסרים נוספים בין המשתתפים הכוללים אישור/דחייה. כמו כן, הפתרון מציג את ה "Happy path" ולא מתייחס לתרחיש של דחיית הפעולה על ידי מי מהגורמים.

[15] לצורך הפשטות, מוצג פתרון רק לכיוון אחד - המרה ממזומן לשקלים דיגיטליים.

[16] נכון להיום, בישראל ניתן להפקיד מזומן רק במכשיר ATM של הבנק בו הלקוח מנהל את החשבון. ייתכן שבעתיד ניתן יהיה לאפשר הפקדת מזומן בכל ATM בנקאי, בדומה לאפשרות הקיימת במשיכת מזומן.

ייתכן כי הפתרון הגנרי המוצג לעיל יוכל לאפשר המרות בסכומים לא גבוהים, עד ספים מסוימים אשר יקבעו בין היתר על בסיס סוגיות הקשורות לאיסור הלבנת הון ומימון טרור. בסכומים גבוהים יותר, המענה יינתן על בסיס ההליך הדו שלבי אשר הוצג לעיל ודורש הפקדה או משיכה מ/אל חשבון הבנק של משתמש הקצה.

6. שכבת ה- "Back-end"

6.1 חלופות מרכזיות לפעילות "מנוע" הסליקה:

בנק ישראל כמנפיק המטבע ומנהל המערכת יפעל כגורם האחראי והבלעדי לביצוע פעולת הסליקה בין משתמשי ומשתתפי מערכת השקל הדיגיטלי. ניתן להבחין בין שתי גישות מרכזיות לתמיכת הבנק המרכזי בפעולת הסליקה ב-CBDC קמעונאי:

- <u>סליקה מבוססת חשבון</u> – על פי גישה זו פעולת הסליקה מתבצעת על ידי עדכון של יתרות משתמשי הקצה (חיוב המשלם וזיכוי המוטב) בבסיס מידע כלשהו ("לדג'ר") המסוגל לקשר בין המשתמש[17] ליתרתו. זו למעשה הגישה המסורתית הקיימת לטיפול בפעולות סליקה כיום - למשל בחשבונות הציבור בבנקים, או בחשבונות של המשתתפים במערכת ה-RTGS ;
- <u>סליקה מבוססת טוקנים</u> – על פי גישה זו, לצורך תמיכה בפעולת הסליקה לא נדרש הבנק המרכזי לדעת מהי היתרה הכוללת של המשתמשים והפעולה מבוססת על אימות האותנטיות והבעלות על יתרה מסוימת (המיוצגת על ידי טוקן או קבוצת טוקנים). ניתן להקביל גישה זו לפעולות במזומן. כך למשל, בכדי לבצע תשלום בסך 20 ₪ יכול משתמש הקצה לבצע שימוש בשטר של 20 ₪ מבלי לחשוף את כלל היתרה בארנק שלו ועדיין להשלים את פעולת התשלום. חשוב להזכיר שבעוד שבהתאם להחלטות שהתקבלו בפרויקט בנושא הפרטיות, לבנק ישראל לא תהיה גישה למידע פרטני מזוהה אודות משתמשי הקצה, הרי שהשקל הדיגיטלי לא יהיה אנונימי בדומה למזומן, ומערכת השק"ד תצטרך לתמוך בהליכים הנדרשים מטעמים רגולטוריים שונים כגון KYC, AML, CFT, גביית מס, וכד'. לכן, סביר להניח שיתרה כוללת של משתמשי הקצה תצטרך להתנהל במאגר מידע כלשהו. עם זאת, היא אינה הכרחית לבנק המרכזי לצורך ביצוע תפקידו הבסיסי - פעולת הסליקה.

6.2 מודלים מרכזיים למבנה המידע:

ניתן לחשוב על מספר מודלים על פיהם ניתן לממש את מנגנון הסליקה, שייבדלו ביניהם בין היתר על פי מבנה בסיס המידע , היקף המידע הקיים לבנק המרכזי כברירת מחדל (לצורך תמיכה בפעולת הסליקה), ואופן חלוקת ניהול המידע בין הבנק המרכזי לבין משתתפי המערכת.

<u>מבנה המידע בסליקה מבוססת חשבון</u>

[17] אין הדבר אומר שהקישור נעשה על בסיס זהות המשתמש וייתכן שימוש בזהות מוצפנת או בכל מזהה חד ערכי אחר אשר אינו מאפשר לדעת את זהות המשתמש.

היות ופעולת הסליקה בגישה המבוססת חשבון מתבטאת בעדכון היתרות של משתמשי הקצה, קיומו של מאגר מידע באמצעותו ניתן לקשר בין משתמשים (או זהות מוצפנת של משתמשים) ליתרות הינו תנאי הכרחי. למימוש גישה זו, קיימים שני מודלים קונספטואליים[18] לחלוקת המידע ולניהולו בין הבנק המרכזי למשתתפי המערכת:

- לדג'ר מרכזי קמעונאי – יתרות משתמשי הקצה מנוהלות בבסיס מידע מרכזי המנוהל על ידי הבנק המרכזי. יודגש כי אין הדבר אומר שבניהול המידע ושיתופו לא יכול להתבצע שימוש בטכנולוגיה ללדג'ר מבוזר (DLT), בין אם הוא מבוזר בין שרתים שונים של הבנק המרכזי ובין אם הוא מנוהל על ידי הבנק המרכזי אבל מבוזר טכנולוגית גם לשרתים של גופים אחרים.
- לדג'ר מרכזי סיטונאי + מספר לדג'רים קמעונאיים – במודל זה ספקי התשלום מנהלים לדג'ר קמעונאי עבור לקוחותיהם – משתמשי הקצה, והיתרה האגרגטיבית של כלל משתמשי הקצה של ספק תשלום מסוים מקבלת ביטוי בלדג'ר הסיטונאי אשר מנוהל על ידי הבנק המרכזי (וגם כאן ייתכן שימוש בטכנולוגיית DLT).

<u>מבנה המידע בסליקה מבוססת טוקנים</u>

בסליקה מבוססת טוקנים הבנק המרכזי לא נדרש לדעת את היתרה הכוללת של משתמש הקצה ולכן לא חייב להצטבר אצלו מידע אודות דפוס הפעילות של אותו משתמש. עם זאת, בסיס מידע מרכזי עדיין עשוי להידרש לצורך מטרות נוספות, כגון : ניהולה התקין של המערכת, יעילות, שמירה על האפשרות להצעת שירותים על בסיס מידע מרכזי, ניהול מגבלות ההחזקה, וכד'. במודל זה ישנה גמישות גבוהה יותר לקבוע האם לנהל בכלל בסיס מידע מרכזי מפורט, אם כן, מי צריך לנהל אותו, מה הוא יכלול, ומה תהיינה הרשאות הגישה של הבנק המרכזי ושאר המשתתפים אל המידע.

ייתכנו כאמור חלופות רבות למבנה בסיס המידע. להלן שתי אפשרויות קצה:

- מידע מינימלי בידי הבנק המרכזי וניהול יתרות המשתמשים על ידי ספקי התשלום[19] – מאגר המידע המנוהל על ידי הבנק המרכזי יכלול אך ורק את המידע הנדרש לצורך תמיכה בפעולת הסליקה המבוססת טוקנים כגון: טוקנים זמינים לשימוש ואינדקס מסוים[20] (למשל מפתח ציבורי) המקשר בין טוקן לבעליו. במודל זה, ניהול המידע הרגיש והמפורט יבוצע אך ורק על ידי ספקי התשלום (זהות משתמשים, יתרות כוללות, היסטוריית פעולות התשלום של משתמש הקצה ועוד) והבנק המרכזי מתפקד אך ורק כ "מנוע" סליקה. דוגמא לכך הינה פעולת סליקה מבוססת UTXO (הרחבה בתיבה 2).
- מידע מרכזי הדומה בהיקפו למידע הקיים בלדג'ר קמעונאי בגישה מבוססת חשבון – גם במצב בו יחליט הבנק המרכזי לטפל בפעולת הסליקה בגישת הטוקנים, עדיין ניתן להחליט לנהל בסיס מידע דומה לזה הקיים בלדג'ר קמעונאי יחיד, על ידי מתן אינדקס אחד וייחודי לכל משתמש קצה ושמירה של היסטוריית הטרנסאקציות של משתמש הקצה במאגר המידע.

