UNLOCKING LOCKFILES

A DEVELOPERS GUID PACKAGE MANAGEM

Another *CodingWithCallum* ses

WHAT ARE W
COVERING?

WHAT ARE W COVERING?

- History

WHAT ARE W
COVERING?

- History
- *Fun*damentals

HISTORY LESSON

HISTORY LESSON

NEED (>201

HISTORY LESSON

NEED (>2010

- include libraries via `<script>`

HISTORY LESSON

NEED (>2010

- include libraries via `<script>`
- copypasta code from stackover

HISTORY LESSON

NEED (>201

an extremely embarrassing exa

HISTORY LESSON

BIRTH (2010

HISTORY LESSON

BIRTH (2010

- npm is created

HISTORY LESSON

BIRTH (2010

- `npm` is created
- Originally designed for No

HISTORY LESSON

BIRTH (2010

- `npm` is created
- Originally designed for No
- Created standardised regi

HISTORY LESSON

BIRTH (2010

- `npm` is created
- Originally designed for No
- Created standardised regi
- `package.json` created

HISTORY LESSON

BIRTH (2010

another... extremely embarrassing a

HISTORY LESSON

BIRTH (2010

HISTORY LESSON

BIRTH (2010

- Recursive dependency reso

HISTORY LESSON

BIRTH (2010

- Recursive dependency reso
- 🐢🐢🐢🐢

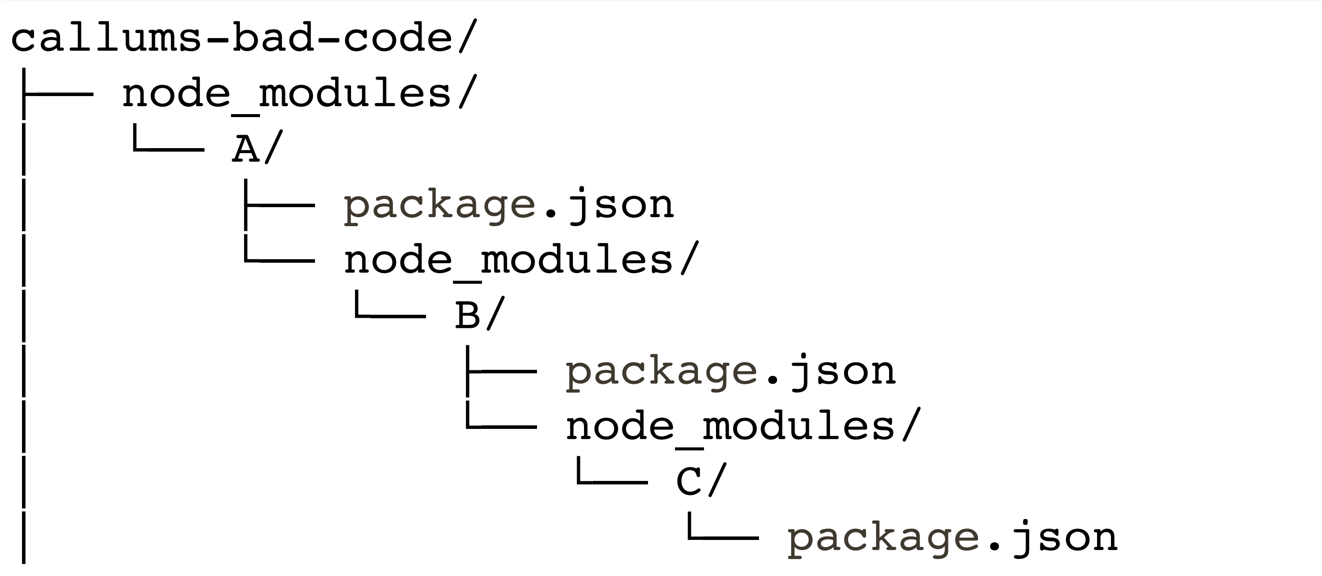
HISTORY LESSON

BIRTH (2010

- Recursive dependency reso
- 🐢🐢🐢🐢
- Nested `node_modules`

HISTORY LESSON

BIRTH (2010



```
callums-bad-code/
├── node_modules/
│   └── A/
│       ├── package.json
│       └── node_modules/
│           └── B/
│               ├── package.json
│               └── node_modules/
│                   └── C/
│                       └── package.json
│
```

