שאלות:

1. בהפעלת פעולת op_CHECKMULTISIG ישנו מספר מקסימלי של n שמתוכו אפשר לבצע אישור –
מצא את המספר n בקוד המקור של ביטקוין.
אלו עוד הגבלות ישנן באותו מקום בקוד? מדוע הגבלות אלו קיימות? בפרט, מדוע ישנה הגבלה על מינימום עמלה לעסקה על מנת שתכנס לבלוק?
2.
   א. ציין לפחות חמישה יתרונות של P2SH.
   ב. סקריפט מסובך המיוצג ע"י כתובת, יכול להיות מאושר בשרשרת הבלוקים אפילו מבלי לבדוק את נכונות הסקריפט עצמו (שהרי הסקריפט העומד מאחורי הכתובת אינו מיוצג בשום מקום בהעברה). אם כן, מה יקרה כאשר הסקריפט אינו Valid?
3. מה הוא שדה המספר סידורי (nSequence field)? איך הוא בא לידי ביטוי במנעולי זמן?
4.
   א. מה עושה הסקריפט הבא:

```
IF
    2 <Alice's pubkey> <Bob's pubkey> <Escrow's pubkey> 3 CHECKMULTISIG
ELSE
    "30d" CHECKSEQUENCEVERIFY DROP
    <Alice's pubkey> CHECKSIG
ENDIF
```

   ב.
      i. מה עושה הסקריפט הבא:

```
IF
  IF
    2
  ELSE
    <30 days> CHECKSEQUENCEVERIFY DROP
    <Abdul the Lawyer's Pubkey> CHECKSIGVERIFY
    1
  ENDIF
  <Mohammed's Pubkey> <Saeed's Pubkey> <Zaira's Pubkey> 3 CHECKMULTISIG
ELSE
  <90 days> CHECKSEQUENCEVERIFY DROP
  <Abdul the Lawyer's Pubkey> CHECKSIG
ENDIF
```

      ii. תן דוגמא לקוד פותח שייתן true עבור הסקריפט בפחות מ30 יום.
      iii. מדוע העו"ד לא יכול לפדות את הכסף בכל זמן רק עם הסקריפט הבא?:

```
<Abdul's Sig> FALSE
```

      iv. בכמה דרכים אפשר לפדות את הכסף 5 ימים אחרי הכרייה?
      35 ימים אחרי הכרייה?
      105 ימים אחרי הכרייה?
      v. איך השותפים יכולים "לאפס" את השעון כדי שהעו"ד לא יוכל לפדות את הכסף לבד?
5.
   א. כתבו סקריפט שקיימים בו 6 מפתחות ציבוריים: A, B, C, D, E, F כך ש:
   מיד יהיה אפשר לפתוח עם **אחת** מהחתימות של A וB;
   לאחר 10 ימים יהיה אפשר לפתוח עם **שתי** החתימות של C וD;
   לאחר 30 יום יהיה אפשר לפתוח עם **אחת** מהחתימות של E וF.
   ב. כתבו דוגמא ל3 סקריפטים פותחים שונים עבור סעיף א' (מיידית, לאחר 10 יום בלבד, לאחר 30 יום בלבד).

תשובות:

1.

https://github.com/bitcoin/bitcoin/blob/c536dfbcb00fb15963bf5d507b7017c241718bf6/src/policy/policy.h

```
/** Default for -blockmaxweight, which controls the range of block weights the mining code will create **/
static const unsigned int DEFAULT_BLOCK_MAX_WEIGHT = MAX_BLOCK_WEIGHT - 4000;
/** Default for -blockmintxfee, which sets the minimum feerate for a transaction in blocks created by mining code **/
static const unsigned int DEFAULT_BLOCK_MIN_TX_FEE = 1000;
/** The maximum weight for transactions we're willing to relay/mine */
static const unsigned int MAX_STANDARD_TX_WEIGHT = 400000;
/** The minimum non-witness size for transactions we're willing to relay/mine (1 segwit input + 1 P2WPKH output = 82 bytes) */
static const unsigned int MIN_STANDARD_TX_NONWITNESS_SIZE = 82;
/** Maximum number of signature check operations in an IsStandard() P2SH script */
static const unsigned int MAX_P2SH_SIGOPS = 15;
/** The maximum number of sigops we're willing to relay/mine in a single tx */
static const unsigned int MAX_STANDARD_TX_SIGOPS_COST = MAX_BLOCK_SIGOPS_COST/5;
/** Default for -maxmempool, maximum megabytes of mempool memory usage */
static const unsigned int DEFAULT_MAX_MEMPOOL_SIZE = 300;
/** Default for -incrementalrelayfee, which sets the minimum feerate increase for mempool limiting or BIP 125 replacement **/
static const unsigned int DEFAULT_INCREMENTAL_RELAY_FEE = 1000;
/** Default for -bytespersigop */
static const unsigned int DEFAULT_BYTES_PER_SIGOP = 20;
/** Default for -permitbaremultisig */
static const bool DEFAULT_PERMIT_BAREMULTISIG = true;
/** The maximum number of witness stack items in a standard P2WSH script */
static const unsigned int MAX_STANDARD_P2WSH_STACK_ITEMS = 100;
```

