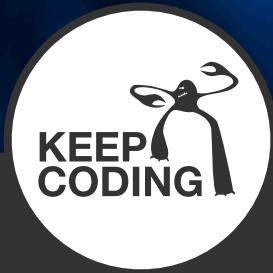
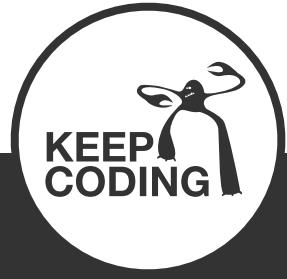
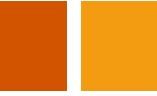


Desarrollo Back End Avanzado

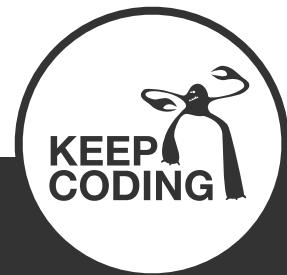






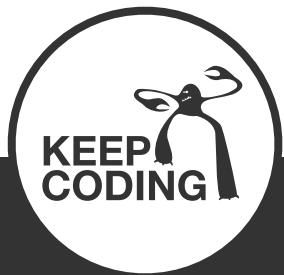
mkcert

<https://github.com/FiloSottile/mkcert>



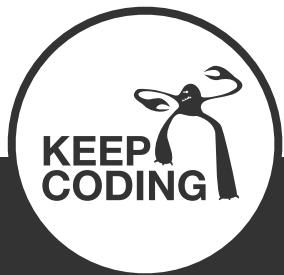


■ Debugging



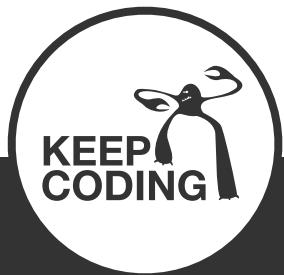


■ Debugging - consola



■ Debugging - consola

```
//mensaje con marcador para un string, salida en stdout stream
console.log("Hello %s", "World");
//mensaje con marcador para un int, salida en stdout stream
console.log("Number of items: %d", 5);
//mensaje con salida en stdout stream
console.info("Hello Info");
//mensaje con salida en stderr stream
console.error("Hello on Stdout");
//mensaje con salida en stderr stream
console.warn("Hello Warn");
```



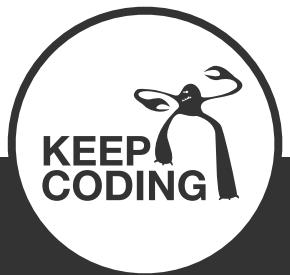
■ Debugging - consola

```
//empieza a contar tiempo
console.time("100mil_elementos");

for(var i=0;i<100000000;i++)
{
    let a = 1;
    a = a * i;
}

//para de contar
console.timeEnd("100mil_elementos");

// 100mil_elementos: 462ms
```

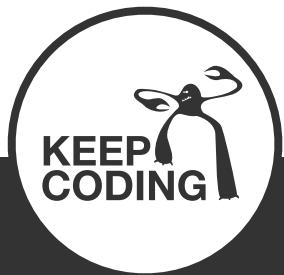


ejemplos/debug

■ Debugging - consola

```
//Escribe a stderr 'Trace : ', seguido de nuestro mensaje  
console.trace("Traza");
```

```
Trace: Traza  
at test (/Users/javi/traza.js:21:13)  
at Object.<anonymous> (/Users/javi/traza.js:25:1)  
at Module._compile (module.js:434:26)  
at Object.Module._extensions..js (module.js:452:10)  
at Module.load (module.js:355:32)  
at Function.Module._load (module.js:310:12)  
at Function.Module.runMain (module.js:475:10)  
at startup (node.js:117:18)  
at node.js:951:3
```



ejemplos/debug

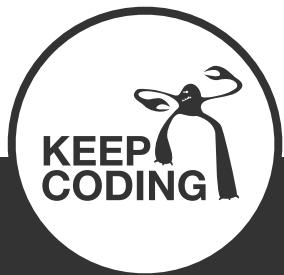
■ Debugging - consola

Si ponemos la instrucción `debugger;` en una linea podremos parar la ejecución ahí. Arrancamos con argumento `debug`:

```
$ node debug prueba.js

< Debugger listening on port 5858
debug> . ok
break in prueba.js:1
> 1 "use strict";
  2
  3 let neo = { name: 'Thomas', age: 33, surname: 'Andreson' };
debug>
```

ejemplos/debug



■ Debugging - consola

Algunos comandos en debugger:

cont, c - Continue execution

next, n - Step next

step, s - Step in

out, o - Step out

pause - Pause running code

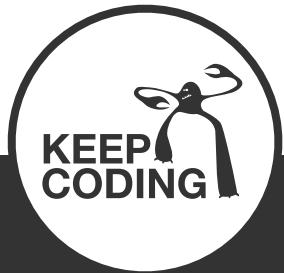
repl - Entra en modo evaluación (Ctrl+c para salir)

help - Muestra comandos

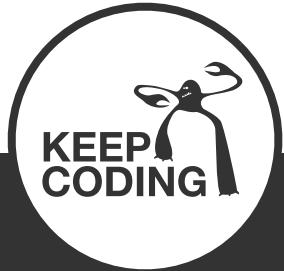
restart - Re-inicia aplicación

kill - Mata la aplicación

scripts - Muestra scripts cargados



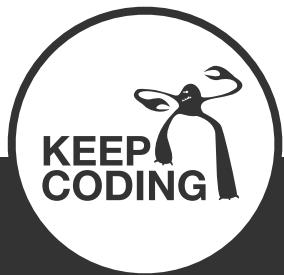
■ --inspect y Chrome



--inspect

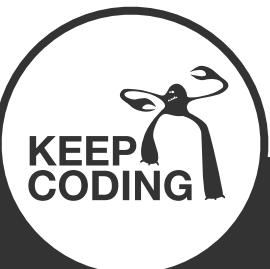
node --inspect-brk index.js

chrome://inspect



--inspect

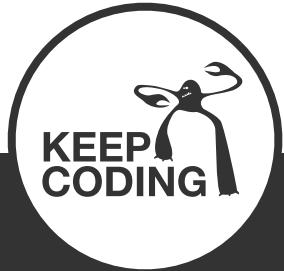
The screenshot shows the Chrome DevTools interface with the title bar "Inspect with Chrome Develop x". The address bar indicates the page is "chrome://inspect/#devices". On the left, a sidebar menu lists "Devices", "Pages", "Extensions", "Apps", "Shared workers", "Service workers", and "Other". The main content area is titled "Devices". It contains two checked checkboxes: "Discover USB devices" with a "Port forwarding..." button and "Discover network targets" with a "Configure..." button. Below these is a link "Open dedicated DevTools for Node". A section titled "Remote Target #LOCALHOST" shows a target entry for "Target (v8.1.0)" with the URL ".bin/www file:///Users/javi/www/cursoronode/keepcoding/_final/nodepop/bin/www inspect".



KEEP
CODING



Debugging - IDE



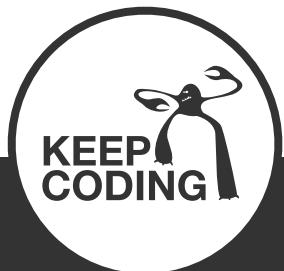
■ Debugging - IDE

The screenshot shows a Node.js debugger interface with the following details:

- Title Bar:** index.js — ejemplo_modulos
- Toolbar:** Includes icons for file operations, a dropdown menu labeled "Mi app", settings, and a search bar.
- Code Editor:** Displays the following JavaScript code:

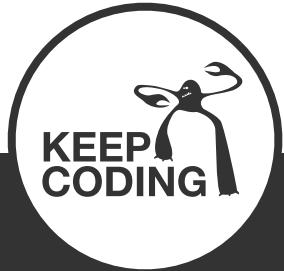
```
1  "use strict";
2
3  const calculadora = require('./calculadora');
4
5  calculadora.marca = 'Siemens';
6
7  console.log(calculadora.suma(5,3));
8
9  const otraCalculadora = require('./calculadora');
10
11 console.log(otraCalculadora.marca);
```
- Variables View:** Shows the "Local" scope with variables like `this`, `__dirname`, `__filename`, `calculadora` (an object with methods `suma`, `resta`, `mult`), `exports`, and `module`.
- Breakpoints:** A red dot indicates a breakpoint at line 3, and a yellow arrow indicates the current execution point at line 5.
- Call Stack:** Labeled "PILA DE LLAMADAS" (Call Stack) and "EN PAUSA POR UN PASO" (Paused by a step). It lists the stack frames:

(anonymous function)	index.js	5:1
Module._compile	module.js	632:14
Module._extensions..js	module.js	646:10





Cluster

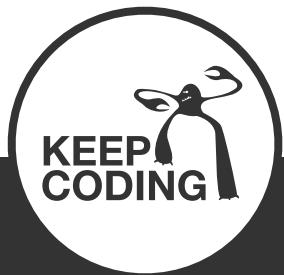


■ Cluster

Desde hace algún tiempo cluster es un módulo core de Node.js.

Podemos requerirlo y pedirle que cree nuevos procesos (fork) compartiendo el mismo puerto de escucha.

Esto debemos hacerlo solo al inicio cuando sabemos que somos el master (`cluster.isMaster`).



Cluster

```
var cluster = require('cluster');

if (cluster.isMaster) {

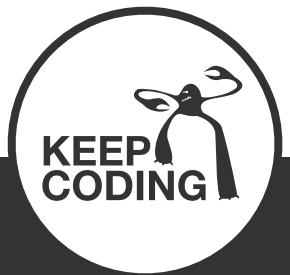
    // hacer forks creando workers, uno por core lógico
    var numCPUs = require('os').cpus().length;
    for (var i = 0; i < numCPUs; i++) {
        cluster.fork();
    }

} else {

    // arranque normal de nuestro server

}
```

ejemplos/cluster



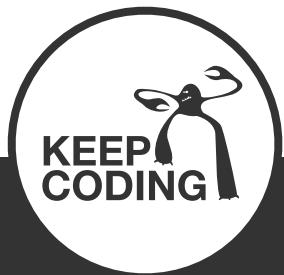
■ Cluster

Esto arrancará n procesos adicionales, a los que el master les irá dando peticiones según lógica round robin.

Cluster emite eventos a los que podemos suscribirnos, como por ejemplo:

- online
- exit
- listening
- disconnect
- message

ejemplos/cluster



Cluster

Los eventos que emite los escucharemos así:

```
// al arrancar un worker...
cluster.on('online', function(worker) {
  console.log('Worker ' + worker.id +
    ' is online with pid ' + worker.process.pid);
});

// al terminar un worker...
cluster.on('exit', function(worker, code, signal) {
  console.log('worker ' + worker.process.pid + ' died');
});
```

ejemplos/cluster



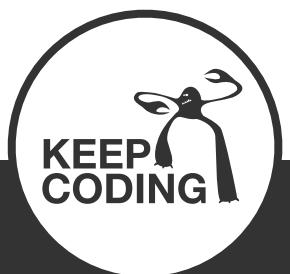
KEEP
CODING

Cluster

Cuando un worker muere emite el evento exit. En este momento podemos reaccionar y crear otro que le sustituya:

```
// al terminar un worker...
cluster.on('exit', function(worker, code, signal) {
  console.log('Worker ' + worker.process.pid +
    ' died with code: ' + code +
    ', and signal: ' + signal);
  console.log('Starting a new worker');
  cluster.fork();
});
```

ejemplos/cluster



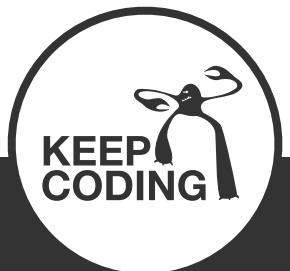
Cluster

El proceso master puede mandar mensajes a los workers.

```
// master
// cluster.workers nos da una lista de los que tenemos
worker.send('hello from the master');

// worker
process.on('message', function(message) {
  console.log(message);
});
```

ejemplos/cluster



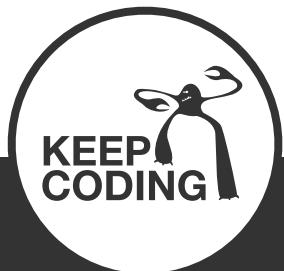
Cluster

Los workers pueden mandar mensajes al master.

```
// worker
process.send('hello from worker with id: ' + process.pid);
```

```
// master
worker.on('message', function(message) {
  console.log(message);
});
```

ejemplos/cluster



■ Cluster

Con cluster aumentaremos notablemente el rendimiento de nuestro servidor, usando más recursos del sistema.

Concurrent Connections	1	2	4	8	16
Single Process	654	711	783	776	754
8 Workers	594	1198	2110	3010	3024

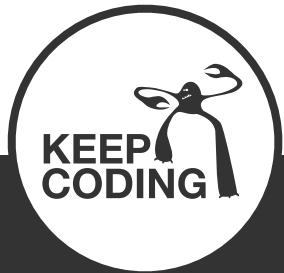
* Ejemplo de medición con peticiones por segundo.

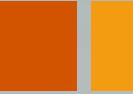


■ Cluster

Es recomendable leer la documentación!

<https://nodejs.org/api/cluster.html>





■ Internacionalización y localización

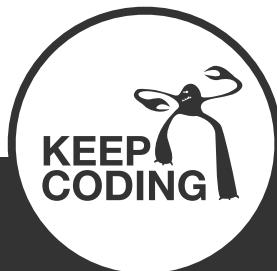
Nuestra web, en varios idiomas



■ Internacionalización y localización

El objetivo de la internacionalización y la localización es permitir a un único sitio web ofrecer sus contenidos en diferentes idiomas y formatos adaptados a su audiencia.

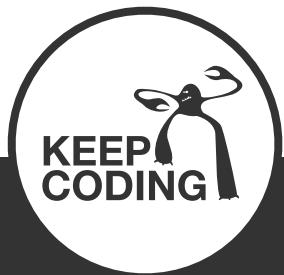
No sólo vale con traducir, también hay que formatear los contenidos en función de las preferencias del usuario.



Ejemplo

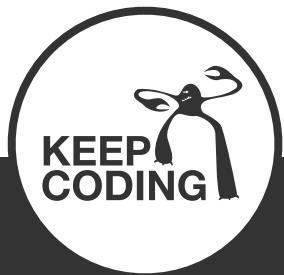
Formato de fecha España: dd/mm/yyyy

Formato de fecha USA: mm/dd/yyyy



■ Definiciones

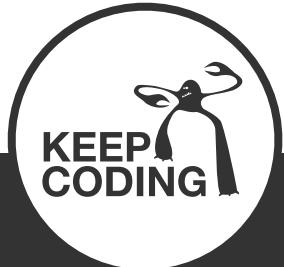
- **Internacionalización:** preparar el software para que sea localizable (trabajo de desarrolladores).
- **Localización:** escribir la traducción y los formatos locales (trabajo de traductores)



Cómo traducir en Node.js

- Instalar i18n-node - **npm install i18n**
- Inicializar i18n con **i18n.configure({ ... })**
- Crear archivos de mensajes en carpeta **locales**
- En nuestro código, usar la función **i18n._()**

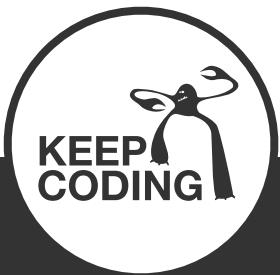
<https://github.com/mashpie/i18n-node>



■ Configuración

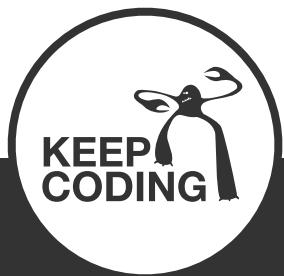
```
const i18n = require("i18n");

i18n.configure({
  directory: path.join(__dirname, '../locales'),
  defaultLocale: 'en',
  queryParameter: 'lang',
  autoReload: true,
  updateFiles: false,
  objectNotation: true,
  register: global
});
```



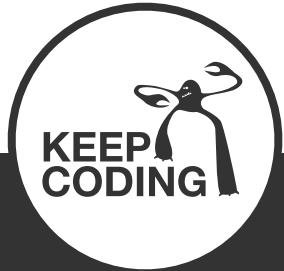
■ Archivo de lenguajes

```
./locales/en.json
{
    "EXAMPLE": {
        "TEXT": "Text",
        "HELLO": "Hello %s, i'm from %s",
        "NAME_AND AGE": "My name is {{name}}",
        "MOUSE": {
            "one": "%s Mouse",
            "other": "%s Mice"
        }
    }
}
```



■ Configuración de Express

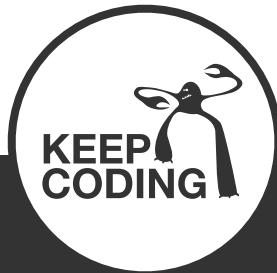
```
app.use(i18n.init);
```



■ Configuración scripts

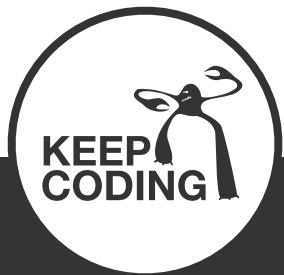
Poner locale para scripts:

```
i18n.setLocale(defaultLocale); // default locale for scripts
```



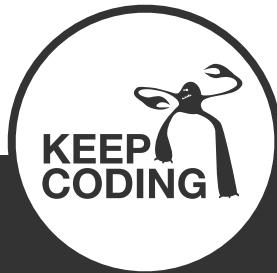
■ Usar __()

```
__('EXAMPLE.TEXT')  
  
__('EXAMPLE.HELLO', 'Pepe', 'Madrid')  
  
__('EXAMPLE.NAME_AND_AGE', {name: 'Javier', age: 33})  
  
__({phrase: 'EXAMPLE.TEXT', locale: 'es'})  
  
__n('EXAMPLE.MOUSE', 2)
```

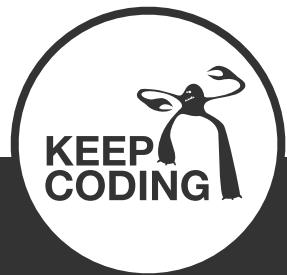


■ ¿Cómo sé qué idioma quiere el usuario?

- A través de la cabecera “Accept-Language” de una petición HTTP los navegadores envían la preferencia de idioma de un usuario.
- Si no se envía la cabecera, devolver el idioma por defecto.
- Existen otras técnicas como la geolocalización por IP (si la IP es de España, redirigir al sitio en español) aunque son más complejas.
- [i18n-node](#) lo gestiona por nosotros automáticamente



Ejemplo de cabecera



KEEP
CODING



Let's code
Jesse



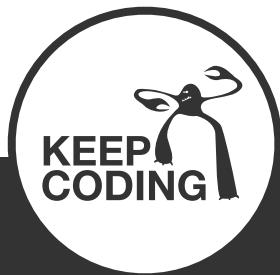


Tareas en segundo plano

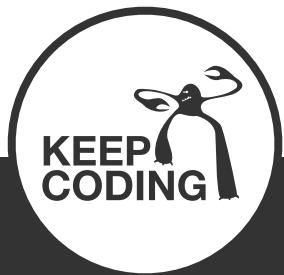
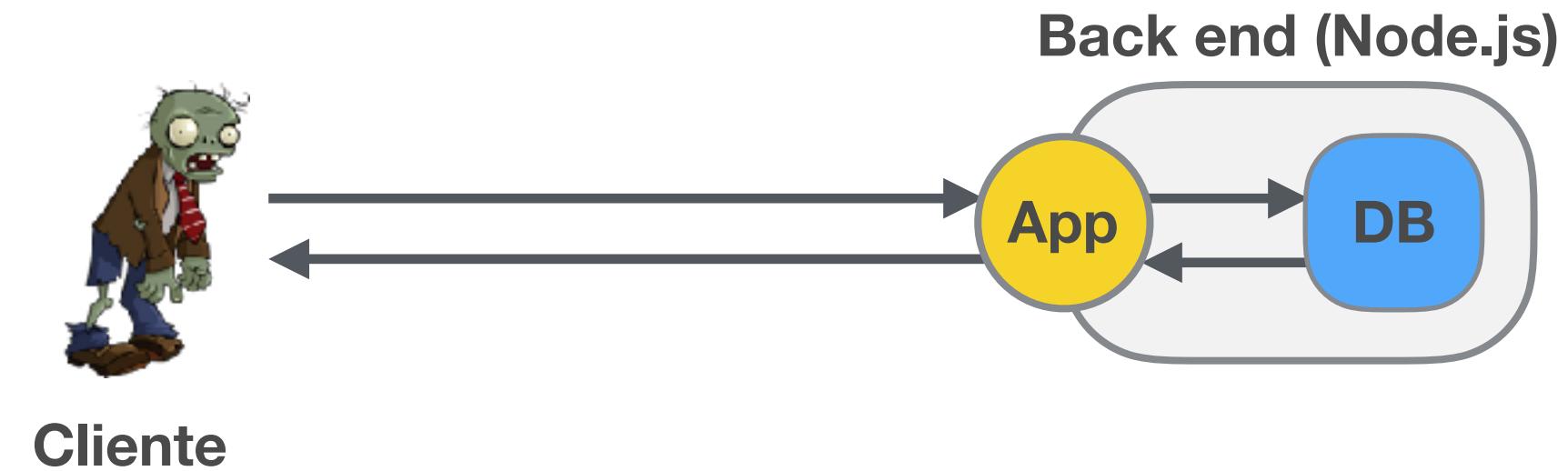


