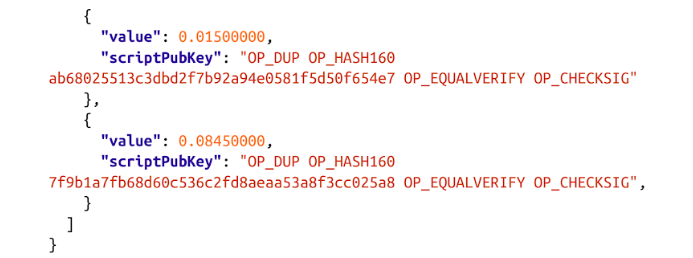
שאלות:

1. בהינתן העברה:



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

מספר העברה:

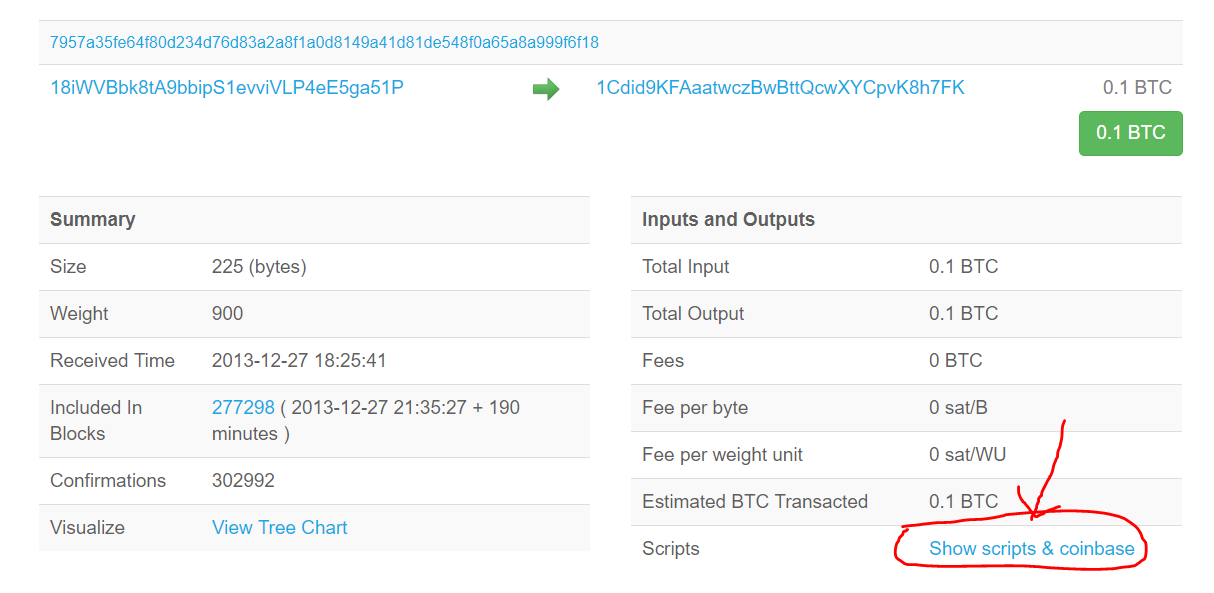
[7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18](https://www.blockchain.com/btc/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18)

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? <https://bitcoin.stackexchange.com/questions/88340/bitcoin-script-execution-unsuccessful>
2. 
3. כתבו סקריפט שמבקש מספר חתימות.
4. 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 תקנית 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.
2. מצא בקוד הפתוח של ביטקוין (interpreter) את פעולת אימות החתימה checksig. הסבר איפה בדיוק הפעולה מתרחשת ואילו ארגומנטים מושווים.
3. כל הבדיקות עבור העברות מסתכמות ב9 שגיאות. מנה אותן (היעזר בקוד המקור כדי לבדוק מהן 9 השגיאות האפשריות **(עבור העברות בלבד)**

תשובות:

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

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

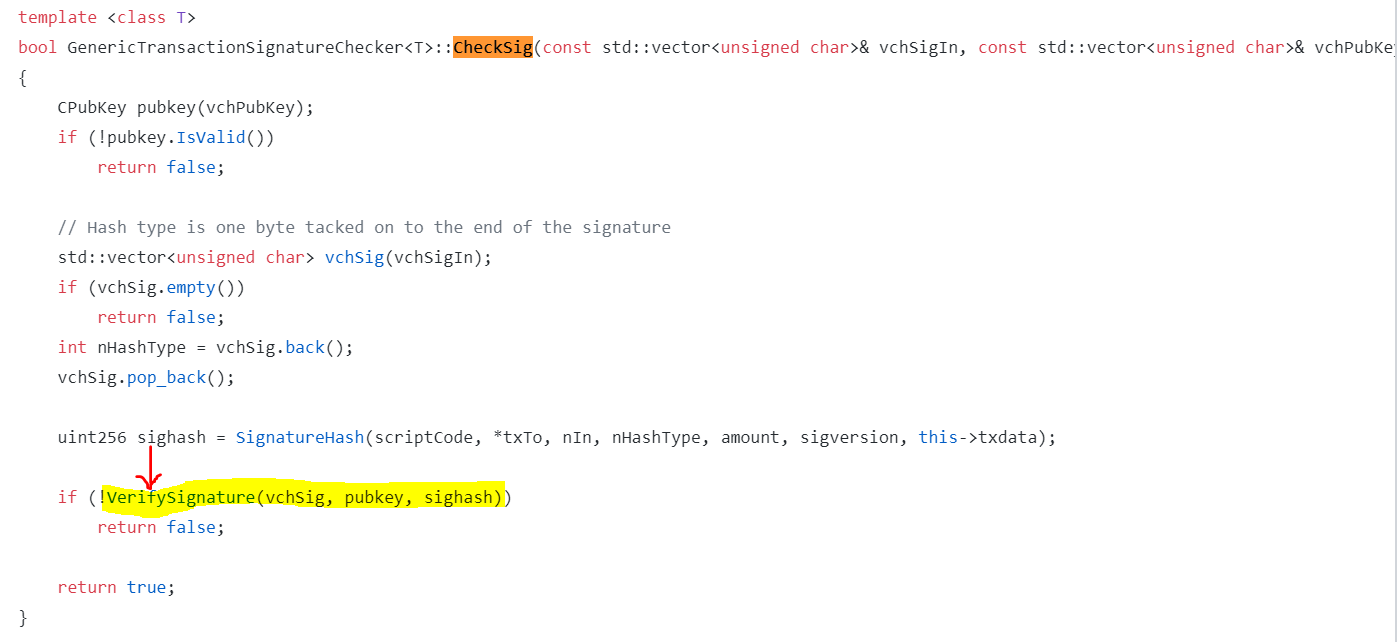
1. <https://siminchen.github.io/bitcoinIDE/build/editor.html>
2. {a b op\_dup op\_verify op\_swap op\_dup op\_mul op\_swap op\_div}
3. {a b c op\_dup op\_mul op\_swap op\_dup op\_verify op\_div op\_swap op\_2div op\_add}
4. לא הצלחתי :

<https://bitcoin.stackexchange.com/questions/88340/bitcoin-script-execution-unsuccessful>

דוגמא לסקריפט שעובר: 304502203f004eeed0cef2715643e2f25a27a28f3c578e94c7f0f6a4df104e7d163f7f8f022100b8b248c1cfd8f77a0365107a9511d759b7544d979dd152a955c867afac0ef78601 044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba687cf2f187f0cee2221c3afb1b5ff7888caced2423916b61444666ca1216f26181398c OP\_DUP OP\_HASH160 2E67490797078511CFDE499434ED6A564AD41EF0 OP\_EQUALVERIFY OP\_CHECKSIG

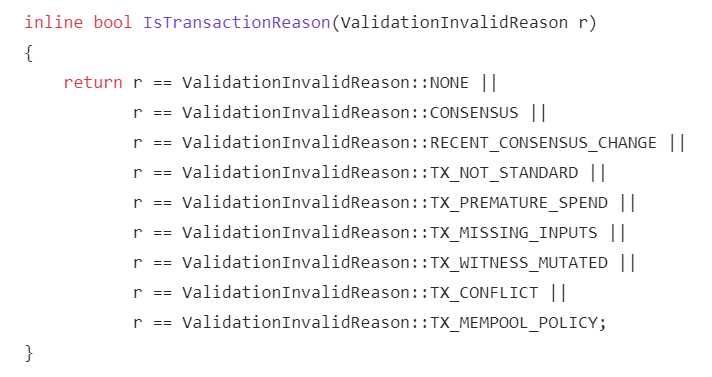
1. <a signature> <a pubkey> <b signature> <b pubkey> OP\_DUP OP\_HASH160 <a public key hash> OP\_EQUAL OP\_CHECKSIG OP\_DUP OP\_HASH160 <b public key hash> OP\_EQUAL OP\_CHECKSIG
2. כל שאר הכסף יועבר בתור עמלה כי כך בדיוק עובדת עמלה, כסף שמוכנס בinput פחות ה amount בoutput.
3. <https://www.youtube.com/watch?v=ir4dDCJhdB4> (דקה 43:30)





המפתח הציבורי והחתימה מושווים (עם גיבוב החתימה).

1. זהו הסיווג בקוד עבור שגיאות של העברות:



קיים הסבר באינומרציה עבור כל אחת מהשגיאות:

