שאלות:

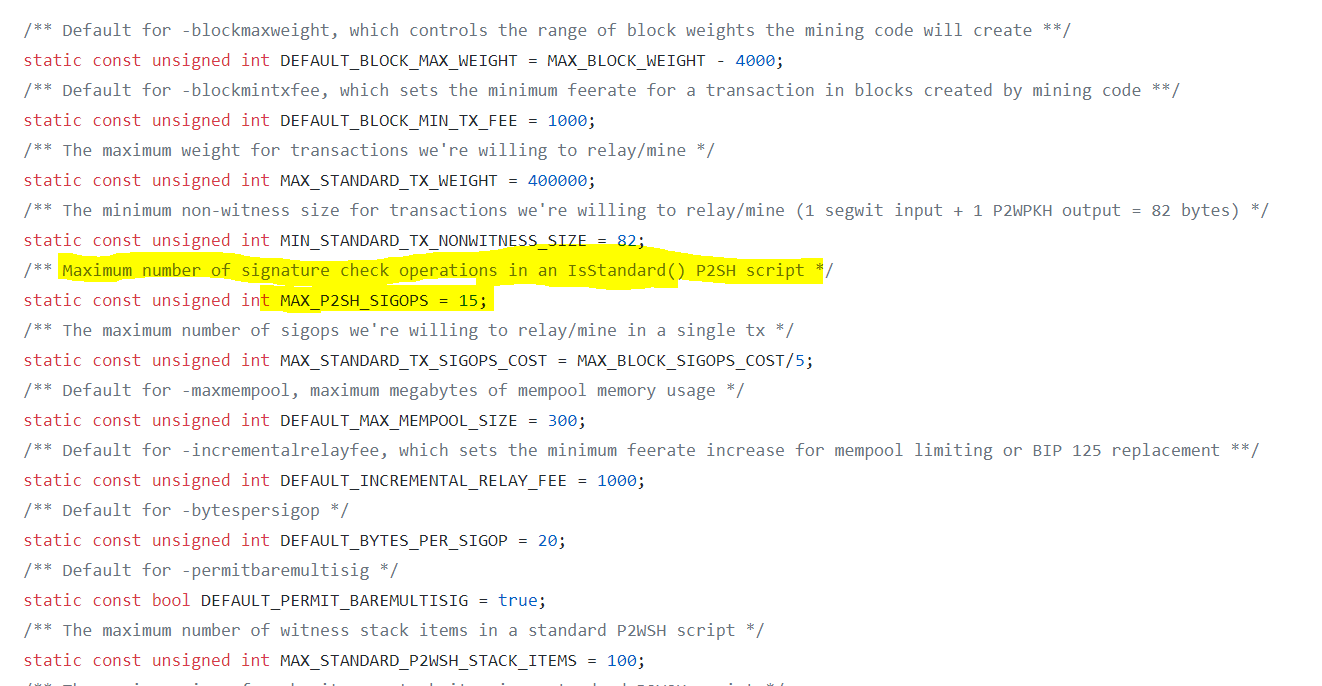
1. בהוצאה לפועל של פעולת op\_CHECKMULTISIG ישנו מספר מקסימלי של n שמתוכו אפשר לבצע אישור –

מצא את המספר הזה 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 P2SK.
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?

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 שתכלל בבלוק וכו'...

1. סקריפטים מסובים מוחלפים בשורה פשוטה יותר להבנה

סקריפט יכולים להיות מקודדים ככתובת כך שלא צריך תכנות מסובך לממש העברה

P2SK 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).

1. הכסף יאבד.