# 第二章: 大模型使用

## 2.1 大模型部署

之前我们有讲过,智能应用就是在传统软件的基础上接入大模型,所以,我们要完成智能应用的开发,首先得把大模型这种软件部署起来,而大模型的部署会有两种方式,自己部署、他人部署。自己部署大模型自己直接用,他人部署的大模型我们掏钱用。接下来我们分别聊一聊这两种方式的优缺点。

#### ℯ 自己部署:

#### 云服务器部署:

优势: 前期成本低,维护简单

劣势:数据不安全,长期使用成本高

#### 本地机器部署:

优势:数据安全,长期使用成本低

劣势: 初期成本高,维护困难

#### 他人部署:

优势: 无需部署

劣势:数据不安全,长期使用成本高

首先看自己部署,我们自己在部署大模型的时候,也会有两种方式,一种是在云端部署,另外一种是 在本地机房部署。在云端部署的优点是前期部署成本低,维护简单,比如你去阿里云租服务器,按天 收费,我们可以花很少的费用,就能快速上手,并且像阿里云这样的平台,服务器维护成本也是很低 的。但缺点就是数据不安全,因为使用别人提供的服务器,数据都得从这个服务器过一圈,数据自然 就不安全了;还有就是长期使用成本高,虽然阿里云租服务器每天的收费看起来不算贵,但是你只要 用一天,就得付一天钱,时间长了,这个费用其实还是蛮高的。

我们自己部署的另外一种方式就是部署在本地机房中,这种方式相比较云端部署,它的优势是数据安全,毕竟自己的服务器嘛,数据并不会向外部暴露,还有就是长期成本低,因为是一次性投入,时间 越长,平均成本就越低。反过来,它的缺点是初期成本高,买服务器的钱是一次性支付的,还有就是维护困难一些,因为自己买的服务器,所有的维护工作都需要自己来做。

我们再来看他人部署,都有谁会帮我们部署大模型呢?这样的好事者有很多,常见的比如有阿里云百炼、百度智能云、硅基流动、火山引擎等等。它们部署好的大模型,我们怎么用呢?常规思路,使用

他们提供的API接口使用,当然了,你使用的时候,它会按照流量进行收费的,毕竟天下没有免费的午餐。使用这些平台的大模型,优点是我们自己无需部署,缺点是数据不安全、长期使用成本高。

### 2.1.1 ollama本机部署大模型并使用

本地机器部署,在工作中,一般都是公司机房的机器,而咱们这里没有公司,就部署到咱们 当前的电脑上即可。

我们要在自己的电脑上部署大模型,通常情况下,需要在电脑上先安装Python解释器、以及大模型软件需要的一些依赖库,并且需要手动下载要安装的模型,编写运行脚本。这一系列工作做完后,大模型才能在本机上真正的部署起来,这一系列的工作,其实还是有一些麻烦的。有一些好心人,为了让我们更快上手,专门提供了一些工具、常见的比如Ollama、LM Studio等,这些工具都有一键下载并运行大模型的功能。有了这些工具,咱们部署大模型就不需要这么麻烦了,只需要在电脑上安装这些工具,执行一行命令就行了。





#### 2.1.1.1 安装ollama

Ollama的官网是:

http://ollama.com

Ollama

Get up and running with large language models.

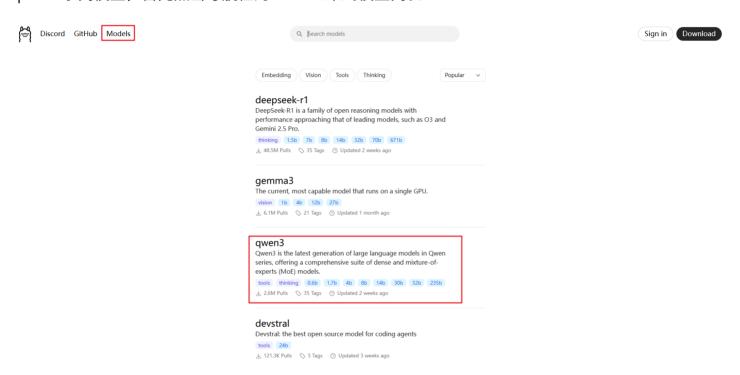
大家打开后,首页就有一个下载按钮,你只要点击一下download,选择对应的操作系统,就可以下载 对应版本的ollama了。当然了,咱们本次课程提供的资料中,已经提供了ollama的安装包,并且也提 供了安装文档,大家记得获取资料,照着操作即可。



