

Web Wallet

MikksChain HDWallet

문서변경이력

[illegible]

목차

개념	4
기능	5
지갑 생성	5
출력	5
지갑 조회	7
출력	7

개념

1. BIP39 니모닉 대신 사용자가 원하는 문장. (조사, 특수기호 포함) 사용

1) NFKD(UTF-8)

2) 최소 글자수 제한 (빈 공백 포함) => 최소 글자수에 대한 정립이 필요

2. 유저 Password (UTF-8 NFKD)

~~1) 도형, 색상, 음식, 장소 등에서 암호 사용을 권장 => 미구현~~

2) 개인별 Password 입력 (최소 글자수 제한)

3. PBKDF2 함수를 이용하여 Seed 생성.

1) Password = "유저가 원하는 문장" + "개인별 Password"

=> personalSentence + personalPassword

2) Salt = "랜덤바이트(2바이트)" + "개인별 Password"

=> rng + personalPassword

4. 생성된 Seed로 HD Wallet의 MasterNode를 구성

1) secp256k1, secp256r1 선택 지원

5. 생성된 MasterNode로 Bip32, Bip44의 제안에 따른 Child 키(Private, Public, Address) 파생

기능

지갑 생성

- 1) 문장과 비밀번호를 작성
- 2) 랜덤바이트를 제공하고 그 외의 MasterNode의 정보를 제공
(Seed, PrivateKey, ChainCode, PublicKey, extendedKey(xprv and xpub))
- 3) extendedKey에 대한 QR Code를 출력
- 4) MasterNode로 부터 파생된 50개의 Child의 Key 값 출력
주소에 마우스 오버시 해당 주소의 QR Code출력

출력

지갑 생성 메인화면

지갑 생성

사용자 정의 문장을 입력해주세요.

테스트 문장입니다.

사용자 비밀번호를 입력해주세요.

테스트 비밀번호입니다.

생성

지갑 생성 시 출력화면

지갑 정보

RandomNumber(*)

32545

PrivateKey

ecc6ab5418b61027e68c56950b5c144abe3738890a7561e81c5839c31352332

ChainCode

038bcb4732b0e6c61b9c9b9eae69b830cdaa125cc2768239d92a980e1181e4fd

PublicKey

b4fe06b2d13ed7ba861b1d1a5914f1f84184e877bb3536f29c1d774c1f1ea34

Extended PrivateKey

xprv9k21ZrQH143K3rsUoW19wq2p1S23c3g9K7r7S5yb1N3AaPkdS5aBQwLbA1cDpX5TKWkE8NSVPhFhFhYzKLLU5LBJeNkgEStp0P59QbtrnQF

Extended PublicKey

xpub661MyMwAq6bcGLwUuPFAKqyZGfrv11WPvh533Hz4ybW7NdRnFN1XK8ue#sp3F2W84gaDKLcy1oSPp170N2b1QaEDAOL6GJULY4T1EFT r

