

## 17 | WebAPI: XMLHttpRequest是怎么实现的?

2019-09-12 李兵

《浏览器工作原理与实践》

课程介绍 >



讲述：李兵

时长 14:10 大小 12.98M



在 [上一篇文章](#) 中我们介绍了 `setTimeout` 是如何结合渲染进程的循环系统工作的，那本篇文章我们就继续介绍另外一种类型的 WebAPI——XMLHttpRequest。

自从网页中引入了 JavaScript，我们就可以操作 DOM 树中任意一个节点，例如隐藏 / 显示节点、改变颜色、获得或改变文本内容、为元素添加事件响应函数等等，几乎可以“为所欲为”了。

不过在 XMLHttpRequest 出现之前，如果服务器数据有更新，依然需要重新刷新整个页面。而 XMLHttpRequest 提供了从 Web 服务器获取数据的能力，如果你想要更新某条数据，只需要通过 XMLHttpRequest 请求服务器提供的接口，就可以获取到服务器的数据，然后再操作 DOM 来更新页面内容，整个过程只需要更新网页的一部分就可以了，而不用像之前那样还得刷新整个页面，这样既有效率又不会打扰到用户。



关于 XMLHttpRequest，本来我是想一带而过的，后来发现这个 WebAPI 用于教学非常好。首先前面讲了那么网络内容，现在可以通过它把 HTTP 协议实践一遍；其次，XMLHttpRequest 是一个非常典型的 WebAPI，通过它来讲解浏览器是如何实现 WebAPI 的很合适，这对于你理解其他 WebAPI 也有非常大的帮助，同时在这个过程中我们还可以把一些安全问题给串起来。

但在深入讲解 XMLHttpRequest 之前，我们得先介绍下**同步回调**和**异步回调**这两个概念，这会帮助你更加深刻地理解 WebAPI 是怎么工作的。

## 回调函数 VS 系统调用栈

那什么是回调函数呢（Callback Function）？

将一个函数作为参数传递给另外一个函数，那作为参数的这个函数就是**回调函数**。简化的代码如下所示：

```
1 let callback = function(){
2     console.log('i am do homework')
3 }
4 function doWork(cb) {
5     console.log('start do work')
6     cb()
7     console.log('end do work')
8 }
9 doWork(callback)
```

 复制代码

在上面示例代码中，我们将一个匿名函数赋值给变量 callback，同时将 callback 作为参数传递给了 doWork() 函数，这时在函数 doWork() 中 callback 就是回调函数。

上面的回调方法有个特点，就是回调函数 callback 是在主函数 doWork 返回之前执行的，我们把这个回调过程称为**同步回调**。

既然有同步回调，那肯定也有异步回调。下面我们再看看异步回调的例子：



```
1 let callback = function(){
2     console.log('i am do homework')
```

 复制代码

```

3 }
4 function doWork(cb) {
5     console.log('start do work')
6     setTimeout(cb,1000)
7     console.log('end do work')
8 }
9 doWork(callback)

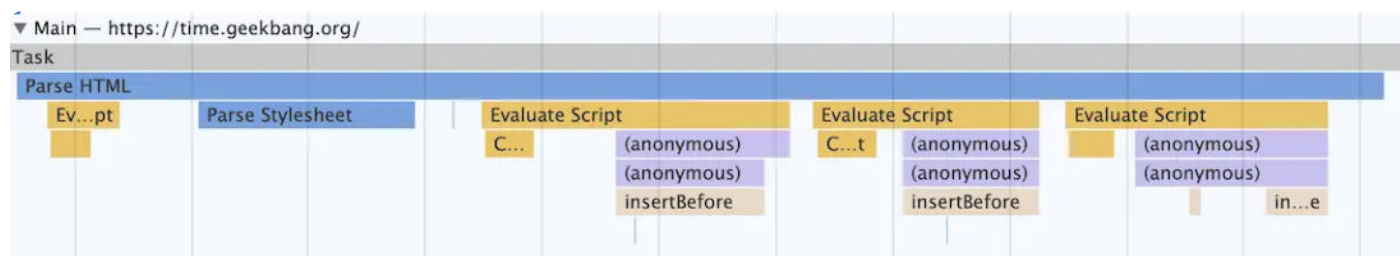
```

