Генерация мнемоники

Мнемоника должна кодировать энтропию в кратных 32 битах. С увеличением энтропии повышается безопасность, но увеличивается длина фразы. Начальная длина энтропии обозначается как ENT. Допустимые размеры ENT составляют от 128 до 256 бит.

Сначала генерируется начальная энтропия длиной ENT бит. Контрольная сумма создаётся путём взятия первых ENT / 32 бит от её SHA256-хэша. Эта контрольная сумма добавляется в конец начальной энтропии. Далее, эти объединенные биты разбиваются на группы по 11 бит, каждая из которых кодирует число от 0 до 2047, являясь индексом в списке слов. Наконец, мы преобразуем эти числа в слова и используем соединённые слова в качестве мнемонической фразы.

Следующая таблица описывает соотношение между длиной начальной энтропии (ENT), длиной контрольной суммы (CS) и длиной сгенерированной мнемонической фразы (MS) в словах.

```
CS = ENT / 32
MS = (ENT + CS) / 11
```

ENT	CS	ENT+CS	MS
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

Список слов

Идеальный список слов обладает следующими характеристиками:

a) умный подбор слов

- список слов создан таким образом, что достаточно набрать первые четыре буквы для однозначной идентификации слова b) избегание похожих слов
- пары слов, как "build" и "built", "woman" и "women", "quick" и "quickly" не только усложняют запоминание фразы, но и более подвержены ошибкам и труднее угадываются c) отсортированные списки слов

- список слов отсортирован, что позволяет более эффективно искать кодовые слова (т.е. реализации могут использовать бинарный поиск вместо линейного)
- это также позволяет использовать префиксное дерево (trie), например, для лучшей компрессии

Список слов может содержать символы родного языка, но они должны быть закодированы в UTF-8 с использованием формы нормализации совместимости декомпозиции (NFKD).

От мнемоники к семени

Пользователь может защитить свою мнемонику с помощью пароля. Если пароль отсутствует, используется пустая строка "".

Для создания бинарного семени из мнемоники используется функция PBKDF2 с мнемонической фразой (в UTF-8 NFKD), используемой в качестве пароля, и строкой "mnemonic" + пароль (также в UTF-8 NFKD), используемой в качестве соли. Число итераций установлено на 2048, а HMAC-SHA512 используется в качестве псевдослучайной функции. Длина получаемого ключа составляет 512 бит (= 64 байта).

Это семя может быть использовано для создания детерминированных кошельков с использованием BIP-0032 или аналогичных методов.

Преобразование мнемонической фразы в бинарное семя полностью независимо от ее генерации. Это приводит к довольно простому коду; нет ограничений на структуру фразы, и клиенты могут реализовать свои собственные списки слов или даже генераторы фраз, обеспечивая гибкость в списках слов для обнаружения опечаток или других целей.

Хотя использование мнемоники, не сгенерированной описанным алгоритмом в разделе "Генерация мнемоники", возможно, это не рекомендуется, и программное обеспечение должно вычислять контрольную сумму для мнемонической фразы, используя список слов, и выдавать предупреждение, если она недействительна.

Описанный метод также обеспечивает правдоподобное отрицание, поскольку каждый пароль генерирует действительное семя (и, соответственно, детерминированный кошелек), но только правильный пароль сделает доступным желаемый кошелек.

Списки слов

Поскольку подавляющее большинство кошельков BIP39 поддерживают только английский список слов, настоятельно не рекомендуется использовать не английские списки слов для генерации мнемонических фраз.

Если вы всё же считаете, что ваше приложение действительно нуждается в использовании локализованного списка слов, используйте один из следующих вместо создания своего собственного.

Ссылка на список слов на английском:
https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt