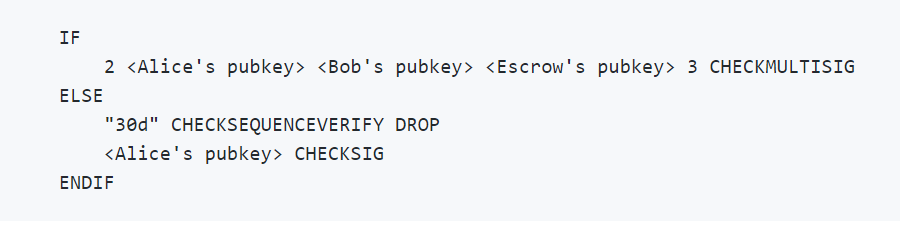
שאלות:

1. בהפעלת פעולת op\_CHECKMULTISIG ישנו מספר מקסימלי של n שמתוכו אפשר לבצע אישור –

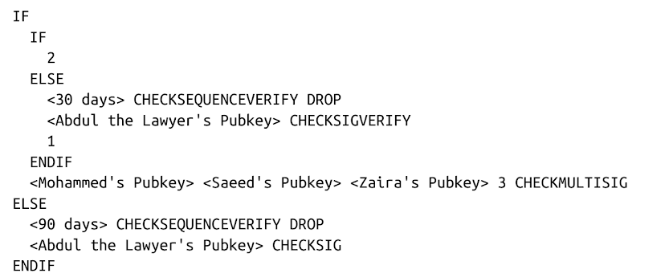
מצא את המספר n בקוד המקור של ביטקוין.

אלו עוד הגבלות ישנן באותו מקום בקוד? מדוע הגבלות אלו קיימות? בפרט, מדוע ישנה הגבלה על מינימום עמלה לעסקה על מנת שתכנס לבלוק?

1. ציין לפחות חמישה יתרונות של P2SH.
2. 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. מה עושה הסקריפט הבא:



1. מה עושה הסקריפט הבא:



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



1. בכמה דרכים אפשר לפדות את הכסף 5 ימים אחרי הכרייה?

35 ימים אחרי הכרייה?

105 ימים אחרי הכרייה?

1. איך השותפים יכולים "לאפס" את השעון כדי שהעו"ד לא יוכל לפדות את הכסף לבד?
2. כתבו סקריפט שקיימים בו 6 מפתחות ציבוריים: A, B, C, D, E, F כך ש:

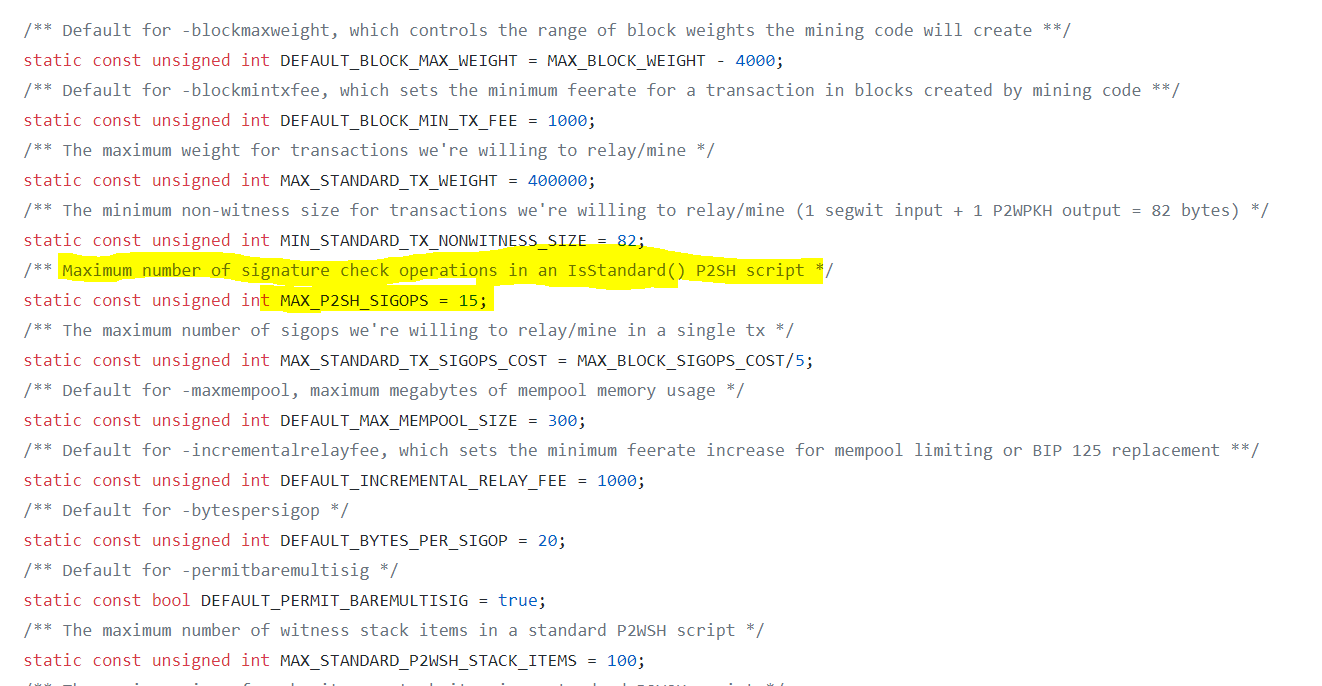
מיד יהיה אפשר לפתוח עם **אחת** מהחתימות של A וB;

לאחר 10 ימים יהיה אפשר לפתוח עם  **שתי** החתימות של C וD;

לאחר 30 יום יהיה אפשר לפתוח עם **אחת** מהחתימות של E וF.

1. כתבו דוגמא ל3 סקריפטים פותחים שונים עבור סעיף א' (מיידית, לאחר 10 יום בלבד, לאחר 30 יום בלבד).

תשובות:

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

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.

* 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.

1. ההעברה תאושר והכסף יאבד.
2. <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.

1. 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>

1. 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.
2. 0 <Mohammed Sig><Zaira Sig> TRUE TRUE
3. כיוון שהתשובה של הסקריפט תהיה שלילית והסקריפט יכשל.
4. 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.

1. 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>

1. 