区块链资产钱包的定义
：区块链中的钱包和我们日常生活中使用的钱包是不一样的，我们平常用的钱包是用来装钱的；在区块链中，我们的资产是类似比特币、以太坊这样的各种代币或者通证，区块链中的钱包不是用来装这些资产的，而是作为密钥的管理工具。

这里要注意听，区块链钱包要通过数学算法生成的一个密钥来管理的，密钥是成对出现的，由一个私钥和一个公钥所组成。公钥经过一定的算法就得到了你的钱包地址，这个地址就是用于交易时别人给你打币的地址；它们是一串数字和字母的组合，看起来有点像乱码。而私钥就是交易时对这笔交易进行数字签名，从而证明你拥有交易的输出权。所以地址是可以公开的，可以给任何人看；而私钥是千万不能给别人看的，谁拥有了私钥，谁就拥有了对钱包资产的控制权。

根据区块链钱包储存私钥的方式是否联网，钱包可以分为冷钱包、热钱包两种。**冷钱包也称离线钱包，**在离线的环境下网络不能访问到你私钥的位置。冷钱包可以是专业的硬件钱包，可以是拔掉网线的电脑，也可以是锁在保险柜里的U盘，冷钱包的私钥或者助记词更是远离网络，可以写在纸上，木头上，或者牢记在你的大脑里，市场比较知名的库神钱包就是冷钱包。

而热钱包正好相反，是处于一直联网状态的，比如电脑客户端，手机APP钱包，浏览器钱包等。

热钱包相对于冷钱包被盗的风险更大，但冷钱包使用程序会更复杂，对于新手来说更为困难，且携带不便捷，一旦损坏，数字资产将永远找不回来。冷钱包一般建议用于储存大额数字资产。比如前面我们讲到的交易所或者 一些基金公司，而热钱包，移动方便，只要有网都可以使用，但被盗的风险也高，一般建议储存小额资产，市场比较知名的就是imtkoen，Cloud Wallet。

这里重点给大家介绍以上Cloud Wallet,Cloud

Wallet项目成立于2017年3月，是武汉云链科技旗下的项目，Cloud Wallet从2017年6月上线以来，经过两年多的时间努力，他们在钱包的安全和坚固性上做了很大的努力和突破，他们通过领先的技术、安防过硬、应用丰富等特点赢得了广大用户的信赖，同时多项技术独步全球电子钱包领域，以明显的技术代差领跑全行业，目前用户已经突破120万大关。

地址

在数字货币交易的过程中，只要知道对方的钱包地址，就可以给对方转账了。它相当于我们现实生活中的银行卡号，而这个地址是创建完钱包以后就会自动生成一个钱包地址，那么这个地址是怎么来的呢？创建钱包的时候系统由椭圆加密算法（ECDSA）来产生私钥和公钥。基于椭圆加密的原理，由私钥是可以计算出公钥的，然后再由公钥经过数字签名和哈希算法的运算就会得到钱包地址。现在清楚了吧，地址不等于公钥，或者说地址是公钥的另外一种表现形式。有了这个钱包地址你就可以用于接收别人给你转币了。

那私钥是什么
：私钥类似于银行的账号密码，它的本质是一个随机数，私钥储存在钱包文件里，由钱包软件进行管理，私钥本质上是一个64位的随机数，比如：6KYZdSDo39z3GDrtuX2QcowGnNP5zTd7yfr2SC1j239sBCnWjee。只要有了私钥，就代表了你拥有了对应的比特币，私钥是唯一能够证明这笔资产是你的资产的唯一信息，并且能够转账交易使用这些比特币，所以保管好自己的私钥是非常重要的。

所以保管私钥一定要小心，为了防止被黑客攻击，大家都是用笔写在纸上备份起来，并且保管好。要是你丢了，那你的资产就永远的找不回来了，因为区块链世界没有任何机构提供这个服务。再说一遍，私钥不要用文本的方式，不要用图片的方式保存在手机或者电脑上，不要通过网络传输你的私钥。这是大家一定要小心的地方！

公钥：
公钥由私钥通过椭圆曲线加密算法生成的，变换后是一个65个byte的数组，一般是通过16进制处理后显示。早期比特币开发者不知道可以压缩公钥，压缩后公钥有33个byte数组。拥有私钥就能生成钱包地址以及数字签名，公钥是可公开的。

助记词
：在创建钱包的过程，会生成一个助记词，而且会让我们备份，助记词一般由12个单词构成，2个单词之间由1个空格隔开，这些单词都来源于一个固定词库，是由私钥根据一定算法得来，所以私钥与助记词之间的转换是互通的，助记词实际上就是私钥的另一种表现形式。助记词最好用纸记下来，千万不可用联网的东西来保存，照片也不行。助记词的功能等同于私钥，如果别人拿到了你的助记词，就可以用来导入钱包，进而进入钱包并拥有这个钱包的掌控权。

KeyStore：KeyStore看上去就是JSON 格式的字符串, 一般以文件形式存储。Keystore的本质是加密后的私钥，Keystore必须配合你的钱包密码来使用才有效。