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).

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

טכניקת מנמוניקה

מְנֶמוֹנִיקָה (מיוונית עתיקה μνημονικός: מְנֶמוֹנִיקוֹס" ,קשור לזיכרון") או עזר זיכרון היא אמצעי או שיטה חזותיים או מילוליים העוזרים לזכור דברים – למשל גימטריה למספרים או ראשי תיבות.

המרת שורש מספרי כלשהו למילים יוצר אפקט שמאפשר לזכור ביתר קלות את שיטת השחזור אך מצד שני מקלה על גורם עוין לשחזר יתרת ארנק ועסקאות ע"י סדרת המילים הפשוטה לכאורה.

יצירת המילים (או יותר) נוצרת באופן הבא:

1. יצירת רצף אקראי (אנטרופיה) של 128 עד 256 סיביות
2. צור Checksum של הרצף האקראי על ידי לקיחת החלקים הראשונים של SHA256 שלה
3. הוסיפו את Checksum לסוף הרצף האקראי
4. מחלקים את הרצף למקטעים של 11 סיביות
5. כל 11 סיביות כאלה להמיר למילה מתוך המילון של 2048 המילים
6. לצרף את כל המילים לייצוג של קוד הזיכרון.

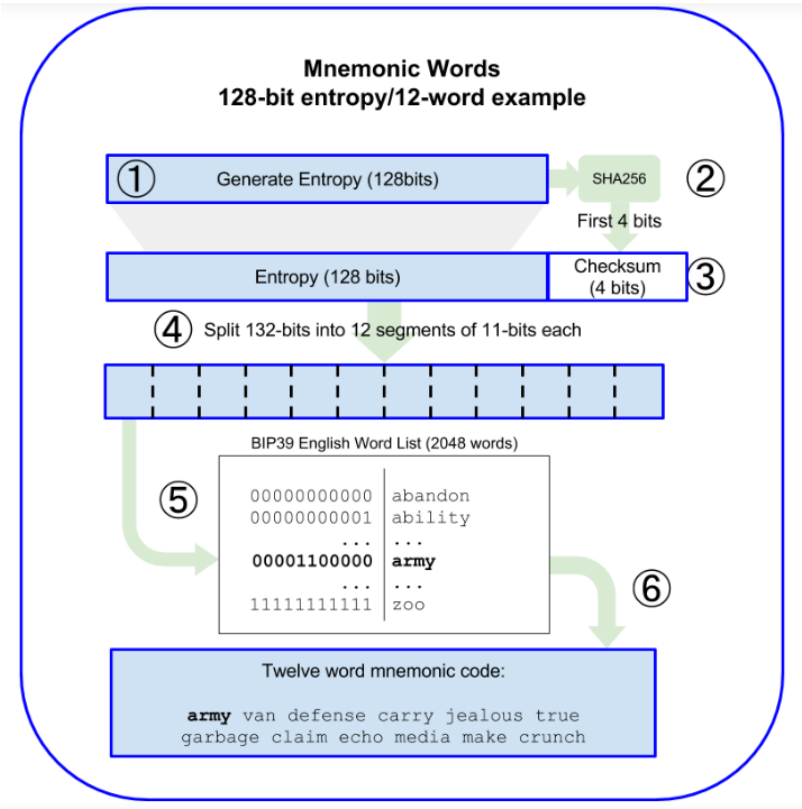


Table 4-5. Mnemonic Codes: Entropy and Word Length

Entropy (bits)	Checksum (bits)	Entropy+Checksum	Word Length
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

עבור סוגים שונים של אנטרופיית ביטים יהיה גודל שונה של Checksum (מפורט בטבלה).

רשימת המילים בBIP39 באנגלית בגיטהאב של ביטקוין:

https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

השימוש בBIP השונים תלוי במימוש בפועל. עבור ארנקים דטרמיניסטיים פשוטים מממשים הארנקים את מנמוניקת BIP39. עבור ארנקים דטרמיניסטיים היררכיים ממומש BIP32. עבור ארנקים דטרמיניסטיים בעלי מספר חשבונות מממשים BIP44.

כדי לשחזר ארנק דטרמינסטי, אפליקציית הארנק מחפשת את המפתחות הציבוריים הראשונים שנוצרים מתוך מפתח המקור (Seed).

היא עוברת מפתח-מפתח ובודקת באילו כתובות נעשה שימוש. כאשר מתגלים 30 כתובות ציבוריות שלא נעשה בהם שימוש, אפליקציית הארנק עוצרת.

