大家好，这周的课程主题是：  防患于未然，数字资产持有者的“安全”必修课

先来介绍一下钱包的重要性

区块链钱包简介：

由于以比特币为首的加密货币所采用的去中心化架构特性，用来储存加密货币的钱包，实际上并非将货币放在钱包内，而是泛指能在区块链上交易所使用的公钥与私钥、私钥所对应的地址、该地址（群）的货币结算，以及货币交易的支援系统。有时该系统甚至包含了整个区块链的记账与维护。由于加密货币是以区块链为主，所以实际金额是以区块链最后的记录结果为准。（维基百科）

比特币钱包基本功能：

（1）生成比特币地址

（2）接收比特币

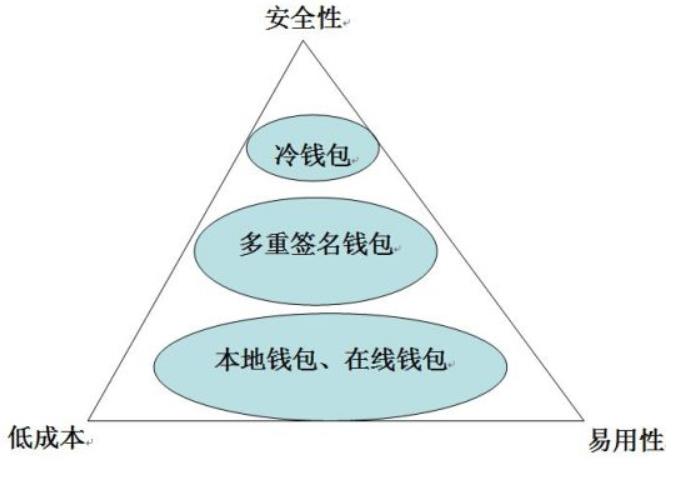
（3）发出比特币

（4）生成并导出私钥

（4）对自己的每笔交易，进行签名核实

（5）保护你的资产

如果说比特币是钱的话，你的钱包地址就是你的银行卡号，不论是别人给你汇钱，还是你给别人汇钱，都需要用到这个地址



1、冷钱包

数字货币安全的存储方式，冷钱包是脱离网络连接的离线钱包。也就是说，你不会面临被网络黑客/木马袭击，出现丢币，盗币等情况，但因为操作相对复杂，不适合刚开始的小白。

优点:

安全等级MAX

自己拥有私钥

随时可以提币，转币

真正实现了个人资产不可侵犯，不受别人监管

缺点：

价格较贵（RMB1000+）

只支持大部分主流币种，小币种（新的ICO）不能存在冷钱包里

操作相对复杂

适宜人群：拥有价值10+比特币，准备长期持有，屯着不动，不炒短线交易的人。

推荐：Ledger Nano S （目前市场性价比最好的冷钱包，方便好用，淘宝就能直接买到）





目前Ledger Nano 支持的币种

在手机AppStore，电脑上可以直接下载的钱包。因为轻钱包的私钥也是掌握在自己手里，安全等级比较高。记住！一定要把私钥保管好，放到一个安全的地方

优点：

操作简单, 手机上免费下载后，可以直接使用

自己拥有私钥，自己的币掌握在自己手里

缺点：

手机有一定几率被黑客攻击

只支持大部分主流币种。很多拥有新技术的币，不支持存入手机钱包

适宜人群：闲钱屯币，募资项目，不经常短线交易的人。

推荐：

比特派 ：国内安全，方便的轻钱包之一。钱包的设计和使用都不依赖于任何第三方管控。 就算比特派的设计团队没了，钱包里的币也是归你所有。

BlockChain：全球著名的轻钱包，目前只支持：比特币和以太坊

imToken：以太坊系列钱包。支持所有ERC20代币的存储。







交易所：

想问大家一个问题，我们存在交易所的币，我们真正拥有吗？不！钱包的私钥是在交易所手里，你账户上拥有的资产，只是交易所给你打的一张白条罢了。但为什么还有人把钱放在交易所呢？交易所解决的痛点就是方便快捷，还有一定的安全保障。

假如你拥有很多不同的代币，如果全部自己掌控，估计要申请不同冷钱包，轻钱包，在线钱包，来分别存储不同种类的代币。同时要一口气管理6-7个钱包，就会变得十分琐碎、麻烦。但如果是存在交易所，你只需要记住你的账户密码，谷歌验证，就能把所有的币聚集在一起。还有交易所是专业机构管理，基本不会出现丢币，盗币等情况。就算被盗了，交易所一般也会给用户等值的补偿。

优点：

1. 操作简单，普通人可以很快上手

2. 安全等级高（大部分交易所的钱包都是冷钱包管理）

3. 流动性高，交易简单迅速，当你想买入，卖出的时候，不用从其他钱包转入

4. 币种齐全，市场上的币一般都可以在交易所直接存储。

缺点：

1. 个人没有币的直接拥有权

2. 交易所账户密码可能被黑客盗取（所以一定要用谷歌二次验证）

3. 当交易所维护的时候，提币，充值可以会出现问题

小交易所：

小的交易所，他们是拥有你的钱包私钥的，意味着可以随时可以跑路，大家选择的时候一定要注意：投资币种较多，短期交易频繁，需要随时提现。

多重签名钱包

原理：取一个多重签名地址作为钱包地址，如果要动用这个地址上的币，必须有2个（或多个）私钥同时签名才可以。打个比方，就是一把锁，需要2把不同的钥匙一起用，才能打开。这样一来，我一把钥匙自己掌握（也可能是加密后托服务器保管，参看在线钱包），另一把交给服务器，如果只有一把钥匙被盗，黑客没有我本地的私钥。这样应该是多了一重安全。

缺点：多重签名机制看起来是更安全了，但易用性受到很大的影响，用户需要理解一些技术细节，还要保护好本地私钥和未来地址的私钥，学习和使用成本高了不少。

5、纸钱包和脑钱包

纸钱包和脑钱包并不是完整意义上的比特币钱包，因为使用纸钱包或脑钱包，你无法使用上面的比特币，发币时还得借助其他钱包导入私钥。纸钱包和脑钱包仅仅是保存比特币私钥的两种方式。

纸钱包：就是把比特币的私钥打印在纸上，然后保存起来，一般用于冷藏比特币，也可以作为本地钱包或在线钱包的私钥备份。

优点：打印私钥的环境是安全的，那么纸钱包安全性是比较高的，成本也很低。

缺点：要注意防火防水防盗，如果是热敏纸打印的，还要注意热敏纸字迹容易褪掉。

钱包的选择：

钱包首要的要求是安全，但是世界上没有绝对的安全。绝对的安全意味着绝对的高成本和绝对的不好用。绝对的安全是没有必要的，我们需要的是满足自己需求的相对安全。

比特币土豪：那大额比特币肯定建议冷储

对技术比较了解：多重签名钱包也可以试试

脑钱包：一般情况下不推荐使用，因为人的思维和记忆总是不那么可靠，但是脑钱包在某些极端情况下非常有用，比如战争、严重自然灾害，没有人能够抢走你的币。

最后总结一下，存放区块链资产的安全排名：冷钱包>手机轻钱包>靠谱交易所>小交易所

好的 今天的课程到此结束，接下来是互动时间，欢迎你提出感兴趣的问题