第23课：数字货...

大家好，我是丹华。上节我们研究了数字货币估值方法与泡沫，本节我们讨论区块链投资的最后一个话题： 投资风险。

任何投资都隐含了多个风险因素。投资者应清醒地认识到，区块链行业处于行业早期，且处于无监管状态，骗局遍地、乱象丛生是常态。要想在数字货币领域获得较高的回报，就必须深刻理解数字货币的投资风险。

本节内容主要包括：

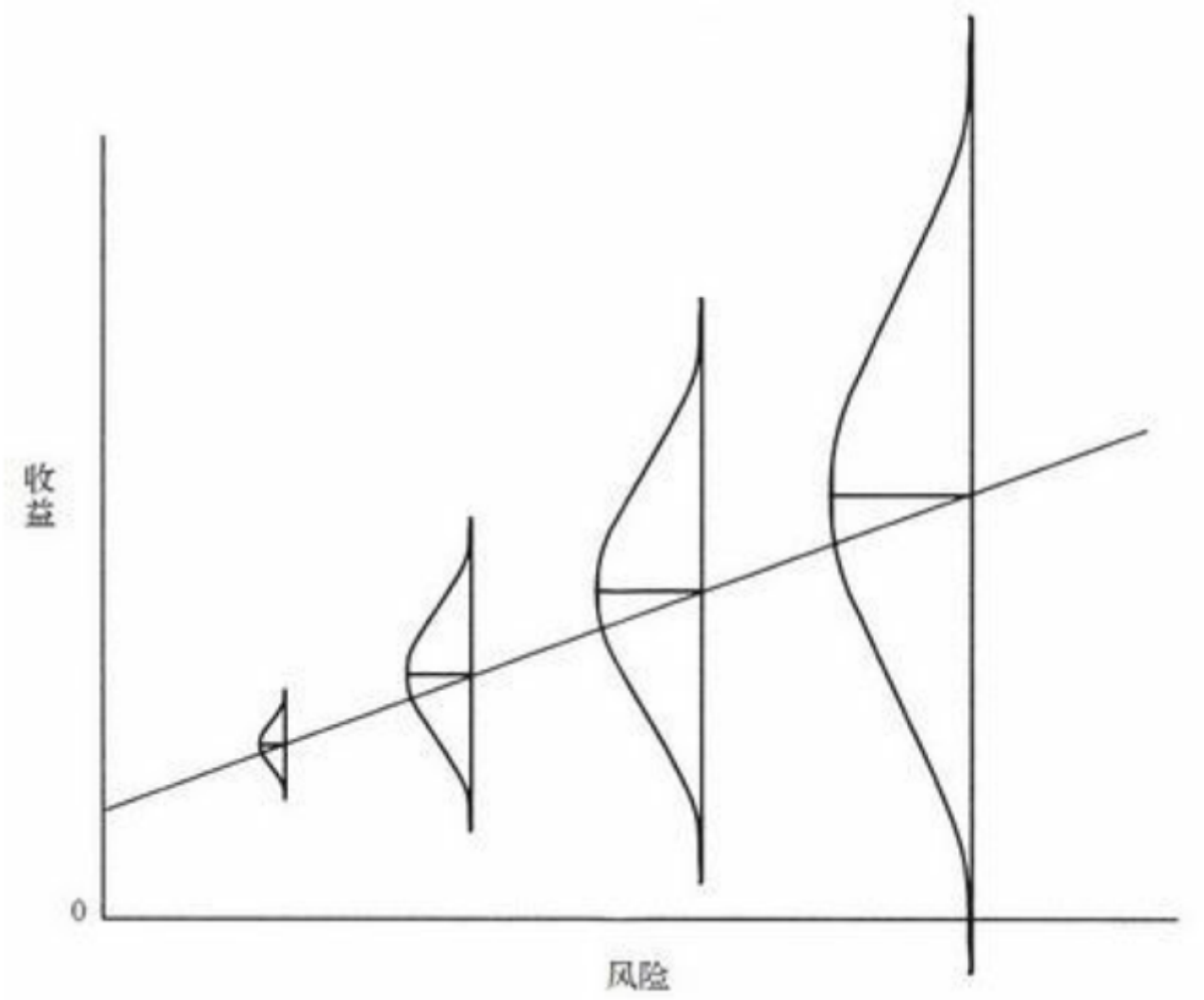
- 风险的哲学
- 跑路风险（项目方或代投跑路，发生于一级市场 ICO时）；
- 交易所风险（交易所被盗，发生于将币存于交易所时）；
- 流动性风险（交易所流动性不足，发生于日常交易时）；
- 私钥存储风险（发生于用户不当保存数字货币时）；
- 区块链分叉导致的操作风险（涉及分叉前后的操作时）；

炒币有风险，投资需谨慎。

风险的哲学

什么是投资风险?