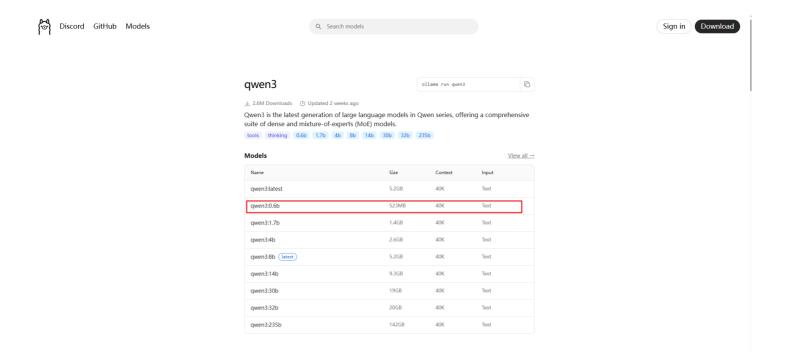
ollama安装完毕后,会自动的配置系统环境变量,因此接下来我们就可以直接执行ollama的命令去部署大模型了,如果有同学将来执行命令的时候报错,请记得检查一下你的环境变量,可以手动的配置一下

#### 2.1.1.2 部署大模型

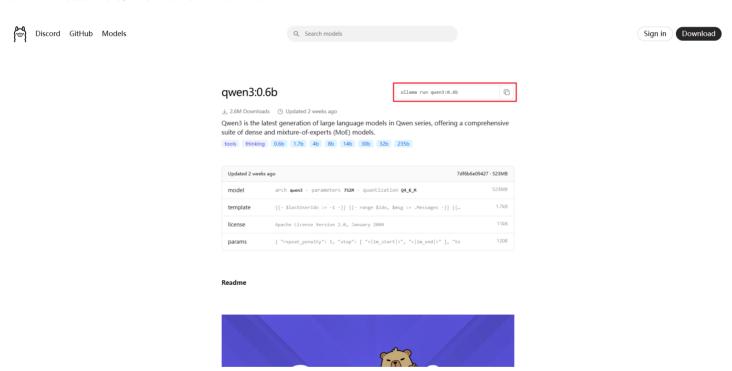
ollama官网上给出了很多大模型,大家可以根据自己的需求选择对应的大模型安装,这里咱们安装 gwen3系列模型,首先点击导航栏的**Models**来到模型列表



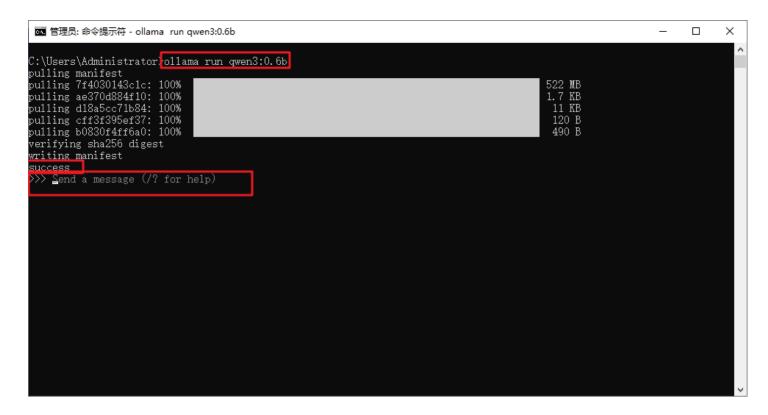
然后点击模型列表中的qwen3,来到qwen3详情页面



这里提供了不同参数规模的qwen3模型,由于参数规模越大,对电脑的配置要求越高,为了照顾到大部分同学的电脑,这里我们部署最小参数规模的大模型qwen3:0.6b来部署,点击模型的名称,来到该模型的详情页面,并赋值右上角的命令。



打开命令行提示符窗口,执行这个命令,命令执行的过程中,会自动下载qwen3:0.6b这个模型到电脑本地,并自动的运行起来,命令行提示符窗口如果自动进入到聊天界面,证明模型部署正确。



