

53. 支付流程设计常见问题及最佳实践

[组合支付要不要拆支付流水](#)

[前端轮询查哪个域](#)

[查询要不要穿透到外部渠道](#)

[为什么要做同步受理异步处理](#)

[支付状态补偿怎么做](#)

[如何防重复支付](#)

[万一重复支付了怎么做](#)

[支付成功后用户关单了怎么做](#)

[返回码怎么映射](#)

[支付要不要做系统自动重发](#)

[支付渠道如何做隔离](#)

[支付资损防控怎么做](#)

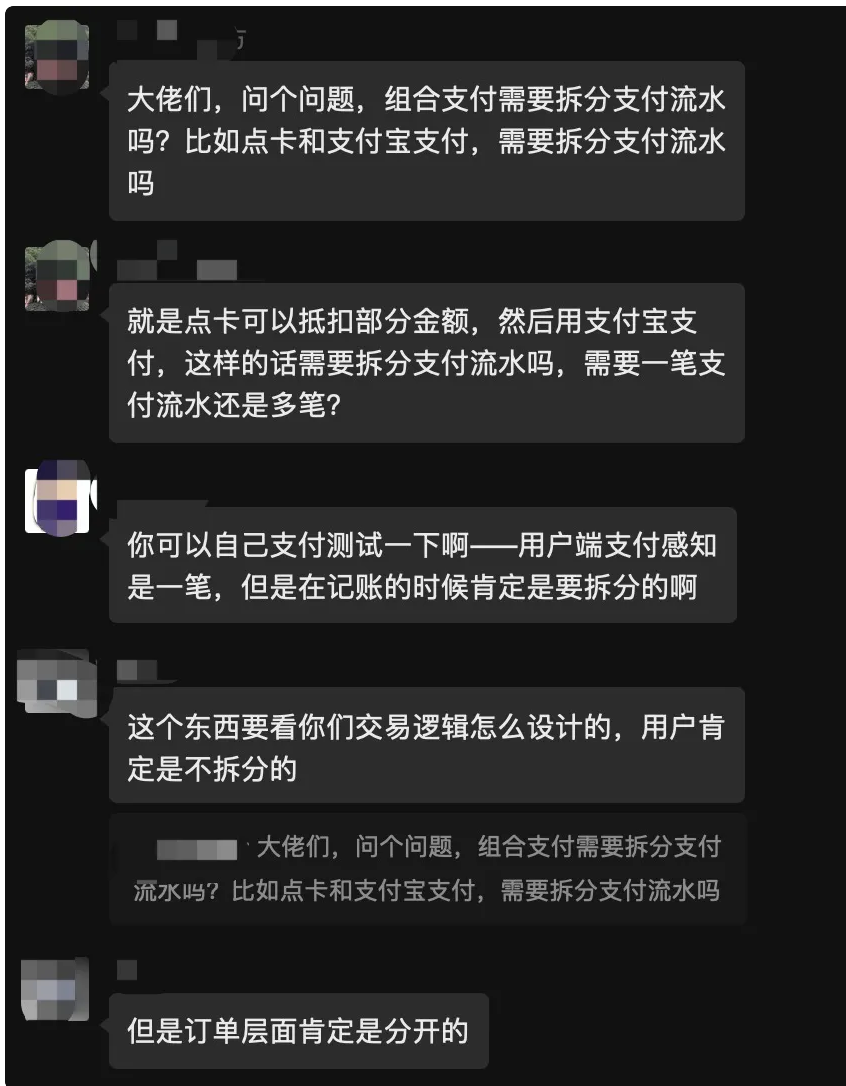
[支付路由怎么做](#)

[结束语](#)

大家好，我是隐墨星辰，专注境内/跨境支付架构设计十余年。今天聊一下支付流程设计的一些常见总是及最佳实践，包括：

组合支付要不要拆支付流水，前端轮询查哪个域，查询要不要穿透到外部渠道，为什么要做同步受理异步处理，支付补偿怎么做，如何防重复支付，万一重复支付了怎么做，支付成功后用户关单了怎么做，返回码怎么映射，支付要不要做系统自动重试，支付渠道如何做隔离，支付资损防控怎么做，支付路由怎么做。