HISTORY LESSON

BIRTH (2010

HISTORY LESSON

BIRTH (2010

- This was pretty revolutionary

HISTORY LESSON

BIRTH (2010

- This was pretty revolutionary
- `node_modules-black-ho`

HISTORY LESSON

BIRTH (2010

- This was pretty revolutionary
- `node_modules-black-ho`
- Poor windows

HISTORY LESSON

RISE (2012-20

HISTORY LESSON

RISE (2012-20

- Bower / RequireJS / Browserfy / Gru

HISTORY LESSON

RISE (2012-20

- Bower / RequireJS / Browserfy / Gru
- `npm` gets used for frontend things *a*

HISTORY LESSON

RISE (2012-20

- Bower / RequireJS / Browserfy / Gru
- `npm` gets used for frontend things *a*
- `node_modules` folder becomes tr

HISTORY LESSON

FLAT (2016

HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook

HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook
  - lockfiles are born

HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook
  - lockfiles are born
  - offline mode

HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook
    - lockfiles are born
    - offline mode
    - security (spoliers!)

HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook
  - lockfiles are born
  - offline mode
  - security (spoliers!)
- `npm` creates `package-lock.`

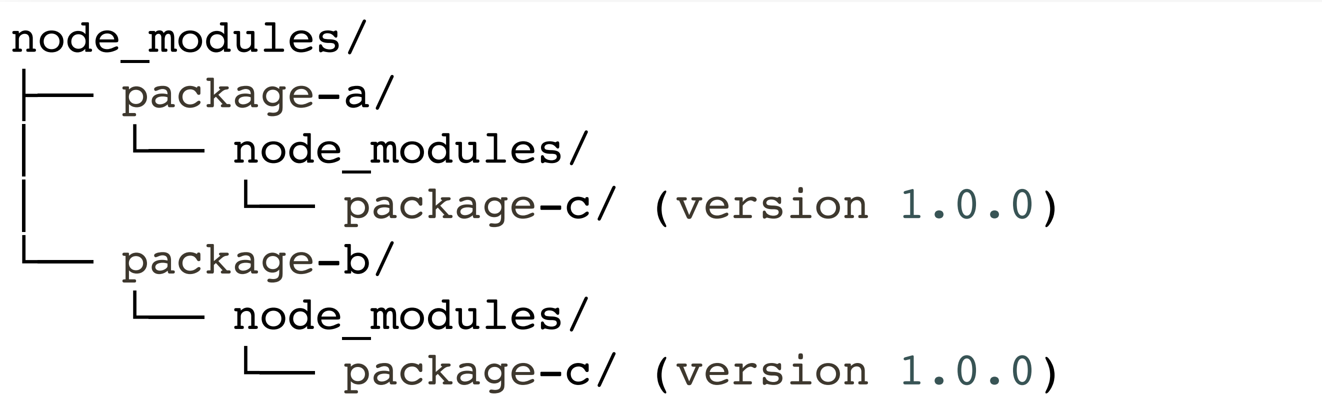
HISTORY LESSON

FLAT (2016

- `yarn` released (from Facebook
  - lockfiles are born
  - offline mode
  - security (spoliers!)
- `npm` creates `package-lock.`
- flat dependency to avoid dupli

HISTORY LESSON

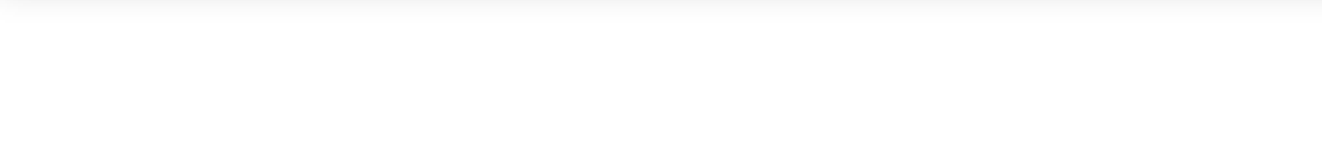
FLAT (2016



```
node_modules/
├── package-a/
│   └── node_modules/
│       └── package-c/ (version 1.0.0)
└── package-b/
    └── node_modules/
        └── package-c/ (version 1.0.0)
```

