



אתגר השקל הדיגיטלי



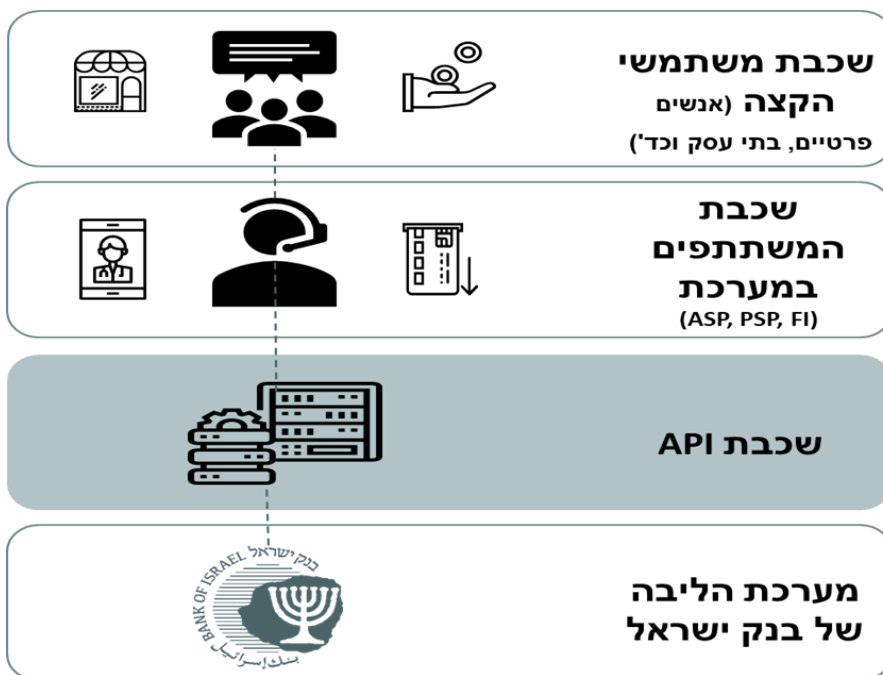
מסמך מלווה לקול קורא

מסמך זה מפורסם בצמוד ל"מסמך הקול הקורא" המופיע [בדף האינטרנט של אתגר השקל הדיגיטלי](#) ומטרתו לספק מידע משלים על אתגר השקל הדיגיטלי למתמודדים פוטנציאליים.

1. במה יתמקד האתגר?

האתגר יתמקד בממשק שבין מערכת הליבה של השקל הדיגיטלי המנוהלת על ידי הבנק המרכזי לבין משתתפי המערכת (אותם ייצגו המתמודדים באתגר). המתמודדים ידרשו להשתמש בשכבת ה APIs אשר תוגש על ידי בנק ישראל, וליישם את הפונקציונליות שלה על תרחיש השימוש (use case) אותו יבחרו להציע באתגר. האתגר לא יערב משתמשי קצה "אמיתיים" - אלה ידומו על ידי המתמודדים עצמם.

איור 1: הרבדים השונים במודל הדו-נדבכי והמיקוד באתגר





אתגר השקל הדיגיטלי



2. שכבת המשתתפים במערכת השקל הדיגיטלי

החזון המתגבש בבנק ישראל בנוגע לשכבת המשתתפים במודל הדו נדבכי במערכת השקל הדיגיטלי כולל 3 סוגי גופים, לכל אחד מהסוגים פונקציונאליות שונה במערכת:

2.1. ספקי שירותי התשלום (ה "DS-PSPs")

גופים אלה יהיו האחראים ליצירת הגישה הטכנולוגית של משתמשי הקצה אל מערכת השקל², 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".

התקשרות משתמש הקצה מול משתתף מסוג זה הכרחית לצורך פעילותו במערכת השקל הדיגיטלי בהתאם להנחת המודל הדו-נדבכי למערכת.

דגשים והנחות לסוג משתתף מסוג זה באתגר

- ה DS-PSP יתמוך בהליך ההצטרפות של משתמש הקצה אל המערכת, ויעמיד ממשק משתמש עבור משתמש הקצה, על בסיס יוכל להציע למשתמש הקצה את כלל הפונקציונאליות המתאפשר על בסיס שכבת ה APIs ;
- לטובת הפשטות, ההנחה באתגר הינה כי כל ארנק משויך רק ל DS-PSP אחד בזמן נתון.³

2.2. מוסדות המנהלים חשבונות עו"ש ("FIs⁴") - גופים פיננסיים המנהלים עבור הציבור חשבונות עו"ש בכסף שאינו השקל הדיגיטלי (בנקים מסחריים, בנק הדואר, אגודות פיקדון ואשראי, גופים למתן שירותים בנקסי פיננסי, וכדומה) ויצטרכו לאפשר פעולת המרה עבור משתמשי הקצה מהחשבונות אותם הם מנהלים, או ממזומן, אל השקל הדיגיטלי ולהיפך.

¹ Digital Shekel Payment Services Provider

² ייתכנו גם ספקי תשלום עקיפים אשר אינם מחוברים אל המערכת באופן ישיר ומספקים שירותי שקל"ד על בסיס חיבוריות אל ספק תשלום המחובר אל המערכת

³ מדובר בהנחה מפשטת לטובת הניסוי אשר איננה משקפת את חזון בנק ישראל לגבי אקוסיסטם תחרותי ופתוח במערכת השקל הדיגיטלי.

⁴ Funding Institutions



אתגר השקל הדיגיטלי



דגשים והנחות לסוג משתתף מסוג זה באתגר

- האתגר לא עוסק בפונקציונאליות המלאה הנדרשת ממשתתף מסוג זה בהתאם למודל ההפצה העקיף לשקלים דיגיטליים המסתמן בפרויקט⁵ ומתמקד בתפקידו לתמוך בפעולת טעינה או פריקה של שקלים דיגיטליים;
- קיומו של משתתף מסוג זה הכרחי לצורך תמיכה באפשרות טעינה ופריקה של משתמשי הקצה כבסיס לתרחישי השימוש השונים שיוצעו על ידי המשתתפים. לכן, לצורך הבטחת פונקציונאליות זו באתגר, ידמה צוות אתגר השקל הדיגיטלי מספר FIs אשר יוכלו לשמש את ה DS-PSPs שיקימו המתמודדים השונים לביצוע פעולות טעינה ופדיון בארנקי משתמשי הקצה.
- עם זאת, ככל שמתמודד מסוים יבחר לפעול כ- FI עבור לקוחותיו לצד תפקידו כ- DS-PSP הוא יוכל לעשות כן.

2.3. **ספקי שירותים מתקדמים נוספים** ("ASPs"⁶) - גופים אלה יוכלו לספק שירותים נוספים אופציונליים למשתמשי הקצה, כגון: ניהול תקציב, שירותי אנליזה לבתי עסק, שירותי ניטור הונאות, וכדומה. בנוסף, הם יוכלו לקחת חלק באספקת שירותי תשלומים מותנים מתקדמים. למשל, הם יוכלו לשמש כצד שלישי האחראי על שליחת ה"טריגר" לנעילה או לשחרור של כספים בעסקת תשלום מותנה.

דגשים והנחות לסוג משתתף זה באתגר

- ההנחה באתגר היא שמשתתף מסוג ASP יוכל לפעול ישירות מול מערכת הליבה בבנק המרכזי (באמצעות שכבת ה APIs) עבור משתמשי הקצה שהתקשרו מולו (בעוד שבמציאות ייתכן ויוחלט כי גישה זו תוגבל לגישה דרך DS-PSP המשרת את הלקוח);
- הרשאות של ASP מוגבלות לסט מצומצם של APIs ביחס ל DS-PSP (כפי שמפורטים בנספח). למשל, משתתף מסוג ASP לא יוכל ליזום פעולת תשלום ישירות מול הבנק המרכזי בשם משתמש הקצה.

⁵ להרחבה ראה פרק 5 במסמך הארכיטקטורה הלוגית למערכת השקל הדיגיטלי. האתגר מניח נקודת מוצא בה ה FIs מחזיקים יתרת שקלים דיגיטליים על בסיס התחשבנות מקדימה ב RTGS בין ה FI או הגורם המייצג אותו ב RTGS ובנק ישראל.

