

Про node_modules

Антон Голубь

 antongolub

 antongolub





```
› jquery.min.js  
  hints.js  
  carousel.js  
  counters.js  
  script.js
```

```
<script src="./static/js/jquery.min.js"></script>  
<script src="./static/js/jquery-table-plugin.js"></script>
```

3 352 621
487 751
201 395



Получение зависимостей

```
// 1.  
function reqListener() {  
    eval(this.responseText);  
}  
const req = new XMLHttpRequest();  
req.addEventListener("load", reqListener);  
req.open("GET", "http://www.example.org/example.txt");  
req.send();  
  
// 2.  
var script = document.createElement("script");  
script.type = "text/javascript";  
script.src = "url";  
document.head.appendChild(script);
```

\$.ajax

Mithgol the
Webmaster



Коллизии в глобале

```
// <script src="./static/js/external-script.js"></script>
(function() {
  // Copypasted libs
  // jquery v1
  // ...
  // Plugins, utils, etc
  // ...
  function start() {
    $('#main').addEventListener()
  }

  $.ready(start)
  window.$ = $
})(window)
```

```
// <script src="./static/js/my-script.js"></script>
(function() {
  // Load jquery v2
  // But $ refers to v1, so, for example
  $.parseXML() // returns DOM Object instead of XMLDOMDocument
})(window)
```



Behold, node.js

Evented I/O for V8 javascript.

```
// An example of a web server written with Node
// which responds with "Hello World" after waiting two seconds:
```

```
include("/utils.js");
include("/http.js");
createServer(function (req, res) {
  setTimeout(function () {
    res.writeHead(200, {"Content-Type": "text/plain"});
    res.sendBody("Hello World");
    res.finish();
  }, 2000);
}).listen(8000);
puts("Server running at http://127.0.0.1:8000/");
```

```
// To run the server, put the code into a file
// example.js and execute it with the node program
```

```
% /usr/local/bin/node example.js
Server running at http://127.0.0.1:8000/
```

Видал Райана
Даля вживую
на Холи. У меня
даже автограф
есть

nodeJS

<https://web.archive.org/web/20091003131634/http://nodejs.org/>

[https://en.wikipedia.org/wiki/Rhino_\(Java_Script_engine\)](https://en.wikipedia.org/wiki/Rhino_(Java_Script_engine))

require

```
var sys = require('sys'),
    http = require('http');

http.createServer(function (req, res) {
  setTimeout(function () {
    res.writeHead(200, {'Content-Type': 'text/plain'});
    res.write('Hello World');
    res.close();
  }, 2000);
}).listen(8000);
sys.puts('Server running at http://127.0.0.1:8000/');
```

require

CommonJS



```
const { PI } = Math
```

```
module.exports = (r) => 2 * PI * r
```

[https://en.wikipedia.org/
wiki/CommonJS](https://en.wikipedia.org/wiki/CommonJS)

require

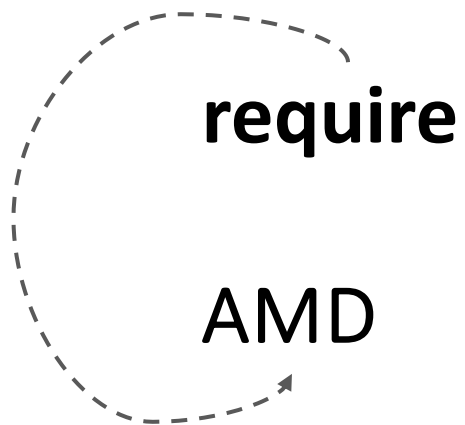
- Независимые контексты
- Кэш загрузки (мутабельный)
- Контекстно-зависимый resolve

```
import { createRequire } from 'node:module'  
const require = createRequire(import.meta.url)
```


require

```
node_modules
  a
    node_modules
      lodash@3
  b
    node_modules
      lodash@2
  lodash@4
index.js
```

```
// index.js
const _ = require('lodash')
require.cache['lodash'] // ?
```



<https://requirejs.org/>

dojo еще был,
<https://dojotoolkit.org/>

```
// foobar.js
define(["jquery"], function ($) {
  // internals
  function foo() {}
  function bar() {}
  function baz() {}

  // exports
  return {
    foo: foo,
    bar: bar,
  }
})
```

```
// some.js
define(function (require) {
  var foo = require('foo')

  return function () {
    foo.doSomething()
  }
})
```

https://en.wikipedia.org/wiki/Asynchronous_module_definition

require.js

r.js: the RequireJS optimizer, and AMD runtime for use in Node.

require.js: The browser-based AMD loader.