Tareas lentes o pesadas

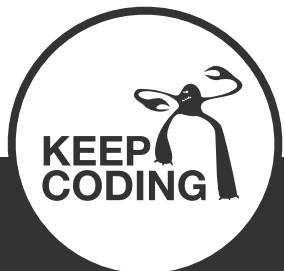
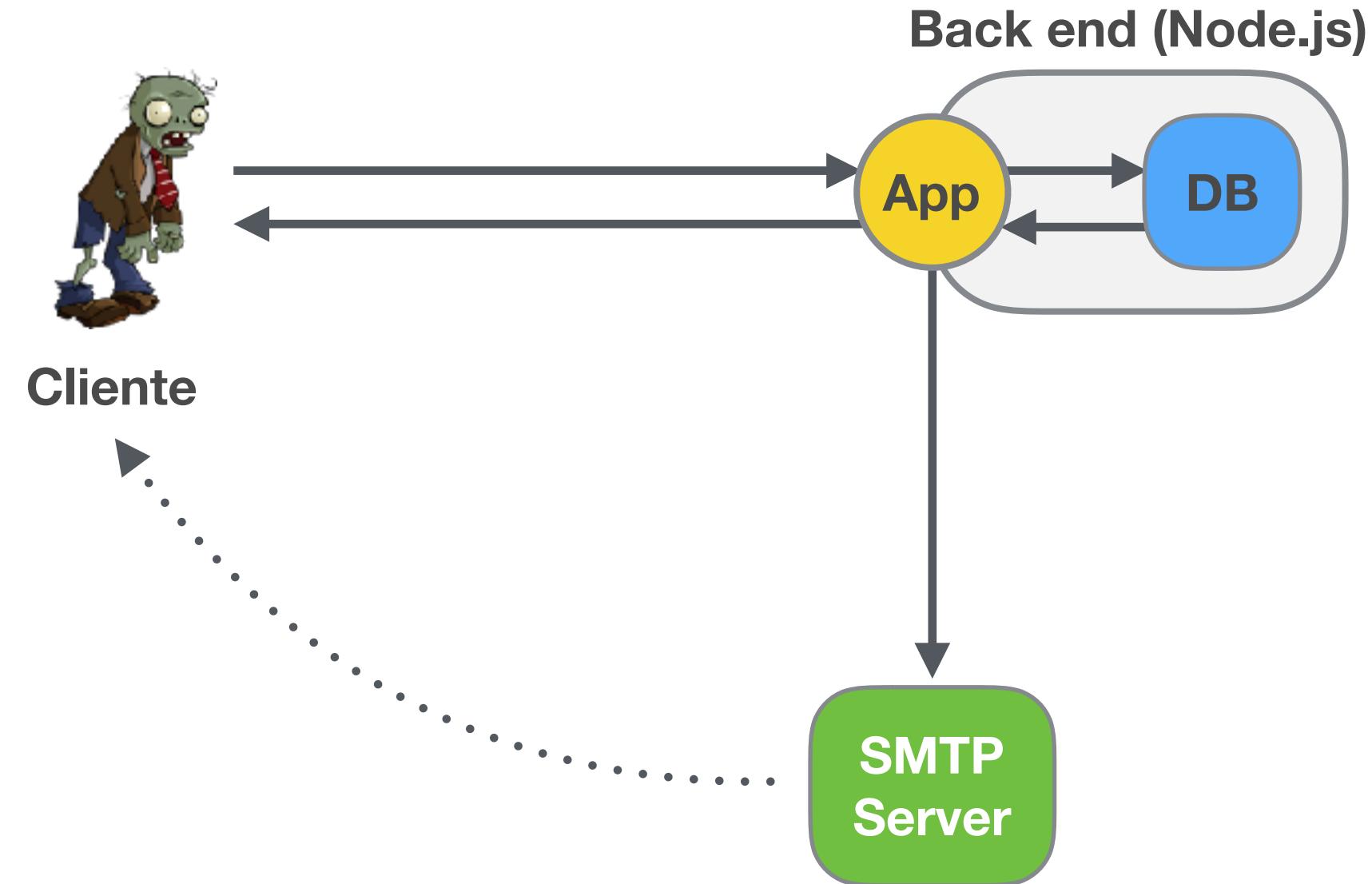
- Las respuestas a las peticiones HTTP deben ser casi inmediatas
- Un backend lento, es un backend mal hecho
- Pero a veces hay que hacer cosas que son lentes como **enviar correo, redimensionar una imagen, leer archivos** gigantes...
- Todas esas tareas lentes, deberemos hacerlas de manera diferida



■ Flujo básico de una petición HTTP



Envío de un e-mail desde un back-end



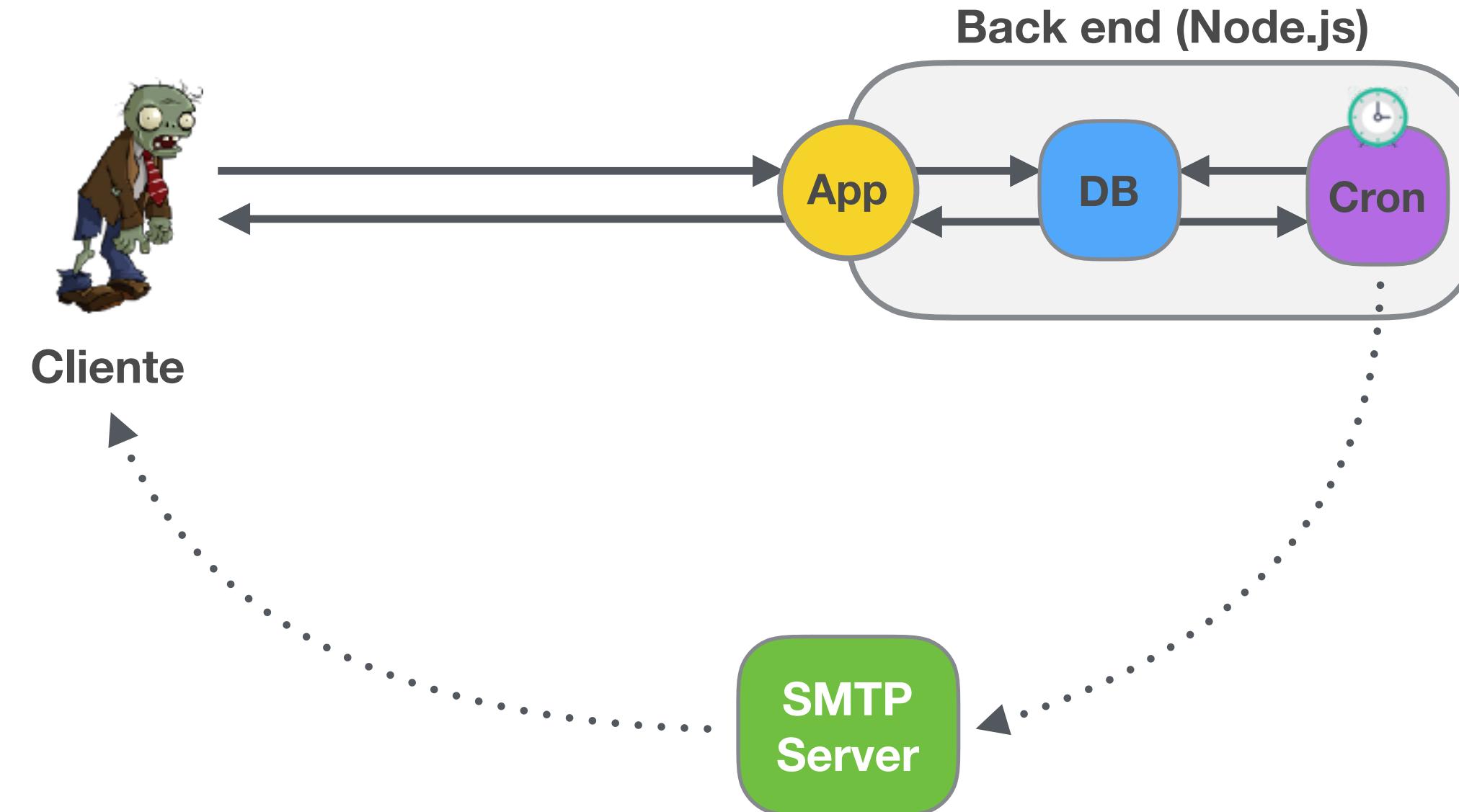
KEEP
CODING



Let's code
Jesse



Envío con tarea programada

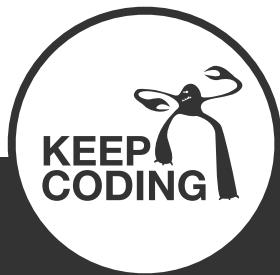


KEEP
CODING

■ Comandos personalizados en NPM

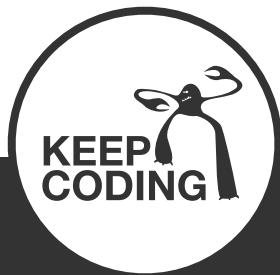
NPM nos permite crear nuestro propios comandos personalizados

Esto es útil para ejecutarlos desde la consola o a través de tareas programadas (con cron)

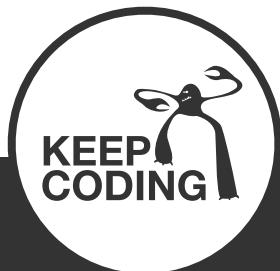
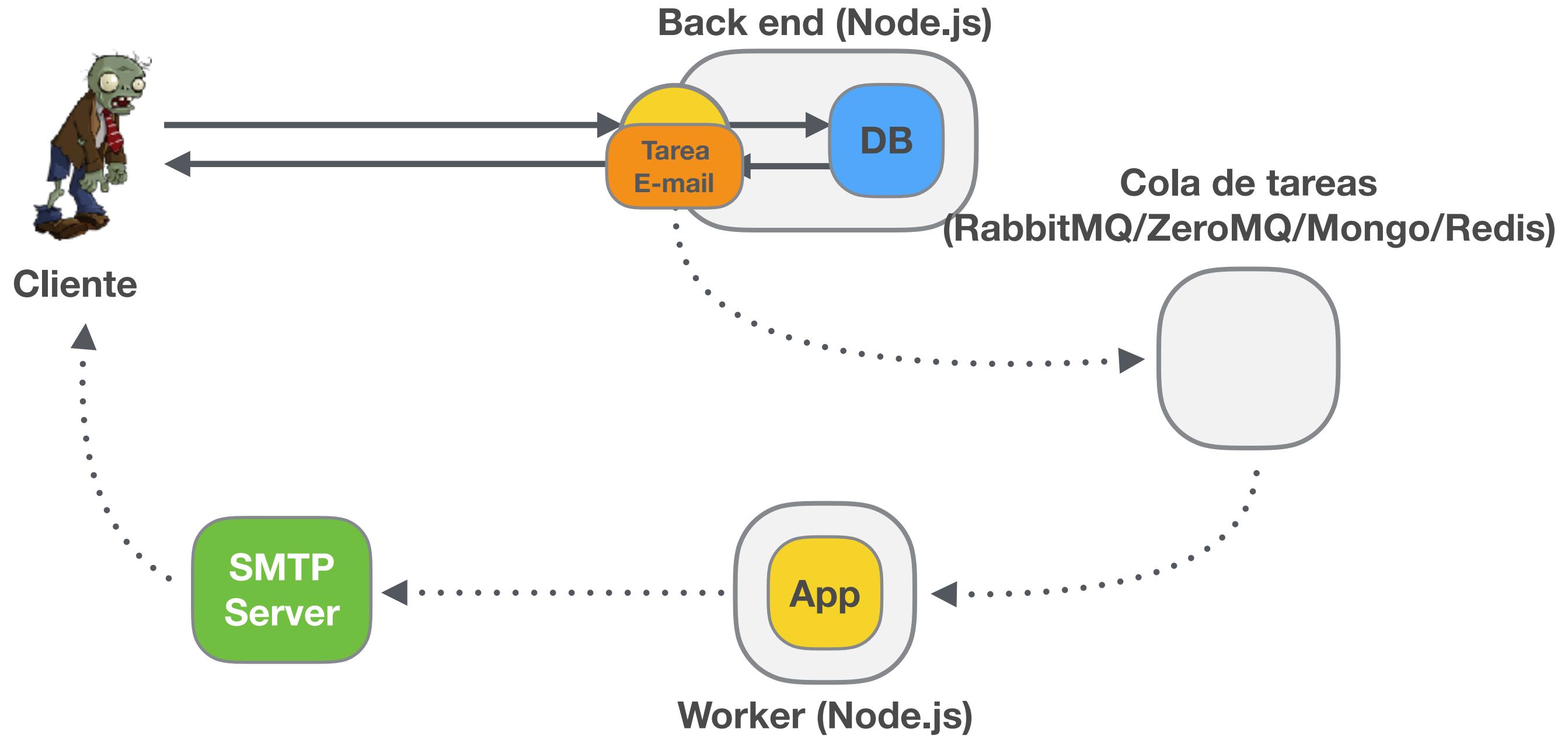


■ Comandos personalizados en NPM

Tan sólo hay que crear una entrada en **package.json**,
apartado **scripts**



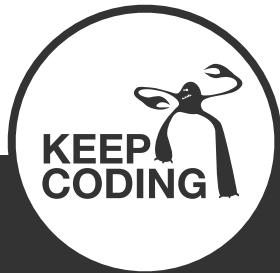
Envío de un e-mail con tareas en background



Tareas en background con RabbitMQ

RabbitMQ es un software de envío de mensajes que implementa el protocolo AMQP

<https://www.rabbitmq.com>

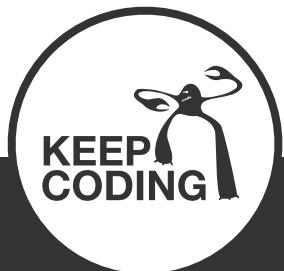


Tareas en background con RabbitMQ

Podemos usarlo desde:

- **Instalación Win/linux/Mac**
 - <https://www.rabbitmq.com/download.html>
- **Docker**
 - https://hub.docker.com/_/rabbitmq/
- **CloudAMQP**
 - <https://www.cloudamqp.com/>

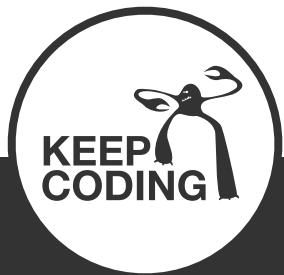
Y más... (amazon, cloud foundry, etc)



Tareas en background con RabbitMQ

Docker

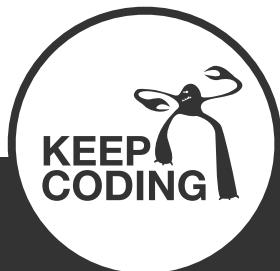
```
docker run  
-d --hostname= mq --name mq -p 8080:15672 -p 5672:5672  
rabbitmq:3-management
```



Tareas en background con RabbitMQ

npm i amqplib

- **Uso con Node.js**
 - <http://www.squaremobius.net/amqp.node/>
- **Ejemplos estratégias**
 - <https://github.com/squaremo/amqp.node/blob/master/examples/tutorials/README.md>



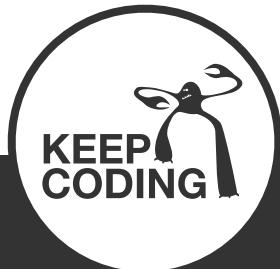
Tareas en background con RabbitMQ

¿Que tamaño pueden tener los mensajes?

Teóricamente: 2^{64} bytes

En la práctica depende de las máquinas que usemos y la conexión.

Si los mensajes son grandes mejor enviar una ruta a un servidor de ficheros o similar.



Tareas en background con otros motores

Usando MongoDB:

<https://github.com/chilts/mongodb-queue>

<https://github.com/scttnlsn/monq>

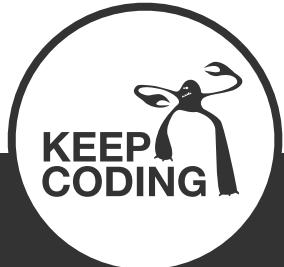
<https://github.com/agenda/agenda>

Usando Redis:

<https://github.com/OptimalBits/bull>

<https://github.com/Automattic/kue>

<https://github.com/bee-queue/bee-queue>



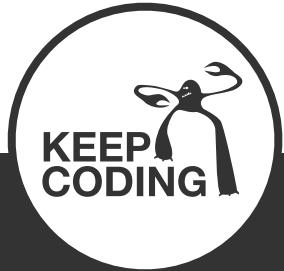


Let's code
Jesse



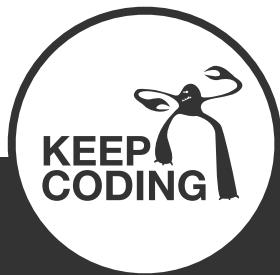


■ WebSockets



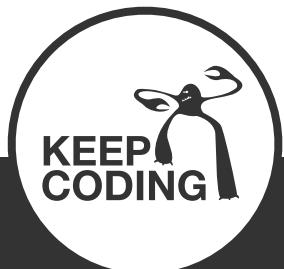
- **WebSockets** es una tecnología avanzada que hace posible abrir una sesión de comunicación interactiva entre el navegador del usuario y un servidor

Fuente: MDN <https://developer.mozilla.org/es/docs/WebSockets-840092-dup>



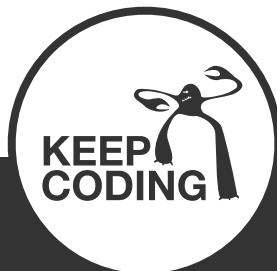
■ Compatibilidad navegadores

Protocolo	Fecha versión preliminar	Internet Explorer	Implementation status					
			Firefox ¹⁷ (PC)	Firefox (Android)	Chrome (PC, Mobile)	Safari (Mac, iOS)	Opera (PC, Móvil)	Android Browser
hixie-75 ↗	February 4, 2010				4	5.0.0		
hixie-76 ↗	May 6, 2010		4.0		6	5.0.1	11.00	
hybi-00 ↗	May 23, 2010		(disabled)				(disabled)	
7 hybi-07 ↗	April 22, 2011		6 ¹⁸					
8 hybi-10 ↗	July 11, 2011		7 ¹⁹	7	14 ²⁰			
13 RFC 6645	December, 2011	10 ²¹	11	11	16 ²²	6	12.10 ²³	4.4



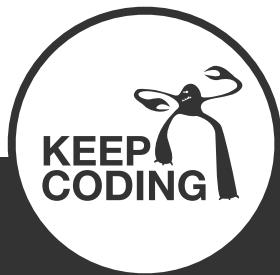
■ Características

- El protocolo es un estándar ([RFC 6455](#))
- Está diseñada para ser implementada en navegadores y servidores web, pero puede utilizarse por cualquier aplicación cliente/servidor
- Usa los puertos habituales HTTP (80,443)
- Atraviesa firewalls y proxies



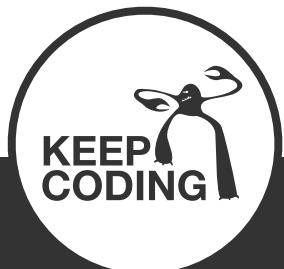
Casos prácticos

- Juegos online multijugador
- Aplicaciones de chat
- Rotativos de información deportiva
- Actualizaciones en tiempo real de las actividades de tus amigos



■ Algunas implementaciones

- **Node.js**
 - Socket.IO
 - WebSocket-Node
 - ws
- **Python**
 - pywebsocket
 - Tornado
- **Ruby**
 - EventMachine
- **Java**
 - Jetty
- **Erlang**
 - Shirasu
- **C++**
 - libwebsockets
- **.NET**
 - SuperWebSocket

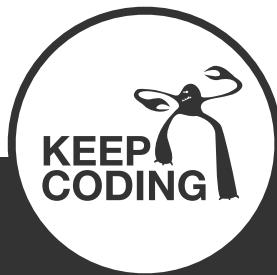


Con socket.io

```
var app = require('express')();
var server = require('http').Server(app);

app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));
```



Con socket.io

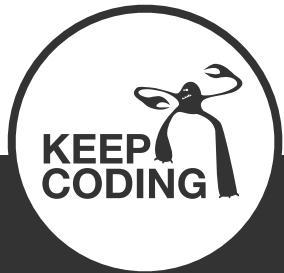
```
var app = require('express')();
var server = require('http').Server(app);

app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));

var io = require('socket.io')(server);

io.on('connection', function(socket){
  socket.on('chat message', function(msg){
    io.emit('chat message', msg);
  });
});
```



Con socket.io

```
var app = require('express')();
var server = require('http').Server(app);

app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));

var io = require('socket.io')(server);

io.on('connection', function(socket){
  socket.on('chat message', function(msg){
    io.emit('chat message', msg);
  });
});
```

Le pasamos a socket.io nuestro server para que se instale en el mismo puerto



■ Con socket.io

```
var app = require('express')();
var server = require('http').Server(app);

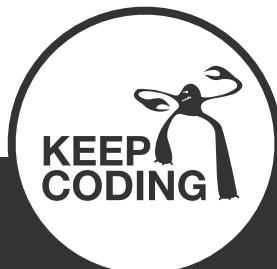
app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));

var io = require('socket.io')(server);

io.on('connection', function(socket){
  socket.on('chat message', function(msg){
    io.emit('chat message', msg);
  });
});
```

Ante cada conexión de un cliente
se crea un socket



■ Con socket.io

```
var app = require('express')();
var server = require('http').Server(app);

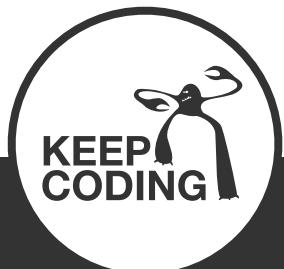
app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));

var io = require('socket.io')(server);

io.on('connection', function(socket){
  socket.on('chat message', function(msg){
    io.emit('chat message', msg);
  });
});
```

Escuchamos eventos del socket



Con socket.io

```
var app = require('express')();
var server = require('http').Server(app);

app.get('/', (req, res) => res.sendFile(__dirname + '/index.html'));

server.listen(3000, () => console.log('listening on *: 3000'));

var io = require('socket.io')(server);

io.on('connection', function(socket){
  socket.on('chat message', function(msg){
    io.emit('chat message', msg);
  });
});
```

Emitimos mensajes



Con socket.io

```
// sending to sender-client only
socket.emit('message', "this is a test");

// sending to all clients, include sender
io.emit('message', "this is a test");

// sending to all clients except sender
socket.broadcast.emit('message', "this is a test");

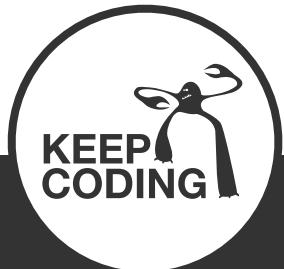
// sending to all clients in 'game' room(channel) except sender
socket.broadcast.to('game').emit('message', 'nice game');

// sending to all clients in 'game' room(channel), include sender
io.in('game').emit('message', 'cool game');

// sending to sender client, only if they are in 'game' room(channel)
socket.to('game').emit('message', 'enjoy the game');

// sending to all clients in namespace 'myNamespace', include sender
io.of('myNamespace').emit('message', 'gg');

// sending to individual socketid
socket.broadcast.to(socketid).emit('message', 'for your eyes only');
```



KEEP
CODING



Let's code
Jesse



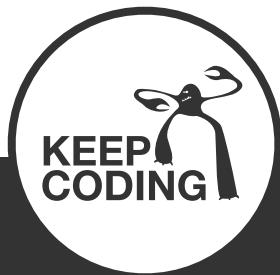


Microservicios



■ Introducción

La arquitectura de microservicios nace como respuesta a la problemática del mantenimiento y evolución de grandes aplicaciones monolíticas.