问题来源于一个讨论，回答也是五花八门。



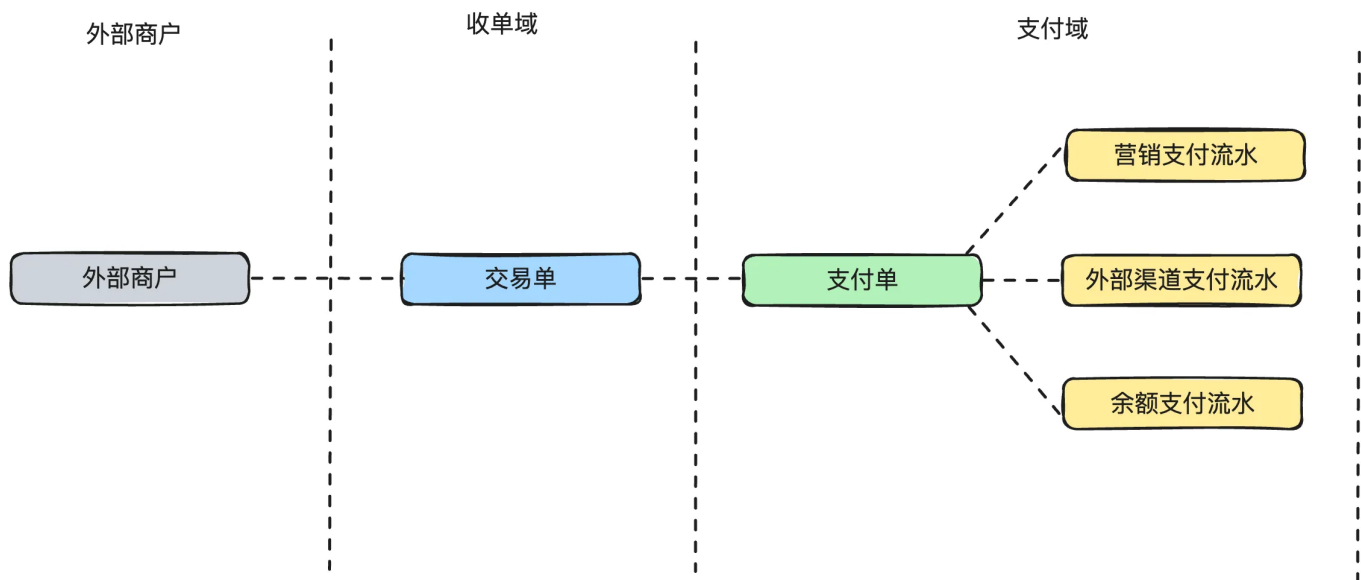
组合支付要不要拆支付流水

当然拆。不拆能不能做？也是可以做，但是坏处很多。有更优解的情况下，我们要选择更优解。

每一种支付方式都有自己的特性，包括但不限于支付金额、支付时间、状态等，如果放在一笔支付单，如何表达得清楚？

这里还有一个分层的概念，就是面向商户的是收单域，生成的是交易单，交易单下面可以挂一个主支付单，这个支付单是支付域的，一个支付单下面挂多个支付流水，一个支付方式就生成一笔支付流水。

由支付域来负责多个支付方式的组合，以及主支付单的推进。



前端轮询查哪个域

有人查收单域，有人查支付域。

我的观点是查收单域。因为收单是针对商户的，商户的订单成功了，才算成功。有时候可能内部出现故障，导致支付域成功但收单域没有成功，还有可能订单因为超时或用户主动操作已经关闭，这个时候支付域哪怕成功，也需要给用户退回去。