⁶ Additional Services Providers



אתגר השקל הדיגיטלי

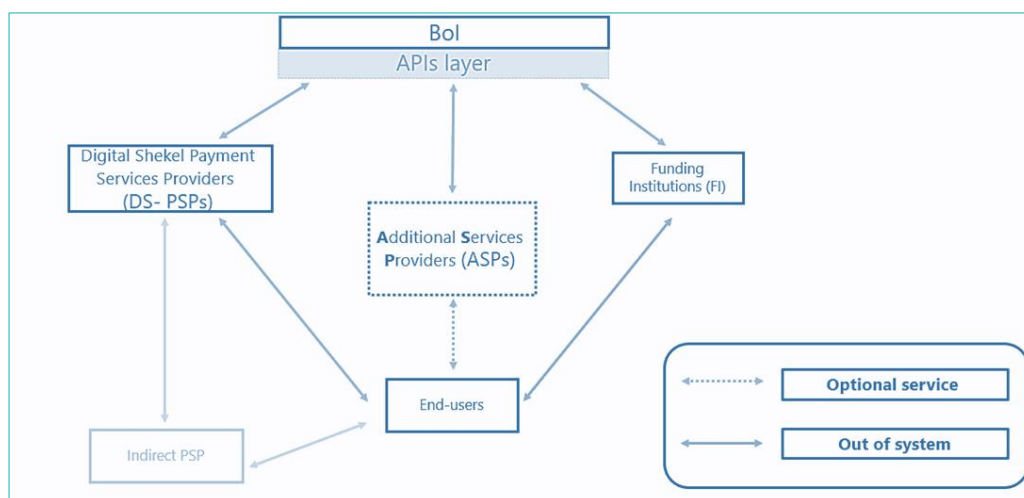


הנחת העבודה בפרויקט השקל הדיגיטלי היא כי חלק מהגופים אשר ישתתפו במערכת השקל הדיגיטלי יבחרו לפעול במערכת השקל הדיגיטלי בתפקיד בודד (למשל רק כ DS-PSP) וחלק אחר יבחר להשתתף ביותר מתפקיד אחר (למשל, גם כ FI וגם כ DS-PSP, או גם כ-ASP).

עבור כל מתמודד שייבחר להשתתף באתגר יוגדרו (כברירת מחדל) הרשאות לפעול ב Sandbox כשני DS-PSPs⁷ שונים וגם כ- ASP⁸ לצורך בחינת הפונקציונאליות המוצעות למשתתף מסוג זה ויכולת תמיכתו במקרי שימוש חדשניים.

כמו כן, יתאפשר למתמודד לקבל גם ארנק משתתף מסוג FI לצורך תמיכה בפעולות הטעינה והפדיון של משתמשי הקצה המקבלים ממנו שירות כ- DS-PSP.

איור 2: סכמת השקל הדיגיטלי



3. איזה החלטות עיצוביות והנחות מרכזיות חשוב להכיר?

- 3.1. השקל הדיגיטלי כמטבע דיגיטלי קמעונאי (Retail CBDC) מונפק על ידי הבנק המרכזי ומייצג התחייבות ישירה של הבנק המרכזי מול המשתמשים;
- 3.2. השקל הדיגיטלי ניתן להמרה ביחס של 1:1 להתחייבות של בנקים מסחריים או מזומן;

⁷ לצורך דימוי מיטבי של ה- Use cases עם מעורבות של יותר מ DS-PSP. למשל, עסקה סינכרונית המשלבת Request to Pay

⁸ לצורך בחינת הפונקציונאליות המוצעות למשתתף מסוג זה ויכולת תמיכתו במקרי שימוש חדשניים



אתגר השקל הדיגיטלי



- 3.3. תפקיד ספקי התשלום במערכת השקל הדיגיטלי (ה DS-PSP) אינו מוגבל רק לגופים שפועלים כיום כבנקים או כמוסדות פיננסיים⁹;
- 3.4. פעולות בין משתמשים בשקל הדיגיטלי מבוצעות בזמן אמת על גבי מערכת הבנק המרכזי, ללא ביצוע התקזזות ("Netting");
- 3.5. פרטים מזהים של משתמשי הקצה במערכת ומידע מורחב בנוגע לטרנזקציה לא יהיו חשופים לבנק המרכזי;
- 3.6. המערכת שיעמיד בנק ישראל באתגר לא תספק את היסטוריית הטרנזקציות של המשתמשים. אלו ינוהלו על ידי המשתתפים;
- 3.7. לא יוחלו מגבלות על יתרות ופעולות בשקל הדיגיטלי במסגרת האתגר.

4. מהם ה APIs אשר יוגשו על ידי הבנק המרכזי?

במסגרת האתגר בנק ישראל יגיש למשתתפים APIs לפונקציונליות שונות: לתפעול ארנק, לביצוע עסקאות על ידי המשתמש, לתכנות פעולות תשלום מתקדמות, ולחיבור ASP לארנק השקל הדיגיטלי.