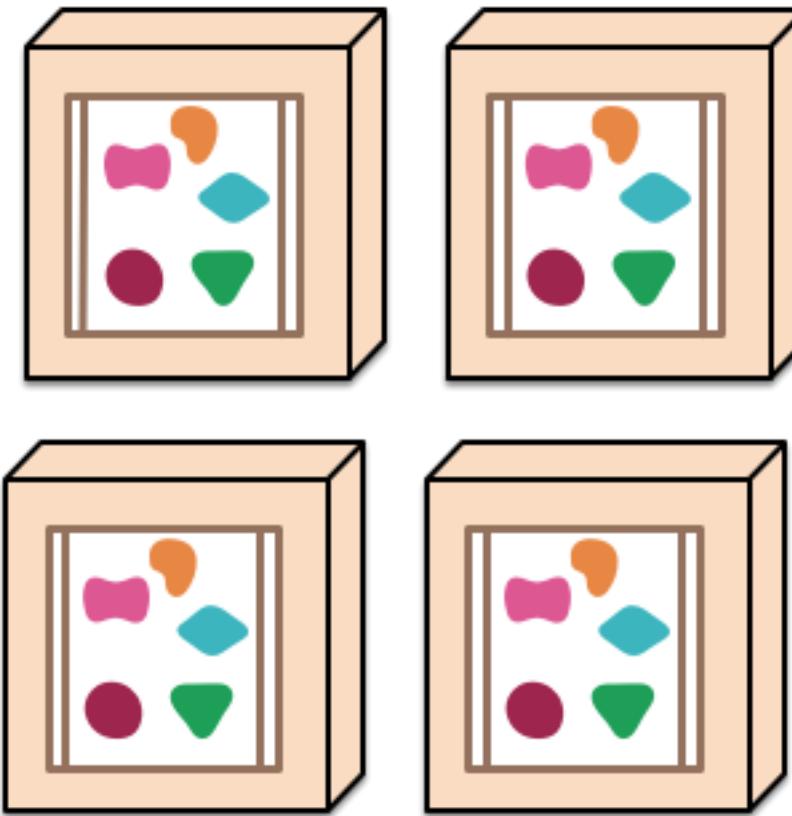




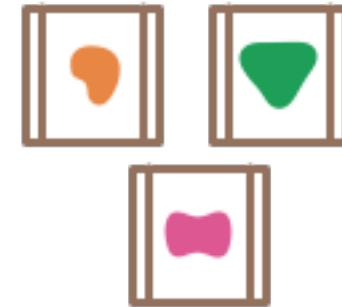
A monolithic application puts all its functionality into a single process...



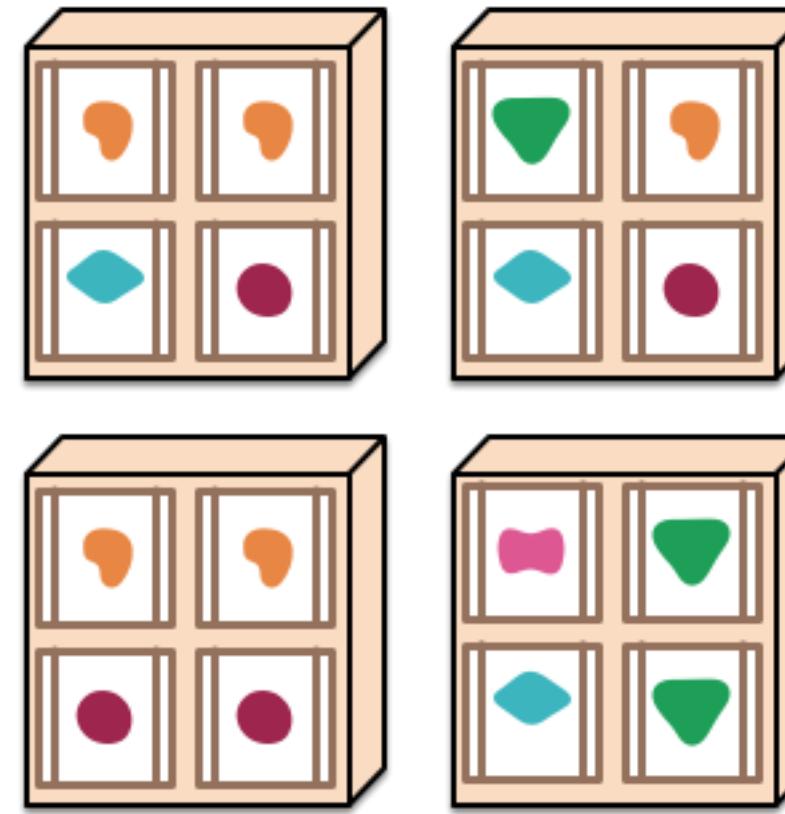
... and scales by replicating the monolith on multiple servers



A microservices architecture puts each element of functionality into a separate service...

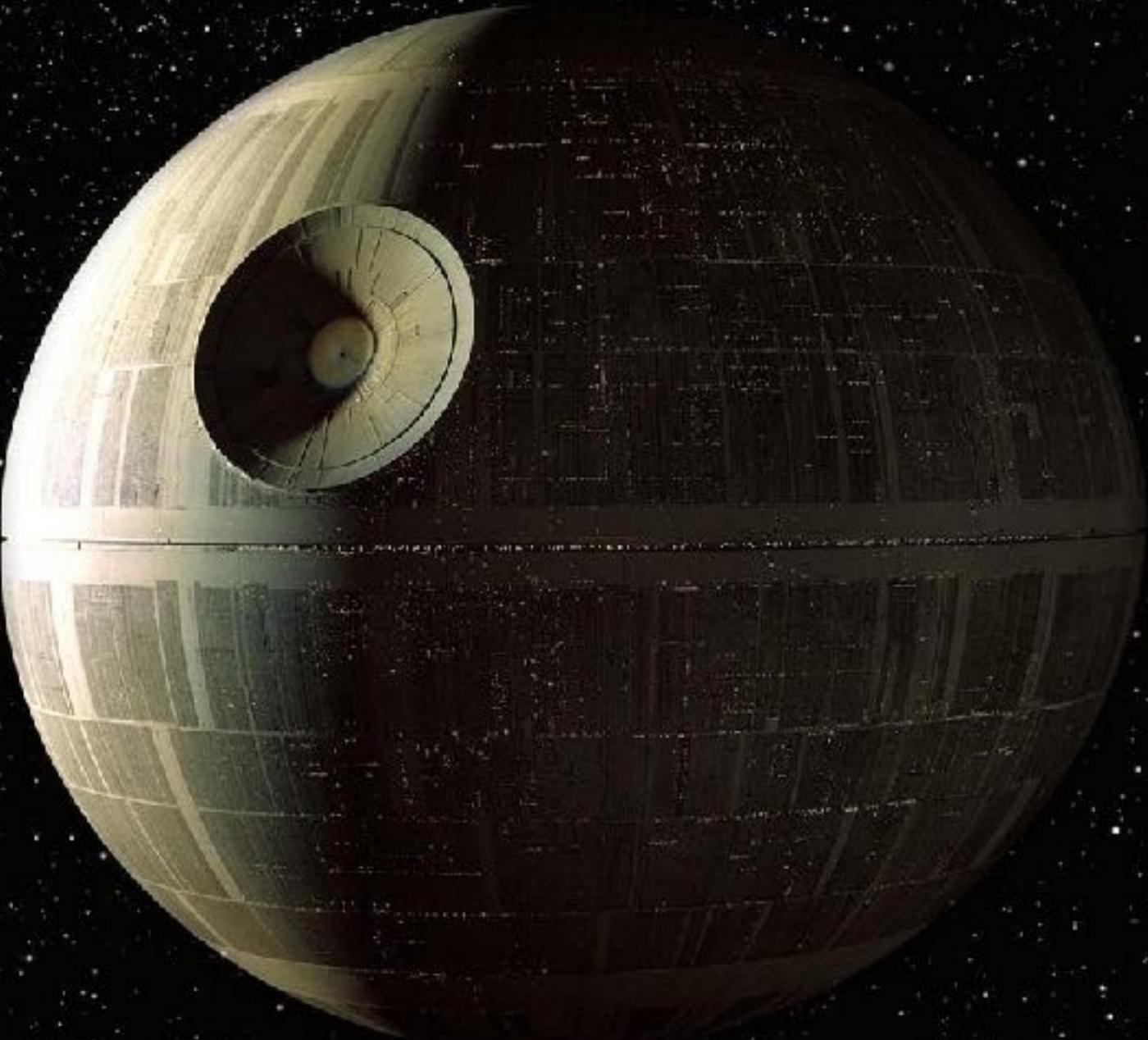


... and scales by distributing these services across servers, replicating as needed.



<http://martinfowler.com/articles/microservices.html>



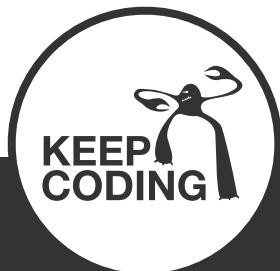


Aplicación monolítica



■ Problemática de las aplicaciones monolíticas

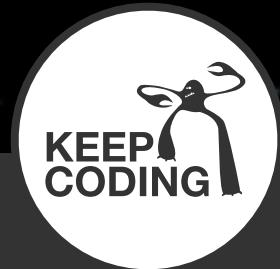
- Si algo falla en la aplicación, todo el sistema se cae
- Son difícil de escalar a nivel de infraestructura
- Es difícil de escalar a nivel de equipo de desarrollo (hasta que todos los desarrolladores saben cómo funciona todo el monolito)
- Es muy difícil mantener la interdependencia de relaciones y un código limpio (spaghetti code, merge conflicts, etc...)
- Es la manera natural de desarrollar (todo software tiende a monolito)







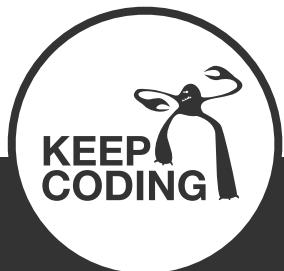
Microservicios

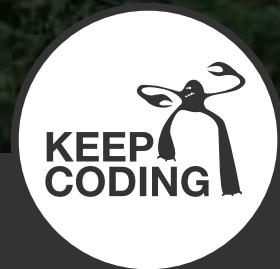


KEEP
CODING

Ventajas de los microservicios

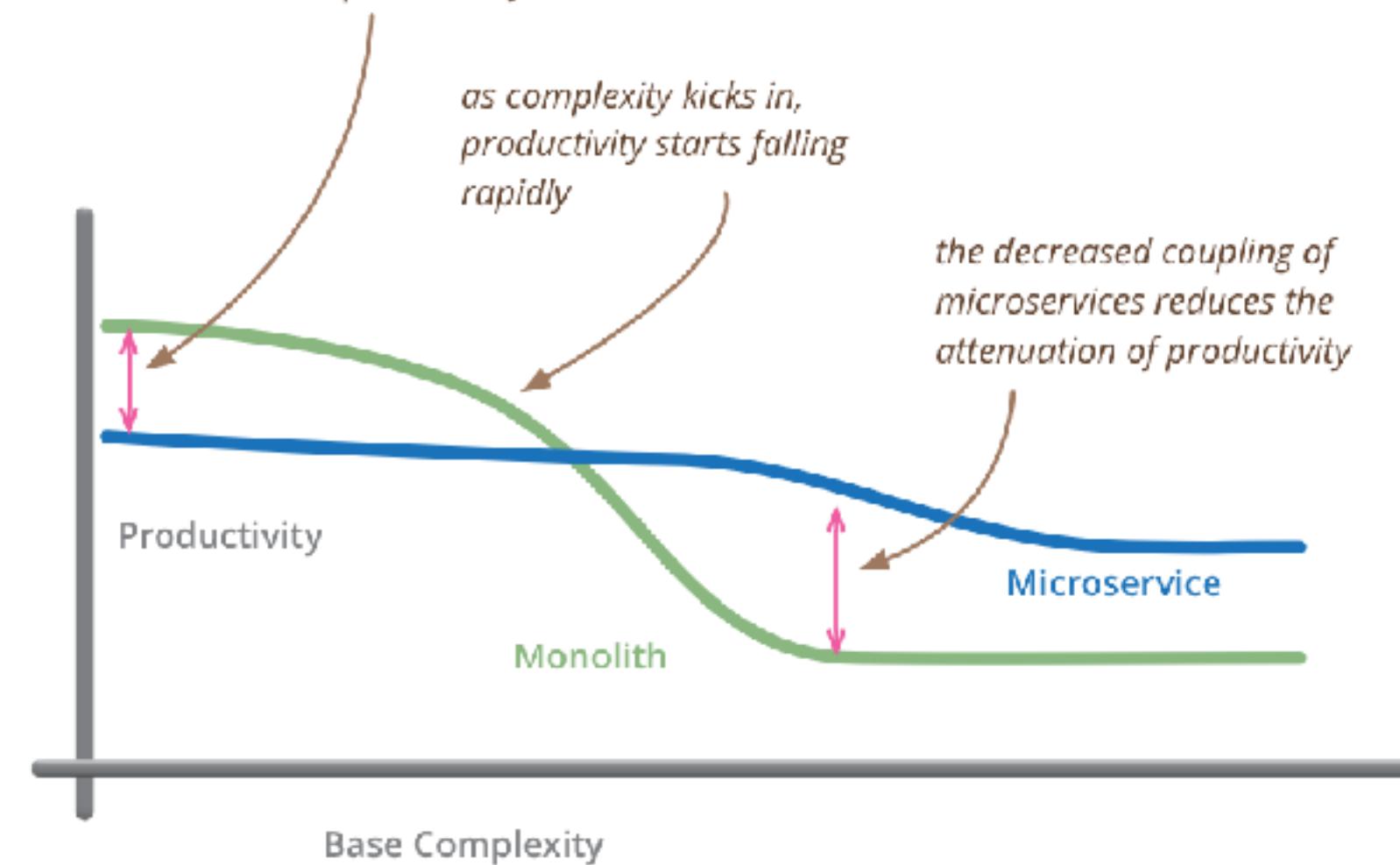
- Si falla un microservicio, no todo el sistema falla
- Su infraestructura es fácilmente escalable
- Fácil de escalar los equipos de desarrollo (cada equipo sólo debe mantener un par de microservicios)
- Código más mantenible y reutilizable (menos interdependencias)
- Permiten utilizar la mejor tecnología para cada problema





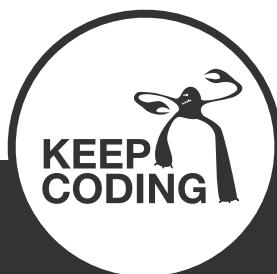


for less-complex systems, the extra baggage required to manage microservices reduces productivity



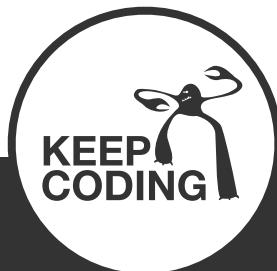
but remember the skill of the team will outweigh any monolith/microservice choice

<http://martinfowler.com/microservices/>

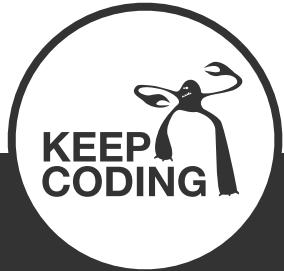
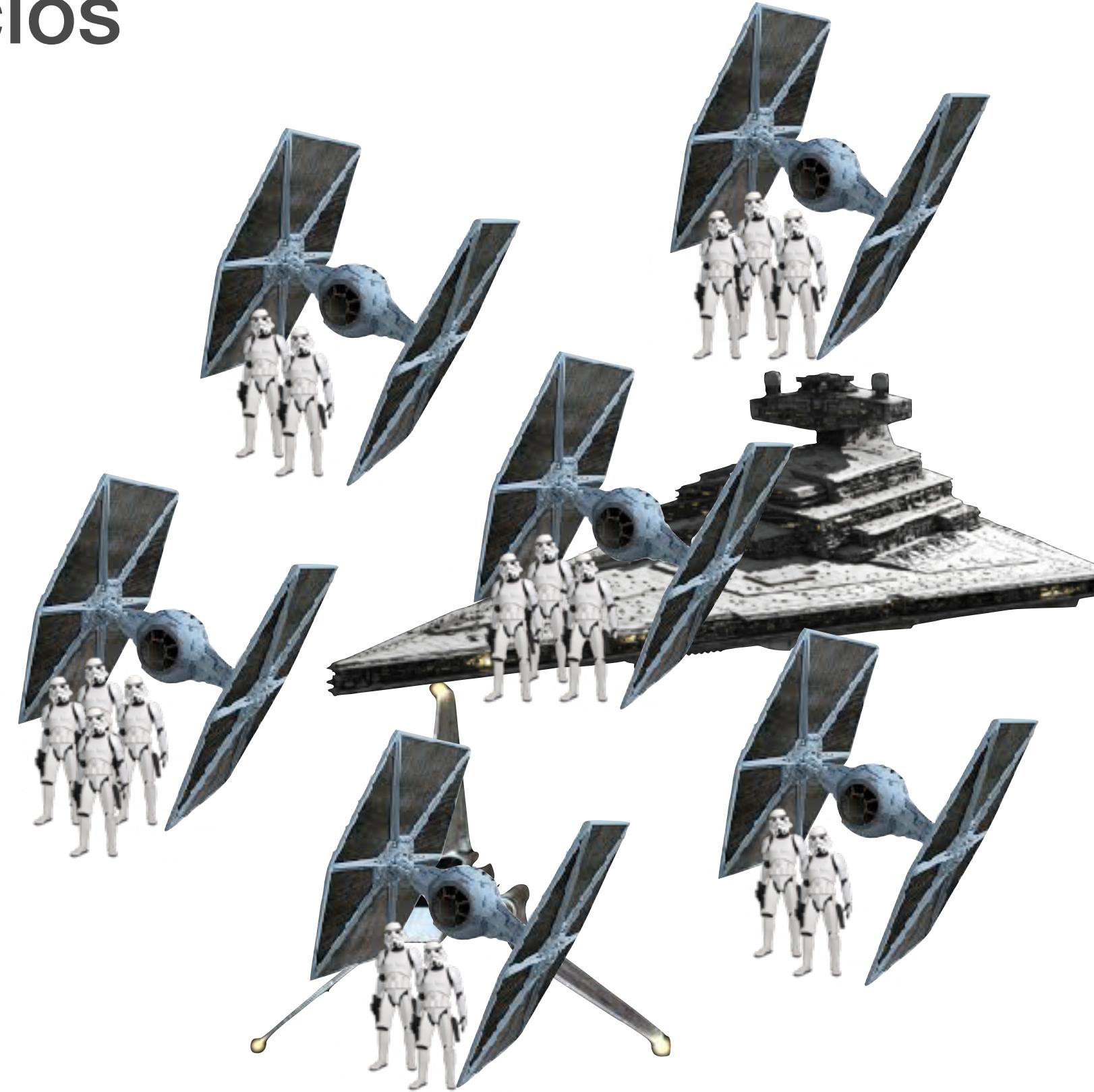
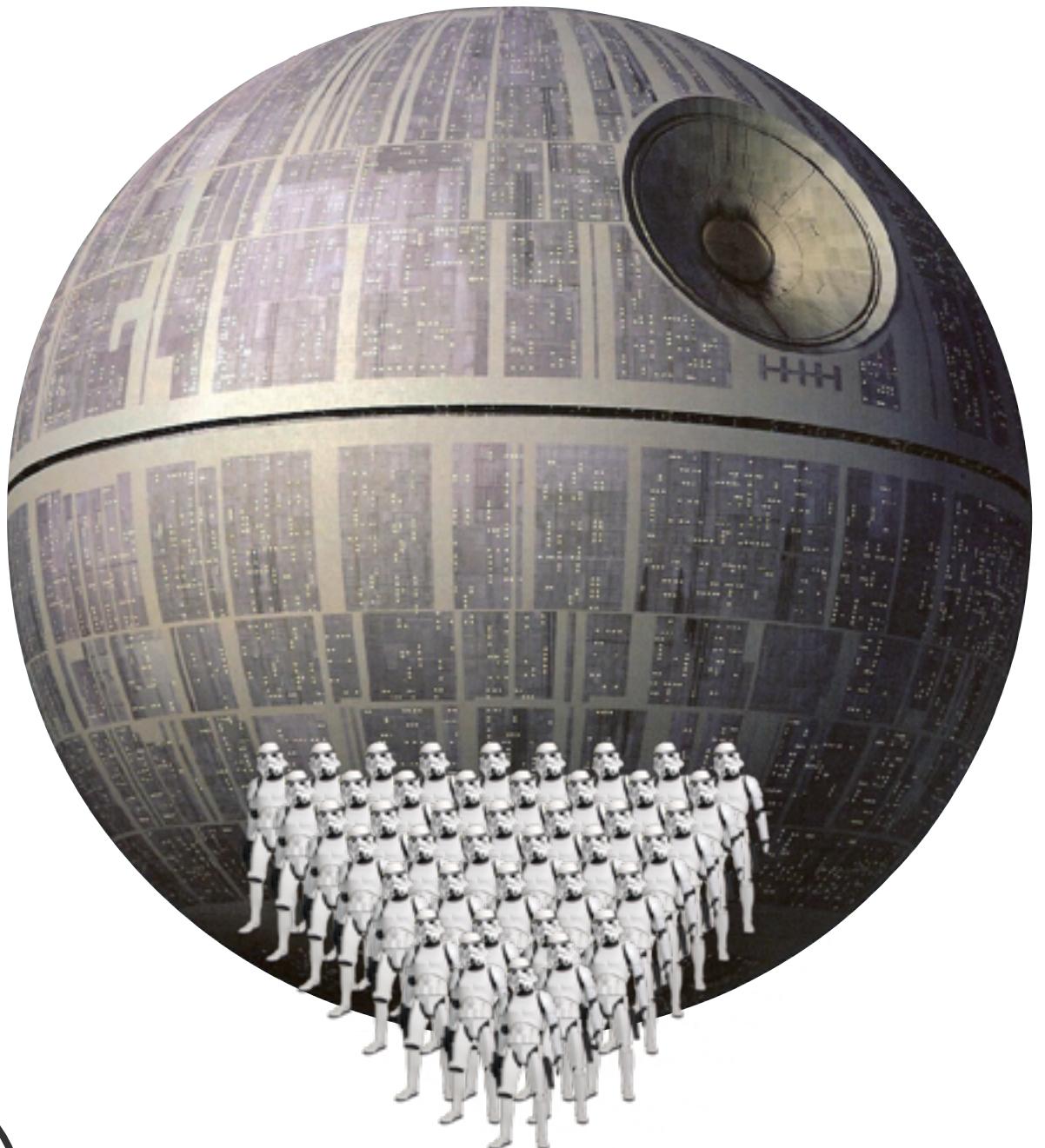