如果是用户充值，就以资金产品域为准。

为避免对收单域的数据库造成过大压力，建议加一层缓存。

标准收银台和前置收银台又有一点不一样。上面说的是前置收银台的情况。

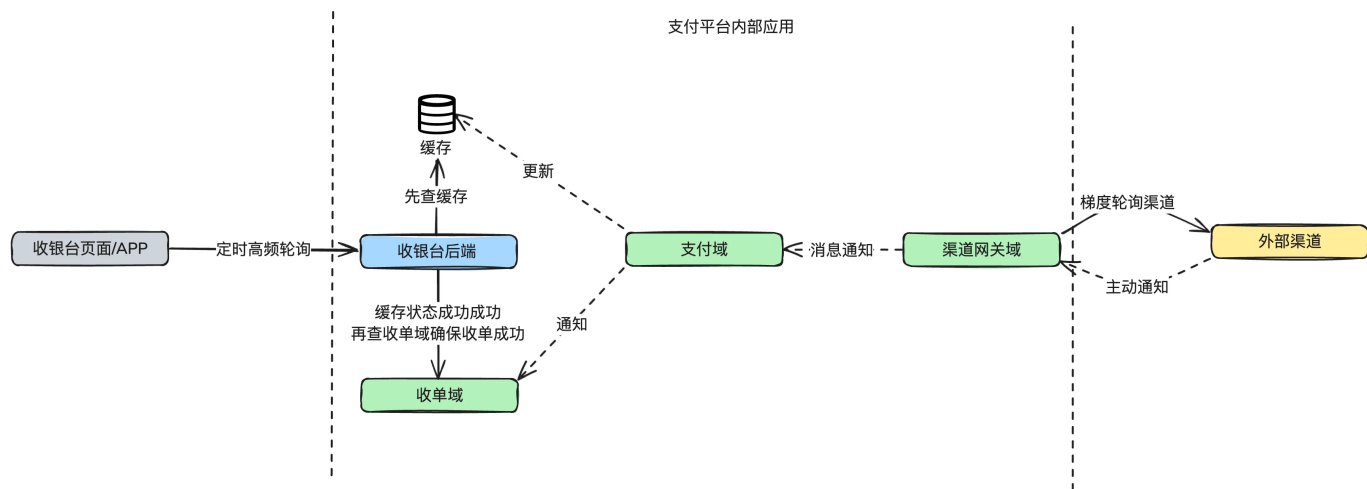
查询要不要穿透到外部渠道

很多人喜欢直接把查询穿透到外部渠道，比如用户提交支付后，在收银台页面转菊花，收银台页面会有一个定时任务高频查询后端的支付结果，这个查询请求链路：收银台页面->收银台后端->收单域->支付域->渠道网关域->外部渠道。