HISTORY LESSON

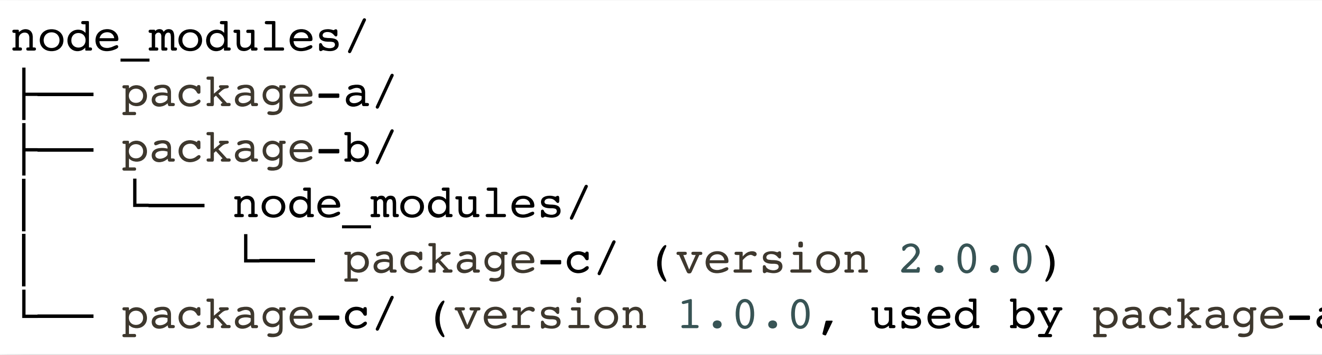
FLAT (2016



```
node_modules/
├── package-a/
├── package-b/
└── package-c/ (version 1.0.0, shared by both pa
```

HISTORY LESSON

FLAT (2016



```
node_modules/
├── package-a/
├── package-b/
│   └── node_modules/
│       └── package-c/ (version 2.0.0)
└── package-c/ (version 1.0.0, used by package-a
```

HISTORY LESSON

FLAT (2016

yarn's new security mode

HISTORY LESSON

FLAT (2016

yarn's new security mode

- checksums

HISTORY LESSON

FLAT (2016

yarn's new security mode

- checksums
- offline mode

HISTORY LESSON

FLAT (2016

yarn's new security mode

- checksums
- offline mode
- resolution

HISTORY LESSON

FLAT (2016

yarn's new security mode

- checksums
- offline mode
- resolution
- license checks

HISTORY LESSON

FLAT (2016

`yarn`'s new security mode

- checksums
- offline mode
- resolution
- license checks
- script execution

HISTORY LESSON

FLAT (2016

yarn's new security mode

- checksums
- offline mode
- resolution
- license checks
- script execution
- auditing

HISTORY LESSON

FLAT (2016

Phantom dependencies (I ain't afraid of

(Using things not listed in package

```
Your package.json: { "dependencies": { "package-
Package A's package.json: { "dependencies": { "p
```

```
node_modules/
├── package-a/
└── package-b/  (hoisted from package-a/node_mod
```

HISTORY LESSON

MODERN (201

HISTORY LESSON

MODERN (201

- pnpm created

HISTORY LESSON

MODERN (201

- pnpm created
  - content-addressable sto

HISTORY LESSON

MODERN (201

- `pnpm` created
  - content-addressable sto
  - symlink all the things

HISTORY LESSON

MODERN (201

- `pnpm` created
  - content-addressable sto
  - symlink all the things
- solved "phantom" dependen

HISTORY LESSON

MODERN (201

- `pnpm` created
  - content-addressable sto
  - symlink all the things
- solved "phantom" dependen
- `yarn` (v2 berry) releases Plug

HISTORY LESSON

MODERN (201

- `pnpm` created
    - content-addressable sto
    - symlink all the things
- solved "phantom" dependen
- `yarn` (v2 berry) releases Plug
- Deno switches to URL import

HISTORY LESSON

MODERN (201

pnpm Content-Addressable Sto

HISTORY LESSON

MODERN (201

`pnpm` Content-Addressable Sto

- Global store in `~/.pnpm-stor`

HISTORY LESSON

MODERN (201

`pnpm` Content-Addressable Sto

- Global store in `~/.pnpm-stor`
  - All packages x versions are s

HISTORY LESSON

MODERN (201

`pnpm` Content-Addressable Sto

- Global store in `~/.pnpm-stor`
  - All packages x versions are s
- Hash-based addressing