QR Code



Extended PrivateKey



Extended PublicKey

파생된 키

Path	Address	Public Key	Private Key
m/44'/0'/0'/0/0	1CL7W5EUjbtazTfwRujZVfFAAmQAR1XWpM	0271b466bcc07e36d9014ae63c47cad76dcf883973ef27a8e3ac2a5a7f92cb4ae9	615787a2f855a5c2585564093183a17eb34052e4923b0d7a4af8f5462dc3afd6
m/44'/0'/0'/0/1	1BIA8dEedYQL5TGMUEtEft7uUkdtS4wg	0248a6f3fd7a6e2fb29679ce917fd7277e6c3645345945622619373613c2d8725	ba8a9023f9b6e44b4b3fa8e5329af85496d65db7f254b54e4116a5886586188
m/44'/0'/0'/0/2	15v7aeVC3164UEot4mCK34WWqZJWJNMdu	028434d4d2286abd69ba901383ec3b34547f33c23ca1e8e6aff28551442a6676fe	b6a5262f742662962f86f9cc1fca2d5afeb18ad30cd0fcd070231707e3dad5
m/44'/0'/0'/0/3	1Jzcwnvoet1RVhg8RUdMzDb4V9vd8x6kT	02b3c87be5a4cd88501b7a73370fa5e4d8eae870168d9780864d296d5696940	1b8d2148d322076a4f349348c67dcf53d8ca1f31c7a00c3a3a56593a9cde353
m/44'/0'/0'/0/4	1HEhE1FqEpYggUHIj5NfHkRErrymePuU	023dc83b109d157817b1cf30c106819e1922126874a4ee82e40969ee2c9cf2647e	b39224883e10492d43c87a7f37cd2e0fa30688016e66c35bf402265159740954
m/44'/0'/0'/0/5	1AT33WbepPstLaLVickmEHdc6R9nmcV4	03c45800e0b8f6a8596c6de92497d7734488997c541f1c2826a3fa4772e67132ae	eb92f681496a1c1956aaf75c1d131e627f29ecf7e923640cb5a5ab49c9db153ba3
m/44'/0'/0'/0/6	1FqngalZpIDZMNTYj7bH9UGDeYzASjYmz	02e46bb4b84c5be4b0776ce7a22f6eed8ce2bf1496c3b377698275940bc180a69	8ad7addaed3e61c11686ffcd410daa4a61e0cb36ef8047bc870ad804080f3e7b
m/44'/0'/0'/0/7	1531m6a8F87vRNngm86mLoEbQ2QN82P15Wq	02086767073710cd80088a5b1ec59aa8da083f697182fd079afc707648866ba58d	cb7b6fd3091019ad30ca519a8a1a12846344e2a1f9f16580e2d647911a68107
m/44'/0'/0'/0/8	1L3mHgyPR8K33vqEFCF656MJG985v6kL	02f9c1840c6817af5a7d449c4f2e76d4dba2133440ea801bed3b0635eae550ee8	c5eaf4326111c2aa53713c63c81e78bac281bb7735a790a0c768f9b3d485ee1
m/44'/0'/0'/0/9	15gwgk21x14E2QtpCUP9844wMMTt9NpTus	029ba3ce933b7eadd35a2590be66a9f670b7a664f25d83bae8509d2fa4f1cf6d7	e9154250b567af2cd2c900ccf0793086975e99c53c7f38c3a8b0f6a24debec
m/44'/0'/0'/0/10	1ANQd5nufuTw8FnC7R3poeKAFng12MsnY	03b5a34199e67f2720242b20e62ed69521eaa0cf9a999b0860f6f4469cce0d3f	4011a9e2a0c851fb03896a004518644d250fec61c819d407d8cae3a11c06a50
m/44'/0'/0'/0/11	1DPbGL25B2o4WUC995CfQ7QGz6V7oPDMc	02e2c64c5a0c48bd4ceb679274cd367eeca1f552351fa6926d793bc61304d52cd4	4fc14989d7d750c2124ead96eb039c9002dfb7fad92470a6d798ca5c122f001
m/44'/0'/0'/0/12	17moFMK73NMTeRA6PLBERQD6ernAJ2uip	038b1a665ed8746f2f848f6a31b832e99f962f6d809ede84da890a7b020fc7da	e788b7b6df93b0ee33ad76395de3532d10f5d3d1b863ef284929688542158
m/44'/0'/0'/0/13	19weZW9LEcuvFpeJLnGw91sYXECyXis6fk	0227a937f274cd42bc6f31428da30e83d665af65e7a0094130622604685444ccb	a2c50cbb3c7c8d37165472a4e39c44a55d03111cfc3fde38687a8144fc7c5ac
m/44'/0'/0'/0/14	1PsfJSDj9nadmhfZ2luHnR58Bp5p7lb	039c4fa91d28ef9f027d4b7e182ea13b09c6ac5028c6fca401e477012b3b9d4852	616f8b33fabde8d8f066969039f1fae8f49733ac7b75c590f03d07c08e661fac
m/44'/0'/0'/0/15	1DB4hKQMSE8ad8Hj7TsYNiCpyakLEH62AE	032a843774a7408f954b36454ae8bad550fd83ee48ca5983f83072c980f52a65	f9d9de5eeb23665f9cbedb14327b26746205284800b513672e554f6e7e0b941
m/44'/0'/0'/0/16	12k9h12Z7r8b7NhtHrHjRy3SFZ5T5uIM	02991526227b62a7682f93446994be1028754d38a69a76f2de7c50a4a0dc449d1	41662497a6e39f2763136606016db70f4da75adbe2d6c2146922719ef18028f
m/44'/0'/0'/0/17	147CUSThwa5djmuaXax5zswuRslQDskK	028c3ad70abea817af51919c92ac961e5418ceff07437b520a3dffae5c74d76e	a2cc1d15cfff5c3dd95f8b883fe1df9524b644d4f021160a9bd2930f119465d
m/44'/0'/0'/0/18	1Ddmjmt6x4hAJC9NCWbimLsbbuUYUjYQTgm	0232f1ab425ae1e5f5d333126837d61a19ce815cab3b116bfe82a495f712623bf	aa7d45db7de78582d79b63e62d5244947595f0df1b0b38f548287d7c544b21
m/44'/0'/0'/0/19	14Aaz7Tuc4d3nKhQ3DuP7y7qEmvQznX	02b6e82feb196d90b8a24fc22c29a03c39c1d64e60c6b3fedb74b9f7c535caf4	3d777db8780b63b91ec9532fca4e54ca6928f300995d0f5a74a82be3b356228
m/44'/0'/0'/0/20	1PQEUmFurVAiK82jwBQvz10dWymzbF	02cf4f32e1efefa34ad404d3c4d9e2c8b7cc4a71f96cdabd41527b05417c17f1	2a2dc4965f846f3bd81dca1b0fe829971a0d8dd532cef0d330f3b1dd41cb2d
m/44'/0'/0'/0/21	1BAghBjpy42ojp8FCU4d3yNUS7Gnh	02255eca8b20c5dce2d861a9e32192849e15ada501cc08f5c8c2fc1bed05d97738	d21a8f200028d6a23aeb7447b9ca3f9ff4d11055c77e71e3e37375b0b21742
m/44'/0'/0'/0/22	1PRLGtU2WQ1L943fjyP9j5jrtaoZnSS	02c890555cd664eaf789a301dc4617853efbcbe56f9c3dbdf937677a5a0b3888e12	8c37996affe5e8169d2da115cced280ac20659c89412bf075a5cb52f6eae709
m/44'/0'/0'/0/23	1Nd3t3WRHUCmPwzKpKcKtRHRUdm6aP7vg	021d78350c14c1131a03311244bd929ea76614e3ce88b17c9c66002212ad7e4	c7b42c78a223c9abe0710b4d6fe536c3994401796ef6d2b23cb1a57951f8ea7

지갑 조회

1) 문장과 비밀번호 랜덤바이트를 입력

2) 지갑의 MasterNode 정보를 제공

(‘1.지갑 생성’과 동일한 출력 화면. ‘랜덤바이트의 초기 값을 받는다’는 차이일 뿐)

출력

지갑 조회 메인화면

지갑 조회

사용자 정의 문장을 입력해주세요.

테스트 문장입니다.

사용자 비밀번호를 입력해주세요.

테스트 비밀번호입니다.

랜덤 숫자를 입력해주세요.

32545

조회

지갑 조회 출력화면은 지갑 생성 출력화면과 동일하다.(생략)