5. דוגמאות לתמיכת APIs בתרחישי שימוש חדשניים:

המשתתפים באתגר יתבקשו לפתח טכנולוגית את הפתרון למימוש תרחישי השימוש החדשניים שיוצעו על ידם תוך שימוש בשכבת ה APIs אשר תפותח על ידי הבנק המרכזי - תרחישי השימוש יכולים להציע פתרון לבעיות קיימות או עתידיות בשוק. להלן שתי דוגמאות לתרחישי שימוש המבוססים על פונקציונליות שכבת ה APIs (רשימה מלאה של ה-APIs מופיעה בנספח):

- 5.1. ארנק ילדים מפוקח על ידי הורה - אפשרות החיבור של ארנקים משניים לארנק מרכזי ראשי ("OpenSubWallet") תוכל לתמוך בצורך העסקי של ארנקי ילדים המקושרים לארנק ראשי (למשל של ההורה), לאפשר להורה לפקח אחר ארנק המשנה של הילד, להחליט להקפיא ("Freeze") או להשבית באופן זמני ("Disable") את פעילות הארנק.

⁹ עם זאת, חשוב לציין כי משתתפים במערכת השקל הדיגיטלי יהיו נתונים לרגולציה, פיקוח ואסדרה אשר יקבעו בהמשך



אתגר השקל הדיגיטלי



5.2. Delivery vs. Payment (DvP) – תרחיש שימוש בו מתבצעת הזמנה של סחורה והתשלום יתבצע, באופן חלקי או במלואו, רק כנגד מסירת החבילה על ידי חברת שליחויות. במקרה זה, נוכל להניח כי מעורבים ספקי תשלום (של המשלם ושל המוטב) וחברת השליחויות המספקת שירותים למוטב פועלת גם כ ASP במערכת השקל הדיגיטלי. לצורך כך תבוצע נעילה בה מעורבים 3 גורמים ("ThreePartyLock") וברגע שהחבילה הועברה בפועל אל היעד שלה תוכל חברת השליחויות לממש את הנעילה ("DrawDownLock"). כתוצאה מכך, תבוצע העברה מלאה של הסכום הנעול אל המוטב, במידה וכל תנאי העסקה התקיימו, או העברה חלקית במידה והתנאים לא התקיימו במלואם.

6. במה לא יעסוק האתגר?

האתגר כאמור מתמקד בפונקציונאליות הטכנולוגית המונגשת על ידי הבנק המרכזי ויכולתה לתמוך במקרי השימוש השונים בדגש על החדשניים שביניהם. האתגר לא יתמקד בסוגיות נוספות כגון: פרטיות¹⁰, איסור הלבנת הון ומימון טרור (CFT / AML), ותשלומים לא מקוונים.

7. דרישות טכנולוגיות

למתמודדים אשר יבחרו מבין כלל הפונים יסופק בהמשך מסמך טכני מפורט. על מנת להתמודד בהצלחה באתגר, נדרש שיהיו בצוות המתמודד היכולות הטכנולוגיות הבאות:

7.1. פיתוח בשפות שמאפשרות שימוש ב APIs ועבודה עם כלים שמאפשרים זאת כמו Postman.

7.2. RESTful APIs: הבנה של עקרונות ומתודולוגיות של REST, כולל פעולות HTTP כמו Get, Post, Delete.

7.3. Json / Xml: יכולת לעבוד עם פורמטים נפוצים להעברת נתונים.

7.4. הכרות עם פרוטוקולי תקשורת מקובלים במערכות תשלומים כגון ISO20022

7.5. אבטחת מידע: הבנה של עקרונות אבטחת מידע והצפנה א-סימטרית להגנה על תעבורת נתונים.

¹⁰ התשתית הטכנולוגית בפרויקט אומנם מאופיינת לתמיכה ברמה גבוהה של פרטיות מובנית ("Privacy by Design") למשל על ידי האפשרות להצפנת מסרים שיועברו על גבי תשתית הבנק המרכזי בין משתתפים אך האתגר איננו עוסק בהיבטים נוספים הקשורים לפרטיות כגון: מבנה המידע בבנק המרכזי, עסקאות אנונימיות וכד'