טכניקת שחזור ארנקים ואחסון זוגות של מפתחות עדיין לא נכנסה רשמית לפרוטוקול הביטקוין וכל ההגדרות עדיין בגדר "הצעת שיפור".

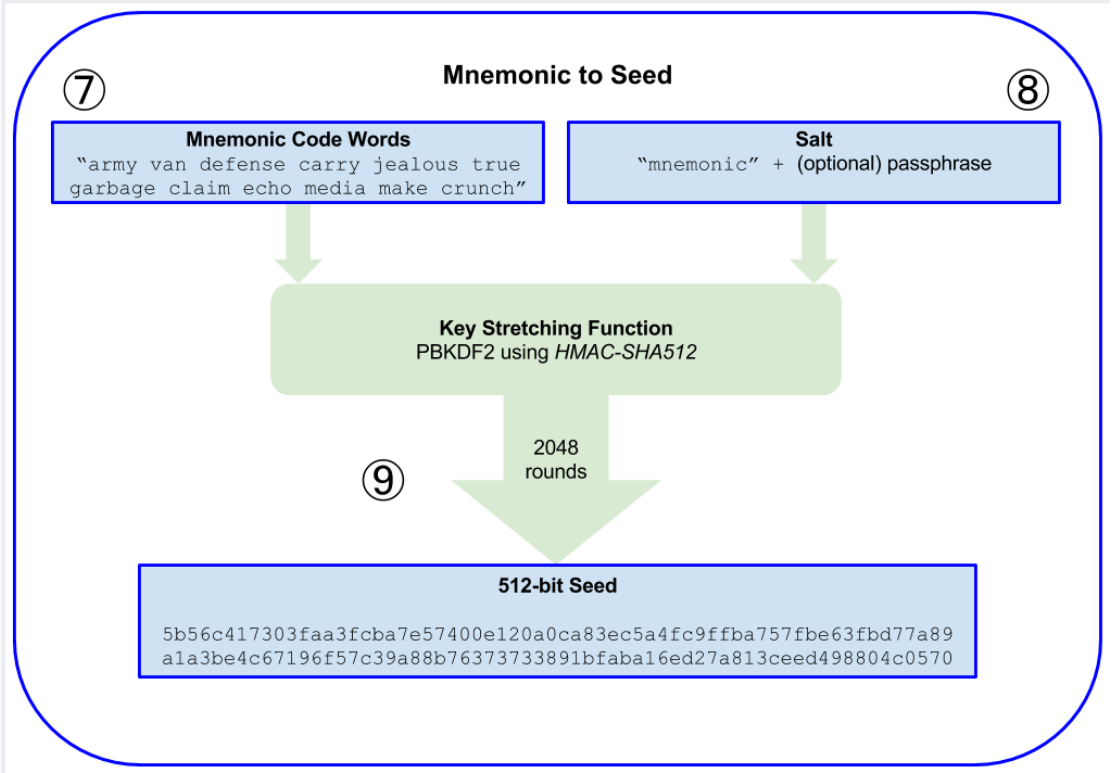
הצעות השיפור של ביטקוין שלא נכנסו עדיין רשמית לפרוטוקול מתועדות בקוד הפתוח של ביטקוין בתור (Bitcoin Improvement Proposal) – BIPS:

https://github.com/bitcoin/bips

להצעות שנמצאות בגיטהאב יש סטטוס – חלקן נכנסו לפרוטוקול, חלקן פעילות כרגע אך לא נכנסו באופן רשמי וחלקן הוחלפו בדרישות או שיפורים אחרים.

הצעות שיפור הקשורות לארנקים הן:

BIP39, BIP32, BIP44, BIP49.



BIP39 Mnemonic code for generating deterministic keys

Read more at the official BIP39 spec

BIP32 Hierarchical Deterministic Wallets

Read more at the official BIP32 spec

See the demo at bip32.org

BIP44 Multi-Account Hierarchy for Deterministic Wallets

Read more at the official BIP44 spec

BIP49 Derivation scheme for P2WPKH-nested-in-P2SH based accounts

Read more at the official BIP49 spec

בדוגמא למטה אפשר לראות מה קורה כשנגדיר אנטרופיה קטנה מדי למציאת האינדקסים של המילים – נוצרו 3 מילים, 2 מתוכן זהות וזמן הפיצוח הוא פחות משניה.

ככל שאנטרופיה גדולה ומסובכת- כך גדל מספר המילים וזמן הפיצוח יתמשך.