一种严格的定义是：投资资金永久损失的可能性。另一种是指价格的波动率，波动率越大，一般而言风险越大。风险既是一种主观的判断，也是一种客观存在的可能性。风险没有发生，不代表这笔交易没有风险。风险一旦发生，就变成100%的风险事件，投资者就可能面临着资金的损失。



理解风险和收益的关系，如上图所示。风险越大，期望收益越大，同时期望收益的波动区间也很大，即损失的概率也随之增加。

价格的变化往往意味着风险，然后仅仅知道这一点无助于我们把握风险。更常见的方式时，建立一个分析框架，将你能想到的可能影响价格下跌的负面事件全部网罗进去，认真衡量每一项实际发生的可能性（虽然有时是极不靠谱的主观评估），并结合当前的价格表现，来“毛估估”当前买入的风险。

某种意义上，资本市场就是交换风险的地方，即俗称的“擦肩而过互道傻逼”。

众筹项目跑路风险

所谓众筹跑路是指，众筹项目发起人或代投方在项目募集资金结束后卷款潜逃。跑路不是数字货币行业独有的现象， P2P平台跑路时有发生，只不过数字货币有匿名性特征，更“适合于跑路”而已。

参与 ICO 代投时容易发生的风险有两种，一是代投者拿到参与者打过来的币后直接跑路，“简单粗暴。”二是在项目的代币上线并翻倍后，谎称代投失败，将募集到的币退给参与者，实际上，自己利用参与者的币赚取从 ICO 到上交易所后翻倍的利润。

说实话，项目跑路风险是很难事前分析发现并避免的，除非你不参加众筹。当前，国内数字货币行业的众筹 ICO 正风风火火，更多了解项目团队的实力、诚信和社会关系，也许能降低未来投资打水漂的风险。另外，数字货币行业也应设立规范，让众筹过程做到透明、可被监管、资金使用多重签名，或引入第三方监管等，或自我约束将规则写入区块链等，减少投资者对团队不负责任、跑路的担忧。

2018年著名的币圈跑路事件一览。

2018年2月的六点公会代投携款跑路，媒体称“是一次有组织有谋略的代投骗局”。

2018年2月，ARTS 被投资人联合举报涉嫌诈骗，并由此引发群体事件，数位投资人已将项目联合创始人蒋杰扭送至北京金融局信访办公室，蒋杰已被警方控制。

2018年3月的 “李诗琴”诈骗13个项目席卷1.5万个 ETH 跑路，所涉项目为 Refereum（RFR）。据“币沙龙”所述，经过投资者和众人层层排查，发现隐藏在 RFR 项目背后的多个项目均为虚假代投。几位带头人涉嫌将募集而来的 ETH（以太坊）充值到交易所进行变现。

德国公司 Savedroid 创始人在 ICO 筹集了 5000 万美元资金后高调的跑路了。Savedroid 此前通过 ICO 和直接融资筹集了 5000 万美元，在 ICO 结束后，该公司网站却处于脱机状态，官网上仅有一张写有“Aannd It's Gone”文字的恶搞配图。更奇葩的是，4月18日，他在 Twitter 晒出自己去埃及海滩度假的照片并配文称：“谢谢大家，都结束了。

交易所风险

如果投资者选择在某一交易所买卖数字货币，就面临交易所可能带来的风险。

交易所的风险主要在于，客户资产被盗、交易所关闭、交易所临时暂停交易或关闭提现的风险。历史上发生了至少6件件较为重大的数字货币交易所事件，简述如下。

Mt.Gox 倒闭事件

2014年2月，当时全球最大的比特币交易所 Mt.Gox 声称被黑客盗走85万枚比特币，宣布破产。Mt.Gox 是一家总部位于日本东京的比特币交易所，在交易高峰期，该交易所处理的比特币交易量占所有比特币交易所的80%。受此影响，比特币价格进入一个长达一年多的熊市。

Bitcoinica 倒闭事件

2012年3月1日，交易所 Bitcoinica 超过43 000枚比特币被攻击者窃取，价值20万美元。几周之后，2012年5月11日，该交易所再次遭遇黑客攻击，其热钱包中的比特币被掏空，18000枚比特币（约合9万美元）不知所踪。这起事件最终导致了 Bitcoinica 关闭下线。有谣言称创始人周同监守自盗，是两起盗窃案的幕后黑手。

Bitfinex 被盗事件

2016年8月3日凌晨，交易平台 Bitfinex 发布公告称“发现安全漏洞，119756枚比特币被盗，价值约合7500万美元。平台已暂时关闭比特币交易及提现业务”。受此消息影响，比特币交易价格从最高4043元人民币下跌至最低3005元人民币，单日跌幅一度超过25%。

日本交易所 Coincheck 内大量新经币 NEM 被盗

2018年1月，日本交易所 Coincheck 遭黑客攻击，交易所内大量 NEM 币被盗。据媒体称，被盗的 NEM 币总共5. 23亿个，价值5.3亿美元，约26万用户受害。随后，交易所发布声明所有提现服务暂停，并停止加密货币交易。