HISTORY LESSON

MODERN (201

`pnpm` Content-Addressable Sto

- Global store in `~/.pnpm-stor`
  - All packages x versions are s
- Hash-based addressing
  - Unique + Free Integrity chec

HISTORY LESSON

MODERN (201

`pnpm` Content-Addressable Sto

- Global store in `~/.pnpm-stor`
  - All packages x versions are s
- Hash-based addressing
  - Unique + Free Integrity chec
- Immutable

HISTORY LESSON

MODERN (201

pnpm Symlinks

HISTORY LESSON

MODERN (201

pnpm Symlinks

- Symlink local to the Global

HISTORY LESSON

MODERN (201

pnpm Symlinks

- Symlink local to the Global
- Strict node module structu

HISTORY LESSON

MODERN (201

pnpm Symlinks

- Symlink local to the Global
- Strict node module structu
- Multi-level linking

HISTORY LESSON

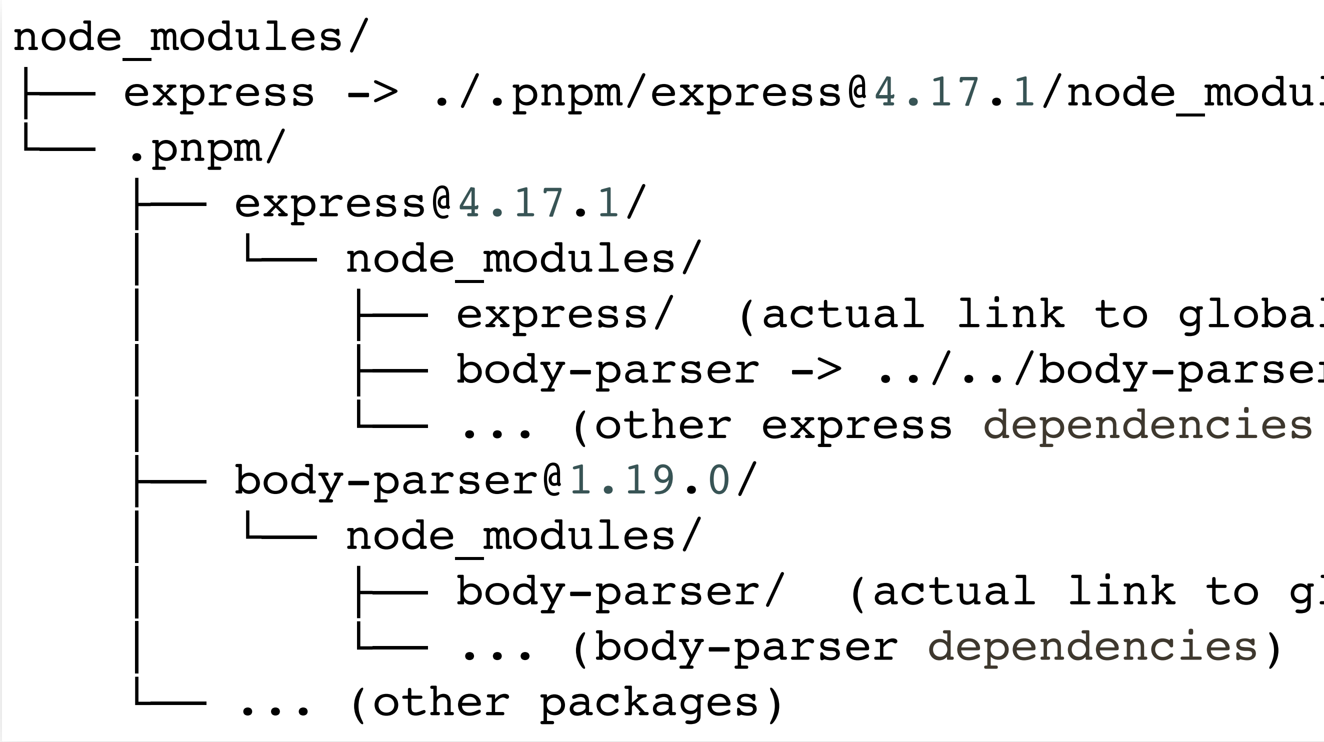
MODERN (201

`pnpm` Symlinks

- Symlink local to the Global
- Strict node module structu
- Multi-level linking
  - symlinks on top of sym