ההגבלה היא n=15. ישנה הגבלה על משקל בלוק, משקל העברה, עמלה מינימלית על העברה כדי שתיכלל בבלוק וכו'...

הגבלה על מינימום עמלה נועדה כדי להבטיח שלא ישלחו העברות "זבל" שיצטרכו להישמר ברשת הביטקוין לצמיתות.

2.

א.

- סקריפטים מסובכים מוחלפים בשורה פשוטה יותר להבנה
- סקריפט יכולים להיות מקודדים ככתובת כך שלא צריך תכנות מסובך לממש העברה
- P2SH מעביר את הצורך לבנות את הסקריפט למקבל ולא לשולח (כיוון שנדרש ליצור את הסקריפט ולקבל את כתובתו)
- מעביר את אחסון המידע מהפלט של ההעברה (שמאוחסן גם בארנקים) לקלט של העברה (שמאוחסן רק בשרשרת הבלוק)
- אדם שמקבל מכתובת כזו הוא זה שיספוג את עלות העמלה כיוון שיצטרך להעביר את הכסף הלאה עם הסקריפט הארוך (ולא שולח הכסף).
- אחסון הסקריפט הארוך נדחה עד להוצאת הכסף ע"י המקבל וחוסך את המקום.

ב. ההעברה תאושר והכסף יאבד.

3. https://bitcoin.stackexchange.com/questions/2025/what-is-txins-sequence

השדה nSequence נועד כדי למספר את ההודעות במקרה של החלפה (בקוד המקור).
בפועל, מימוש השדה הזה נועד כדי לסמן את הזמן שיעבור מרגע שחרור העסקה עד המשך הסקריפט.

4.

א. בכל עת ניתן להעביר הלאה את הכסף באמצעות 2 חתימות מתוך חתימותיהן של אליס, בוב או של הפקיד. אחרי 30 ימים אליס יכולה לחתום לבד.
https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki

ב.

i. מצריך 2 מתוך 3 חתימות של מוחמד, סעד וזאירה. לאחר 30 יום אפשרי רק עם חתימת עבדול העורך דין אם כתב TRUE. אחרת אפשרי רק לאחר 90 יום עם חתימתו של עבדול.

ii. 0 <Mohammed Sig><Zaira Sig> TRUE TRUE

iii. כיוון שהתשובה של הסקריפט תהיה שלילית והסקריפט יכשל.

iv. 5 ימים אחרי הכרייה אפשר לפדות ב3 דרכים (2 חתימות מתוך 3 שותפים).
35 ימים אחרי הכרייה אפשר לפדות ב3 דרכים הראשונות או 3 נוספות (כל שותף ביחד עם עבדול העו"ד) – סה"כ 6 דרכים.
105 ימים אחרי הכרייה ב6 הדרכים הקודמות ועוד עבדול לבד – סה"כ 7 דרכים.

v. לשחרר מחדש את העסקה ל"בריכת הכרייה" ובכך "לדרוס" את ההעברה עם אותו סקריפט בדיוק.
https://bitcoin.stackexchange.com/questions/42570/is-it-possible-to-schedule-a-transaction-in-the-future

.5

```
IF
  IF
    1 <A Pubkey> <B Pubkey>
  ELSE
    <10 days> CHECKSEQUENCEVERIFY DROP
    2 <C Pubkey> <D Pubkey>
  ENDIF
ELSE
  <30 days> CHECKSEQUENCEVERIFY DROP
  1 <E Pubkey> <F Pubkey>
ENDIF
      2 CHECKMULTISIG


      1. 0 <A Sig> <B Sig> TRUE TRUE
      2. 0 <C Sig> <D Sig> FALSE TRUE
      3. 0 <E Sig> <F Sig> FALSE
```