

שאלות:

1. בהינתן העברה:

```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid":
"7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204
b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL]
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d1
72787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160
ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160
7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

א. חשב את סכום העמלה.

ב. כמה satoshi הועברו בעסקה?

מספר העברה:

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

2.

א. כתוב סקריפט המחבר 2 מספרים. תאר בכל שלב במהלך הריצה את מצב המחסנית

ב. כתוב סקריפט המחזיר את תוצאת החישוב של $\frac{a^2}{b}$ כך שהסקריפט מתחיל כך:

$[a \ b \ < fill \ in \ > \dots]$

יש לוודא ש $b \neq 0$ (במקרה ש b הוא 0 נקבל שגיאה ועצירה ולא אינסוף).

ג. כתוב סקריפט המחזיר את תוצאת החישוב של $\frac{a^2}{2} + \frac{c^3}{b}$ כך שהסקריפט מתחיל כך:

$[a \ b \ c \ < fill \ in \ > \dots]$

יש לוודא ש $b \neq 0$ (במקרה ש b הוא 0 נקבל שגיאה ועצירה ולא אינסוף).

3. 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>

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a999f6f18	
18WVBbk8A8bbipS1evviLP4eE5ga51P	1Cd9KFAaateczBwBttQcwXYCpK3h7FK
	0.1 BTC
	0.1 BTC
Summary	
Size	225 (bytes)
Weight	900
Received Time	2013-12-27 18:25:41
Included in Blocks	277298 (2013-12-27 21:35:27 + 190 minutes)
Confirmations	302992
Visualize	View Tree Chart
Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.1 BTC
Fees	0 BTC
Fee per byte	0 sat/B
Fee per weight unit	0 sat/WU
Estimated BTC Transacted	0.1 BTC
Scripts	Show scripts & coinbase

4. כתבו סקריפט שמבקש מספר חתימות.
 א. 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?
 5. אליס מעביר לבוב 2 ביטקוין בהעברה תקנית וחותרם 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.
 6. מצא בקוד הפתוח של ביטקוין (interpreter) את פעולת אימות החתימה checksig. הסבר איפה בדיוק הפעולה מתרחשת ואילו ארגומנטים מושוים.

תשובות:

1. Fees = 0.0005. סכום מועבר $\leftarrow 0.1 - 0.0005$.
<https://www.blockchain.com/btc/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a999f6f18>

2. <https://siminchen.github.io/bitcoinIDE/build/editor.html>.
 א. {a b op_dup op_verify op_swap op_dup op_mul op_swap op_div}
 ב. {a b c op_dup op_mul op_swap op_dup op_verify op_div op_swap op_2div op_add}
 ג. לא הצלחתי:

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

דוגמא לסקריפט שעובר:

```
304502203f004eed0cef2715643e2f25a27a28f3c578e94c7f0f6a4df104e7d163f7f8
f022100b8b248c1cfd8f77a0365107a9511d759b7544d979dd152a955c867afac0ef78
601
044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba687cf2f187
f0cee2221c3afb1b5ff7888caced2423916b61444666ca1216f26181398c OP_DUP
OP_HASH160 2E67490797078511CFDE499434ED6A564AD41EF0 OP_EQUALVERIFY
OP_CHECKSIG
```

4. $\langle a \text{ signature} \rangle \langle a \text{ pubkey} \rangle \langle b \text{ signature} \rangle \langle b \text{ pubkey} \rangle \text{OP_DUP OP_HASH160} \langle a \text{ public key hash} \rangle \text{OP_EQUAL OP_CHECKSIG OP_DUP OP_HASH160} \langle b \text{ public key hash} \rangle \text{OP_EQUAL OP_CHECKSIG}$

ב. כל שאר הכסף יועבר בתור עמלה כי כך בדיוק עובדת עמלה, כסף שמוכנס בinput פחות ה amount בoutput.

5. <https://www.youtube.com/watch?v=ir4dDCJhdB4> (דקה 43:30)

```
case OP_CHECKSIG:
case OP_CHECKSIGVERIFY:
{
    // (sig pubkey -- bool)
    if (stack.size() < 2)
        return set_error(error, SCRIPT_ERR_INVALID_STACK_OPERATION);

    valtype& vchSig = stacktop(-2);
    valtype& vchPubKey = stacktop(-1);

    // Subset of script starting at the most recent codeseparator
    CScript scriptCode(pbegincodehash, pend);

    // Drop the signature, since there's no way for a signature to sign itself
    scriptCode.FindAndDelete(CScript(vchSig));

    if (!CheckSignatureEncoding(vchSig, flags, error) || !CheckPubKeyEncoding(vchPubKey, flags, error)) {
        //error is set
        return false;
    }
    bool fSuccess = checker.CheckSig(vchSig, vchPubKey, scriptCode);

    popstack(stack);
    popstack(stack);
    stack.push_back(fSuccess ? vchTrue : vchFalse);
    if (opcode == OP_CHECKSIGVERIFY)
    {
        if (fSuccess)
            popstack(stack);
        else
            return set_error(error, SCRIPT_ERR_CHECKSIGVERIFY);
    }
}
break;
```

```
template <class T>
bool GenericTransactionSignatureChecker<T>::CheckSig(const std::vector<unsigned char>& vchSigIn, const std::vector<unsigned char>& vchPubKey)
{
    CPubKey pubkey(vchPubKey);
    if (!pubkey.IsValid())
        return false;

    // Hash type is one byte tacked on to the end of the signature
    std::vector<unsigned char> vchSig(vchSigIn);
    if (vchSig.empty())
        return false;
    int nHashType = vchSig.back();
    vchSig.pop_back();

    uint256 sighash = SignatureHash(scriptCode, *txTo, nIn, nHashType, amount, sigversion, this->txdata);
    if (!VerifySignature(vchSig, pubkey, sighash))
        return false;

    return true;
}
```

המפתח הציבורי והחתימה מושוים (עם גיבוב החתימה).