■ Problemática de los microservicios

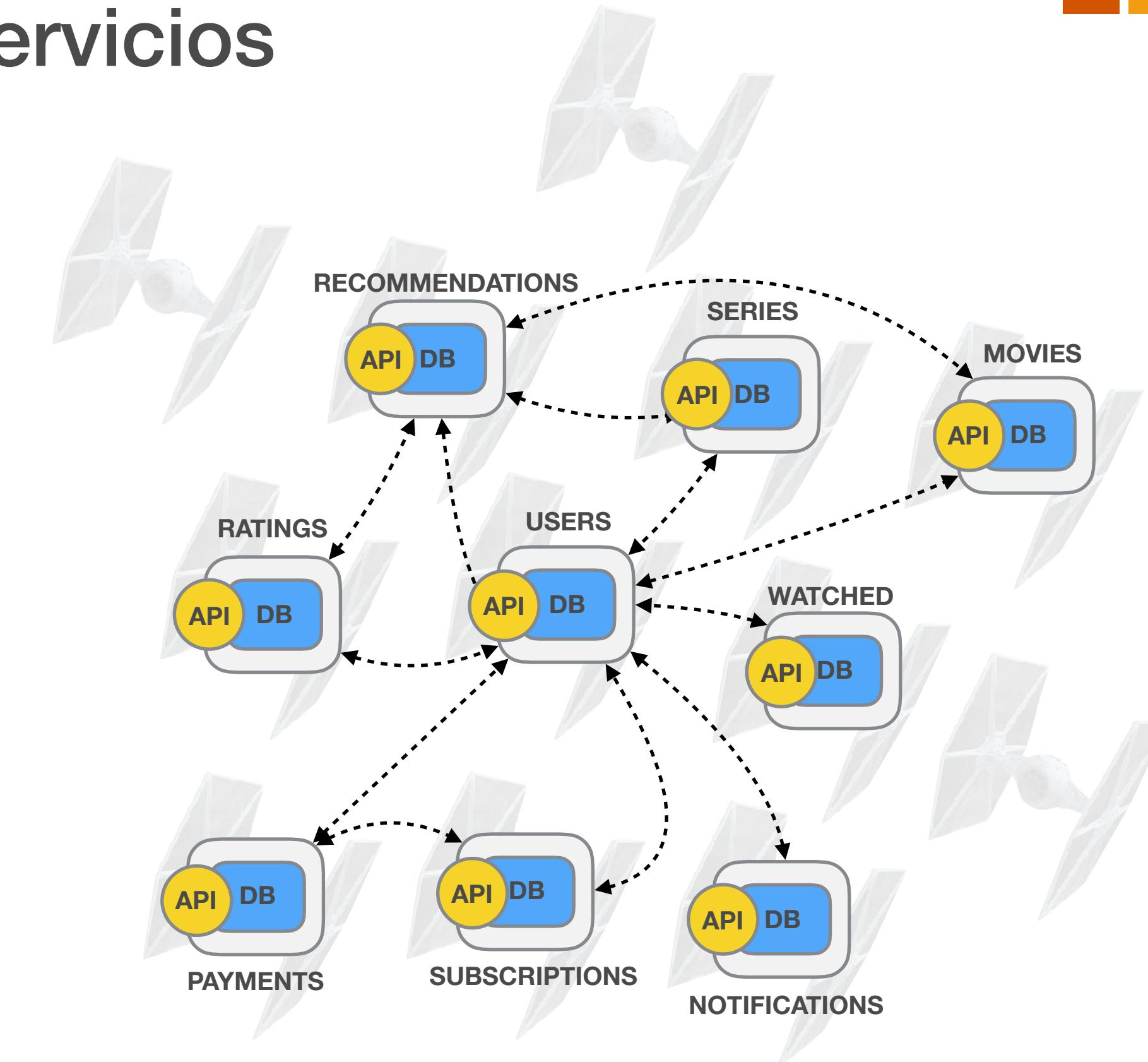
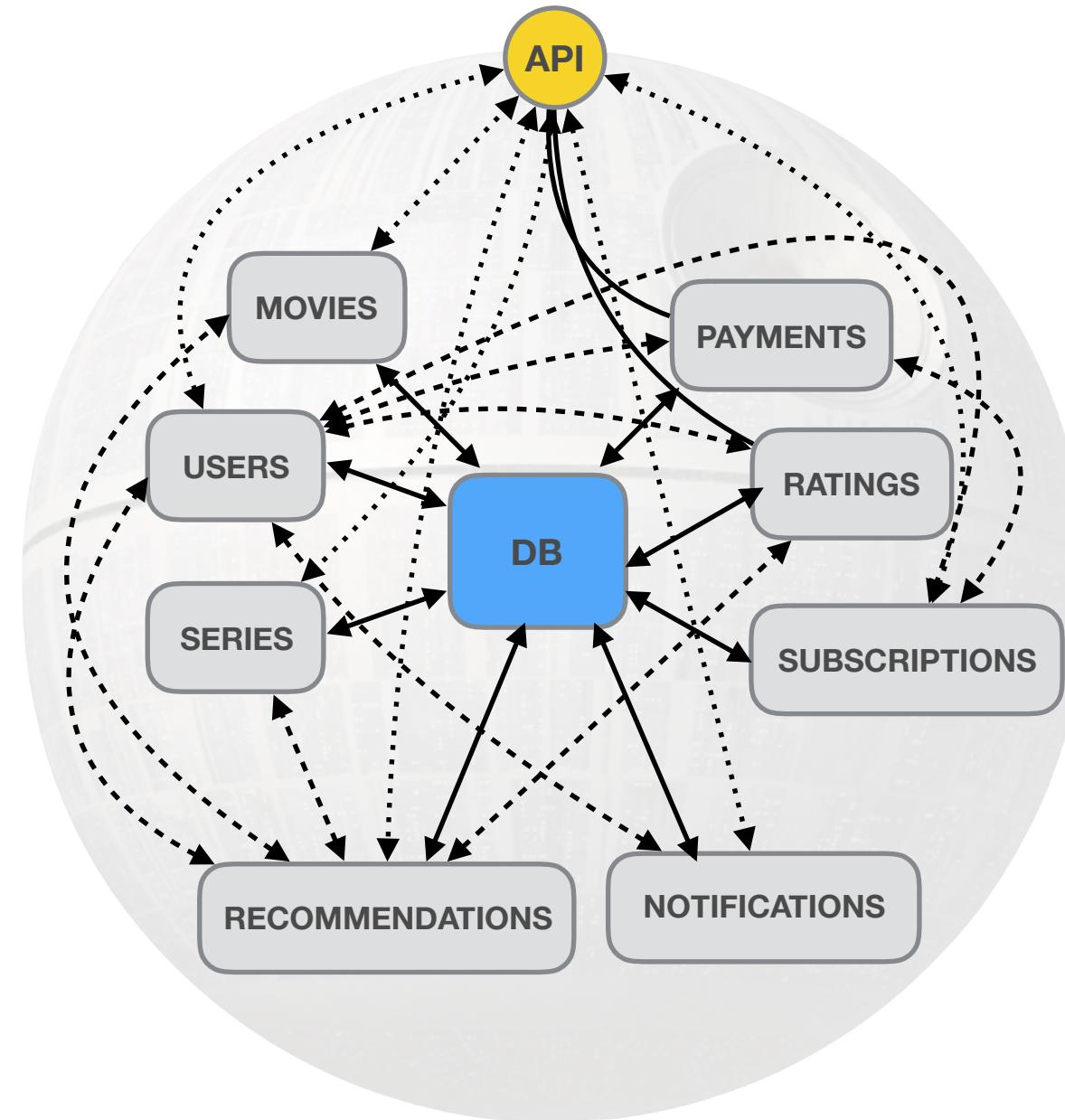
- Orquestación: es más difícil hacer una buena coordinación de todos
- Entorno de desarrollo: arrancar un entorno de desarrollo con 300 microservicios te puede llevar un rato...solución: Docker/Vagrant
- Negociación y compromiso: cada micro servicio debe mantener sus contratos con otros micro servicios que los usan (no podemos cambiar cosas a la ligera).
- Formación: el equipo de desarrollo debe estar muy bien formado.
- Unión de datos: los JOIN debemos hacerlos a mano
- ¿Quién es el responsable de controlar la autenticación y autorización?



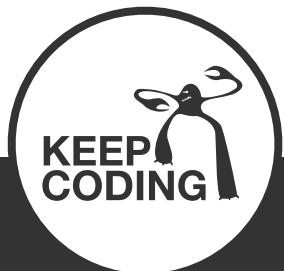
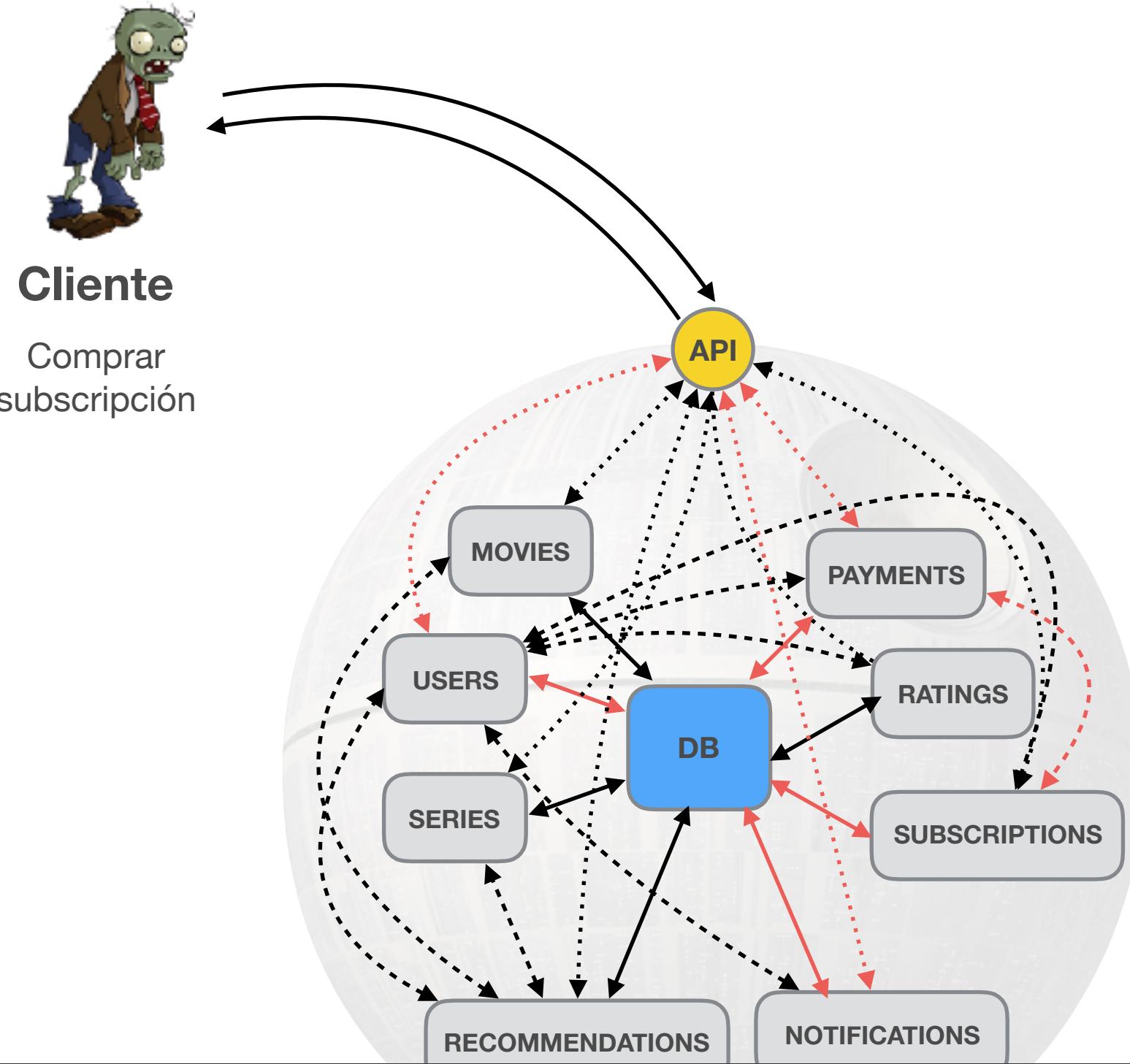
■ Del monolito a microservicios



■ Del monolito a microservicios

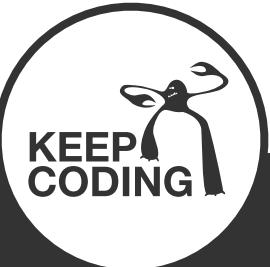
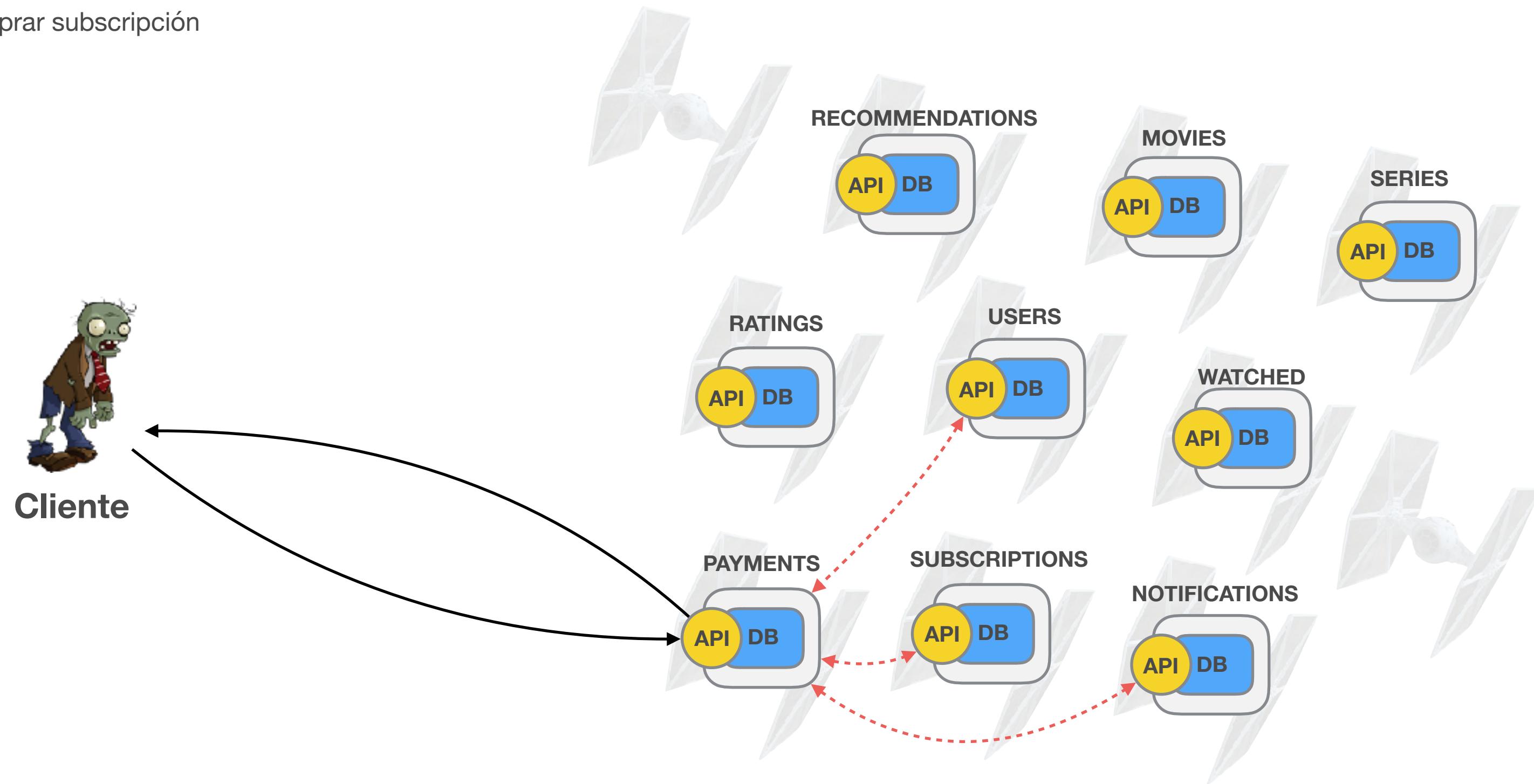


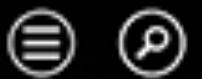
■ Cliente-Servidor con monolito



Conexión directa a microservicios

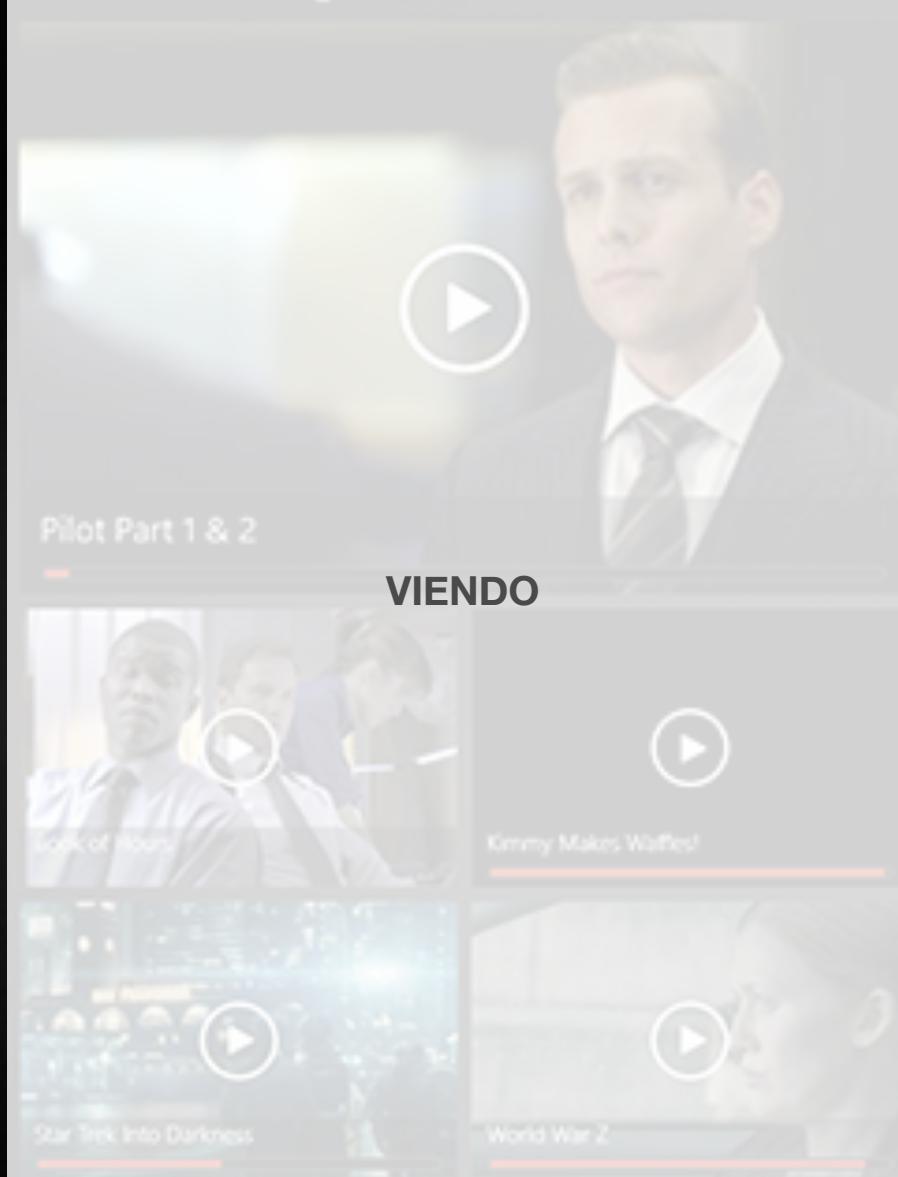
Acción: Comprar subscripción



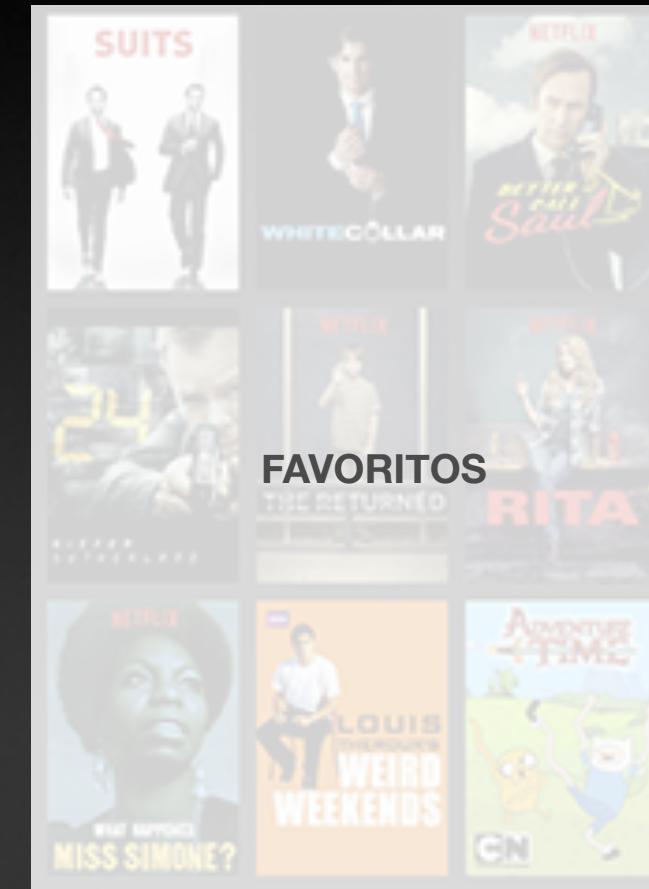


Helen

Continue Watching



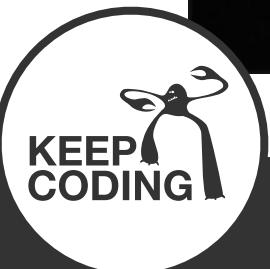
My List



Top Picks for Helen

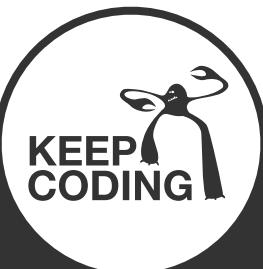
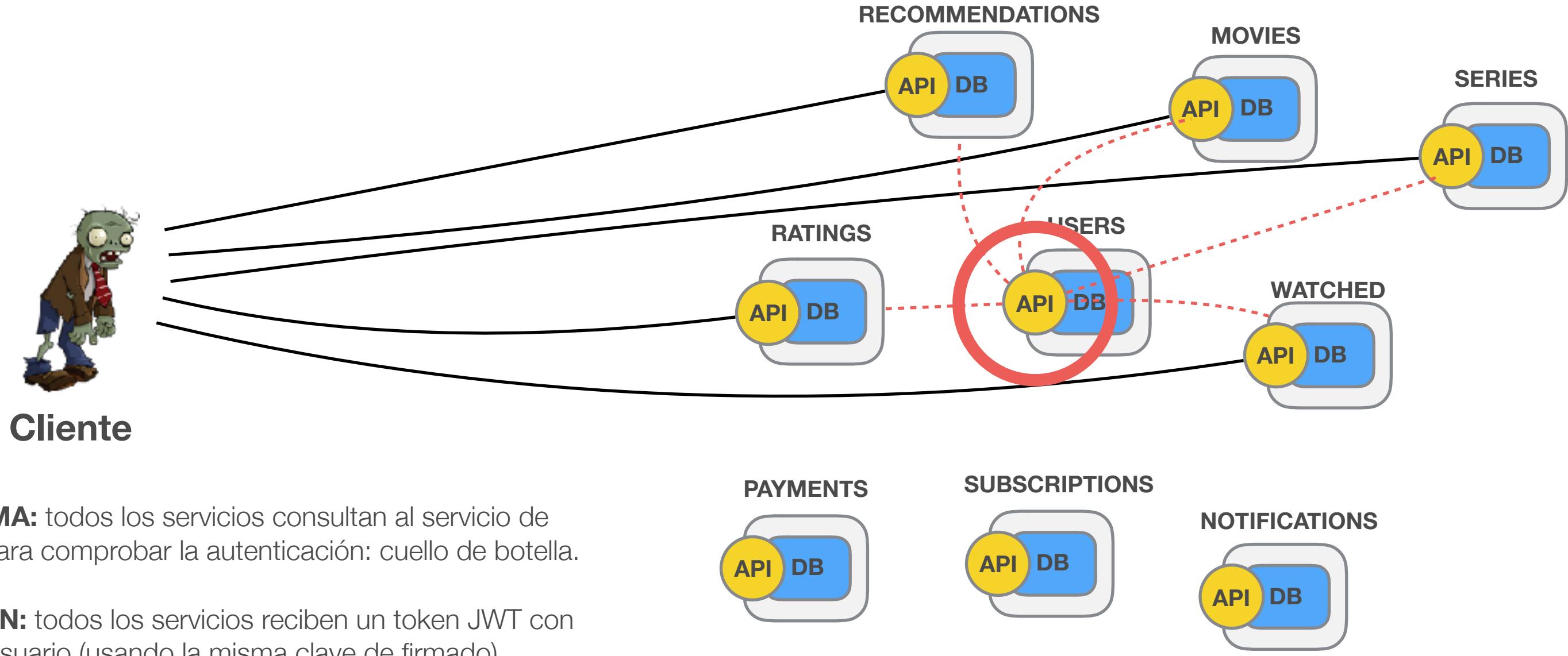


Popular on Netflix



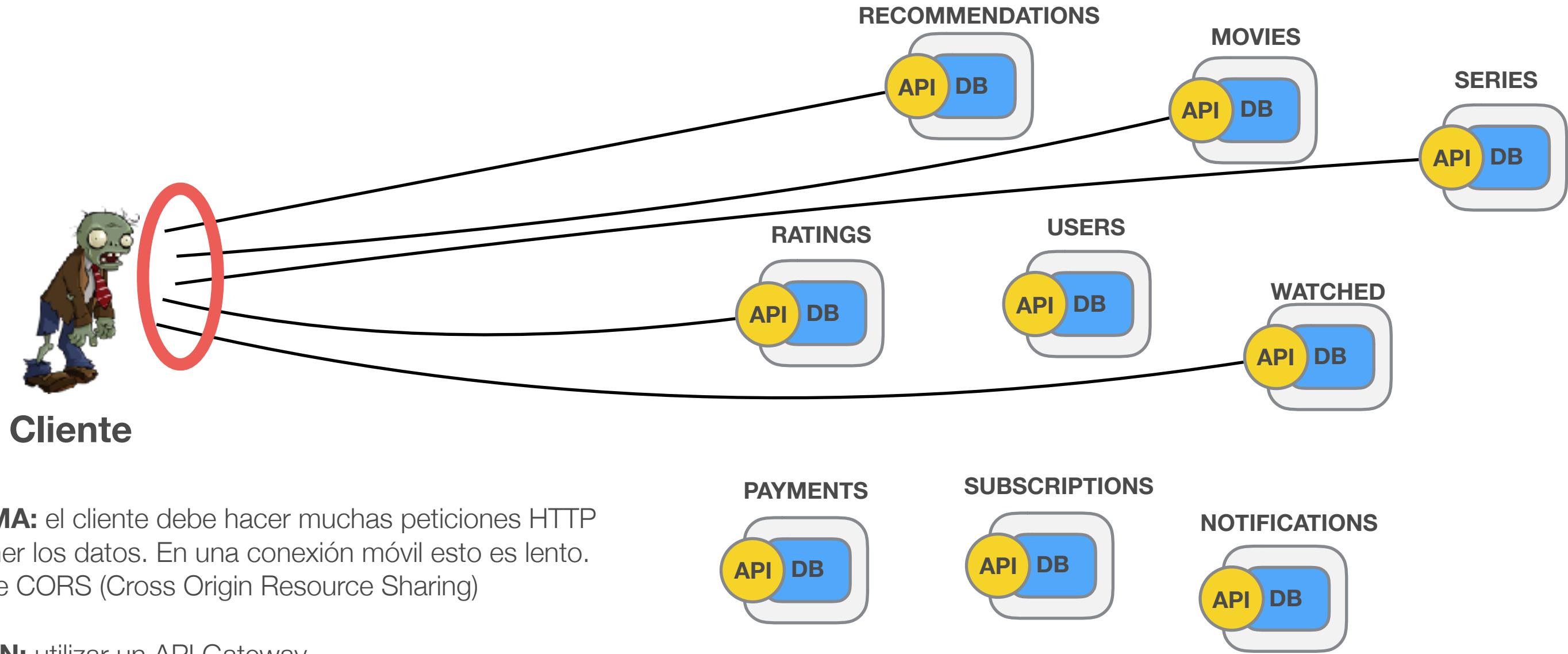
Conexión directa a microservicios

Acción: Recuperar datos para la página principal



Conexión directa a microservicios con JWT

Acción: Recuperar datos para la página principal



Conexión a API Gateway

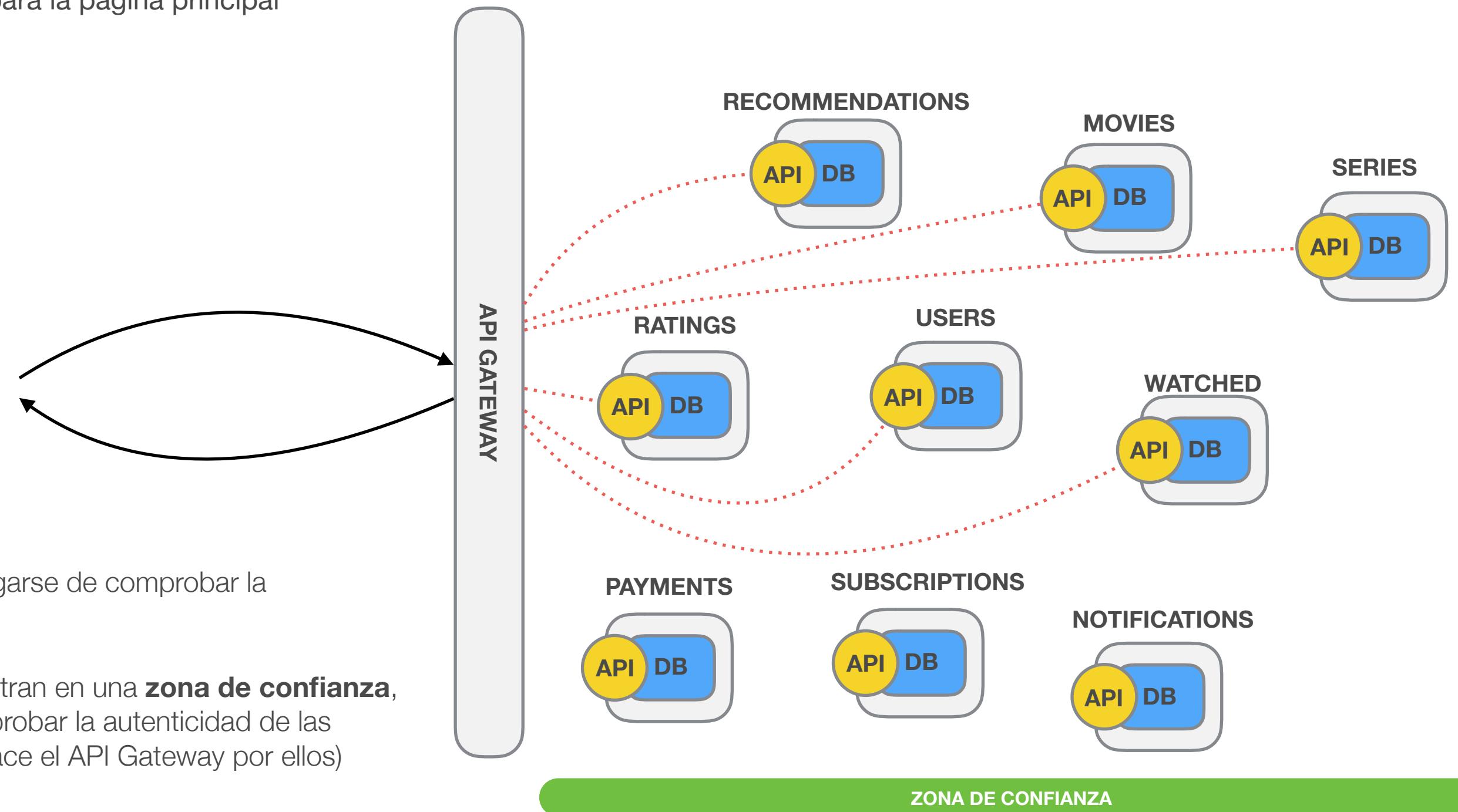
Acción: Recuperar datos para la página principal



Cliente

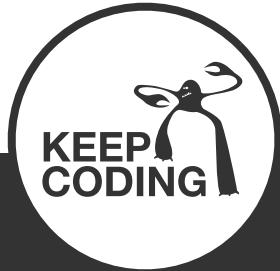
El **API Gateway** puede encargarse de comprobar la autenticación y autorización.

Los servicios tras él se encuentran en una **zona de confianza**, por lo que no tienen que comprobar la autenticidad de las peticiones (ese trabajo ya lo hace el API Gateway por ellos)



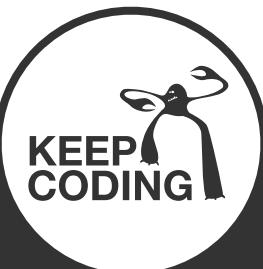
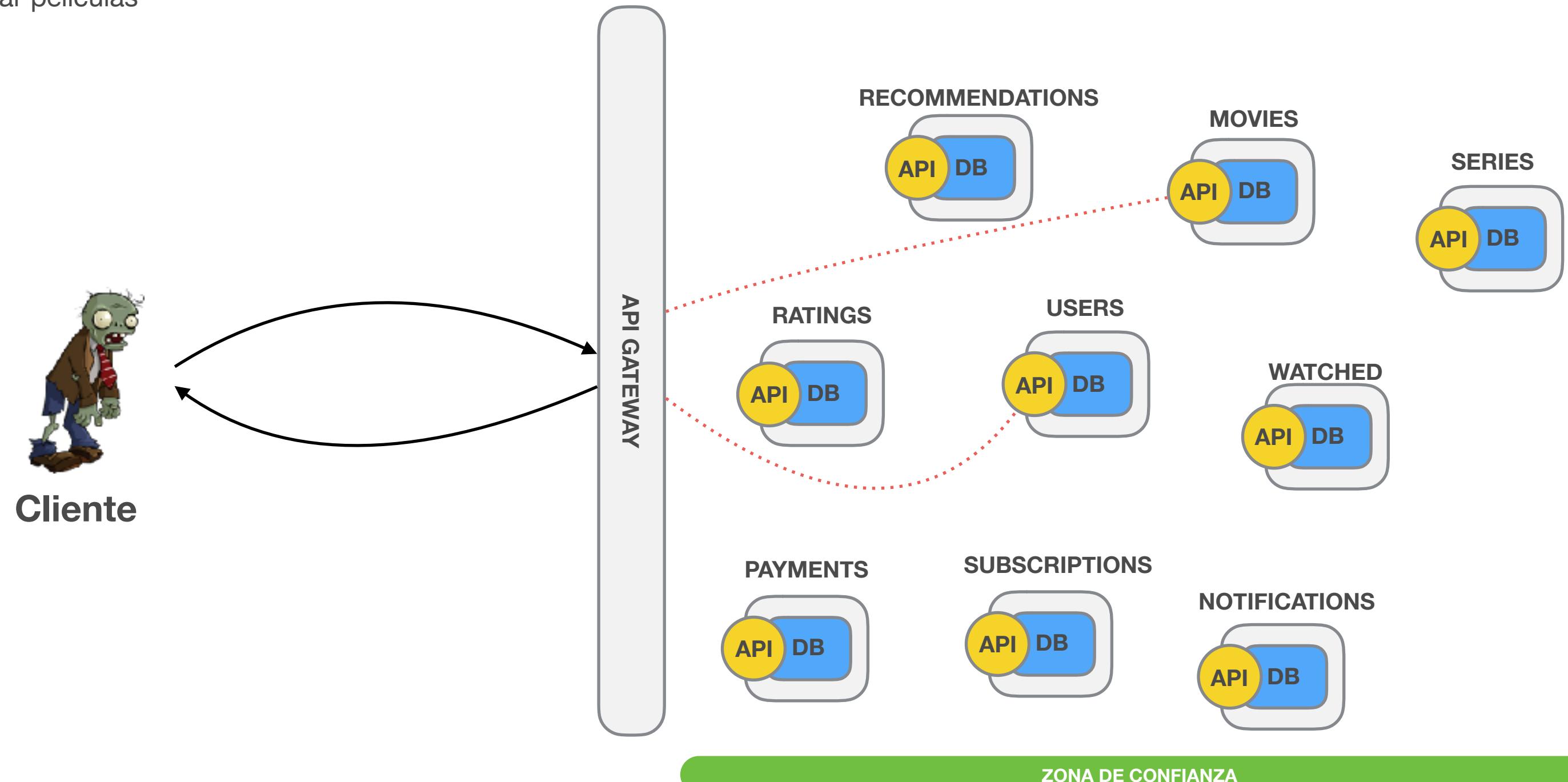
■ API Gateway

- Permite ser el único punto de entrada al sistema
- Comprueba la autenticación y autorización de los usuarios
- Los servicios tras él se despreocupan de la autenticación y autorización
- Puede actuar como proxy/router: enrutando la petición al servicio y devolviendo la misma respuesta que el servicio
- O puede actuar como gestor: haciendo varias peticiones y mezclando el resultado