如果一旦网络抖动或外部渠道抽风，返回耗时增加，就会快速把内部应用的线程全部耗尽，极易引发雪崩。有兴趣的可以翻翻公众号前段时间发布的关于雪崩的超级故障。

正确的做法：

收银台只查自己的缓存，支付域有新数据后，更新到缓存，比如支付成功，或者需要跳到核身验证页面。



为什么要做同步受理异步处理

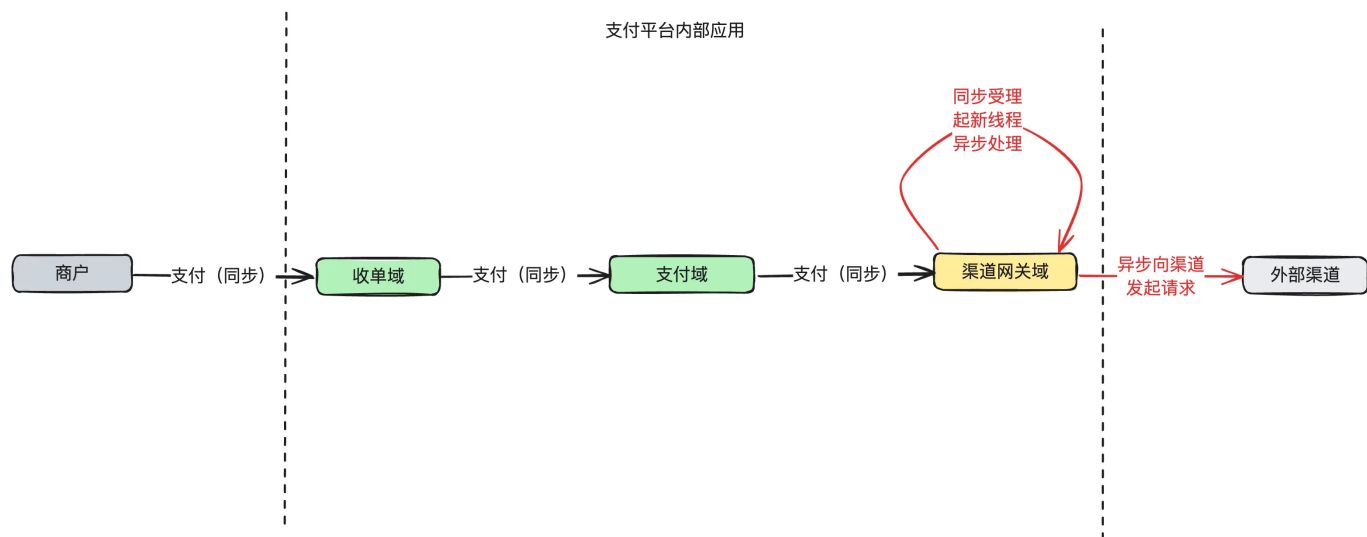
原理和上面的查询不要穿透到外部渠道是一个道理，如果一旦网络抖动或外部渠道抽风，返回耗时增加，就会快速把内部应用的线程全部耗尽，极易引发雪崩。

正确的做法：同步受理商户的请求后，马上返回给商户，然后再异步处理，发送给渠道。

是不是每个域都做同步受理异步处理？也不是，那样就太复杂了。

可以选择在收单域做，也可以选择在渠道网关域做。推荐在渠道网关域做，因为外部渠道的耗时最不可控，大不了多部署几台网关，多开些线程。

如果一定要选择所有域都做，那也是个人的自由。但强烈不建议全部同步调用出去。



支付状态补偿怎么做

支付发出后，有四种情况可以获得支付的结果：

1. 渠道接口实时返回渠道处理的结果。
2. 渠道异步通知支付平台。
3. 支付平台使用定时任务梯度时间查询渠道支付结果。
4. 拿到渠道对账文件。

时效性而言，依次递减，但也不是绝对的，有时候会出现渠道异步通知比接口实时返回还要快。这个时候一定要设计好状态机，否则很容易出现异步结果已经推进成功，实时接口又推进到支付中。具体可以看看公众号以前的发文：状态机设计与最佳实践。

定时查询查询一定要用梯度，一方面减少自己平台和渠道压力，同时又能获得最好的时效性，比如间隔时间：1秒，2秒，5秒，10秒，20秒，40秒，100秒 查到n次就不查了。再查下去也没有意义，就等渠道文件对账好了。如果渠道的对账文件是支付成功，但是平台支付已经关闭订单，那就走差错给用户退回去就好。

如何防重复支付

重复支付在很多公司都出现过，强大如支付宝，也时不时爆出大批量的重复支付。

首先是接口要有幂等设计。幂等的设计也有很多种方式，有人喜欢使用redis分布式锁，我个人是反对的，起码也要使用数据库唯一索引。单机房使用唯一索引就够，如果全球多活怎么办？还得有一个全局幂等组件。具体怎么设计，可以在公众号里找下：支付幂等设计与最佳实践。

但是，幂等设计是基于商户不换号的情况下，如果商户换号重发，就防不住，怎么办？最好是基于用户的维度做个判断，比如同一个用户，在短时间（比如1分钟），已经存在相同金额的支付单，就给用户提示：“当前已经有一笔xx金额的订单，是否仍然支付？”。虽然不能完全避免，但是可以减少。

