一、Solana介绍

Solana是一个新兴的高性能的公链，它提供了快速、便宜且可扩展的交易体验，每秒能够处理数千笔交易，并且出块时间达到了亚秒级。它通过拜占庭容错（BFT）共识机制实现了这一点，该机制利用了一种历史证明（PoH）的创新的密码学函数。并且它还支持使用Rust，C++和C语言来编写智能合约。
官网：https://solana.com/zh

> 之前开了btc、eth、tron等的钱包，现在空闲记录下solana生成离线地址。

钱包

- BIP32：定义 Hierarchical Deterministic wallet (简称 “HD Wallet”)，是一个系统可以从单一个 seed 产生一树状结构储存多组 keypairs（私钥和公钥）。好处是可以方便的备份、转移到其他相容装置（因为都只需要 seed），以及分层的权限控制等。
- BIP39：将 seed 用方便记忆和书写的单字表示。一般由 12 个单字组成，称为 mnemonic code(phrase)，中文称为助记词或助记码。例如：

```
soldier dish answer treat exhibit blade diary glory arrange
shoe ocean card
```

- BIP44：基于 BIP32 的系统，赋予树状结构中的各层特殊的意义。让同一个 seed 可以支援多币种、多帐户等。各层定义如下：

```
  m / purpose' / coin_type' / account' / change / address_in
dex     //purporse': ???44', ???BIP44  //coin_type': ????????
, ????????, ??BTC?0, ETH?60,TRX?195  //account: ???????????
0??  //change: ??0????(????)???1??????????????????????????????
???????????????????????????????????? (??????0)  //address_i
ndex: ??????0???????????  //btc??? m/44'/0'/0'/0  //eth???
m/44'/60'/0'/0  //trx??? m/44'/195'/0'/0
```

币种类型列表

依赖

```
<!-- https://mvnrepository.com/artifact/com.portto.solana/web3 --><dependency>    <groupId>com.portto.solana</groupId>    <artifactId>web3</artifactId>    <version>0.1.3</version></dependency>
```

依赖库编译时遇到的问题：卸载2019版本的idea，装了2022版本

```
// This class file was compiled with different version of Kotlin compiler and can't be decompiled.//// Current compiler ABI version is 1.1.15// File ABI version is 1.6.0
```

生成地址及私钥

```
byte[] seed = MnemonicUtils.generateSeed(mnemonic, "");SolanaBip44 solanaBip44 = new SolanaBip44();//M/44H/501H/0H/0Hbyte[] privateKeyFromSeed = solanaBip44.getPrivateKeyFromSeed(seed, DerivableType.BIP44CHANGE);TweetNaclFast.Signature.KeyPair keyPair = TweetNaclFast.Signature.keyPair_fromSeed(privateKeyFromSeed);System.out.println("??0?" + Base58.encode(keyPair.getPublicKey()));System.out.println("??0?" + Base58.encode(keyPair.getSecretKey()));Account account = new Account(keyPair);System.out.println("Account??0?" + account.getPublicKey());System.out.println("Account??0?" + Base58.encode(account.getSecretKey()));
```

BIP44助记词生成N个地址

```
//?? getPrivateKeyFromSeed(seed, DerivableType.BIP44CHANGE);for (int i = 0; i < 10; i++) {    HdKeyGenerator hdKeyGenerator = new HdKeyGenerator();    SolanaCoin solanaCoin = new SolanaCoin();    HdAddress masterAddress = hdKeyGenerator.getAddressFromSeed(seed, solanaCoin);    HdAddress purposeAddress = hdKeyGenerator.getAddress(masterAddress, solanaCoin.getPurpose(), solanaCoin.getAlwaysHardened());// 44H    HdAddress coinTypeAddress = hdKeyGenerator.getAddress(purposeAddress, solanaCoin.getCoinType(), solanaCoin.getAlwaysHardened())
;// 501H    HdAddress accountAddress = hdKeyGenerator.getAdd
ress(coinTypeAddress, i, solanaCoin.getAlwaysHardened());//0
H    HdAddress changeAddress = hdKeyGenerator.getAddress(acc
ountAddress, 0L, solanaCoin.getAlwaysHardened()); //0H    Ac
count account1 = new Account(TweetNaclFast.Signature.keyPair
_fromSeed(changeAddress.getPrivateKey().getPrivateKey()));
  System.out.println("Account??" + i + "?" + account1.getPub
licKey());    System.out.println("Account??" + i + "?" + Bas
e58.encode(account1.getSecretKey()));}
```