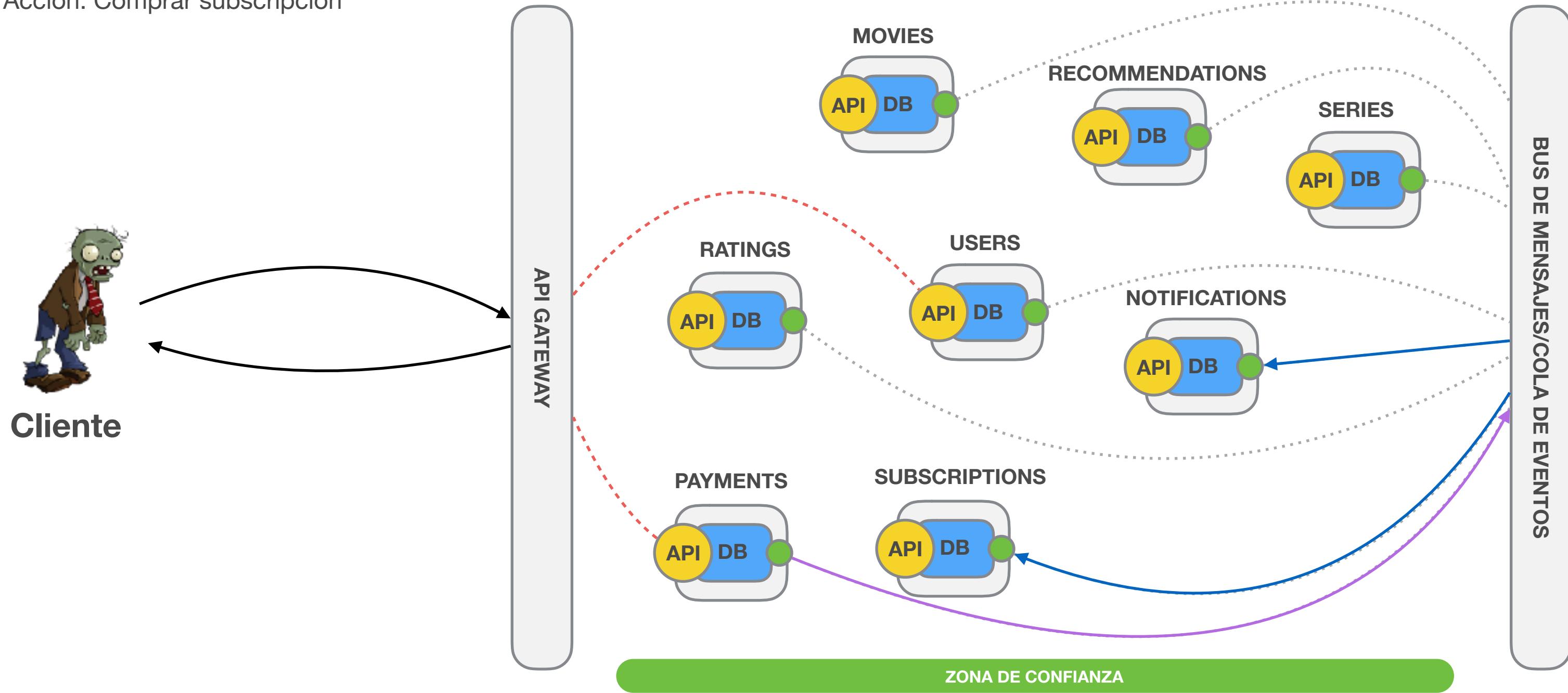
■ API Gateway como router/proxy

Acción: buscar películas

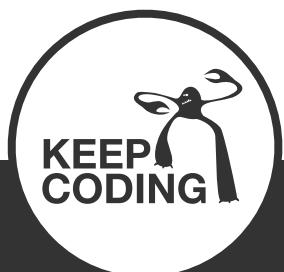


■ Arquitectura basada en eventos

Acción: Comprar subscripción

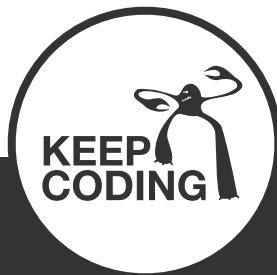


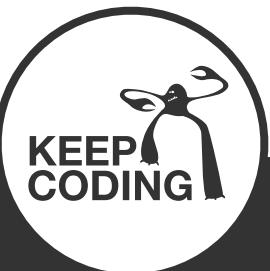
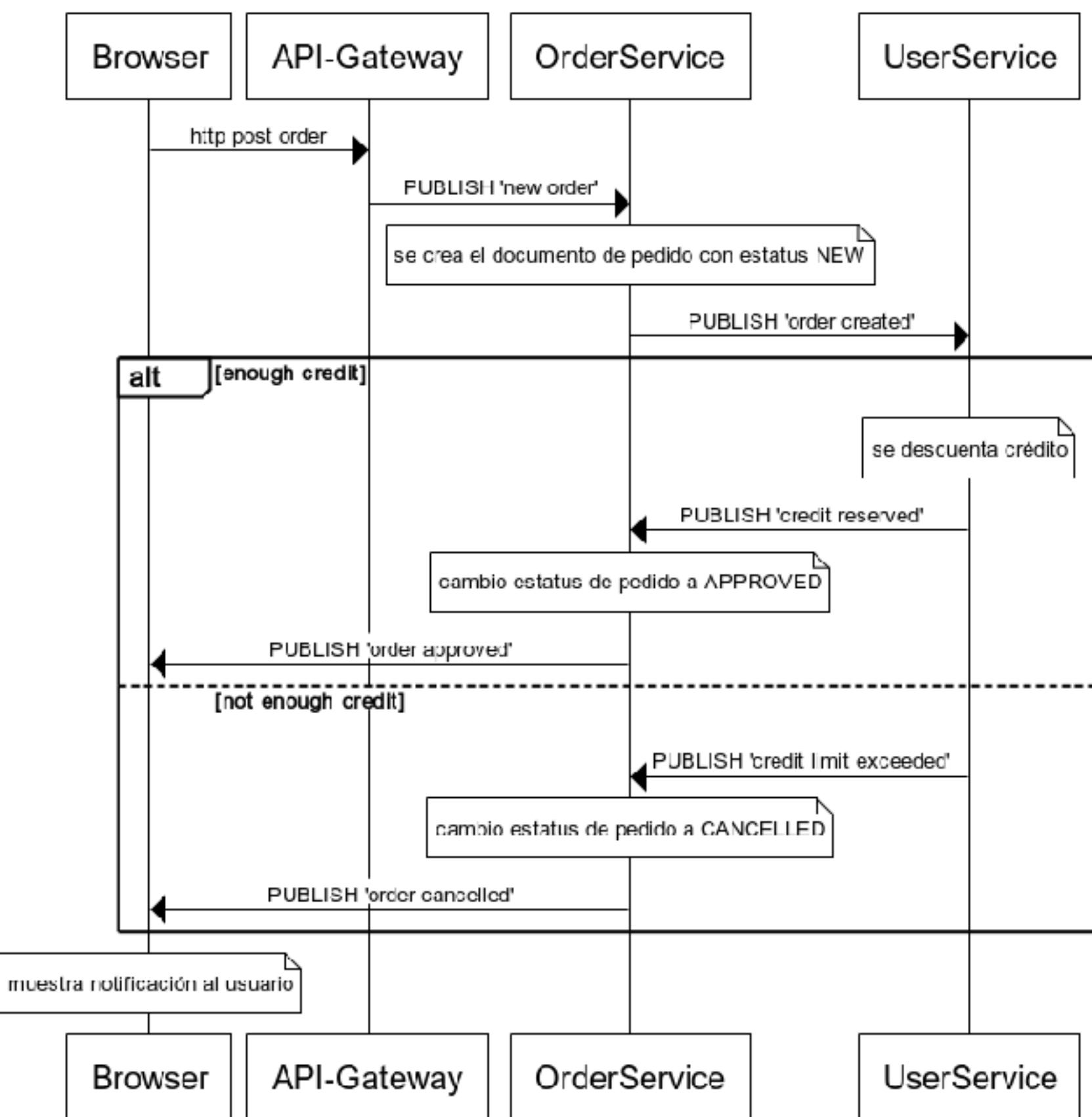
Gracias a la arquitectura basada en eventos podemos coordinar eventos sin tener que conectarlos síncronamente



■ Características de un microservicio

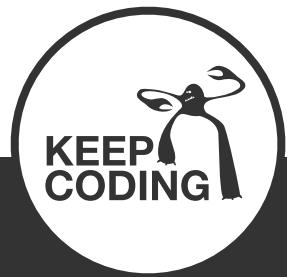
- Resolver un sólo problema y hacerlo muy bien
- Utilizar la mejor tecnología posible para resolver ese problema
- Exponer un API con endpoints para interactuar con él
- Base de datos propia (a ser posible, se aceptan BD compartidas)
- Conexión al bus de mensajes/cola de eventos (si es necesario)
- Librería cliente del API (a ser posible)





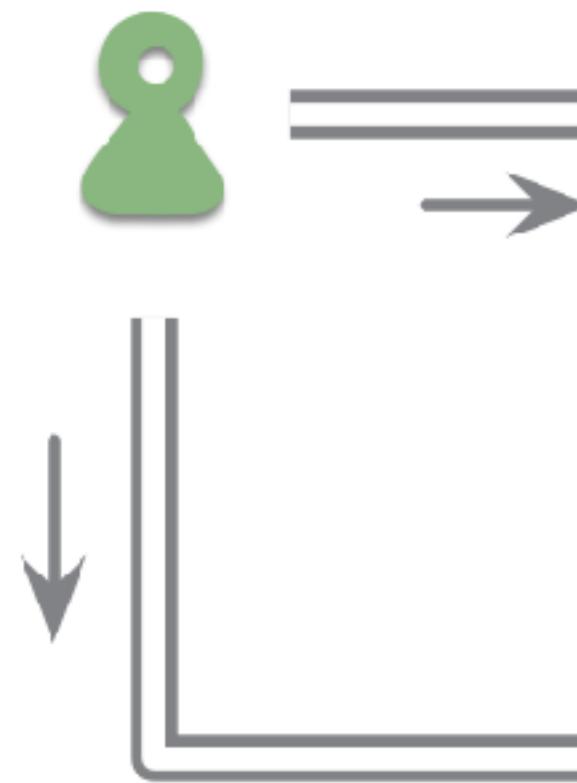


Monolith First

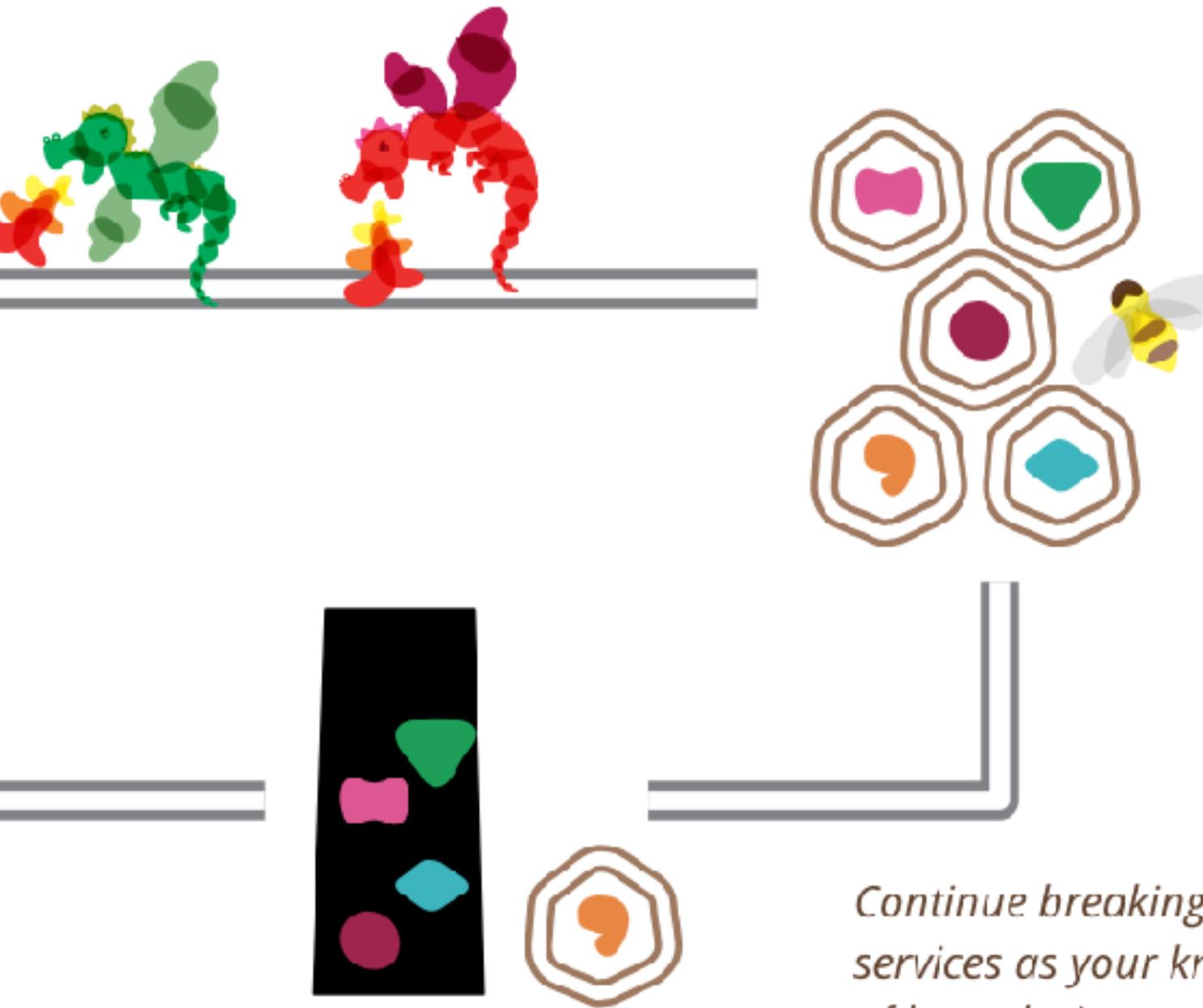




Going directly to a microservices architecture is risky



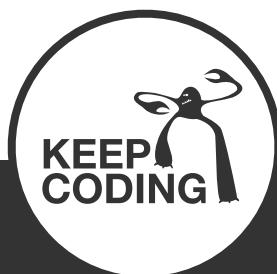
A monolith allows you to explore both the complexity of a system and its component boundaries



As complexity rises start breaking out some microservices

Continue breaking out services as your knowledge of boundaries and service management increases

<https://martinfowler.com/bliki/MonolithFirst.html>





■ Tipos de autenticación HTTP

Sesión, API Key, Tokens (JWT)



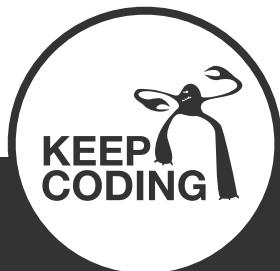
■ Autenticación HTTP

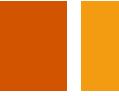
El protocolo HTTP es un protocolo sin estado: cada petición del navegador a un servidor es independiente de las anteriores.

Sin embargo en las aplicaciones web a veces necesitamos mantener el estado para poder relacionar peticiones.

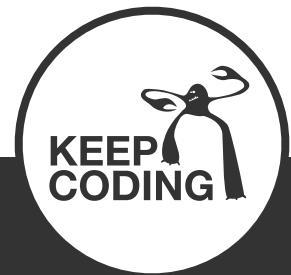
Ejemplo:

- Petición 1: el usuario añade un producto al carrito de compra
- Petición 2: el usuario va a pagar en el proceso de checkout





Sesión

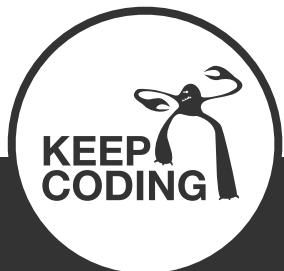


■ Autenticación por sesión

La autenticación por sesión se basa en el uso de **cookies**.

Las cookies son **bloques de información** enviados en las cabeceras HTTP en las respuestas de los servidores a los navegadores.

Los **navegadores** almacenan estos bloques de información y los **envían automáticamente a los servidores** en las siguientes peticiones.



■ Autenticación por sesión

Cliente

Servidor

Base de datos

POST /add/product/to/cart/

{ id: SESSION_A, cart_products: [...] }

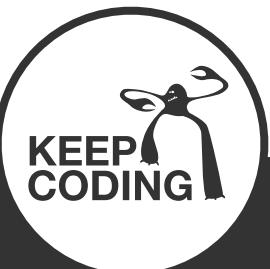
Set-Cookie: sessionid=SESSION_A

GET /products/in/cart/
Cookie: sessionid=SESSION_A

{ id: SESSION_A } ???

Set-Cookie: sessionid=SESSION_A

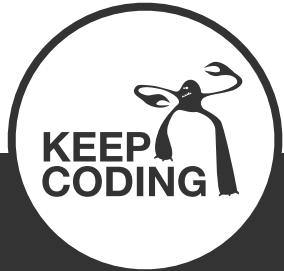
{ id: SESSION_A, cart_products: [...] }



Anatomía de una cookie

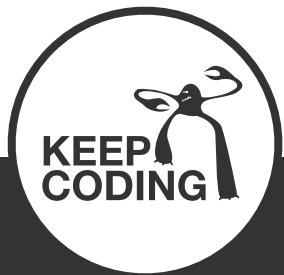
Las cookies están compuestas por los siguientes elementos:

- **domain:** dominio del servidor que ha puesto la cookie
- **path:** ruta opcional de la página que ha puesto la cookie. Si existe, sólo se enviará la cookie de vuelta a esa ruta.
- **expires:** fecha de expiración de la cookie
- **secure:** flag opcional para indicar que la cookie sólo se enviará por protocolo HTTPS
- **httpOnly:** flag opcional que indica que solo la puede leer el servidor
- **value:** separados por ; pueden tener nombre.



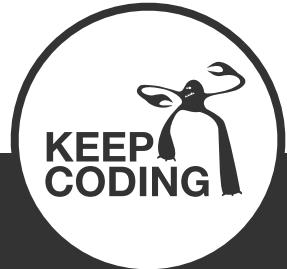
Anatomía de una cookie

```
Set-Cookie: name=darth; role=admin;  
domain=deathstar.com; path=/home; secure;  
expires=Tue, 29 Jan 1985 01:02:03 GMT+2
```



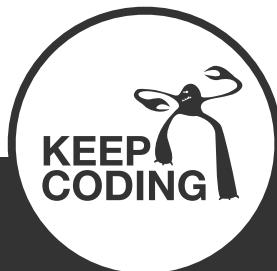


API Key



■ Autenticación por API Key

- La autenticación con API Key se basa en enviar en todas las peticiones un API Key (como cabecera o parámetro GET)
- Éste API Key suele ser suministrada por el servicio tras el registro de usuario.
- El API Key es único e identifica al usuario de manera única.
- El API Key siempre es la misma, no cambia ni hay que renovarla.



■ Autenticación por API Key

Cliente

Servidor

Base de datos

GET /some/list/

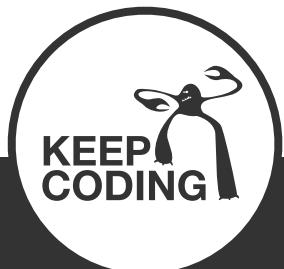
Authorization: ApiKey <API_KEY>



{ api_key: <API_KEY> } ???

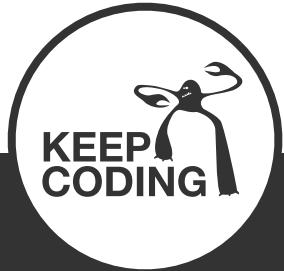


{ user: darth, role: admin }



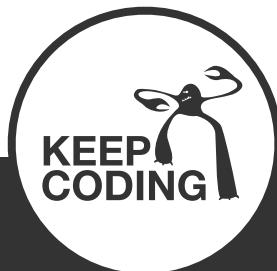


Tokens (y JWT)

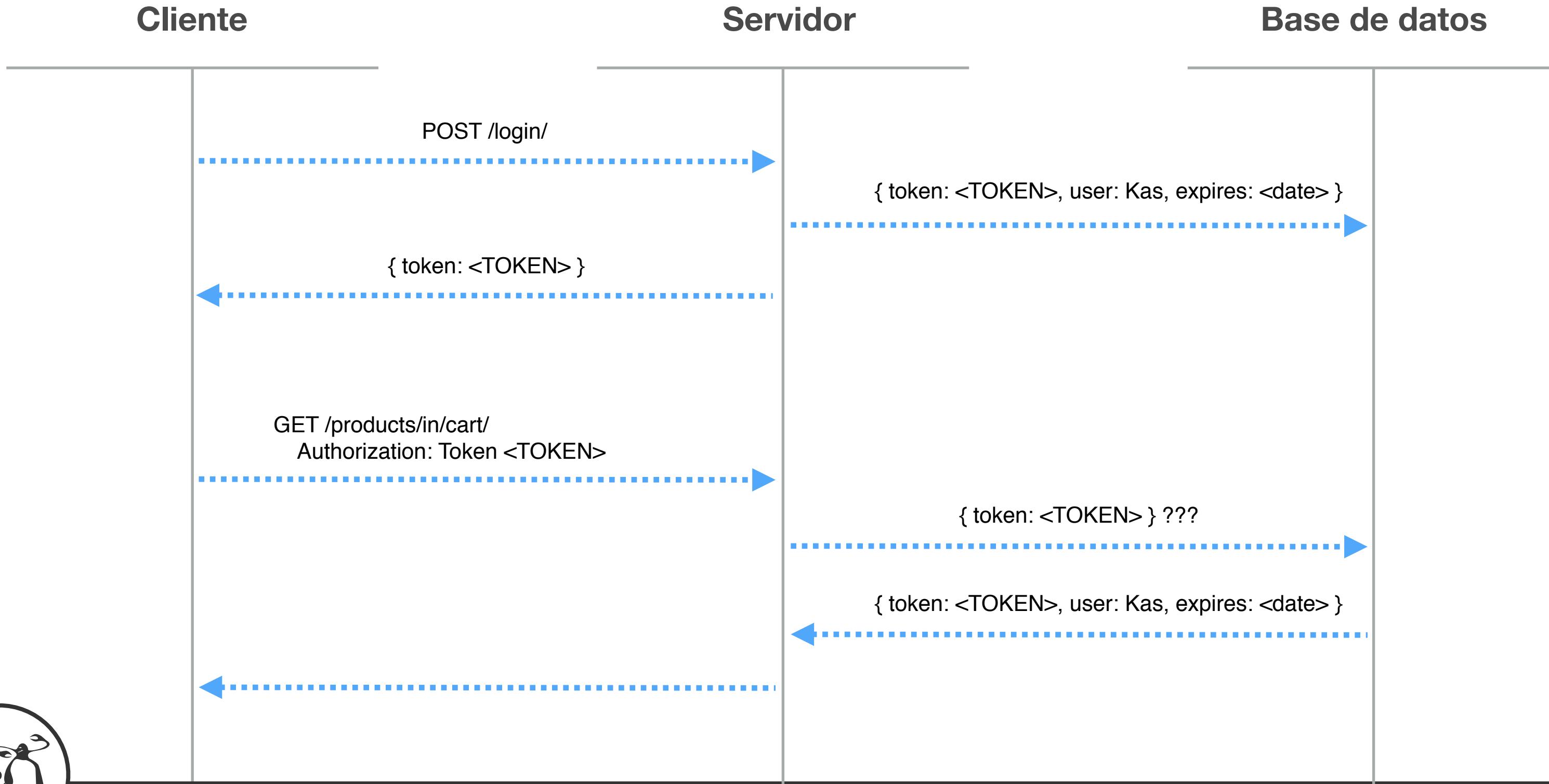


■ Autenticación por Token

- La autenticación por token es similar a la de API Key, salvo porque hay que gestionar el token, el cual es cambiante.
- Primero se debe autenticar el usuario para obtener un token.
- Ese token se debe enviar en cada petición pero también renovarse/actualizarse periódicamente (cada X minutos)