<https://github.com/requirejs/r.js>

<https://requirejs.org/docs/optimization.html>

Еще был steal.js,
но там перемудрили

<https://github.com/stealjs/steal>

<https://github.com/stealjs/steal-conditional>

require.js

*Notice that the above module does not declare a name for itself. This is what makes the module very portable. It allows a developer to place the module in a different path to give it a different ID/name. The **AMD loader** will give the module an ID **based on how it is referenced by other scripts**.*

```
function normalize(name, baseName, applyMap) {
  var pkgMain, mapValue, nameParts, i, j, nameSegment, lastIndex,
      foundMap, foundI, foundStarMap, starI, normalizedBaseParts,
      baseParts = (baseName && baseName.split('/')),
      map = config.map,
      starMap = map && map['*'];

  //Adjust any relative paths.
  if (name) {
    name = name.split('/');
    lastIndex = name.length - 1;
```

<https://requirejs.org/docs/whyamd.html>

<https://github.com/requirejs/requirejs/blob/master/require.js#L269>

require.js

```

//BAD
var mod = require(someCondition ? 'a' : 'b');
//BAD
if (someCondition) {
    var a = require('a');
} else {
    var a = require('a1');
}

// ...
var req, s, head, baseElement, dataMain, src,
    interactiveScript, currentlyAddingScript, mainScript, subPath,
    version = '2.3.6',
    commentRegExp = /\n\n*[\s\S]*?\n\n|([\^:"'=]|^)\n\n.*$/mg,
    cjsRequireRegExp = /[^\.]\s*require\s*\(\s*["']([\^'"\\s]+)["']\s*\)/g,
    jsSuffixRegExp = /\.js$/,
    currDirRegExp = /^\.\.\//,

// ...
callback
.toString()
    .replace(commentRegExp, commentReplace)
    .replace(cjsRequireRegExp, function (match, dep) {
        deps.push(dep);
    });

```

<https://requirejs.org/docs/whyamd.html#commonjscompat>

<https://github.com/requirejs/requirejs/blob/master/require.js#L2088>

UMD

Universal Module Definition

```
(function (root, factory) {  
  if (typeof define === "function" && define.amd) {  
    // AMD  
    define(["foo", "bar"], factory)  
  } else if (typeof exports === "object") {  
    // CommonJS  
    module.exports = factory(require("foo"), require("bar"))  
  } else {  
    // Browser globals  
    root.fooBarExports = factory(root.foo, root.bar)  
  }  
})(this, function (foo, bar) {  
  // ...  
})
```

“universal”

[https://github.com/
umdjs/umd](https://github.com/umdjs/umd)



GRUNT

— Хрю.

ESM

aka ES6 modules, native ES modules

- Независимые контексты
- Иммуutable кэш
- Иммуutable модули
- Динамические и статическая загрузка

2015

<https://hacks.mozilla.org/2018/03/es-modules-a-cartoon-deep-dive/>



ESM

«Безопасно»

- Нет моков модулей
- Никаких оверрайдов (метрики, мемоизация, дебаунсеры-тrottлеры, spyOn, пост-инит инъекты)

⚠ CAUTION

Jest ships with **experimental** support for ECMAScript Modules (ESM).

The implementation may have bugs and lack features. For the latest status check out the [issue](#) and the [label](#) on the issue tracker.

Also note that the APIs Jest uses to implement ESM support are still [considered experimental by Node](#) (as of version `18.8.0`).

With the warnings out of the way, this is how you activate ESM support in your tests.

1. Ensure you either disable `code transforms` by passing `transform: {}` or otherwise configure your transformer to emit ESM rather than the default CommonJS (CJS).
2. Execute `node` with `--experimental-vm-modules`, e.g. `node --experimental-vm-modules node_modules/jest/bin/jest.js` or `NODE_OPTIONS=--experimental-vm-modules npx jest` etc.

<https://github.com/search?q=repo%3Ajestjs%2Fjest+esm+mock&type=issues>

<https://jestjs.io/docs/ecmascript-modules>

ESM

std/esm

...esm is the world's most advanced ECMAScript module loader. This fast, production ready, zero dependency loader is all you need to support ECMAScript modules in Node 6+.

```
require = require("esm")(module/*, options*/)
module.exports = require("./main.js")
```

<https://github.com/standard-things/esm>

ESM

SystemJS

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

...is a hookable, standards-based module loader. It provides a workflow where code written for production workflows of native ES modules in browsers ([like Rollup code-splitting builds](#)), can be transpiled to the [System.register module format](#) to work in older browsers that don't support native modules...

```
System.register(['dependency'], function (_export, _context) {
  var dep;
  return {
    setters: [function (_dep) {
      dep = _dep;
    }],
    execute: function () {
      _export({
        name: 'value'
      });
    }
  };
}, /*optional metas*/ [
  /*optional meta for dependency*/ {assert: {type: 'javascript'}},
]);
```

Комбинаторная дилемма: раздельные артефакты или разделяемое содержимое



<https://2ality.com/2019/10/hybrid-npm-packages.html>

package.json

garbage.json

- Точки входа
- Зависимости
- Конфиги
- Метаинфа
- Ассерты рантайма
- Копирайты / лицензии
- Скрипты / пайплайны
- Реджистри
- ...



package entry points

```
{  
  "name": "foo",  
  "version": "0.0.0"  
}
```



```
{  
  "name": "foo",  
  "version": "0.0.0",  
  "type": "module",  
  "source": "src/foo.js",  
  "types": "./dist/foo.d.ts",  
  "exports": {  
    "require": "./dist/foo.cjs",  
    "default": "./dist/foo.modern.js",  
    "import": "./dist/foo.modern.js"  
  },  
  "browser": "./dist/foo.modern.js",  
  "main": "./dist/foo.cjs",  
  "module": "./dist/foo.module.js",  
  "unpkg": "./dist/foo.umd.js"  
}
```

<https://docs.npmjs.com/cli/v10/configuring-npm/package-json>

<https://parcel2-docs.vercel.app/configuration/package-json/>

<https://github.com/defunctzombie/package-browser-field-spec>

<https://nodejs.org/api/packages.html#conditional-exports>

package

exports & imports

```
{
  "exports": "foo.js"
}

{
  "exports": {
    "import": "./foo.js",
    "require": "./foo.cjs",
    "default": "./foo.js"
  }
}

{
  "exports": {
    "foo": {
      "import": "./foo.js",
      "require": "./foo.cjs",
      "default": "./foo.js"
    },
    "bar/*": {
      "import": "./bar/*.js",
      "require": "./bar/*.cjs",
      "default": "./bar/*.js"
    }
  }
}
```

```
{
  "exports": {
    "foo": [
      "./foo.js",
      "./foo.mjs",
      {
        "require": "./foo.cjs"
      }
    ]
  }
}

{
  "imports": {
    "#foo": "./foo.js"
  }
}
```

<https://stackoverflow.com/questions/71610111/node-package-json-export-vs-imports-fields>

<https://github.com/jestjs/jest/issues/13707>


package

полный не-JS

@types/lodash 










4.14.200 • Public • Published 3 days ago

 [Readme](#)

 [Code](#) Beta

 0 Dependencies

 10

| / @types/lodash / | | |
|---|------------------------|---------|
|  common/ | folder | 456 kB |
|  fp/ | folder | 20.6 kB |
|  LICENSE | text/plain | 1.14 kB |
|  README.md | text/markdown | 763 B |
|  add.d.ts | application/typescript | 45 B |
|  after.d.ts | application/typescript | 49 B |
|  ary.d.ts | application/typescript | 45 B |
|  assign.d.ts | application/typescript | 51 B |
|  assignIn.d.ts | application/typescript | 55 B |



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

package

императивное выполнение не-JS

```
const sh = new Proxy({}, {
  get: (_, bin) => function (...args) {
    const out = require('child_process').spawnSync(bin, args, {...this})
    return Object.assign(new String(out.stdout), out)
  }
})

const {python} = sh
const result = python('./src/py/main.py')
```

<https://www.graalvm.org/>

<https://github.com/antonmedv/tinysh/blob/master/index.js>

package

node-gyp: пост-инсталл компиляция

*Cross-platform command-line tool written in Node.js for compiling native addon modules for Node.js
“generate your projects”*

- Сборка зависимостей на стороне клиента
- Использование низкоуровневых API
- Высокопроизводительная имплементация
- Шорткат для портирования

<https://github.com/nodejs/node-gyp>

<https://blog.logrocket.com/solving-common-issues-node-gyp/>

<https://stackoverflow.com/questions/39739626/what-is-node-gyp>

<https://ru.stackoverflow.com/questions/1453109/node-gyp-что-это-и-на-что-ругается>

package

node-gyp: it's a kind of magic

package.json

```
{
  "name": "hello-world",
  "version": "0.0.0",
  "scripts": {
    "install": "node-gyp rebuild"
  },
  "gypfile": true,
  "dependencies": {
    "node-addon-api": "^7.0.0"
  }
}
```

binding.cc

```
#include <node.h>
#include <v8.h>

using namespace v8;

Handle<Value> Method(const Arguments& args) {
  HandleScope scope;
  return scope.Close(String::New("world"));
}

void init(Handle<Object> target) {
  NODE_SET_METHOD(target, "hello", Method);
}

NODE_MODULE(mybinding, init);
```

binding.gyp

```
{
  "targets": [
    {
      "target_name": "mybinding",
      "sources": [ "binding.cc" ]
    }
  ]
}
```

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

<https://github.com/nodejs/node-v0.x-archive/tree/v0.10.26/test/addons>



<https://www.npmjs.com/package/node-sass?activeTab=code>

package

node-gyp: почему python?