在这个例子中，我们使用了 `setTimeout` 函数让 `callback` 在 `doWork` 函数执行结束后，又延时了 1 秒再执行，这次 `callback` 并没有在主函数 `doWork` 内部被调用，我们把这种回调函数在主函数外部执行的过程称为**异步回调**。

现在你应该知道什么是同步回调和异步回调了，那下面我们再深入点，站在消息循环的视角来看看同步回调和异步回调的区别。理解了这些，可以让你从本质上理解什么是回调。

我们还是先来回顾下页面的事件循环系统，通过 [《15 | 消息队列和事件循环：页面是怎么“活”起来的？》](#) 的学习，你应该已经知道浏览器页面是通过事件循环机制来驱动的，每个渲染进程都有一个消息队列，页面主线程按照顺序来执行消息队列中的事件，如执行 JavaScript 事件、解析 DOM 事件、计算布局事件、用户输入事件等等，如果页面有新的事件产生，那新的事件将会追加到事件队列的尾部。所以可以说是**消息队列和主线程循环机制保证了页面有条不紊地运行**。

这里还需要补充一点，那就是当循环系统在执行一个任务的时候，都要为这个任务维护一个**系统调用栈**。这个**系统调用栈**类似于 JavaScript 的调用栈，只不过系统调用栈是 Chromium 的开发语言 C++ 来维护的，其完整的调用栈信息你可以通过 `chrome://tracing/` 来抓取。当然，你也可以通过 Performance 来抓取它核心的调用信息，如下图所示：



消息循环系统调用栈记录

这幅图记录了一个 `Parse HTML` 的任务执行过程，其中黄色的条目表示执行 JavaScript 的过程，其他颜色的条目表示浏览器内部系统的执行过程。

通过该图你可以看出来，Parse HTML 任务在执行过程中会遇到一系列的子过程，比如在解析页面的过程中遇到了 JavaScript 脚本，那么就暂停解析过程去执行该脚本，等执行完成之后，再恢复解析过程。然后又遇到了样式表，这时候又开始解析样式表.....直到整个任务执行完成。

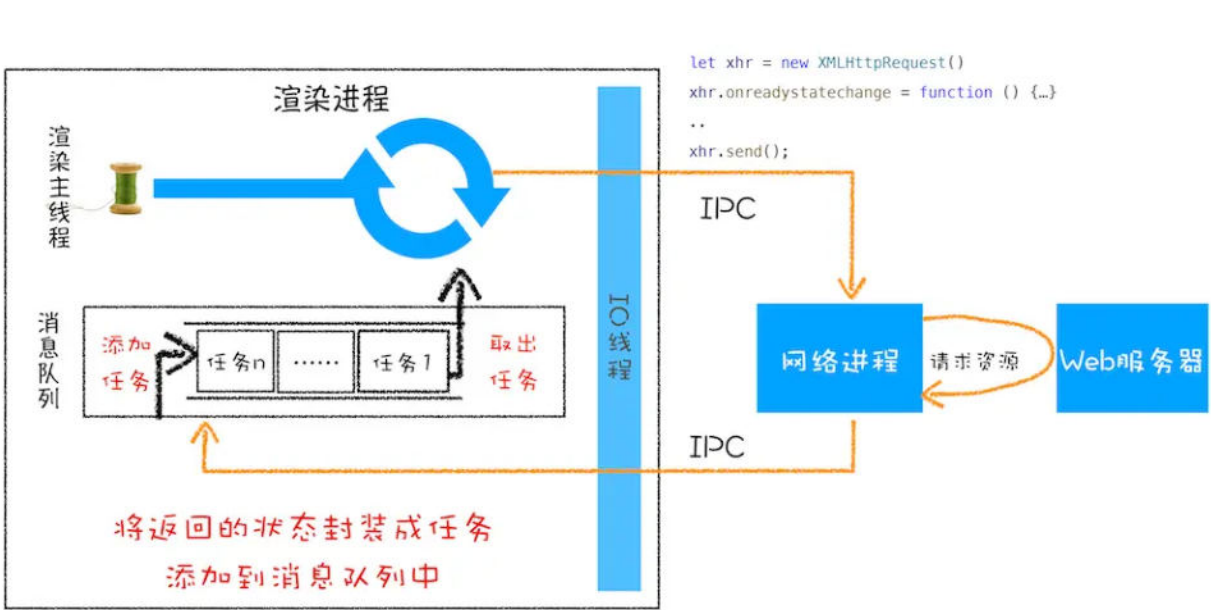
需要说明的是，整个 Parse HTML 是一个完整的任务，在执行过程中的脚本解析、样式表解析都是该任务的子过程，其下拉的长条就是执行过程中调用栈的信息。