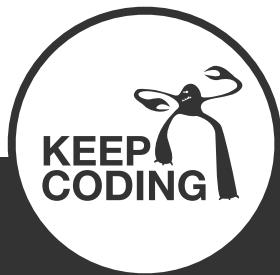


■ Autenticación por token

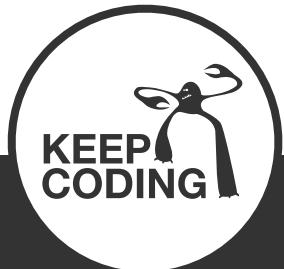
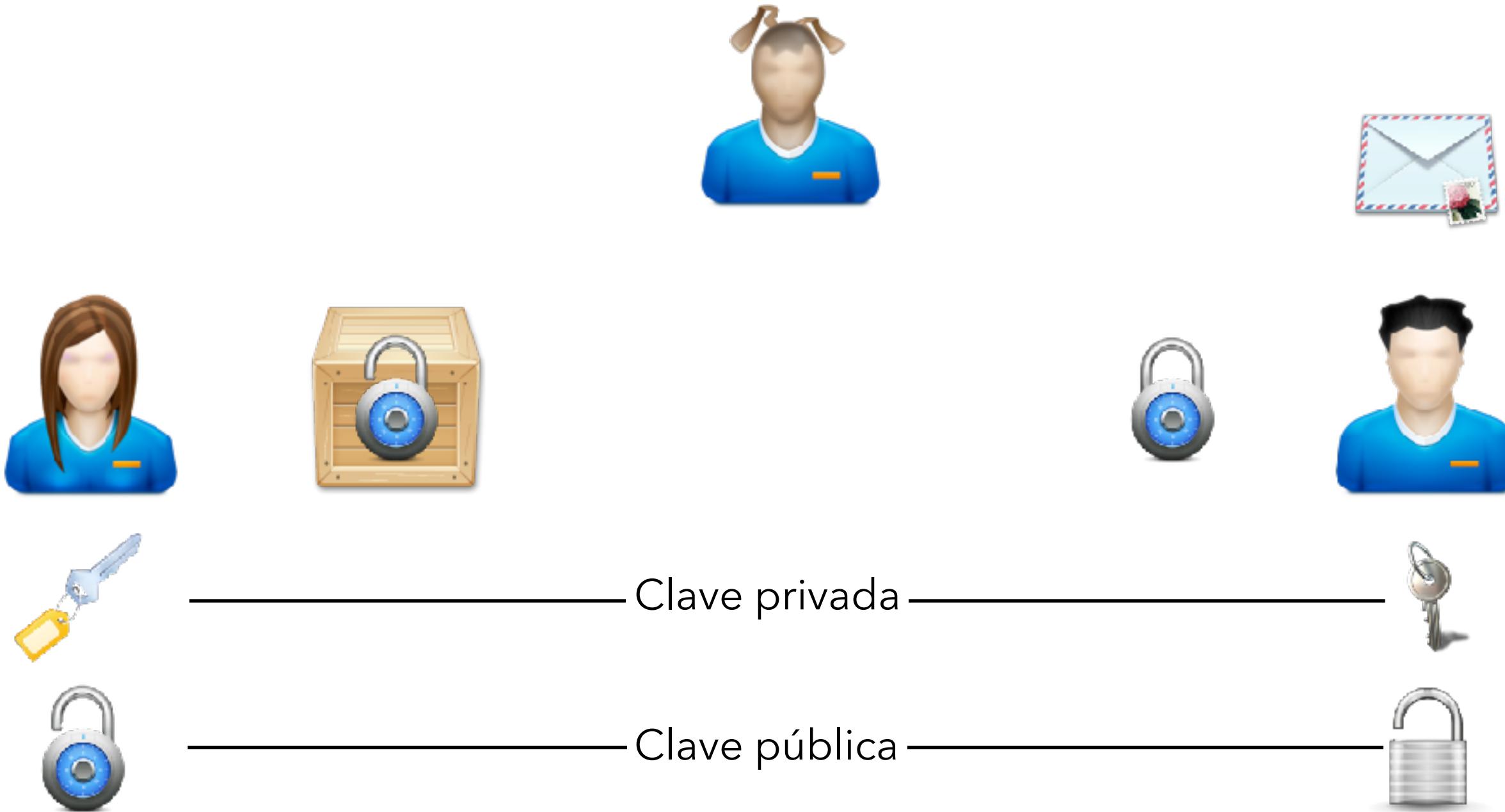


■ JWT (JSON Web Tokens)

- JWT es un estándar abierto ([RFC 7519](#))
- Define una forma segura y compacta de transmitir información entre diferentes partes con un objeto JSON
- La información puede ser verificada porque va firmada digitalmente
- Se pueden firmar los tokens con HMAC (algoritmo secreto) o con un par de claves RSA (pública/privada)



Cifrado asimétrico

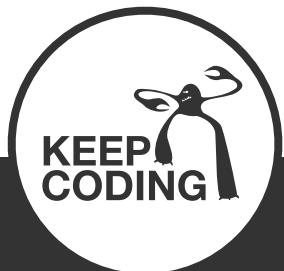


Estructura de un JWT

Un JWT está formado por tres partes:

- Cabecera: JSON en formato base64 que indica el tipo de token y el algoritmo usado para firmarlo
- Payload: JSON de datos en formato base64. Contiene los claims (claves del diccionario de datos).
- Firma: firma del token resultante de aplicar la siguiente fórmula:

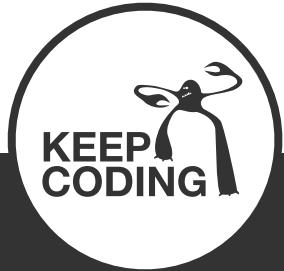
HMACRSA256(base64(header) + base64(payload) + <secret>)



Ejemplo

eyJhbGciOiJIUzI1NilsInR5cCl6IkpxVCJ9.eyJ1c2VybmFtZSI6IkRhcnRoliwiX2IkIjoiczZzZDZzZHV5ZHM2N3NkNmRzIwicm9sZSI6ImFkbWluliwiaWF0IjoxNTA4MDAwNTUxfQ.FfEP4sl3Q-Ggp_HPJaCofpBSO6c6w9_MKtYuecWkvqA

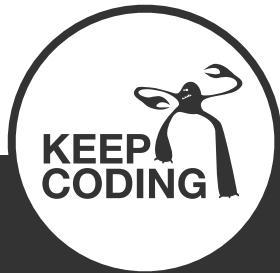
cabecera.payload.firma



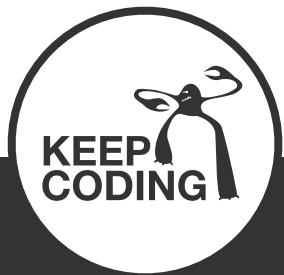
KEEP
CODING

■ ¿Por qué usar JWT?

- Evitamos guardar la información del usuario en la base de datos.
- Es el usuario quien nos envía su información en todo momento.
- Es seguro, porque podemos validar que el token no ha sido alterado desde que nosotros lo enviamos.

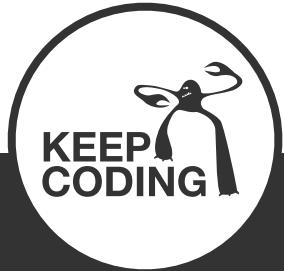


■ Autenticación por JWT





HTTP Basic Auth

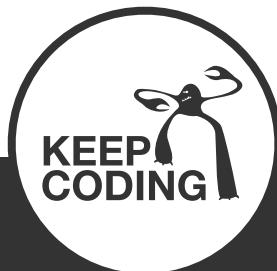


■ Autenticación - basic auth

Basic HTTP Auth es un mecanismo sencillo y muy usado en APIs.

```
npm install --save basic-auth
```

Implementaríamos un middleware que comprobara las credenciales.



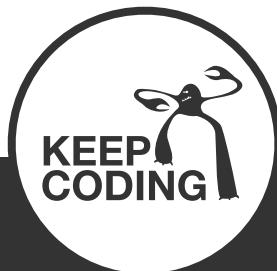
■ Autenticación - basic auth

Ventajas:

- Lo soportan todos los navegadores
- Una persona puede realizar la autenticación manualmente de forma sencilla, por ejemplo para explorar el API

Desventajas:

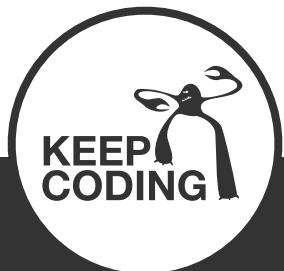
- Hay métodos más seguros



■ Autenticación - basic auth

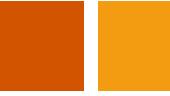
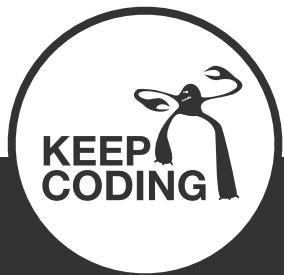
```
npm install --save basic-auth
```

```
router.use(function(req, res, next) {
  var user = basicAuth(req);
  if (!user || user.name !== 'user' || user.pass !== 'pass') {
    res.set('WWW-Authenticate', 'Basic realm=Authorization
Required');
    return res.sendStatus(401);
  }
  next();
});
```



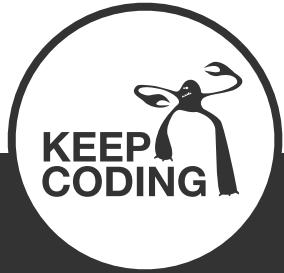


Buenas prácticas





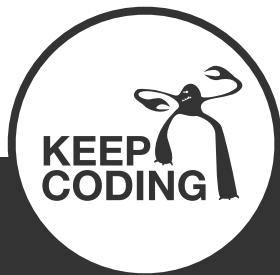
Node.js



Buenas prácticas - Node.js

Formato de los callbacks con el error siempre como primer parámetro.

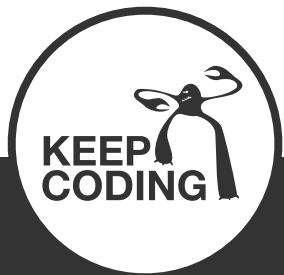
```
var resizeImage(imagePath, callBack) {  
  
    // hacer el procesado que queramos  
    var resizedImagePath = resizer(imagePath, ...);  
  
    // devolvemos en primer lugar error y luego los resultados  
    return callBack(null, resizedImagePath);  
}
```



Buenas prácticas - Node.js

Al recibir un callback, comprobar primero si ha habido error para devolverlo y luego hacer el proceso previsto.

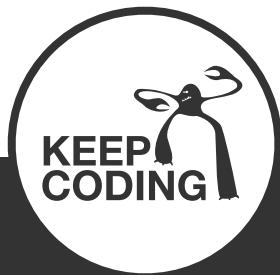
```
function getConfig(callBack) {  
  
    leeFichero('./config.json', function(err, fileContent) {  
        // primero comprobamos y retornamos posibles errores  
        if (err) {  
            return callBack(err);  
        }  
  
        return callBack(null, JSON.parse(fileContent));  
    });  
  
}
```



Buenas prácticas - Node.js

Usar return al invocar callbacks, reduce la posibilidad de errores por olvidar hacer return y llamar varias veces al callback de la función.

```
function saveUpload(res, callBack) {
    leeFichero('./config.json', function(err, fileContent) {
        if (err) {
            callBack(err);
            // aquí deberíamos parar! --> RETURN
            // para no olvidarlo y mejorar la legibilidad usar return callBack(err);
        }
        callBack(null, JSON.parse(fileContent));
        // aquí mejor return callBack(null, JSON...
    });
}
```

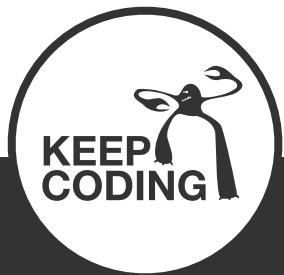


Buenas prácticas - Node.js

En los try/catch usar **solo código síncrono dentro del bloque try**.

```
// Parsear JSON
try {
  object = JSON.parse(data);
} catch (exception) {
  return callback(exception);
}

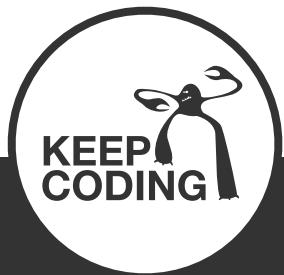
return callback(null, object);
```



Buenas prácticas - Node.js

Evitar cuando podamos el uso de `this` y `new`.

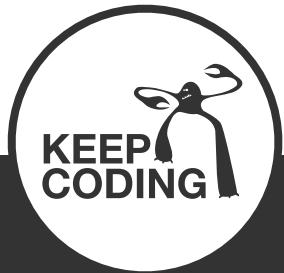
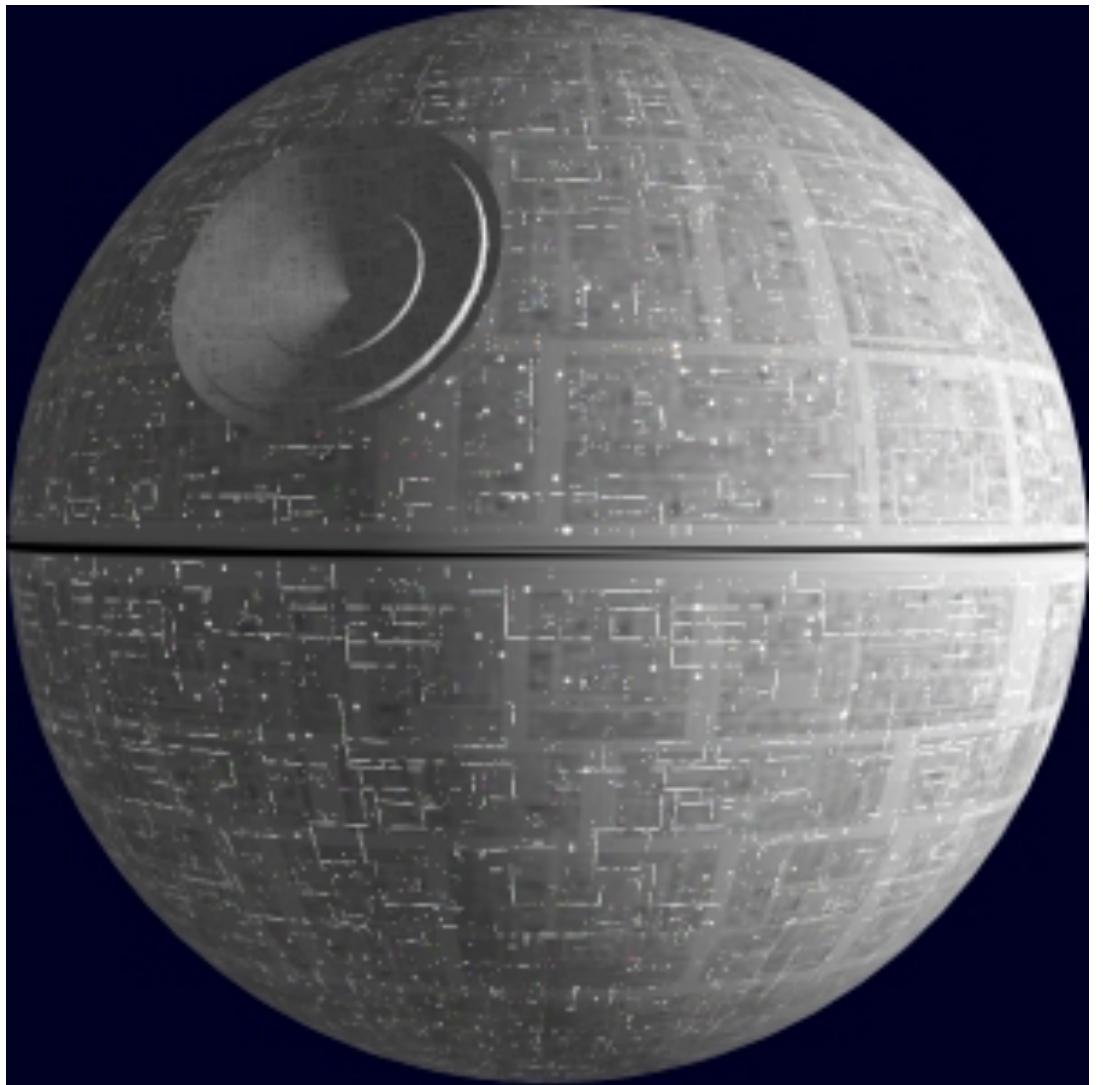
Normalmente usamos múltiples callbacks para gestionar el flujo de nuestro programa, esto puede hacer que fácilmente nos confundamos de scope.



Buenas prácticas - Node.js

Dividir la funcionalidad en varios módulos especializados, cada uno haciendo solo su trabajo y hacerlo bien.

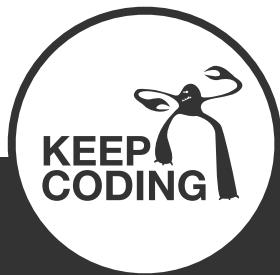
No construyamos estrellas de la muerte que hacen varias cosas, serán difíciles de mantener!



Buenas prácticas - Node.js

Gestionar lo mejor posible los errores:

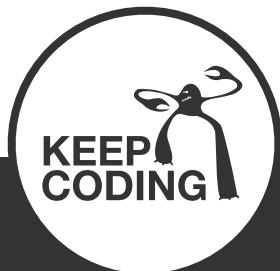
- Hay errores operacionales que se pueden reintentar (una petición a un API de terceros que dio timeout) y errores ante los cuales debemos parar la aplicación (no se pudo leer el fichero de configuración)
- Hagamos log de todo!



Buenas prácticas - Node.js

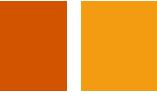
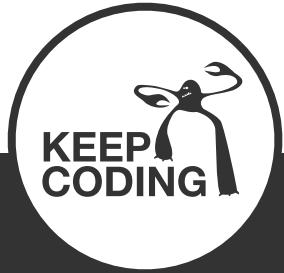
Y algunos consejos más...

- No llamar a una función asíncrona sin pasarle un callback
- Antes de usar propiedades de un objeto pensar si ese objeto puede no existir
- Usar npm init al iniciar una aplicación o un módulo nuevo
- Usar patrones reconocibles al procesar de forma asíncrona (p.e. async, promesas)
- Antes de crear un módulo nuevo mirar si ya existe en npm
- Usar ayudantes de estilo como JSCS, JSHint, etc
- Usar NODE_PATH=lib al arrancar nuestra aplicación o apuntar nuestras librerías en el package.json para resolver fácilmente sus rutas
- Documentar las partes de nuestra aplicación con jsdoc o similar
- No poner datos sensibles en el código, usemos ficheros de configuración o variables de entorno





APIs

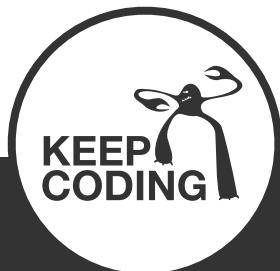


Buenas prácticas en APIs - desacoplamiento

Nuestro API, aunque lo construyamos inicialmente para un software cliente concreto, debería estar diseñado para que otros tipos de clientes puedan consumirlo.

Por ejemplo GET /homeltems

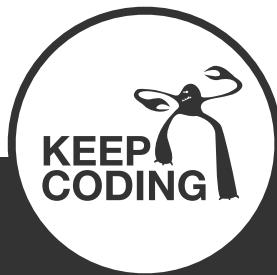
Estaría mejor como **/offers** al margen de si en una aplicación aparecen en la home o no.



Buenas prácticas en APIs - versionado

Pongamos versión a nuestro API desde el principio.

Cuando tengamos clientes consumiéndola y tengamos que cambiarla tendremos que hacer una nueva versión.

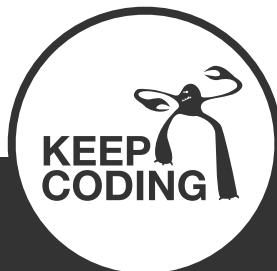


Buenas prácticas en APIs - versionado

Podemos versionar de múltiples formas, las dos más usadas son:

1. Versión en la ruta base /apiV1/users o api/V1/users
2. Versión en la cabecera. El cliente pone la versión que quiere consumir en el header.

La **opción 1** es más visible y por tanto más segura.

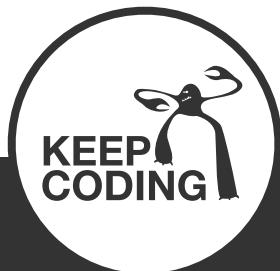


Buenas prácticas en APIs - nombres

Hacer un API rest implica exponer recursos que son invocados con GET, POST, PUT, etc.

Los recursos deberían ser nombres, no verbos.

GET /users	(mejor que GET /getUserList)
POST /users	(mejor que POST /insertUser)



Buenas prácticas en APIs - nombres

GET /users - Devuelve lista de usuarios

GET /users/12 - Devuelve un usuario concreto

POST /users - Crea un usuario

PUT /users/12 - Actualiza usuario #12

PATCH /users/12 - Actualiza parcialmente el usuario #12

DELETE /users/12 - Elimina usuario #12

Solo tenemos que acordarnos del nombre del recurso (users) y la lista de métodos ya nos la sabemos!