GYP is the only Python dependency of Node.js



<https://github.com/nodejs/node-gyp/blob/main/lib/find-python.js>

<https://gyp.gsrc.io/>

<https://github.com/indutny/gyp.js/>

package

wasm

WASI API provides an implementation of the [WebAssembly System Interface](#) specification.

WASI gives sandboxed WebAssembly applications access to the underlying operating system via a collection of POSIX-like functions

- C, Cpp, C#, Go → wat
- wat → wasm

```
import { readFile } from "node:fs/promises";
import { WASI } from "wasi";
import { argv, env } from "node:process";

const wasi = new WASI({
  version: "preview1",
  args: argv,
  env,
  preopens: {
    "/sandbox": "/some/real/path/that/wasm/can/access",
  },
});

const wasm = await WebAssembly.compile(
  await readFile(new URL("./demo.wasm", import.meta.url)),
);
const instance = await WebAssembly.instantiate(
  wasm, wasi.getImportObject()
);
wasi.start(instance);
```



<https://wasi.dev/>

<https://nodejs.dev/en/learn/nodejs-with-webassembly/>

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

<https://github.com/harryheman/Blog-Posts/tree/master/wasm-test>

https://developer.mozilla.org/ru/docs/WebAssembly/Understanding_the_text_format

package

loaders & resolvers

- Транспиляция на лету
- Кастомные провайдеры ресурсов
- Тестирование, мокирование, покрытие
- ISEC надзор
- Реинициализация контекста, hot-reload

```
NODE_OPTIONS="--loader ts-node/esm"
```

<https://github.com/nodejs/loaders>

<https://github.com/TypeStrong/ts-node>

<https://dev.to/mxfellner/dynamic-import-with-http-urls-in-node-js-7og>

package

VM

- Динамическое наполнение контекста
- Виртуальное дерево зависимостей
- Метрики ресурсов

```
// Create an initial module
const module = new vm.SourceTextModule('const a = 1;');

// Create cached data from this module
const cachedData = module.createCachedData();

// Create a new module using the cached data. The code must be the same.
const module2 = new vm.SourceTextModule('const a = 1;', { cachedData });
```

```
NODE_OPTIONS=--experimental-vm-modules
```

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

<https://nodejsdev.ru/api/vm/#vmmodule>

<https://github.com/felixge/node-sandboxed-module>

<https://snyk.io/blog/security-concerns-javascript-sandbox-node-js-vm-module/>

package

PnP

*This loader file, named **.pnp.cjs**, contains all information about your project's dependency tree, informing your tools as to the location of the packages on the disk and letting them know how to resolve require and import calls.*

```
const dynamicFsLayer = new DynamicFS();
let manager;
const defaultApi = Object.assign(makeApi(defaultRuntimeState, {
  fakeFs: dynamicFsLayer,
  pnpapiResolution: defaultPnpapiResolution
}), {
  makeApi: ({
    basePath = void 0,
    fakeFs = dynamicFsLayer,
    pnpapiResolution = defaultPnpapiResolution,
    ...rest
  }) => {
    const apiRuntimeState = typeof basePath !== `undefined` ? $$SETUP_ST
    return makeApi(apiRuntimeState, {
      fakeFs,
      pnpapiResolution,
      ...rest
    });
  },
  setup: (api) => {
    applyPatch(api || defaultApi, {
      fakeFs: defaultFsLayer,
      manager
    });
    dynamicFsLayer.baseFs = new NodeFS(fs__default.default);
  }
});
manager = makeManager(defaultApi, {
  fakeFs: dynamicFsLayer
});
```

<https://yarnpkg.com/features/pnp>

<https://raw.githubusercontent.com/yarnpkg/berry/master/.pnp.cjs>

package

PnP

- Архивы в репе
- Ломается аудит
- Отладка депсов недоступна
- Лишняя зависимость в проде

<https://github.com/pnpm/pnpm/releases/tag/v5.9.0>

Пакетные менеджеры

В чем различия?

