Module API

MikksChain HDWallet

문서변경이력

버전 번호	작성일	변경사항 요약	작성자	확인자
0.01	9/18/2018	Initial Release	정병두	류준선

목차

API List

require('./mikks.js')	
mikks.passphraseToSeed()	
mikks.hdnode.fromSeedBuffer()	

실행

node를 실행하고 mikks.js 모듈을 변수로 등록하여 사용한다.

```
> mikks = require('./mikks.js')
```

기능

기능 설명이므로 세부 동작에 대한 내용은 'Mikks 지갑 구조 문서'를 참고하세요.

MIB-0039 : BIP-0039 대체 알고리즘

1. RandomByte를 생성하고 그 값과 문장, 비밀번호를 조합하여 Seed를 생성한다.
2. Seed와 RandomByte를 반환한다.

```
> seed = mikks.passphraseToSeed("사용자 정의 문장","비밀번호")
> seed.seed // => Buffer로 정의된 Seed
> seed.rng // => Buffer로 정의된 RandomByte
```

BIP-0032 & BIP-0044 적용

1. Seed 값을 이용하여 MasterNode 생성

```
> masterNode = mikks.hdnode.fromSeedBuffer(seed.seed)
```

2. MasterNode의 Data 출력

```
> extendedPrivateKey = masterNode.toBase58()

> extendedPublicKey = masterNode.neutered().toBase58()

> publicKey = masterNode.getPublicKeyBuffer().toString('hex')

> privateKey = masterNode.keyPair.d.toString(16)

> chainCode = masterNode.chainCode.toString('hex')
```

3. MasterNode로 부터 Child 파생

```
> ChildNode = MasterNode.derivePath("44'/0'/0'/0/0")
```

예제

지갑에 있는 example.js 파일입니다.

```
> node example.js
```

example.js 실행화면