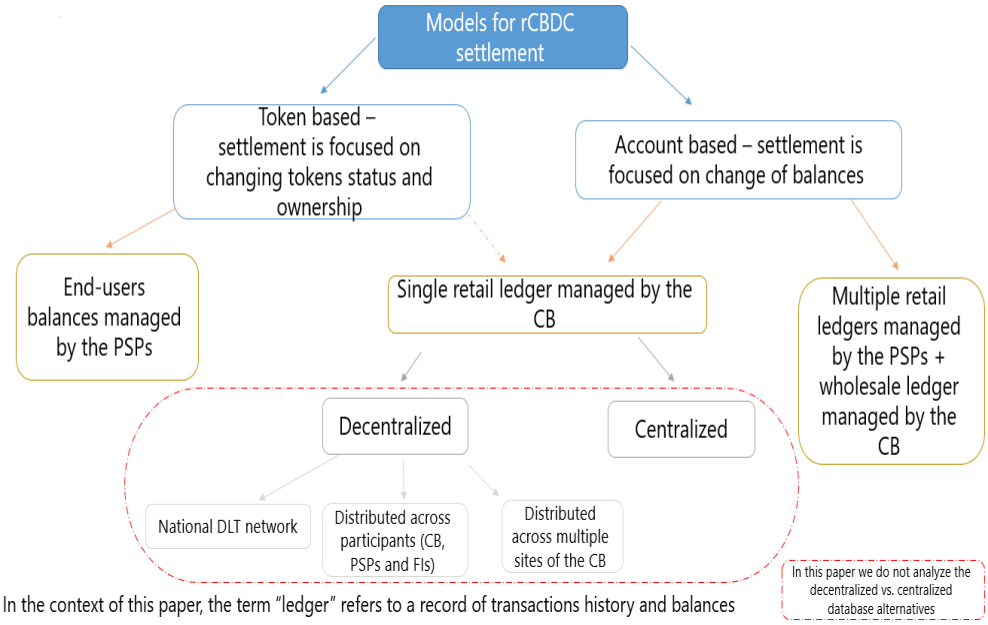
---

[18] See BIS (2022)

[19] מודל זה מייצג את גישת ה ECB אשר הוצגה במסמך ה Prototyping (ECB 2023) ולפיה הבנק המרכזי יפעל כמנוע סליקה בלבד על בסיס מודל ה- UTXO כאשר יתרות המשתמשים תנוהלנה על ידי ספקי התשלום.

[20] במודל זה מתאפשרת קונפיגורציה לפיה כמה מפתחות או כמה אינדקסים מקושרים לבעלות אחת והבנק המרכזי לא חייב לדעת את הבעלות (גם לא המוצפנת) של כלל המפתחות בכדי לטפל בפעולת הסליקה.

איור 13 - מודלים שונים לטיפול בפעולת הסליקה ולמבנה המידע



6.3 שיקולים מרכזיים בהחלטה בנוגע למודל מבנה המידע:

- <u>עמידה בהנחות המקדימות לארכיטקטורה</u> - מבנה המידע צריך לאפשר למערכת לעמוד בכל ההנחות שהוגדרו בסעיף 2.1, כולל באפשרות לאכוף מגבלות החזקה ולהחיל ריבית. בפרט, במצב בו הריבית תלויה בסוג המשתמש ו/או בגובה היתרה, קיים יתרון למאגר מידע מרכזי;
- <u>פונקציונאליות נדרשת</u> - מבנה המידע יצטרך לאפשר לבנק המרכזי לתמוך בהליכים הנדרשים לו כמנהל המערכת, כמנפיק המטבע, וכגורם הבלעדי לטיפול בפעולת הסליקה, וגם בהליכים נוספים בהם ייתכן והבנק המרכזי יחליט להיות מעורב, כגון: פתרון קונפליקטים בין משתמשים, תמיכה בשחזור יתרת שק"ד של משתמש קצה (למשל במצב חירום בו PSP מסוים חדל לפעול), וכדומה.
- <u>חתירה למבנה שוק תחרותי</u> - מבנה המידע יצטרך לתמוך באפשרות של משתמש הקצה לקבל שירות ממספר PSPs בזמן נתון, לעבור באופן קל ופשוט בין PSPs, ובכך שחסמי כניסה הטכנולוגיים והעסקיים לכניסה של משתתפים אל האקוסיסטם יהיה נמוכים ככל שניתן.

הניתוח לעיל מעלה כי **עיצוב המערכת באופן בו לבנק המרכזי יהיה בסיס מידע מפורט ככל שניתן או לדג'ר קמעונאי** (גם אם לא מזוהה) **מאפשר גמישות גבוהה מבחינת כל אחד מהשיקולים המצוינים לעיל. מאידך, ניהול של מאגר מידע מרכזי זה עלול ליצור לבנק המרכזי חשיפה לאחריות בסוגיות שאמורות להיות מנוהלות על ידי המגזר הפרטי,**

בפרט בנושאים כגון פרטיות המשתמשים ואכיפת כללי איסור הלבנת הון ומימון טרור. כעיקרון, רצוי שמעורבות הבנק המרכזי בנושאים אלה תהיה מצומצמת ככל הניתן. תחלופה זו מקבלת מענה בסעיף הבא, המציג מודל בו ישנה הפרדה ברורה בין המידע הנדרש לבנק המרכזי לצורך פעולות הסליקה לבין בסיס המידע הרחב יותר.

תיבה 2 – סליקה מבוססת מודל ה- UTXO (Unspent Transaction Output)

<u>תיאור כללי של המודל</u>:

מודל ה- UTXO הינו יישום אפשרי לסליקה מבוססת טוקנים. כל טרנסאקציה גוררת שינוי סטטוס של הטוקן או של קבוצת הטוקנים בהם בוצע שימוש (ה – Input) לסטטוס של "spent tokens" אשר אינם זמינים עוד לשימוש, גם אם ערכם של הטוקנים גבוה מהערך הנדרש לטובת השלמת הטרנסאקציה. ה- Output של פעולת ה UTXO כולל בין שתיים לשלוש קבוצות טוקנים חדשות:

- קבוצת הטוקנים ששימשה כ Input כקבוצה חדשה בסטטוס של "spent tokens" ;
- קבוצת טוקנים חדשה בסטטוס של "unspent tokens" המונפקת אל המוטב כקבוצת טוקנים אחת בערכה של הטרנסאקציה ;
- אופציונלי (כתלות בסכום הטוקנים בהם השתמש מבצע הטרנסאקציה ובסכומה) - קבוצת טוקנים חדשה בסטטוס של "unspent tokens" אשר מייצגת את העודף המונפק חזרה אל המשלם.

בכל פעולת סליקה Spent tokens value (Input) = Unspent tokens value (Output) ויתרות המשתמשים בכל זמן נתון מחושבות על ידי סכמה של כלל ה-unspent tokens בבעלותם.

<u>דוגמא</u>:

נניח כי ברשותו של בוב שני טוקנים בשווי של 50 ₪ כל אחד ולצורך ביצוע תשלום של 30 ₪ לאליס משתמש בוב באחד מהטוקנים שברשותו. פעולת הסליקה תתבצע באופן הבא:

- הטוקן של ה- 50 ₪ בו בוב השתמש יישונה לסטטוס של "spent tokens"
- יונפק "unspent token" חדש בערך של 20 ₪ חזרה אל בוב
- יונפק "unspent token" חדש בערך של 30 ₪ אל אליס

חישוב היתרות של בוב ואליס בסוף הטרנסאקציה תתבסס כאמור על סכמה של כלל ה- unspent tokens שברשותם. כלומר, 70 ₪ לבוב (50 ₪ בהם לא ביצע עדיין שימוש + 20 שהתקבלו כעודף בטרנסאקציה הנוכחית) ו-30 ₪ לאליס (התקבול מהעסקה הנוכחית).