- Протоколы доступа
- Отображение nmtree, deptree и depgraph
- Обработка ошибок
- Переопределение зависимостей
- Воркспейсы
- **Скорость работы**
- Кастомизируемость и расширяемость
- Хуки
- Кэширование
- Верификация пакетов

npm
bower
yarn
pnpm
bun
jlpm
jspm
cnpm
volt
ultra

Верификация и локфайлы

- Определяют источники
- Контрольные суммы, хэши
- Фиксируют снимок дерева
- Проецируют метаинфу

```
# THIS IS AN AUTOGENERATED FILE. DO NOT EDIT THIS FILE DIRECTLY
# yarn lockfile v1
```

```
"@aashutoshrathi/word-wrap@1.2.3":
  version "1.2.6"
  resolved "https://registry.yarnpkg.com/@aashutoshrathi/word-wrap"
  integrity sha512-1Yjs2SvM8TfLER/OD3c0jhWw0Zb58A2t7wpE2S9XfE
```

```
"@babel/code-frame@7.0.0":
  version "7.21.4"
  resolved "https://registry.yarnpkg.com/@babel/code-frame/-/code-frame-7.21.4.tgz"
  integrity sha512-13K8qGxv7KZ6Sx32Gk/diMzT13YCz3IiKUq+bq7WUyV7XpbbidQXWqZS6dSUZUj4/4N4Fk4X4DE8w+2qy"
  dependencies:
    "@babel/highlight" "^7.18.6"
```

```
"@babel/helper-validator-identifier@7.18.6", "@babel/helper-validator-identifier@7.19.1":
  version "7.19.1"
  resolved "https://registry.yarnpkg.com/@babel/helper-validator-identifier/-/helper-validator-identifier-7.19.1.tgz"
  integrity sha512-13K8qGxv7KZ6Sx32Gk/diMzT13YCz3IiKUq+bq7WUyV7XpbbidQXWqZS6dSUZUj4/4N4Fk4X4DE8w+2qy"
```

```
"@babel/highlight@7.18.6":
  version "7.18.6"
  resolved "https://registry.yarnpkg.com/@babel/highlight/-/highlight-7.18.6.tgz"
  integrity sha512-7kSAKOoOxR8xkzKzQ8o3sN46A342DyB+Oxm+vZWVzFpW94yFLZD7zuc9xtiQFQAQfqyHycUsy+bvz43g"
  dependencies:
```

<https://docs.npmjs.com/cli/v10/configuring-npm/package-lock-json>

<https://github.com/antongolub/lockfile>

Деревья

От проекции к декларации

nmtree

```
node_modules/a@0.0.1
node_modules/b@0.0.1
node_modules/a@0.0.1/node_modules/b@0.0.2
node_modules/c@0.0.1
```

deptree

```
a@0.0.1
b@0.0.1
a@0.0.1 → b@0.0.2 → c@0.0.1
```

depgraph

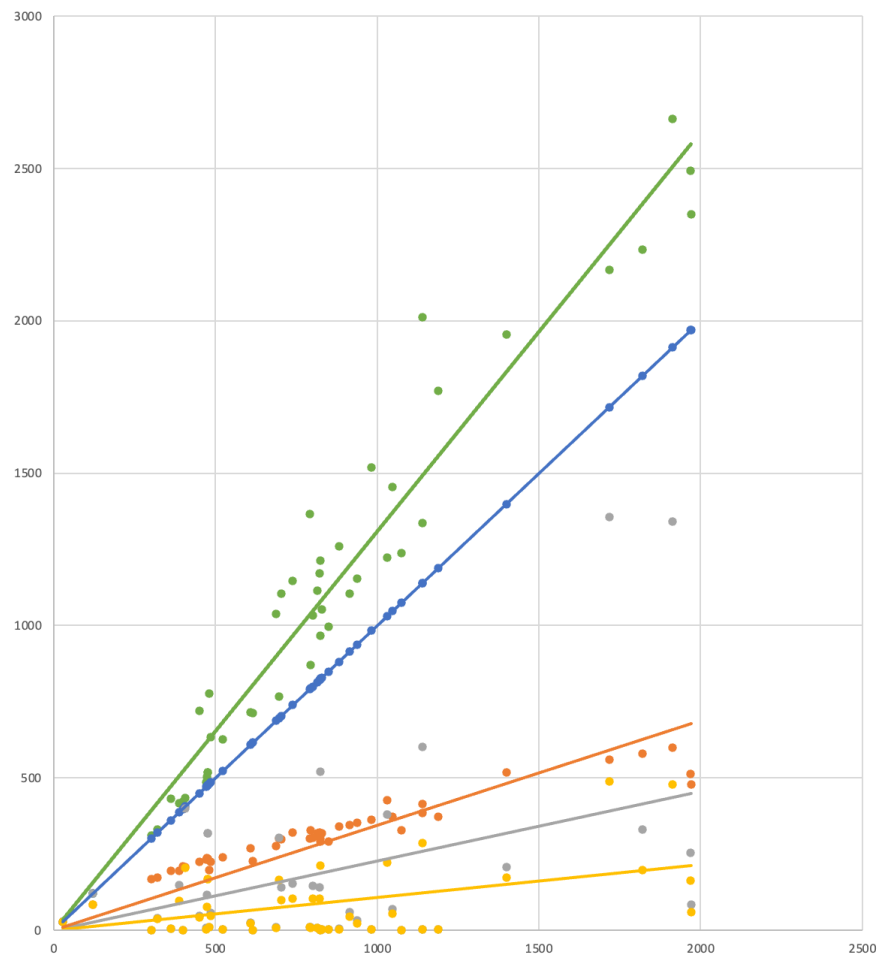
```
"" → [a@0.0.1, b@0.0.1]
a@0.0.1 → [b@0.0.2]
b@0.0.1 → [],
b@0.0.2 → [c@0.0.1]
c@0.0.1 → []
```