每个任务在执行过程中都有自己的调用栈，那么同步回调就是在当前主函数的上下文中执行回调函数，这个没有太多可讲的。下面我们主要来看看异步回调过程，异步回调是指回调函数在主函数之外执行，一般有两种方式：

- 第一种是把异步函数做成一个任务，添加到信息队列尾部；
- 第二种是把异步函数添加到微任务队列中，这样就可以在当前任务的末尾处执行微任务了。

## XMLHttpRequest 运作机制


理解了什么是同步回调和异步回调，接下来我们就来分析 XMLHttpRequest 背后的实现机制，具体工作过程你可以参考下图：



XMLHttpRequest 工作流程图

这是 XMLHttpRequest 的总执行流程图，下面我们就来分析从发起请求到接收数据的完整流程。

我们先从 XMLHttpRequest 的用法开始，首先看下面这样一段请求代码：

 复制代码

```
1  function GetWebData(URL){
2      /**
3       * 1:新建XMLHttpRequest请求对象
4       */
5      let xhr = new XMLHttpRequest()
6
7      /**
8       * 2:注册相关事件回调处理函数
9       */
10     xhr.onreadystatechange = function () {
11         switch(xhr.readyState){
12             case 0: //请求未初始化
13                 console.log("请求未初始化")
14                 break;
15             case 1://OPENED
16                 console.log("OPENED")
17                 break;
18             case 2://HEADERS_RECEIVED
19                 console.log("HEADERS_RECEIVED")
20                 break;
21             case 3://LOADING
22                 console.log("LOADING")
23                 break;
24             case 4://DONE
25                 if(this.status == 200||this.status == 304){
26                     console.log(this.responseText);
27                 }
28                 console.log("DONE")
29                 break;
30         }
31     }
32
33     xhr.ontimeout = function(e) { console.log('ontimeout') }
34     xhr.onerror = function(e) { console.log('onerror') }
35
36     /**
37      * 3:打开请求
38      */
39     xhr.open('Get', URL, true); //创建一个Get请求,采用异步
40
41
42     /**
43      * 4:配置参数
```



```
44     */
45     xhr.timeout = 3000 //设置xhr请求的超时时间
46     xhr.responseType = "text" //设置响应返回的数据格式
47     xhr.setRequestHeader("X_TEST","time.geekbang")
48
49     /**
50     * 5:发送请求
51     */
52     xhr.send();
53 }
```

上面是一段利用了 XMLHttpRequest 来请求数据的代码，再结合上面的流程图，我们可以分析下这段代码是怎么执行的。

### 第一步：创建 XMLHttpRequest 对象。

当执行到 `let xhr = new XMLHttpRequest()` 后，JavaScript 会创建一个 XMLHttpRequest 对象 `xhr`，用来执行实际的网络请求操作。

### 第二步：为 xhr 对象注册回调函数。

因为网络请求比较耗时，所以要注册回调函数，这样后台任务执行完成之后就会通过调用回调函数来告诉其执行结果。

XMLHttpRequest 的回调函数主要有下面几种：

- `ontimeout`，用来监控超时请求，如果后台请求超时了，该函数会被调用；
- `onerror`，用来监控出错信息，如果后台请求出错了，该函数会被调用；
- `onreadystatechange`，用来监控后台请求过程中的状态，比如可以监控到 HTTP 头加载完成的消息、HTTP 响应体消息以及数据加载完成的消息等。