<u>דוגמאות לשימושים מוכרים במודל</u>:

מטבעות קריפטוגרפים רבים, כולל ביטקוין, מתבססים על מודל ה UTXO לצורך הסליקה. אזכורים לשימוש פוטנציאלי במודל זה גם בהקשר של rCBDC ניתן למצוא בין היתר בפרויקט ה-e-Krona של הבנק המרכזי של שבדיה (Sveriges Riksbank 2022), בפרויקט Aurum של ה-BIS והרשות המוניטרית של הונג קונג (BIS 2022), וגם במסמכים של פרויקט האירו הדיגיטלי (ECB 2023) ושל הבנק המרכזי של אנגליה (Bank of England 2023) בהם המודל מוזכר כחלופה אפשרית למימוש מנוע הסליקה במערכת הפאונד הדיגיטלי לצד בחינה גם של האפשרות לשימוש בסליקה מבוססת חשבון.

<u>המידע הקיים בטוקנים מסוג UTXO</u>:

המידע הקיים בכל טוקן UTXO מכיל 3 שדות:

- הערך אותו מייצג הטוקן ("Value")
- מספר סידורי ייחודי לטוקן ("Serial number")
- פרמטר מסוים הקובע מי רשאי לבצע שימוש בטוקן ואיך ("Witness Program Commitment") - היישום הפשוט ביותר לפרמטר זה הוא על ידי שימוש במפתח ציבורי הקובע מי רשאי להשתמש בטוקן, כאשר השימוש יכול להתבצע רק על ידי שימוש במפתח הפרטי הנמצא ברשותו של מחזיק הטוקן.

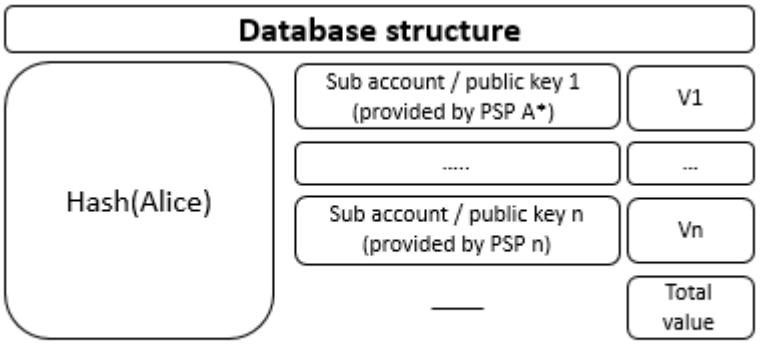
בשונה מגישת ה "Account based" אשר מאפשר רמת פרטיות של זהות פסאודואנונימית לכל היותר, מודל UTXO מאפשר גמישות גבוהה יותר ורמת פרטיות גבוה היותר, למשל על ידי שימוש ב"מפתחות" מתחלפים או מספר מפתחות למשתמש אחד.

6.4 הפרדת בסיס המידע מפעולת הסליקה – המודל המוצע:

עקרונות מרכזיים במודל:

- בשלב זה של הפרויקט אנחנו משתדלים להימנע מהעדפה של טכנולוגיה כזו או אחרת ובפרט לא רוצים להחליט שמנגנון הסליקה יהיה מבוסס חשבון או מבוסס טוקנים. הדוגמאות שיוצגו יניחו סליקה מבוססת טוקנים לצורך הפשטות בלבד, אך ניתן ליישם את המודל המוצע גם בסליקה מבוססת חשבון, על ידי שימוש במספר תתי חשבונות המשויכים אל "חשבון אב" אחד, בדומה לקונפיגורציה לפיה טוקנים משויכים לאינדקסים שונים המקושרים לבעלות אחת;
- הקונפיגורציה הבסיסית במערכת תתמוך בכך שהמידע המועבר מה-PSPs אל הבנק המרכזי לצורך טיפול בפעולה בשקל הדיגיטלי יהיה אך ורק המידע המינימלי הנדרש לבנק המרכזי לביצוע הסליקה. קרי: המפתח הציבורי או כל אינדקס אחר אליו מקושרים היתרה/טוקנים של המשלם, אינדקס חד ערכי כלשהו המשויך אל המוטב, וסכום הטרנסאקציה[21];.
- מאפייני מאגר המידע המרכזי:
  - תפעול וניהול המאגר יכול להתבצע על ידי הבנק המרכזי, המגזר הפרטי או על ידי שילוב של שניהם. בכל מקרה, הגורם הבלעדי בעל הרשאות לבצע שינויים בבסיס המידע (למשל, שינויי יתרה בגין סליקת תשלום בין שני משתמשים) הינו הבנק המרכזי, בעוד שהרשאת הגישה של המשתתפים מהמגזר הפרטי אל בסיס המידע תהא הרשאה לקריאה בלבד,[22] ובהתאם להרשאות שיתנו משתמשי הקצה למשתתפים ובהתאם לכללי המערכת;
  - מבנה המידע המרכזי יכלול עבור כל משתמש במערכת זהות מוצפנת כלשהי (עמודה שמאלית באיור 14), את כלל תתי החשבונות או האינדקסים המשויכים אליו (עמודה אמצעית באיור 14) יחד עם היתרה הזמינה לשימוש בכל תת חשבון / אינדקס (עמודה ימנית באיור 14). העובדה שהיתרה מחולקת בין מספר אינדקסים לא מונעת ממשתמש הקצה להשתמש בכלל היתרה שלו באמצעות PSP אחד (כולל זו המשויכת לאינדקס שסופק על ידי PSP אחר). דבר זה יוכל להתאפשר כתלות בכללי המערכת ובהרשאות המשתמש ל PSP מסוים.

איור 14 - דוגמא למידע הקיים בנוגע למשתמשת אליס בבסיס המידע

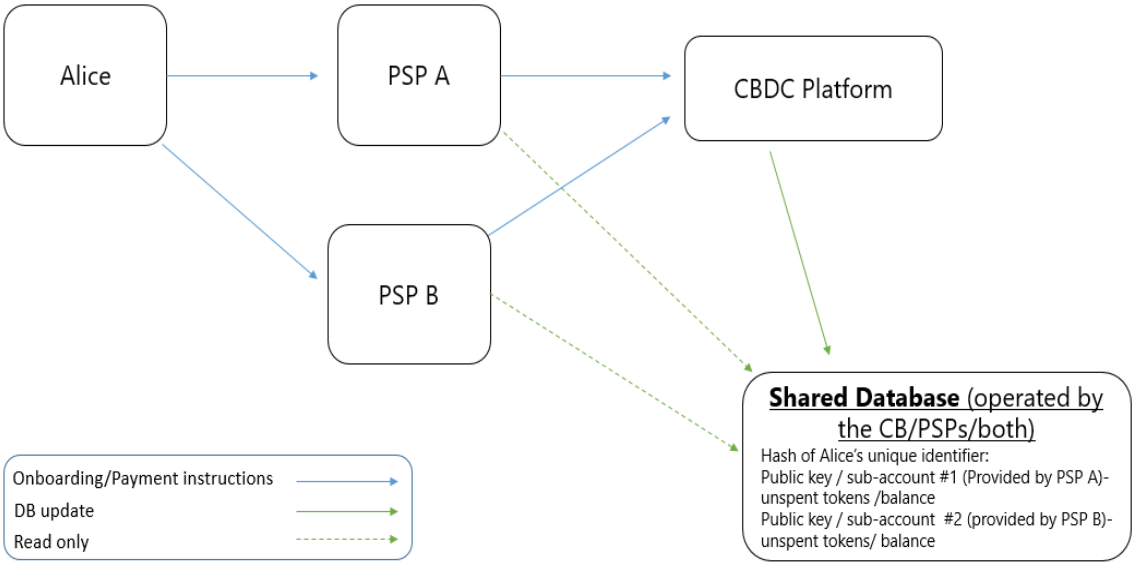


*PSPs will be able to provide more than one sub-account / public key to the end user

[21] בהמשך יוכל הבנק המרכזי להחליט כי לצורך תפעולה התקין של המערכת או לטובת צרכים סטטיסטיים המסר המתקבל מספק התשלום יכלול גם מאפיינים נוספים של העסקה או של המשתמשים, ובלבד שאלה לא יוכלו לשמש לחשיפת זהות המשתמשים.