私钥转换地址

```
package com.hlf.test.solana;import com.portto.solana.web3.Ac
count;import com.portto.solana.web3.util.TweetNaclFast;impor
t org.bitcoinj.core.Base58;/** * @ClassName: PrivateKeyAddre
ss * @Author: huanglefei * @CreateDate: 2022/4/2 8:29 PM * @
Description: * @Version: 1.0 **/public class PrivateKeyAddre
ss {    //??0?2Hyaw6rryApLpffVYZxvT2BTAAARoJzoCBSs6Zy3bVow
  //??0?3WWsrp38veGfPJcdfmPDwGwqgaGGFQ7uZrk61rcYCbGyKjFXLYWi
d6CJgBUXTA8Ls2vSS8gMGhjtFrGSLYuAtZ4D    public static void m
ain(String[] args) {        String privateKey = "3WWsrp38veG
fPJcdfmPDwGwqgaGGFQ7uZrk61rcYCbGyKjFXLYWid6CJgBUXTA8Ls2vSS8g
MGhjtFrGSLYuAtZ4D";        byte[] decode = Base58.decode(pri
vateKey);        Account account1 = new Account(TweetNaclFas
t.Signature.keyPair_fromSecretKey(decode));        Account a
ccount2 = new Account(TweetNaclFast.Signature.keyPair_fromSe
ed(decode));        System.out.println("???????" + account1.
getPublicKey());        System.out.println("??????-
???" + Base58.encode(account1.getSecretKey()));    }}
```

示例代码

```
package com.hlf.test.solana;import com.portto.solana.web3.Ac
count;import com.portto.solana.web3.util.TweetNaclFast;impor
t com.portto.solana.web3.wallet.*;import org.apache.commons.
lang3.StringUtils;import org.bitcoinj.core.Base58;import org
.web3j.crypto.*;import java.io.File;import java.io.IOExcepti
on;import java.math.BigInteger;/** * @ClassName: MnemonicAdd
```

```
ress * @Author: huanglefei * @CreateDate: 2022/4/2 8:19 PM *
 @Description: * @Version: 1.0 **/public class MnemonicAddre
ss {    private static final String KEYSTORE_PATH = "/Users/
huanglefei/Downloads/";    public static void main(String[]
args) {        String mnemonic = "soldier dish answer treat
exhibit blade diary glory arrange shoe ocean card";        i
f (StringUtils.isBlank(mnemonic)) {            try {
        // generate Mnemonic and keystone File
  Bip39Wallet bip39Wallet = generateBip44Wallet("hlf", KEYST
ORE_PATH);                //???                mnemonic = bi
p39Wallet.getMnemonic();               System.out.println("
????" + mnemonic);            } catch (CipherException e) {
               throw new RuntimeException(e);            } c
atch (IOException e) {                throw new RuntimeExcep
tion(e);            }        }        byte[] seed = Mnemonic
Utils.generateSeed(mnemonic, "");        SolanaBip44 solanaB
ip44 = new SolanaBip44();        //M/44H/501H/0H/0H        b
yte[] privateKeyFromSeed = solanaBip44.getPrivateKeyFromSeed
(seed, DerivableType.BIP44CHANGE);        TweetNaclFast.Sign
ature.KeyPair keyPair = TweetNaclFast.Signature.keyPair_from
Seed(privateKeyFromSeed);        System.out.println("??0?" +
 Base58.encode(keyPair.getPublicKey()));        System.out.p
rintln("??0?" + Base58.encode(keyPair.getSecretKey()));
   Account account = new Account(keyPair);        System.out
.println("Account??0?" + account.getPublicKey());        Sys
tem.out.println("Account??0?" + Base58.encode(account.getSec
retKey()));        System.out.println();        //M/44H/501H
/0H/0H        //???????n??????        //?? getPrivateKeyFrom
Seed(seed, DerivableType.BIP44CHANGE);        for (int i = 0
; i < 10; i++) {            HdKeyGenerator hdKeyGenerator =
new HdKeyGenerator();            SolanaCoin solanaCoin = new
 SolanaCoin();            HdAddress masterAddress = hdKeyGen
erator.getAddressFromSeed(seed, solanaCoin);            HdAd
dress purposeAddress = hdKeyGenerator.getAddress(masterAddre
ss, solanaCoin.getPurpose(), solanaCoin.getAlwaysHardened())
;// 44H            HdAddress coinTypeAddress = hdKeyGenerato
r.getAddress(purposeAddress, solanaCoin.getCoinType(), solan
aCoin.getAlwaysHardened());// 501H            HdAddress acco
untAddress = hdKeyGenerator.getAddress(coinTypeAddress, i, s
olanaCoin.getAlwaysHardened());//0H           HdAddress cha
ngeAddress = hdKeyGenerator.getAddress(accountAddress, 0L, s
olanaCoin.getAlwaysHardened()); //0H           Account acco
unt1 = new Account(TweetNaclFast.Signature.keyPair_fromSeed(
changeAddress.getPrivateKey().getPrivateKey()));
System.out.println("Account??" + i + "?" + account1.getPubli
cKey());            System.out.println("Account??" + i + "?"
 + Base58.encode(account1.getSecretKey()));        }    }
 public static Bip39Wallet generateBip44Wallet(String pwd, S
tring dirPath) throws CipherException, IOException {
File dir = new File(dirPath);        if (!dir.exists()) {
         if (!dir.mkdirs()) {               throw new Runti
meException("make wallet dir error");           }        }
       return Bip44WalletUtils.generateBip44Wallet(pwd, dir)
;    }    public static String generateMnemonicFile(String p
wd, String mnemonic, String dirPath) throws CipherException,
 IOException {        // make dir        File dir = new File
(dirPath);        if (!dir.exists()) {            if (!dir.m
kdirs()) {                throw new RuntimeException("make w
allet dir error");            }        }        // string to
 pk        byte[] entBytes = MnemonicUtils.generateEntropy(m
nemonic);        BigInteger entBigInteger = new BigInteger(e
ntBytes);        ECKeyPair entEcKeyPair = ECKeyPair.create(e
ntBigInteger);        return WalletUtils.generateWalletFile(
pwd, entEcKeyPair, dir, false);    }}
```