אתגר השקל הדיגיטלי



נספח רשימת ה- APIs

נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
ארנק	ניהול ארנק	Open	פתיחת ארנק ראשי של שקל דיגיטלי במערכת הליבה בבנק ישראל (ארנק פרטי או עסקי).	הליך חיבור (Onboarding) של משתמש קצה אל המערכת (על ידי DS-PSP) יכול להקמת ארנק עבור משתמש הקצה במערכת.
		OpenSubWallet	פתיחת ארנק משני מקושר לארנק הראשי.	מאפשר למשל הקצאת יתרה מסוימת מיתרת השקל הדיגיטלי למטרה מסוימת: ארנק לילד, הקצאת יתרה לפעילות משותפת של בני זוג או שותפים, ארנק ליחידה עסקית בחברה, ועוד.
		Disable	השבתה זמנית של פעילות הארנק (ראשי או משני)	לאחר ההשבתה, לא תתאפשר כל פעילות בארנק, ולא



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
			במערכת השקל הדיגיטלי.	ניתן יהיה לבצע או לקבל בו תשלומים.
		Freeze	הקפאת הפעילות של ארנק ראשי או משני.	לאחר ההקפאה, עדיין יתאפשר לשלם אל הארנק המושבת, אך לא ממנו. למשל לצורך תמיכה ביכולת הפיקוח של ארנק ראשי על ארנק משני (הורה וילד) או תמיכה ביכולת ההגנה על הארנק במקרה של חשש לאבדן או גניבה של אמצעי הגישה.
		Enable	ביטול השבתה זמנית או הקפאה של ארנק ראשי או משני.	
		Close	סגירת הארנק הראשי או המשני במערכת הליבה של הבנק המרכזי.	בשונה מ-freeze או disable, פעולה זו איננה זמנית. לאחריה, אם משתמש הקצה ירצה לחזור לפעול



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
	ניהול מזהה ייחודי ללקוח (Alias)	Alias	יצירת מזהה אלטרנטיבי (Proxy) לארנק השקל הדיגיטלי של המשתמש	בשקל הדיגיטלי, יידרש הליך חיבור חדש.
		DeleteAlias	מחיקת מזהה אלטרנטיבי מהארנק של המשתמש.	
		LookUpAlias	חיפוש פרטי ארנק לפי מזהה אלטרנטיבי.	כאשר משתמש קצה מעוניין לבצע תשלום הוא מוסר ל-DS-PSP את ה-Alias של המוטב. באמצעות API זה ה-DS-PSP מאתר את כתובת הארנק של המוטב.
		ConnectFI	חיבור הארנק לגוף מסוג FI - הם גופים המנהלים חשבונות עו"ש לציבור מחוץ למערכת השקל הדיגיטלי	חיבור הארנק באתגר לגוף מסוג FI (אשר ידומה על ידי צוות האתגר או על ידי המתמודד) הכרחי בכדי לתמוך
	הגדרת FI			



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
			ויאפשרו ללקוחותיהם להמיר כסף מהיתרה בחשבון המנוהל על ידם לשקל דיגיטלי (פעולת טעינה, funding) ולהיפך (פעולת פריקה, defunding)	בפעולת הטעינה והפריקה מהארנק.
		DisconnectFI	ניתוק ארנק מגוף מסוג FI	למשל, במידה ומשתמש הקצה החליף את חשבון הבנק שלו, והוא מעוניין לנתק את הארנק מחשבון הבנק הישן ולחברו לאחר מכן לחשבון החדש.
		Balance	שחזור סך היתרות של ארנק מסוים	
יתרות		AvailableBalance	הצגת היתרה הזמינה לשימוש בארנק מסוים	היתרה הכוללת בניכוי יתרה נעולה.



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
עסקאות	תשלום (Credit) (Transfer)	Pay	העברת שקל דיגיטלי מארנק אחד לשני	
		SplitPay	העברה מפוצלת- מארנק אחד למספר ארנקים שונים.	
	בקשת תשלום	RequestToPay	בקשת תשלום של ארנק המוטב מהארנקים המשלמים	
		Authenticated RequestToPay	מאפשר ל-DS של PSP מקבל התשלום לכלול חבילת אימות עם הבקשה לתשלום כך שה DS-PSP של המשלם יוכל לאשר את הבקשה ללא פניה אל משתמש הקצה.	למשל, לתשלום בנקודות מכירה (PoS) או למצב בו המשלם מעניק למוטב הרשאה לחיוב החשבון (נניח, לתשלומי חשבון תקופתי לחברות תשתית)



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
	טעינה ופריקה	Fund	המרה של כסף דיגיטלי שאינו מייצג התחייבות של הבנק המרכזי (למשל, עו"ש 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.	פעולה זו תבוסס על העברה של שקלים דיגיטליים מארנק משתתף מסוג FI אל ארנק משתמש הקצה (כנגד חיוב חשבון משתמש הקצה מול ה FI – מחוץ למערכת השקל הדיגיטלי)
		Defund	הפעולה ההפוכה לפעולת הטעינה – המרה של שקל דיגיטלי לכסף דיגיטלי אחר או למזומן	תבוצע על ידי העברה של שקלים דיגיטליים מארנק משתמש הקצה אל ארנק ה FI (כנגד זיכוי של חשבון המשתמש מול ה FI – מחוץ



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
				למערכת השקל (הדיגיטלי)
תכנותיות (Programmability)	הגדרת נעילות (כלל) הנעילות מוגבלות לפרק זמן מסוים בכדי למנוע נעילה פרמננטית)	RequestToLock	בקשה לנעילה של יתרה בארנק של משתמש קצה על בסיס אחת משלוש הנעילות המתוארות בהמשך.	מסר זה ישלח מה PSP של המוטב הפוטנציאלי אל ה PSP של המשלם הפוטנציאלי ויכלול את הנתונים הנדרשים בהתאם לסוג הנעילה (סוג נעילה, סכום, הגורם המוסמך לבטל או לממש את הנעילה ועוד)
		TwoPartyLock	נעילת סכום של שקל דיגיטלי בארנק המשלם - הטריגר למימוש או ביטול הנעילה ישלח על ידי ה PSP של הצד המוטב	



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
		ThreePartyLock	פונקציונאליות זו מאפשרת מעורבות של גורם שלישי (שאינו ה PSP של המשלם או המוטב) - הטריגר למימוש או ביטול הנעילה ישלח על ידי הגורם השלישי. למשל, ASP המספק שירותים לצד המוטב ויזום את פעולת הנעילה מול ה PSP של הצד המשלם.	דוגמא לשימוש בפונקציונאליות זו- חברת שליחויות שיכולה לוודא שהחבילה הגיעה אל המוטב ולממש את התשלום כנגד המסירה.
		HTLCLock	נעילת שקל דיגיטלי על בסיס מנגנון Hash) HTLC Time Lock (Contract - הטריגר למימוש הנעילה והשלמת הטרינסאקציה	API זה יכול לשמש למשל להבטחת תשלום בשקל הדיגיטלי כנגד העברת נכס דיגיטלי כלשהו ברשת אחרת



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
	ביטול ומשיכה של נעילות		בין הצדדים יבוסס על שימוש ב "Secret" (בהתאם למקובל במנגנוני HTLC).	
		CancelLock	ביטול נעילת שקלים דיגיטליים שהוגדרה בעבר.	למשל, במידה והצדדים מחליטים לבטל את העסקה שבגינה בוצעה הנעילה
		DrawDownLock	מימוש של נעילה מסוג Two/Three party והעברה חלקית או מלאה של סכום הנעילה אל המוטב	יבוצע על ידי המשתתף שאחראי לאשר שהתנאים בעסקה התקיימו וניתן להעביר את התשלום
		DrawDownHTLC	מימוש של נעילה מסוג HTLC והעברה מלאה של סכום הנעילה אל המוטב	על ידי שימוש ב "Secret"



אתגר השקל הדיגיטלי



נושא	תת-נושא	שם ה API	תיאור	הסבר נוסף
	מידע בנוגע לנעילות	LockbyLockID	קבלת מידע על נעילה ספציפית בהתבסס על ה Lock ID	למשל, כדי לעדכן את משתמש הקצה לגבי הכסף שהוא נעל בעסקה מסוימת
		LockbyPSP	קבלת מידע על כלל הנעילות הקיימות בארנקי לקוחות של ה PSP המבקש	
		LockbyWallet	קבלת מידע על כלל הנעילות הפעילות בארנק	למשל, כדי לעדכן את משתמש הקצה לגבי כלל הכסף שהוא נעל בכל העסקאות הפתוחות אצלו
	חיבור ASP לארנק השקל הדיגיטלי	ConnectASP	חיבור לארנק גוף מסוג ASP אשר מספק שירותים נוספים אופציונאליים למשתמשי הקצה	שירותים פוטנציאליים: ניהול תקציב, שירותי אנליזה לבתי עסק, שירותי ניטור הונאות, יישומי תשלום חדשניים, וכד'
		DisconnectASP	ניתוק גוף מסוג ASP	



אתגר השקל הדיגיטלי



זמין גם למשתתף מסוג ASP