[22] בפרט, המשתתפים לא יוכלו לבצע שינויים ביתרות של המשתמשים. תיתכן קונפיגורציה במסגרתה יוכלו ספקי התשלום לכתוב "חוזים חכמים" על גבי בסיס המידע המרכזי בהתאם להחלטות שיתקבלו לגבי אופן מימוש ה Programmability במערכת.

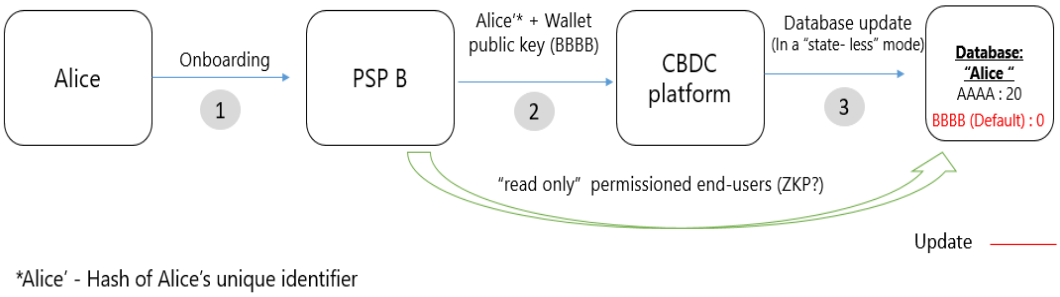
איור 15 - מבנה כללי של מודל המידע.



דוגמאות ליישום המודל:

- מקרה א' – משתמשת הקצה אליס מחזיקה בנקודת המוצא 20 שק"ד באמצעות ארנק שסופק לה על ידי PSP A והיא פונה אל PSP B (שלב 1, איור 16) מאחר והיא מעוניינת לבצע Onboarding גם אצלו, ובנוסף להגדיר את B כארנק ברירת המחדל לקבלת תשלומים בשקל הדיגיטלי[23]. PSP B פונה למערכת השקל הדיגיטלי, (שלב 2), ומבקש להקים עבור הזהות המוצפנת של אליס ('Alice) ארנק נוסף. מערכת השקל הדיגיטלי מקימה את הארנק הנוסף בבסיס המידע (שלב 3).

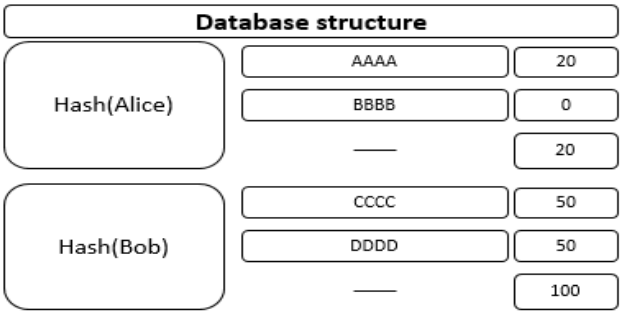
איור 16 – ביצוע פעולת Onboarding במודל המוצע



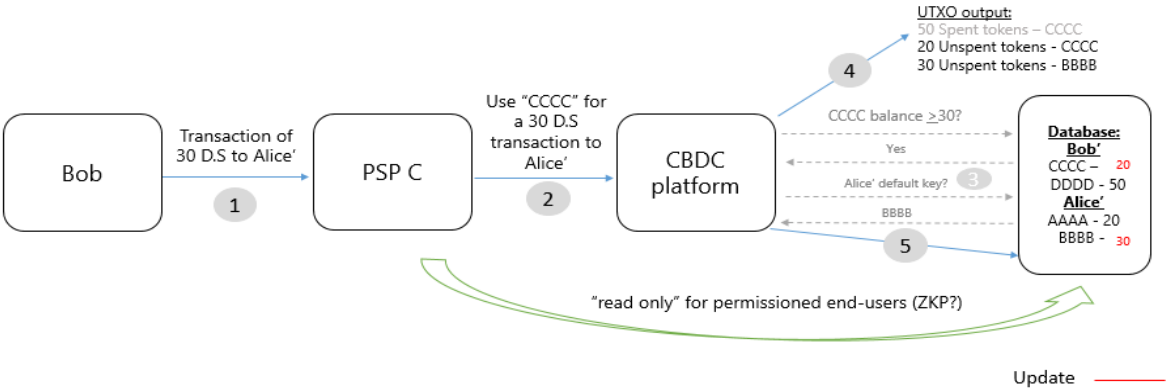
- מקרה ב' - בוב הינו משתמש נוסף במערכת והוא מחזיק ב 100 שק"ד סך הכול (50 שק"ד באמצעות ארנק שסיפק לו PSP C ועוד 50 שק"ד באמצעות ארנק שסיפק לו PSP D - איור 17.1). הוא מעוניין לשלם לאליס סכום של 30 שק"ד באמצעות PSP C(איור 17.2). הוא מעביר את ההוראה ל-PSP C (שלב 1) שמעביר אותה למערכת השקל הדיגיטלי (שלב 2). המערכת מוודאת שלבוב יש את היתרה הנדרשת ומהו חשבון ברירת המחדל של אליס לתקבולים בשקל הדיגיטלי (שלב 3), מבצעת את הסליקה (שלב 4) ומעדכנת את בסיס המידע בדבר היתרות החדשות של שני המשתמשים (שלב 5).

[23] בעוד שהמשתמש יכול לבחור באמצעות איזה PSP לבצע כל פעולת תשלום, סביר שיהיה צורך להגדיר PSP כברירת מחדל לקבלת תשלומים. באופן זה המשלם יצטרך לדעת רק את הכתובת הכללית של המוטב, מבלי להזדקק למידע נוסף אודות ה-PSPs השונים שהמוטב הוא לקוח שלהם.

איור 17.1 - מאגר המידע בנקודת המוצא למקרה ב'



איור 17.2 – ביצוע פעולת תשלום מבוב לאליס



6.5 יתרונות מרכזיים של המודל המוצע:

- **גמישות גבוהה ביישום**
  - המודל המוצע מאפשר מצד אחד להפחית את המידע הזמין לבנק המרכזי למינימום הנדרש לצורך טיפול בפעולת הסליקה, ומצד שני משאיר את הגמישות להחליט על מאפייניו של מאגר המידע בהתאם לצרכים הנוספים שאינם פעולת הסליקה. ניתן להחליט על היקף המידע הקיים במאגר וזמין לבנק, ועל האופן בו יוכלו הבנק המרכזי והמשתתפים הנוספים לגשת אל המידע הקיים במאגר זה;
  - המודל ניתן למימוש הן בגישת סליקה מבוססת חשבון והן בסליקה מבוססת טוקנים.
- **ניהול גמיש של בסיס המידע והרשאות הגישה אליו**
  - במקרה של שימוש במודלים המסורתיים לסליקה מבוססת חשבון, סביר להניח כי בסיס המידע המרכזי יתופעל על ידי הבנק המרכזי בצורה ריכוזית כזו או אחרת, שכן השינוי בבסיס המידע מייצג למעשה את פעולת הסליקה שהיא באחריות הבלעדית של הבנק המרכזי. המודל המוצע במסמך זה מציע גישה פתוחה יותר לשאלת ניהול בסיס המידע תוך הבחנה בין המידע הבסיסי אליו נחשף הבנק המרכזי אגב פעולת הסליקה לבין ניהול מאגר המידע, גם אם הסליקה היא בגישת מבוססת חשבון. בכך המודל מאפשר גמישות גבוהה יותר בנוגע להחלטת הניהול והשליטה במאגר המידע. לדוגמא, ניתן להחליט שמאגר המידע ינוהל על ידי רשת מבוזרת של משתתפי המערכת, רשת מבוזרת של משתתפי המערכת והבנק המרכזי, וכד';
  - ניהול יעיל וגמיש של הרשאות הגישה אל המידע

- ניתן להחליט מה תהיינה הרשאות הגישה של הבנק המרכזי אל המידע, כמו כן גם באיזו טכנולוגיה הדבר יבוצע. למשל, ניתן לוודא שכל גורם במערכת נחשף אך ורק למידע הדרוש לו באמצעות שימוש בגישות מתקדמות של "הוכחה באפס ידיעה" (ZKP), ולהבטיח שלא נעשה שימוש לא הולם במידע.
- הרשאות ספקי התשלום אל יתרת המשתמש – על בסיס כללי מערכת ו/או בכפוף להרשאות משתמש הקצה, ניתן להחליט אם PSP מסוים רשאי יהיה לגשת וליזום תשלומים גם ביתרות שק"ד המקושרות לספקי תשלום נוספים. למשל, משתמש קצה יוכל להחליט לחלק את יתרת השקל הדיגיטלי שלו כך שכל PSP מורשה לפעול רק על אותו חלק של היתרה ש"הוקצה" לו. לחילופין, המשתמש יוכל לפעול דרך PSP מסוים בכל היתרה שלרשותו, גם אם חלקה נמצא תחת תת חשבון / מפתח ציבורי שהוקצה לו על ידי PSP אחר[24].
- ניהול ארנקים נפרדים של משתמש הקצה – הפרדת יתרת המשתמש למספר אינדקסים/תתי חשבונות/מפתחות פרטיים מאפשרת למשתמש הקצה לפצל יתרות בשקל הדיגיטלי לכמה ארנקים ייעודיים. למשל, סכום מסוים בארנק משותף עם בן או בת הזוג. יצוין כי ההפרדה הזו יכולה להתבצע גם על בסיס מספר ארנקים המסופקים על ידי אותו ספק תשלום ולא רק בין ספקי תשלום.

- **פוטנציאל לתרומה חיובית לביצועי המערכת**

בשונה מהמודלים המסורתיים לסליקה מבוססת חשבון, אין תלות בין עדכון היתרה הכוללת של משתמש הקצה לבין היכולת להשלים פעולת סליקה עוקבת עבור המשתמש. האפשרות לטיפול במקביל במספר פעולות סליקה עבור משתמש אחד (בכמה תתי חשבונות למשל) בעלת פוטנציאל לשפר את ביצועי המערכת.

[24] אפשרות זו תורמת ליצירת אקוסיסטם תחרותי אך עשויה להיות בעייתית ומבלבלת מבחינת חוויית המשתמש. בכל אופן, המודל מאפשר אותה.

7. סוגיות נוספות:

7.1 אינטראופרביליות:

סוגיה חשובה בעיצוב הארכיטקטורה המלאה למערכת השקל הדיגיטלי הינה האינטראופראביליות עם:

- מערכות ותשתיות קיימות בשוק התשלומים המקומי ובמשק בכלל;
- מערכת שתאפשר תשלומי אופליין;
- פתרונות שיתגבשו לביצוע תשלומים חוצי גבולות.

בחינה מעמיקה של ההיבטים העסקיים והטכנולוגיים של כל אחד מהנושאים הללו תתבצע בהמשך העבודה של פרויקט השקל הדיגיטלי. בנייר זה נתייחס אליהם אך ורק לטובת הערכה ראשונית של ארכיטקטורה מלאה של מערכת השקל הדיגיטלי, כולל רכיבים ומערכות מולם נדרשת אינטראופראביליות.

אינטראופראביליות נדרשת עם מערכות ותשתיות קיימות

- מערכת זה"ב – סעיף 5.2 בנייר מתאר את מודל ההפצה, במסגרתו תשמש מערכת ה- RTGS לצורך ההתחשבנות בין הבנק המרכזי לבין ה-FI כנגד הנפקה או שריפה של שקלים דיגיטליים[25].
- מתג ה-ATM – לצורך תמיכה של המערכת בפתרון הגנרי להמרת מזומן לשק"ד (ולהפך) המתואר בסעיף 5.4 בנייר, תידרש חיבוריות בין מערכת השק"ד אל מתג ה ATM (במישרין או דרך ה-PSPs).
- מס"ב – חלק מהשירותים שמס"ב מספקת לגופים עסקיים על גבי חשבונות בנק (למשל – שירות תשלום משכורת, שירות תשלום לספקים, וכדומה), יכולים להתקיים גם בשקל הדיגיטלי – משתמש קצה עסקי יכול לבחור לשלם לספקיו או לעובדיו באמצעות שקל דיגיטלי במקום מחשבון או אל חשבון הבנק. עם זאת, ייתכן וחלק מהשירותים המוצעים כיום על ידי מס"ב בחשבונות בנק יוצעו בשקל הדיגיטלי על ידי ספקי תשלום אשר יציעו שירותים מתקדמים ללא התבססות על שירותי מס"ב.
- שב"א – התקשורת בין סולקים ומנפיקים בשוק כרטיסי האשראי מבוססת כיום על המתג של שב"א. סביר להניח כי התקשורת בין ספקי התשלום במערכת השקל הדיגיטלי תתבסס בראש ובראשונה על מערכת השק"ד עצמה, ואולי גם על תשתיות קיימות כגון התשתית הקיימת ל – Open banking API. עם זאת, לא מן הנמנע שבכדי לאפשר למשתמשי הקצה תשלום בבתי עסק על בסיס התשתית הקיימת ל-PoS אשר מחוברים גם אל הקופות של בתי העסק תידרש חיבוריות מסוימת באמצעות הפרוטוקולים הקיימים של שב"א. בנוסף, תיתכן קונפיגורציה בה משתמש קצה יבחר שכרטיס האשראי שלו יחייב את ארנק השק"ד במקום את חשבון הבנק.
- תשתית ה Open banking API – לצורך פעילות תקינה של המערכת נדרשת תקשורת שוטפת גם בין משתתפי המערכת (ראו תיבה 1 לעיל). קישוריות הנדרשת לצורך קיום פעולות מקדימות ו/או משלימות לאלה המבוצעות על גבי פלטפורמת השקל הדיגיטלי יכולה להתבסס על תשתית ה-Open banking API בתנאי שתשתית זו יכולה לתמוך בכך.

פתרון לתשלומי אופליין

בשלב זה לא ברור כיצד יראה פתרון לתשלומי אופליין במערכת השקל הדיגיטלי. עם זאת, ההשפעה של פתרון האופליין הנבחר על עיצוב מערכת האונליין ככל הנראה מוגבלת, ומסתכמת בקיומו של מנגנון המאפשר המרה מאונליין לאופליין,

[25] בטווח הארוך, מערכת השקל הדיגיטלי תוכל לשמש כמטבע דיגיטלי רב תכליתי של הבנק המרכזי, ולשמש גם כ-RTGS.

ולהיפך. לכן, מבחינת הארכיטקטורה ניתן בשלב זה לראות בפתרון האופליין רכיב חיצוני מולו תידרש אינטראופראביליות של המערכת.

עם זאת, נציין כי ישנן שתי גישות קונספטואליות מרכזיות לניהול המידע בנוגע ליתרות האופליין במחזור :

- שיוך יתרת אופליין לכל משתמש קצה – מדובר ביתרה הידועה נכון למועד החיבור האחרון של משתמש הקצה לרשת. סביר להניח שברוב הזמן יתרות המשתמשים המופיעות במאגר המידע לא תייצגנה את יתרות האופליין המדויקות של המשתמשים, מאחר והם ביצעו פעולות בעת שלא היו מחוברים לרשת ולכן הן לא תועדו במאגר. עם זאת, כלל יתרת האופליין של המשתמשים תייצג תמיד בצורה נכונה את היקף שקלים הדיגיטליים במצב אופליין במחזור (יתרה זו משתנה רק במקרה של המרה מאונליין לאופליין או להפך). גישה זו יכולה לסייע בניהול הסיכון שכרוך ביישום פתרון אופליין (טבלה 3).

טבלה 3 – דוגמא לשיוך יתרות אופליין אל משתמשי הקצה

End-user	Online balance	Offline balance	Total
A	100	20	120
B	50	30	80
Outstanding CBDC	150	50	200

As of last online update

- ניהול כלל יתרות ה CBDC באופליין במחזור כמקשה אחת (בדומה ליתרת מזומן במחזור). בגישה זו לא יהיה כל מידע במאגר למעט יתרת האופליין הכוללת. זאת, בדומה למידע הקיים בידי בנק ישראל לגבי יתרת המזומן (טבלה 4).

