Аннотация

Этот BIP вводит «Поле назначения» для использования в детерминированных кошельках на основе алгоритма, описанного в BIP-0032 (далее BIP32).

Назначение

Мы предлагаем использовать первый уровень структуры дерева BIP32 в качестве «назначения». Это назначение определяет дальнейшую структуру под этим узлом.

```
m / purpose' / *
```

Апостроф указывает на использование усиленного вывода BIP32.

Мы призываем различные схемы подавать заявки на назначение отдельного номера BIP и использовать тот же номер для поля назначения, чтобы адреса не генерировались из пересекающихся пространств BIP32.

Коды назначения от 10001 до 19999 зарезервированы для SLIPs.

Пример: схема, описанная в BIP44, должна использовать 44' (или 0x8000002C) в качестве назначения.

Обратите внимание, что m / 0' / * уже занято BIP32 (аккаунт по умолчанию), который предшествовал этому BIP.

Не все кошельки могут захотеть поддерживать весь спектр функций и возможностей, описанных в этих BIP. Вместо выбора произвольного подмножества определенных функций и заявлений о совместимости с BIPxx, мы предлагаем программному обеспечению, которому нужна только ограниченная структура, описать такую структуру в другом BIP и использовать другое значение «назначения».

Сериализация узлов

Поскольку эта схема может использоваться для генерации узлов для нескольких криптовалют одновременно или даже для чего-то совершенно не связанного с криптовалютами, нет смысла использовать специальную магическую версию, описанную в разделе «Формат сериализации» BIP32. Мы предлагаем всегда использовать 0x0488B21E для публичных узлов и 0x0488ADE4 для приватных узлов (что приводит к префиксам «xpub» и «xprv» соответственно).