<https://github.com/snyk/nodejs-lockfile-parser>

<https://medium.com/helpshift-engineering/package-lock-json-the-complete-guide-2ae40175ebdd>

Деревья

Расходование ресурсов fs

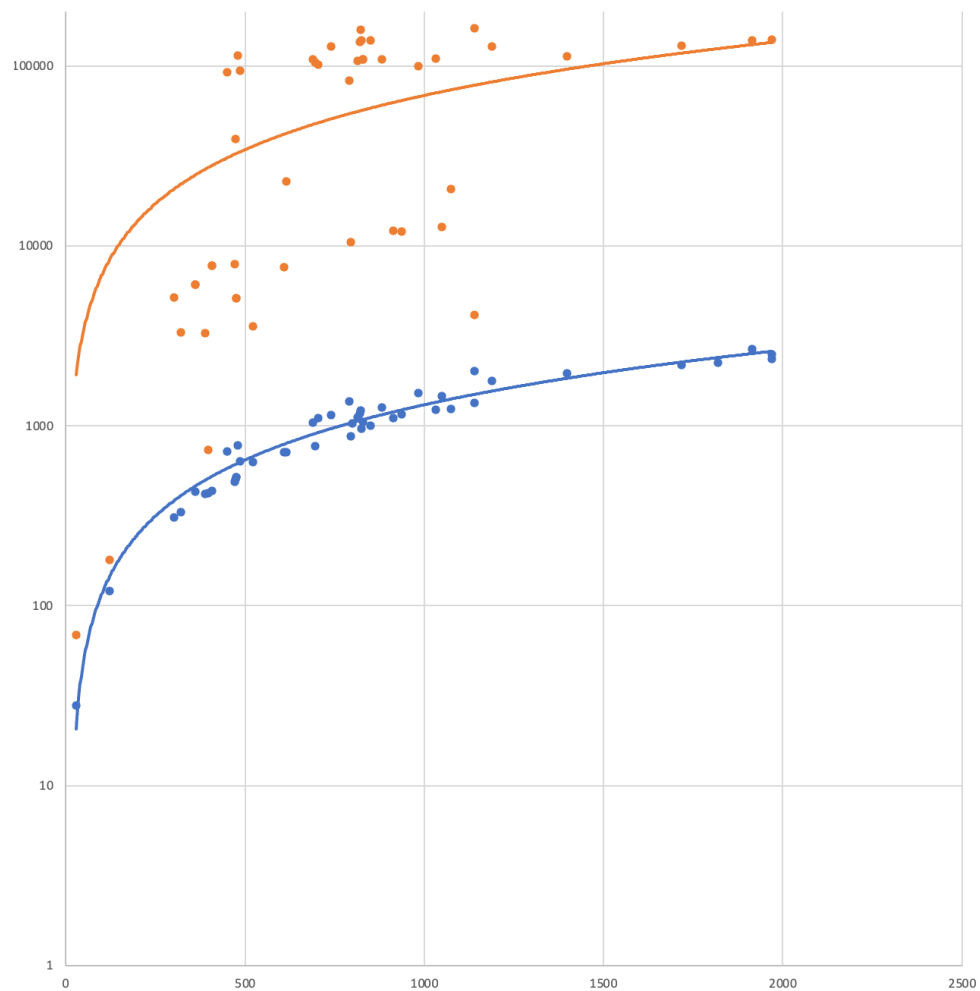


nmtree
depgraph
unique
prod
prod unique

Рандомная выборка
JS/TS репозиторийев
<https://github.com/qiwi>
<https://<nda>.qiwi.com>