טבלה 4 – ניהול יתרות האופליין כמקשה אחת

	Online balance	Offline balance
A	100	50
B	50	
Total outstanding	200	

פתרונות לתשלומים חוצי גבולות ב-CBDC

ברמה הקונספטואלית, קיימים מספר מודלים אפשריים להשגת התועלות בנושא של העברות חוצות גבולות משימוש ב-rCBDC. למשל, שימוש במערכת אחת לכמה מדינות (Common platform) או חיבור בין מספר מערכות על בסיס רכיב מקשר (Hub & spoke)[26]. בעת הזו, לא מסתמן כיוון עולמי ברור לגבי האופן בו תוכל להתקיים אינטראופראביליות בין מערכות rCBDC של מדינות שונות.

[26] המודל שמומש בפרויקט Icebreaker

7.2 שירותים מבוססי מאגר מידע מרכזי:

קיומו של מאגר מידע מרכזי במערכת השקל הדיגיטלי יוכל לאפשר יעילות גבוהה יותר באספקת שירותים מסוימים. למשל, הוא יוכל לתמוך במערכת מרכזית בה יוכלו ה-PSPs להיעזר לטובת ביצוע הליכי "הכר את הלקוח", או במערכות לניטור הונאות. למערכות כאלה, בין אם יופעלו על ידי הבנק המרכזי, גורם מטעמו, או על ידי יצירת התשתית הטכנולוגית והרגולטורית שתאפשר תמיכת המגזר הפרטי בשירותים אלה, ייתכנו השלכות עסקיות ורגולטוריות כגון: שיקולי פרטיות, מידת המעורבות רצויה של הבנק המרכזי באספקת השירות, תרומת השירות ליצירת היעילות בשוק, ההתכנות הרגולטורית, ועוד. השלכות אלו יצטרכו להיבחן לפני החלטה על הקמת מערכת כזו בהתבסס על מאגר המידע המרכזי.

7.3 נקודות עיקריות בשכבת ה-Front-end:

בעוד שנייר זה עוסק בעיקר בארכיטקטורה של ליבת המערכת, אביזרי הקצה בהם ישתמשו משתמשי הקצה והאופן בו הם יתחברו למערכת הם חלק בלתי נפרד מהארכיטקטורה של מערכת השקל הדיגיטלי. אביזר קצה (Access Technology) יכלול שני רכיבים מרכזיים:

- User interface – רכיב זה מאפשר זיהוי של משתמש הקצה ומנגיש לו את השימוש בשקל הדיגיטלי.
- Secured container – רכיב זה מאפשר אחסון מידע רגיש של משתמש הקצה, למשל - את המפתח הפרטי, או את הטוקנים לשימוש אופליין. זהו הרכיב שיוזם את הביצוע המאובטח של הטרנסאקציות, לאחר הוראה שניתנה על ידי משתמש הקצה באמצעות ה-user interface.

8. מסקנות והמלצות:

מסמך זה נכתב כחלק מתהליך האפיון של השקל הדיגיטלי. במסגרת התהליך מנתח צוות הפרויקט את הסוגיות השונות[27], וועדת ההיגוי מקבלת החלטות אודות העיצוב המתגבש על בסיס המלצות הצוות. מאחר וקיימת תלות הדדית בין הנושאים השונים, ההחלטות המתקבלות אינן סופיות. עם זאת, ההחלטות מצטברות לכדי מסמך מאפיינים מפורט ומנחות את עבודת הצוות בניתוח הסוגיות השונות. להלן מפורטות ההמלצות להחלטה על בסיס נייר זה.

<u>משתתפי המערכת והחיבוריות ביניהם:</u>

מערכת השקל דיגיטלי תתמוך בהשתתפות אפשרית של משתתפים מ-3 סוגים: ספק שירותי תשלום בשקל הדיגיטלי (DS-PSP)[28], מוסד מנהל חשבון עו"ש (FI) וספק שירותי ערך מוסף אופציונאליים (ASP). עם זאת, ייתכן שתתאפשר פעילות של משתתף הממלא יותר מתפקיד אחד במערכת. למשל, FI הפועל גם כ PSP;

- המערכת תתמוך בהשתתפות של מנהלי חשבונות עו"ש (FI) מסוגים שונים, בין אם הם מחוברים למערכת ה RTGS ובין אם לא;
- פעילותו של משתתף מסוג ASP על בסיס הפונקציונאליות המוצעת במערכת השק"ד תוגבל למספר מצומצם של פעולות, תוך חתירה למצב בו הנטל הרגולטורי והטכנולוגי על משתתף מסוג זה יהיה הנמוך ביותר מבין משתתפי המערכת;
- המערכת תעוצב באופן שישאף ככל שניתן לבסס את התקשורת הנדרשת בין משתתפי המערכת לטובת פעילות מקדימה או משלימה לזו המבוצעת על בסיס פלטפורמת השקל הדיגיטלי (ברור יתרה בחשבון FI לפני פעולת טעינה, הפעלת מנגנון Waterfall במקרה של פעולה הגוררת חריגה ממגבלת ההחזקה, וכד') על בסיס התשתיות הקיימות (והעתידיות) להתקשרות בין גופים במערך התשלומים, למשל, Open banking API. עם זאת, ככל שיימצא כי הערוצים הקיימים לא מאפשרים את הפונקציונאליות והיעילות הנדרשת בהתקשרות זו, תיבחנה חלופות נוספות (שיפור התשתיות הקיימות והתאמתן לצורכי מערכת השק"ד, תקשורת באמצעות פלטפורמת השק"ד , וכד').

<u>מודל ההפצה:</u>

- בנק ישראל יבצע שימוש במודל ההפצה העקיף להפצת שקלים דיגיטליים. בהתאם לכך, ההפצה לציבור הרחב תבוצע באמצעות FIs ;
- מערכת השקל הדיגיטלי תתמוך בפתרון אוניברסלי לביצוע הליך ההמרה בין מזומן לשק"ד ולהפך, וללא תלות במעבר דרך חשבון הבנק של משתמש הקצה או בקיומו של חשבון בנק בכלל. הספים לשימוש בפתרון האוניברסלי יצטרכו להיקבע תוך התחשבות בסוגיות העסקיות והרגולטוריות השונות; עם זאת, המערכת תוכל לתמוך גם בפעולת המרה המבוססת על הליך דו שלבי של הפקדה או משיכה של מזומן למול חשבון הבנק של משתמש הקצה, ולאחר מכן פעולת טעינה או פדיון כנגד הכסף בחשבון.

<u>עקרונות בעיצוב שכבת ה Back-end:</u>

- שכבת ה – "Back-end" תעוצב תוך הבחנה ברורה בין מנוע הסליקה לבין מאגר המידע הרחב היותר יותר, לגביו יוכל להחליט הבנק המרכזי אם לנהלו וכיצד;
- המערכת תתמוך בקונפיגורציה לפיה בברירת המחדל, המידע המועבר מהמשתתפים אל הבנק המרכזי לצורך טיפול בפעולה בשקל הדיגיטלי יהיה המידע המינימלי הנדרש לבנק המרכזי לביצוע הסליקה;

---

[27] לרשימת הנושאים המנותחים במסגרת תהליך העיצוב ראה:
Bank of Israel: Where we stand with the digital shekel project – Yoav Soffer

[28] ייתכן גם PSP שהינו משתתף עקיף. כלומר, לא מחובר באופן ישיר אל המערכת.

- המערכת תתמוך גם בהרחבה אפשרית לפיה יוכל הבנק המרכזי להחליט כי לצורך תפעולה התקין של המערכת או לטובת צרכים סטטיסטיים, המסר המתקבל מספק התשלום יכלול גם מאפיינים נוספים של העסקה או של המשתמש, ובלבד שאלה לא יוכלו לשמש לחשיפת זהות המשתמש;
- מאפייני מאגר המידע המרכזי:
  - הגורם הבלעדי בעל הרשאות לבצע שינוי בבסיס המידע הינו הבנק המרכזי, בעוד שלמשתתפים מהמגזר הפרטי תתאפשר גישה אל בסיס המידע לקריאה בלבד, בהתאם להרשאות משתמש הקצה וכללי המערכת;
  - מבנה המידע המרכזי יכלול עבור כל משתמש במערכת מזהה ייחודי, ואת כלל תתי החשבונות או האינדקסים המשויכים אליו, יחד עם הערך הזמין לשימוש בכל אינדקס ובסך הכל.

