ארנקים

מנקודת מבט מתכנת – הכוונה במושג "*ארנק*" היא מבנה הנתונים שבו מאוחסנים המפתחות הפרטיים של אותו סוחר.

בתוך הארנק מאוחסנים זוגות של מפתחות פרטיים/ציבוריים ולא מטבעות כמו שהיה אפשר לטעות בהקשר המושג. למעשה, יתרת הסכומים אינה מתחלקת לפי ארנקים אלא לפי מטבעות שמועברים למפתח ציבורי מסוים.

לכן, במקרים רבים העברה אחת מאדם אחד תכלול מספר רב של מפתחות מקור כך שסכום קטן מועבר מכל מפתח וסך כל ההעברה נעשה מארנק אחד לשני.

**ארנק דטרמינסטי**

יש כמה סוגי ארנקים. הפרימיטיבי ביותר (Bitcoin Core) הוא כמובן ארנק שמאחסן בתוכו פשוט אוסף של זוגות -מפתחות פרטיים וציבוריים שהוגרלו מחדש בכל עסקה או בכל פקודת יצירת מפתח (שיכולה להפקד ידנית). כיוון שיצירת מפתח פרטי בכל פעם היא אקראית לגמרי, נהיה חייבים לאחסן את כל המפתחות באופן מלא. כמות גדולה של מפתחות יכולה ליצור מעמסה של ממש על אפליקציות ארנק ועלולה לגרום לצד לקוח לעבוד באופן מסורבל ואיטי ובאבדת מפתח לא תהיה האפשרות לשחזר אותו והכסף יאבד לנצח.

ברשת הביטקוין ישנם המון כספים אבודים שאין דרך לחלץ אותם. באין גורם מרכז שאצלו הרשאות, לא ניתן להוציא כסף שהמפתח הפרטי של הבעלים אבד לו או שהבעלים נפטר ולא מסר את המפתח הפרטי לאף אחד.

לשם כך נוצר *ארנק דטרמיניסטי* אשר עצם יצירת הארנק היא בעצם יצירת שורש (SEED) אחד שממנו יופקו כל המפתחות הפרטיים והציבוריים.

השורש שנוצר הא משפט בעל 12-24 מילים אקראיות. שורש הארנק הוא הבסיס ליצירת כל המפתחות הפרטיים בארנק הדטרמיניסטי כך שאפשר יהיה במידת הצורך להנפיק את המפתחות הפרטיים מחדש בהינתן שורש הארנק (SEED). שורש הארנק מוצג באמצעות מילים כדי שיהיה קל לזכור אותן ולגבות אותן ובכך לשחזר את הארנק (איך לשחזר? נראה בהמשך).

<https://iancoleman.io/bip39/> - Mnemonic Code Converter