Деревья

Расходование ресурсов fs



deptree
depgraph

Типы зависимостей

Границы условны

optional — отрицание

bundled — гнев

dev — торг

peer — печаль

prod — принятие

[https://github.com/npm/
npm/issues/19428](https://github.com/npm/npm/issues/19428)

[https://www.geeksforgeeks.
org/what-are-the-different-
types-of-dependencies-in-
node-js/](https://www.geeksforgeeks.org/what-are-the-different-types-of-dependencies-in-node-js/)

[https://maven.apache.org/
guides/introduction/introdu
ction-to-dependency-
mechanism.html#dependen
cy-scope](https://maven.apache.org/guides/introduction/introduction-to-dependency-mechanism.html#dependency-scope)

Типы зависимостей

prod vs dev

SPA

react → bundle
webpack polyfills → bundle

SSR

react → runtime

<https://maven.apache.org/guides/introduction/introduction-to-dependency-mechanism.html#dependency-scope>

Типы зависимостей

peer

- Снижает степень «разноверсионности»
- Обратный ход при построении дерева
- Ресолв опирается на deptime, а не nmtree

```
NODE_PATH=$(npm root -g)../my_modules/ node
```

<https://javascript.plainenglish.io/understanding-peer-dependencies-a-key-concept-in-coding-aa8507cc74ea>

<https://www.geeksforgeeks.org/difference-between-dependencies-devdependencies-and-peerdependencies/>

<https://github.com/npm/cli/blob/94f535b5d9bf912c25f08d522b3208dedb8ace0a/workspaces/config/lib/definitions/definitions.js#L1179>

https://nodejs.org/api/modules.html#modules_loading_from_the_global_folders

Типы зависимостей

bundled

- Когда bundle.js не собрать: импорты из переменных, бинарники
- Для ускорения установки

```
{  
  "name": "foo",  
  "version": "1.0.0",  
  "bundledDependencies": [  
    "bar", "baz"  
  ]  
}
```

<https://docs.npmjs.com/cli/v7/configuring-npm/package-json#bundleddependencies>

<https://github.com/npm/cli/issues/2491>

<https://github.com/pnpm/pnpm/issues/1643>

<https://www.npmjs.com/package/npm?activeTab=code>

Типы зависимостей

optional

<https://github.com/yarnpkg/yarn/issues/6487>

- Установка по условию: рантайм, архитектура, os
- Замещение peer api на advanced, если пакет доступен (console.debug → debug)

```
Yarn0076: | esbuild-linux-riscv64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-linux-s390x@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-netbsd-64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-openbsd-64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-sunos-64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-windows-32@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-windows-64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
Yarn0076: | esbuild-windows-arm64@npm:0.15.18 The darwin-arm64 architecture is incompatible with this module, link skipped.
```

Типы зависимостей

протоколы

| | | |
|------------------|--|--|
| semver | <code>^1.2.3</code> | Resolves from the default registry |
| tag | <code>latest</code> | Resolves from the default registry |
| npm | <code>npm:name@...</code> | Resolves from the npm registry |
| git | <code>git@github.com:foo/bar.git</code> | Downloads a public package from a Git repository |
| github | <code>github:foo/bar</code> | Downloads a public package from GitHub |
| github | <code>foo/bar</code> | Alias for the github: protocol |
| file | <code>file:./my-package</code> | Copies the target location into the cache |
| link | <code>link:./my-folder</code> | Creates a link to the ./my-folder folder (ignore dependencies) |
| patch | <code>patch:left-pad@1.0.0#./my-patch.patch</code> | Creates a patched copy of the original package |
| portal | <code>portal:./my-folder</code> | Creates a link to the ./my-folder folder (follow dependencies) |
| workspace | <code>workspace:*</code> | Creates a link to a package in another workspace |

<https://docs.npmjs.com/cli/v10/configuring-npm/package-json#dependencies>

<https://yarnpkg.com/protocols>

<https://v3.yarnpkg.com/features/protocols>

<https://bower.io/docs/api/>

Реджистри

GET

Meta Endpoints

GET·/

GET·-/all

```
{
  "db_name": "registry",
  "doc_count": 399172,
  "doc_del_count": 354,
  "update_seq": 3351374,
  "purge_seq": 0,
  "compact_running": false,
  "disk_size": 2118398075,
  "data_size": 1600835750,
  "instance_start_time": "1475135224217333",
  "disk_format_version": 6,
  "committed_update_seq": 3351374
}
```