HISTORY LESSON

MODERN (201



```
node_modules/
├── express -> ./.pnpm/express@4.17.1/node_modul
└── .pnpm/
    ├── express@4.17.1/
    │   └── node_modules/
    │       ├── express/  (actual link to global
    │       ├── body-parser -> ../../body-parser
    │       └── ... (other express dependencies
    ├── body-parser@1.19.0/
    │   └── node_modules/
    │       ├── body-parser/  (actual link to gl
    │       └── ... (body-parser dependencies)
    └── ... (other packages)
```

HISTORY LESSON

MODERN (201

yarn (v2 berry) Plug'n'play

HISTORY LESSON

MODERN (201

`yarn` (v2 berry) Plug'n'play

- Solves the same problems I jus

HISTORY LESSON

MODERN (201

yarn (v2 berry) Plug'n'play

- Solves the same problems I jus
- Peer dependency issues

HISTORY LESSON

MODERN (201

`yarn` (v2 berry) Plug'n'play

- Solves the same problems I jus
- Peer dependency issues
- Zero install

HISTORY LESSON

TODAY (2024

HISTORY LESSON

TODAY (2024

- Package management is everywhere

HISTORY LESSON

TODAY (2024

- Package management is everywhere
- Security concerns are now just supp attacks

HISTORY LESSON

TODAY (2024

- Package management is everywhere
- Security concerns are now just supp attacks
- Monorepo management

HISTORY LESSON

TODAY (2024

- Package management is everywhere
- Security concerns are now just supp attacks
- Monorepo management
- The rise of bun

*FUN*DAMENTALS

*FUN*DAMENTALS

SEMVER

*FUN*DAMENTALS

SEMVER

- Basic format: `MAJOR.MINOR.PATC`
`2.3.1`)

*FUN*DAMENTALS

SEMVER

- Basic format: `MAJOR.MINOR.PATC`
`2.3.1`)
- **MAJOR:** Breaking changes

*FUN*DAMENTALS

SEMVER

- Basic format: `MAJOR.MINOR.PATC`
  `2.3.1`)
- **MAJOR:** Breaking changes
- **MINOR:** New features, no breaking c

*FUN*DAMENTALS

SEMVER

- Basic format: `MAJOR.MINOR.PATC`
`2.3.1`)
- **MAJOR:** Breaking changes
- **MINOR:** New features, no breaking c
- **PATCH:** Bug fixes, no new features o
changes

COMMON VERS
RANGES

COMMON VERS
RANGES

- Exact version: `"react": "17.0.`

COMMON VERS
RANGES

- **Exact version:** `"react": "17.0.`
  - Only use exactly version 17.0.2

COMMON VERS
RANGES

- **Exact version:** `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret (^):** `"react": "^17.0.2"`

COMMON VERS
RANGES

- **Exact version**: `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret** (^): `"react": "^17.0.2"`
  - Allow updates to any 17.x.x vers
    18.0.0 (MINOR / PATCH)

COMMON VERS RANGES

- **Exact version**: `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret** (^): `"react": "^17.0.2"`
  - Allow updates to any 17.x.x vers 18.0.0 (MINOR / PATCH)
- **Tilde** (~): `"react": "~17.0.2"`

COMMON VERS
RANGES

- **Exact version**: `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret (^)**: `"react": "^17.0.2"`
  - Allow updates to any 17.x.x vers
    18.0.0 (MINOR / PATCH)
- **Tilde (~)**: `"react": "~17.0.2"`
  - Allow updates to 17.0.x but not
    only)

COMMON VERS
RANGES

- **Exact version**: `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret (^)**: `"react": "^17.0.2"`
  - Allow updates to any 17.x.x vers
    18.0.0 (MINOR / PATCH)
- **Tilde (~)**: `"react": "~17.0.2"`
  - Allow updates to 17.0.x but not
    only)

- **Wildcard (*)**: `"react": "17.*.*` `"react": "17.*`"