### 第三步：配置基础的请求信息。

注册好回调事件之后，接下来就需要配置基础的请求信息了，首先要通过 `open` 接口配置一些基础的请求信息，包括请求的地址、请求方法（是 `get` 还是 `post`）和请求方式（同步还是异步请求）。





然后通过 `xhr` 内部属性类配置一些其他可选的请求信息，你可以参考文中示例代码，我们通过 `xhr.timeout = 3000`来配置超时时间，也就是说如果请求超过 3000 毫秒还没有响应，那么这次请求就被判断为失败了。

我们还可以通过`xhr.responseType = "text"`来配置服务器返回的格式，将服务器返回的数据自动转换为自己想要的格式，如果将 `responseType` 的值设置为 `json`，那么系统会自动将服务器返回的数据转换为 JavaScript 对象格式。下面的图表是我列出的一些返回类型的描述：

类型	描述
" "	将 <code>responseType</code> 设为空字符串，与设置为 <code>"text"</code> 相同， 是默认类型（UTF-16字符串）。
"text"	返回的是UTF-16字符串文本。
"json"	<code>response</code> 是一个 JavaScript 对象。
"document"	<code>response</code> 是一个 DOM对象。
"blob"	<code>response</code> 是一个包含二进制数据的 Blob 对象 。
"arraybuffer"	<code>response</code> 是一个包含二进制数据的 JavaScript ArrayBuffer 。

假如你还需要添加自己专用的请求头属性，可以通过 `xhr.setRequestHeader` 来添加。

第四步：发起请求。

一切准备就绪之后，就可以调用`xhr.send`来发起网络请求了。你可以对照上面那张请求流程图，可以看到：渲染进程会将请求发送给网络进程，然后网络进程负责资源的下载，等网络进程接收到数据之后，就会利用 IPC 来通知渲染进程；渲染进程接收到消息之后，会将 `xhr` 的回调函数封装成任务并添加到消息队列中，等主线程循环系统执行到该任务的时候，就会根据相关的状态来调用对应的回调函数。

- 如果网络请求出错了，就会执行 `xhr.onerror`；
- 如果超时了，就会执行 `xhr.ontimeout`；



- 如果是正常的数据接收，就会执行 `onreadystatechange` 来反馈相应的状态。

这就是一个完整的 `XMLHttpRequest` 请求流程，如果你感兴趣，可以参考下 Chromium 对 `XMLHttpRequest` 的实现，[🔗 点击这里查看代码](#)。

## XMLHttpRequest 使用过程中的“坑”

上述过程看似简单，但由于浏览器很多安全策略的限制，所以会导致你在使用过程中踩到非常多的“坑”。

浏览器安全问题是前端工程师避不开的一道坎，通常在使用过程中遇到的“坑”，很大一部分都是由安全策略引起的，不管你喜不喜欢，它都在这里。本来很完美的一个方案，正是由于加了安全限制，导致使用起来非常麻烦。

而你要做的就是去正视这各种的安全问题。也就是说要想更加完美地使用 `XMLHttpRequest`，你就要了解浏览器的安全策略。

下面我们就来看看在使用 `XMLHttpRequest` 的过程中所遇到的跨域问题和混合内容问题。

### 1. 跨域问题

比如在极客邦的官网使用 `XMLHttpRequest` 请求极客时间的页面内容，由于极客邦的官网是 [www.geekbang.org](http://www.geekbang.org)，极客时间的官网是 [time.geekbang.org](http://time.geekbang.org)，它们不是同一个源，所以就涉及到了跨域（在 A 站点中去访问不同源的 B 站点的内容）。默认情况下，跨域请求是不被允许的，你可以看下面的示例代码：

 复制代码

```
1 var xhr = new XMLHttpRequest()
2 var url = 'https://time.geekbang.org/'
3 function handler() {
4     switch(xhr.readyState){
5         case 0: //请求未初始化
6             console.log("请求未初始化")
7             break;
8         case 1://OPENED
9             console.log("OPENED")
10            break;
11         case 2://HEADERS_RECEIVED
12            console.log("HEADERS_RECEIVED")
13            break;
```





```

14     case 3://LOADING
15         console.log("LOADING")
16         break;
17     case 4://DONE
18         if(this.status == 200||this.status == 304){
19             console.log(this.responseText);
20         }
21         console.log("DONE")
22         break;
23     }
24 }
25
26 function callOtherDomain() {
27     if(xhr) {
28         xhr.open('GET', url, true)
29         xhr.onreadystatechange = handler
30         xhr.send();
31     }
32 }
33 callOtherDomain()

```

你可以在控制台测试下。首先通过浏览器打开 [www.geekbang.org](http://www.geekbang.org)，然后打开控制台，在控制台输入以上示例代码，再执行，会看到请求被 Block 了。控制台的提示信息如下：

 复制代码

```
1 Access to XMLHttpRequest at 'https://time.geekbang.org/' from origin 'https://www
```

因为 [www.geekbang.org](http://www.geekbang.org) 和 [time.geekbang.com](http://time.geekbang.com) 不属于一个域，所以以上访问就属于跨域访问了，这次访问失败就是由于跨域问题导致的。

## 2. HTTPS 混合内容的问题

了解完跨域问题后，我们再来看看 HTTPS 的混合内容。HTTPS 混合内容是 HTTPS 页面中包含了不符合 HTTPS 安全要求的内容，比如包含了 HTTP 资源，通过 HTTP 加载的图像、视频、样式表、脚本等，都属于混合内容。

通常，如果 HTTPS 请求页面中使用混合内容，浏览器会针对 HTTPS 混合内容显示警告，用来向用户表明此 HTTPS 页面包含不安全的资源。比如打开站点

<https://www.iteye.com/groups>，可以通过控制台看到混合内容的警告，参考下图：





## HTTPS 混合内容警告

从上图可以看出，通过 HTML 文件加载的混合资源，虽然给出警告，但大部分类型还是能加载的。而使用 XMLHttpRequest 请求时，浏览器认为这种请求可能是攻击者发起的，会阻止此类危险的请求。比如我通过浏览器打开地址 <https://www.iteye.com/groups>，然后通过控制台，使用 XMLHttpRequest 来请求 <http://img-ads.csdn.net/2018/201811150919211586.jpg>，这时候请求就会报错，出错信息如下图所示：



## 使用 XMLHttpRequest 混合资源失效

## 总结

好了，今天我们就讲到这里，下面我来总结下今天的内容。



首先我们介绍了回调函数和系统调用栈；接下来我们站在循环系统的视角，分析了 XMLHttpRequest 是怎么工作的；最后又说明了由于一些安全因素的限制，在使用 XMLHttpRequest 的过程中会遇到跨域问题和混合内容的问题。

本篇文章跨度比较大，不是单纯地讲一个问题，而是将回调类型、循环系统、网络请求和安全问题“串联”起来了。

对比 [🔗 上一篇文章](#)，setTimeout 是直接将延迟任务添加到延迟队列中，而 XMLHttpRequest 发起请求，是由浏览器的其他进程或者线程去执行，然后再将执行结果利用 IPC 的方式通知渲染进程，之后渲染进程再将对应的消息添加到消息队列中。如果你搞懂了 setTimeout 和 XMLHttpRequest 的工作机制后，再来理解其他 WebAPI 就会轻松很多了，因为大部分 WebAPI 的工作逻辑都是类似的。

## 思考时间


网络安全很重要，但是又很容易被忽视，因为项目需求很少涉及到基础的 Web 安全。如果忽视了这些基础安全策略，在开发过程中会处处遇到安全策略挖下的“大坑”，所以对于一名开发者来说，Web 安全理论很重要，也必须要学好。

那么今天我留给你一道开放性的思考题：你认为作为一名开发工程师，要如何去高效地学习前端的 Web 安全理论呢？

欢迎在留言区与我分享你的想法，也欢迎你在留言区记录你的思考过程。感谢阅读，如果你觉得这篇文章对你有帮助的话，也欢迎把它分享给更多的朋友。

分享给需要的人，Ta 订阅超级会员，你将得 50 元

Ta 单独购买本课程，你将得 20 元

 生成海报并分享

 赞 18

 提建议



## 学习推荐

# JVM + NIO + Spring

各大厂面试题及知识点详解

限时免费



## 精选留言 (47)

写留言



蓝配鸡

2019-09-12

如何高效学习安全理论

1. why, 知道为什么有这个安全机制, 历史是什么样的
2. how, 知道why之后自己先想想怎么解决这个问题, 再去看看别人是怎么解决的, 分析利弊
3. 学完之后自己上手试试
4. 拉个你身边最蠢的小伙伴把这件事给他说明白

作者回复: 很赞, 学安全一定要知道why, 知道why才知道how!