Package Endpoints

GET·/{package}

GET·/{package}/{version}

GET·/{package}/{version}.tgz

GET·-/v1/search

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

<https://github.com/npm/registry/blob/master/docs/REGISTRY-API.md>

Реджистри

packument.json

- Метаданные
- Каналы (теги)
- Список всех версий и их манифесты
- Данные о публикации

```
"_id": "@ampproject/remapping",
"_rev": "37-199d3607a07a98bf2a50668d5f0411b6",
"name": "@ampproject/remapping",
"dist-tags": {
  "latest": "2.2.1"
},
"versions": {
  "0.1.0": {
    "name": "@ampproject/remapping"
```

```
"time": {
  "created": "2019-08-08T17:52:34.963Z",
  "0.1.0": "2019-08-08T17:52:35.249Z",
  "modified": "2023-07-09T22:06:24.934Z",
  "0.2.0": "2020-01-29T01:35:22.956Z",
  "0.3.0": "2020-06-13T09:17:15.752Z",
```

```
"_npmUser": {
  "name": "jridgewell",
  "email": "justin+npm@ridgewell.name"
},
```

<https://registry.npmjs.org/@ampproject/remapping>

Реджистри

PUT

```
curl -u user:password -X POST "https://<registry>" -F "npm.asset=@pkg-name-1.0.0.tgz" -v
```

<https://github.com/npm/npm-registry-client/tree/latest#clientpublishuri-params-cb>

<https://github.com/verdaccio/verdaccio/blob/master/packages/api/src/publish.ts>

<https://help.sonatype.com/repomanager3/integrations/rest-and-integration-api/components-api#ComponentsAPI-NPM>

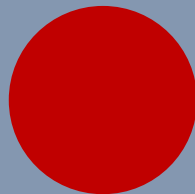
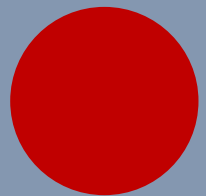
<https://github.com/taskforcesh/nandu>

Реджистри Audit

```
yarn audit --json > audit-report.txt
```

```
{
  "type": "auditAdvisory",
  "data": {
    "resolution": {
      "id": 1094415,
      "path": "prettier-config-qiwi@trivago/prettier-plugin-sort-import",
      "dev": false,
      "optional": false,
      "bundled": false
    },
    "advisory": {
      "findings": [
        {"version": "7.22.20", "paths": []},
        {"version": "7.17.3", "paths": ["prettier-config-qiwi@trivago/"]},
      ],
      "metadata": null,
      "vulnerable_versions": "<7.23.2",
      "module_name": "@babel/traverse",
      "severity": "critical",
      "github_advisory_id": "GHSA-67hx-6x53-jw92",
      "cves": [
        "CVE-2023-45133"
      ],
      "access": "public",
      "patched_versions": ">=7.23.2",
      "cvss": {
        "score": 9.3,
        "vectorString": "CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
      },
      "updated": "2023-10-20T13:27:09.000Z",
      "recommendation": "Upgrade to version 7.23.2 or later",
      "cwe": [
        "CWE-184"
      ],
      "found_by": null,
      "deleted": null,
      "id": 1094415,
      "references": "- https://github.com/babel/babel/security/advisori",
      "created": "2023-10-16T13:55:36.000Z",
      "reported_by": null,
      "title": "Babel vulnerable to arbitrary code execution when compi",
      "npm_advisory_id": null,
      "overview": "### Impact\n\nUsing Babel to compile code that was s",
      "url": "https://github.com/advisories/GHSA-67hx-6x53-jw92"
    }
  }
}
```

<https://github.com/antongolub/npm-registry-firewall/blob/master/src/main/js/firewall/plugins/audit.js>



- Error [ERR_REQUIRE_ESM]: require() of ES Module not supported
- Переполненность пакетов (bloating)
- Размытый контракт зависимостей

Ок, что делать?

- Прокси
 - Патчить пакументы
 - Патчить тарболы
- Снижать «разноверсионность»
- Depcheck
- Перенести dev & build депсы в инфраструктуру
- Свой клиент

Что дальше?

- Аудируемые реестры (tidelift?)
- npm chatgpt fix
- Инфраструктурные бустеры
- Новые протоколы доставки



EOF

Антон Голубь

 antongolub

 antongolub