COMMON VERS
RANGES

- **Exact version**: `"react": "17.0.`
  - Only use exactly version 17.0.2
- **Caret (^)**: `"react": "^17.0.2"`
  - Allow updates to any 17.x.x vers
    18.0.0 (MINOR / PATCH)
- **Tilde (~)**: `"react": "~17.0.2"`
  - Allow updates to 17.0.x but not
    only)

- **Wildcard (*)**: `"react": "17.*.*` `"react": "17.*"`
    - Any version starting with 17

UN-COMMO

VERSION RANG

UN-COMMO
VERSION RANG

- Greater than (>): `"react": ">17`

UN-COMMO
VERSION RANG

- **Greater than (>):** `"react": ">17`
  - Any version higher than 17.0.0

UN-COMMO
VERSION RANG

- **Greater than (>):** `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal (>=):** `"react`
`">=17.0.0"`

UN-COMMO
VERSION RANG

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react`
  `">=17.0.0"`
  - Version 17.0.0 or higher

UN-COMMO
VERSION RANG

- **Greater than (>):** `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal (>=):** `"react`
`">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than (<):** `"react": "<18.0`

UN-COMMO VERSION RANG

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react`
  `">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than** (<): `"react": "<18.0`
  - Any version lower than 18.0.0

UN-COMMO
VERSION RAN

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react` `">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than** (<): `"react": "<18.0`
  - Any version lower than 18.0.0
- **Range**: `"react": ">=16.0.0 <`

UN-COMMO
VERSION RANG

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react`
`">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than** (<): `"react": "<18.0`
  - Any version lower than 18.0.0
- **Range**: `"react": ">=16.0.0 <`

- Between 16.0.0 and 18.0.0 (excl

UN-COMMO
VERSION RANG

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react`
`">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than** (<): `"react": "<18.0`
  - Any version lower than 18.0.0
- **Range**: `"react": ">=16.0.0 <`

    - Between 16.0.0 and 18.0.0 (excl

- **OR**: `"react": "15.0.0 || 16`

UN-COMMO
VERSION RAN

- **Greater than** (>): `"react": ">17`
  - Any version higher than 17.0.0
- **Greater than or equal** (>=): `"react` `">=17.0.0"`
  - Version 17.0.0 or higher
- **Less than** (<): `"react": "<18.0`
  - Any version lower than 18.0.0
- **Range**: `"react": ">=16.0.0 <`

    - Between 16.0.0 and 18.0.0 (excl

- **OR**: `"react": "15.0.0 || 16`
    - Either exactly 15.0.0 or 16.0.0

*FUN*DAMENTALS

LOCKFILE

*FUN*DAMENTALS

LOCKFILE

- Locking / Freezing your dependenci

*FUN*DAMENTALS

LOCKFILE

- Locking / Freezing your dependenci
- Same immutable state of dependen

*FUN*DAMENTALS

LOCKFILE

- Locking / Freezing your dependenci
- Same immutable state of dependen
- Stop drift of dependencies between

*FUN*DAMENTALS

UPDATING T
LOCKFILE

*FUN*DAMENTALS

UPDATING TH LOCKFILE

- Install dependencies within defin

*FUN*DAMENTALS

UPDATING TH LOCKFILE

- Install dependencies within defin
  - `"react": "^18.3.1"`

*FUN*DAMENTALS

UPDATING TH LOCKFILE

- Install dependencies within defin
    - `"react": "^18.3.1"`
        - registry has `react@18

*FUN*DAMENTALS

UPDATING T
LOCKFILE

- Install dependencies within defin
    - `"react": "^18.3.1"`
        - registry has `react@18`
- Update lockfile to point to `reac`

*FUN*DAMENTALS

UPDATING T
LOCKFILE

- Install dependencies within defin
  - `"react": "^18.3.1"`
    - registry has `react@18`
- Update lockfile to point to `reac`
- `package.json` stays the same

*FUN*DAMENTALS

RENOVATE

*FUN*DAMENTALS

RENOVATE

- Update the `package.js`

*FUN*DAMENTALS

RENOVATE

- Update the `package.js`
  - Within defined range

*FUN*DAMENTALS

RENOVATE

- Update the `package.js`
  - Within defined range
- Update lockfile

PHEW

we made it

QUESTIONS

- How does `pnpm` handle `workspac` resolution?
- You didn't go into peer dependencie them?
- How is your beard not grey by now?