万一重复支付了怎么做

前面有提出防重复支付，但是万一真出现重复支付了怎么办？

没有什么好办法，原路退回就是。

这也是我们为什么在前面把交易单和支付单区分出来的原因。各是各的单，出现问题好处理。

还有一个问题，如何发现内部有大批量的重复支付？总不能全部等客诉吧？后面有时间再聊聊支付平台内部多域之间实时两两对账。

支付成功后用户关单了怎么做

不仅是重复支付后需要原路退回，如果渠道扣款成功，但是我们的订单已经关闭（超期关闭，用户主动关闭等），都需要做原路退回。

这里还可以引申出另外一个问题，为什么记账的时候，有一个“商户待结算户”，还有一个“支付网关过渡户”。如果没有支付网关过渡户，支付成功，钱直接到了商户待结算户，但是如果收单域的订单已经关闭，这笔钱就不应该进入到商户待结算户里去，而是应该直接从支付网关过渡户给用户退回去。

返回码怎么映射

对于支付来说，不要轻易推进到成功，只有渠道非常明确地说，某个返回码代表成功，才能推进成功。否则很容易出现资损。

当然也不要轻易推进失败，也只有明确失败才能推进失败，否则用户支付成功被推进失败，容易引起客诉。

尤其要注意的是，有很多渠道有两级返回码，要区分如何组合使用。还有，查询接口一定要区分通信成功和业务成功，只能通过业务成功来推进状态。

更详细的说明，可以翻翻公众号的文章：返回码映射设计与最佳实践。

支付要不要做系统自动重发

网络经常超时，如果用户发起支付，超时了，再次重试，就会成功，那到底要不要系统自动重试呢？建议根据自己的业务场景和团队的技术实力选择。

业务场景，比如代扣，一定要系统自动重试，包括余额不足，超时等场景都需要重试。余额不足再换个支付方式或换张卡再试，超时多次查询都返回“订单不存在”，那也需要系统自动重试。

如果是普通的支付，那看团队是否能做到避免重复扣款，如果能，那就系统自动重试，提高成功率。给一个思路：特定的返回码 + 指定时间内查询都是返回“订单不存在”。

支付渠道如何做隔离

有人喜欢为每一个渠道都编写独立的代码，美其名曰：“隔离性好”，一个渠道有问题不影响另外一个。

我却觉得技术和架构能力需要提高。渠道接入四个层次：

1. 为每个渠道写独立的代码。
2. 抽象出模板方式，每个渠道只需要写特定的代码，比如报文组装、签名验签。流程由模板方法驱动。
3. 配置文件接入渠道。把渠道的处理分解成多个子能力，通过配置文件驱动。
4. 直接在后台页面配置映射就能接入。

只要领域抽象能力强，技术过硬，哪怕做到第四层，仍然可以做到很好的隔离。比如通过外部渠道分配的商户号，隔离出不同的配置，不同的渠道配置不同的参数，自动化测试回归，保存历史报文用于自动化MOCK测试等。质量仍然是上乘的，隔离性也完全没问题。

支付资损防控怎么做

直接翻公众号历史发文：支付资损防控指南（精华版），说得非常详细，涵盖资损防控的方方面面。

支付路由怎么做

直接翻公众号历史发文：简洁而强大的支付渠道路由设计，功能很强大，但实现又非常简单。

结束语

答案不是唯一的，上面只是给出了一些相对优的解，供参考。

如果对支付系统设计与实现感兴趣，可以看看公众号的其它文章，就四个字：[好评如潮](#)。如果翻了一圈后不满意，觉得浪费了你的时间，加我微信，给你发个大红包表示歉意和补偿。

欢迎在评论区给出你的见解或遇到的问题，我将送出一份神秘礼物给获得点赞最多的同学，时间截止2025.1.10 24点。

深耕境内/跨境支付架构设计十余年，欢迎关注并[星标](#)公众号“隐墨星辰”，及时获得最新文章更新推送，和我一起深入解码支付系统的方方面面。

专栏系列文章PDF合集不定时更新，欢迎关注我的公众号“隐墨星辰”，留言“PDF”获取。

隐墨星辰 公众号

10年顶尖境内/跨境支付公司架构经验



著有《图解支付系统设计与实现》
和我一起解码支付系统方方面面

有个支付讨论群，添加个人微信（yinmon_sc）备注666进入。

隐墨星辰 个人微信

10年顶尖境内/跨境支付公司架构经验



著有《图解支付系统设计与实现》
备注666进支付讨论群