Buenas prácticas en APIs - nombres

Singular o plural?

- GET /user
- GET /users

Decisión nuestra, pero usémoslo igual para todos los recursos.

El plural es comúnmente más usado.



Buenas prácticas en APIs - nombres

¿Como hacemos con las relaciones?

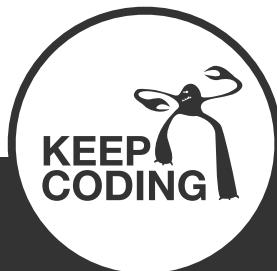
GET /users/12/emails - Devuelve lista de emails de usuario

GET /users/12/emails/7 - Devuelve un email concreto

POST /users/12/emails - Crea un email al usuario

PUT /users/12/emails/7 - Actualiza email #7 del usuario

...



Buenas prácticas en APIs - nombres

¿Como hacemos con las acciones distintas a GET, POST, etc?

Si la acción podemos usarla como un campo: PATCH /users/5/active

O podemos usarlo como un sub-recurso. Por ejemplo como hace github PUT /gists/:id/star pone una estrella y DELETE /gists/:id/star la quita.

A veces lo que queremos hacer no encaja con nada o implica múltiples recursos como por ejemplo una búsqueda sobre mensajes, usuarios y teléfonos, para estos casos /search tendrá mucho sentido!

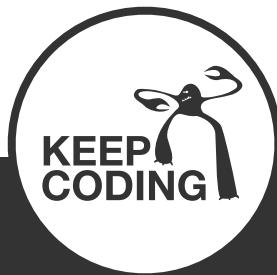


Buenas prácticas en APIs - browser explorability

Facilitar las cosas al consumidor de nuestro API es bueno para que le guste y lo maneja bien.

Tratemos de que la lectura de todos los recursos sea posible desde un navegador.

Por ejemplo, usando el versionado en la ruta, haciendo un índice de los recursos con URLs clickables.



Buenas prácticas en APIs - documentación

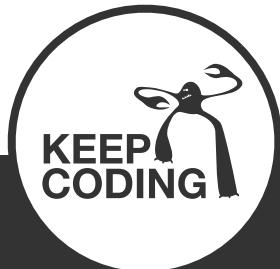
Podemos usar herramientas como apidoc, iodocs o swagger para ayudarnos.

Un par de ejemplos de con iodocs:

- <https://developers.egnyte.com/io-docs>
- <http://developer.klout.com/io-docs>

Ejemplos de documentación de otras APIs:

- <https://swapi.co/documentation>

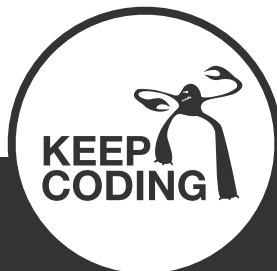


Buenas prácticas en APIs - errores

Un buen API debe devolver errores en un formato estandarizado o previsible.

Los errores de cliente (tipo 400) deberían devolver un objeto JSON con propiedades similares en los distintos casos.

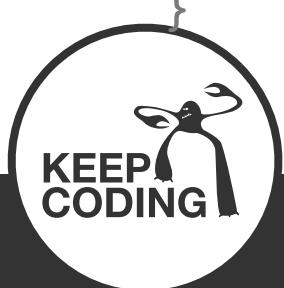
Los errores de servidor (tipo 500) no podrán hacerlo en todos los casos (un balanceador caído es difícil que devuelva JSON), pero al menos los que estén en nuestra mano deberían hacerlo.



Buenas prácticas en APIs - errores

Para los errores de validación donde están involucrados multiples campos pueden devolver algo como:

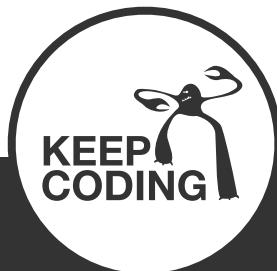
```
{  
  "code" : 1024,  
  "message" : "Validation Failed",  
  "errors" : [  
    {  
      "code" : 5432,  
      "field" : "first_name",  
      "message" : "First name cannot have fancy characters"  
    },  
    {  
      "code" : 5622,  
      "field" : "password",  
      "message" : "Password cannot be blank"  
    }  
  ]  
}
```



Buenas prácticas en APIs - cambios

Cuando un cliente solicita un cambio en un recurso (con PUT o PATCH) es bastante común que luego tenga que hacer un GET para recuperar los datos guardados y mostrarlos.

Muchos APIs facilitan esto devolviendo siempre una representación del objeto modificado.



Buenas prácticas en APIs - filtros, paginación, etc

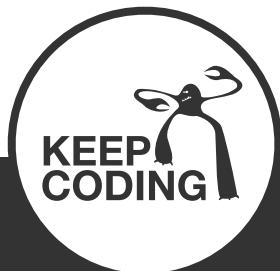
Usemos la query-string. Por ejemplo:

Para filtros GET /messages?state=sent&archived=false

Para ordenación GET /messages?sort=-priority,created_at

Para paginación GET /users?skip=30&limit=10&returnTotal=true

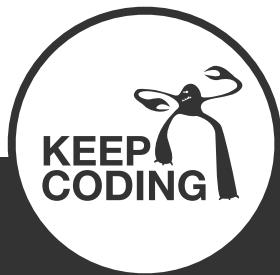
Para búsquedas GET /messages?q=frr149&sort=created_at



Buenas prácticas en APIs - alias

Para consultas típicas a nuestro API, quien lo consuma agradecerá que le hagamos alias.

`GET /messages/recently_sent`

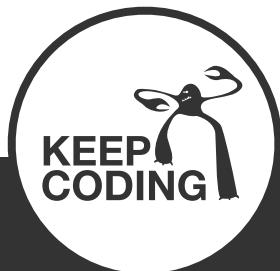


Buenas prácticas en APIs - reducción de campos

Es muy útil permitir al consumidor que elija si quiere menos o más campos de los que devuelve el recurso por defecto.

```
GET /messages?fields=id,subject,send_date,updated_at&state=sent&sort=-updated_at
```

Algunos usan una cabecera como por ejemplo x-extended o similar para obtener todos los campos disponibles. Cuando no se especifica esta cabecera se devolverían los campos de mayor uso.

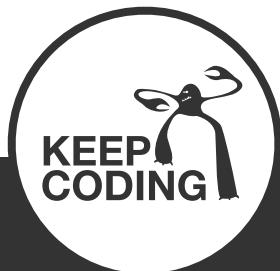


Buenas prácticas en APIs - HATEOAS o no?

Hypermedia As The Engine Of Application State

Consiste en que nuestro API devuelva links a recursos o acciones que se pueden hacer con los recursos.

```
{  
  "content": [ {  
    "price": 499.00,  
    "description": "Apple tablet device",  
    "name": "iPad",  
    "links": [ {  
      "rel": "self",  
      "href": "http://localhost:8080/product/1"  
    } ],  
    "attributes": {  
      "connector": "socket"  
    }  
  }  
}
```

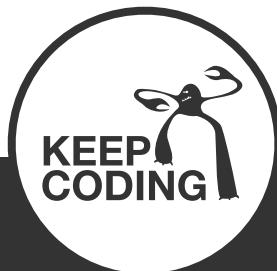


Buenas prácticas en APIs - timestamps

Permitir solicitar al API los elementos que hayan cambiado desde la última vez que los descargamos es muy bueno para que las apps usen el menor ancho de banda posible y la experiencia sea mejor.

Esto lo conseguimos devolviendo el timestamp actual en cada lista, e implementando un filtro opcional al que pasarle dicho timestamp para que el API nos de solo los elementos que hayan cambiado desde el momento del timestamp.

Los elementos que nos dará serán o nuevos (tendrán un ID que nosotros no tenemos), actualizados (los localizamos por el ID) o borrados (localizados por ID y llevarán una marca de 'DELETED' para que los borremos).



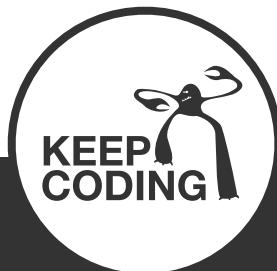
Buenas prácticas en APIs - method override

Hay clientes que solo pueden usar GET y POST por ejemplo.

Por tanto no podrán llamar a nuestros PUT, PATCH o DELETE.

Para solucionar esto habilitamos una cabecera llamada '*X-HTTP-Method-Override*' (por convención) con un string que contendrá uno de los métodos PUT, PATCH or DELETE.

Usemos esto solo para POST! (los métodos GET nunca deben hacer modificaciones!)

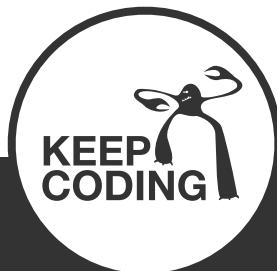


Buenas prácticas en APIs - rate limiting

Para evitar abusos del API se suele implementar algún sistema que controle e informe al consumidor sobre los límites de llamada al API.

Hay muchos módulos de terceros que nos darán estas habilidades, como por ejemplo:

- <https://github.com/jhurliman/node-rate-limiter>
- <https://github.com/ded/express-limiter>

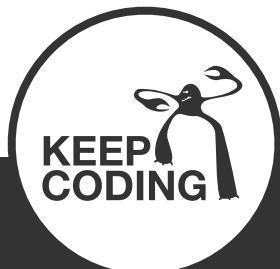


Buenas prácticas en APIs - CORS

Aunque los primeros clientes de nuestro API sean aplicaciones móviles nativas, es bastante posible que más adelante algún cliente web tenga que consumirlo. Para facilitarlo, habilitemos CORS en nuestro servicio.

http://enable-cors.org/server_expressjs.html

```
app.use(function(req, res, next) {  
  res.set("Access-Control-Allow-Origin", "*");  
  res.set("Access-Control-Allow-Methods", "GET, POST, PUT, DELETE");  
  res.set("Access-Control-Allow-Headers", "Origin, X-Requested-With,  
Content-Type, Accept");  
  next();  
});
```

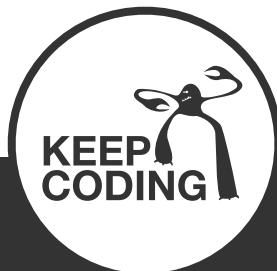


Buenas prácticas en APIs - HTTPS

HTTPS everywhere - all the time!

Nuestra API va a ser consultada desde wifis de aeropuertos, bares, bibliotecas, etc.

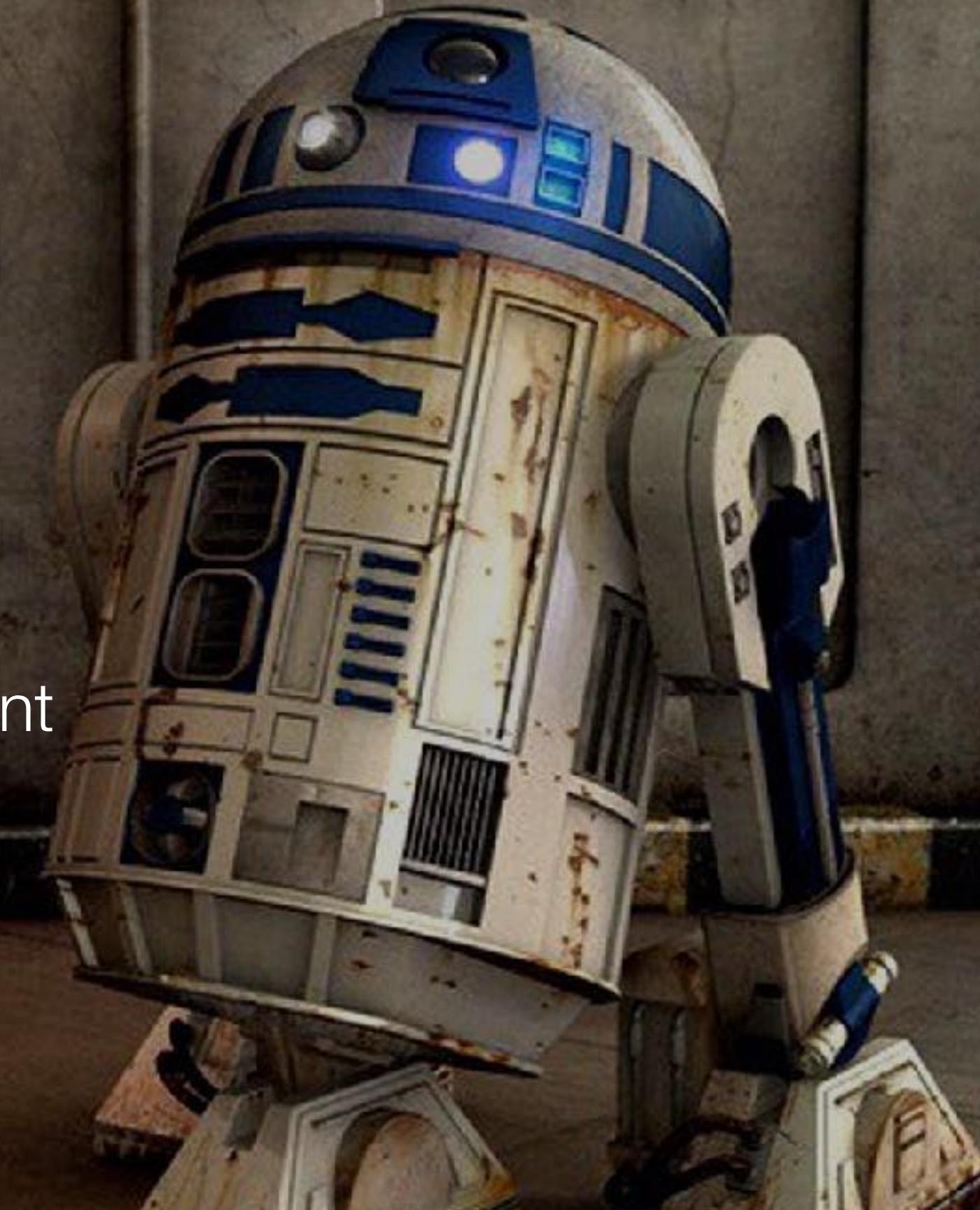
A veces se implementa que una petición HTTP redirige a la misma con HTTPS. No hagamos esto, en vez de eso devolvamos un error, hagamos saber claramente **que nuestra API no usa métodos inseguros**.





TDD

Test Driven Development

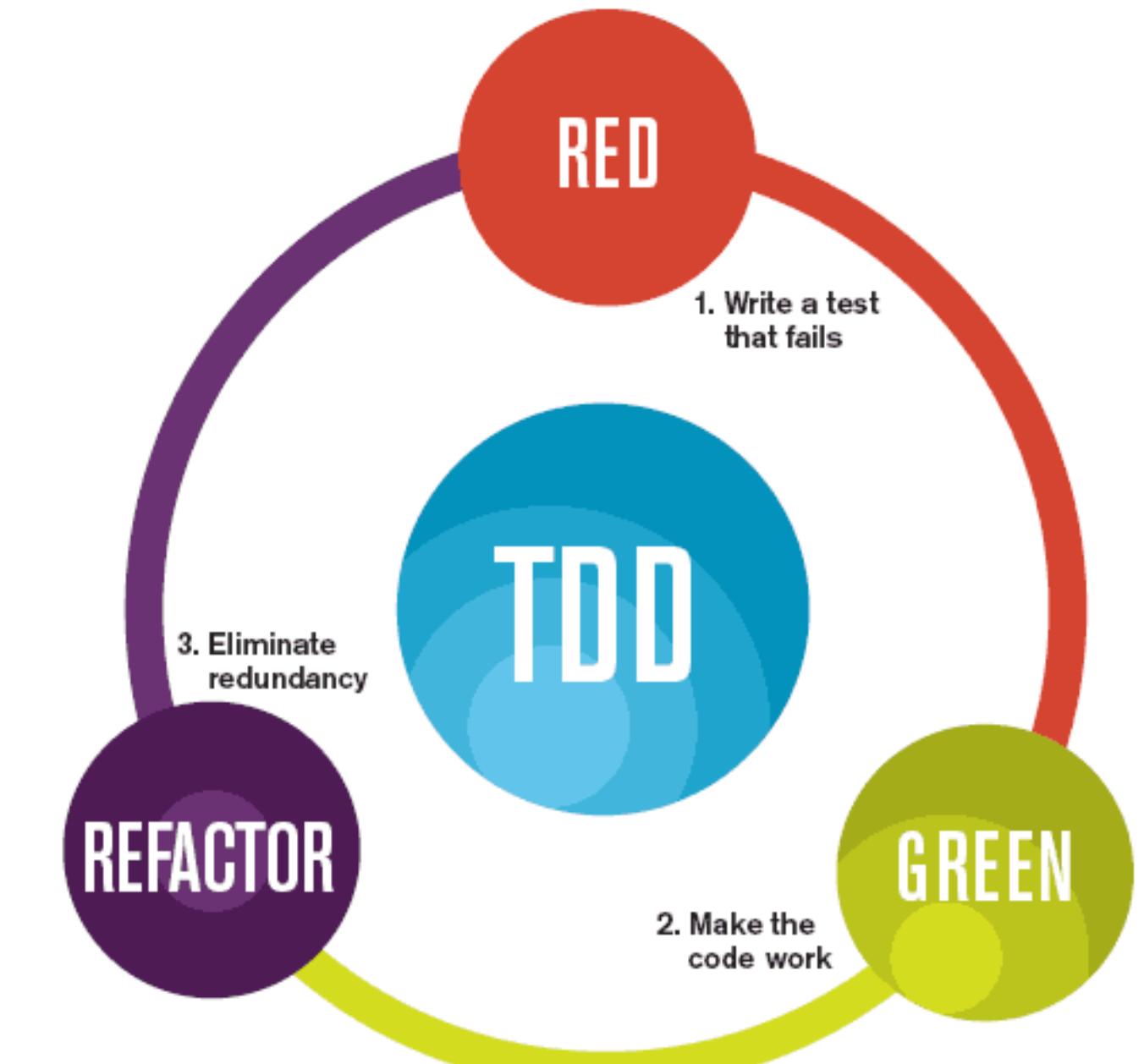


■ ¿Qué es TDD?

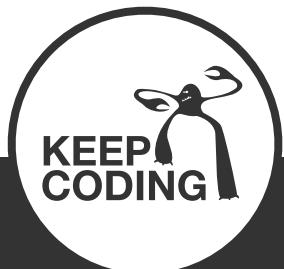
- Es un proceso de desarrollo de software. Una manera de desarrollar software.
- La base de TDD es escribir programas que prueban nuestro programa para que, cuando introduzcamos cambios, las pruebas estén automatizadas (y no tengamos que volver a ejecutar todas las pruebas manualmente).
- Al principio puede parecer que hace nuestro desarrollo más lento: no es así. A la larga, ahorras mucho tiempo (y disgustos).



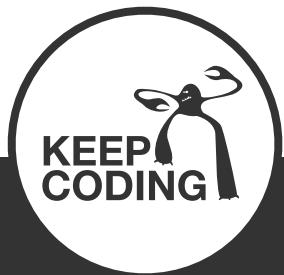
■ El mantra de TDD: Red, Green, Refactor



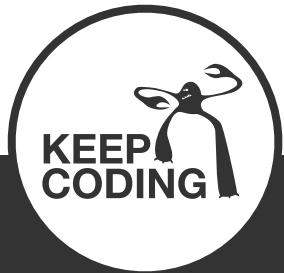
The mantra of Test-Driven Development (TDD) is “red, green, refactor.”



- Debemos escribir un test que falle.
- Es un **requisito obligatorio: el test debe fallar** al menos una vez.
- La idea es hacer que los bugs nos exploten en la cara (y no en producción).

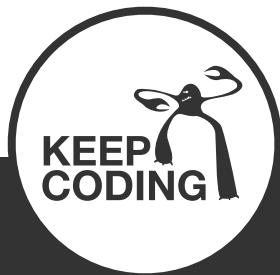


- Debemos **hacer que el test pase.**
- Incorporando el menor código posible.
- Se admiten chapuzas (ya las limpiaremos luego)



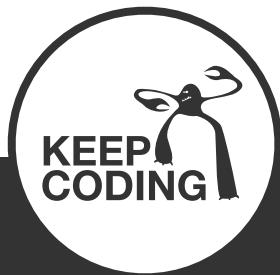
■ Refactor

- Una vez el test pasa, debemos **refactorizar** el código
- Eliminar las chapuzas
- Eliminar duplicidades de código



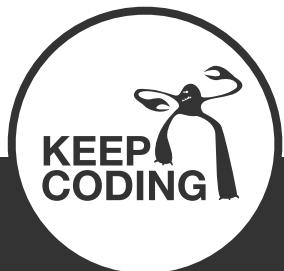
■ Características de un buen test

- Es rápido
- Es repetible: siempre obtiene el mismo resultado
- Tiene un nombre claro y explícito
- Sólo comprueba una cosa (es atómico)
- No debe depender del entorno (internet, bases de datos, etc.)



■ Tipos de tests

- **Unit tests.** Aseguran que partes individuales de la app, como funciones y clases, funcionan como se espera. Las aserciones prueban que esas partes retornan el resultado esperado para distintas entradas.
- **Integration tests.** Aseguran que la colaboración entre partes de la app es como se espera. Las aserciones pueden probar un API, UI, o interacciones que pueden tener efectos colaterales (como BD, I/O, logging, etc)
- **End-to-end tests.** Aseguran que el software en su conjunto funciona como se espera desde el punto de vista del usuario. Las aserciones principalmente prueban el interfaz de usuario.





Gracias
Javier Miguel - @javiermiguelg