币安出现大量交易异常，疑似被盗

2018年3月8日，最大交易所币安发生大量异常交易现象，遗失被盗。但币安官方一直未予承认。事后，币安立即反应，关闭了平台的充币提币功能。

去中心化交易所 Bancor 被盗

2018年7月9日加密货币交易平台 Bancor 被黑客攻击，超过20000个 ETH（价值1250万美元）被窃取，同时还有价值约1000万美元的 Bancor 代币 BNT 也被窃取。

流动性风险

对于投资者来说，流动性风险是指在对市场价格不造成太大冲击的前提下，你可能无法快速地将持有的资产卖掉变现为现金（法币形式）。简单地说，你想买入或者卖出的时候，发现买不到或者卖不掉。

可以将流动性风险分解为三部分：买卖价差（bid-ask spread）、市场深度及市场和品种特性三种。

买卖价差

买卖价差就是最高的买价和最低的卖价之间的差额。在一个公开叫价系统中，会存在从高到低的一系列的报价。除非买入价与卖出价相同，否则这些报价不会成交。理论上说，如果交易者在买入之后迅速卖出该资产，账面净损失就是当前最高买入价格和最低卖出价格之差，英文中一般称为 bid-ask spread。买卖价差越小，该市场的流动性风险就越小。

市场深度

市场深度是指交易所报价中每一价位的所有报单量（即可成交量）。单一价位报单量越大，表明市场深度越好，可以承接的交易金额也就越高。如果报单量较小，表明市场深度较差，或市场很“薄”，很容易被击穿。

市场和品种特性

市场本身和品种自身的特性也会影响到流动性，比如债券到期、新股上市或退市等。

例如，交易所新上线的品种前几个月的交易量必然比较大，对应的流动性会非常好。随着价格逐渐稳定，交易活跃度下降，流动性也回归正常。一个品种的流动性也不是时刻稳定保持在一个水准的，比如暴涨暴跌时，长期横盘时的流动性状况，白天、晚上和凌晨都会有很大不同。还有些有明确的时间概念，比如期权和期货，那么在临近到期的几天，波动性会远大于平时，也会影响市场的流动性状况。

上面的分析仅仅是针对在交易所上线、随时都有公开报价的资产。然而，有些资产根本就没在交易所交易，不存在可供参考的公开报价，其流动性风险更是投资者首先要注意的问题。

跟日常交易有关的另一个风险是爆仓风险，发生在杠杆交易中，如期货期权等。

私钥储存风险

假如投资者选择自己保管数字货币，请务必理解以下几种技术陷阱（以 Bitcoin Core 这款软件为例）。

技术陷阱一：没有及时备份或备份错了钱包文件

很多人意识到重装系统时需要备份比特币的钱包，不过遗憾的是有部分人备份错了文件，如把比特币客户端的程序文件（C:\Program Files\Bitcoin）备份了下来，而钱包文件却没有备份，结果装完系统发现币没了。

技术陷阱二：忘记密码

不论是哪种形式的钱包（包括 Bitcoin core），都应该设置足够长、足够复杂的密码。

为何不能用自己常用的6位银行卡密码？

因为这么做是有安全隐患的：银行卡密码在输错几次后会被锁住，依赖穷举法破解是不可能的。但是在 Bitcoin Core 这类软件中，没有尝试次数限制，因此6位密码和没设密码仅一墙之隔。一般而言，密码还是越长越好，至少需要15位密码。

技术陷阱三：下载到篡改过的钱包软件

下载钱包软件一定要到比特币官方网站或者第三方钱包的官方网站。篡改过的钱包软件可以嵌入木马，或者黑客在钱包文件上做手脚，误导投资者把币汇入黑客的地址。

技术陷阱四：钱包文件被盗

钱包文件被盗是最常见、最隐蔽、危害性最大的技术陷阱。 钱包被盗有以下几种可能：

- wallet.dat 被木马盗取且没设置密码；
- wallet.dat 被木马盗取，设置密码了，但密码过于简单被暴力破解了；
- 没有感染木马，自己把钱包上传到了网上，密码被暴力破解了；
- 私钥被明文暴露过（如 blockchain.info 的用户通过电子邮件导出私钥），或导入/导出私钥的时候被木马获取；
- 私钥正好被人碰撞到。发生这种情况的概率小到可以忽略，一般发生这种事是由于钱包软件的随机数产生器有问题。

要确保钱包安全，理论上只要确保两点：一是保证没有木马，二是保证私钥不主动外泄。

区块链分叉导致的操作风险

主流的数字货币可能会分叉，产生很多所谓的分叉币，分叉币与母链比特币共享一套区块链、历史地址、历史公私钥和历史交易记录。因此，用户在处理分叉币和比特币时，一定要心里有数，分叉前的比特币和分叉后的比特币是不等同的。分叉前的旧地址在新旧两个链上都是有效

的，分叉后的地址，只在某一条链上有效。但是！另一条链认不出来这个地址是不是产生过，即使是新链未产生过的地址，也可能发送成功。已经发现有人误将旧 BTC（=新 BTC+BCH）发送到了 BCH 的地址上，那么你的新 BTC 就彻底消失了。

切记切记，分叉后的首次使用，一定要确保自己完全理解了分叉的具体意义和所有细节。