<u>אינטראופראביליות ושירותים מבוססי מאגר מידע מרכזי:</u>

- מערכת השק"ד תעוצב תוך התחשבות באינטראופראביליות הנדרשת לכל הפחות עם המערכות והתשתיות הבאות: מערכת זה"ב, מתג ה ATM , מס"ב, שב"א ו-Open banking API;
- פתרון האונליין במערכת השק"ד יפותח תוך התחשבות בצורך למעבר בין יתרת אונליין לאופליין ולהפך על ידי משתמש הקצה (בהתאם לפתרון האופליין שימומש).
- במסגרת עיצוב המערכת תובא בחשבון גם האפשרות לאספקת שירותים מסוימים על בסיס שימוש במאגר המידע המרכזי.

ביבליוגרפיה

בנק ישראל (2021). "שקל דיגיטלי של בנק ישראל תועלות אפשריות, טיוטת מודל וסוגיות לבחינה". ירושלים: בנק ישראל.

Bank of England (2023): " The digital pound: a new form of money for households and businesses?", Consultation Paper, February.

BIS (2022): "A Prototype for Two-tier Central Bank Digital Currency (CBDC)", Project Aurum, October.

BIS (2023a): "An accessible and secure retail CBDC ecosystem", Project Sela, September.

BIS (2023b): "Breaking new paths in cross-border retail CBDC payments", Project Icebreaker, March.

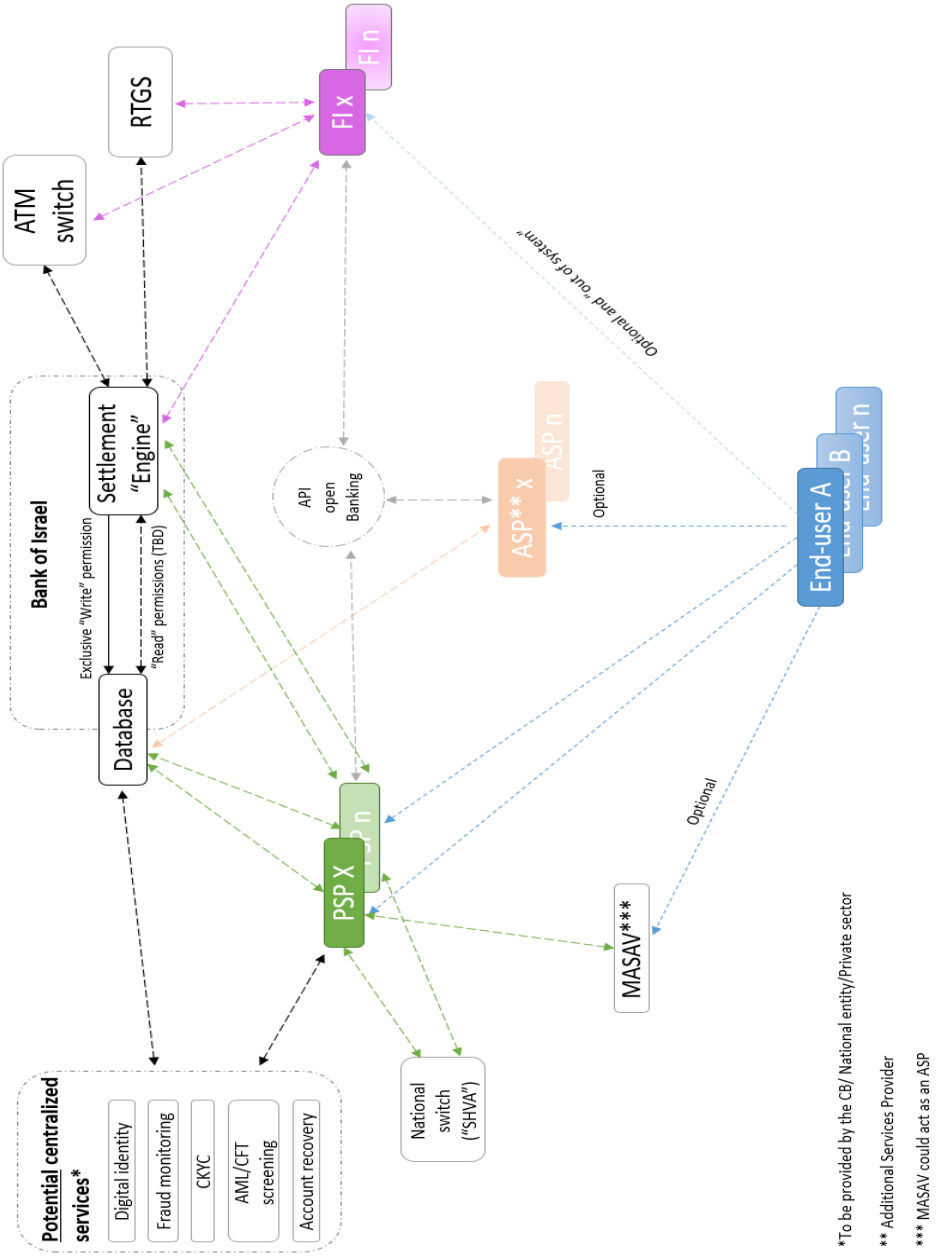
BIS (2023c): “Project Rosalind: developing prototypes for an application programming interface to distribute retail CBDC”, Final report, June.

ECB (2023): "Digital euro – Prototype summary and lessons learned", May.

Sveriges Riksbank (2022): "E-Krona pilot – Phase 2", April.

נספח 1 - קונפיגורציה אפשרית לארכיטקטורה לוגית מלאה למערכת השק"ד

איור 18: ארכיטקטורה לוגית מלאה

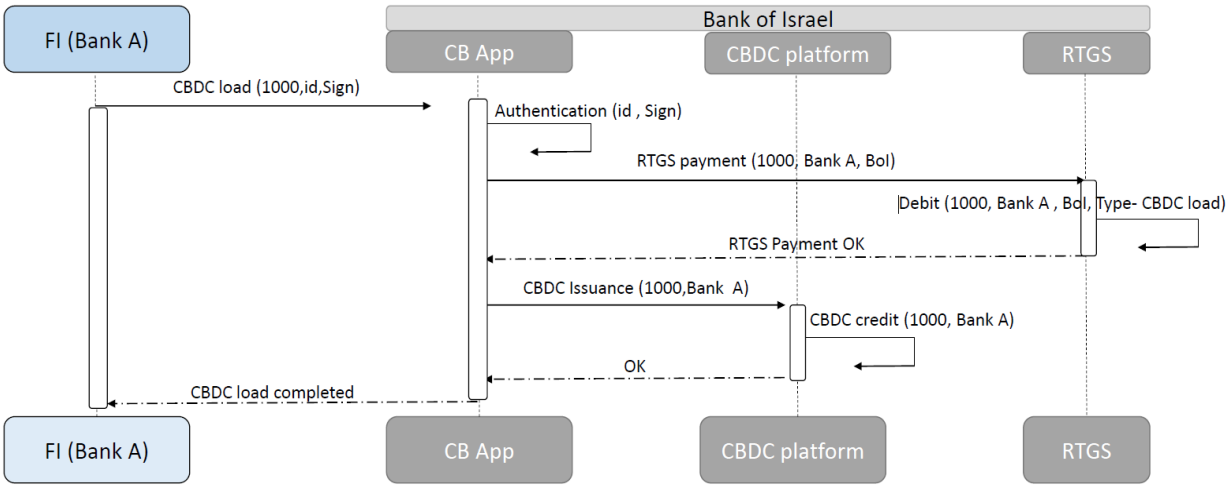


נספח 2 - תרשימי רצף להפצה של השקלים הדיגיטליים במודל עקיף

איורים 19.1 ו- 19.2 מציגים את רצף ההליכים העסקיים הנדרשים לצורך תמיכה בפעולת טעינה של ארנק השקל הדיגיטלי של משתמש קצה שהינו גם לקוח של FI אשר מחובר באופן ישיר אל מערכת ה RTGS ומחזיק ארנק שקלים דיגיטליים (קונפיגורציה A בסעיף 3 לעיל).

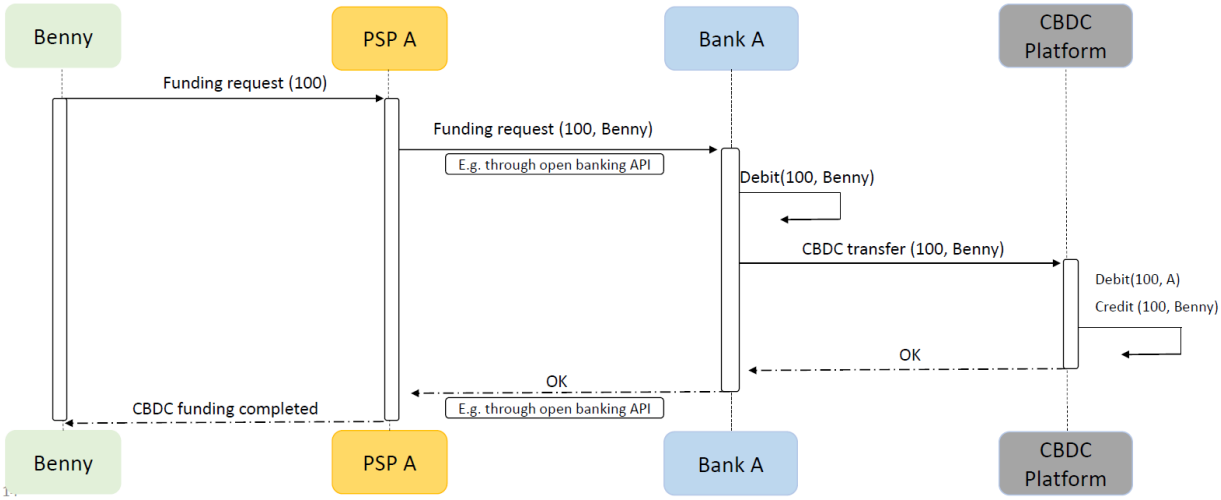
איור 19.1: רכישת שקלים דיגיטליים על ידי "Bank A"

בשלב הראשון ה- FI מבצע רכישה של שקלים דיגיטליים כנגד יתרה בחשבון ה RTGS שלו:



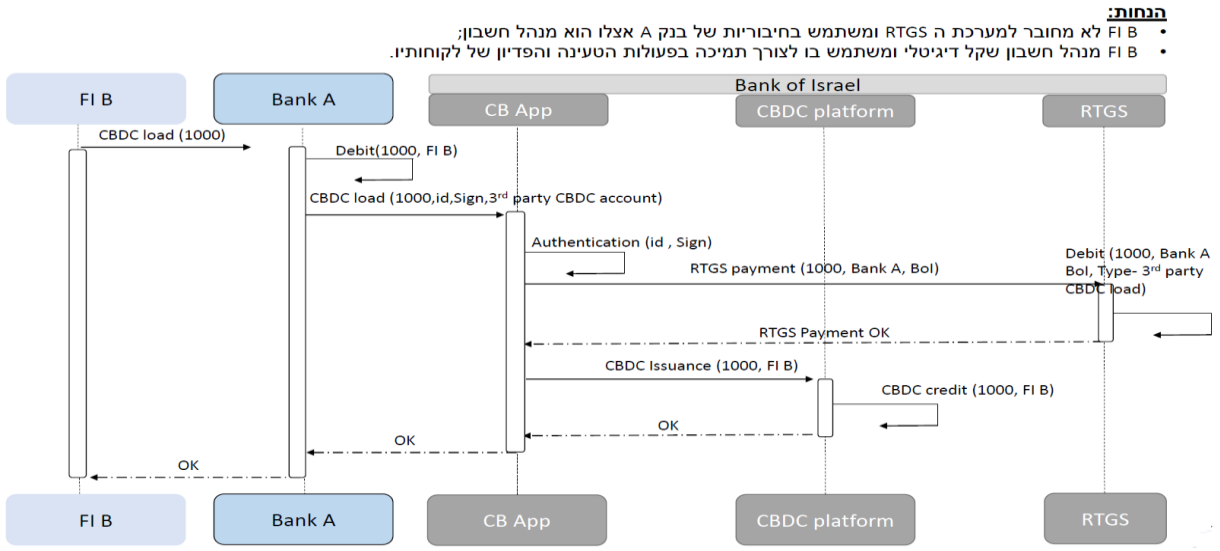
איור 19.2: טעינת שקלים דיגיטליים על ידי לקוח של "Bank A"

כעת נניח שבני הוא לקוח של "PSP A" והוא מבקש לבצע טעינה של 100 שקלים דיגיטליים כנגד חיוב חשבון הבנק שלו ב- "Bank A" (המקושר לארנק):



איור 20 להלן מציג את רצף ההליך העסקי במסגרתו יוכל FI הפועל בקונפיגורציה B (בטבלה המופיעה בסעיף 3 לעיל) לרכוש שקלים דיגיטליים בכדי לתמוך בפעולת הטעינה של לקוחותיו.

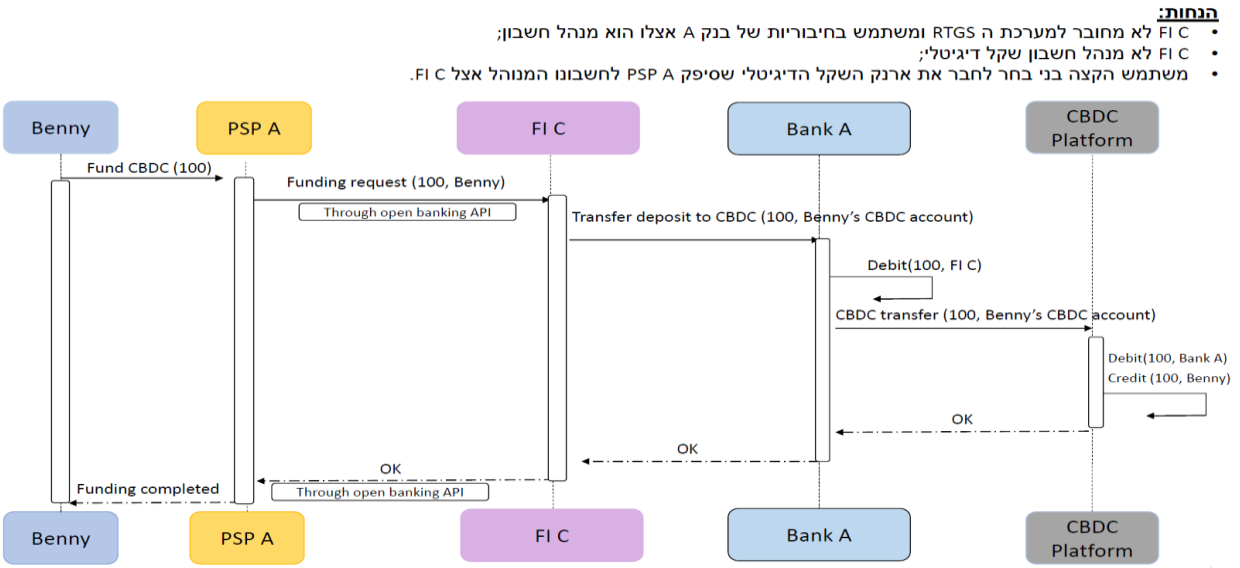
איור 20: רכישת שקלים דיגיטליים על ידי FI שאינו מחובר למערכת ה RTGS ("FI B")



לאחר ש "FI B" רוכש את השקלים הדיגיטליים הוא יוכל לתמוך בפעולת הטעינה והפדיון עבור לקוחותיו בדיוק כמו בנק A בתרשים 19.2.

איור 21 להלן מציג את ההליך העסקי במסגרתו יוכל FI הפעול בקונפיגורציה C (בטבלה המופיעה בסעיף 3 לעיל) לתמוך בפעולת הטעינה ללקוחותיו גם ללא החזקה של "מלאי" שקלים דיגיטליים.

איור 21: טעינת שקלים דיגיטליים על ידי לקוח של FI שאינו מחזיק בשקלים דיגיטליים ("FI C")



* תרשימי הרצף (ה- "Sequence diagrams") אשר מוצגים במסמך זה נועדו להמחשה בלבד ואינם משקפים עיצוב סופי של ההליך העסקי והטכנולוגי.