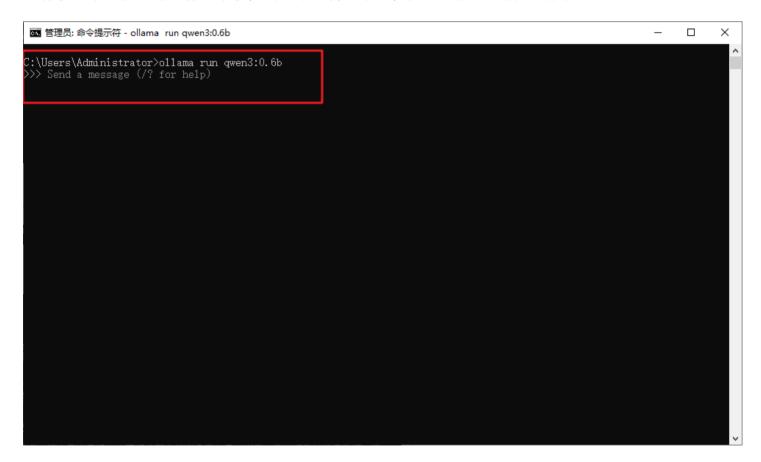
接下来你就可以跟本地部署的大模型进行对话了,输入问题敲回车即可



如果不想继续与大模型对话,可以使用 /bye 命令退出聊天界面



如果想继续与大模型聊天,可以再次执行 ollama run qwen3:0.6b, 这一次再执行的时候,由于本地已经有了这个大模型并运行起来了,所以不会再次下载,而是直接进入聊天界面。

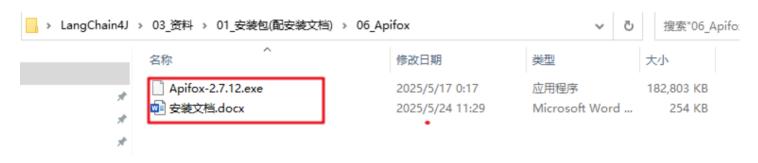


有关ollama提供的命令有很多,如果大家有兴趣,可以参考资料中提供的文档自行学习。



### 2.1.1.3 发送http的方式调用大模型

ollama平台也开放了API,程序员可以使用发送http请求的方式调用本地部署的大模型,这里咱们借助于Apifox工具调用大模型,有关Apifox软件,大家可以参考资料中提供的安装包和文档自行操作!



本机ollama默认占用的端口为11434,调用大模型时发送的请求方式必须是post,请求数据必须是json格式,具体样例如下:



有关调用时详细的请求参数,后面我们详细介绍!

#### 2.1.2 云平台大模型使用

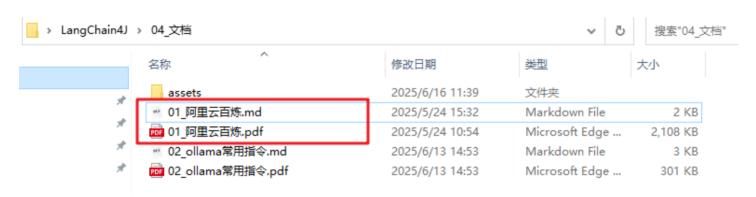
之前我们介绍过,部署大模型的平台常见的有阿里云百炼,百度智能云,硅基流动,火山引擎等等,在咱们本次课程中使用阿里云百炼平台提供的大模型给大家做演示,其它的平台,大家有兴趣可以课后自己试一试,因为这不同的平台,使用方式都大差不差!

#### 2.1.2.1 阿里云百炼平台使用

如果要使用阿里云百炼,需要有如下四个步骤的操作:

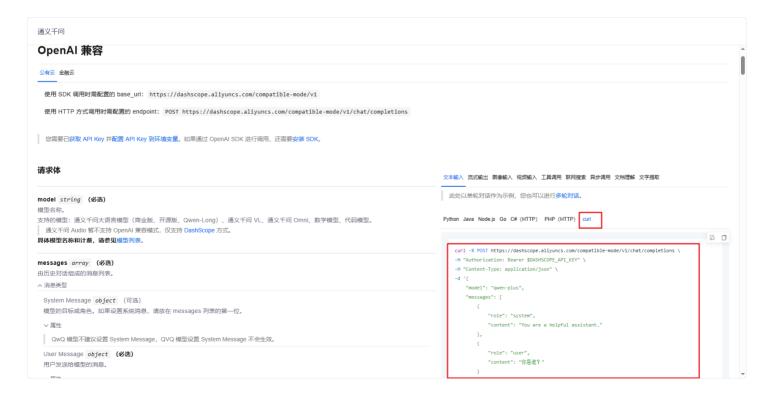
- A. 登录阿里云 https://aliyun.com
- B. 开通 **大模型服务平台百炼** 服务
- C. 申请百炼平台 API-KEY
- D. 选择大模型使用

有关上述操作,在咱们配套的资料中提供了对应的文档,大家可以参考操作!