等到了我们专栏的安全篇时, 这套理论再结合实践就完美了。



**Geek\_d972f2**

2019-09-13

建立tcp连接是在xhr open还是send?

作者回复: open方法仅仅是配置数据, 没有任何真实的连接产生, 所有连接阶段都是在send之后

共 2 条评论 &gt;

👍 37

**yihang**

2019-09-12

请教老师, 我看到 es6中可以通过一个 fetch api来请求, 它的实现是用了 XMLHttpRequest 么? 如果不是, 原理上有什么不同?

作者回复: fetch采用了promise来封装, 在使用方式上更强现代化, 同时还原生支持async/await。在 chromium中, fetch是完全重新实现的, 和xmlhttprequest没有什么关系!

在项目中推荐使用fetch

共 3 条评论 &gt;

👍 24

**レイン小雨**

2019-09-14

老师后面能详细的讲一下浏览器同源策略的具体实现吗? 作为前端最基本的常识性知识却总是感觉理解的不够深入, 开始我以为是跨域的请求是被浏览器“拦截在了门内”----即请求没有发送出去, 但是看了很多文章中说, 其实跨域的请求是发送出去了, 服务器也接收到了并响应了, 而是在返回的时候被浏览器“拦截在门外”, 还有人说, 不同的浏览器实现也不一样, 很是困惑这里, 希望老师能给一个确定的答案。

共 12 条评论 &gt;

👍 18

**imperial**

2019-10-24

老师, 异步函数的调用不应该有三种方式吗, 可以放到队列尾, 微任务中, 也可以放入延迟队列中, 为什么不放入延迟队列中呢

作者回复: 延时队列中的任务包含JS通过定时器设置的回调函数、还有一些浏览器内部的延时回调函数。它们属于宏任务!

另外正常的消息队列中的任务也属于宏任务!



所以通常我说放入消息队列就是指放入了宏任务队列（包括了延时队列或者正常的消息队列）

因为分开来描述会有点啰嗦！



14



淡

2019-09-17

老师你好，我有以下几个疑问：

- 1.渲染进程里的主线程while循环空转，为啥不会造成系统卡死？我们自己code里空while死循环会造成卡死
- 2.就是网络进程IPC给渲染进程时，渲染进程收到消息。这里的”消息“具体包含哪些内容啊？谢谢。

共 5 条评论 >

8



Hurry

2019-09-14

IPC是什么

作者回复: 进程间通信，比如浏览器进程需要网络进程下载数据，浏览器进程就是通过IPC告诉网络进程需要下载哪些数据，网络进程接收到之后才会开启下载流程

共 2 条评论 >

8



bobi

2019-09-12

老师，什么时候专门讲微任务？

作者回复: 后面三节

微任务

Promise

async/await



5



oc7

2019-09-12

异步回调的第二种方式 把异步函数添加到微任务队列中 具体是哪些WebAPI呢？Promise.then？



作者回复: Promise的resolve和reject会创建微任务。

还有MutationObserver，如果监听了某个节点，那么通过DOMAPI修改这些被监听的节点也会产生微任务。



mfist

2019-09-12

作为一名前端开发工程师，要如何高效地学习前端web安全理论呢？

作为web工程师可以稍微把自己领域知识向后端扩展一些，这样理解web问题、网络传输问题会更加得心应手。

比如说前端浏览器因为跨域block，后端到底有没有处理请求；XSS 漏洞 以及 CSRF

漏洞如果能前后端一起模拟一下，会更容易理解的。

今日总结

xmlhttprequest是为了解决网页局部数据刷新产生的技术。通过同步回调和异步回调以及系统调用栈来引出了

xmlhttprequest运行机制。一个xhr主要包含下面四个步骤：1. 创建xmlhttprequest对象；2. 为xhr对象

注册回调函数（ontimeout、onerror、onreadystatechange）；3. 打开请求（xhr.open（'GET', url,true））4. 配置基础的请求信息（timeout/responseType/setRequestHeader）；5. 发送请求。xhr中场景的坑（

跨域和混合内容）

作者回复: 通过这些实践理解安全问题是好方法，最好还要搞清楚为什么有这种或者那种的安全问题，这样我们对安全问题就会融会贯通。



l1shu

2019-10-22

为什么有些文章说渲染进程中有一个定时器线程用来计时的 到时间后会 把回调函数塞到消息队列 而没有提到延迟队列这个说法 求老师解答

共 3 条评论 >



朱维娜 🍷

2019-09-12

想知道 延时任务是不是一种微任务啊

作者回复: 不是, 宏任务, 定时器产生的任务都会保存到延时队列中



3



蹦哒

2020-07-16

老师请问是否可以这样理解:

异步的本质, 就是通过把方法 (函数) 添加到消息队列尾部, 通过循环系统在下次循环中去执行;

同步的本质, 就是在当前方法中执行另外一个方法, 执行完之后接着执行原来的方法



2



AICC

2019-09-23

老师什么时候出一个web安全的专栏啊, 好想系统性的学学

共 1 条评论 >

2



zhangbao

2020-05-26

老师好! 关于 XMLHttpRequest 的工作机制, 有一个疑问, 想不太明白: xhr 的 onreadystatechange 回调, 在整个请求过程中, 会触发好几次, 那么封装成任务的 xhr 的回调函数, 第一次从消息队列中取出执行一次后, 不就没有了吗, 怎么能保证后续 state 改变时的还有回调来执行的呢?

共 2 条评论 >

1



健忘症。

2020-04-09

老师, 我有一些疑问想请教您一下。

您说过 MutationObserver、和 Promise 是可以实现微任务的两种方式。

而微任务的执行时机又是主线程执行结束后, 当前宏任务结束前的时机。

那么说明微任务是依赖与宏任务存在的, 而宏任务是指存放在消息队列中的回调函数。

那是不是可以说, 我使用 Promise 包装了一下 XMLHttpRequest 请求, 有 .then 的操作, 那么 XMLHttpRequest 请求成功后返回的结果, 通过 IPC 包装成了宏任务进入了消息队列中。

当消息队列执行到XMLHttpRequest 回调函数的时候, 是执行了一个宏任务, 那么为什么.the



n 中的回调函数就可以被判定为微任务而去执行的呢??

还有一个问题就是，如果 Promise 并没有进行异步操作，而是直接 new Promise(resolve => {resolve(1)}).then((res) => {})

那么.then 中的回调函数还是不是一个微任务了呢??

望指点一二，再次感谢老师的付出。

共 2 条评论 >

👍 1



**KaKaKa**

2020-04-08

执行 JS 代码是一个任务，执行任务时会维护一个系统调用栈。那当执行 JS 代码这个任务时，系统调用栈和 JS 代码内的执行上下文栈有什么关联?

共 2 条评论 >

👍 1



**Geek\_177f82**

2019-09-16

有个疑惑，就是使用setTimeout执行任务时会把任务添加到延迟消息队列，但是在函数中使用setTimeout就是异步回调。而异步回调函数有两种方式：1，放入微任务处理；2，放入消息队列处理。这样以来就有点迷糊了。那使用setTimeout执行的任务到底应该放哪里执行。还是依据执行环境分别处理。希望老师解答疑惑。谢谢🙏!

共 3 条评论 >

👍 1



**一步**

2019-09-14

文中说：网络进程接收到数据之后，就会利用 IPC 来通知渲染进程；渲染进程接收到消息之后，会将 xhr 的回调函数封装成任务并添加到消息队列中

-----  
这里网络进程收到数据之后，会进行资源请求的结果状态判断吗？只是把对应的资源请求的结果状态 和 响应数据通知给 渲染进程，然后渲染进程 根据请求结果状态选择对应的回调函数加入任务队列中的呢？



👍 1



**一粟**

2019-09-12

随着互联网金融的发展，web安全越来越重要了



👍 1