控制台

```
Connected to the target VM, address: '127.0.0.1:56354', tran
sport: 'socket'??0?2Hyaw6rryApLpffVYZxvT2BTAAARoJzoCBSs6Zy3b
Vow??0?3WWsrp38veGfPJcdfmPDwGwqgaGGFQ7uZrk61rcYCbGyKjFXLYWid
6CJgBUXTA8Ls2vSS8gMGhjtFrGSLYuAtZ4DAccount??0?2Hyaw6rryApLpf
fVYZxvT2BTAAARoJzoCBSs6Zy3bVowAccount??0?3WWsrp38veGfPJcdfmP
DwGwqgaGGFQ7uZrk61rcYCbGyKjFXLYWid6CJgBUXTA8Ls2vSS8gMGhjtFrG
SLYuAtZ4DAccount??0?2Hyaw6rryApLpffVYZxvT2BTAAARoJzoCBSs6Zy3
bVowAccount??0?3WWsrp38veGfPJcdfmPDwGwqgaGGFQ7uZrk61rcYCbGyK
jFXLYWid6CJgBUXTA8Ls2vSS8gMGhjtFrGSLYuAtZ4DAccount??1?HwKQF8
979cc1pwpGD8xD1GppJJTbvzbSXxQgjP5hmjCEAccount??1?4JAgHSGvBnS
eNNiwk17eqHMdLXFqw53mmiRL8ef9rpL1ZXzVJ4GUPgYbWcRhpaZnohpt7fY
```

```
e45thJKJfEed8FMrAAccount??2?5iCnsERHGXMHApMC1J4EsTnEqcWfSew2
yGmAGEjsr12ZAccount??2?2V9wRtqRZYAeyTHx99sKN3BNxpbVgt82Trejp
mBLNR593ZqnxhteC2m9mWQuiEg9VFbttBhE4YzmxZSxZdQwaVrqAccount??
3?22ogk3ArAet5SL43zVYT4Ej8FaBfgZyFwFG8biJx9VBbAccount??3?3dE
wx6otjGzvmXm4dB518dHpGX1cxdfnm5E4V9r1Hw4gjyDPWRARariQ293TNdo
jbGRWbhawLgWET58HF5dZufkqAccount??4?CnmxbaWTKqKWvCnMSJgaAP8a
xfxL3udy7kLkgAU32qVMAccount??4?2JSvZYqaxxg92VxfpTBNonR8xQUjK
oADudjzquZ33FSiMbhcdk2dfawgWMBF2NXtGReLXiz3D1678EEPsnGsaQXdA
ccount??5?5gMkZhETUgBMVRVxzdZarHSTLvFFCziCkSkKrSurWTWjAccoun
t??5?4DiUbrs7vcFYMCyqe4dMehiNQBhx2iRbGKsW6nmBJLzyyPuRMRdorqc
Eq2yME1wM7skxTMRpcYcA9dCkSduQGmUfAccount??6?5t1DS9h3tvCGCQfW
Sg4MP8bpZDPZp4Gavu2w5p7hymyzAccount??6?2hAst5LWJuBpeqE5C4H3M
vTQb2BzC4mGCrfSi9QRHA7G322KgFmp4kVEcssry1wvLVMFv7WaUUDkFosuX
eWnz8txAccount??7?DLYHSMwPodh5Qms93JcHJL17vfFsqiqJ7SBEVShqdY
R8Account??7?tpn1HxEWXoChunYWeixisxJ5DefhGzMhySu5M2VGUWCiaie
YBUGPVJWSXfPqcxPyxqjbwEypHAktVsPbAB4tJ8JAccount??8?DoBeV5gBo
jXEF9WjmwVAd2Ukd5PZrxFLL8taC4h4YynuAccount??8?PbkuETqeHWuCHc
rYSWPVDHvmD57D25CLdSUfYe3d1FpXK3qDBZj6UWT9mcy6LWvHimHmY4ciVd
R14dmk7EWPAJHAccount??9?6V5TdtRzBMNFAbbfZUQ6y7cQzk7Eg1HPnWPJ
uENSmckuAccount??9?4D9sM3zcQyTjrTtnfruNYLpA4HDRtU9PBkxVmCzYB
LVnmjjKBPutumS3Q4MQP2whBJGM4jLhMvp31MJEaVPWQEAhDisconnected
from the target VM, address: '127.0.0.1:56354', transport: '
socket'Process finished with exit code 0
```

Phantom钱包对比

solana生态钱包中生成的地址。