## 2.1.2.2 发送http的方式调用大模型

百炼平台对于大模型API的使用,给出了详细的参考文档,其中就包括http方式的调用,大家可以点击目标模型下方的API参考,查看详细的文档。



这里需要注意的是,由于百炼平台是一个收费的平台,所以发送http请求的时候,需要以请求投的方式将api-key,接下来我们介绍一下如何在apifox中配置api-key。

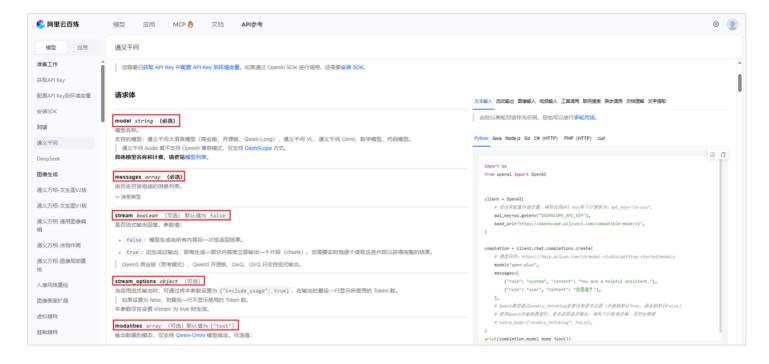


api-key配置好了以后,我们调用百炼平台提供的大模型,也需要指定url,请求方式以及请求参数,这里可以参照百炼平台提供的文档,最终效果如下:



# 2.2 大模型调用

有关大模型调用过程中,请求数据和响应数据都给出了详细的说明,大家可以参照百炼平台的api文档查看,同时不同平台的请求参数,基本都类似,接下来我们挑选几个核心的数据给大家做说明。



### 2.2.1 请求数据

使用大模型需要传递的参数,在访问大模型时都需要在请求体中以json的形式进行传递,下面是给出的一个样例:

```
代码块
    {
 1
         "model": "qwen-plus",
 2
 3
         "messages": [
 4
             {
                "role": "system",
 5
                 "content": "你是东哥的助手小月月"
 6
 7
            },
 8
             {
 9
                "role": "user",
                "content": "你是谁?"
10
            },
11
12
                "role": "assistant",
13
                "content": "您好,有什么可以帮助您?"
14
            }
15
        ],
16
        "stream": true,
17
18
         "enable_search": true
19
    }
```

下面是每一个参数的含义:



messages: 发送给模型的数据,模型会根据这些数据给出合适的响应

• content: 消息内容

• role: 消息角色(类型)

• user: 用户消息

• system: 系统消息

。 assistant: 模型响应消息

stream: 调用方式

• true: 流式调用

false: 流式调用(默认)

enable search: 联网搜索,启用后,模型会将搜索结果作为参考信息

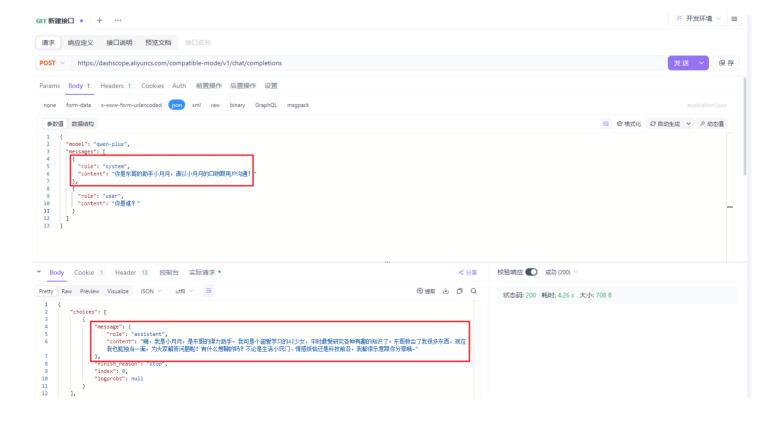
true: 开启

false: 不开启(默认)

