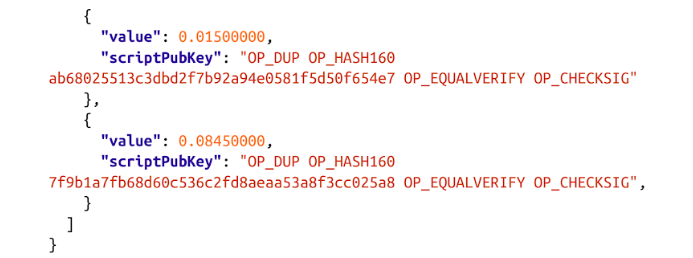
שאלות:

1. בהנתן העברה:



1. חשב את סכום העמלה.
2. כמה סטושי הועברו בעסקה?

מספר העברה:

[7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18](https://www.blockchain.com/btc/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18)

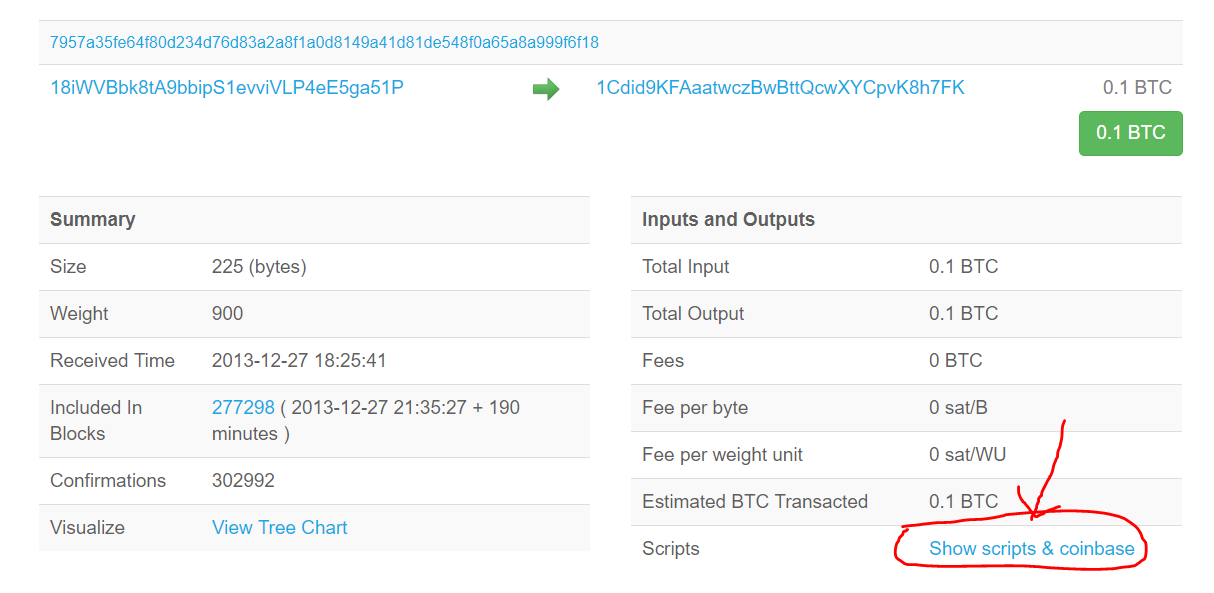
1. כתוב סקריפט המחבר 2 מספרים. תאר בכל שלב במהלך הריצה את מצב המחסנית
2. כתוב סקריפט המחזיר את תוצאת החישוב של כך שהסקריפט מתחיל כך:

יש לוודא ש (במקרה שb הוא 0 נקבל שגיאה ועצירה ולא אינסוף).

1. כתוב סקריפט המחזיר את תוצאת החישוב של כך שהסקריפט מתחיל כך:

יש לוודא ש (במקרה שb הוא 0 נקבל שגיאה ועצירה ולא אינסוף).

1. התבוננו בהעברה כלשהי, כנסו לסקריפט והראו בסימולטור שהסקריפט אכן נותן תוצאה טובה (true). איזה סקריפטים צריך לצמד כדי שיעבדו?



1. כיתבו סקריפט שמבקש מספר חתימות.
2. כאמור, בהעברה של חלק מסכום הביטקוין, שאר הUTXO צריך להיות מועבר חזרה אל כתובת בארנק – בארנקים מתקדמים ואפליקציות הארנק מבצע את ההעברה הזאת אוטומטית (שולח ל2 כתובות – לנמען ולמען).

אם כתבתי בעצמי את ההעברה ושכחתי להוסיף את כתובת הארנק ליתרה – מה יקרה לשאר הכסף?

1. אליס מעביר לבוב 2 ביטקוין בהעברה תיקנית וחותם עם המפתח הפרטי שלו. אם ינסה ג'ורג' לקחת את ההעברה הזו, לחתום אותה עם המפתח הפרטי שלו ולהעביר כסף הלאה – באיזה שלב הסקריפט יכשל? תאר את מצב המחסנית בכל שלב.

תשובות:

1. Fees = 0.0005. סכום מועבר 🡨 0.015. total input: 0.1

<https://www.blockchain.com/btc/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18>

1. <https://siminchen.github.io/bitcoinIDE/build/editor.html>
2. {a b op\_dup op\_verify op\_swap op\_dup op\_mul op\_swap op\_div}
3. {a b c op\_dup op\_mul op\_swap op\_dup op\_verify op\_div op\_swap op\_2div op\_add}
4. לא הצלחתי – האם תלוי בהאש כלשהו?
5. <a signature> <a pubkey> <b signature> <b pubkey> OP\_DUP OP\_HASH160 <a public key hash> OP\_EQUAL OP\_CHECKSIG <b public key hash> OP\_EQUAL OP\_CHECKSIG
6. כל שאר הכסף יועבר בתור עמלה כי כך בדיוק עובדת עמלה, כסף שמוכנס בinput פחות ה amount בoutput.
7. <https://www.youtube.com/watch?v=ir4dDCJhdB4> (דקה 43:30)