每一个参数的作用不一样,接下来对每一个参数做详细说明。

首先是model,由于百炼平台提供了各种各样的模型,所以你需要通过model这个参数来指定接下来 要调用的是哪个模型。

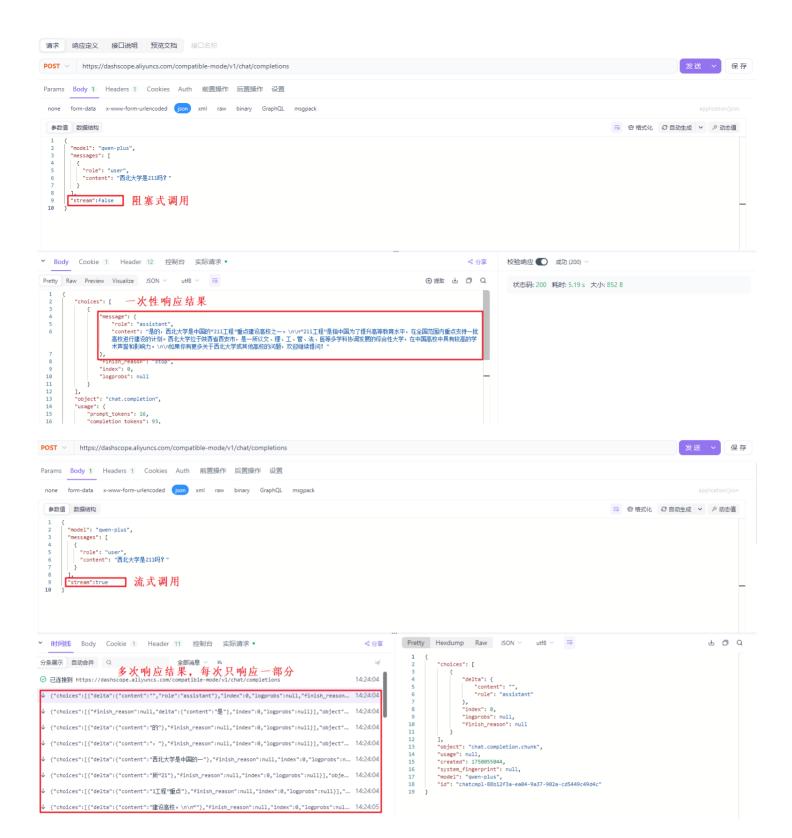
其次是messages,用户发送给大模型的消息有三种,使用role来进行分别,其中user代表的是用户问题,这个在咱们之前的演示中一直在用,不再过多介绍。system代表的系统消息,它是用于给大模型设定一个角色,然后大模型就可以用该角色的口吻跟用户对话了,下面是一个演示案例:



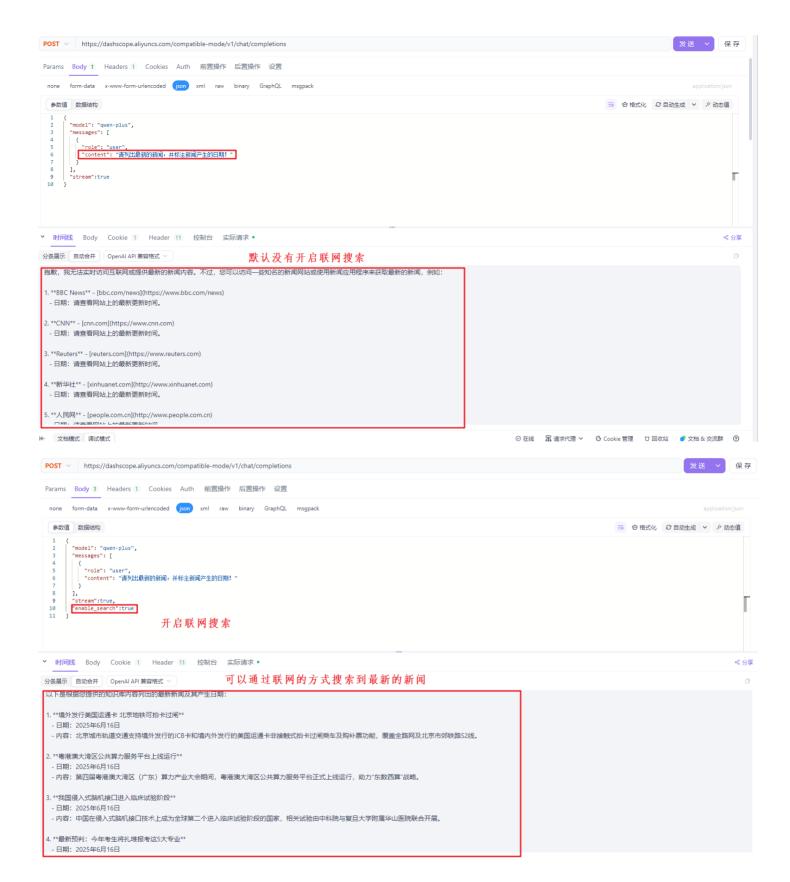
最后assistant代表的是大模型给用户响应的消息,这里很奇怪,为什么大模型响应给用户的消息,再次请求大模型时需要携带给大模型呢?这是因为大模型没有记忆能力,也就是说用户跟大模型交互的过程中,每一次问答都是独立的,互不干扰的。但是实际上我们人与人之间的聊天不是这样的,比如我问你**西北大学是211吗?**你回答我是!我再问你是985吗?你会回答不是!虽然我第二次问你的时候我并没有问具体哪个大学是985,但是你可以从咱们之前的聊天信息中推断出我要问的是西北大学,因为你已经记住了之前的聊天信息。但是大模型目前做不到,如果要让大模型在与用户沟通的过程中达到人与人沟通的效果,我们唯一的解决方案就是每次与大模型交互的过程中,把之前用户的问题和大模型的响应以及现在的问题,都发送给大模型,这样大模型就可以根据以前的聊天信息从而做出推断了,下面是一个演示的案例:



sream代表调用大模型的方式,如果取值为true,代表流式调用,此时大模型会生成一点儿数据,就给客户端响应一点儿数据,最终通过多次响应的方式把所有的结果响应完毕。如果取值为false,代表阻塞式调用,此时大模型会等待将所有的内容生成完毕,然后再一次性的响应给客户端。默认情况下stream的取值为false,下面是两种不同调用方案的演示案例:



enable\_search代表是否开启联网搜索,由于大模型训练完毕后,它的知识库不再更新了,比如大模型时2023年10月训练完毕的,那么2023年10月以后新产生的数据,大模型就无法感知了,如果要让大模型可以根据最新的数据回答问题,其中有一种解决方案就是开启联网搜索,大模型可以根据联网搜索的结果生成最终的答案。默认情况下enable\_seach为false,也就是不开启,如果要开启联网搜索,需要手动设置请求参数enable\_search为true。下面是一个演示案例:



### 2.2.2 响应数据

在与大模型交互的过程中,大模型响应的数据是json格式的数据,下面是一份响应数据的示例:

```
代码块
1 {
2 "choices": [
3 {
```

```
4
                  "message": {
                      "role": "assistant",
 5
                     "content": "我是通义千问,阿里巴巴..."
 6
 7
                 "finish_reason": "stop",
 8
                 "index": 0
 9
             }
10
11
         ],
12
         "object": "chat.completion",
13
         "usage": {
             "prompt_tokens": 22,
14
             "completion_tokens": 80,
15
             "total_tokens": 102,
16
17
         },
         "created": 1748068508,
18
19
         "system_fingerprint": null,
         "model": "gwen-plus",
20
         "id": "chatcmpl-99f8d040-0f49-955b-943a-21c83"
21
22
    }
```

#### 下面是每一个参数的含义:

choices:模型生成的内容数组,可以包含一条或多条内容

- message: 本次调用模型输出的消息

- finish\_reason: 自然结束(stop),生成内容过长(length)

- index: 当前内容在choices数组中的索引

object: 始终为chat.completion, 无需关注

usage: 本次对话过程中使用的token信息

- prompt\_tokens: 用户的输入转换成token的个数

- completion\_tokens: 模型生成的回复转换成token的个数

- total tokens: 用户输入和模型生成的总token个数

created: 本次会话被创建时的时间戳

system fingerprint: 固定为null,无需关注

model: 本次会话使用的模型名称

id: 本次调用的唯一标识符

有关响应数据,大家基本上作为了解的知识,种地那关注choices和usage,其中choices里面封装的是大模型响应给客户端的核心数据,也就是用户问题的答案。而usage代表本次对话过程中使用的token信息,这里对token给大家做一个解释:在大语言模型中,**token**是大模型处理文本的基本单位,可以理解为模型**"看得懂"**的最小文本片段,用户输入的内容都需要转换成token,才能让大模型更好的处

理。将来文本要转化成token,需要使用到一个叫分词器的东西,不同的分词器,相同的文本转化成token的个数不完全一致,但是目前大部分分词器在处理英文的时候,一个token大概等于4个字符,而处理中文的时候,一个汉字字符大概等于1~2个token。顺便给大家说一下,其实我们通过API调用百炼平台提供的大模型,我们之前讲过,是按照流量收费的,其实更准确的说法应该是按照token数量进行收费。

